May 11, 2021 | CyberWise – How to Create a Strong Password

Recently, the State Department's Directorate of Cyber and Technology Security released their guidance on creating strong passwords. Considering that most Federal and contract employees continue to work remotely, continued reliance on strong passwords for both business and personal accounts is very important.

The most used passwords are extremely easy to guess and only take hackers a few seconds to crack. For example, "Admin1234" would only take 0.22 seconds to crack. By contrast, a memorable phrase such as "WherecanIfindagoodsandwich?" would take 771 years to crack with current brute force methods.

How to stay CyberWise, according to the State Department:

- When possible, use your PIV or multi-factor authentication.

- Use different passwords for different accounts. If you are reusing a password on multiple accounts and a hacker cracks one of them, they may try the recovered passwords on your other accounts too.

- Do not include personal identifiers like your phone number, name, child or pet's name, or birth date, especially for those who were affected by the OPM breach in 2015 – this information is already on the Dark web.

- Avoid selecting commonly used words (e.g., colors, fruits, animals, days) or phrases (e.g., "Password1234," "DOSadmin1"). Password cracking tools include dictionary-based testing capabilities.

- Do not use repetitive characters or patterns (e.g., "0000," "1234," "aaa," or "7878").

- Consider using a unique passphrase that is easy to remember or picture in your mind, but difficult to guess. According to the National Institute for Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible.

May 3, 2021 | CyberWise – Scams Involving Fictitious Taxes Owed and "Secret Federal Accounts" Are on the Increase

Back in March 2016, the Federal Reserve Bank of New York became aware of a scam wherein fraudsters claiming to be from the Federal Reserve contacted the public through unsolicited phone calls claiming the individuals owed back taxes. The fraudsters tried to scare the victims by threatening to have the them or their family members arrested for not paying these undocumented or imaginary back taxes. The fraudsters demanded immediate payment through prepaid debit cards and often tried to elicit other personal information from the victims.

In a recent post of scams involving the Federal Reserve name, the Federal Reserve Bank of New York documents how scammers have evolved and are claiming that secret accounts are held by the Federal Reserve for every citizen since birth, and now is a good time to tap into those fictitious monies using the Fed's routing numbers. In fact, use of those routing numbers is a Federal offense, and can lead to prosecution of the unwitting victim.

While those scams involve fictitious Federal Reserve agents, other efforts involve scammers identifying themselves as IRS agents. The IRS highlighted this attack on their website back in 2013. In yet another version of this scam, the bad actors claimed to be from the Federal Reserve's Office of the Inspector General (OIG) claiming to be in possession of ATM cards that can be sent to the victim after paying certain fees via gift cards; the FRS OIG have guidance about this attack on their fraud and scams website. Given last year's and this year's increased scamming efforts while we work from home, we all remain targets.

Please remember to be Cyber-Wise:

- Be suspicious of all unsolicited calls and emails. You are safer to just not answer if you have doubts. If someone really needs to contact you, they will leave a non-automated message.

- No Federal agency will contact you via unsolicited phone calls or e-mails asking for or demanding money or request any other type of personal information.

- Never provide credit card, debit card, or other financial information over the phone or by email to an unsolicited, unknown, or new contact.

- Never provide or confirm personal information to an unsolicited phone call or email - if you don't know who they are, then deny or at least delay to a later date, any request for financial and personal information.

- If you receive such a call, report the matter to the Federal Trade Commission using its FTC Complaint Assistant.

- If you wish to report scams that fraudulently use the name of the Federal Reserve OIG, contact the OIG Hotline.

April 27, 2021 | CyberWise- 88% Of Data Breaches Are Caused by Human Error

Researchers from Stanford University and a top cybersecurity organization found that human error is the driving force behind the overwhelming majority of cybersecurity problems, with approximately 88 percent of all data breaches are caused by employee mistakes.

Other interesting report findings include:

- Nearly 45% of respondents cited distraction as the top reason for falling for a phishing scam.
- 57% of remote workers admit they are more distracted when working from home.
- The top reasons for clicking on phishing emails are the perceived legitimacy of the email (43%) and the fact that it appeared to have come from either a senior executive (41%) or a well-known brand (40%). (See our CyberWise tip on identifying phishing red flags).

Tips to avoid a potential data breach:

- STOP. THINK before you CLICK. Do not click any links or attachments that are included in a suspicious email. Avoid emails that insist you act now. A common manipulation tactic malicious actors use is to create a sense of urgency or demand immediate action.

• Report phishing attempts by using the “report phishing” button in your Outlook application or forward the email as an attachment to [redacted] (b) (6)

• If you believe you are a victim of a data breach on your CFPB device or involves CFPB data , you can report it to our [redacted] (b) (6)

• If you believe you are a victim of a data breach on your personal device (non-government issued laptop, cell phone, etc), you can report it to the Federal Trade Commission by visiting www.ftc.gov/complaint. Check out the full " “Psychology of Human Error” Could Help Businesses Prevent Security Breaches article from CISOMag to learn more.

April 23, 2021 | CyberWise – Credential harvesting attacks targeted against U.S. federal agencies are on the rise

Mobile security vendor, Lookout, recently released its U.S. Government Threat Report, highlighting new problems arising from increased mobile use by government employees. The increased use and reliance on mobile devices has generated substantial security implications for Government organizations. A key area of concern is just how “security-aware” employees are when the access systems, applications, and data from their mobile devices that may be cloud-based and not necessarily secured within a government-hardened network. This is especially seen as the use of personal devices increases/ According to the report, 91% of mobile devices used by federal employees are unmanaged, and the exposure to mobile phishing attacks on unmanaged devices is nearly 8 times greater than managed devices.

The report also states:

- In 2020, 71.5% of phishing attacks were focused on harvesting, a 67% increase over 2019
- In the same timeframe, only 28.5% of phishing attacks delivered malware, a decrease of 50% over 2019. (See CyberWise- What is malware?)

How can you protect your devices?

- Physical security. NEVER leave your device unattended in public. Access to a device makes it easier for an attacker to extract or corrupt information.
- Secure Browsing. Only use sites that begin with “https://” when online shopping or banking.
- Use strong passwords. Create passwords difficult for malicious actors to guess (Pro tip: do not use any words found in the dictionary), and use different passwords for different accounts, services, devices. (See Cyber Wise Tips to Protect your ID and Passwords Online)
- Disable remote connectivity. Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.
- Use Public Wi-Fi with caution. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, while connected to a public wireless (Wi-Fi) network.
- If you suspect you have been the victim of an incident, report it to [redacted] (b) (6) immediately.

Check out our CyberWise archive to learn more about mobile device cybersecurity.

April 20, 2021 | CyberWise – FBI 2020 Internet Crime report released; losses exceed $4.2 Billion

The FBI 2020 Internet Crime Report includes information from 791,790 complaints of suspected internet crimes—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion.

The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Notably, 2020 saw the emergence of scams exploiting the COVID-19 pandemic. The FBI received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals.

With the release of the report, the FBI is reminding the public to immediately report suspected criminal internet activity to the FBI at ic3.gov. By reporting internet crime, victims are not only alerting law enforcement to the activity but aiding in the overall fight against cybercrime.

If you suspect you have received a malicious email from a spoofed email address on your CFPB devices, report it using the "report phishing" button in your Outlook application or forward as an attachment to (b) (6)
Check out the 2020 Internet Crime Report to learn more about the 2020 Internet crimes.

April 13, 2021 | CyberWise – Beware of Smishing

Did you know that about 87% of all phishing attacks on mobile devices use messaging, gaming and social media apps? Most people don't and cybercriminals take advantage of this to lure us via texts to steal our personal information or infect our smartphones to get access to it. Once they succeed, they can easily steal our money, information or identity. And if you use your smartphone for work related issues, smishers can also get access to your business accounts or information, which means even more problems!

Examples of Smishing:

- Text message alert (allegedly from your 'bank'), saying there was a large transfer done from your account and that you need to call a certain number to block the fake transfer. If you call, you will be asked to confirm your personal and banking information, after which your money will disappear faster than you can hang up!
- Unsolicited text message with your personal information (date of birth, social security number, account number) to convince you it's legitimate
- A link that takes you to a website asking to enter your personal details, very often stating failure to do so will result in additional services charges and fees
- Link to download an app (which is usually malware)
- Message about transferring money to charity or an entity overseas that needs your help, ASAP.

How to Protect Yourself Against Smishing

- Be suspicious of unsolicited SMS messages from unknown numbers being sent to your CFPB mobile phone
- Do not click on any links sent via SMS originating from an unknown number
- Smishing attacks will generally attempt to instill a sense of urgency to rush the user into making a mistake

• A generic salutation like "Dear Customer" from an unknown number is usually a sign the text message might be malicious
• Advanced attacks might include personal information that can be found easily on the internet
• Check out the CFPB Security training wiki page to learn how to report a Smishing attack.

April 09, 2021 | CyberWise – Beware of Trickbot Malware

Malicious actors have launched a new phishing campaign that claim to contain proof of a traffic violation. The email contains a link that sends users to a website, the victim to click on a photo to see proof of their violation. Once the user clicks the photo, a files gets downloaded to their computer that, when opened, installs Trickbot onto their system.

How to avoid falling for the Trickbot phishing attempt:

• Stay vigilant regarding attachments and links within emails. Malicious emails or phishing usually have red flags. Be sure to use your mouse button to hover over the links to see where it leads.

• STOP**. THINK before you CLICK.** Do not click any links or attachments that are included in a suspicious email. Check the email address or link. Sometimes, it's obvious the web address is not legitimate when hovering over it. Keep in mind phishers can create links that closely resemble legitimate addresses.

• Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.

• Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete or report the message.

• If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your Outlook application or forward as an attachment to [redacted] (b) (6).

See CISA's Security publication Avoiding Social Engineering and Phishing Attacks for more ways to detect and avoid phishing efforts.

April 06, 2021 | CyberWise – Beware of Tax scams

It's that time of year again — **tax time**. Tax season can be a stressful time for many Americans and scammers know this. Bad actors are waiting for you to slip up so they can steal your personal information, money and identity. However, there are simple, actionable steps you can take to stay one step ahead of any tax scammer. The National Cyber Security Alliance and the Internal Revenue Service (IRS) have published a new tip sheet Stay Safe Online During Tax Time, to promote online safety practices this tax season.

Tips to stay safe online:

• Lock down your login & utilize multi-factor authentication
• Keep software updated on personal devices. Within CFPB device settings, you have the ability to turn on a feature that notifies you when a system patch has become available.

- Beware of public Wi-Fi & use a Virtual Private Network (VPN) whenever possible. CFPB laptops use Always on VPN, which allows Bureau users to work more efficiently regardless of location. If you have a CFPB laptop and an internet connection, then you are automatically connected to the CFPB VPN. It's a more secure and consistent experience from any location.

Check out additional resources to help you stay safe, avoid scams, prevent identity theft.

April 01, 2021 | CyberWise - How to stay safe online – in the pandemic and beyond

Follow these top tips to stay safe online to protect both yourself and your CFPB network.

- **Never share personal details** Keep your full name, date of birth, and other personal information private; never post personal information in public and check your privacy settings on any website for which you have an account- especially social media sites- to check your information is secure.
- **Watch out for scams** 2020 saw an explosion in health-related social engineering attacks, as criminals tried to leverage peoples' fears around coronavirus and desperation for a vaccine. Be sure to check the sender's email address and any links they ask you to click; and if you can, navigate to the relevant website yourself.
- **Choose a strong passphrase** Don't reuse the same password or passphrase between sites or accounts. Be sure to never share it with anyone else and avoid storing it or leaving yourself logged in on shared devices.
- **Keep your device secure** While using your CFPB work-supplied laptop or device, continue to ensure the Always on VPN (AOVPN) is in use. For personal devices, try and utilize a VPN and set up two-factor authentication for as many of your online accounts as possible.

To learn more check out this here's how to stay safe online – in the pandemic and beyond article published by the National Cybersecurity Alliance.

March 31, 2021 | CyberWise - Angler phishing

Email is the most common way to be on the receiving end of a phishing attack, but it's certainly not the only way. There's also angler phishing. Angler phishers use social media to target you, often impersonating real brands and extracting personal information from you under the guise of customer service. Next time your favorite National Pizza tries to help you with a pizza order in response to your disgruntled tweet, take a second to double-check whether that's really @nationalpizza and not @nationalpizzaplace. (Hint: look for that blue checkmark to confirm the account is verified).

Recommendations to avoid these threats:

- Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB email Address
- Watch out for vague language or a generic request to click on a link or enter information
- Call the individual personally if possible, to see if the message was legitimate
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "Report phishing" button in outlook or send as an attachment to (b) (6)

Check out the recently published Phishing: Staying Off The Hook article by Living Security, a cybersecurity training platform, to learn more.

March 26, 2021 | CyberWise - Stop & think, before clicking email attachments

While email attachments are a popular and convenient way to send documents, they are also a common means for transmitting cyber viruses. Use caution when opening attachments, even if they appear to have been sent by someone you know. Some of the same characteristics that make email attachments convenient and useful for collaborating with colleagues also make them a popular tool for cyber attackers. Email is so easily circulated – forwarding email is so simple that viruses can quickly infect many machines. Most viruses do not even require users to forward the email—they scan a users' mailbox for email addresses and automatically send the infected message to all the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open a message that comes from someone they know.

Steps to protect yourself and others in your address book

- **Be wary of unsolicited attachments, even from people you know.** Just because an email message looks like it came from someone you know does not mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, call the person who supposedly sent the message to make sure it's legitimate before opening.

- **Keep software up to date.** Install software patches so attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it. (see Understanding Patches and Software Updates for more information)

- **Trust your instincts.** If an email or attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the antivirus software might not have the signature. At the very least, contact the person who supposedly sent the message to make sure it's legitimate before you open the attachment. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.

- **Stop. Think before you click.** Do not click on unknown links in messages. Report suspicious activity by clicking the **"Report Phishing"** button in Outlook or sending screenshots of any social media contacts as an attachment to (b) (6)

March 25, 2021 | CyberWise - COVID-19 Vaccine Social Engineering Scams

Be aware of COVID-19 vaccine social engineering attempts. Social engineering attacks come in many forms, but phishing remains the main method, with attempts increasing 26% from October 2020 to January 2021. Federal agencies such as the Federal Bureau of Investigation (FBI), Department of Health and Human Services, and Centers for Medicare and Medicaid Services say hackers are using the public's interest in COVID-19 vaccines to obtain personally identifiable information (PII) and money through various schemes.

To guard against COVID-19 vaccine scams, do the following:

- Beware of offers for early access to the COVID-19 vaccine that require a fee or deposit as well as advertisements for vaccines through social media platforms, email, phone calls, or from unsolicited/unknown sources. The vaccine is not for sale and is only available at locations approved by federal, state, and local authorities.
- **STOP. THINK before you CLICK.** Watch out for unexpected emails (phishing) or text messages (SMiSing) that contain attachments or links, especially those related to the vaccine. Do not click any links or attachments that are included in a suspicious email. Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Keep in mind social engineers will create links that closely resemble legitimate addresses. LOOK CLOSELY!
- If you believe you are being targeted by a phishing or smishing campaign, please do not open the attachment – Click the "Report phishing" button in outlook or send as an attachment to (b) (6)

Only use trusted sources for coronavirus information and guidance such: CFPB guidance pages, Centers for Disease Control, and Prevention World Health Organization Federal Trade Commission scam alerts.

March 17, 2021 | CyberWise: St. Patrick's Day Adventure

Malware is malicious (purposefully harmful) software. There are many software programs that carry out malicious activities such as viruses, worms, ransomware, rootkits, and logic bombs.

Play along with a fun chose your own adventure video created by InfoSec Institute, to see if you can defeat the malware zombies!

March 12, 2021 | CyberWise - What's reverse social engineering?

Reverse social engineering occurs when malicious actors invent a problem, then contact an end-user posing as the friendly helper. They usually create a scenario where the end-user contacts them (See What is reverse social engineering? And how does it work?). They know that making the one with the problem will make you more eager to share information or perform actions in exchange for assistance.

Here's an example. You're working from home one morning and your work phone rings. *"Hey, it's Bill from Living security company I'm just calling to ask if you've noticed any suspicious activity on your work computer recently? We've had a few team members open a forwarded email containing malware and they're spreading it around like it's COVID!"* You tell him no but ask what the email was about. He makes up some fake email message (that he knows you wouldn't have received because it never went out...yet).

"Anyways," Bill says, "Just watch out for that message and if you get a weird email, call me at XXX-XXX-XXXX. Trust me, you don't want this crap on your computer. It's putting people out for days and getting people in hot water with management." A few days pass. You check your email shortly before lunch and see a funky email. You figure it's best to call Bill since you can't afford to be computer-less a few days and the last thing you need is to tick off your boss.

How to avoid falling for reverse social engineering tactics:

- Stay vigilant regarding the attachments and links within emails. Be sure to use your mouse button to hover over the links to see where it leads. Malicious emails or phishing usually have red flags.

- Beware of online requests for personal information. An email or online request that seeks personal information like your Social Security Number (SSN) or login information is likely a scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.

- Look for generic greetings. Phishing emails or vishing calls are unlikely to use your name. Greetings like "Dear sir or madam" signal this is not a legitimate actor.

- **STOP. THINK before you CLICK**. Do not click any links or attachments that are included in a suspicious email. Avoid emails that insist you act now. A common manipulation tactic malicious actor use is creating a sense of urgency or demand immediate action.

Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind social engineers can create links that closely resemble legitimate addresses.

- If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your Outlook application or forward as an attachment to [redacted] (b) (6)

Check out the full Livingsecurity blog Social Engineers: Wolves in Sheep's Clothing to learn more about social engineering exploits in action.

March 10, 2021 | CyberWise - Don't Share Passwords

Not only is sharing passwords is extremely unsecure. There are a few scenarios where you might want to, but here's why you don't share passwords. No amount of promises will ensure that a shared password doesn't get re-shared, and shared again, until your second uncle once removed has access to all your baby pictures online AND your Netflix account. This is the easiest way to lose control not only of your passwords but also of things random people know about you. And the more they know about you, the more vulnerable you become. Vulnerability is exactly what cybercriminals excel at exploiting.

You may want someone to have access to an app you like or to a utility bill you both pay. If this is the case, see if there is a way to help them create an account of their own. Most services which allow sharing, have this option available. That way, you keep positive control over your account, password and online safety. Using a password manager is another way to deal with it. Those useful programs have an option of sharing credentials without disclosing them to the person you want to share them with. Isn't it just a perfect solution, not only in your personal life, but also at the workplace, where sharing passwords is a common problem, which may lead to serious breaches.

Check out this Sharing isn't always caring article by LivingSecurity to learn more.

March 05, 2021 | CyberWise- What COVID-19 teaches about Cyber Hygiene

Fight Cyber Viruses the Way We Fight COVID-19

Living Security, a cybersecurity training platform, recently published an article that explains the impact of malicious software and how we can apply the lessons learned from COVID-19, to effectively fight computer viruses and malware.

COVID-19, like all biological viruses, spread quickly and cause harm. The word virus comes from a root word meaning 'poison,' and this poison is good at only one thing: attacking the protection mechanism of its host. Cyber viruses act in the same way as a biological virus like COVID-19.A cyber virus attacks its host, does not discriminate, and spreads fast.

Hygiene and Cyber Hygiene

"Wash your hands, cover your mouth when you sneeze, stay at home when you are unwell" – these are just some of the recommendations from the World Health Organization to combat and mitigate the risk of getting and spreading COVID-19. These are simple measures, but not necessarily easy in practice. In the cyber world, there are some very similar tips we should follow to maintain our computing systems health and improve our online security. We often neglect them because they take a little extra time. But when we embrace them, we develop a cyber immune system that is hard to beat.

Cyber hygiene recommendations:

- Utilize multi-factor authentication (MFA). Using MFA requires two different methods of authentication in order to gain access.
- Use strong and complex passwords.

(b) (5)

- Back up your data regularly using either physical devices and/or cloud storage resources
- Only connect to trusted Wi-Fi (not public Wi-Fi or your neighbor's Wi-Fi) and use a VPN wherever possible. CFPB laptops uses AOVPN, which allows Bureau users to work more efficiently regardless of location. If you have a CFPB laptop and an internet connection, then you are automatically connected to the CFPB VPN.
- Disable or delete unused and unnecessary features and applications. Mobile devices can come with a variety of services such as remote access, often enabled by default. If you don't need it, be sure to disable it.

For more information visit: www.stopthinkconnect.org and Living Security's blog homepage.

March 04, 2021 | CyberWise tip- Beware: Telephony Denial of Service (TDoS) Attacks Can Disrupt Emergency Call Center Operations

What is A TDoS Attack?

The Federal Bureau of Investigation recently issued a Private Industry Notification to provide awareness regarding Telephony Denial of Service attacks. TDoS attacks affect the availability and readiness of 911 call centers and can undermine public trust in emergency services. A TDoS attack is an attempt to make a telephone system unavailable to the intended user(s) by preventing incoming and/or outgoing calls. The objective is to keep the distraction calls active for as long as possible to overwhelm the victim's telephone system, which may delay or block legitimate calls for service. Hacktivists occasionally use TDoS attacks to annoy and harass a targeted agency. Malicious actors have previously used TDoS attacks as part of ransom demand by conducting a short TDoS against the targeted agency, then demanding payment to stop the TDoS. Occasionally, TDoS attacks are accidental, such as a mistake in a text message phishing (SMSishing) campaign that inadvertently directs respondents to call 9-1-1. Historically, malicious cyber actors used TDoS attacks to prevent a target from receiving notification of a pending, unauthorized financial transfer.

Recommendations during a TDoS Attack

Save the voice recording of suspects who may call before, during or after the TDoS attacks. All suspicious activity should immediately be reported to the CFPB SOC team by forwarding the voicemail as an attachment to (b) (6) Check out the Cybersecurity wiki page for more in-depth vishing guidance linked here.

February 26, 2021 | CyberWise- What is Cybercrime?

Cybercrime is criminal activity that targets or uses a computer, a computer network, or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Some organized attackers utilize advanced techniques and are highly technically skilled while others are novice hackers. Cybercriminals are increasingly targeting U.S. critical infrastructure to generate profit, whether through ransomware, e-mail impersonation fraud, social engineering, or malware. (See CyberWise: Social Engineering 101). Victims of cybercriminal activity in 2018 reported over $2.7 billion in losses—more than twice the amount lost in 2017. This number does not represent the full scope of loss because some victims do not report incidents.

Ransomware attacks—which have at least doubled since 2017—are often directed against critical infrastructure entities at the state and local level by exploiting gaps in cybersecurity. (See CyberWise Tip- Ransomware explained).

Tips to stay safe against cybercrime:

- Watch out for vague language or a generic request to click on a link or enter information.

- Be vigilant with attachments and links in emails. Think twice before clicking on links found in emails, especially if you don't know the sender. Be sure to STOP and THINK before you CLICK. Do not click any links or attachments that are included in a suspicious email.
- If you believe you are being targeted by a malicious cyber-attack, immediately report the suspicious email by clicking the "Report Phishing" button for Windows users or forwarding the email as an attachment to (b) (6)

To learn more, check out the DHS's Homeland Threat Assessment published in October 2020.

February 25, 2021 | CISA Launches Campaign to Reduce the Risk of Ransomware

Ransomware is a form of malware designed to encrypt the victim's files and then demand ransom in exchange for decrypting the files. In recent years, the number of ransomware attacks have increased across government entities and critical infrastructure organizations, and have become more destructive and financially damaging, with some demands exceeding US $1 million. Cyber criminals continually adjust their tactics to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as another form of extortion. Malicious actors use tactics, such as deleting system backups, that make restoration and recovery more difficult, if not feasible for impacted organizations.

The following resources provide useful information in the fight again ransomware:

- Alerts and Statements:

For official CISA updates to help guard against the ever-evolving ransomware threat environment. (See Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data)

- Guides and Services:

Tips and best practices for home users, organizations, and technical staff to guard against the growing ransomware threat. (See Ransomware: What It Is & What To Do About It)

- Fact Sheets and Infographics:

Easy-to-use, straightforward information to help organizations and individuals better understand the threats from and the consequences of a ransomware attack. (See CISA Fact Sheet on Cyber Threats to K-12 Remote Learning Education for non-technical educational professionals with contributions from the FBI)
Trainings and Webinars: This information provides technical and non-technical audiences, including managers, business leaders, and technical specialists with an organizational perspective and strategic overview. (See Combating Ransomware Video)

How to protect against ransomware

- Keep applications and operating systems up to date on Bureau laptops, personal computers, and mobile devices.

- Be vigilant regarding the attachments and links you decide to click on within emails. Malicious emails or phishing usually have red flags. For example, you can inspect a link or email address by hovering your mouse button over the link to see where it leads. Sometimes, it's obvious the web or email address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.

● Please do not open the attachment or click a link if you believe the email to be malicious – Click the "report phishing" button in Outlook or send the email as an attachment to [redacted] (b) (6)

• Use multi-factor authentication (MFA) for accounts whenever available. Multi-factor authentication (sometimes called two-factor authentication) works by requiring two different methods to authenticate the user. It is highly recommended that MFA is used for critical services, such as logging into email accounts, online banking, or storing files online as it's a more secure solution than using just passwords. Learn more about MFA from our Cyber Tip of the week archive.

• Back it up early and often. Protect your work, images, and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.

• If you believe you are being targeted by ransomware or any malicious cyber-attack, please contact [redacted] (b) (6) or [redacted] (b) (6)

Check out our Cybersecurity Tip of the week page for more ransomware best practices and the Ransomware Guide available on CISA's website at www.cisa.gov/publication/ransomware-guide. Feel free to also see our previous Cyber tip of the week for full guidance on how to protect against ransomware CISA established a new one-stop resource at cisa.gov/ransomware. To learn more check out this Ransomware fact sheet published by the Internet Crime Complaint Center (IC3).

February 19, 2021 | Different Phishing Attacks to Know and Beware of

CISO Magazine recently published a fun Five Baits that get you phished infographic

1) Spear Phishing A highly targeted form of phishing. Spear phishing involves hackers sending tailored and personal emails to well-researched victims purporting to be a trusted sender. Spear phishing attacks are hard to spot without close inspection and difficult to stop with technical controls alone. While regular phishing campaigns go after large numbers of relatively low-yield targets, spear phishing aims at specific targets using specially emails crafted to their intended victim. Some targeted spear phishing attacks involve documents containing malware or links to malicious web sites to steal sensitive information or valuable intellectual property, or to simply compromise payment systems. Watch out for spear phishing & whaling attacks CyberWise tip).

2) Whaling Like spear phishing, except attackers go after authoritative leaders within the organization, i.e. the big fishes/whales. This kind of attack often involves the attacker impersonating or pretending to be a senior executive in the organization Watch out for spear phishing & whaling attacks CyberWise tip).

3) Business Email Compromise Business Email Compromise (BEC) attacks are a sophisticated type of scam that target both businesses and individuals with the aim of transferring funds from victims' bank accounts to criminals. The FBI's 2019 Internet Crime Report states that the total annual losses generated by BEC in the US alone reached $1.7 billion. BEC scams also accounted for half of all cybercrime losses in the US in 2019, making BEC the #1 cyber threat in terms of economic damage. (See Beware of Business Email Compromise Attacks)

4) Vishing A combination of the words voice and phishing, vishing is the telephone equivalent of email phishing. Vishing is a form of criminal phone fraud, using social engineering over a telephone system to gain access to private, personal, and financial information to steal identities, money, or access. Vishing is not a legitimate attempt to sell you a product or service – more often referred to as spam. Vishing is a scam. (See What is Vishing?)

5) Smishing SMiShing or SMS phishing is about sending fake text messages, claiming the mobile user that they have won a free product or needs to complete a specific action. Within the fake text message, there is typically a fake URL link that would lure the individual into clicking the link. After the user has clicked the link, that is when the hacking starts. (See How to avoid SMiShing attempts)

Recommendations to avoid this threat:

- Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address
- Watch out for vague language or a generic request to click on a link or enter information
- Call the individual personally if possible, to see if the message was legitimate
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the “Report phishing” button in outlook or send as an attachment to [redacted] (b) (6)

February 18, 2021 | CyberWise Tip- What is Social Engineering?

Social engineering is when a cybercriminal obtains access, information, or resources that they shouldn’t have by manipulating people rather than technology. While you may think the most common way hackers breach a system is by breaking through a firewall or using a fancy password cracking algorithm, often breaches occur as the result of social engineering. (See CyberWise: Social Engineering 101) Simply put, the social engineer makes up a convincing story to trick you into doing something for them or granting them access to private information. Instead of exploiting security patches or planting targeted digital attacks on a company’s server, social engineers are bad guys who try to trick employees into sharing heavily guarded secrets (i.e., an authorized CFPB username and password). They are mastermind manipulators who pretend to be credible figures and con people within an organization into handing over the keys to the kingdom - passwords, access, money, etc.

How to avoid falling for social engineering tactics:

- Stay vigilant regarding the attachments and links within emails. Malicious emails or phishing usually have red flags. Be sure to use your mouse button to hover over the links to see where it leads.
- Beware of online requests for personal information. An email or online request that seeks personal information like your Social Security Number (SSN) or login information is likely a scam. Legitimate government agencies won’t ask for that information. Never respond to the email with your personal data.

- STOP. THINK before you CLICK. Do not click any links or attachments that are included in a suspicious email. Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind social engineers can create links that closely resemble legitimate addresses.
- If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your Outlook application or forward as an attachment to (b) (6)

Check out the full Livingsecurity blog Social Engineers: Wolves in Sheep's Clothing to learn more about social engineering exploits in action.

February 11, 2021 | CyberWise- Phishing by the numbers (Infographic)

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. The National Cyber Security Alliance (NCSA) published an infographic detailing the prevalence of phishing attacks.

Phishing by the Numbers

If you think phishing is no big deal, you might want to check out these numbers. Protecting privacy is a team sport and it's easy for everyone to step up and do their part.

#BeCyberSmart during Cybersecurity Awareness Month.

Find out more about how to spot and stop phishing attempts at staysafeonline.org

CYBERSECURITY
AWARENESS
MONTH

3.5 Billion

phishing emails are sent every day.

Source: Verizon, 2019 Data Breach Investigations Report

94%

of malware is delivered via email.

Source: Verizon, 2019 Data Breach Investigations Report

45%

of malware is disguised as a Microsoft Office document.

Source: Verizon, 2019 Data Breach Investigations Report

32%

of all information breaches involve phishing.

Source: Verizon, 2019 Data Breach Investigations Report.

Every 20 seconds

a new phishing website is created.

Source: 2020 Mobile Threat Landscape Report, Wandera

667%

Increase of targeted phishing attempts during the COVID-19 pandemic.

Source: Barracuda "Threat Spotlight: Coronavirus-Related Phishing" 2020

How to avoid falling for phishing emails:

- STOP. THINK before you CLICK. Do not click any links or attachments that are included in a suspicious email. Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.
- Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email.
- Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.
- Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete or report the message
- If you suspect you have received a malicious email from a spoofed email address, report it using the "Report Phishing" button in your Outlook application or forward as an attachment to (b) (6)

February 10, 2021 | CyberWise- Basic Home Wi-Fi Security tips

Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet. An unsecured Wi-Fi network could put your data at risk of being compromised. To confirm that your Wi-Fi network is secure, you should see a "lock" icon next to the network name, as seen in the image below. Additionally, the security standard can be found by looking at the connection configuration details. For more information, reference How to tell what security type your Wi-Fi is article.

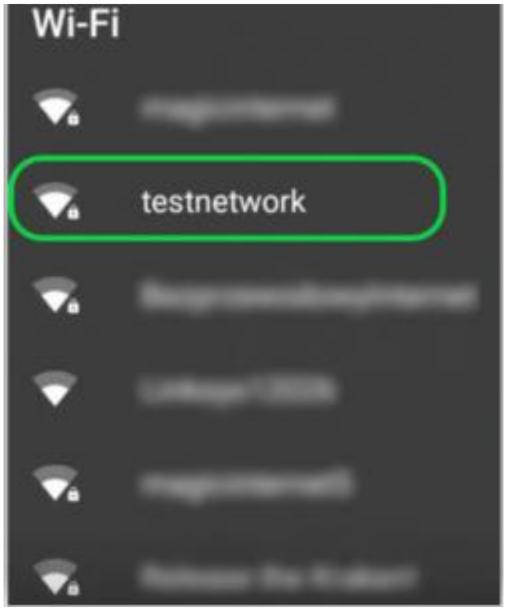


Image of secure Wi-Fi connection, identified by the lock to the left of the Wi-Fi name

Basic Wi-Fi Home Security tips:

- **Change the default Wi-Fi Router Admin Password:** Most Wi-Fi routers are shipped with a default password for the administrator account that allows you to change the device. Often these default passwords are publicly known, perhaps even posted on the Internet. Be sure to change the admin password to a unique and strong password, so only authorized users to have access to it. (see How To Change Your Wireless Router Admin Password article).

- **Create a Wi-Fi Network Password:** Your Wi-Fi network password is the way only people and devices you trust can join your home network. Configure your Wi-Fi network password, so it has a unique, strong password as well (make sure it is different from your router admin password).

- **Use a Guest Network:** A guest network is a virtual separate network that your Wi-Fi router can create. This means that your Wi-Fi router has two networks. The primary network is the one that your trusted devices connect to, such as your computer, smartphone, or tablet devices. The guest network is what untrusted devices connect to, such as guests visiting your house or perhaps some of your personal smart home devices. When something connects to your guest network, it cannot communicate with any of your trusted personal devices connected to your primary network.

For more tips home Wi-Fi security tips, check out this Securing Wi-Fi at Home article from CISA.

February 04, 2021 | CyberWise Tip: Cybersecurity Aware behaviors

The United Kingdom (UK) National Cyber Security Centre (NCSC) has launched a new cyber security campaign encouraging the public to adopt certain behaviors to stay safe online. The CyberAware campaign recommends the following actions:

- Utilize multi-factor authentication (MFA). Using MFA, also referred to as Two Factor authentication (2FA), requires two different methods of authentication in order to gain access. CFPB laptops use Always on VPN, which allows Bureau users to work more efficiently regardless of location. If you have a CFPB laptop and an internet connection, then you are automatically connected to the CFPB VPN. It's a more secure and consistent experience from any location.

- Create strong passwords. Use a strong password and different passwords for different accounts and devices.

- Keep your devices updated. Out-of-date software, apps, and operating systems contain weaknesses making them easier to hack. Vendors and companies fix the weaknesses by releasing updates (see Ten Ways to Improve Your Computer Security Cyberwise tip). Updating your devices and software helps to keep your device secure. Turn on automatic updates for your devices and software that offer it.

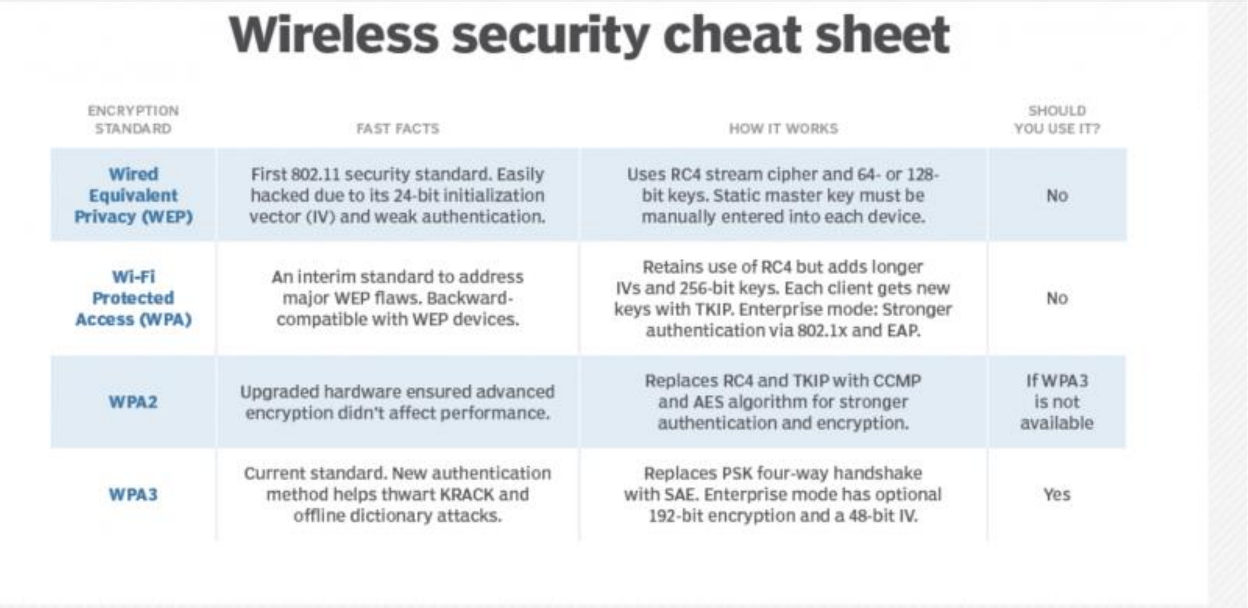
- Back up your data. Backing up means creating a copy of your information and saving it to another device (Universal Storage Bus (USB) stick) or to cloud storage (online). Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users to review the official NCSC website as well as CISA's Tips page for more information and additional resources.

February 01, 2021 | CyberWise Tip: Wireless Security: WEP, WPA, WPA2 and WPA3

Choosing the proper level of security for your Wi-Fi network is very important. As wireless networks have evolved, so too have the protocols for securing them. The right choice will determine whether your wireless network is a house of straw or a resilient fortress.

Most wireless access points (WAPs), responsible for relaying data between a wired network and wireless devices, come with the ability to enable one of four wireless standards: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 or WPA3. The cheat sheet below includes fast facts and describes how each of the wireless standard work.



Wireless security cheat sheet

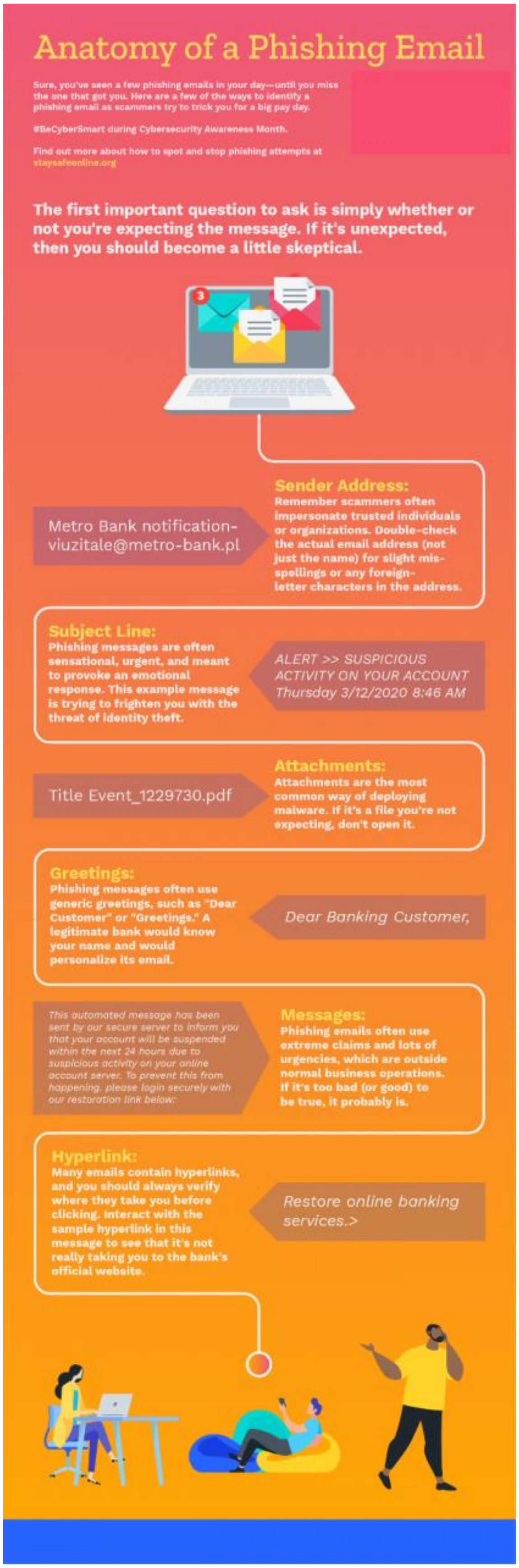
ENCRYPTION STANDARD	FAST FACTS	HOW IT WORKS	SHOULD YOU USE IT?
Wired Equivalent Privacy (WEP)	First 802.11 security standard. Easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64- or 128-bit keys. Static master key must be manually entered into each device.	No
Wi-Fi Protected Access (WPA)	An interim standard to address major WEP flaws. Backward-compatible with WEP devices.	Retains use of RC4 but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	No
WPA2	Upgraded hardware ensured advanced encryption didn't affect performance.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	If WPA3 is not available
WPA3	Current standard. New authentication method helps thwart KRACK and offline dictionary attacks.	Replaces PSK four-way handshake with SAE. Enterprise mode has optional 192-bit encryption and a 48-bit IV.	Yes

Wireless Security Cheat Sheet published by Search Networking

Be sure to research and learn which personal wireless security standard is best for your network needs. Check out this Search Networking article learn more about the differences among WEP, WPA, WPA2 and WPA3 wireless security protocols.

January 29, 2021 | CyberWise Tip: Learn the Anatomy of a Phishing attack (Infographic)

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. The National Cyber Security Alliance (NCSA) published an infographic detailing the anatomy of a phishing attack.



Anatomy of a Phishing Email

Sure, you've seen a few phishing emails in your day—until you miss the one that got you. Here are a few of the ways to identify a phishing email as scammers try to trick you for a big pay day.

#BeCyberSmart during Cybersecurity Awareness Month.

Find out more about how to spot and stop phishing attempts at staysafeonline.org

The first important question to ask is simply whether or not you're expecting the message. If it's unexpected, then you should become a little skeptical.

Metro Bank notification-viuzitale@metro-bank.pl

Sender Address: Remember scammers often impersonate trusted individuals or organizations. Double-check the actual email address (not just the name) for slight misspellings or any foreign-letter characters in the address.

Subject Line: Phishing messages are often sensational, urgent, and meant to provoke an emotional response. This example message is trying to frighten you with the threat of identity theft.

ALERT >> SUSPICIOUS ACTIVITY ON YOUR ACCOUNT
Thursday 3/12/2020 8:46 AM

Title Event_1229730.pdf

Attachments: Attachments are the most common way of deploying malware. If it's a file you're not expecting, don't open it.

Greetings: Phishing messages often use generic greetings, such as "Dear Customer" or "Greetings." A legitimate bank would know your name and would personalize its email.

Dear Banking Customer,

This automated message has been sent by our secure server to inform you that your account will be suspended within the next 24 hours due to suspicious activity on your online account server. To prevent this from happening, please login securely with our restoration link below:

Messages: Phishing emails often use extreme claims and lots of urgencies, which are outside normal business operations. If it's too bad (or good) to be true, it probably is.

Hyperlink: Many emails contain hyperlinks, and you should always verify where they take you before clicking. Interact with the sample hyperlink in this message to see that it's not really taking you to the bank's official website.

Restore online banking services.>

The Anatomy (structure) of a phishing scam attempt

- Be sure to STOP and THINK before you CLICK. Do not click any links or attachments that are included in a suspicious email.
- Immediately report the suspicious email by clicking the **"Report Phishing"** button for Windows users or forwarding the email as an attachment to (b) (6)

January 25, 2021 | CyberWise Tip: What is Multi-factor authentication (MFA)?

Passwords are a good first layer of protection, but malicious actors can guess and crack passwords. Avoiding passwords based on personal information (like where you went to school or your pets' name); using the longest password or passphrase possible (8–64 characters); and not sharing your passwords with anyone else adds more protection (See Choosing and Protecting Passwords for more information.), but multi-factor authentication is really what makes your accounts more secure.

Multi-factor authentication (MFA), sometimes referred to as two-factor authentication, uses multiple pieces of information to verify your identity. Even if an attacker obtains your password, he may not be able to access your account if it's protected by MFA. The theory behind this approach is like requiring two or more forms of identification to open a safe deposit box. You should always enable MFA where it's available. Authentication categories that are used within MFA include **something you know, something you have**, and **something you are**.

- **Something you know** – This category includes something the user knows, such as username/password.

- **Something you have** – This category includes something the user possesses, such as a small physical token like a PIV card, a special key fob, or software-based authentication token (ie RSA or Google Authenticator apps). You might use this token in conjunction with a password to log into an account. Software-based tokens are common, since these software-based tokens can generate a single-use login personal identification number (PIN). Other variations include SMS messages, phone calls, or emails sent to the user with a verification PIN. These token PINs can often be used only once and are voided immediately after use.

- **Something you are** – Biometric identification can include scanning of eyes (retinas or irises) or fingerprints, facial recognition, voice recognition, or authentication through signatures or keystroke movements. A common example of biometric identification is the fingerprint scanner used to sign in users on many modern smartphones.

Whenever possible, be sure to utilize MFA. It is highly recommended that MFA be used for critical services, such as logging into email accounts, online banking, or storing files online as it's a more secure solution than using just passwords.

Learn more about MFA from our Cyber Tip of the week archive.

January 22, 2021 | CyberWise Tip- Know What Information Is Being Collected When You Visit a Website

When visiting unknown websites, be vigilant about protecting your identity. Remember that some information is automatically made visible to the site. Information such as the computer's IP address, domain name (e.g., .com, .gov, or .edu), software details, and page visit information is often saved in cookies so that the organization may develop and store user profiles of website visitors. If a website uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you've visited.

- If the site you're visiting is malicious, the files on your computer, as well as passwords stored in the temporary memory, may be at risk. Generally, organizations use the information that is gathered automatically for legitimate purposes, such as generating statistics about their sites.
- Be careful supplying personal information. Unless you trust a site, don't give your address, password, or credit card information.
- Look for indications that the site uses encryption to secure your information (such as HTTPS in the URL web browser section). Although some sites require you to supply your Social Security Number (e.g., sites associated with financial transactions such as loans or credit cards), be especially wary of providing this information online

January 19, 2021 | CyberWise Tip- Personal Security Considerations

In recent months, the U.S. has experienced civil unrest across multiple jurisdictions. Due to continued sociopolitical issues, there remains a potential for further unrest. Domestic terrorists and other violent extremist actors may continue to leverage peaceful protests to attempt to incite hate, destroy critical infrastructure, and inflict bodily harm. Extremist actors have also used rhetoric to attempt to threaten high- profile individuals associated with the management and operation of critical infrastructure. To reduce risk, the Cybersecurity and Infrastructure Security Agency (CISA) recommends that individuals, particularly those with higher profile status, implement basic security measures to increase personal safety.

Behavioral Indicators Critical Infrastructure owners and their personnel can reduce the probability of becoming a victim of an attack by remaining vigilant. Individuals should report suspicious behavior that others may exhibit, such as:

- Loitering at a location without a reasonable explanation
- Taking pictures of people or infrastructure in an unusual or covert manner
- Avoiding security personnel or systems
- Expressing or implying threats of violence
- Unauthorized people trying to enter a restricted area or impersonating authorized personnel
- Placing an object or package, either in a concealed or blatant manner, that has unexplainable wires or other bomb-like components

Personal Security Measures Applying basic security measures can enhance the protection of critical infrastructure and mitigate threats to personal safety. Follow the tips below to establish these security measures:

- Create a personal or family emergency action plan
- Change daily routine, particularly routes to and from work
- Let a trusted person know where you are going, particularly if outside of daily functions
- Exercise caution when using underground and enclosed parking
- Stay in well-lit public areas and avoiding isolated streets
- Identify scheduled local demonstrations to avoid large crowds
- Hide personally identifiable information while in public areas
- Carry simple to use protective tools such as pepper spray
- Head to nearest police station if being followed
- Avoid suspicious packages, and recognizing potential indicators of a suspected explosive device to notify law enforcement
- Avoid text messaging or lengthy cell phone use while walking alone
- Be extra alert and knowing who and what are in the vicinity
- Ask for help – contact security for escort to vehicle

Visit cisa.gov/hometownsecurity for additional resources.

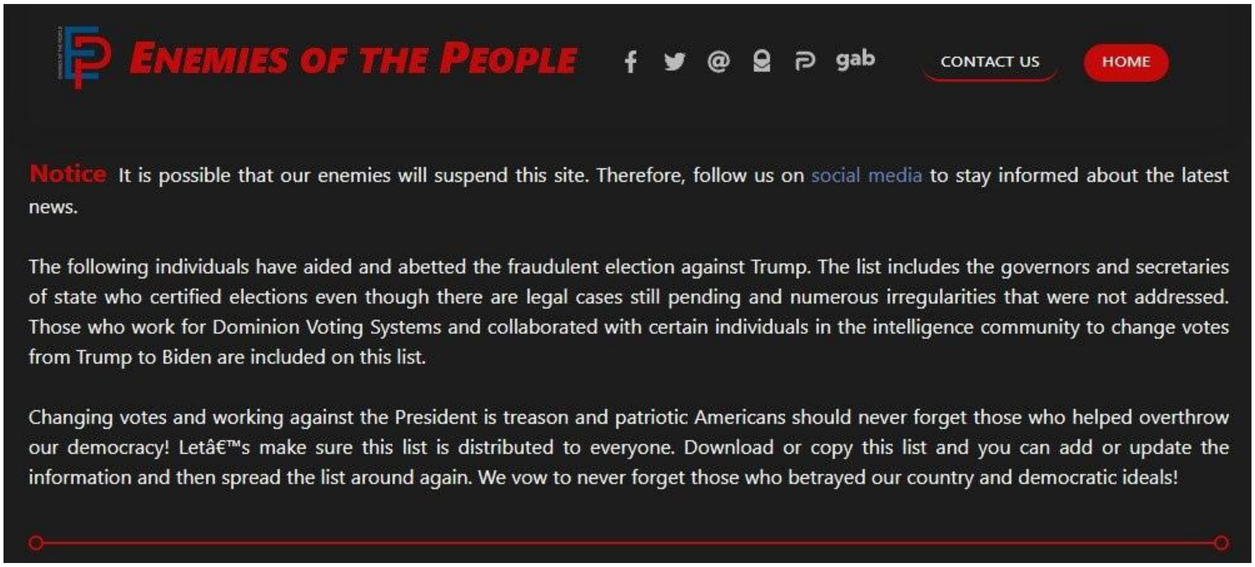
January 15, 2021 | CyberWise Tip- Beware of suspicious emails and websites

There is increased awareness surrounding the Presidential Inauguration due to the massive amount of disinformation from foreign adversaries. These adversaries have encouraged deadly violence against U.S. state officials certifying the 2020 election results. These adversaries have created email accounts and websites to threaten or reveal personal information and photos of government officials and individuals in the private sector involved in the Presidential election. Below are examples of this kind of activity:

Email accounts created by adversaries:

- enemiesofthepeople@tutanxxa.com
- 6e.nemiesOfThepeople.e9@protonmxxl.com
- 3e.nemiesOfThePeopl.e3@protonmxxl.com
- 3e.nemiesOfThePeopl.e3@gmaxx.com

Website created by adversaries:



Notice It is possible that our enemies will suspend this site. Therefore, follow us on social media to stay informed about the latest news.

The following individuals have aided and abetted the fraudulent election against Trump. The list includes the governors and secretaries of state who certified elections even though there are legal cases still pending and numerous irregularities that were not addressed. Those who work for Dominion Voting Systems and collaborated with certain individuals in the intelligence community to change votes from Trump to Biden are included on this list.

Changing votes and working against the President is treason and patriotic Americans should never forget those who helped overthrow our democracy! Letâ€™s make sure this list is distributed to everyone. Download or copy this list and you can add or update the information and then spread the list around again. We vow to never forget those who betrayed our country and democratic ideals!

Titled "Enemies of the People," the website was created on December 6th and included personal details (home addresses, email, names, and photos with a target) exposing the personal details of individuals who did not support the current U.S. President's claims of voter fraud</small>
The FBI and CISA are urging the public to check the sources of information before making an opinion and to seek verified news from trustworthy publications. The FBI also encourages the public to report information concerning suspicious or criminal activity to their local field office or online at tips.fbi.gov. Whether it's a scam or spam, it is important to stay vigilant when reading through your inbox (see Do you know the difference between a scam and spam?). Be aware that there are individuals who hope to trick you into falling for one of their schemes. Be skeptical and if something does not seem right, report it!

- **STOP. THINK before you CLICK.** It's important to always be distrustful of any email directing you to take action either by clicking a link (known as phishing), downloading an attachment, or providing prompt payment to avoid a punitive action.
- All suspicious emails should immediately be reported using the Report Phishing button in the Outlook ribbon or forwarding the email as an attachment to (b) (6)

This tip was created in coordination with the Cybersecurity Incident Response Team (CSIRT) Team. If you have any general security questions for the team reach out to (b) (6) The Cyber training team can be contacted via (b) (6)

January 13, 2021 | CyberWise Tip- Understanding the value of digital data and how to protect it

Oftentimes, the greatest value of data for companies is the digital fingerprint that users leave behind while going about their daily routine. Companies routinely gather what they call "passive" data—not something we generate consciously—about our online habits: what we buy, websites we visit, our online searches, even the books we check out online from our local library. That's all data—data about us—and its valuable. To companies capturing passive personal data, it's big business. The world produces 2.5 quintillion bytes of data each day, a number so large it's hard to comprehend, and 90% of all the data that has ever been produced in all of history happened in just the last two years.

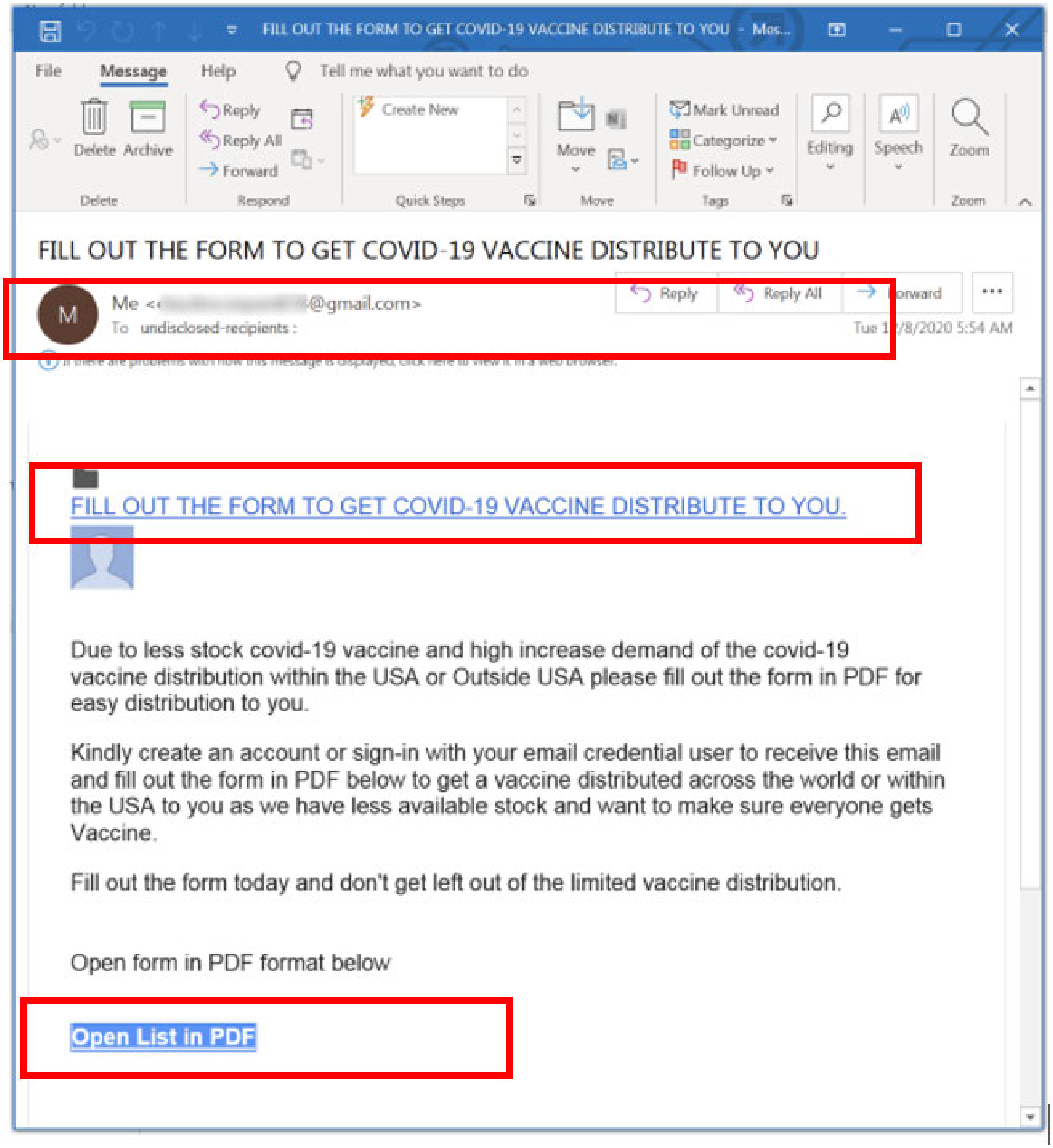
What's My Data Worth? Mining personal data is a gold rush for many companies. But what does it mean for individuals? That's harder to calculate. In 2015, Comcast paid $100 to each victim of a data breach. These Comcast customers paid about $1.50 a month to have their personal information unlisted. By most accounts, this was a first because it valued an individual’s personal data that was hacked at $100, which Comcast paid back to the victims of the hack. Another possible way to look at the value of personal data is to see it as the value of your personal privacy. What would it cost you if someone hacked your accounts and stole your identity? What if they impersonated you on your social media accounts, alienating your friends and family? How much is your reputation worth?

Tips to protect your data:

- Use a strong password and different and strong passwords for different accounts and devices.
- Utilize multi-factor authentication (MFA). Using MFA requires two different methods of authentication in order to gain access.
- Make sure websites are using HTTPS, before entering any credentials for your online accounts.
- Own Your Online Presence. Be sure to review the privacy and security settings on websites before submitting your data in order to ensure you are comfortable with their use of your data. It’s OK to limit how and with whom you share information.

January 08, 2021 | CyberWise Tip: COVID-19 vaccine phishing scams

The security awareness training vendor KnowBe4 has reported that COVID-19 vaccine-themed phishing campaigns are being observed. In this phishing campaign, the email appears to be trying to exploit a Washington Post article stating that Pfizer may not be able to supply additional doses of its vaccine to the United States in large volumes until sometime in the spring of 2021. The link in the email body takes unsuspecting users to a phishing scam to gain the users credentials.



FILL OUT THE FORM TO GET COVID-19 VACCINE DISTRIBUTE TO YOU

Me <[redacted]@gmail.com>

To undisclosed-recipients :

Tue 12/8/2020 5:54 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

FILL OUT THE FORM TO GET COVID-19 VACCINE DISTRIBUTE TO YOU.

Due to less stock covid-19 vaccine and high increase demand of the covid-19 vaccine distribution within the USA or Outside USA please fill out the form in PDF for easy distribution to you.

Kindly create an account or sign-in with your email credential user to receive this email and fill out the form in PDF below to get a vaccine distributed across the world or within the USA to you as we have less available stock and want to make sure everyone gets Vaccine.

Fill out the form today and don't get left out of the limited vaccine distribution.

Open form in PDF format below

Open List in PDF

Example of COVID Vaccine phish attempt. Phishing red flags are indicated in red boxes

The social engineering scheme in this campaign exploits some of the basic questions and concerns that users and employees will have about the several vaccines currently on the cusp of widespread distribution.

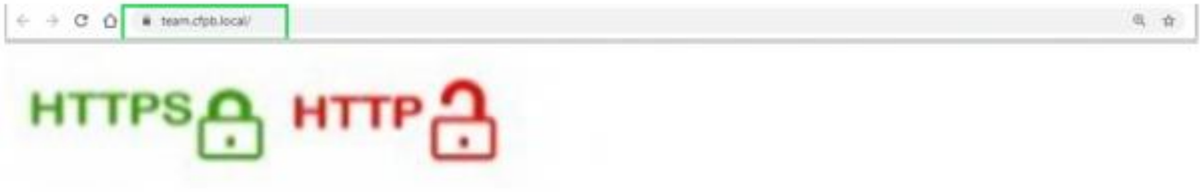
How to avoid falling for phishing emails:

- Stay vigilant regarding the attachments and links within emails. Malicious emails or phishing usually have red flags. Be sure to use your mouse button to hover over the links to see where it leads.
- Beware of online requests for personal information. A coronavirus-themed email that seeks personal information like your Social Security Number (SSN) or login information is a phishing scam. Legitimate government agencies won’t ask for that information. Never respond to the email with your personal data.

- **STOP. THINK before you CLICK.** Do not click any links or attachments that are included in a suspicious email. Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.
- Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email.
- Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.
- Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete or report the message.
- If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your Outlook application or forward as an attachment to (b) (6)

January 04, 2021 | CyberWise Tip: Data Management is a key part of cybersecurity

Data management is a key part of cybersecurity. Data, defined as "information in digital form that can be transmitted or processed", can include information types such as Personally Identifiable Information (PII), user browsing habits and website visits, message and email content, online purchases, and financial information. Everything from our web browsing, mobile devices, and even the Internet of Things (IoT) products (i.e. smart speakers like Alexa or Google Home) installed in our homes collect and use data. These technologies have the potential to erode our privacy and cybersecurity, and users should not depend on vendors to keep them protected or safe. In the wrong hands, this information can also prove to be a gold mine for advertisers and cyber attackers.



How to protect your data and online information: Be sure to use HTTPS when visiting websites! End-to-end encryption is becoming more utilized to protect the user's web browsing data. This form of encryption prevents anyone except those communicating from accessing or reading the content of messages, including vendors themselves.

HTTP vs. HTTPS: When using a web browser, you should see either Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) in the URL section. The latter option uses a layer of end-to-end encryption to enable secure communication between a browser and a server. Be sure to only enter Personally Identifiable Information (PII), when visiting a website address that uses HTTPS. When it comes to online purchases it is crucial to confirm you are using HTTPS to protect your payment details from eavesdropping and theft. Companies often use HTTPS, to encrypt information and encode information to make it unreadable by unauthorized parties.

December 23, 2020 - CyberWise Tip: Mobile payment app risks to be aware of this holiday season

Due to the pandemic many families are celebrating the holidays from a distance, relying on mobile money payment apps (e.g., Venmo, Zelle, and Cash App) to gift money to loved ones near and far. Many retailers, both brick-and-mortar and online, have also started accepting payments through services like ApplePay, GooglePay, Android Pay, and Paypal. Approximately 90 million Americans use money payment apps, as they offer flexibility and conveyance in an increasingly connected world.

Money payments apps have had a fair share of security incidents, many of which could be avoided by users' cyber vigilance. In the first quarter of 2018, Venmo reported a $40 million loss in fraud reimbursements. While Venmo did not specify the sources of fraud, one common scam involves sending an "accidental payment," then asking the victim to return the payment.

Mobile payment cybersecurity best practices:

- Choose apps that offer Multi-Factor Authentication. Use a strong passwords and unique passwords for different accounts and devices. Users should also utilize multi-factor authentication (MFA). Using MFA requires two different methods of authentication in order to gain access.
- If someone sends money by mistake, immediately ask them to cancel the transaction. If the individual refuses, it is most likely a scam and should be reported.
- If you receive a suspicious email or text on your CFPB device that you think may be a scam, stop and think before you click. Do not click any links or attachments that are included in a suspicious email, immediately report the suspicious link to the CFPB Suspect Inbox (b) (6)
- For personal and home devices, suspicious email can be reported to CISA via https://www.us-cert.gov/report-phishing. If you receive an unexpected email or text that asks for money, do not click on any links, even if the request appears to come from someone you know. Log in to the app to see if you have any requests for money. If there are no requests, the email or text is probably a phishing scam.

Learn more about money payment app fraud and best practices at the Federal Trade Commission website.

December 21, 2020 - CyberWise Tip: Cybersecurity IoT risks to be aware of this holiday season Internet of Thing devices

As mentioned in our tip posted in October for National Cybersecurity Awareness Month (NCSAM), cybercriminals can harness the power of Internet of Things (IoT) devices against their very own users. The IoT appliances and devices that connect to the internet and to each other on your home network — have created new opportunities for cybercriminals. Cybercriminals might infiltrate your IoT devices to do harm or they might use the devices and others to launch a broad attack.
Since IoT devices are a popular gift over the holidays, you want to be aware of the cybersecurity concerns associated with these appliances! Many of these risks can be addressed by following best practices and choosing well-known, reputable, American-owned brands with a good cybersecurity track record.

Tips to make your IoT devices more secure:

- **Change default usernames and passwords.** Cybercriminals will research the default passwords that come with many IoT products. That makes it easy for them to access your IoT devices and, potentially, the information on them.

- **Use strong passwords and Multi-Factor Authentication (MFA).** Internet-enabled devices are configured with default passwords to simplify setup. These default passwords are easily found online, so be sure to update your device with strong passwords to help secure your device as soon as possible. Using MFA requires two different methods of authentication in order to gain access.

- **Disable unused and unnecessary features.** IoT devices come with a variety of services such as remote access, often enabled by default. If you don't need it, be sure to disable it.

- **Keep your software up to date.** When your IoT manufacturer sends a software update, be sure to install it as soon as possible. It might be a patch for a security flaw. Be sure to download updates and apply them to your device to help stay safe.

Check out the detailed guide Mozilla recently released, which rates the privacy of many popular connected devices.

December 18, 2020 - CyberWise Tips: Beware of Holiday Charity Cyber scams

According to the Federal Bureau of Investigation (FBI), criminals are fraudulently soliciting donations for "individuals, groups, and areas affected by COVID-19," exploiting the global pandemic. Online charity scams occur through various channels including emails, cold calls, social media posts and ads, and crowdfunding platforms. They often imitate a real charity's name or spoof a legitimate website in attempts to attract more donations. Other signs of charity fraud include unsolicited emails thanking you for a donation you don't remember giving, urgent requests for donations, and a preference for cash, prepaid gift cards, or money wire donations.

Safely donate to charities this holiday season with the following guidance:

- **Verify the organization's legitimacy** using websites like CharityWatch. Also check the National Association of State Charity Officials to see if the charity is registered in your state. Additionally, ask the charity for their Employer Identification Number (EIN), which legitimate organizations will provide upon request.

- **Do not click or open unknown links or email attachments** and never give out sensitive information without verifying the requester's identity. Phone numbers are easy to spoof, and scammers are cold-calling, direct messaging and creating fake websites and pages on social media to raise funds.

  > Think twice before clicking on links found in emails, especially if you don't know the sender. Be sure to **STOP** and **THINK** before you **CLICK**. Do not click any links or attachments that are included in a suspicious email.

- **Donate using a credit card** to ensure the payment is tracked. After making a donation with your credit card, be sure to monitor financial statements and turn on credit card transaction alerts to ensure no additional fees were charged and you didn't unknowingly sign-up for recurring donations.

Check out the Cybersecurity Tips archive to learn more about holiday scams to beware of.

December 14, 2020 - CyberWise Tips: Beware of Holiday Cyber scams

While the holiday season is often considered the best time of the year to slow down and spend time with loved ones, it's also prime time for hackers, scammers, and online thieves. According to CISA, scammers often use this time of the year, which experiences higher online traffic, by looking for security weakness in our devices and/or internet connections. These nefarious actors even utilize fake websites and charities to gain personal and financial information from unsuspecting users. By being aware of the Grinches are trying to do each of us can put the "BaHumbug" in their efforts. This year, these schemes are accompanied by widespread COVID-19 scams being conducted globally.

Holiday scams to stay away from:

- Secret Sister scam & social media gift exchange schemes

Popularized on Facebook in 2015, the scam tells participants that if they join, they could receive up to 36 gifts in exchange for sending one gift. The scheme leans on the consistent recruitment of individuals, and most end up not receiving a gift and in-turn quit. These scams collect personally identifiable information like names, home addresses, and emails, etc.

- Puppy scams

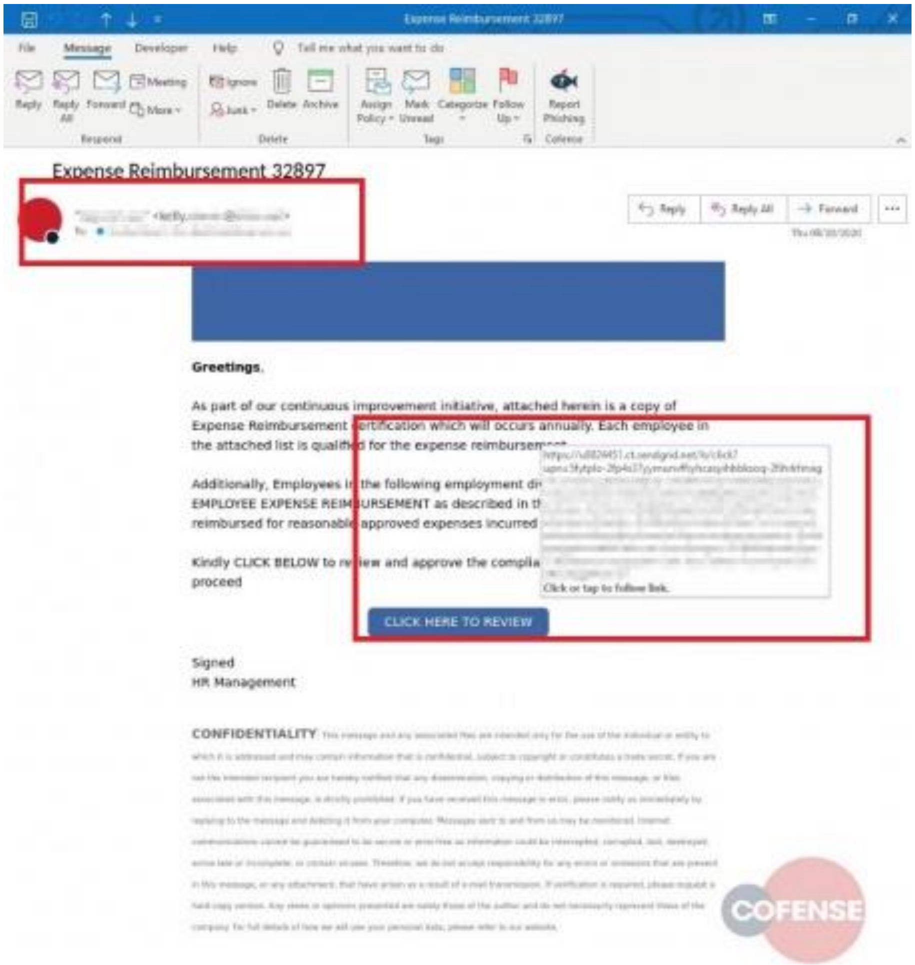
Back in August 2020, the Better Business Bureau (BBB) reported an increase in pet adoption scams, and the numbers are expected to continue to rise during the holidays. Scammers are using the pandemic as an opportunity to ask for money up-front or to explain why the victims cannot meet the animals before paying. Generally, the animals listed for sale do not exist and never make it to the victim.

Visit the Better Business Bureau's Scam Tracker to learn about other scams to stay away from.

December 10, 2020 CyberWise Tip: Beware - Threat Actors Weaponize Companies' Employee Reimbursements During the Pandemic

Due to the COVID-19 global health pandemic, many employees have been primarily working from home for an extended period. The shift to remote work has led to many companies offering employees reimbursable work from home resources needed for their newly designated remote positions. The [Phishing Defense Center (PDC)] has identified a campaign attempting to steal employee credentials by using fake reimbursement emails. This campaign was seen across multiple industries such as the insurance, medical, professional services and banking fields.

In this realistic scam email, users will see the nickname field displays their company's name, making it appear as if the email originated from within the company to trick users into believing it is legitimate. However, users should pay attention to the real sender. The email body includes the reason for the email and mentions an attached file with expense reimbursement certification, list of qualified employees and attached reimbursement policy. Although there is no attached file, the email contains a button "CLICK HERE TO REVIEW" with a hyperlink to take the recipient to the phishing landing page.



Expense Reimbursement 32897

<kelly.[illegible]@[illegible]>

Greetings,

As part of our continuous improvement initiative, attached herein is a copy of Expense Reimbursement certification which will occurs annually. Each employee in the attached list is qualified for the expense reimbursement

Additionally, Employees in the following employment d[illegible] EMPLOYEE EXPENSE REIMBURSEMENT as described in th[illegible] reimbursed for reasonable approved expenses incurred [illegible]

Kindly CLICK BELOW to review and approve the complia[illegible] proceed

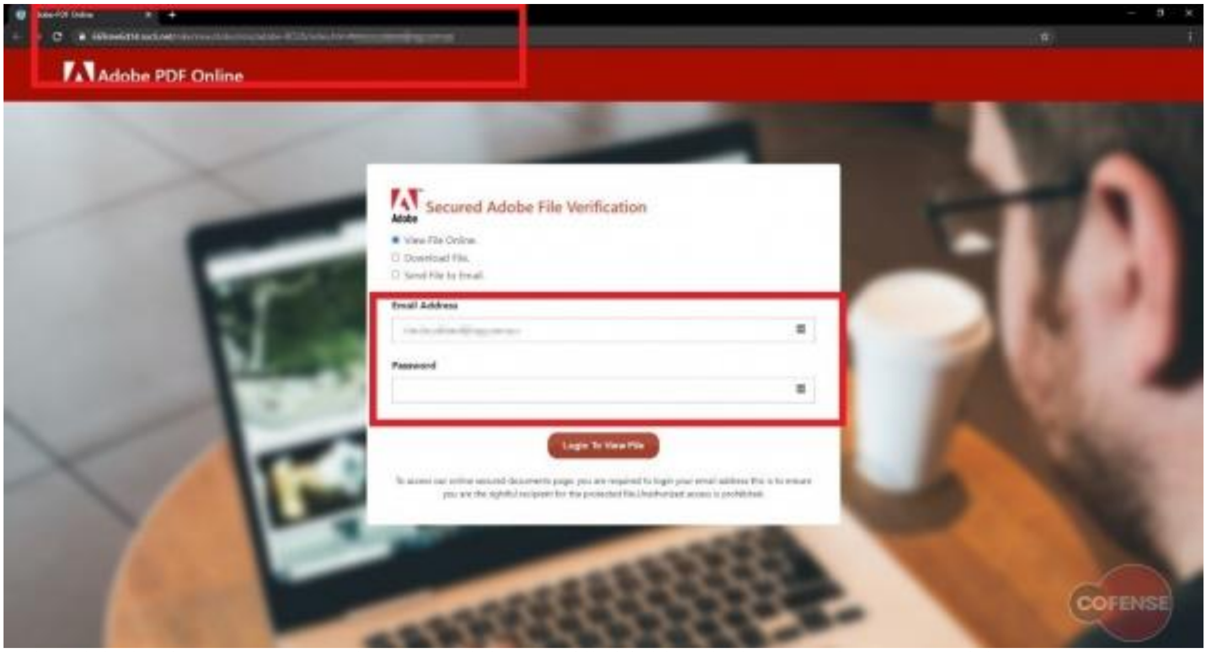
https://u8824451.ct.sendgrid.net/ls/click?upn=[illegible]

Signed
HR Management

CONFIDENTIALITY This message and any associated files are intended only for the use of the individual or entity to which it is addressed and may contain information that is confidential, subject to copyright or constitutes a trade secret. If you are not the intended recipient you are hereby notified that any dissemination, copying or distribution of this message, or files [illegible]

Example of expense reimbursement scam email

Once users click on the link in the email, they are redirected to a landing page that looks like the Adobe PDF online site. However, users should note that the email of the recipient is already filled out and the only the password field left blank, which is a red flag. Users should also pay attention to the URL in the address bar which shows that is not Adobe.com and this isn’t the typical Adobe login users would normally receive.



Secured Adobe File Verification

● View File Online.
□ Download File.
□ Send File to Email.

Email Address

Password

Login To View File

To access our online secured documents page you are required to login your email address this is to ensure you are the rightful recipient for the protected file.Unauthorized access is prohibited.

Fake Adobe landing page. Notice the URL and the auto filled fields, which are not legitimate Adobe.com practices

In order to avoid falling victim to this threat, be sure to STOP and THINK, before you CLICK on unknown links in messages. Report suspicious activity by clicking the **"Report Phishing"** button in Outlook or sending screenshots of any social media contacts as an attachment to (b) (6)

Check out our previous CyberWise tip on how to detect a COVID-19 phishing scams.

December 03, 2020 | CyberWise Tip - Cybersecurity threats to corporate America are present now 'more than ever,' according to SEC

The Securities and Exchange Commission (SEC) Chairman Jay Clayton is advising corporate American organizations to become much more vigilant on cybersecurity. *"Cyber risks have not gone away with the unfortunate, unforeseen risks we've faced with COVID and other uncertainties in our economy,"* Chairman Clayton stressed on CNBC during a recent Power Lunch interview, *"They're still there, and they're there more than ever."*

Specifically, the SEC has recently issued cybersecurity related warnings for the following cyber threats:

Ransomware: An increase in sophistication of attacks on broker-dealers, investment advisers, and investment companies, and attacks impacting service providers to companies that are under the SEC's purview.

Tips for preventing ransomware include:

- Keep applications and operating systems patched and up to date. Updates and patches address weaknesses on a system and its applications (e.g., MSOffice, Chrome, and Adobe).

- Be vigilant with attachments and links in emails. Malicious emails or phishing usually have red flags. Use your mouse to hover over the links and view the linked landing page before clicking on it.

Credential compromises: An increase in cyber-attacks against brokers and dealers using "credential stuffing," a method of cyber-attack that uses compromised client login credentials, resulting in the possible loss of customer assets and unauthorized disclosure of sensitive personal information.
Tips for preventing credential compromises include:

- Use a strong password and different passwords for different accounts and devices.
- Utilize multi-factor authentication (MFA). Using MFA requires two different methods of authentication in order to gain access. CFPB laptops use Always on VPN, which allows Bureau users to work more efficiently regardless of location. If you have a CFPB laptop and an internet connection, then you are automatically connected to the CFPB VPN. It's a more secure and consistent experience from any location.

November 30, 2020 | CyberWise Tip - Tips for Safeguarding Personal Information online during the holiday season

Black Friday and Cyber Monday holiday sales kick off the holiday shopping season attracting millions of shoppers online for deals and savings. This year due to COVID, more retailers and businesses are utilizing online shopping, which provides more opportunities for an attacker to steal personal information. The Cybersecurity and Infrastructure Security Agency (CISA) reminds users to remain vigilant when browsing or shopping online.

Shop Securely Online

*But **NOT** with your Government credentials*

Do not use your CFPB email address or credentials when accessing any online shopping site. Doing so can lead to **identity theft** and **credential stuffing** attacks.

Credential stuffing occurs when criminals gain access to your login details, typically by purchasing a list based on a data breach on the dark web. They then attempt to access various accounts using those credentials. Once they succeed at breaking into an account, they take it over **(identity theft)** and use it to perform activities such as theft, fraud, and data exfiltration.

3 Safety Tips for Online Shopping

1) Always look for HTTPS before shopping online

If you see an "S" on the end of HTTP it means you're connected to a secure website. If the URL of the site you plan to shop on doesn't have an HTTPS prefix, **DON'T SHOP THERE.**

HTTPS 🔒 HTTP 🔓

2) Check out as a guest to avoid saving payment information online

Although inconvenient to re-enter your data later, re-entry keeps you safer because your payment information is not saved or ready to be used by anyone who gets access to your account.

3) Do not use your work email address or password for retail accounts

Use a free webmail account such as Gmail or Hotmail. This can also help prevent criminals from knowing where you work, which is information than can be potentially used to hack into your work account and the entire Bureau!

If you have clicked on a real phishing attempt, please immediately notify the Bureau's Security Operations Center at **CFPB_SOC@CFPB.GOV** or **202-435-7200.**
For incidents after business hours the On-Call Analyst can be reached at **202-308-6574.**

CISA encourages Cyber Monday shoppers to review the following online shopping safety tips:

- Do business with reputable vendors. Before providing any information, make sure that you are interacting with a reputable, established vendor. Some attackers may try to trick you by creating malicious websites that appear to be legitimate, so you should verify the legitimacy before supplying any information. (See Avoiding Social Engineering and Phishing Attacks.)

- Use caution with email links and attachments. Take appropriate precautions when using email and web browsers to reduce the risk of an infection. Be wary of unsolicited email attachments and avoid clicking on email links, even if they seem to come from people or businesses you know. (See Using Caution with Email Attachments.)

- Pay using a credit card. There are laws to limit your liability for fraudulent credit card charges, but debit cards may not have the same level of protection.
- Ensure your information is encrypted. Check website URLs to ensure they begin with "https:" (instead of "http:") accompanied by a padlock icon to verify that the site is secure.
- Do not use your work email address when shopping online. Doing so can lead to identity theft and credential stuffing attacks. Personal use of any CFPB email address is not recommended however the CFPB Acceptable Use Policy (AUP) notes that, “limited personal use of IT resources is a privilege, and may be exercised only when the use does not result in a loss of productivity, interfere with official duties or business, or involve more than minimal additional expense to the government.”

To learn more about personal use of your CFPB resources check out the AUP.

November 25, 2020 | CyberWise Tip- How to protect yourself against getting cyber scammed this Black Friday

Over the past few months, malicious actors have been preparing to abuse the popularity of Black Friday online shopping. According to Performanta, there has been a surge in threat actors getting ready to scam users and infect them with malware. Although cyber criminals are constantly finding new ways to deceive users into divulging usernames and passwords, below we have the common techniques attackers use and how to avoid falling for them.

Malware is a type of malicious and purposefully harmful software. There are many software programs that carry out malicious activities such as viruses, worms, ransomware, rootkits, and logic bombs. This year there have been many coronavirus themed malware families such as Emotet and TrickBot, deployed primarily through e-mail. Online criminals will every opportunity to trick you into opening a malicious e-mail.

Online scams During online scams malicious actors try to lure users into using fake online shops purposely set up to scam users. This often happens by e-mail, so don’t trust unrecognized e-mails, especially those claiming to have exclusive Black Friday deals. Some scammers will also create counterfeit versions of popular items and sell them on online marketplaces like eBay and Amazon.

Phishing is a serious threat that can cost individuals and companies both money and peace of mind. These attacks are attempts by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate.

Tips to stay protected against Black Friday scams:

Malware Review the link included in the email by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate; however, phishers can create links that closely resemble legitimate addresses. If you experience suspicious activity to your CFPB workstation after opening or clicking an attachment, report to (b) (6) or (b) (6)

Online scams When using multi-seller marketplaces, like eBay, check the seller's account age and reputation before purchasing anything. Be careful when opening e-mails, especially those that claim that your account has been locked/restricted or that you need to verify payment details.

Phishing Most phishing attempts are conducted by e-mail, often using a sense of urgency in the subject lines such as: "Your account has been locked, act now" or "Verify your credentials". Expect an increase in phishing for accounts involved in Black Friday purchases, especially with Amazon and PayPal accounts.

- Watch out for vague language or a generic request to click on a link or enter information.
- Think twice before clicking on links found in emails, especially if you don't know the sender. Be sure to STOP and THINK before you CLICK. Do not click any links or attachments that are included in a suspicious email.
- Call the sender to verify that they sent you an email if the tone or wording does not sound like him or her. It is easy for a cyber attacker to create a message that appears to be from a friend or co-worker.
- Don't use your CFPB email account for non-CFPB related work
- Immediately report the suspicious email by clicking the **"Report Phishing"** button for Windows users or forwarding the email as an attachment to (b) (6)

November 19, 2020 | CyberWise Tip- Best Practices for using Public Wi-Fi

Public wireless networks can be a threat to your online security. According to Extreme Networks, a global networking solutions provider, a Wi-Fi attack on a public network can take less than 2 seconds.
The next time you are considering connecting to a public Wi-Fi connection, keep in mind that any data sent while you are connected can easily be tracked by others. That means any password you type or any private message you write – is not that private the second you press send.

Best practices for staying safe while using Public Wi-fi:

- **Think before you connect.** If possible, avoid directly connecting personal devices to a public network. If you must connect to the public Wi-Fi, connect using a Virtual Private Network (VPN) first. VPNs provide a secure way of connecting to the internet by sending user data through an encrypted tunnel and hiding the true IP address.

Before you connect to any public wireless hotspot be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate.

- **Use your mobile network connection.** This is the preferred method, if you are unable to connect to a private network. Your own mobile network connection is generally more secure than using a public wireless network. Use this feature (i.e., turn off your wi-fi feature and use your 5GE/4G/LTE mobile data) if you have it included in your mobile plan.

- **Avoid conducting sensitive activities while on a public Wifi.** Conducting financial transactions or accessing work/school resources while on public networks can be dangerous because it does not provide security or data encryption protection.

- **Keep software up to date.** Application vendors and your phone manufacturer (such as Apple, Android, etc.) release software patches and new versions to fix vulnerabilities and bugs found on their system. Best practice is to install the approved updates as soon as possible unless directed otherwise by our Service Desk. Be sure to always comply with CFPB prompts for system updates in a timely manner so that attackers can't take advantage of known vulnerabilities.

- **Use strong passwords and/or multi-factor authentication (MFA).** Use different passwords for different accounts and devices. Using MFA works by requiring two different methods to authenticate yourself. CFPB laptops use Always on VPN which allows Bureau users to work more efficiently regardless of location. If you have a CFPB laptop and an internet connection, then you are automatically connected to the CFPB VPN. It's a more secure and consistent experience from any location.

November 10, 2020 | CyberWise Tip- Beware of Targeted Ransomware attacks at K-12 student data during COVID-19

COVID-19 has caused a shift to online learning for most K-12 schools in the United States. During this time, there have been reports of more ransomware attacks launched by cybercriminals targeting student data and online safety. Ransomware is a form of malware designed to encrypt the victim's files and then demand ransom in exchange for decrypting the files. Cyber criminals have increasingly targeted K-12 schools and even universities, who typically have fewer cybersecurity resources, in order to extract student data for extortion purposes.

For example, the Clark County School District (CCSD) in Nevada was the target of a ransomware attack in August, which resulted in the student body's data being compromised. Ransomware attacks usually begin with phishing campaigns and "malvertising," which involves injecting malware into legitimate online networks and web pages.

Tips to keep student data protected against ransomware: Keep applications and operating systems are patched and up to date. Updates and patches address weaknesses on a system and its applications (e.g., MSOffice, Chrome, and Adobe). These weaknesses allow "bad guys" to steal your data or control your system. Ensuring that automatic updates are enabled (the system update feature can be found under the Computer settings) will patch these weaknesses and keep your system safe and up to date.

- **Be vigilant with attachments and links in emails**. Malicious emails or phishing usually have red flags. Use your mouse to hover over the links and view the linked landing page before clicking on it.

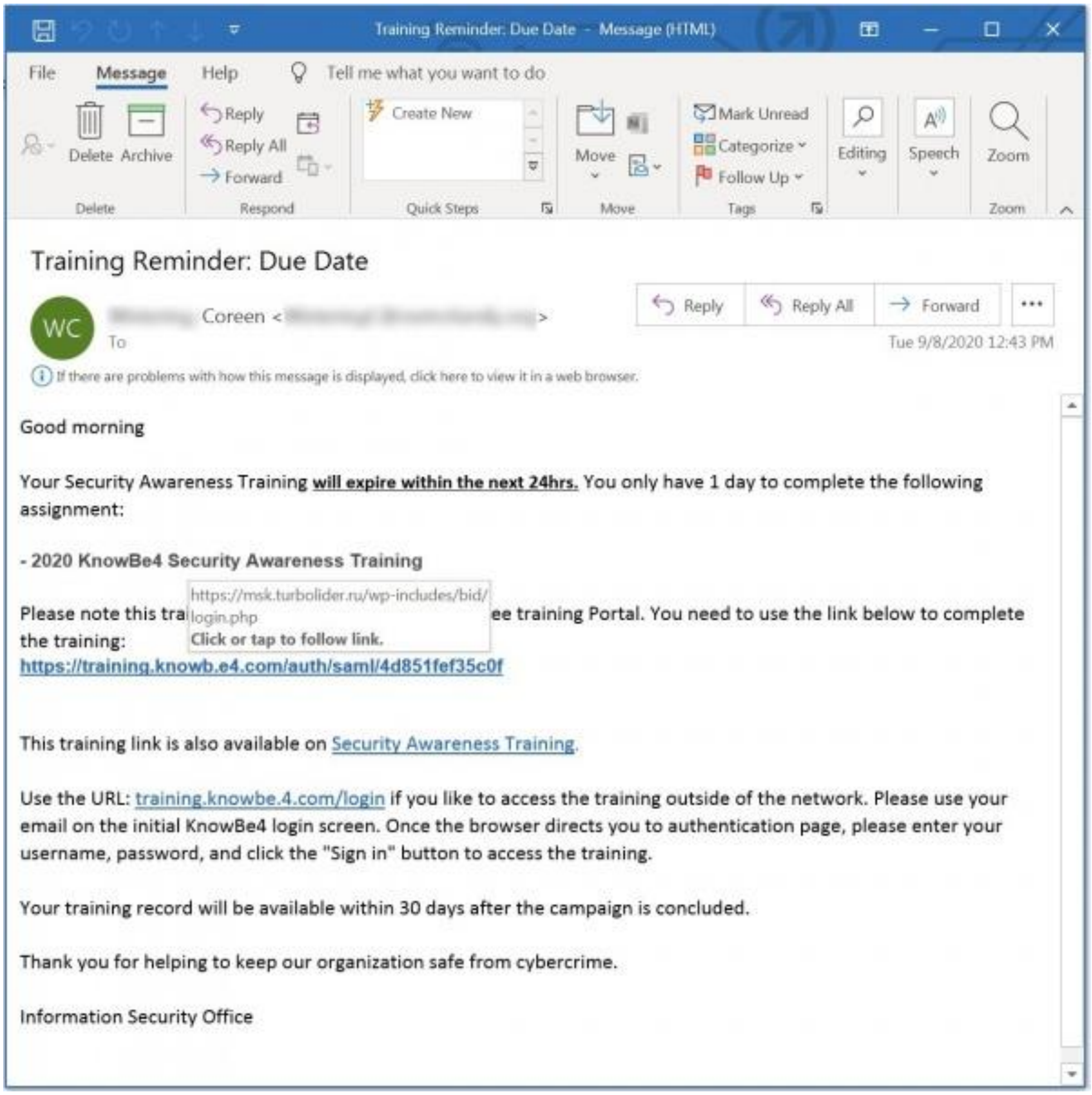
- **Make sure your student backs up their data early and often**. All work, images, and other digital information should be protected by making an electronic copy and storing it safely. If a copy of the data is created before the device falls victim to ransomware, the backup data you can be used to restore all that was stolen.

If you believe you are being targeted by a malicious cyber-attack, please do not open the attachment – Click the “report phishing” button in outlook or send as an attachment to [redacted] (b) (6)

To learn more about the state of Ransomware in K-12, check out this video published by Ed Tech magazine. Check out the Cybersecurity Tip of the week page for more ransomware best practices.

November 09, 2020 | CyberWise Tip - CyberWise tip: Malicious Actors Spoof KnowBe4 Again

Although the Bureau was not impacted, other customers of the security awareness training vendor KnowBe4, reported receiving spoofed KnowBe4 security awareness training emails using the Phish Alert Button (PAB) earlier this fall. The malicious actors gained access to a user's inbox and replicated the training notifications as click-bait for a phishing campaign.



Training Reminder: Due Date

[redacted] Coreen <[redacted]>

To

Tue 9/8/2020 12:43 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

Good morning

Your Security Awareness Training **will expire within the next 24hrs.** You only have 1 day to complete the following assignment:

- 2020 KnowBe4 Security Awareness Training

https://msk.turbolider.ru/wp-includes/bid/login.php
Click or tap to follow link.

Please note this tra ee training Portal. You need to use the link below to complete the training:
https://training.knowb.e4.com/auth/saml/4d851fef35c0f

This training link is also available on Security Awareness Training.

Use the URL: training.knowbe.4.com/login if you like to access the training outside of the network. Please use your email on the initial KnowBe4 login screen. Once the browser directs you to authentication page, please enter your username, password, and click the "Sign in" button to access the training.

Your training record will be available within 30 days after the campaign is concluded.

Thank you for helping to keep our organization safe from cybercrime.

Information Security Office

Image of spoofed KB4 training email

This is a reminder that no one, not even a cybersecurity training company, is immune to being spoofed as part of a malicious email campaign. Online brands, traditional businesses of all sizes, and even government agencies are all susceptible to such attacks, and everyone should be aware of this phenomenon.

How to avoid falling for spoofed emails:

*** Stay vigilant regarding the attachments and links within emails.** Malicious emails or phishing usually have red flags. Be sure to use your mouse button to hover over the links to see where it leads.

- If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your Outlook application or forward as an attachment to (b) (6)

- Check out our watch out for spoofed emails post, to learn more about indicators of a spoofed email.

November 05, 2020 | CyberWise Tip - How to create a secure and perfect password

Leading Security expert, Bruce Schneier, published a technique a decade ago on how to create a strong password by using a sentence to help you remember your passwords.
Use Bruce Schneier's password method to turn a sentence/story into a password. Examples:

- I cannot wait to turn 30 in July = 1CntWa2Tu30In07
- I like to be at home = Il1k32B@Ho
- I went to the shops at work and bought chocolate = 1We2ThSh@Wo&BoCh

Although its critical to create strong passwords, utilizing multi-factor authentication (MFA) is more secure and should be implemented whenever possible. Using MFA works by requiring two different methods to authenticate yourself.

Check out our previously posted Cyber tip on how to create a complex password you can remember too.

November 02, 2020 | CyberWise Tip - Rising Trend of Ransomware Infiltrating Public Schools Leads to Real Consequences

The move to virtual schooling is creating a new host of cybersecurity concerns, affecting teachers, students and parents. There have been over 380 ransomware attacks reported over the last four years, with some incidents compromising both teacher's and student's personal data as well as financial data. In the face of COVID-19, these attacks are also impacting the ability for schools to continue educating their students. Last month, a public school in Yazoo Country, Mississippi revealed it paid a cybersecurity firm $300,000 to help recover data that had been encrypted and stolen in a ransomware incident. The payment made up 1.5% of the entire school budget. Back in September of this year, a school in Hartford, Connecticut had to delay the start of the school year after a ransomware infection. These attacks are also impacting universities; the University of California San Francisco paid a ransom of $1.14 million after negotiating the price down from $3 million.

What can you do to prevent this from happening? If you have children participating in remote learning:

- Be proactive and secure your home network by using Virtual Private Networks (VPNs) and ensuring that the computer has the latest vendor issued system patches
- Ensure the device being used by any student is password protected
- Work with students to save/back up information assignments to school sponsored cloud locations (e.g. Google Drive) securely.
- Do not store Personally Identifiable Information (PII) on school laptops. Best practices state that you should always keep PII off any school electronic devices, whenever possible.

Please see our CyberWise Tip archive for password best practices and read more regarding the school ransomware attacks here.

October 30, 2020 CyberWise Tip: Cyber Fun Fact

Cyber Fun fact

Did you know that cybercriminals can harness the power of your Internet of Things (IoT) devices against you?

Cybercriminals can act locally and globally. They might infiltrate your IoT devices to do you harm. Or they might use your devices and others to launch a broad attack. This happened in 2016, when hundreds of thousands of compromised connected devices were pulled into a botnet dubbed Mirai. A botnet can combine the processing power of small devices to launch a large-scale cyberattack. The result? You may remember when major websites such as Spotify, Netflix, and PayPal were temporarily shut down. To learn more about the Mirai attack, check out this CSO online article which explains how teen scammers and CCTV cameras almost brought down the internet

Thank you for your participation in National Cybersecurity Awareness Month (NCSAM). If you have any questions, please contact [redacted] (b) (6)

October 21, 2020 CyberWise Tip: Using Caution with Email Attachments

Email programs offer many "user-friendly" features – Some email programs have the option to automatically download email attachments, but in doing so can immediately expose your computer to viruses within the attachments. Email is easily circulated and is the main tool that malicious actors use to launch phishing attacks. Features such as forwarding email makes it so easy to send viruses that can quickly infect many machines. Most viruses don't even require users to forward the email, because they scan a user's mailbox for email addresses and automatically send the infected message to all the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open a message that comes from someone they know.

What steps can you take to protect yourself and your contacts?

Be wary of unsolicited attachments, even from people you know.
Just because an email message looks like it came from someone you know does not mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. Be sure to check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments.

Make sure the option to automatically download attachments is turned off.
To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it. Utilize the "preview file" feature available in your Outlook application. Don't let your curiosity put your computer at risk.

October 19, 2020 CyberWise: National Cybersecurity Awareness Month - Week 3!

October is National Cybersecurity Awareness Month (NCSAM)! NCSAM was established to raise awareness about the importance of cybersecurity across our Nation.

This week's theme is **"Securing Devices at Work"** and we have a lot of activities planned to include: a discussion on the how to protect CFPB systems through procurement decisions and virtual escape rooms. Please check out calendar of event on the NCSAM wiki.

If you have any questions, please contact [redacted] (b) (6)

October 16, 2020 NCSAM Cyber Fun fact

Cyber Fun fact Did you know that by 2025, the global collective data will reach 175 zettabytes (that's 175 followed by 21 zeros), according to this video from Seagate Technology. This includes everything from streaming videos, dating apps, and heath care databases. Securing all this data is vital.
October is National Cybersecurity Awareness Month (NCSAM)! Please check out calendar of events on the NCSAM wiki to see what we have planned next week! If you have any questions, please contact [redacted] (b) (6)

October 14, 2020 CyberWise Tip: What are Botnets?

Botnets are a group of computers that work together to accomplish a shared task, they are not malicious by default, but they are made malicious by hackers using malicious code. Botnets use other people's computing resources to accomplish their tasks. Once a device is compromised, they are used to launch distributed denial of service (DDoS) attacks, spread malware, and mine cryptocurrency without the owner of the computer even knowing they have been hijacked.

How to tell your device has been infected by a Botnet?

- Mysterious social media posts being sent from your accounts?

Malicious software attempting to propagate itself can use some ingenious methods of spreading without being detected. One way is via social media. If you've noticed some posts you didn't make yourself, or if people have warned you that you've sent direct messages you know you didn't send it's possible, you're infected. As with the above, malware on your computer may not be the cause of this--your account may have been hacked, your password stolen in a data breach, or another device may be compromised.

- Unable to download system updates?

Some malware, especially the kind that relies on known vulnerabilities, will prevent a computer from downloading updates in order to keep its essential vulnerabilities available for exploitation. If you can't download updates this is a serious issue that needs to be rectified immediately.

- Friends, family, or coworkers mention they received a suspicious email from you that you didn't send?

Botnets often send spam, and if one has infected your computer it can use your accounts to send malicious messages to your contacts

How to keep your devices from becoming a part of a Botnet?

- Always update your operating system whenever new updates are released
- Never download attachments from suspicious sources, or suspicious emails from people you don't know
- Don't click login links in an email—navigate to the website manually and log in from there
- Practice good password hygiene: Don't duplicate passwords, make them complicated, and change them regularly
- Use multi-factor authentication for any services that offer it

Check out our CyberWise archive to learn more about Botnets.

October 13, 2020 CyberWise- National Cybersecurity Awareness Month - Week 2!

Week 2 Theme- Securing Devices at Home

October is National Cybersecurity Awareness Month (NCSAM)! NCSAM was established to raise awareness about the importance of cybersecurity across our Nation.

This week's theme is **"Securing Devices at Home"** and we have a lot of activities planned to include: a discussion on Emerging Cyber Threats, two external speakers from OPM and DHS, and virtual Cyber escape rooms. Please check out calendar of event on the NCSAM wiki.

If you have any questions, please contact [redacted] (b) (6)

October 09, 2020 CyberWise- NCSAM Cyber Fun fact

Did you know that the public sector had over 6800 cyber incidents in 2019, 346 of those with confirmed data disclosure? According to Verizon's 2020 Data Breach Investigations Report, 75% of those incidents were financially motivated, while 19% was motivated by espionage. Of those incidents, 51% of the data compromised was personal data.

October is National Cybersecurity Awareness Month (NCSAM)! Please check out calendar of events on the NCSAM wiki to see what we have planned next week! If you have any questions, please contact [redacted] (b) (6)

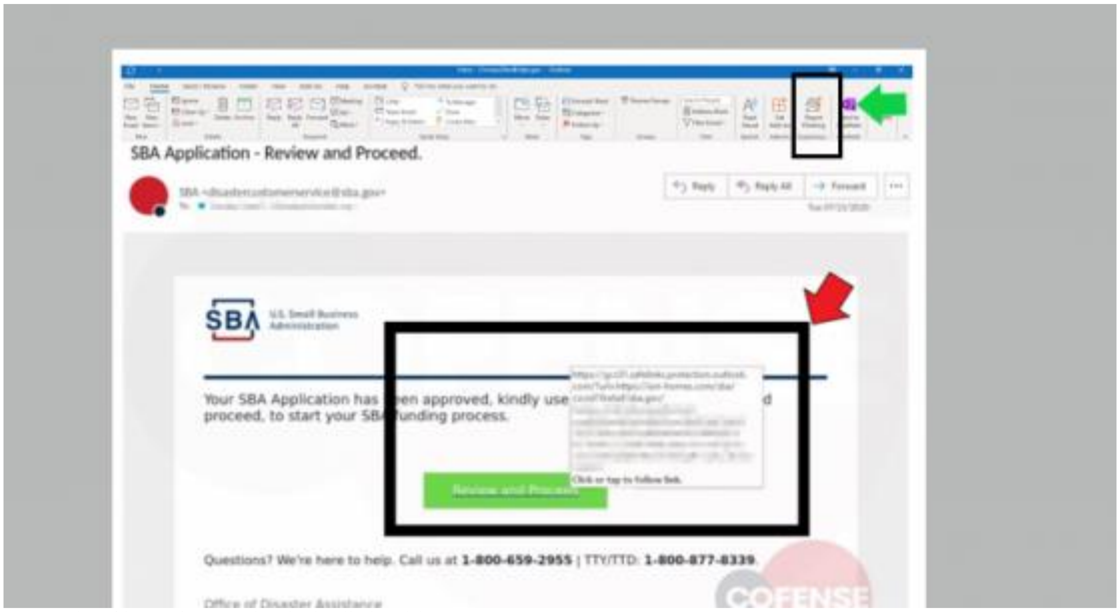
October 08, 2020 CyberWise Tip - Ransomware explained

Last week, the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a best practices Ransomware Guide. This guide is a one-

stop resource intended to help inform, protect, and respond to a ransomware attack and contains two sections focused on ransomware prevention best practices and a ransomware response checklist.
What is Ransomware Ransomware is a form of malware designed to encrypt the victim's and then demand ransom in exchange for decrypting the files. In recent years, the number of ransomware attacks have increased among government entities and critical infrastructure organizations, and have become more destructive and financially damaging, with some demands exceeding US $1 million. Cyber criminals have adjusted their tactics to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as another form of extortion.
Malicious actors use tactics, such as deleting system backups, that make restoration and recovery more difficult or not feasible for the impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

How to protect against ransomware

- Keep applications and operating systems up-to-date on Bureau laptops, personal computers, and mobile devices.
- Be vigilant regarding the attachments and links you decide to click on within emails. Malicious emails or phishing usually have red flags. For example, you can inspect a link or email address by hovering your mouse button over the link to see where it leads. Sometimes, it's obvious the web or email address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.



SBA Application - Review and Proceed.

Your SBA Application has ...en approved, kindly use ... d proceed, to start your SB... funding process.

Questions? We're here to help. Call us at **1-800-659-2955** | TTY/TTD: **1-800-877-8339**.

Office of Disaster Assistance

Reply
Reply All
Forward
SBA U.S. Small Business Administration
Review and Proceed
Click or tap to follow link.
COFENSE

Example of hovering to check the link address

Please do not open the attachment or click a link if you believe the email to be malicious – Click the **"report phishing"** button in Outlook or send the email as an attachment to (b) (6)

- Use multi-factor authentication (MFA) for accounts whenever available. Multi-factor authentication (sometimes called two-factor authentication) works by requiring two different methods to authenticate the user. It is highly recommended that MFA is used for critical services, such as logging into email accounts, online banking, or storing files online as it's a more secure solution than using just passwords. Learn more about MFA from our Cyber Tip of the week archive.

- Back it up early and often. Protect your work, images, and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.
- If you believe you are being targeted by ransomware or any malicious cyber-attack, please contact (b) (6)

Check out our Cybersecurity Tip of the week page for more ransomware best practices and the Ransomware Guide available on CISA's website at www.cisa.gov/publication/ransomware-guide.

Feel free to also see our previous Cyber tip of the week for full guidance on how to protect against ransomware.

October 07, 2020 CyberWise Tip: Make sure you are using HTTPS

Keep it locked down. You've probably seen a little lock to the left of a website that begins with the letters HTTPS. HTTPS sites will encrypt data making them much safer to use. This is important on any device-never provide any personal details to a site that doesn't have HTTPS. Indications that your information will be encrypted include a URL that begins with "https:" instead of "http:" and a lock icon in the left corner of the window like the image below shows.

To protect attackers from hijacking your information, any personal information submitted online should be encrypted so that it can only be read by the appropriate recipient.

Be sure to check the address bar. Look for **https:// (not http) and the lock** before the website address prior to doing anything on the Internet that includes personal information only you should know, like when proving banking or work credentials.
To learn more, check out this CISA protecting your privacy security tip.

October 05, 2020 CyberWise: National Cybersecurity Awareness Month - Week 1!

CyberWise: National Cybersecurity Awareness Month - Week 1!
October is National Cybersecurity Awareness Month (NCSAM)! NCSAM was established to raise awareness about the importance of cybersecurity across our Nation.

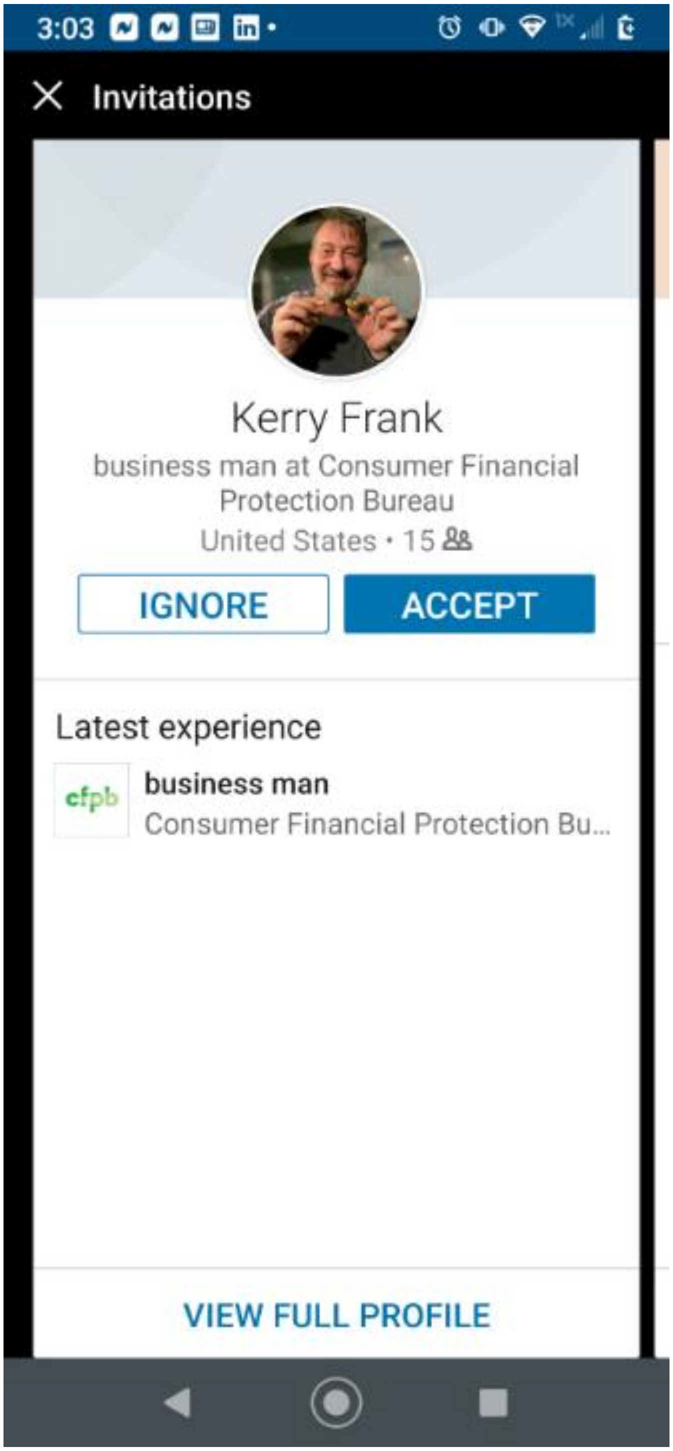
This week's theme is **"If you Connect it, Protect it"** and we have a lot of activities planned, to include: discussion on Kids and Internet Security, online gamification, and virtual escape rooms. Please check out calendar of events on the NCSAM wiki.

If you have any questions, please contact [redacted] (b) (6)

[redacted] 02, 2020 CyberWise- Be on the lookout for fake CFPB connection requests on social media

Scammers have recently been leveraging of a variety of social networks for Social Engineering. Through social engineering, these scammers aim to manipulate individuals into divulging confidential or personal information. As a result, the stolen information may be used for fraudulent purposes such as gaining access to individuals' personal financial information, corporate trade secrets, or even government confidential information. Scammers count on negligence, indifference, and distracted participants. This tip speaks to one of the most common types of Social Engineering attacks that appear on LinkedIn: Scammers creating fake LinkedIn accounts impersonating personnel at organizations.

Picture this: You receive the below LinkedIn request from an individual who claims he works at CFPB. He accompanies his request with a message to you that includes a survey link, asking for feedback on "a recent Bureau-wide update he helped develop."



Kerry Frank

business man at Consumer Financial Protection Bureau

United States • 15

Latest experience

business man

Consumer Financial Protection Bu...

Example of LinkedIn fake job profile. Note the lack of formal job title for the individual

Here is what you should do if you think you received communication linked to a social engineering attack:

1. Confirm that the individual works at the Bureau (check the Active Directory).
2. If you have any reason to doubt the instructions provided, be sure to call or otherwise confirm with someone from the Bureau before interacting with the message, especially if those instructions are likely to grant access to someone else or adversely impact the Bureau.

3. **Stop. Think before you click.** Do not click on unknown links in messages.
4. Report suspicious activity by clicking the “Report Phishing” button in Outlook or sending screenshots of any social media contacts as an attachment to (b) (6)

September 28, 2020 CyberWise- What is Spam?

According to US CERT, “Spam is the electronic version of “junk mail.” The term spam refers to unsolicited, often unwanted, email messages. Spam does not necessarily contain viruses—valid messages from legitimate sources could fall into this category.

Tips to reduce spam in your inboxes

- **Be careful about who you give your email address to.**

Spammers can harvest email addresses posted on a website, so be mindful of who you share your information with. Do not use your CFPB email for non-CFPB related use. Even when you give your email address to a company to be added to a newsletter or for coupons, that information is stored in database so user information can be tracked. If these email databases are sold to or shared with other companies, you can receive email that you didn’t request.

- **Don’t click links in spam messages**.

Some spammers use tools that generate email addresses variations for certain domains (ex: cfpb.gov, gmail.com). When you reply to the message or click a link in the email message, you are just confirming that your email address is valid.

- **Consider opening an additional email account (for non-CFPB use)**.

For online shopping, signing up for services or subscription services (Spotify, Apple Music, Amazon, UberEATS/Door Dash), use a secondary email address to protect your primary email account from any spam. This secondary account can be used when posting to public mailing lists, social media sites, blogs, and web forums. If the account starts to fill up with spam, you can get rid of it and open a different one.

Want to know the difference between a scam (such as phishing attack) and spam? Check out our Scam vs Spam post. For more details, check out US-CERT’s What is spam article.

September 17, 2020 CyberWise- Complete your Cybersecurity Role-Based Training (RBT)!

Strengthen your Cybersecurity knowledge through completing Cybersecurity RBT! Eligible federal employees and contractors with significant information technology (IT) and security responsibilities were notified of their Cybersecurity RBT requirements the first week of August and must complete training by September 30, 2020. Taking Cybersecurity RBT helps creates a common language for cybersecurity and outlines specific knowledge, skills, and abilities we all need to know to do our jobs successfully and continually our Bureau’s security posture. The Cybersecurity RBT requirements are based on guidance provided by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The NICE Cybersecurity Workforce Framework provides a resource for how organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks.

These following NICE categories are used to guide our role-based training program.

- Securely Provision: Conceptualizes designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
- Operate and Maintain: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
- Oversee & Govern: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
- Protect & Defend: Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
- Analyze: Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
- Collect & Operate: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- Investigate: Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

If you have any questions please visit the RBT wiki page.

September 3, 2020 CyberWise: Virtual Private Network (VPN) terms to know

Did you know that more than 80% of Americans are concerned about how companies use their data. Furthermore, ad blockers, VPNs, and anonymizers are becoming the new norm for users seeking more privacy.

A virtual private network (VPN) is a secure way of connecting to the internet by sending user data through an encrypted tunnel and hiding the true IP address. VPN's are used by remote workers who require network access without being on-site and provides a secure method for sending private or confidential communications.

VPN Terms to know:

Encryption - encryption is data conversion from plain text that anyone can read to ciphertext that can only be read by authorized users. Encryption does not prevent hackers from intercepting your data. Instead, it makes your data unreadable.

- To encrypt your data, there are several VPN encryptions protocols your vendor can utilize. OpenVPN is the current golden standard for encryption.

Split tunneling - split tunnel VPN gives users the chance to access public networks like the internet, while simultaneously connected to a local network (either your CFPB network or your home network).

- With split tunneling enabled, users can connect to company servers like database and email through the VPN and all other traffic will be directed through the Internet Service Provider (ISP).

Proxy (or proxy service)- Any computer that reroutes traffic, either as infrastructure or to implement or avoid monitoring.

Check out the full list of VPN terms to know from CNET here

August 28, 2020 CyberWise: Social Engineering 101

Just like computers, people can be “hacked” using a process called social engineering. An estimated 98% of cyberattacks are launched using social engineering. According to security consulting firm Social Engineer, Inc., social engineering is “any act that influences a person to take an action that may or may not be in their best interest.”

Commonly used social engineering attacks:

- Phishing attacks attempt to get unsuspecting users to click on a link, download a file, or respond with personal details.
- Phone spoofing, aka “vishing attacks,” when unsuspecting users receive a call from a scammer attempting to gain personally identifying information or reset a password.
- Baiting attacks involve exploiting someone’s curiosity to get them to something an attacker wants, like plugging in a found USB stick that then injects malware into a network.
- SMS spoofing aka “SMiShing attacks” are used to convince smartphone users to call a number set up to harvest data, steal bank account information, etc.

These techniques present a false front that convinces someone to do something, unwittingly, against their best interests.

Recent real-life social engineer attack examples:

- In late February 2020, an unknown party successfully conned Shark Tank investor Barbara Corcoran out of nearly $400,000 by sending a phishing email with a fake renovation invoice. The attackers used an email nearly identical to her assistant's email address to trick her.
- In 2015, a 15-year old British boy successfully vished his way into the accounts of CIA chief John Brennan, FBI director Mark Giuliano, and US Homeland Security secretary Jeh Johnson, stealing government documents, resetting personal iPads, and displaying taunting messages on Johnson's home television.

How to protect yourself against social engineer attacks?

Be aware of what information you make available because most social engineering attacks rely on knowing something about the intended target. Something as seemingly innocent as posting a photo of your birthday party, vacation location, favorite book, or even the name of your pet gives a social engineer several security question attempts, PIN tries, and password guesses.

- Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.
- Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email.
- Look for generic greetings. Phishing emails or vishing calls are unlikely to use your name. Greetings like "Dear sir or madam" signal this is not a legitimate actor.
- Avoid emails that insist you act now. A common manipulation tactic malicious actor use is creating a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete or report the message
- If you believe you are experiencing a social engineering attack please do not open the attachment – click the "Report Phishing" button in Outlook or send as an attachment to (b) (6)

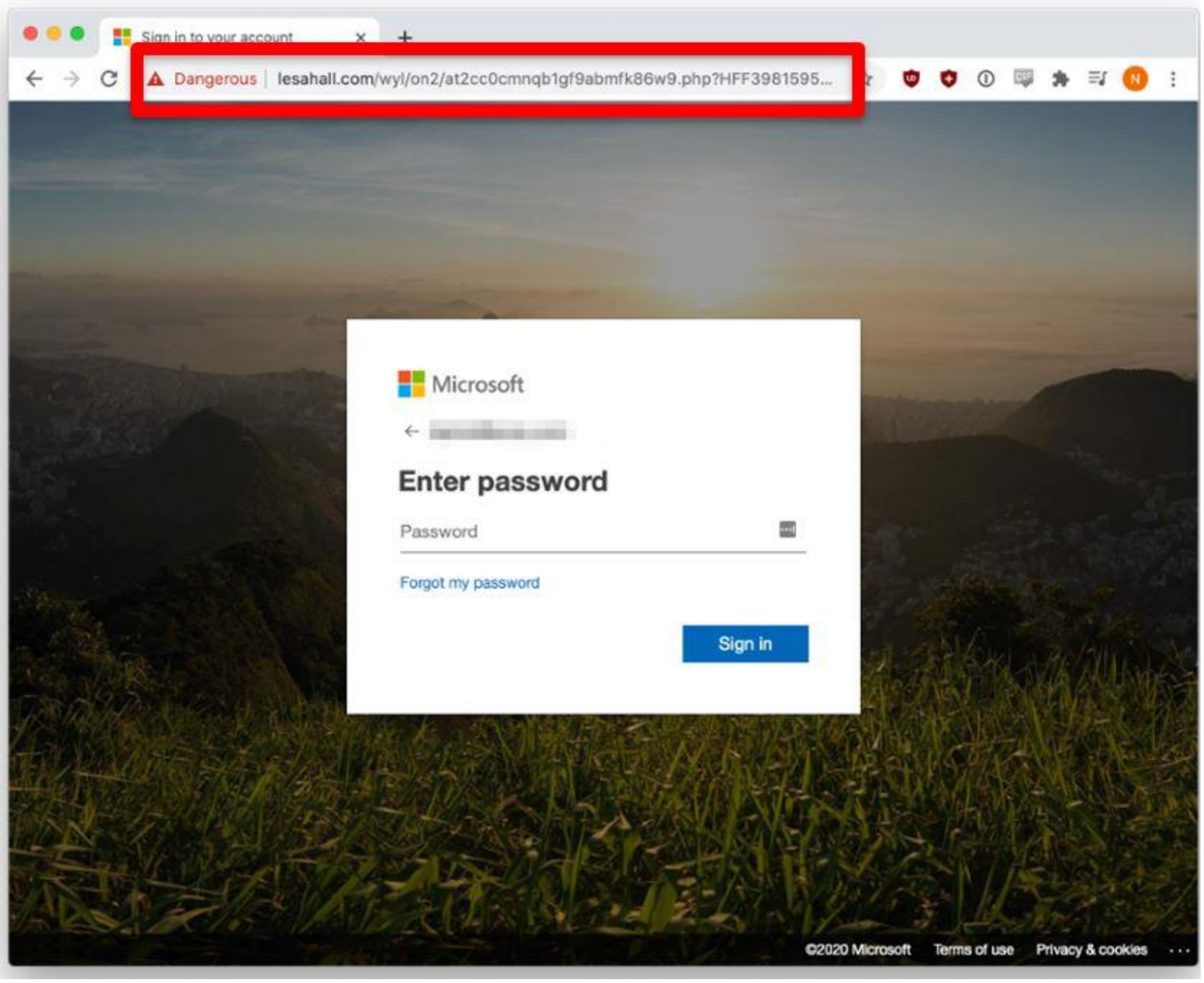
See our previous post 5 clues that an email is really a phishing scam

August 27, 2020 CyberWise: Explosion of Zoom Meeting Phishing Attacks Targeting O365 and Outlook

Did you know that more than 90% of successful hacks and data breaches start with phishing scams? Researchers at INKY have reported an increase of Zoom-themed phishing attacks starting in the spring of 2020. See our previously posted tips on how to spot red flags of a potential phishing email. Most of these attacks use hijacked accounts and legitimate looking spoofed domains (ex: zoomcommuncations.com and zoomvideoconfrence.com). Ultimately, they attempt to steal credentials to services like Outlook and Office 365 by directing users to spoofed login pages.

Watch out for spoofed domains

During this attack, victims that clicked on either malicious links or HTM/HTML attachments were directed to spoofed Office365 and Outlook login pages, like the one shown below. If the hacker includes a fake attachment, it often leads to a fake login page that’s hosted on the recipient’s computer, not by Microsoft.

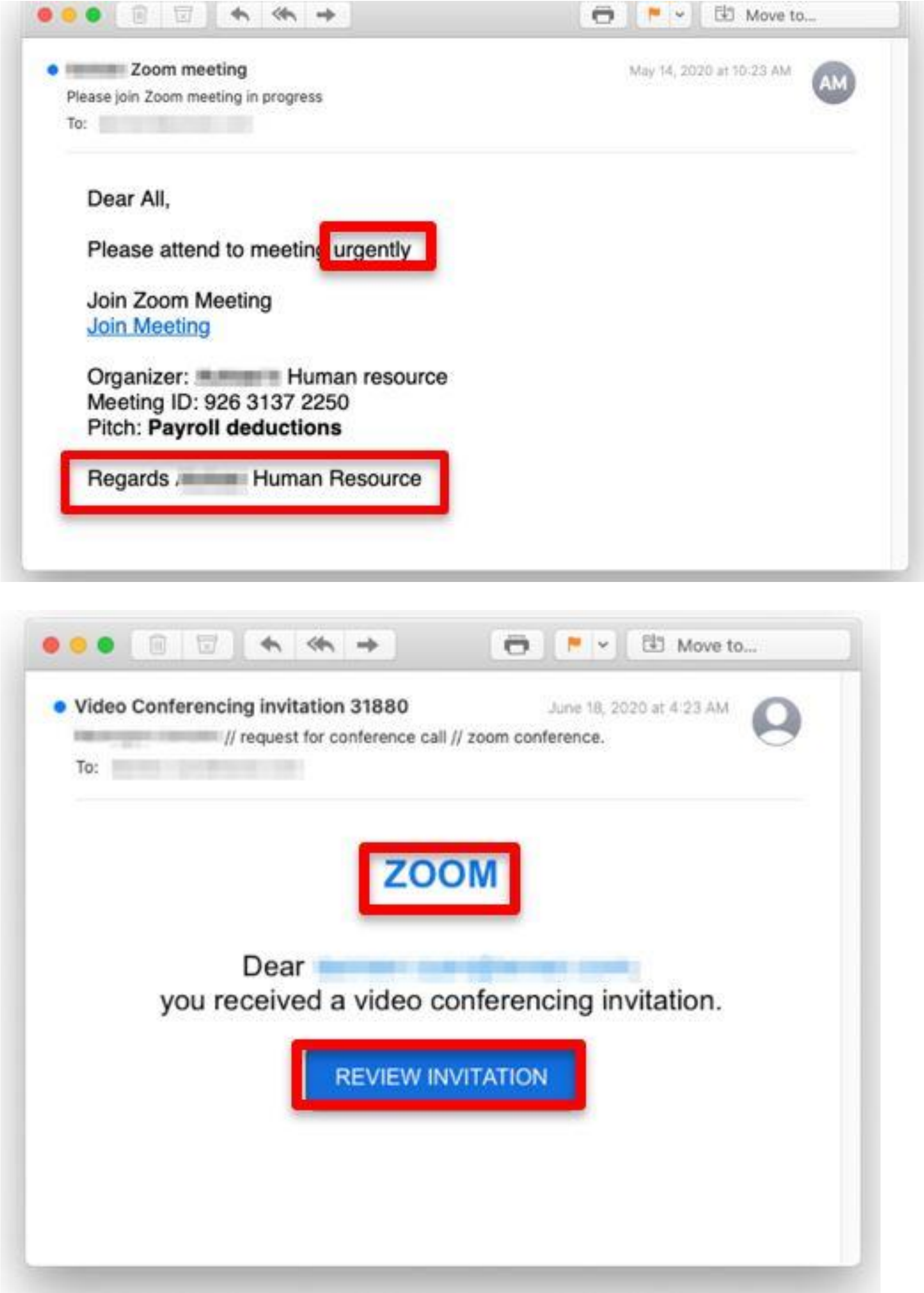


Dangerous | lesahall.com/wyl/on2/at2cc0cmnqb1gf9abmfk86w9.php?HFF3981595...

Image of a fake login page that’s hosted on the recipient’s computer, not the internet

Stop and think before you click

Similarly, the hackers also included a malicious link, which redirected to a fake login hosted on a compromised server or a hosting service the attacker paid for. When the victim entered their login credentials, that data was directly emailed to the hacker or stored on a compromised server. These fake login pages look very convincing because hackers simply copy and paste real source code from Microsoft.



[redacted] Zoom meeting

May 14, 2020 at 10:23 AM

AM

Please join Zoom meeting in progress

To: [redacted]

Dear All,

Please attend to meeting urgently

Join Zoom Meeting
Join Meeting

Organizer: [redacted] Human resource
Meeting ID: 926 3137 2250
Pitch: **Payroll deductions**

Regards [redacted] Human Resource

Video Conferencing invitation 31880

June 18, 2020 at 4:23 AM

[redacted] // request for conference call // zoom conference.

To: [redacted]

ZOOM

Dear [redacted]
you received a video conferencing invitation.

Example of a Zoom phishing attempts using malicious links and indicators of malicious activity.

Check out the full Zoom credential phishing scam report by Inky here.

August 21, 2020 CyberWise: Mobile Device Cybersecurity

Did you know that mobile devices such as smartphones and video game systems are just as vulnerable to a cybersecurity attack as your desktop computer or laptop?

Many electronic devices are computers—from cell phones, tablets, to video games, and GPS devices. While computers offer many fun and convenient features and flexibility they also introduce new risks. There are cybersecurity tools attackers can use to target devices previously considered "safe." For example, a malicious actor may try to infect your cell phone with a virus to secure access to the data on your device.

Not only does this expose your personal information, which users should not store on their CFPB provided devices, this can also be very detrimental if you store corporate information on the same device and vice versa.

How can you protect your devices?

Physical security. Do not leave your device unattended in public or easily accessible area. Access to a device makes it easier for an attacker to extract or corrupt information.

- Only use sites that begin with “https://” when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.

Use strong passwords. Create passwords difficult for malicious actors to guess (Pro tip: do not use any words found in the dictionary), and use different passwords for different accounts, services, devices. You should not allow your computer to remember your passwords, if a criminal gains access to your web browser, they will gain access to all your saved passwords too. (See Cyber Wise Tips to Protect your ID and Passwords Online)

Disable remote connectivity. Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.

- Stop auto connecting to wireless networks. Some devices will automatically seek and connect to available wireless networks. Disable these features so that you only connect to wireless and Bluetooth networks when you want to.

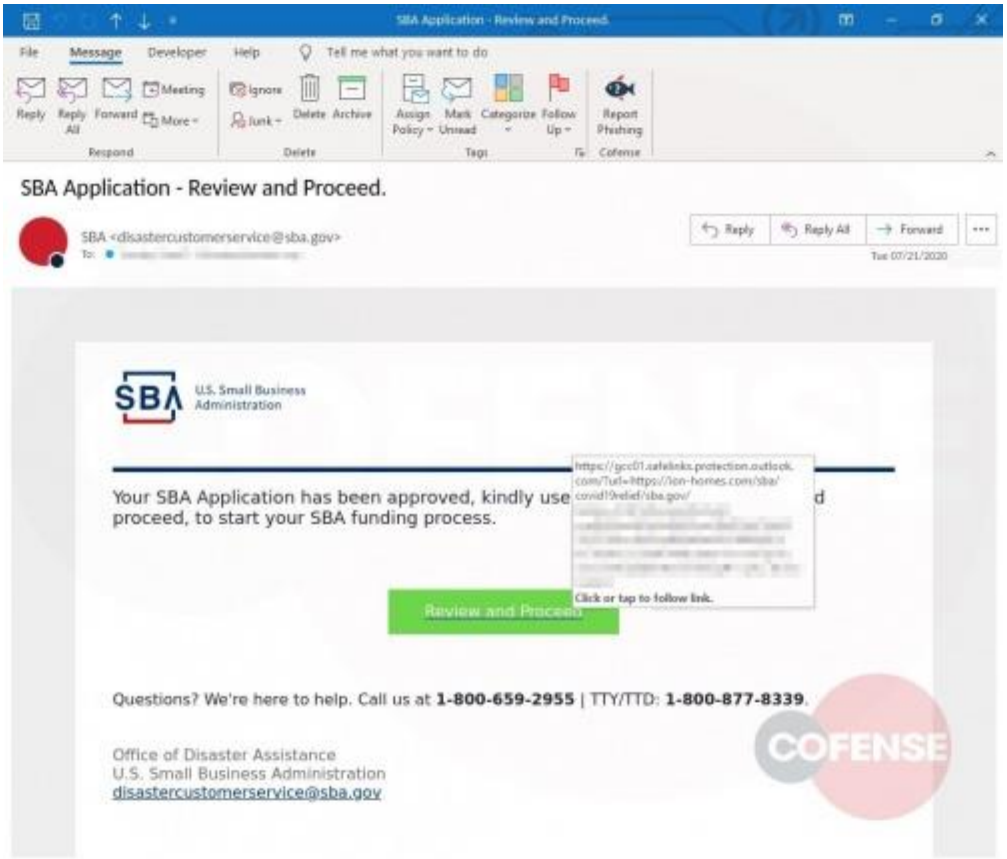
Encrypt files. If you are storing personal or corporate information, see if your device offers the option to encrypt the files. By encrypting files, unauthorized people are unable to view the data even if they can physically access it. When you use encryption, it’s important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.

Use Public Wi-Fi with caution. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, while connected to a public wireless (Wi-Fi) network

August 20, 2020 CyberWise: Coronavirus phishing emails: How to protect against COVID-19 scams

Cybercriminals will always exploit a crisis, and the coronavirus outbreak is no different. In recent months, cybercriminals have leveraged the COVID-19 pandemic to stage more phishing attacks. As a genre of cybercrime, phishing attacks are nothing new. Phishing scams vary in complexity, but at the heart of it all, the goal is to get an individual to download malware or give away personal information via email or phone by exploiting their fear, anxiety, curiosity or trust.

Often, cybercriminals pose as a trusted friend, official government agency or a well-known business. In fact, there have already been numerous phishing scams related to COVID-19 relief aid programs offered through the World Health Organization (WHO) and the United Nations (UN) since the start of the outbreak. More recently, a new phishing scam targeting Paycheck Protection Program (PPP) loan recipients appears to be an email from the Small Business Administration (SBA). The email includes the SBA logo and asks the recipient to download, sign, and return the documents.



SBA Application - Review and Proceed.

SBA <disastercustomerservice@sba.gov>
To: [redacted]
Tue 07/21/2020

Your SBA Application has been approved, kindly use [...] d proceed, to start your SBA funding process.

https://gcc01.safelinks.protection.outlook.com/?url=https://ion-homes.com/sba/covid19relief/sba.gov/
[redacted]
Click or tap to follow link.

Questions? We're here to help. Call us at **1-800-659-2955** | TTY/TTD: **1-800-877-8339**.

Office of Disaster Assistance
U.S. Small Business Administration
disastercustomerservice@sba.gov

Figure 1 Example of Malicious Phishing Email.

The email body of this phish is very clean, well-constructed, and looks legitimate at a glance. The threat actor has even compiled legitimate logo images and contact information to help sell the deception. When you hover over the “Review and Proceed” button, however, it is clear that this is a phish. Instead of sending users to SBA.gov, this button will redirect to the phishing page: hXXps://ion-homes.com/sba/covid19relief/sba.gov/.

Phishing is a serious threat that can cost individuals and companies both money and peace of mind. Hackers are always changing tactics to exploit our greatest vulnerabilities. To stay ahead of these criminals, we must be vigilant, especially during the pandemic. Here are some ways to recognize and avoid coronavirus-themed phishing emails:

* **Beware of online requests for personal information.** A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.

* **Check the email address or link.** You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.

* **Watch for spelling and grammatical mistakes.** If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email.

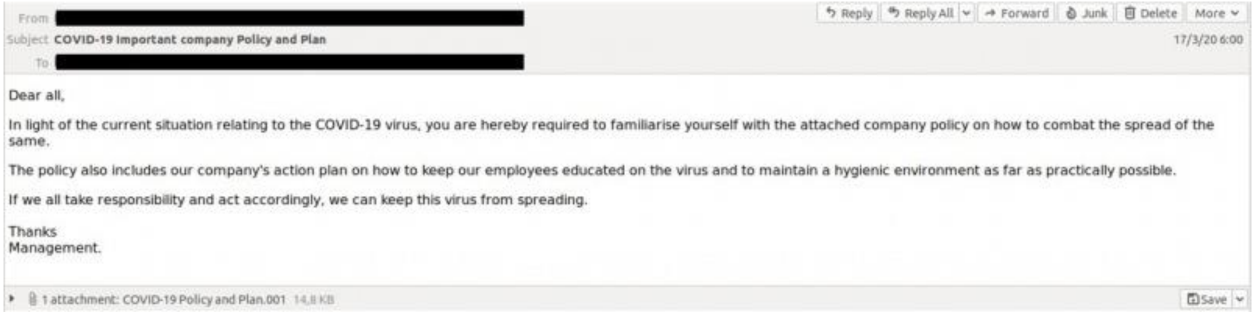
* **Look for generic greetings.** Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.

* **Avoid emails that insist you act now.** Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete or report the message
If you believe you are being targeted by a phishing campaign, please do not open the attachment – click the "Report Phishing" button in Outlook or send as an attachment to (b) (6)

August 13, 2020 CyberWise: Be Aware of COVID Scam- RATicate Upgrades Attacks

RATicate is a group of actors spreading remote administration tools (RATs) and malware via malicious email campaigns.

During a recent email campaign, RATicate attempted to distribute the Lokibot password-stealing malware by using an email message to spoof company emails on COVID-19 response policy and lure targeted users to open the malicious attachment.



From [redacted]
Subject COVID-19 Important company Policy and Plan
17/3/20 6:00
To [redacted]

Dear all,

In light of the current situation relating to the COVID-19 virus, you are hereby required to familiarise yourself with the attached company policy on how to combat the spread of the same.

The policy also includes our company's action plan on how to keep our employees educated on the virus and to maintain a hygienic environment as far as practically possible.

If we all take responsibility and act accordingly, we can keep this virus from spreading.

Thanks
Management.

1 attachment: COVID-19 Policy and Plan.001 14,8 KB

A COVID-19 themed email carrying a RATicate-authored malware installer

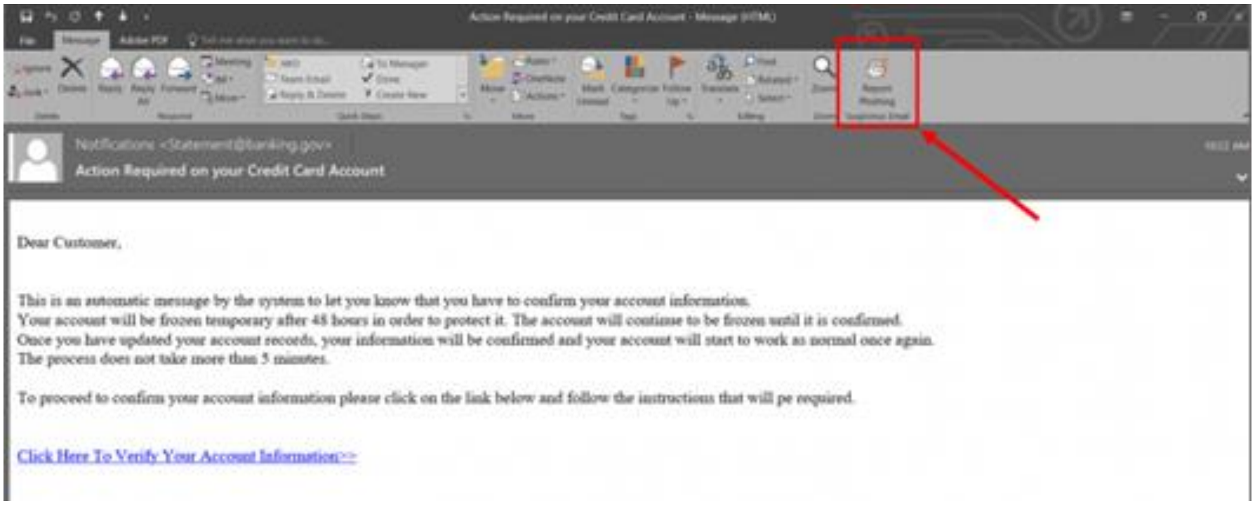
Recommendations:

- Watch out for vague language or a generic request to click on a link or enter information.
- Think twice before clicking on links found in emails, especially if you don't know the sender.
- Call the sender to verify that they sent you an email if the tone or wording does not sound like him or her. It is easy for a cyber attacker to create a message that appears to be from a friend or coworker.
- Watch out for a generic salutation like "Dear Customer." Most companies or friends contacting you know and will use your name.
- Use the common-sense approach as your best defense. If an email or message seems odd, suspicious, or too good to be true, it may be a phishing attack.
- Do not open the attachment if you believe you are being targeted by a phishing campaign.
- Follow the instructions below to report a phishing attempt.

For Microsoft Windows Users with Outlook 2016:

Use the Report Phishing button

1. Click the "Report Phishing" button while the email is open.



Notifications <Statement@banking.gov>

Action Required on your Credit Card Account

Dear Customer,

This is an automatic message by the system to let you know that you have to confirm your account information.
Your account will be frozen temporary after 48 hours in order to protect it. The account will continue to be frozen until it is confirmed.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.

To proceed to confirm your account information please click on the link below and follow the instructions that will pe required.

Click Here To Verify Your Account Information>>

2. A prompt will ask you if you want to report the email as a phishing email. Click Yes to report the email or click No to not report the email.

The email you report will be forwarded to the Suspect Inbox (b) (6) and then deleted from your inbox. If you report an email in error, you can retrieve the email from your Trash/Deleted Items.

For Mac Users:

1. Send the suspicious email as an attachment to the Suspect Inbox (b) (6)

2. Wait for a response from CFPB Security Operation Center (SOC). After forwarding the email, CFPB

SOC will respond back with an acknowledgment of receipt and will provide you proper handling procedures after investigating the email.

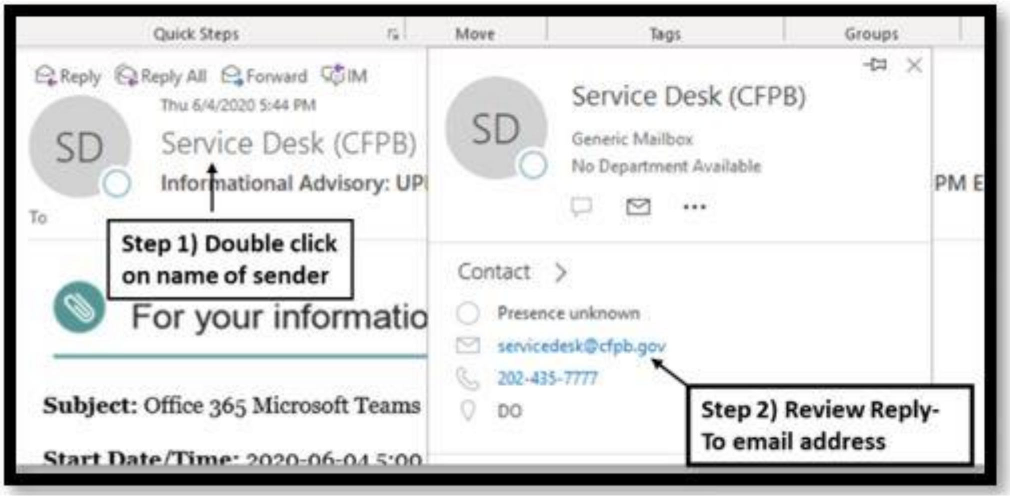
3. DO NOT open any attachments, click any links within the body of the email or forward the email to anyone other than (b) (6).

For more detailed information, please visit the Phishing Wiki page

August 10, 2020 CyberWise: How to recognize a suspicious email and what steps to take to protect yourself and the Bureau

Have you ever received an email and noticed any of the following indicators of a phishing attempt?

- The email includes a generic salutation like “Dear Customer” or has poor grammar or spelling
- The email requests highly sensitive information, such as your credit card number, password, or any other information that a legitimate sender should already know
- When you hover over the link to a website in the body of the email and the link does not go to the actual destination or website (e.g. www.google.com may be redirected to www.suspicious.com)
- The email includes an attachment that you weren’t expecting. Attachments, such as a PDF or Word doc, can include malicious software or a phishing link that can be activated when clicked/opened
- The email comes from someone you know, but the tone or wording does not sound like him or her
- The email address is “spoofed.” Spoofed email addresses appear to come from a Bureau email address (such as from your boss) but has a Reply-To address going to someone’s personal email account. Follow the steps in the figure below to validate Reply-To address.



Step 1) Double click on name of sender

Step 2) Review Reply-To email address

Thu 6/4/2020 5:44 PM

Service Desk (CFPB)

Informational Advisory: UP

For your informatio

Subject: Office 365 Microsoft Teams

Start Date/Time: 2020-06-04 5:00

Service Desk (CFPB)

Generic Mailbox

No Department Available

Contact

Presence unknown

servicedesk@cfpb.gov

202-435-7777

DO

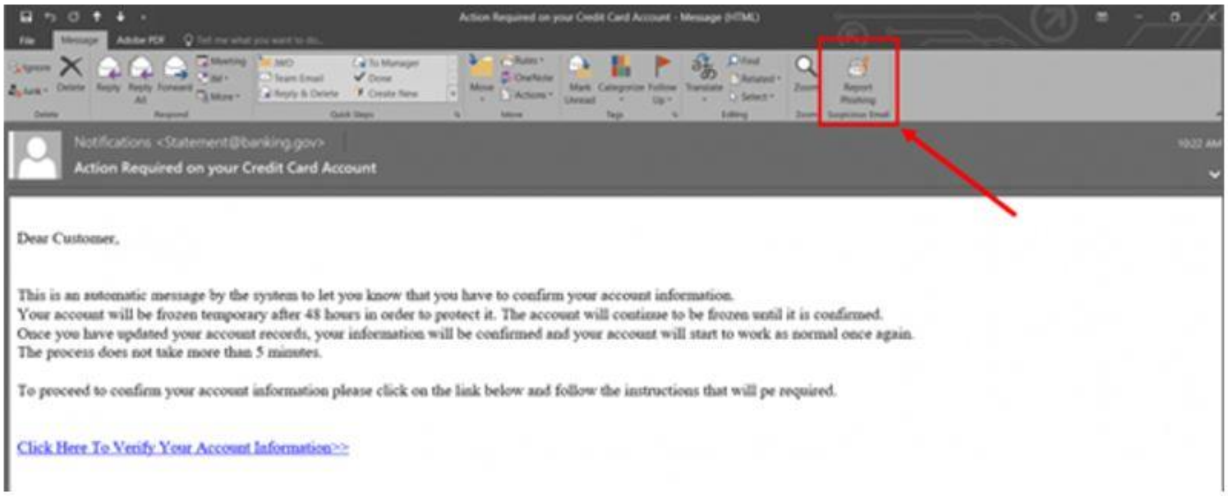
If so, this could be evidence of a phishing email. Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. A phishing email could result in your personal information, such as account usernames and passwords being compromised, or it could expose your computer to malicious code.

So, how can you help the Bureau prevent incidents caused by phishing?

1. STOP. THINK before you CLICK Do not click any links or attachments that are included in a suspicious email. **2. Immediately report the suspicious email to the CFPB Suspect Inbox:**

For Microsoft Windows Users with Outlook 2016: **Use the Report Phishing button**

1. Click the “Report Phishing” button while the email is open.



Notifications <Statement@banking.gov>

Action Required on your Credit Card Account

Dear Customer,

This is an automatic message by the system to let you know that you have to confirm your account information.
Your account will be frozen temporary after 48 hours in order to protect it. The account will continue to be frozen until it is confirmed.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.

To proceed to confirm your account information please click on the link below and follow the instructions that will pe required.

Click Here To Verify Your Account Information>>

2. A prompt will ask you if you want to report the email as a phishing email. Click **Yes** to report the email or click **No** to not report the email.

The email you report will be forwarded to the Suspect Inbox (b) (6) and then deleted from your inbox. If you report an email in error, you can retrieve the email from your Trash/Deleted Items.

For Mac Users:

1. Send the suspicious email as an attachment to the Suspect Inbox (b) (6)

2. Wait for a response from CFPB Security Operation Center (SOC). After forwarding the email, CFPB SOC will respond back with an acknowledgment of receipt and will provide you proper handling procedures after investigating the email.

3. DO NOT open any attachments, click any links within the body of the email or forward the email to anyone other than (b) (6).

For more detailed information, please visit the Phishing Wiki page.

August 7, 2020 CyberWise: Home Distractions a Major Cause of Cybersecurity Errors During Lockdown

During the height of the COVID-19 pandemic in April, InfoSecurity Magazine conducted an analysis of major cybersecurity incidents which showed that the additional stress and distractions of remote working are making organizations more vulnerable to cyber-attacks facilitated by human error.

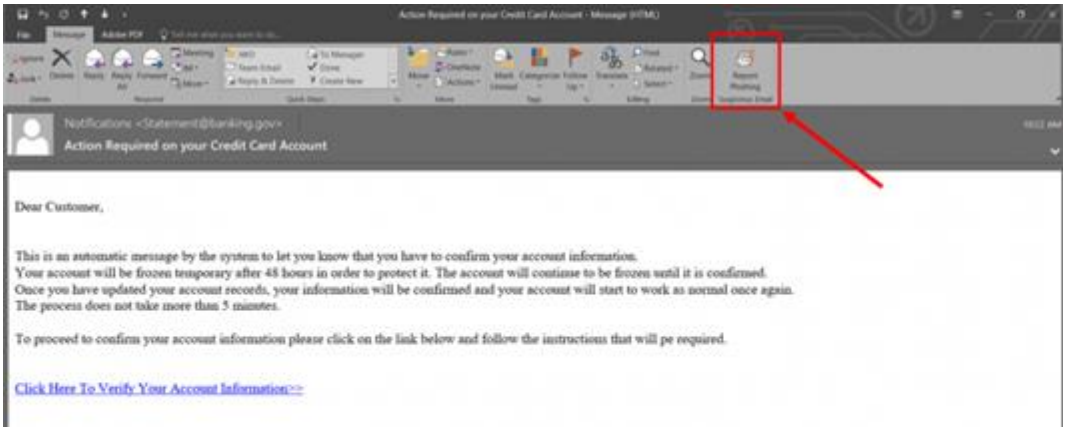
These cybersecurity errors most commonly occurred in the technology sector (47%). Additionally, 20% of companies revealed they have lost customers due to sending an email to the wrong person. This was a mistake 58% of employees admitted to making and a further 10% said they faced drastic consequences as a result.

Recommendations:

- Watch out for vague language or a generic request to click on a link or enter information.
- Think twice before clicking on links found in emails, especially if you don't know the sender.
- Call the sender to verify that they sent you an email if the tone or wording does not sound like him or her. It is easy for a cyber attacker to create a message that appears to be from a friend or coworker.
- Watch out for a generic salutation like "Dear Customer." Most companies or friends contacting you know and will use your name.
- Use the common-sense approach as your best defense. If an email or message seems odd, suspicious, or too good to be true, it may be a phishing attack.
- Do not open the attachment if you believe you are being targeted by a phishing campaign. Follow the instructions below to report a phishing attempt.

For Microsoft Windows Users with Outlook 2016: Use the Report Phishing button

1) Click the "Report Phishing" button while the email is open.



Notifications <Statement@banking.gov>

Action Required on your Credit Card Account

Dear Customer,

This is an automatic message by the system to let you know that you have to confirm your account information.
Your account will be frozen temporary after 48 hours in order to protect it. The account will continue to be frozen until it is confirmed.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.

To proceed to confirm your account information please click on the link below and follow the instructions that will pe required.

Click Here To Verify Your Account Information>>

2) A prompt will ask you if you want to report the email as a phishing email. Click Yes to report the email or click No to not report the email.

The email you report will be forwarded to the Suspect Inbox [redacted] (b) (6) and then deleted from your inbox. If you report an email in error, you can retrieve the email from your Trash/Deleted Items.

For Mac Users:

1) Send the suspicious email as an attachment to the Suspect Inbox [redacted] (b) (6).

2) Wait for a response from CFPB Security Operation Center (SOC). After forwarding the email, CFPB SOC will respond back with an acknowledgment of receipt and will provide you proper handling procedures after investigating the email.

3) DO NOT open any attachments, click any links within the body of the email or forward the email to anyone other than [redacted] (b) (6)

For more detailed information, please visit the CFPB Phishing wiki page.

July 23, 2020 CyberWise Tip- Brazilian banking malware goes global

Cofense Phishing Defense Center (PDC) has notified the CFPB Computer Security Incident Response Team (CSIRT) of a new Covid-19 themed malware phishing campaign in which originated in Brazil that we want to use as a malware attack example to be aware of.

Note: CSIRT reviews all published reports for any new technical indicator information to apply to Bureau defenses.

There has been a group of four large Trojan malware families created, developed and spread by Brazilian malicious actors, now being spread on a global level. The article on SecureList offers a deep dive explanation of these four banking trojan families: Guildma, Javali, Melcoz and Grandoreiro, as they expand abroad, targeting users not just in Brazil, but throughout Latin America and Europe.
The malware family relies on anti-debugging, anti-virtualization and anti-emulation tricks, and New Technology File system (NTFS) is the file system that the Windows operating system uses for storing and retrieving files) Alternate Data Streams to store downloaded payloads that come from cloud hosting services such as CloudFlare's Workers, Amazon AWS and popular websites like YouTube and Facebook.

This attack is relies heavily on emails containing a malicious file in compressed format, attached to the email body. Most of the phishing messages emulate business requests, packages sent over courier services or any other regular corporate subjects, including the **COVID-19 pandemic**, but always with a corporate appearance.

<u>Recommendations to avoid this threat:</u>

- Watch out for vague language or a generic request to click on a link or enter information.
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

  For examples of social media attacks to be aware of, view our Tip of the Week wiki here.

July 22, 2020 CyberWise Tip- Spoofed HR Credential Phishing Attack

Cofense Phishing Defense Center (PDC) has notified the CFPB Computer Security Incident Response Team (CSIRT) of a new Covid-19 themed phishing campaign in which attackers spoofed an email from the recipient's HR department in order to steal user account credentials by utilizing the IRS extended tax filing deadline date of (July 15) due to the COVID-19 pandemic. Although Tax day has passed, this kind of attack is likely to occur again so this tip is provided in order to remain vigilant and educate on the red flags to be aware of when receiving any email communications.

What was the attack? Email Attack: The message spoofs (mimics an internal notification of the recipient's company) the email domain of the recipient's company, with a brief message in the body claiming that the recipient must verify their W2 file. The email contains a .jpg attachment that is embedded with a link that leads to the credential phishing website.

Payload: It contains a malicious link hosted on a site controlled by the attacker which imitates the Microsoft Outlook login page. The webpage has the recipient's work email address auto filled, so the recipient is only required to enter their account password.

Result: Users will have their login credentials and any other information stored on their Microsoft Outlook account compromised.

Why is this attack effective?

Urgency: Once receiving this message, five days prior to the US tax submission deadline, the recipient might panic due to the limited timeline available to correct any information before the tax deadline. Due to the urgency that this creates, recipients may overlook important red flags.

Concealed URL: The payload link is hidden in the .jpg email attachment. So, the recipient may not be able to verify the validity of the URL before clicking on it and may not realize that the link is malicious.

Spoofed email and landing page: The email looks like it's coming from the HR department of the recipient's company, due to the attacker successfully spoofing the email domain of the company. The landing page of the attack looks identical to the Microsoft login page and is hosted on a domain that is registered by Microsoft.

Recommendations to avoid this threat:

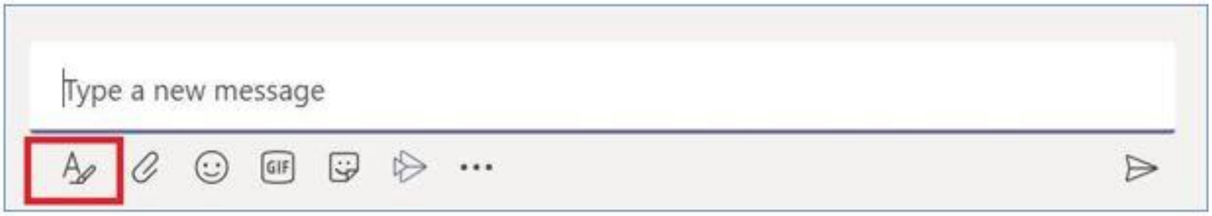
- Watch out for vague language or a generic request to click on a link or enter information.
- Call the individual personally if possible, to see if the message was legitimate
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the **"report phish"** button in outlook or send as an attachment to (b) (6)

July 21, 2020 CyberWise Tip- Microsoft Teams Messaging best practice

In coordination with the Cloud Office Team, there is a MS Teams chatting feature best practice tip the Cyber team would like to share.

Microsoft Teams Messaging best practice

Pressing **"Enter"** on the keyboard will automatically send the chat message. Users may want to get used to clicking the **Format icon** (which is the first option on the chat bar. For reference see image below) *BEFORE* they start drafting a chat message. That way, if they press "Enter" on the keyboard, it will just create a new hard return/line and won't send the message accidentally. The only way they can send the message when viewing the format options will be to click the **Send** button.



Friendly reminder: Users should not use 1:1 or group chat for sending sensitive information including sharing files with CSI, PII, or CII data.

Data & Privacy on MS Teams More information around sensitive data and Teams will be provided once the full version of Teams is rolled out across the Bureau. For more information and training resources regarding Microsoft Teams, view the Cloud Office MS Teams wiki page.

July 17, 2020 CyberWise Tip- Beware of New COVID Tax Relief Act phishing campaign

New Covid-19 Phish Abuses Tax Relief Act to Steal Credentials

The Cybersecurity & Infrastructure Security Agency (CISA) has notified the CFPB Computer Security Incident Response Team (CSIRT) of a new phishing attack campaign which attempts to use the tax relief act to steal user credentials. In this attack, the user is sent a malicious email impersonating the "US Department of Revenue" with the subject: **CARES Relief Certificate**

The message body references information regarding the 2019 Act that has received attention in media outlets and social platforms. The clickbait includes references to an application deadline and links to a fake IRS website using a top-level domain in a New Zealand territory. If you believe you are being targeted by a malicious cyber-attack, please do not open the attachment – Click the *"report phish"* button in outlook or send as an attachment to (b) (6)

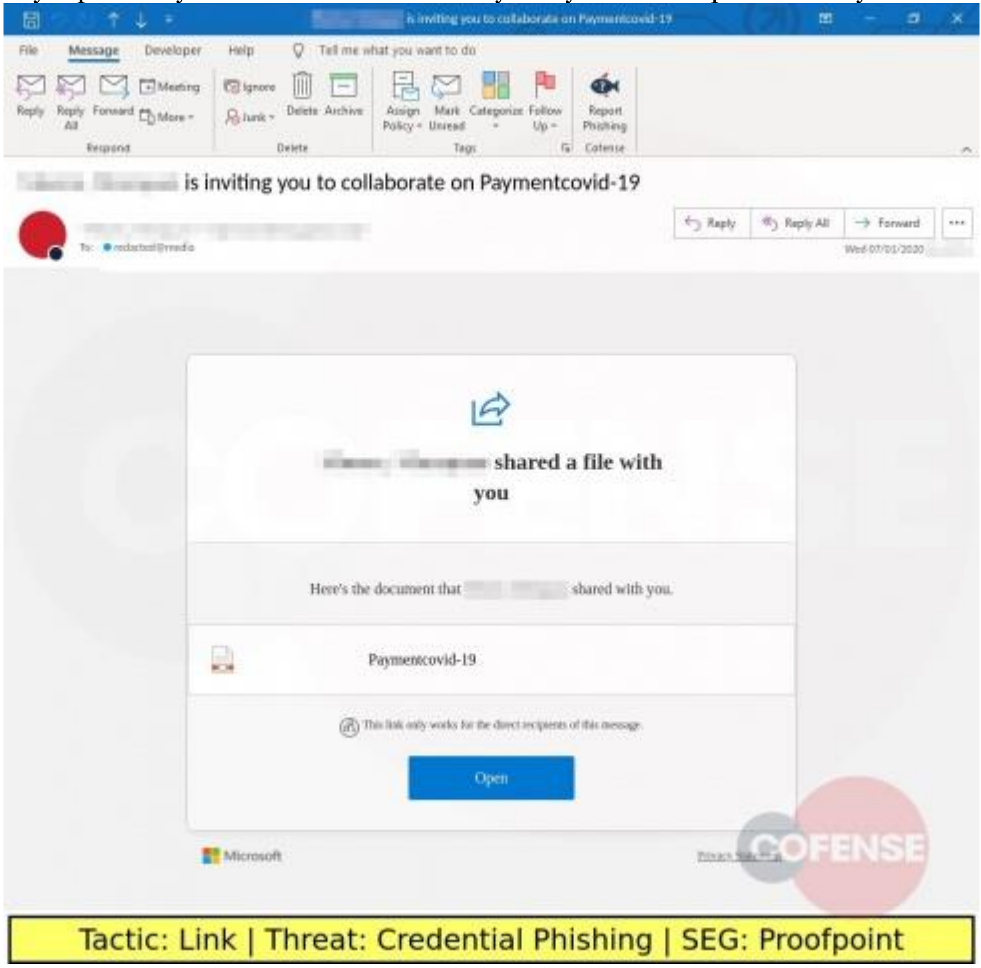
Recommendations to avoid this threat:

- Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address
- Watch out for vague language or a generic request to click on a link or enter information.
- Call the individual personally if possible, to see if the message was legitimate
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance.

- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the “report phish” button in outlook or send as an attachment to (b) (6)

July 16, 2020 CyberWise Tip- Phishing emails are being found in Proofpoint-protected environments

Cofense Phishing Defense Center (PDC) has notified the CFPB Computer Security Incident Response Team (CSIRT) of phishing email campaigns found in Proofpoint-protected environments, which are environments protected by advanced tools such as Secure Email Gateways (SEGs). These attacks were successfully reported by humans and automatically analyzed and dispositioned by their triage platform.



is inviting you to collaborate on Paymentcovid-19

shared a file with you

Here's the document that shared with you.

Paymentcovid-19

This link only works for the direct recipients of this message.

Open

Tactic: Link | Threat: Credential Phishing | SEG: Proofpoint

Many companies are rolling out multi-factor authentication (MFA) solutions to reduce the risk from compromised accounts. Learn more about MFA from our Tip of the week archive.

It is recommended that organizations train their personnel to identify and report these suspicious emails.

Recommendations to avoid this threat:

- Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address
- Watch out for vague language or a generic request to click on a link or enter information.
- Call the individual personally if possible, to see if the message was legitimate
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

July 15, 2020 CyberWise Tip- Beware of Spoofed Zoom Notification Attacks

Spoofed Zoom Attack

Attackers are impersonating a notification from Zoom in order to steal Microsoft Office 365 credentials of employees at organizations targeted for this attack. This mimics an automated notification from Zoom and claims the recipient will be unable to utilize the service until they use the link provided in the email to reactivate their account.

The spoofed email contains a link concealed within the text that redirects the recipient to a page hosted on an unrelated domain, which was likely hijacked by the attackers. The recipient is then redirected to a fake Microsoft login page hosted on another domain. Though the email impersonates the Zoom brand, the attacker is targeting the recipient's Microsoft login credentials.

Recommendations to avoid this threat:

- Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address
- Use of Zoom on CFPB devices is not permitted. Please see the CFPB Coronavirus Communications for the Acceptable Use Policy regarding the approved use of Third-Party-teleconferences/virtual meeting applications.
- Watch out for vague language or a generic request to click on a link or enter information.
- Call the individual personally if possible, to see if the message was legitimate<
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

July 9, 2020 CyberWise Tip- Be mindful of Your WIFI Connections

Over the past few years, wireless networking has become more available, affordable, and easy to use. Mobile device users often find free wireless connections in places like coffee shops and airports. As active mobile technology users we should know about the security threats we may encounter daily.

If you are out in public:

Before you connect to an open Wi-Fi network, stop and ask yourself if you really need to connect to that unprotected Wi-Fi network to post your Cappuccino in your favorite coffee shop? Always treat any public Wi-Fi points with caution and question if you need it.

If you know you won't be connecting to it again:

Forget that network. If you have used a Wi-Fi network that you know you won't be using again (ex: hotel, university, airport Wi-Fi networks) in the near future, make sure you forget it from your device. This will stop you automatically connecting to it if you're just passing in the range of the network later.

For an in-depth understanding of the kind of threats wireless technology users should be aware of, check out the Using Wireless Technology Securely article published by US-CERT.

July 8, 2020 CyberWise Tip- Ransomware 101

As technology evolves, so does the growth of ransomware attacks among businesses and consumers. It's important for digital citizens to be vigilant about basic digital hygiene in an increasingly connected world.

What is Ransomware?

It is a type of malware that denies the victim access to his or her data unless a ransom is paid. Malicious actors use these attacks to try to get users to click on attachments or links that appear legitimate but contains malicious code.

The FBI advises that you should not pay the ransom, as it only encourages and funds these cyber criminals.

Even if the ransom is paid, there is no guarantee that the victim will regain access to their data. However, the National Cybersecurity Alliance (NCSA) does understand that this is a difficult decision to make, and you should consult CFPB Computer Security Incident Response Team before making a decision. See our previous Cyber tip of the week for full guidance on how to protect against ransomware.

How to protect against ransomware

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Use two-step authentication – also known as two-step verification or multi-factor authentication – should be turned on for accounts where available.

- Back it up early and often. Protect your work, images, and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup
- If you believe you are being targeted by a malicious cyber-attack, please do not open the attachment – Click the “report phish” button in outlook or send as an attachment to (b) (6)

Check out the Cybersecurity Tip of the week page for more ransomware best practices.

July 7, 2020 CyberWise Tip- Cyware: COVID-19 Themed Spear Phishing Campaign

The Cybersecurity & Infrastructure Security Agency (CISA) has notified the CFPB Computer Security Incident Response Team (CSIRT) of a new spear phishing attack.

Cyware’s COVID-19 Themed Spear phishing campaign uses LokiBot Infostealer malware to steal user credentials such as e-mail passwords. The attackers are using images and trademarks associated with the World Health Organization (WHO) to deceive unsuspecting users. The messaging attempts to address false information associated with COVID-19. The email includes the subject line “Coronavirus disease (COVID-19) Important Communication.”.

What is Spear phishing?

A highly targeted form of phishing. Spear phishing involves hackers sending tailored and personal emails to well-researched victims purporting to be a trusted sender. Spear phishing attacks are hard to spot without close inspection and difficult to stop with technical controls alone. While regular phishing campaigns go after large numbers of relatively low-yield targets, spear phishing aims at specific targets using specially emails crafted to their intended victim. Some targeted spear phishing attacks involve documents containing malware or links to malicious web sites to steal sensitive information or valuable intellectual property, or to simply compromise payment systems.

How to Identify Spear Phishing Campaigns

To learn more on how to identify Spear Phishing, check out our CFPB Cyber wise tip on how to spot a spear phishing campaign here.

Recommendations to avoid this threat:

- Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address
- Watch out for vague language or a generic request to click on a link or enter information.
- Call the individual personally if possible, to see if the message was legitimate
- Check out the CFPB Phishing Awareness site for more phishing reporting guidance.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the “report phish” button in outlook or send as an attachment to (b) (6)

July 1, 2020 CyberWise Tip- Example of a COVID-19 themed attack

The Cybersecurity & Infrastructure Security Agency (CISA) has notified CFPB Computer Security Incident Response Team (CSIRT) of a new COVID-19 phishing attack threat report to be aware of.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist.

Vendetta Group Targeting Users with COVID-19 Phishing Campaigns and Malicious URLs

A new group is targeting Taiwanese users with Covid-19 themed phishing campaign. Cybersecurity researchers note the email was high quality and indicated sophisticated targeting, unlike most phishing emails which contain grammatical mistakes or appear to be fake. The most recent campaign indicates a clear intent to victimize users in Taiwan based on the content and language. The email claims that the attachment contains information regarding making an appointment for testing at the Taiwan CDC.

Recommendations to avoid similar phishing threats:

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to (b) (6)

June 30, 2020 CyberWise Tip: COVID themed social media attacks to be aware of

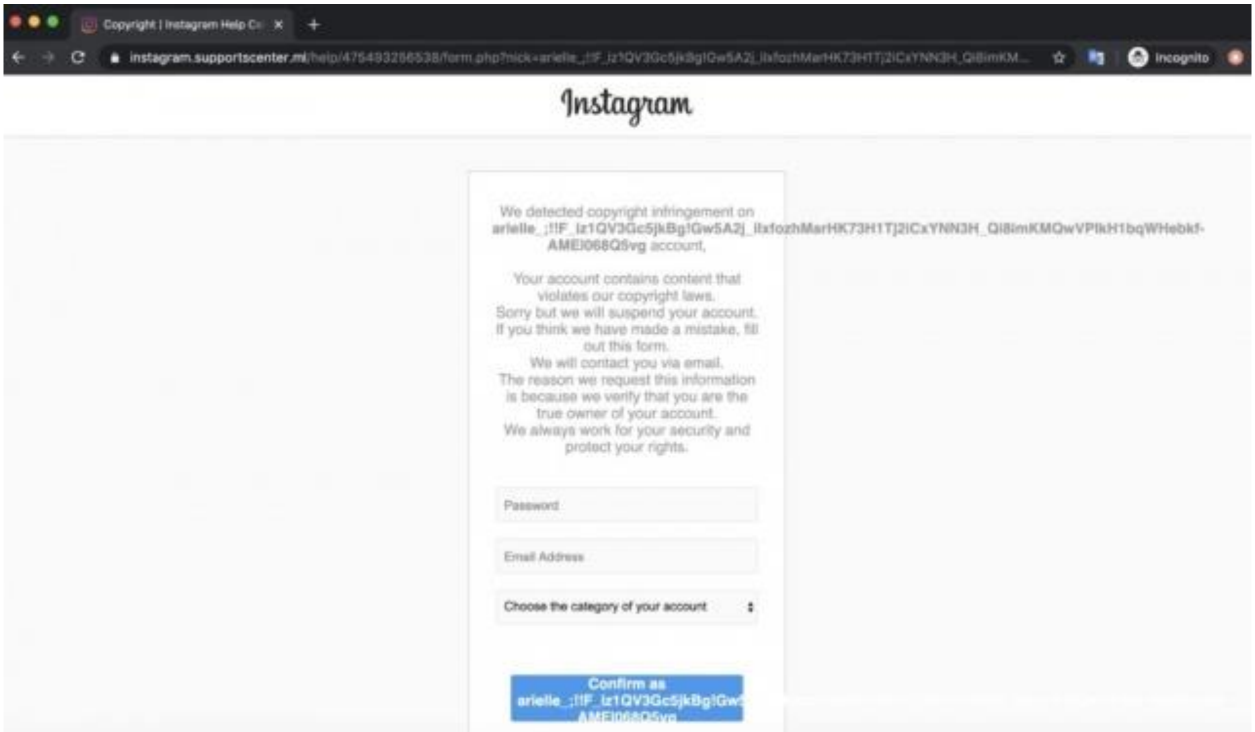
The Cybersecurity & Infrastructure Security Agency (CISA) has notified CFPB Computer Security Incident Response Team (CSIRT) of a new social media attack threat report to be aware of.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist.

Abnormal Security: Social Media Attacks

Abnormal Security has observed attackers impersonating social media platforms like Instagram, Facebook, and Twitter to steal the login credentials of employees at major companies.

Here are samples of these attacks on various social media platforms:



Copyright | Instagram Help Ce
instagram.supportscenter.ml/help/475493256538/form.php?nick=arielle_;!!F_Iz1QV3Gc5jkBg!Gw5A2j_IlxfozhMarHK73H1Tj2iCxYNN3H_QI8imKM...
Incognito
Instagram

We detected copyright infringement on arielle_;!!F_Iz1QV3Gc5jkBg!Gw5A2j_IlxfozhMarHK73H1Tj2iCxYNN3H_QI8imKMQwVPIkH1bqWHebkf-AMEI068Q5vg account,

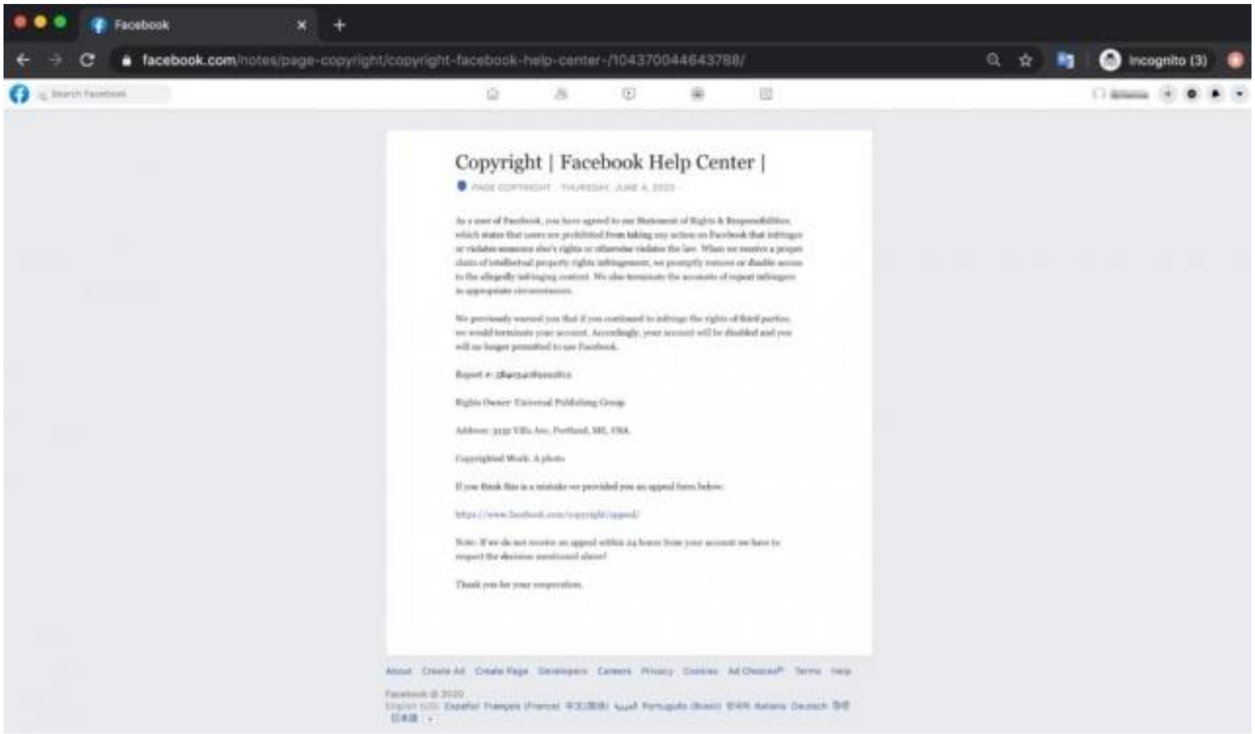
Your account contains content that violates our copyright laws.
Sorry but we will suspend your account.
If you think we have made a mistake, fill out this form.
We will contact you via email.
The reason we request this information is because we verify that you are the true owner of your account.
We always work for your security and protect your rights.

Password

Email Address

Choose the category of your account

Confirm as arielle_;!!F_Iz1QV3Gc5jkBg!Gw5 AMEI068Q5vg



Facebook
facebook.com/notes/page-copyright/copyright-facebook-help-center-/104370044643788/
Incognito (3)
Search Facebook

Copyright | Facebook Help Center |

PAGE COPYRIGHT · THURSDAY, JUNE 4, 2020

As a user of Facebook, you have agreed to our Statement of Rights & Responsibilities, which states that users are prohibited from taking any action on Facebook that infringes or violates someone else's rights or otherwise violates the law. When we receive a proper claim of intellectual property rights infringement, we promptly remove or disable access to the allegedly infringing content. We also terminate the accounts of repeat infringers in appropriate circumstances.

We previously warned you that if you continued to infringe the rights of third parties, we would terminate your account. Accordingly, your account will be disabled and you will no longer permitted to use Facebook.

Report #: [illegible]

Rights Owner: Universal Publishing Group

Address: [illegible] Villa Ave, Portland, ME, USA.

Copyrighted Work: A photo

If you think this is a mistake we provided you an appeal form below:

https://www.facebook.com/copyright/appeal/

Note: If we do not receive an appeal within 24 hours from your account we have to respect the decision mentioned above!

Thank you for your cooperation.

About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices Terms Help
Facebook © 2020

Why are these attacks effective?

<u>Urgency:</u> A key reason these attacks are effective is the use of language that conveys a sense of urgency throughout the email. It claims the recipient has violated the terms of service for the platform and thus the platform has decided to suspend the recipient’s account. The emails also provide an opportunity for

the recipient to reactivate their account if they act within a certain period. Due to the urgency this creates, attackers are hoping the recipients will overlook suspicious signals they would normally notice.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

June 29, 2020 CyberWise Tip: (NSHC Red Alert) Activities of the SectorJ17 hacking group to be aware of

The Cybersecurity & Infrastructure Security Agency (CISA) has notified CFPB Computer Security Incident Response Team (CSIRT) of a critical vulnerability in Microsoft Exchange being actively exploited.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist.

NSHC Red Alert: Activities of the SectorJ17 hacking group aimed at stealing user information The SectorJ17 group is a hacking group comprised of cybercriminals. The SectorJ17 group used spear phishing emails disguised as being sent by manufacturing organizations or companies. They have been using compressed files containing an executable disguised as a document file icon as an email attachment as the method of attack. Most of the executable files use the Adobe Reader (PDF) document icon, and the file name is mainly written with content that may be of interest to the general private enterprise, such as invoices or payment details.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

June 25, 2020- CyberWise Tip: Trend Micro & Adaptive Mobile Security COVID-19 Reports to be aware of

The Cybersecurity & Infrastructure Security Agency (CISA) has identified two (2) new COVID-19 threat reports that attempt to capitalize on unsuspecting users by using COVID-19 to get malicious files and steal user resources and/or credentials.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist.

COVID-19 Reports

Trend Micro: COVID-19 Used in Malicious Campaigns

The malware file has *"Coronavirus Installer"* in the description. It is a coronavirus-themed malware that overrides a systems' master boot record (MBR), making it unbootable. When the malware executes, it will automatically restart the machine and display a virus-themed window that cannot be closed.

The usual exit button on the top right side of the window does not function. Clicking on the "Help" button on the bottom left will bring up a pop-up message indicating the Task Manager cannot be activated. The malware also creates a hidden folder named "COVID-19," which contains several secondary modules. Manually restarting the system will execute another binary file and display a grey screen.

Cyber is reviewing this report content and malicious domains will be added to weekly blocklist

AdaptiveMobile Security: Scammers seek financial help during Covid-19 pandemic

This COVID-19 themed SMS spam campaign is exploiting the fear around the pandemic to sell fake prevention's and cures, push false offers and sell payday loans. The SMS mentions that the message is from the Canadian Government and baits the subscriber to click the link mentioned in the message to receive financial help. Canadian mobile subscribers have been the recent target of such SMS spam messages. The subscriber is invited to choose their bank from a list of real Canadian banks. Once the subscriber clicks the link, a fake mobile website with Canadian Government logo appears and entices recipient to start an application after choosing their preferred language.

Choosing BMO (Bank of Montreal) leads to a login page with genuine logos and convincing looking links to register, change language and reset password. Scammers are trying to steal the subscriber's credit/debit card details.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to (b) (6)

June 24, 2020- CyberWise Tip: Black Lives Matter spam & ZOOM meetings Phishing Campaigns to be aware of

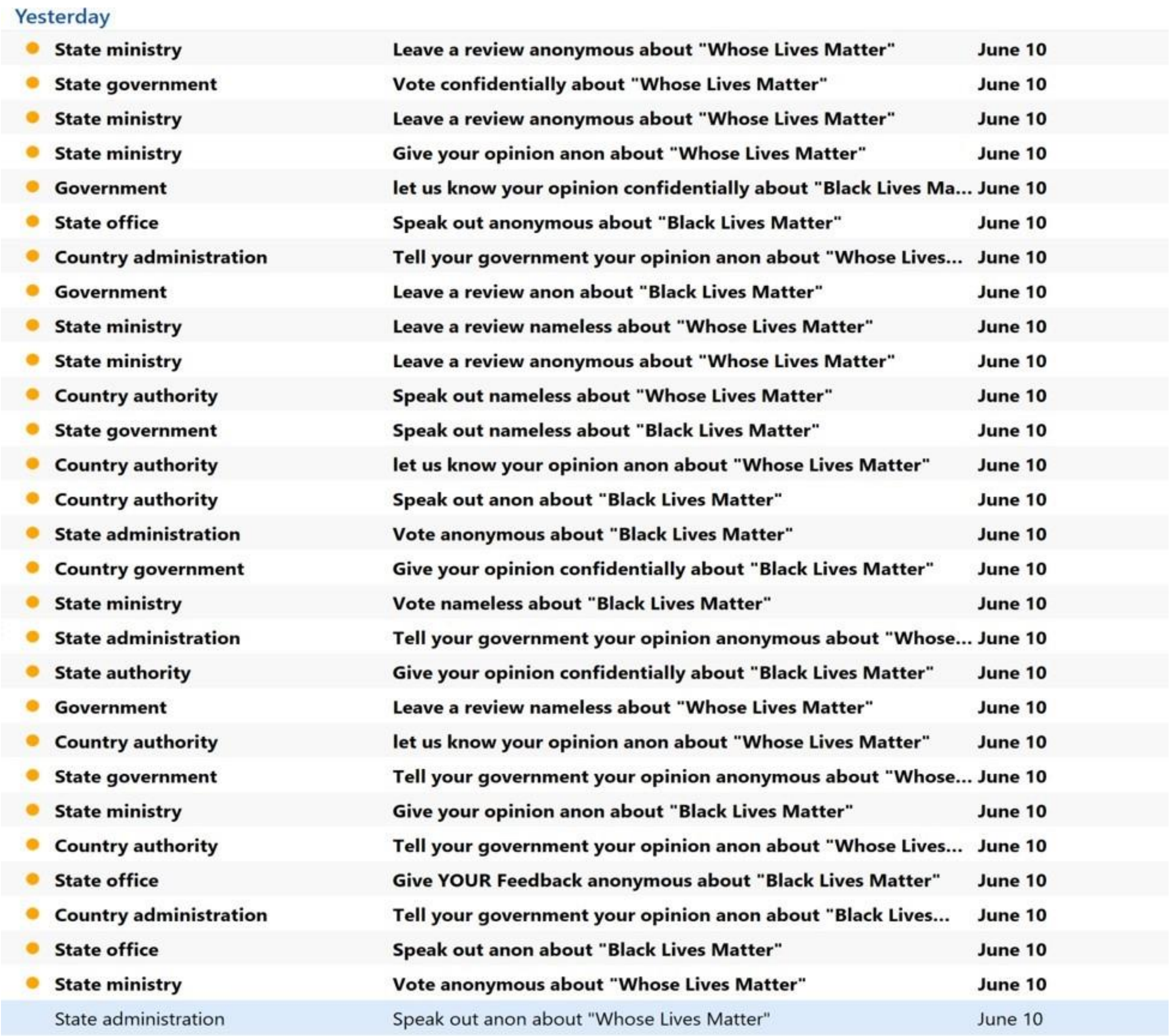
The Cofense Phishing Defense Center (PDC) & FortiGuard Labs have identified two new COVID-19 threat reports that attempt to capitalize on unsuspecting user by using COVID-19 to get malicious files and steal user resources and/or credentials.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist.

COVID-19 Reports

Fortinet: Global Malicious Spam Campaign Using Black Lives Matter as a Lure.

FortiGuard Labs has observed a global malicious spam campaign that is targeting users who may be sympathetic to the Black Lives Matter movement. The campaign uses a variety of subject lines for emails with an attached malicious Microsoft Word document to compel the user into opening the attachment. The content of the body is written in haste and uses poor grammar, but the Black Lives Matter subject line is used to compel victims into opening the attachment, as shown in the image below.



Yesterday

●	State ministry	Leave a review anonymous about "Whose Lives Matter"	June 10
●	State government	Vote confidentially about "Whose Lives Matter"	June 10
●	State ministry	Leave a review anonymous about "Whose Lives Matter"	June 10
●	State ministry	Give your opinion anon about "Whose Lives Matter"	June 10
●	Government	let us know your opinion confidentially about "Black Lives Ma...	June 10
●	State office	Speak out anonymous about "Black Lives Matter"	June 10
●	Country administration	Tell your government your opinion anon about "Whose Lives...	June 10
●	Government	Leave a review anon about "Black Lives Matter"	June 10
●	State ministry	Leave a review nameless about "Whose Lives Matter"	June 10
●	State ministry	Leave a review anonymous about "Whose Lives Matter"	June 10
●	Country authority	Speak out nameless about "Whose Lives Matter"	June 10
●	State government	Speak out nameless about "Black Lives Matter"	June 10
●	Country authority	let us know your opinion anon about "Whose Lives Matter"	June 10
●	Country authority	Speak out anon about "Black Lives Matter"	June 10
●	State administration	Vote anonymous about "Black Lives Matter"	June 10
●	Country government	Give your opinion confidentially about "Black Lives Matter"	June 10
●	State ministry	Vote nameless about "Black Lives Matter"	June 10
●	State administration	Tell your government your opinion anonymous about "Whose...	June 10
●	State authority	Give your opinion confidentially about "Black Lives Matter"	June 10
●	Government	Leave a review nameless about "Whose Lives Matter"	June 10
●	Country authority	let us know your opinion anon about "Whose Lives Matter"	June 10
●	State government	Tell your government your opinion anonymous about "Whose...	June 10
●	State ministry	Give your opinion anon about "Black Lives Matter"	June 10
●	Country authority	Tell your government your opinion anon about "Whose Lives...	June 10
●	State office	Give YOUR Feedback anonymous about "Black Lives Matter"	June 10
●	Country administration	Tell your government your opinion anon about "Black Lives...	June 10
●	State office	Speak out anon about "Black Lives Matter"	June 10
●	State ministry	Vote anonymous about "Whose Lives Matter"	June 10
	State administration	Speak out anon about "Whose Lives Matter"	June 10

The attachment is a standard Microsoft Word document with a generic image enticing the user to enable macros. This campaign utilizes the same strategy as previous TrickBot attacks. The campaign just prior to the current one leveraging the Black Lives Matter movement in the United States, was focused on COVID-19, which we previously analyzed

Zoom Phish scam amid pandemic

The Cofense Phishing Defense Center (PDC) has observed a new phishing campaign that acts as a Zoom video conference invitation to obtain Microsoft credentials from users. Users are informed of an invite to a video conference from what appears to be "Zoom Video Communications". When visiting either domain, it may appear to be a German site speaking on different Lasik treatments and surgery options. This is merely a cover for its true purpose of helping send malicious emails while impersonating teleconferencing giant Zoom. The threat actor has utilized Microsoft's Azure is used to host the phishing domain, but this is not a new tactic.

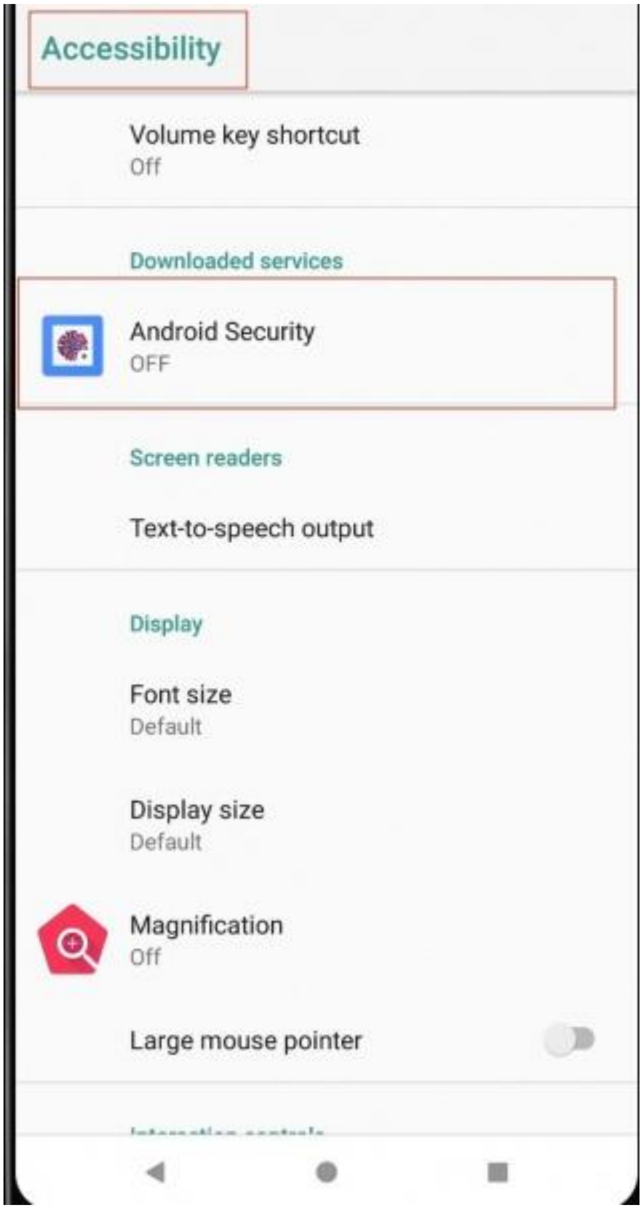
Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the “report phish” button in outlook or send as an attachment to (b) (6)

June 23, 2020- CyberWise Tip- COVID-19 Phishing Campaigns to be aware of

The Cybersecurity & Infrastructure Security Agency (CISA) has identified two (2) new COVID-19 threat reports to be aware of:

Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Monitor Devices, Steal Personal Data.



Accessibility

Volume key shortcut
Off

Downloaded services

Android Security
OFF

Screen readers

Text-to-speech output

Display

Font size
Default

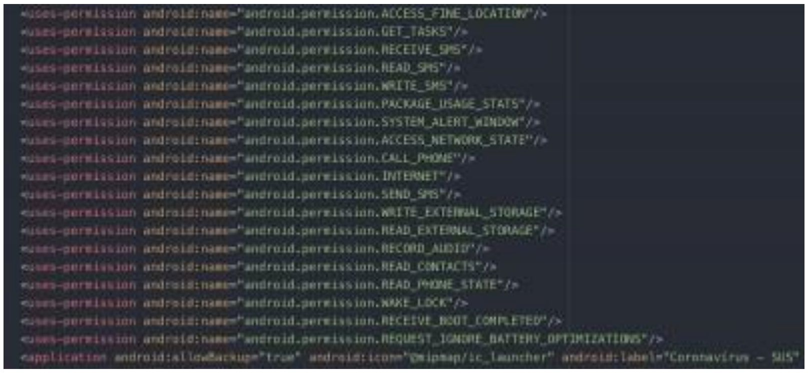
Display size
Default

Magnification
Off

Large mouse pointer

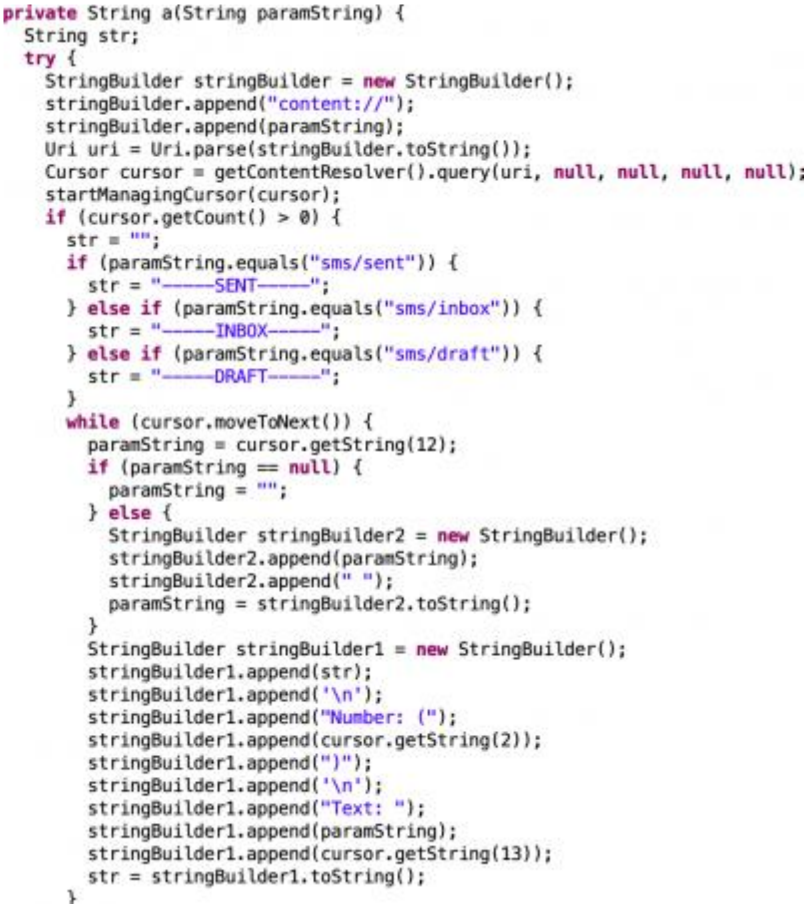
Threat actors are distributing fake Android applications themed around official government COVID-19 contact tracing apps. There have been multiple applications identified that contain malware, primarily Anubis and SpyNote, designed to monitor infected devices, and to steal banking credentials and personal data.

Anubis is an Android banking Trojan that utilizes overlays to access infected devices and steal user credentials.



```
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="Coronavirus - SUS"
```

SpyNote is an Android trojan with the primary objective of gathering and monitoring data on infected devices.



```
private String a(String paramString) {
  String str;
  try {
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("content://");
    stringBuilder.append(paramString);
    Uri uri = Uri.parse(stringBuilder.toString());
    Cursor cursor = getContentResolver().query(uri, null, null, null, null);
    startManagingCursor(cursor);
    if (cursor.getCount() > 0) {
      str = "";
      if (paramString.equals("sms/sent")) {
        str = "-----SENT-----";
      } else if (paramString.equals("sms/inbox")) {
        str = "-----INBOX-----";
      } else if (paramString.equals("sms/draft")) {
        str = "-----DRAFT-----";
      }
      while (cursor.moveToNext()) {
        paramString = cursor.getString(12);
        if (paramString == null) {
          paramString = "";
        } else {
          StringBuilder stringBuilder2 = new StringBuilder();
          stringBuilder2.append(paramString);
          stringBuilder2.append(" ");
          paramString = stringBuilder2.toString();
        }
        StringBuilder stringBuilder1 = new StringBuilder();
        stringBuilder1.append(str);
        stringBuilder1.append('\n');
        stringBuilder1.append("Number: (");
        stringBuilder1.append(cursor.getString(2));
        stringBuilder1.append(")");
        stringBuilder1.append('\n');
        stringBuilder1.append("Text: ");
        stringBuilder1.append(paramString);
        stringBuilder1.append(cursor.getString(13));
        str = stringBuilder1.toString();
      }
```

Rewterz Threat Alert – COVID-19 Phishings Distribute GuLoader Targeting Greek Banks.

The latest phishing campaign exploiting the Covid-19 pandemic has been observed targeting Greek Banks. Emails are spoofed to be sent from Alpha Bank with a bank transaction theme and malicious attachment. The attachment contains a variant of GuLoader, which is considered one of the most advanced downloaders and known as a popular Remote access Trojan (RAT) distribution program. All malicious indicators have been added to CFPB Cybersecurity weekly block list.

Threat actors continue to imitate official apps to take advantage of the brand recognition and perceived trust of those released by government agencies. The global impact of the COVID-19 pandemic makes the virus a recognizable and potentially fear inducing name, of which bad cyber actors will continue to abuse. This alert reveals some of the applications threat actors are actively distributing, and there are likely numerous others in the wild that have not yet been detected.

Recommendations:

- Always be suspicious about emails sent by unknown senders.
- Never click on the links/attachments sent by unknown senders.

June 22, 2020-CyberWise Tip- Vulnerability in Microsoft Exchange being Actively Exploited

COVID-19 Reports to be aware of:

The Cybersecurity & Infrastructure Security Agency (CISA) has notified CFPB Computer Security Incident Response Team (CSIRT) of a critical vulnerability in Microsoft Exchange being actively exploited.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist. Broken phishing accidentally exploiting Outlook as zero-day attack (on Thu Jun 18th).

There is a new zero-day phishing campaign targeting Outlook users. The e-mail allows a sender to include or change a link in an e-mail when it is forwarded by Outlook. The e-mail in question uses a COVID-19-related subject line to lure unsuspecting users and when “View details” is clicked, it will direct the victim to a phishing site. If a user opens such an e-mail, the link will point to the Internet Storm Center website. If a user forwards the message, the link will change to point to an untrusted network.

Recommendations to avoid this threat:

- Keep applications and operating systems patched and up to date.
- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the “https” prefix before the site URL, indicating the connection to the site is secure.

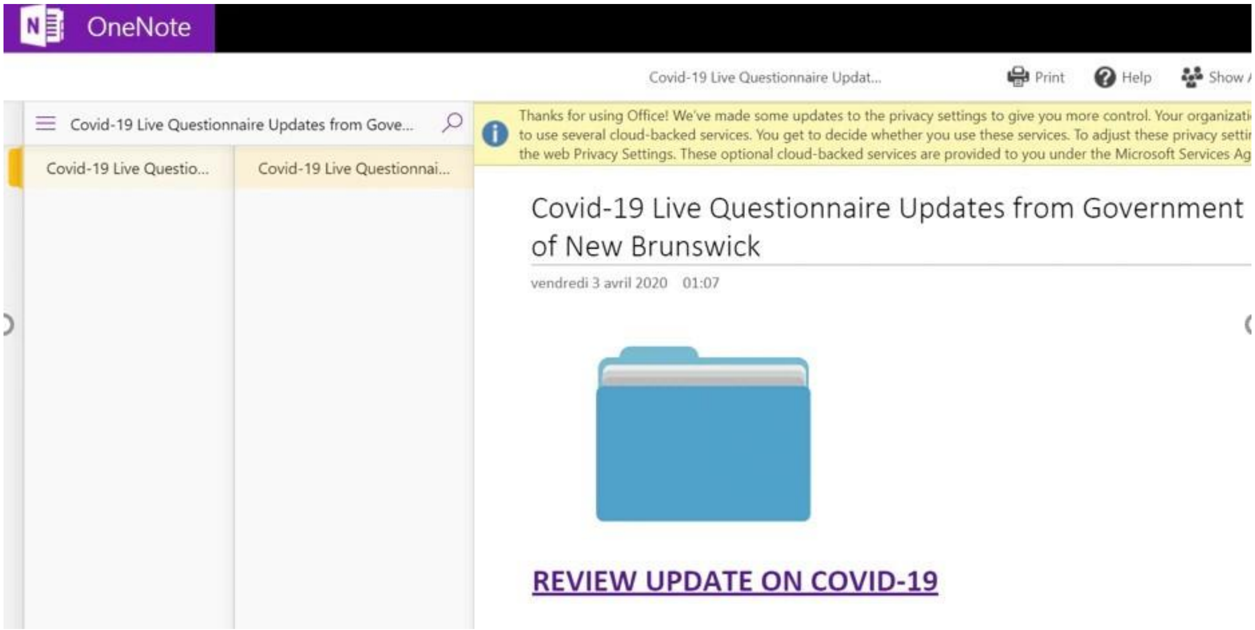
June 18, 2020- CyberWise Tip- OneDrive Phishing Awareness

There are number of ways scammers use phishing to target personal information and one current example is, how cyber attackers are sending phishing and scam emails to Microsoft OneDrive users, trying to profit from Coronavirus/COVID-19. They e-mail unsuspecting users under the guise of an e-mail account from a government, consulting, or charitable organization in order to steal the victim’s OneDrive details. OneDrive scammers will steal sensitive account information like usernames and passwords.

Fake Government Email Baits Victims

Below is an example of a purported attack coming from a government organization hosted in OneDrive to make them appear more genuine to users. As the screenshot below illustrates, the goal is to steal the user’s OneDrive credentials.

Scammers pretend to be from government offices and deliver documents that contain the latest live questionnaire regarding COVID-19. Remember, governments generally do not send mass e-mails or un-requested documents, so a user can verify the origin of the e-mail by examining the sender email address and location in the email headers.


OneNote
Covid-19 Live Questionnaire Updat...
Print
Help
Show
Covid-19 Live Questionnaire Updates from Gove...
Covid-19 Live Questio...
Covid-19 Live Questionnai...

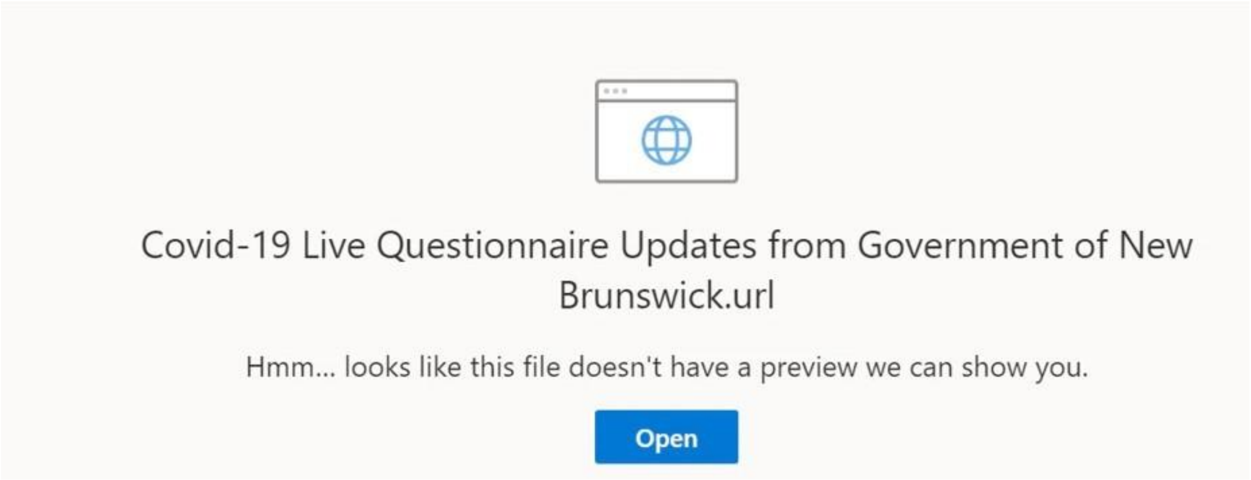
Thanks for using Office! We've made some updates to the privacy settings to give you more control. Your organizati to use several cloud-backed services. You get to decide whether you use these services. To adjust these privacy setti the web Privacy Settings. These optional cloud-backed services are provided to you under the Microsoft Services Ag

Covid-19 Live Questionnaire Updates from Government of New Brunswick

vendredi 3 avril 2020 01:07

REVIEW UPDATE ON COVID-19

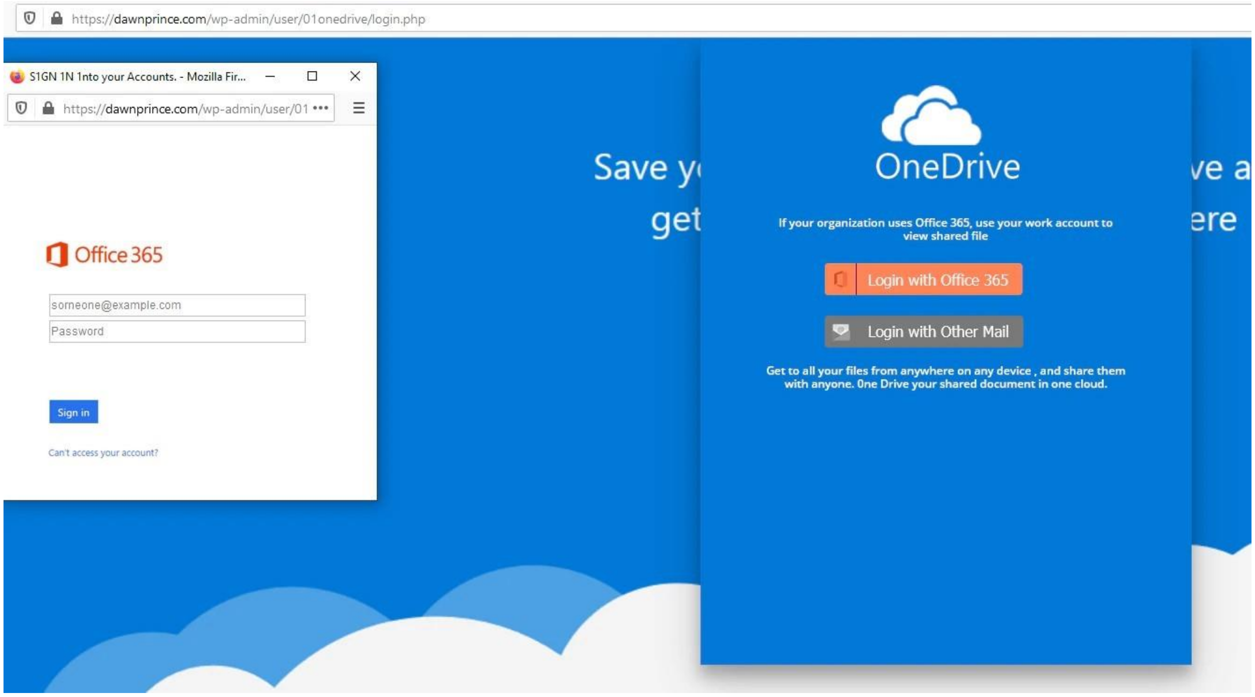
When the folder in the above image is clicked on, it redirects to the screenshot shown below.



Covid-19 Live Questionnaire Updates from Government of New Brunswick.url

Hmm... looks like this file doesn't have a preview we can show you.

A warning saying **“Hmm… looks like this file doesn’t have a preview we can show you”***Italic text* baits the visitor into clicking on the Open button. When clicked, it takes them to the below OneDrive screenshot prompting them to enter their personal information. The link points users to a vulnerable WordPress site that contains a credential phishing landing page. A user should be aware that a legitimate OneDrive login page will never be hosted on a non-Microsoft domain. This should be a red flag to the user that this may be a scam or phishing attack.

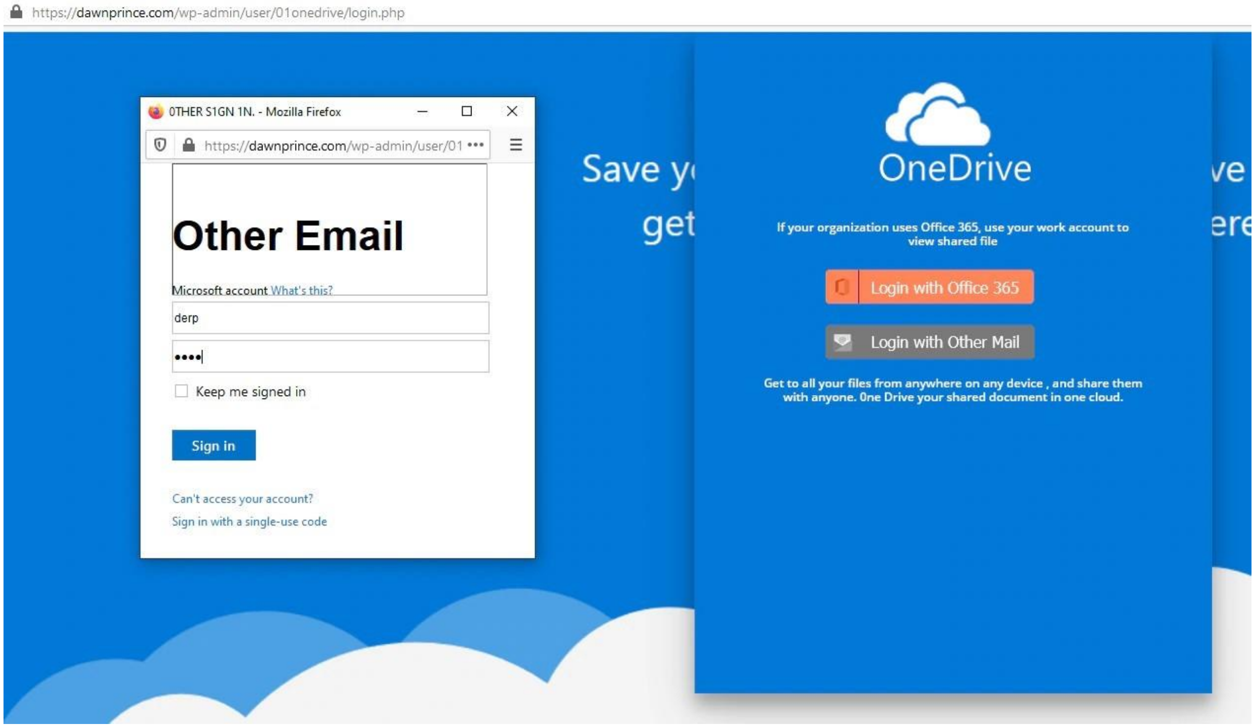


https://dawnprince.com/wp-admin/user/01onedrive/login.php
S1GN 1N 1nto your Accounts. - Mozilla Fir...
https://dawnprince.com/wp-admin/user/01
Office 365
someone@example.com
Password
Sign in
Can't access your account?
Save y
get
OneDrive
Login with Office 365
Login with Other Mail
ve a
ere

If your organization uses Office 365, use your work account to view shared file

Get to all your files from anywhere on any device , and share them with anyone. One Drive your shared document in one cloud.

As intended by the scammers, the user cannot access the OneDrive document to view the updated government questionnaire and, instead, will receive an error message to try again later. By this stage, the scammers would have already stolen the user's OneDrive personal information.



https://dawnprince.com/wp-admin/user/01onedrive/login.php
0THER S1GN 1N. - Mozilla Firefox
https://dawnprince.com/wp-admin/user/01
Other Email
Microsoft account What's this?
Keep me signed in
Sign in
Can't access your account?
Sign in with a single-use code
Save y
get
OneDrive
Login with Office 365
Login with Other Mail
ve
ere

derp

••••

□ Keep me signed in

If your organization uses Office 365, use your work account to view shared file

Get to all your files from anywhere on any device , and share them with anyone. One Drive your shared document in one cloud.

Recommendations Be aware of scammers trying to harvest OneDrive details and should follow these best practices: –

- Be careful of any charity or businesses requesting their OneDrive user information. Stick with organizations known to be reputable. Never share financial or personal information over the phone, via email, or with untrusted sites.
- Remember that legitimate organizations will almost never send an email asking for personal information. Never click on suspicious links or download attachments from unknown sources.
- Never log in to a web page reached through a link from an email.
- Remember email addresses can be spoofed so if a message looks suspicious, contact the sender via a known telephone number taken from their official website.

June 17, 2020- CyberWise Tip- COVID-19 Relief fund campaigns to be aware of

The Cybersecurity & Infrastructure Security Agency (CISA) has identified two (2) new COVID-19 threat reports that exploit government relief funds for small businesses affected by COVID-19 by capturing user credentials.

Note: CFPB Cybersecurity reviews all phishing reported content and malicious domains and adds to our weekly blocklist.

COVID-19 Relief Phishing Through Dropbox Transfer

This attack attempts to exploit current efforts by the government to provide relief funds for small business owners affected by COVID-19 closures and shelter-in-place orders.

Phishing emails are automated messages from the sender "no-reply@dropbox[.]com" which is an official Dropbox domain. The body contains a link to the file "COVID-19-Relief-Payment.PDF" with information about the size of the file, a brief description of the file, and an expiration date. The link provided in the email leads to a standard drop box transfer landing page with the enablement to download the file. After clicking on the download button, the page is redirected to a phishing landing page. The landing page contains an O365 image with a button to "Access Document." This is where the intent is revealed, which is to gain access to the user's Microsoft credentials.

Rewterz: Rewterz Threat Alert – Covid-19 – Malicious URLs

This campaign includes newly registered malicious domains related to Covid-19 pandemic. Cyber is reviewing this report content and malicious IOCs will be added to the weekly blocklist

Recommendations:

If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your outlook or forward as an attachment to [redacted] (b) (6). For additional questions or information, please reach out to the Cybersecurity Training Team at [redacted] (b) (6)

June 16, 2020- CyberWise Tip- Beware of Business Email Compromise Attacks

Business Email Compromise (BEC) attacks are a sophisticated type of scam that target both businesses and individuals with the aim of transferring funds from victims' bank accounts to criminals. The FBI's 2019 Internet Crime Report states that the total annual losses generated by BEC in the US alone reached $1.7 billion. BEC scams also accounted for half of all cybercrime losses in the US in 2019, making BEC the #1 cyber threat in terms of economic damage.

Over the years, these attacks have grown in sophistication, mostly in the social engineering aspect. Rather than targeting the companies directly, attacks now target customers, HR departments, suppliers, related accountants, and law firms, and even tax authorities. In addition to directly generating or diverting currency transactions, BEC attacks have also been used to fraudulently purchase gift cards, divert tax returns, and even transfer millions of dollars' worth of hardware and equipment into the control of cybercriminals.

COVID-19 driving a pandemic of BEC attacks: The new working conditions enforced by the global outbreak has triggered a spike in BEC scams because more remote working means increases the opportunity to catch users off guard.

What is behind a BEC attack? An attacker typically constructs an email that impersonates a high-level executive of a company – either by hacking into the organization's email system, or by designing a legitimate-looking fake – and sends it to an employee, requesting a transfer of money to a bank account under the attackers' control. This is often done with the excuse of urgency or communication problems to prevent the manager from communicating in alternative ways.

The three main ways of impersonation are:

35. The attacker spoofs the source email address
36. The attacker sends emails from the authentic email account of the impersonated victim by gaining control of their email account through phishing, credentials theft, or other means.
37. The attacker sends an email using a look-alike domain, which they register. In this case, the domain differs from the authentic address by a minor detail, such as sending an email from "example.co" rather than "example.com". BEC frauds requires, in addition to the fake email account, detailed knowledge of the identity

Check out CheckPoint's website for more details regarding how BEC's are driving the cyber-crime pandemic.

Recommendations to avoid this threat:

- Use digital signatures in emails.
- Set email options to flag external emails.
- Include a sentence on multi-factor authentication.
- Keep applications and operating systems up to date.
- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.

- Enter your username and password only over a secure connection. Look for the “https” prefix before the site URL, indicating the connection to the site is secure.
- Be vigilant with attachments and links in emails. Stop and Think, before you click.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the “report phish” button in outlook or send as an attachment to (b) (6)

June 12, 2020- Beware of Bank Text Phishing Attacks Using COVID-19

Threat actors are attempting to phish banking credentials under the guise of COVID-19 protection from fraud.

The onslaught of COVID-19 threats continues to grow daily, threat actors have taken to text messages to steal banking credentials through a "locked debit card" scam. The text message contains a link when clicked, takes the victim to a spoofed Canadian bank's website. A second campaign is nearly identical with the exception being the link included when clicked, takes victims to a website asking victims to choose their bank.

Both campaigns appear to target Canadian citizens. As with other phishing schemes observed during the pandemic, the levels to which threat actors will stoop to trick victims out of their money continues to sink lower and lower.

Recommendations

- Be mindful regarding personal password/credentials hygiene (are all your account passwords the same? They shouldn’t be) and detecting phishing attempts.
- Use official links from banking websites to conduct financial business

June 11, 2020- Beware of COVID-19 Global Banking Scams Offer Financial Relief (part 2)

In continuation of our part 1, here are a few more COVID- 19 Global banking scams to be aware of:

Wells Fargo- The next example claiming to be from Wells Fargo where recipients are told to download an attachment that contains answers to the most urgent questions regarding the COVID-19 pandemic. The HTML attachment contains an encoded URL shortened link *ow.ly/yqzX30quLL0*. The landing page is a Russian site under the domain "uralpirog.ru".

The following subject lines used during this campaign:

- Wells Fargo - COVID-19 Update Critical information

Wells Fargo - This email campaign claiming to be from Wells Fargo; the goal of the attackers is to steal the login credentials of bank customers. This is done by luring the customer to accept a COVID-19 relief payment credited to their account from another customer. To do this, the victim has to login to their Wells Fargo account by clicking within the email. However, the link "h**ps://theruncoach.icu/home.php" shows a fake login page of Wells Fargo that tries to steal account login information.

The following subject lines used during this campaign:

- Wells Fargo - COVID 19 RELIEF PAYMENT

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the **"https"** prefix before the site URL, indicating the connection to the site is secure.
- Stop and Think, before you click that link.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to (b) (6)

June 10, 2020 - Beware of COVID-19 Global Banking Scams Offer Financial Relief (part 1)

In this two part Cyber Wise tip, we will list some COVID- 19 Global banking scams to be aware of:

American Express - The threat email purporting to come from American Express asks the recipient to claim the aid stimulus package. The contained link goes to a Google Docs document which claims to redirect to American Express but redirects to <*worldsatellitemedia.com/wp-includes/class.php*> which is no longer reachable.

The following different subjects used in this campaign:

- Covid-19 Relief Cash
- Covid-19 Relief Funds
- Late Payment Waived
- Stimulus Package
- Stimulus Funds
- Stimulus Bill

American Express- Another example purports to be from American Express. The recipient is informed that they have a pending payment and to accept the payment, the "Approve Your Payments Now" button should be clicked. The link goes to SendGrid, which is a legitimate platform used for email marketing, was disabled in the meantime.

The following subject lines used during this campaign:

- American Express - COVID-19 Payment

Standard Bank of South Africa Limited – Phishing user credentials attack via email claiming to be from the Standard Bank of South Africa Limited and offering government relief. The HTML attachment contains obfuscated JavaScript code which shows a login page of this bank. The entered data will be sent to the zahraa.qtr.me domain which is likely under the control of the attackers.

The following subject lines used during this campaign:

- Standard Bank - Redeem SBSA-COVID-19-Financial Relief

Recommendations

- Keep applications and operating systems up to date.
- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the "https" prefix before the site URL, indicating the connection to the site is secure.
- Be vigilant with attachments and links in emails. Stop and Think, before you click.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment

– Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

June 09, 2020 - Cyber Wise Tip- Virtual Private Network (VPN) Impersonation Phishing Attacks

What is a VPN impersonation phishing attack?

In this attack, attackers are impersonating a notification from the user's organization regarding VPN configuration. However, the email link hosts a phishing website designed to steal credentials of employees.

Example VPN impersonation phishing attack:

> Platform: Microsoft Office 365
> Technique: Spoofed Email
>
> Email Attack: The attack impersonates a notification email from the IT support at the recipient's company. The sender email address is spoofed to impersonate the domain of the user's respective organization. The link provided in the email allegedly directs to a new VPN configuration for home access. Though the link appears to be related to the target's company, the hyperlink directs the user to an Office 365 credential phishing website.

Payload: Numerous versions of this attack have been seen across different clients, from different sender emails and originating from different IP addresses. However, the same payload link was employed by all these attacks, implying that these were sent by a single attacker that controls the phishing website.

Result: Should the recipient fall victim to this attack, the user's credentials would be compromised. Information available with the user's Microsoft credentials via single-sign on are also at risk.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the "https" prefix before the site URL, indicating the connection to the site is secure.
- Be vigilant with attachments and links in emails. Stop and Think, before you click.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to (b) (6)

June 04, 2020 - CyberWise Tip- Beware of Fake HSBC & FMLA COVID-19 Phishing Campaigns

The Cybersecurity & Infrastructure Security Agency (CISA) has identified two (2) new COVID-19 threat reports:

1) HSBC COVID-19 themed phishing campaign lures users in order to steal their credentials and sensitive data, leading to possible financial loss
2) FMLA (Family and Medical Leave Act) campaign using malicious Microsoft Word attachments.

COVID-19 Reports

- Rewterz: Rewterz Threat Alert – Bank Phishing Use COVID-19 To Trick Victims.
- COVID-19 based threats identified a phishing attempt by cybercriminals using a HSBC Bank-themed email to trick victims.
- These kind of phishing emails attempt to lure users to keep themselves updated on the status of COVID-19 or finding invoices of their payments are continuously being used to rob users of their credentials and their sensitive data and financial loss as well.
- Yoroi-CERT: Himera and AbSent-Loader Leverage Covid19 Themes.
- Malware-spam (malspam) campaign emails were detected leveraging FMLA (Family and Medical Leave Act) requests related to the ongoing Coronavirus pandemics. These emails were weaponized with two versatile cyber-criminal tools: Himera and Absent-Loader

- Loaders are a type of malicious code specialized in loading additional malware code into the victim's machine.
- The malicious email wave contained a .doc attachment. The user is led to double-click on the malicious icon, once clicked, it allows this malicious document to execute a malicious file named HimeraLoader.exe.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the “https” prefix before the site URL, indicating the connection to the site is secure.
- Be vigilant with attachments and links in emails. Stop and Think, before you click.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the “report phish” button in outlook or send as an attachment to (b) (6)

June 03, 2020 - CyberWise Tip- World Health Organization (WHO) Impersonation related campaign

The Cybersecurity & Infrastructure Security Agency (CISA) has identified a new abnormal attack: WHO

Impersonation related cyber threat attempt.

Cyber criminals continue to impersonate the World Health Organization in order to steal user credentials. Threat campaign uses COVID-19 bait to download malicious software.

COVID-19 Reports

- New threat report analyzed- Abnormal Attack Stories: WHO Impersonation

- Attackers impersonate World Health Organization in order to steal credentials. Should victims fall for this attack, any information submitted on the fake WHO page will be sent to the attacker. Accounts and any information associated with submitted credentials will be compromised. When victims go to the fake WHO website, they are asked to sign in with their email and password. If they do so, they are further prompted for their phone number before being redirected to the real WHO website.
- An email is sent to the victim with a fake message from the WHO. This email contains a link to a webpage imitating the World Health Organization homepage with a login pop-up.
- The URL of the fake World Health Organization website is obfuscated by text asking victims to click to open a supposed message from the WHO.
- Obfuscation is a technique that tries to make something unclear or difficult to understand on purpose. It’s normally used to try and hide data within data.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.

- Always check the link before clicking. Hover over it to preview the URL and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the "https" prefix before the site URL, indicating the connection to the site is secure.
- Be vigilant with attachments and links in emails. Stop and Think, before you click.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB.
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to [redacted] (b) (6)

May 28, 2020 - CyberWise Tip- Beware of weak passwords

Try to avoid using personal information when creating passwords

Passwords that contain personal information can be guessed easily. Your birthday, children's names, anniversary, pet's names, hometown, or favorite sports team could all be easily gleaned from social media accounts or other sources. If possible, use a password that has no personal connection to you that would be possible to glean from publicly available information from sites like Facebook.

If using somewhat personal information or keywords in passwords, try to avoid using complete words or phrases that can be found in a dictionary. Instead, try breaking up words with numbers or special characters to increase the complexity of your passwords.

May 27, 2020 - CyberWise Tip- Password Best Practices

Use unique passwords for each account.

Using the same password for multiple accounts could expose all your accounts following a single security breach. If you use the same password for multiple accounts, you increase your overall risk. The breach of a single account could to the breach of all your accounts because when a hacker knows your username and password on one service, they will try the same login information on other services.

With the amount of username and password data breaches that have occurred in the past several years including Yahoo and several social media sites, you can assume at least one of your passwords has been breached at this point. If you use the same password to log into your CFPB machine, those bad actor groups could potentially get access to your laptop, as well.

Instead, use unique passwords for every account you have and change them periodically. Your email addresses, personal banking, web services, mobile devices, and work computers should all have separate passwords.

May 26, 2020 - CyberWise Tip- Beware of new COVID-19 Themed Campaigns

Executive Summary:

The Cybersecurity & Infrastructure Security Agency (CISA) has identified two new COVID-19 related cyber threat attempts

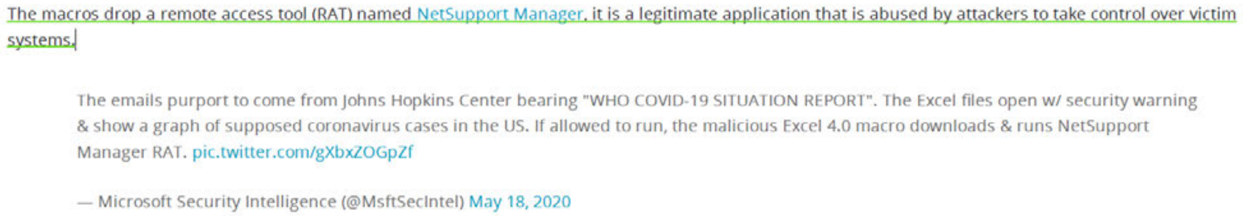
- New phishing campaign impersonates LogMeIn to trick remote users.
- Massive phishing campaign using COVID-19 themed emails observed by Microsoft.
- So far there have been no significant incidents beyond nuisance cyber activity resulting from these attacks.

COVID-19 Reports

- Email phishing scam impersonates LogMeIn to trick remote workers.

The phishing emails appear to come from LogMeIn, alerting the recipient of a patch to a zero-day vulnerability affecting the company's products. This bug, of course, does not really exist. Recipients are asked to click on a link that looks like a LogMeIn URL but leads to a convincing-looking phishing page.

- Security Affairs: Microsoft warns of "massive campaign" using COVID-19 themed emails.
- Massive phishing campaign using Covid-19 themed emails has been observed by Microsoft Intelligence team.



The macros drop a remote access tool (RAT) named NetSupport Manager, it is a legitimate application that is abused by attackers to take control over victim systems.

> The emails purport to come from Johns Hopkins Center bearing "WHO COVID-19 SITUATION REPORT". The Excel files open w/ security warning & show a graph of supposed coronavirus cases in the US. If allowed to run, the malicious Excel 4.0 macro downloads & runs NetSupport Manager RAT. pic.twitter.com/gXbxZOGpZf
>
> — Microsoft Security Intelligence (@MsftSecIntel) May 18, 2020

The emails contain an Excel documents that drop a remote access tool (RAT) named NetSupport Manager, it is a legitimate application that is abused by attackers to take control over victim systems.

Recommendations to avoid this threat:

- Keep applications and operating systems up to date.
- Be vigilant with attachments and links in emails.
- Review our Cybersecurity Phishing wiki page for phishing best practices at CFPB
- If you believe you are being targeted by a phishing campaign, please do not open the attachment – Click the "report phish" button in outlook or send as an attachment to (b) (6)

May 15, 2020 - CyberWise Tip- Treat Your Personal Information Like Cash

Do not share your personal information with just anyone.

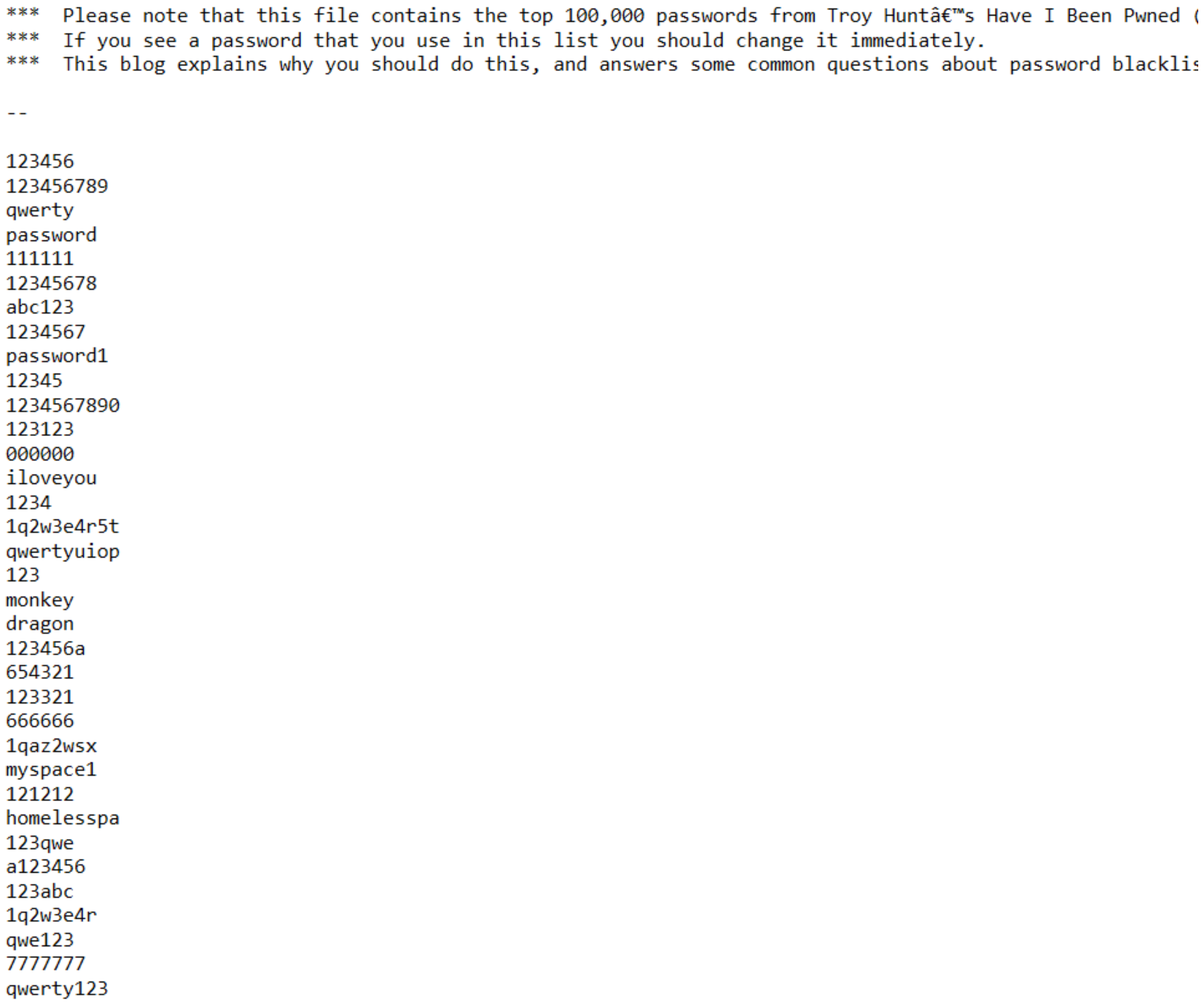
Your Social Security number, credit card numbers, and bank account numbers can be used to steal your money or open new accounts in your name. In order to steal your information, scammers will do everything they can to appear trustworthy.

So, every time you are asked for your personal information - whether in a web-form, an email, a text, or a phone message - think about whether you can really trust the request.

May 14, 2020 - CyberWise Tip- Advanced Persistent Threat Alert

There has been ongoing activity by advanced persistent threat (APT) actors against organizations involved in both national and international COVID-19 responses. APT actors are targeting pharmaceutical companies, medical research organizations, and government agencies in order to gather information related to COVID-19.

Most recently, APT actors are conducting large-scale COVID-19 related password spraying attacks, which is a style of brute force attack in which the attacker tries a single and commonly used password (e.g. “password123”) against many accounts before moving on to try a second password, and so on. This technique allows the attacker to remain undetected by avoiding rapid or frequent account lockouts. These attacks are successful because, for any given large set of users, there will likely be some with common passwords.



```
***  Please note that this file contains the top 100,000 passwords from Troy Huntâ€™s Have I Been Pwned (
***  If you see a password that you use in this list you should change it immediately.
***  This blog explains why you should do this, and answers some common questions about password blacklis

--

123456
123456789
qwerty
password
111111
12345678
abc123
1234567
password1
12345
1234567890
123123
000000
iloveyou
1234
1q2w3e4r5t
qwertyuiop
123
monkey
dragon
123456a
654321
123321
666666
1qaz2wsx
myspace1
121212
homelesspa
123qwe
a123456
123abc
1q2w3e4r
qwe123
7777777
qwerty123
```

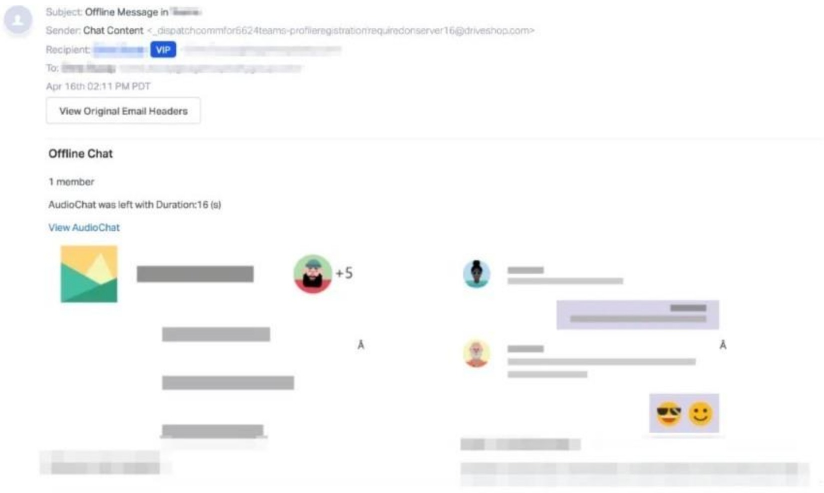
(sample list of passwords that get hacked)

CISA and NCSC are actively investigating large-scale password spraying campaigns conducted by APT groups, but always be sure to create a unique password for your CFPB account login and change it every 90 days. Be sure to check out our previous Cyber Wise tip on how to create a strong password and update any of your passwords that you think may need to get stronger.

May 13, 2020 - CyberWise Tip- Beware of Fake Microsoft Team Alerts/Office 365 Phishing Campaign

Cybersecurity has been informed of a recent phishing attack which uses pictures from automated Microsoft Teams notifications in an attempt to gain access to Office 365 credentials. This spoofed email phishing campaign was sent to between 15,000 to 50,0000 targets so far and is likely to be sent to more.

When attackers send phishing emails that mimic collaboration services (like MS Teams, Slack, Skye) they do so in an attempt to get users to ignoring any warning signs that would otherwise allow them to realize they’re being attacked.



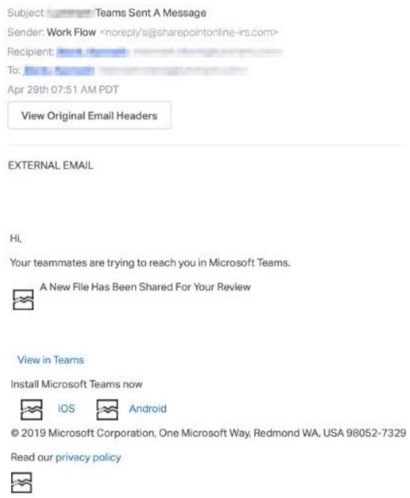
Subject: Offline Message in [redacted]
Sender: Chat Content <_dispatchcommfor6624teams-profileregistrationrequiredonserver16@driveshop.com>
Recipient: [redacted] VIP [redacted]
To: [redacted]
Apr 16th 02:11 PM PDT

Offline Chat

1 member

AudioChat was left with Duration:16 (s)

View AudioChat



Subject [redacted] Teams Sent A Message
Sender: Work Flow <noreply's@sharepointonline-irs.com>
Recipient: [redacted]
To: [redacted]
Apr 29th 07:51 AM PDT

EXTERNAL EMAIL

Hi,

Your teammates are trying to reach you in Microsoft Teams.

A New File Has Been Shared For Your Review

View in Teams

Install Microsoft Teams now

iOS Android

© 2019 Microsoft Corporation, One Microsoft Way, Redmond WA, USA 98052-7329

Read our privacy policy

Impact of this attack:

Credential theft or breach of cloud systems or data

Remediation for this attack:

- Always be suspicious about emails sent by unknown senders.
- Never click on the links/attachments sent by unknown senders.

May 7, 2020 - CyberWise Tip- Protect Your Mobile Devices

It's important to secure all mobile devices (e.g. laptops, tablets, cell phones) to protect both the device and the information contained on the device.

Ways to Protect Mobile Devices

- Always use a unique password to access your device.

- Try to use different passwords for different accounts. Passwords should include numbers, special characters (such as $,#,&), and avoid using words found in the dictionary: for example instead of 124password, use Drow$$12@p1

- If the Bluetooth functionality is not in use, disable it.

- Some devices have Bluetooth enabled by default. Be sure to check your device Bluetooth settings.

- Don't open attachments from untrusted sources. Your mobile device is susceptible to the same kind of cyber risk as your traditional desktop. You are still at risk of being exposed to malware when opening unexpected attachments on portable devices.

- Do not follow links to untrusted sources, especially from unsolicited email or text messages. Again, as with your desktop, your portable devices risk being infected with malware.

- Review the setting on your device to ensure all apps and operating systems are up to date. Be sure to encrypt emails whenever possible using the zix secure feature in outlook.

- If your CFPB device is lost or stolen, report it immediately to the ServiceDesk at extension (b) (6) or (b) (6)

May 6, 2020 - CyberWise Tip- Be aware of current Cisco WebEx credential Phishing scam

Please be advised that there is a current credential phishing scam targeting federal employees and seeking to steal credentials and distribute malware. The title of this scam email typically looks something like: Cisco WebEx “Alert!" "Your account access will be limited!”

Key Points: This small campaign in the United States attempted to harvest WebEx users’ credentials with emails claiming that recipients need to take immediate action to address a WebEx security vulnerability. Industries targeted include technology, accounting, aerospace, energy, healthcare, telecommunications, transportation, government, and manufacturing companies.

This campaign uses subject lines such as:

- Critical Update! - Alert! - Critical Update!, Your account access will be limited! - Your account access will be limited in 24h - Your account access will be limited!

If you believe you are being targeted by a phishing campaign, please do not open the attachment or respond to the email – report it using the “report phishing” button in outlook or send it as an attachment to our Cyber Operations team via (b) (6)

For the full report you can check out the Proof point website for a full report.

May 5, 2020 -CyberWise Tip- Do you know what information is being collected when you visit a website?

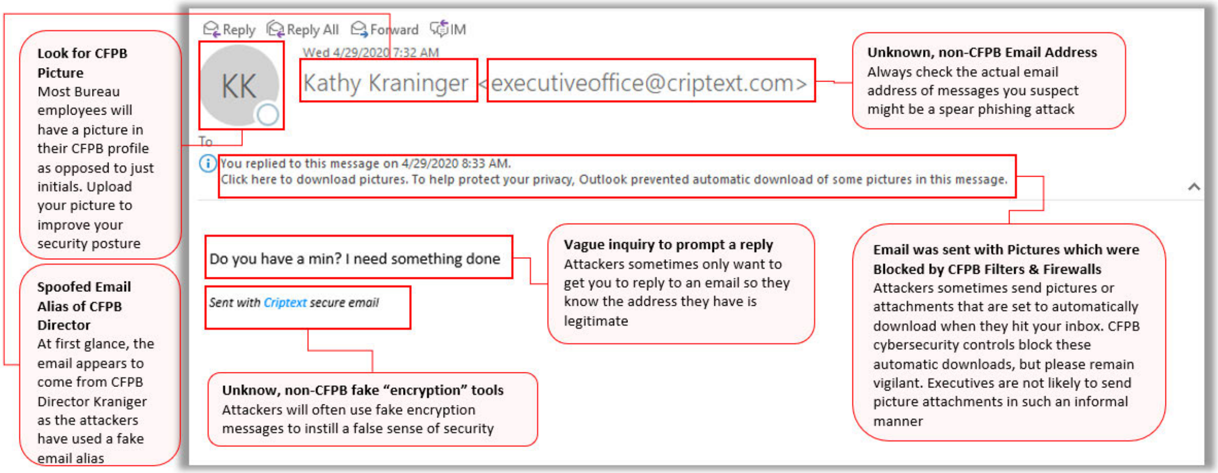
When visiting unknown websites, try to be vigilant about protecting your identity. Remember that some information is automatically made visible to the site. Personal information (such as your device's IP address, domain name, details about the software in use, or page visit information) is often saved in cookies so that the organization may develop and store user profiles of their website visitors.

If a website uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you've visited. If the site you're visiting is malicious, the files on your computer, as well as passwords stored in the temporary memory, may be at risk. Generally, organizations use the information that is gathered automatically for legitimate purposes, such as generating statistics about their sites. However, there are other malicious actors who are trying to gather this information to use it for financial gain or criminal activity.

Be mindful of the sites you visit, because you will be supplying them with some level of personal information. Unless you trust a site, don't give your address, password, or any other information.

April 30, 2020 - CyberWise Tip: Watch out for Spear Phishing & Whaling Attacks

A highly targeted form of phishing, spear phishing involves hackers sending tailored and personal emails to well-researched victims purporting to be a trusted sender. Spear phishing attacks are hard to spot without close inspection and difficult to stop with technical controls alone. While regular phishing campaigns go after large numbers of relatively low-yield targets, spear phishing aims at specific targets using specially emails crafted to their intended victim. Some targeted spear phishing attacks involve documents containing malware or links to malicious web sites to steal sensitive information or valuable intellectual property, or to simply compromise payment systems.



Wed 4/29/2020 7:32 AM

Kathy Kraninger <executiveoffice@criptext.com>

You replied to this message on 4/29/2020 8:33 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Do you have a min? I need something done

Sent with *Criptext secure email*

Look for CFPB Picture
Most Bureau employees will have a picture in their CFPB profile as opposed to just initials. Upload your picture to improve your security posture

Spoofed Email Alias of CFPB Director
At first glance, the email appears to come from CFPB Director Kraniger as the attackers have used a fake email alias

Unknown, non-CFPB Email Address
Always check the actual email address of messages you suspect might be a spear phishing attack

Vague inquiry to prompt a reply
Attackers sometimes only want to get you to reply to an email so they know the address they have is legitimate

Unknow, non-CFPB fake "encryption" tools
Attackers will often use fake encryption messages to instill a false sense of security

Email was sent with Pictures which were Blocked by CFPB Filters & Firewalls
Attackers sometimes send pictures or attachments that are set to automatically download when they hit your inbox. CFPB cybersecurity controls block these automatic downloads, but please remain vigilant. Executives are not likely to send picture attachments in such an informal manner

Spear-phishing attacks targeting high-level executives are often known as whale phishing attacks, and usually involve an attacker attempting to impersonate the CEO or similarly important person within the organization with the aim of using superiority to coerce the victim into sharing information. How to spot & thwart a spear phishing attack The Bureau employs many technical controls to prevent spear phishing emails from reaching your inbox including spam filters, malware detection and antivirus. However, these controls will not stop 100% of targeted attacks. Here are some characteristics of these types of attacks and actions for preventing them:

-Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address - Watch out for vague language or a generic request to click on a link or enter information. -Call the individual personally if possible, to see if the message was legitimate

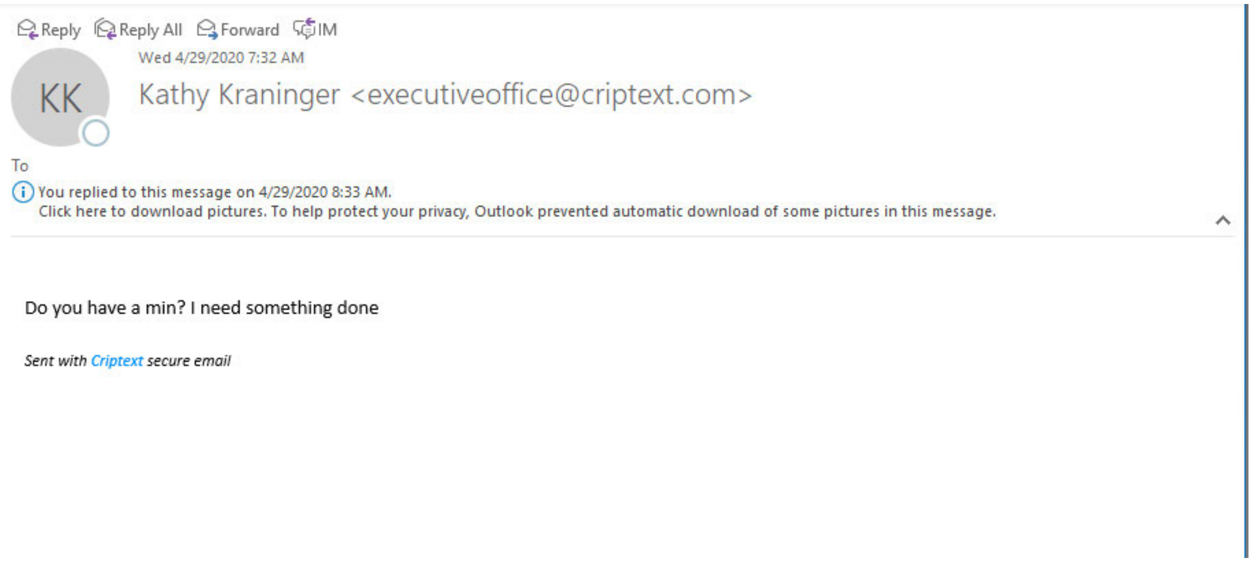
If you believe a message is suspicious, report it using the "report phishing" button in outlook or by sending as an attachment to (b) (6)

April 29, 2020 – CyberWise Tip- Watch out for spoofed emails!

We have seen an increase in attacks recently since bad actors often increase the frequency and severity of cyber-attacks during the current global heal crisis. One attack that is particularly popular with hackers lately is sending phishing email attacks to your work email that appear to come from your supervisor/boss. We experienced one of these attacks just today, with an attempt that appeared to come from the Director.

A bad actor can pose as top-level officials by masquerading their "From" email address, a signature or weblinks. Federal email addresses, like the ones we use at CFPB, can be requested via a Freedom of Information Act (FOIA) request. Some scammers may even send a spam email to your boss first to see if it is auto-replied with an "out of office" message, specifically so they can reach out to you under your boss' names since they are not in the office.

The boss gift card scam is so simple and requires almost no tech know-how. The email claims to be from your boss or someone you know. They might have “spoofed” your boss’ work email by subtly changing the address (e.g. John.Doe@cfpb.net), actively hacked into someone’s account, or are pretending they are locked out of their account and using a stranger’s phone or computer.



Wed 4/29/2020 7:32 AM

Kathy Kraninger <executiveoffice@criptext.com>

You replied to this message on 4/29/2020 8:33 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Do you have a min? I need something done

Sent with Criptext secure email

In this email scam, you are given a very plausible story as to why they need you to click on a link or send them something. These emails might ask you to buy a gift card and send over the numbers from the back or ask you to open a malicious attachment.

It is important to remember that there is no plausible reason why someone at work would need you to purchase a gift card. Most major companies will sell their gift cards in stores and online, and retailers like Amazon and Walmart who sell other companies’ gift cards will even sell others’ cards on their websites. The best way to avoid becoming a victim of this type of attack is to report emails to the security operations center (b) (6) and refrain from clicking all links or replying. Trust your instincts and protect yourself (and the organization).

If you suspect you have received a malicious email from a spoofed email address, report it using the “report phishing” button in your outlook or forward as an attachment to (b) (6). For additional questions or information, please reach out to the Cybersecurity Training Team at (b) (6)

-Your Cyber Training Team

April 28, 2020 – CyberWise Tip- Beware of COVID-19 Email Phishing Against US Healthcare Providers

Following a global increase in malicious cyber activity exploiting the uncertainties from the COVID-19 pandemic, the FBI was notified of targeted email phishing attempts against US-based medical providers. These attempts use COVID-19 related email subject lines and content to distribute malicious attachments, which exploited Microsoft Word Document files, 7-zip (.7z) compressed files, Microsoft Visual Basic

Script, Java, and Microsoft Executables. Here are a few examples of some of the known characteristics of the scam message:

Header text	Email Subject	Attachment Filename
srmanager@combytellc.com	PURCHASE ORDER PVT	Doc35 Covid Business Form.doc
srmanager@combytellc.com	Returned mail: see transcript for details	Covid-19_UPDATE_PDF.7z
srmanager@combytellc.com	COVID-19 UPDATE !!	Covid-19_UPDATE_PDF.7z
admin@pahostage.xyz	Information about COVID-19 in the United States	covid50_form.vbs

Steps to take to stay CyberWise:

- Be wary of unsolicited attachments, even from people you know. Cyber actors can "spoof" the return address, making it look like the message came from a trusted associate.
- Keep software up to date. Install software patches when prompted so that attackers can't take advantage of known vulnerabilities.
- If an email or attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the antivirus software might not have the signature.
- If possible, turn off the option to automatically download attachments. Check your email settings to see if your software offers the option and disable it.

If you believe you are being targeted by a phishing campaign, please do not open the attachment – just forward it to our Cyber Operations team via (b) (6)

April 23, 2020 – CyberWise Tip- Denial-of-Service Attacks, explained

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. This may impact services including email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network.

A denial-of-service attack is accomplished by flooding the targeted website or service with traffic until the target cannot respond or simply crashes, preventing access for legitimate users

Symptoms of an attack include unusually slow network performance (opening files or accessing websites), unavailability to access an individual website or any websites. If you believe a system has been the target of such an attack, there are a few recommended steps to take.

On Bureau provided devices connecting to the CFPB network: If you are connected to the internet but are losing connection to any Bureau systems, contact the CFPB Service Desk (b) (6)) to report the issue and get advised on the appropriate steps to take.

On a home network: Check to see if other devices in your home are connected. If multiple devices lost connection, you can reach out to your Internet Service Provider (ISP) to ask if there is an outage on their end and they will advise you on an appropriate course of action.

April 22, 2020 – CyberWise Tip- Email attachments, click with caution

Did you know email attachments are often used as tools for attacks by cyber criminals? Think about how easy it is to circulate messages to thousands, even millions of people with just a few clicks. Many of the programs we use day-to-day offer the ability to download attachments automatically, which can lead to an unsuspecting user downloading a virus without a second thought.

Tips to keep yourself protected:

- Be wary of unsolicited attachments, even from people you know. Many viruses can "spoof" the return address, making it look like the message came from someone else.
- Keep software up to date. Always comply with CFPB prompts for system updates in a timely manner

April 21, 2020 - CyberWise Tip- Here's why you probably shouldn't share your old senior photos on Facebook

In a recent social media trend, people have been sharing their own senior photos on Facebook with the hashtag #ClassOf2020. This is meant to be an act of solidarity with students who have had their graduation ceremonies cancelled due to COVID-19. However, these posts could help potential hackers crack into your private accounts. Attackers scan sites like Facebook for this hashtag where they can also find the name of a person’s high school and graduating year -- two common online security questions. And if that user’s social media account is not set to private, hackers can find plenty of data that they can use for social engineering attacks. Before sharing, users should make sure their accounts are set to private and that they are using strong passwords for all accounts. Also, ensure there is no public-facing information on social media sites that users would not like in the hands of a hacker.

April 16, 2020 - CyberWise Tip: Advanced Persistent Threats (APT)

Advanced persistent threat (APT) style cyber-attacks usually involve politically or financially-motivated actors with the skills and intention of deploying a targeted and sophisticated attack on a single entity.

With the evolving global health situation, APT style attacks are on the rise as nation states or enterprising cyber criminals attempt to exploit user vulnerabilities.

The best action is prevention.

Remember to always stay vigilant and on alert for potential suspicious activity. Be sure to check out the social engineering tactics we've previously mentioned available on our Tip of the week wiki page.

April 15, 2020 - CyberWise Tip: Bluesnarfing, explained

There are many ways which your Bluetooth-enabled device can be compromised. One way is with bluesnarfing via which a cyber-criminal steals your information by using a Bluetooth connection to hack into your phone.

Many mobile capabilities, including Airdrop, use Bluetooth LE to broadcast and discover connections and point-to-point Wi-Fi to transfer data. While these attacks are rare and require close physical proximity, leaving these Airdrop features enables increases the risk an attacker will find and target your mobile device.

Check to see if your device allows for PIN numbers or passwords to be used for your Bluetooth enabled devices when pairing or turn off your Bluetooth when not in use. When in public places be wary of accepting unexpected connection requests – including unsolicited airdrops.

For more actionable tips on how to stay Cyber Wise, we have tips on Mobile Device security 101 and What you should know about Mobile App Security?

Check out our full archive of Cybersecurity Tips on our Cyber wiki page
- https://team.cfpb.local/wiki/index.php/Cybersecurity_Tip_of_the_Week

April 14, 2020 - CyberWise Tip: You are always the target

It’s important to keep in mind that you, as the end-user, are always the target of a cyber-crime.

A common user misconception is that their data is not valuable and therefore would not be the target of an attack. This assumption is incorrect -- all personal, government, or corporate information is valuable to the right buyer, and any user with an online presence can be a target.

While some risk is inherent with any online activity, it’s important to know that everyone has a key role to play in cyber safety whether onsite or at home. For more actionable tips on how to stay Cyber Wise, check out our Cybersecurity Tip of the week archive at
https://team.cfpb.local/wiki/index.php/Cybersecurity_Tip_of_the_Week

April 10, 2020 - CyberWise Tip: Spyware, explained

Spyware (also known as adware) is software often installed on a computer system to monitor the computer and end-user's activities without the user's awareness or consent. This often includes collecting confidential data such as passwords, PINs and credit card numbers, monitoring keyword strokes, tracking browsing habits and harvesting email addresses. This also tends to affect network performance, slowing down the system and affecting the whole business process. It is generally classified into four main categories: Trojans, adware, tracking cookies and system monitors.

- Trojan spyware that infects computers in the form of Trojan malware.

- Adware that also serves as spyware to monitor computers and devices.

- Tracking cookie are files put on hard drives by website that track a user on the Internet if a site is aware of the tracking cookies and designed to use them.

- System monitors are designed to monitor any activity on a computer and capture sensitive data such as keystrokes, sites visited, emails and more.

The best way to control spyware is by preventing it from getting on your computer in the first place. We know not downloading programs and never clicking on email attachments isn't always an option, so try to remember to always, *stop and think, before clicking*

April 9, 2020 - CyberWise Tip: Botnets, explained

Botnet is the generic name given to any collection of compromised PCs controlled by an attacker remotely — think "virtual robot army." The individual PCs that are part of a botnet are known as "bots" or "zombies," and their owners may not even know they're being used.

Beware, many botnets are typically designed to harvest data, such as passphrases, Social Security numbers, credit card numbers, addresses, telephone numbers and other personal information. The data is then used for nefarious purposes, such as identity theft, credit card fraud, spamming (sending junk email), website attacks and malware distribution.

April 8, 2020 - CyberWise Tip: Malware, explained

Malware is malicious (purposefully harmful) software. There are many software programs that carry out malicious activities such as viruses, worms, ransomware, rootkits, and logic bombs.

- **Virus-** malicious code that attaches itself to the host application. Once the host application is executed, the virus' malicious code executes.

- **Worm-** A self-replicating kind of malware that travels through a network. They do not need any user action in order to run.

- **Ransomware-** A kind of malware that is used to extort money from people and/or organizations. Often encrypts your data and demands ransom payment before decrypting the data.

- **Rootkits-** Malware that gains system-level access to your computer. Often able to hide themselves from users and antivirus software.

- **Logic bombs-** Malware that executes in response to an event. The event can be a specific date/time, or an action like a user launched program.

The best way to control malware is through prevention. By not downloading programs or clicking on email attachments from unknown sources in the first place, you will be able to prevent it from getting on your computer.

Remember to always, *stop and think, before clicking*.

April 1, 2020 - CyberWise Tip: Beware of Stimulus relief fraudulent activities

The Secret Service is observing a rise in stimulus relief fraud over the past several days and expect the fraud attempts to continue throughout the pandemic. Criminal actors are using a variety of means to contact potential victims. In one instance, the criminal actors are using spoofed email addresses posing as U.S. Treasury officials requesting that the victim provide personal identifying information (PII), so that they can receive their share of the stimulus.

Criminal cyber actors are exploiting the COVID-19 pandemic through scams and malicious activity. These actors seek to profit from a sudden growth in teleworking, increased use of virtual education systems for online classes, a surge in online shopping, public appetite for information related to the pandemic, and the criticality of maintaining functioning critical infrastructure networks, particularly in the Healthcare and Public Health Sector. Attackers are attempting to deliver Remote Access Tool (RAT) payloads on the systems of small businesses via phishing emails impersonating the U.S. Small Business Administration (U.S. SBA)

US Secret Service (USSS) Field Offices and USSS Electronic Crimes Task Forces around the country are actively working with federal, state and local partners to combat cyber enabled fraud, such as ransomware and business e-mail compromise attacks against the health care industry and state/local governments.

- FEMA has created a Coronavirus Rumor Control page: https://www.fema.gov/Coronavirus-Rumor-Control - New government website for COVID-19 guidance: https://www.coronavirus.gov/

March 31, 2020 - CyberWise: Staysafeonline.org resources for home online safety

STOP. THINK. CONNECT. ™ is a global online safety awareness campaign to help all digital citizens stay safer and more secure online. The Department of Homeland Security leads the federal side of the campaign with leadership provided by the National Cyber Security Alliance (NCSA). The campaign was launched in October of 2010 by the STOP. THINK. CONNECT in partnership with the U.S. government, including the White House.

There are many free resources provided by the site, but since everyone is online more than usual, we wanted to link to their free online security checkups and tools you may want to check out:

OpenDNS

DNS stands for Domain Naming Service. Its the service that runs when you access the internet to resolve host names (think google.com) to IP addresses (ex: 172.11.31.22) to pull in the web resources that you need to access.

- OpenDNS Web content filtering keeps parents in control of what websites children visit at home.
- OpenDNS blocks phishing websites that try to steal your identity and login information by pretending to be a legitimate website. Surf the Web with confidence.

Visit https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools/ for the full list of free resources you may want to implement on your home network.

March 26, 2020 - CyberWise: Cybersecurity Remote Fundamentals

Here are a few tips sourced from industry experts about safe teleworking practices:

Remote Basics

Experts recommend using the following basics to ensure a successful and stress free teleworking experience:

- Computer with good internet connection
- Dedicated workspace
- Phone, camera, chat and conference applications (Skype or WebEx/MyMeeting)
- A comfortable routine with self-motivation and a bit of discipline

Utilize Virtual private network (VPN) when possible

A virtual private network encrypts your network traffic (the data you send over your internet connection) to prevent eavesdroppers and cyber snoopers. Your CFPB provided devices are equipped with Citrix always-on-VPN, so be sure to use as-is, especially when trying to access CFPB shared folders or drives.

Update your passwords

Make sure your passwords are unique and complex enough across all your accounts. Check out our previous tip on how to create a unique and strong passwords for your accounts here.

Keep your devices updated

Within your device settings, you have the ability to turn on a feature that notifies you when a system patch has become available.

Use separate user accounts

In your home environment, experts recommend that you have different accounts set up for individual users, with limited administrators.

That allows for greater transparency and accountability regarding system use because devices have activity logging capabilities which works best when each user is separated, especially guest users.

Check out our Cyber Tip of the week wiki page for our archive full of helpful cybersecurity tips, Cybersecurity tip of the week wiki page here.

March 25, 2020 - CyberWise: Tips to Detect a COVID-19 Phishing Scam

Following our on Coronavirus scams tips last week (all tips can be found on our Cybersecurity tip of the week wiki page), we wanted to provide a few tips on the red flags to look out for that might indicate you are being targeted for a Coronavirus scam email. Cofense has a fun infographic that you can view on their website via: https://cofense.com/wp-content/uploads/2020/03/Coronavirus-Scams_Infographic.pdf

- Use sense of urgency language?

If the sender is someone you are not familiar with and use words that attempt to play on fear or try to rush you, that's a major red flag. For instance, if they ask you to click a link to learn about "high risk areas" or "infection rates near you now", they may be trying to get you to act fast. Remember, stop and think before you click. We recommend using the World Health Organization, CFPB, and CDC's websites as official sources.

- Asking for your info

Is the person asking for your information? Think about it, does it make sense for a public health organization or professional that you don't know to ask for your personal information? If the email is doing so, that is a major red flag. As we mentioned previously, the FTC has a resource you can access to check if there is a charity you are interested in financially supporting. Check the Federal Trade Commission's website for more information about donating: https://www.consumer.ftc.gov/articles/0074-giving-charity

- Using awkward phrasing?

I know you have gotten emails using "Greetings Sir or Madam". Red flag. If someone is using extremely generic and unspecific greetings like a stranger, you should probably treat them like a stranger. Please do not trust an untrusted source. Forward the email to our Cybersecurity analysts to review via [redacted] (b) (6)

- Grammar and spelling errors?

You would be surprised, but often phishing emails have spelling or grammar mistakes that a business professional normally wouldn't make. If it doesn't read right, something else is probably not right.

If you believe this is a potential scam, please forward to our Cyber team via [redacted] (b) (6) Use your best judgement when opening emails, especially if it's COVID-19 related.

Check out our Cyber Tip of the week wiki page for our archive full of helpful cybersecurity tips, Cybersecurity tip of the week wiki page here

March 24, 2020 - CyberWise: How to stay Cyber safe at home

Following our tips last week on Coronavirus scams to keep an eye out for (all tips can be found on our Cybersecurity tip of the week wiki page). We wanted to provide a few tips on how to protect your cybersecurity at home:

- Be sure to only use the CFPB provided teleworking resources for work activities

CFPB provided many resources perfect for working at home securely during this time. Cisco Always-on-VPN (always-on-virtual private network), mobile device, laptop, and teleconferencing lines (Skype and/or Webex/Mymeetings).

It's important to conduct all your work using devices that already have enhanced security features. That will slow down and prevent bad actors from using your account to access government network resources.

- Update your passwords and use Two Factor whenever possible

On your home network, be sure to update your passwords. Remember to use complex and different passwords for every account you have (email, social media, food delivery accounts, etc).

We also recommend turning on two factor authentication on your personal email accounts as well. Google, Microsoft, and RSA all have account authentication apps you can download to your mobile device from your App store. With that app on your phone, it will send an alert to your phone once someone (hopefully you) enters a password to access your account. This allows you have to permit access to your account two times, before you can actually login. Imagine how much more difficult that feature will make it for cyber criminals to access your account.

- Be aware of Phishing Scams

It can be easy to let your guard down when working from a more non-traditional work setting, but remember to always *Stop and think, before you click.*

Take an extra second and hover on the URL provided to you. Is it from someone you know? Were you expecting this link or resource? If so, proceed as usual. If you answered no to any of the questions I asked you to ask yourself, try and utilize the preview attachment feature available in your email. That is a feature that allows you to take a look at parts of the attachment without downloading or opening the full attachment.

If you believe this is a potential scam, please forward to our Cyber team via [redacted] (b) (6). Use your best judgement when opening emails, especially if it's COVID-19 related.

- Be wary of emails and phone calls asking for COVID-19 donations

Do your research first, especially for organizations unfamiliar to you. If you want to donate, we suggest running a quick verify of the charity's authenticity before making donations. Check the Federal Trade Commission's website for more information about donating.
https://www.consumer.ftc.gov/articles/0074-giving-charity

If you believe you are a victim of a cybersecurity scam or data breach, you can report it to our Cybersecurity analysts via [redacted] (b) (6) if it happened on your CFPB device. If the violation occurred on your personal device (non-government issued laptop, cell phone, etc),you can report it to the FTC. To report fraud to the Federal Trade Commission, visit www.ftc.gov/complaint.

Check out our Cyber Tip of the week wiki page for our archive full of helpful cybersecurity tips.

March 19, 2020 - Android ransomware posing as a Coronavirus tracking app

Please watch out for an android app called **Coronavirus Tracker** from the URL *hxxp://coronavirusapp[.]site/mobile.html*. Do not download on your personal mobile devices. While it alleges to track the spread of coronavirus globally, the app actually is ransomware, meaning it will lock you out of your phone and demand you pay money to unlock it.

It will attempt to trick users into allowing it to have admin access by stating that it will notify you if an infected patient is close to you, but is actually trying to gain admin access to your phone to lock you out and begin the attack.

The app is also persistent, meaning even if you reboot your device the app will execute every time.

Cyber pro-tip: Be very skeptical of any application requesting administrative privileges. It is a huge red flag to watch out for. If an app is asking for admin access, you are essentially giving them the master key to control your device. Really question if an application should have that much control over your device.

Luckily this app is not that complicated to remove. Zscaler has a resource to assist in better understanding how to remove the app here.

If you are a victim of the ransomware, you can use **pin 4865083501** to unlock your device. Then remove the app from the Apps list on your device, under the Settings feature on your device ASAP.

T&I is assessing the risk similar external apps pose to Bureau-issued iPhones. Please stay tuned for any updates.

March 18, 2020 - Don't fall for these Corona virus online scams

As we all figure out a way to stay safe and informed as the Corona virus continues to impact our daily lives, we will be using our Cyber tips to notify you of online scams (including malware and ransomware attacks spread through emails and apps) to the best of our ability.

Here are the latest COVID-19 scams you should be aware of:

1) APT36, an Advanced Persistent Threat group posing as the government of India
There is currently an online attack that pretends to provide corona virus guidance from the Indian government but is actually a program managed from a remote distance (remote access Trojan) to steal your data.

It's believed that this scam comes from a Pakistani state-backed threat actor. It is designed to look like a coronavirus health advisory, but once a user clicks the link on the attached document the program installs remote access trojans on your device and goes to work discovering your devices specs to pull out your data.

Please look out for emails with links appearing as *(email.gov.in.maildrive[.]email/?att=1579160420)*. If you receive this link please forward to our Cyber SOC team via [redacted] (b) (6).

2) Many state-sponsored threat actors are in on the fun

Don't believe the stereotype about the guy sitting in his mother's basement as the cybercriminal you should fear. There are many instances were nations-state actors are bankrolling expansive teams in order to hack our government networks and resources. We know that China, Russia, and North Korea already have the following groups using the coronavirus outbreak to attempt online scams:

- Chinese APT: Vicious Panda, Mustang Panda
- North Korean APTs: Kimsuky
- Russian APTs: Hades group (ties with APT28), TA542

Especially on your Bureau provided devices, please be very aware of who is sending you emails with attachments and links before you open or click.

Stop and think before you click. By hovering over the link with your mouse and using the attachment preview option, you can see the link or attachment before you act on it.

March 17, 2020 - CyberWise: Tip: Watch out for Bogus COVID-19 Scams

Hi All,

Unfortunately, there have been a rise in online scams using Corona virus to try and take advantage of people during this time. Last week we posted about attackers using a fake live map from John Hopkins University to infect concerned citizen. Please be wary and a little skeptical of any unsolicited advice or guidance about the Coronavirus. We advise using your best judgement and highly trusted news resources when staying informed.

Two more scams to look out for:

1) World Health Organization (WHO) COVID-19 scam: Phishing emails sent to users which encourages them to download an attachment by clicking on a link called "Safety measures". PLEASE DO NOT CLICK. The WHO will never email attachments that were not explicitly requested. Visit www.who.int/about/communications/cyber-security to read about cyber tips from WHO.

2) CDC Doctor COVID-19 Scam:

Phishing attacks where emails from fake doctors from the CDC are sent to users promising secret information regarding how to stay protected from COVID-19. These secrets do not exist so please do not click on any links promising this information. Please go directly to the CDC web page, to stay up to date on their reporting's. For up to date COVID-19 info from the CDC visit www.cdc.gov/coronavirus/2019-ncov/index.html

Remember that cyber criminals often use tactics like sense of urgency to try and trick you to go against your better judgement. Don't reward them for it. Be sure not to click links you are not sure about (pro-tip: hover over the link to see the URL, if it's is not trustworthy don't click).

March 11, 2020 - CyberWise: So your Cybersecurity department has been bugging you to create a complex password...?

Yes, we keep lovingly reminding you that you need a complex or strong password. And yes, we get how annoying we can be about it. Stay with me, there is a reason.

Did you know that more than 14 million Americans are victims of cyber related identity theft? I bet you also didn't know that about 3.3 million of them have to bear the financial responsibilities of the fraud committed under their identity.

Okay, so I can feel through this screen that you still don't believe me, so check out this Newsweek article backing me up here (promise it's not a phishing attempt).

Here is an easy way to make creating a strong AND unique password simple:

- **Think of a password more as a passphrase**

Try piecing together a string of four or five un-associated words, such as "hairy moose scares grandma" to create a unique set of characters that is easy recall but hard for someone to crack.

The sequence will look like 1harryM0ose@Scar3sgrandm@

Nice and easy right? Pro-tip courtesy of Newsweek: Try using the first letter of each word in a line or two of your favorite song or quote. Say, for instance, you're a fan of Old Town Road by Lil Nas X, which begins: "Yeah, I'm gonna take my horse to the old town road. I'm gonna ride 'til I can't no more." Using the first letter of each word of these two lines of the song results in a password that looks like this: **yigtmhttotrigrticnm**

Now that you are armed with this handy-dandy tactic, be sure to rinse and repeat with all your passwords so they are different. Remember, once a cyber criminal gets one of your passwords, they will try it on all your accounts. If they do that with you, will they be able to access more than one of your accounts?

Check out the full Newsweek article here to see the remaining 6 tips to create a unique and strong password every time.

March 10, 2020 - CyberWise: Managing your Digital Footprint

Have you heard that data is new gold?

Continuing our digital awareness theme, here are a few things to keep in mind with any digital technology you use.

Now is the time to be as mindful as possible about your digital footprint, privacy, and data security.

Here are a few ways to manage your digital footprint:

- **Google yourself**

Yes, seriously search for yourself on your favorite search engine and see what pops up.
Did you know that many employers look you up before hiring you? You should know what is out there about you and decide if anything needs to be regarding the data on you.

- **Check your old social media accounts and posts**

First, be sure to check your account privacy settings.
You should set your account to private, but if you are willing to have your account set to public, make sure everything that is publicly available is what you want to be available.
There is nothing wrong with doing a scrub of old tweets or posts that didn't age well or are inappropriate.

Take a few minutes to review your posts and make sure you are proud of everything attached to your name.

- **Hide or modify accounts that don't allow you to delete your old accounts**

Unfortunately, some services don't allow you to delete your presence easily. In cases where someone else may have uploaded your likeness, consider trying to change the name or email address attached so it doesn't follow you forever. If possible, try swapping out an unflattering picture of yourself with a more innocent image. Hopefully with time, the image should stop appearing in search engines.

- **Consider use of a secondary email**

Create a non-federal email account for any personal shopping or non-work related activities. It would also be good to use that email account for sites that insist on sending you marketing or sales materials. The email should be used for any correspondence that is not related to family, friends, or school activities. These companies are more likely to be hacked or spoofed, which can lead to the theft of your information. So be sure to give them the fake stuff.

March 4, 2020 - Digital Spring Cleaning Tips

With spring right around the corner, that means spring cleaning is quickly approaching. Now is the time to clean your digital devices to ensure an optimized and secure environment.

Here are a few cyber spring cleaning tips, inspired by the SANS March newsletter:

- **Refresh your passwords**

Take a look at your passwords. Yes, all of them. Do you have a habit of reusing the same password for all your accounts? That is a big risk and increases the likelihood that your account can be compromised. Change any account password that is not unique and be sure to include complex passwords. Complex passwords utilize the combination of numbers, special characters (ex: @, &, !, $), and both capitalize and lower case letters.

- **Clean desk policy**

Make sure you do your best to keep a clean desk. Meaning no papers, removable media devices (usb drives), or sticky notes with too much personal info is left out or in an unlocked and visible location.

- **Consider an email purge**

This may work better for your home environment, but its still worth considering doing a mass purge of old email files that you have not looked at in more than 2 years. Do you really need all of that info? If not, consider moving the important emails to a secure cloud drive location, or even better to a secure hard drive.

- **Update your devices and apps.**

Make sure you have the latest version of your apps installed. If you notice any apps you use have not released an update or patch of any kind in the last 8 months consider deleting that app. Apps that do not regularly patch their own system vulnerabilities (every form of tech has vulnerabilities) will leave you open to feeling the effects of a breach. Uninstall that app before you have the chance to be hacked. Consider uninstalling apps you have not used or opened in a year.

- **Double check your financial & social media accounts privacy and alert settings**

This will be an often-repeated tip. Check all your social media and bank/credit cards to ensure your privacy settings are at a level comfortable to you. Also take a few minutes to opt-into the transaction alerts feature, so you have the ability to spot and report fraudulent activities as soon as possible.

March 3, 2020 - Mobile Device Security 101

Have you ever stopped to consider how secure or safe your device is?

In 2020, it seems like everyone has at least one if not two mobile devices. These convenient little devices go everywhere with us. They enable us to conveniently connect to several different networks and services based on proximity and access. We can quickly check email, text messages, social media, bank and credit card accounts, watch movies and other media at the drop of a dime.

How sure are you that if you lost your phone tomorrow some unauthorized person won't be able to access your personal information? If you have a CFPB issued mobile device, are you doing your part to protect the Bureau network data and resources?

With the ability to connect to many different data resources, comes great responsibility. Here are a few tips to keep your device secure:

- **Enable fingerprint logins for your device**

Your fingerprint is much more complex and harder to crack than any strong password you can create. Also, it's hard to forget your fingerprint.

Pro-tip: Use your fingerprint (something you have) *with* a complex password (something you know) for multi-factor authentication. Multi-factor authentication requires at least two different forms of identification verification, so even if your device is lost, the criminals are far less likely to pull any info from you before you report the device stolen to our Service Desk.

- **Be wary of which apps with access to your location. Disable location services when you can**

Many apps request permission to access your location-based service (aka GPS) available in most smart devices. Be wary of who you allow to have this. An app that has this access permission but does not provide updates to their app can introduce security risks to you.

- **Consider remote wiping software**

Most smart phones come with the ability (check your device settings) for the data to be erased from a remote location. In order to prevent your data from getting into the wrong hands, you may want to look into how your device remote wipe technology works before it's too late.

- **Back up your data. Early and often.**

Hopefully you will never need to wipe your data due to a ransomware attack, however you should be backing your data up on a hard drive or onto your cloud account (which has a [passphrase]) regularly.

February 26, 2020 - What you should know about Mobile App Security?

Mobile security is not the hottest term on the block right now. Even software developers, who tend to be more technically savvy than the average person, focus on technical performance, optimization, design, or user experience before thinking about mobile application security.

"75% of the apps in the public app stores do not pass basic security checks." -AppKnox. View the rest of the article discuss 10 reasons Apple app store rejects apps, here.

So, how you can ensure the apps on your phone are secure?

- **Do NOT install or download 3rd party apps to your device, especially your government issued device.**

The official app store (Play Store, Apple Store, etc) should be your first place to search for apps. They have security filters, however just because they are in the app store does not mean they are safe to use. If they require too many permissions, you should consider not installing. For example, does a flashlight or QR scanner really need permission to access your contacts?

- **Update your device software often**

Your phone manufacturer (Apple, Android, etc) releases software patches and new versions to fix vulnerabilities and bugs found on their system. Best practice is to install the approved updates as soon as possible unless directed otherwise by our Service Desk.

- **Remove old apps**

The older the app, the more likely it is to present vulnerabilities to your device and privacy. Check the app to make sure you have the latest update, and if the latest update is more than 8 months old, consider deleting the app. If developers are not updating the app, you probably should not be using it. Also, if you are not using the app, delete it.

- **Don't leave your device unattended**

Lock your phone when not in use and check to make sure no new and/or unauthorized applications, services, or processes have been added to your device without your knowledge.

February 25, 2020 - Stay secure on your mobile devices

Every device comes with the risk of being hacked, especially if it has internet connectivity. Are you sure your device is secure?

How to keep your government issued mobile device secure:

- **Use strong passwords**

Use at least 10 characters; 12 is ideal. Do not repeat passwords between different accounts.

- **Keep software up to date**

Application vendors and your phone manufacturer (Apple, Android, etc) release software patches and new versions to fix vulnerabilities and bugs found on their system. Best practice is to install the approved updates as soon as possible unless directed otherwise by our Service Desk.

- **Disable remote connectivity**

Technology such as WiFi and Bluetooth should be turned off when not in use. Those are often used mechanisms for unauthorized access to your device, network, and data without your knowledge.

- **Don't leave your device unattended**

Lock your phone when not in use and never leave it unattended in public.

For more of a deep dive, the Federal Communications Commission has a smartphone security checker to help smartphone owners keep their devices secure. Access the FCC checklist here.

February 21, 2020 - Tips to Protect your ID and Passwords Online

Protect Your Personal Information

These days your data is like cash, so protect it like you would your wallet. Think about it, your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or more importantly **- your identity**. When entering your personal information – in web form, email, text, or a phone call – think about why the requester needs it and if you can fully trust the request. Do you really know this person? Do they know you? Scammers will do everything possible to appear trustworthy to gain your credentials (such as name, password, personally identifiable data).

Protect Your Passwords Here are a few ideas for creating strong passwords and keeping them safe:

- Use at least 10 characters; 12 is ideal.

- Be unpredictable – don’t use names, dates, or common words. Mix numbers, symbols, and capital letters into the middle of your password, not at the beginning or end.
- Don’t use the same password for more than one account. If it’s stolen from you or one of the companies where you do business – thieves can use it to take over all your accounts.
- Don’t share passwords on the phone, in texts or by email. Legitimate companies will not ask you for your password, especially here at CFPB.
- If you write down a password, keep it locked up, out of plain sight.

January 29, 2020 - Tips to Prevent Identity Theft during Tax Season

Did you know that you can be a victim of identity theft even if you never use a computer?

As noted by CISA here, the internet has made it easier for thieves to obtain personal and financial data. Most companies and other institutions store information about their clients in databases; if a thief can access that database, he or she can obtain information about many people at once rather than focus on one person at a time.

Tips to prevent Identity Theft this Tax Season

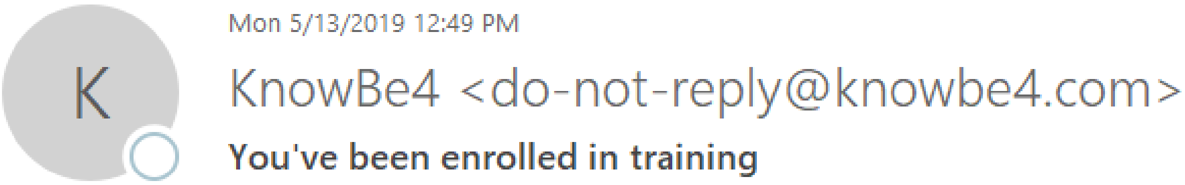
- Take advantage of security features – Passwords and other security features add layers of protection if used appropriately.
- Be careful what information you publicize online – Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums.
- Keep your anti-virus software and a firewall up to date – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. Keep your virus definitions up to date.
- Be aware of your account activity– Pay attention to your statements and check your credit report yearly. You can grab a free copy of your credit report from each of the main credit reporting companies once every twelve months.

For more resources to help you stay cyber safe this tax season, check out the FTC's article on Tax-Related Identity Theft and the IRS's Taxpayer Guide to Identity Theft

For the Cyber Tips of the Week archive
- https://team.cfpb.local/wiki/index.php/Cybersecurity_Tip_of_the_Week

January 15, 2020 - Mandatory Compliance Period for Cybersecurity Awareness Begins Next Week!

All CFPB employees and contractors are required to complete cybersecurity awareness training as part of the Mandatory Compliance Training period. Look for an email from "KnowBe4" next week which will contain a link to the ~30-minute training. The email will appear similar to the below in your outlook:



Mon 5/13/2019 12:49 PM

KnowBe4 <do-not-reply@knowbe4.com>

You've been enrolled in training

Please run the course in the Google Chrome browser. If the course does not open in Google Chrome, copy and paste the provided link in a new Chrome browser window.

This communication is not a phishing exercise and is being sent on behalf of Cybersecurity Training. If you have any questions regarding this mandatory cybersecurity awareness training contact (b) (6)

January 8, 2020 - Announcement: Increased Potential for Cyber Threat

The DHS Cybersecurity Infrastructure Security Agency (CISA) issued an alert describing the potential threats to US cybersecurity interests as a result of recent developments in Iran. Iran continues to engage in more "conventional" cyber threat activities ranging from website defacement, distributed denial of service (DDoS) attacks, and theft of personally identifiable information (PII), but they have also demonstrated a willingness to push the boundaries of their activities, which include destructive wiper malware. The original DHS alert is posted here

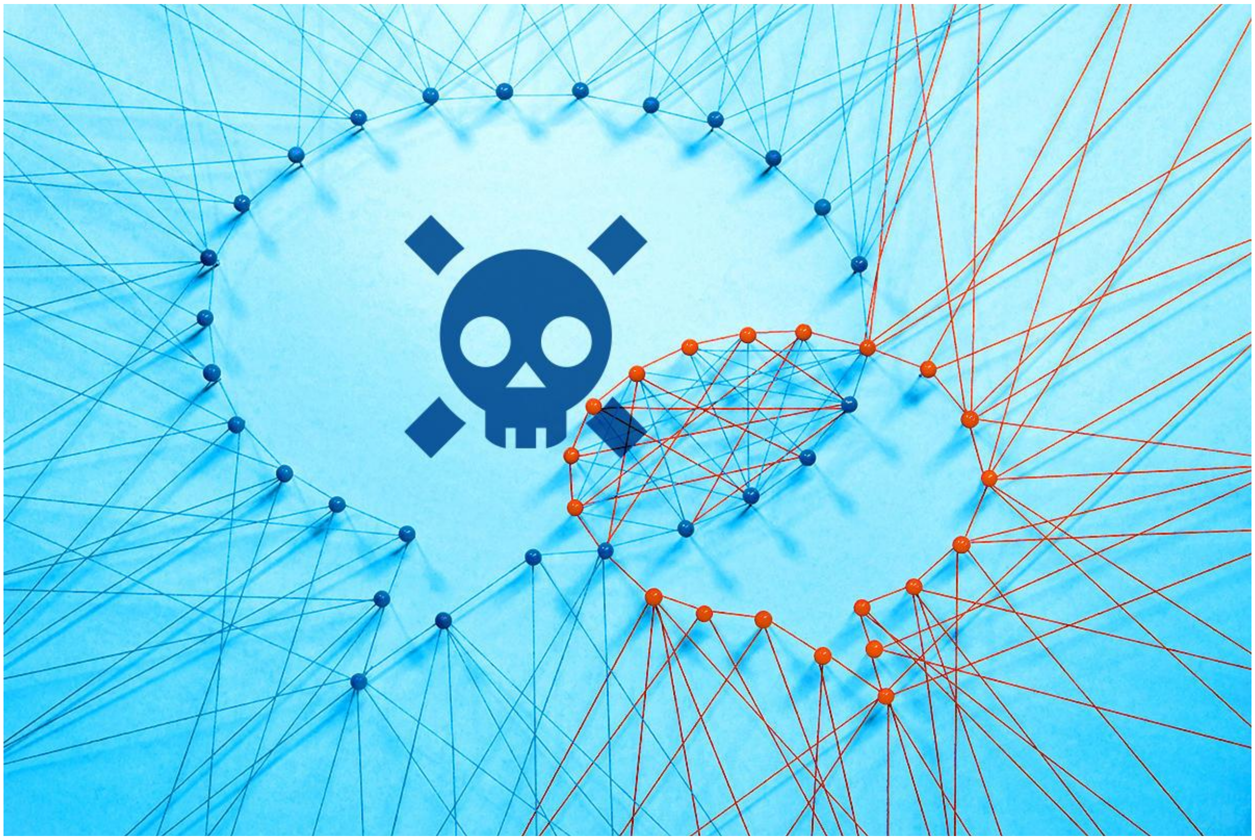
Bureau personnel are reminded to be vigilant in their daily work and report suspicious activity on IT systems to Service Desk for analysis by the Cybersecurity Team.

January 2, 2020 - Oversharing and identity theft: How to avoid both and stay safe online

Oversharing can influence your online security aka make you a target for cyber criminals.

According to CSO, "Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data. For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password."

Check out CSO's Social Engineering Explained Guide here.



Data like phone numbers, names of relatives, your pet’s name, credit card info and more can be collected and put together to:

- Attack your accounts
- Compromise your accounts
- Empty your credit card
- Send spam and malware from your computer or email address.

Here are a few tips to use to prevent oversharing and ID theft (Part 1):

1) Choose and utilize a strong & unique password for your online accounts. A strong password is between 8-20 characters long. Features at least one uppercase, special characters (ex: @,!,&)

2) Don’t post confidential information online. Take a quick pause before you post personal information online, especially to social networks. Be paranoid, and protect your data like anyone could be watching. Remember, once it's posted online, it exists forever.

3) Watch out for phishing scams
Phishing scams- an online attempt used by cyber attackers to gain confidential information and/or money.

a) Phishing scams to be aware of at work:
Be vigilant when it comes to communications that claim to be from law enforcement agencies, such as the IRS, FBI or any other entity.
The most fraudulent attempts in the past years were created to mimic IRS communication, in an attempt to steal your financial information.

You should **know that government agencies don't initiate contact with taxpayers via email**, especially to request personal or financial information.

b) Phishing scams to be aware of at home:
Social media phishing Beware of sites created that look similar to Facebook, Linkedin, etc. They attempt to use the look-alike sites to steal login information. If they ask you to reset your password, use your web browser and manually enter the social media site that is requesting a password reset and use your account settings to manually do so (if at all).

If you receive a suspicious email on your CFPB device that you think may be a phishing scam, report it to our CFPB Cyber SOC team (b) (6)

At home and on your personal devices, suspicious email can be reported to CISA via
- https://www.us-cert.gov/report-phishing.

For more Cybersecurity tips, check out our Tip of the Week wiki here.