SITSD NEWSBYTES

March 30, 2020

COVID-19 Cyber Awareness

The Department of Administration – State Information Technology Services Division (SITSD) reminds everyone to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19).

Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes.

Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

Please remain vigilant and take the following precautions.

- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

Please read below on more information to protect yourself and your organization against these scams.

Coronavirus: Scammers follow the headlines

Scammers are ***taking advantage of fears*** surrounding the Coronavirus. They're setting up ***websites to sell bogus products, and using fake emails, texts, and social media posts*** as a ruse to take your money and get your personal information.

The ***emails and posts may be promoting awareness and prevention tips, and fake information about cases in your neighborhood***. They also may be asking you to donate to victims, offering advice on unproven treatments, or contain malicious email attachments.

Here are some tips to help you keep the scammers at bay:

Don't click on links from sources you don't know

It could download a virus onto your computer or device. Make sure the anti-malware and ***anti-virus software on your computer is up to date.***

Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying that have information about the virus

For the most up-to-date information about the Coronavirus, visit https://covid19.mt.gov/ .

Fake emails, texts and phishing

Scammers use ***fake emails or texts to get you to share valuable personal information*** like account numbers, Social Security numbers, or your login IDs and passwords. They use your information to steal your money, your identity, or both. They also use phishing emails to get access to your computer or network. ***If you click on a link***, they can install ransomware or other programs that can lock you out of your data. ***Scammers often use familiar company names or pretend to be someone you know***.

What to do: Protect your computer by keeping your ***software up to date and by using security software, your cell phone by setting software to update automatically, your accounts by using multi-factor authentication***, and your data by backing it up.

Robocalls

Scammers are using ***illegal robocalls*** to pitch everything from scam Coronavirus treatments to work-at-home schemes.

What to do: ***Hang up***. ***Don't press any numbers.*** The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robocalls, instead.

Ignore online offers for vaccinations

If you see ads touting prevention, treatment, or cure claims for the Coronavirus, ask yourself: if there's been a medical breakthrough, ***would you be hearing about it for the first time through an ad or sales pitch***?

Undelivered goods

Online sellers claim they have in-demand products, like cleaning, household, and health and medical supplies. You place an order, but you never get your shipment. Anyone can set up shop online under almost any name — including scammers.

What to do: Check out the seller by searching online for the person or company's name, phone number and email address, plus words like "review," "complaint" or "scam." If everything checks out, ***pay by credit card and keep a record of your transaction***. If you're concerned about the pricing of products in your area, contact your state consumer protection officials. For a complete list of state Attorneys General, visit naag.org.

Misinformation and rumors

Scammers, and sometimes well-meaning people, share information that hasn't been verified.

What to do: Before you pass on any messages, and certainly before you pay someone or share your personal information, do some fact checking by contacting trusted sources. For information related to the Coronavirus, visit What the U.S. Government is Doing. There you'll find links to federal, state and local government agencies.

What is a social engineering attack?

In a social engineering attack, an ***attacker uses human interaction (social skills) to obtain or compromise*** information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a ***form of social engineering***. Phishing attacks ***use email or malicious websites*** to solicit personal information by ***posing*** as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

What is a vishing attack?

Vishing is the social engineering approach that ***leverages voice communication***. This technique can be combined with other ***forms of social engineering that entice a victim to call a certain number and divulge sensitive information.*** Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services. Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor.

What is a smishing attack?

Smishing is a form of social engineering that ***exploits SMS, or text, messages***. Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

What are common indicators of phishing attempts?

Spoofed hyperlinks and websites

If you ***hover your cursor over any links*** in the body of the email, and the ***links do not match the text that appears when hovering over them, the link may be spoofed***. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

Suspicious attachments

An unsolicited email ***requesting a user download and open an attachment*** is a common delivery mechanism for malware. A cybercriminal ***may use a false sense of urgency or importance*** to help persuade a user to download or open an attachment without examining it first.

Suspicious sender's address

The sender's address may imitate a legitimate business. Cybercriminals ***often use an email address that closely resembles*** one from a reputable company by altering or omitting a few characters.

Generic greetings and signature

Both a ***generic greeting***—such as “Dear Valued Customer” or “Sir/Ma’am”—and a ***lack of contact information in the signature block*** are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

Spelling and layout

Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. ***Reputable institutions have dedicated personnel that produce***, verify, and proofread customer correspondence.

How do you avoid being a victim?

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claim to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not ***provide personal information or information about your organization***, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not ***reveal personal or financial information in email, and do not respond to email solicitations for this information.*** This includes following links sent in email.

Don't send sensitive information over the internet before checking a website's security.

Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with ***"https"—an indication that sites are secure—rather than "http.”***

Look for ***a closed padlock icon***—a sign your information will be encrypted.

Ensure your ***anti-virus software has been updated*** and set to auto update

Ensure your workstation/smartphone has the ***latest security patches applied***.

What do you do if you think you are a victim?

If you believe you might have revealed sensitive information about your organization, ***report it to the appropriate people within the organization. Your IT ServiceDesk*** should be notified as soon as possible. Ask your supervisor If you do not know who to contact to ensure you and your fellow staff know who to contact.

Ways Teleworkers Can Improve Their Personal Cyber Defenses

The COVID-19 (coronavirus) pandemic is prompting more companies to allow their employees to work from home or telecommute. But, ***home IT devices are still subject to many of the same threats as on-site business devices***. Unsecured off-site routers, modems, and other network devices can cause big headaches for employers. "***Poorly configured home devices can negatively affect entire organizations***," said Curtis Dukes, CIS Executive Vice President of Security Best Practices & Automation Group. "They can be attacked from any device on the internet, and they are also vulnerable to unauthorized access from neighbors and passersby."

Here are some suggestions teleworkers can implement now to improve their cybersecurity:

Update/Patch your home devices

(Laptops, workstations, Smartphone). Use automatic updates where possible.

Windows 10

Windows 10 offers you the choice of when and how to get the latest updates to keep your device running smoothly and securely. To manage your options and see available updates, select Check for Windows updates. Or select the Start Windows logo Start button button, and then go to Settings Gear-shaped Settings icon > Update & Security Circular arrows Sync icon > Windows Update Circular arrows Sync icon.

If any updates are available, click the Update Now button to install them. Or click "More info" to see details about each update and select specific updates to install.

Apple/Mac

https://support.apple.com/en-us/HT201541

Choose System Preferences from the Apple menu, then click Software Update to check for updates.

iPhone/iPAD

https://support.apple.com/en-us/HT204204

Android Devices:

https://support.google.com/android/answer/7680439?hl=en

Practice smart password management and enable two-factor authentication (2FA). This includes accessing the administrative router/modem, Internet Service Provider (ISP) web portal, or a mobile app used for home network management. Anyone with access to these platforms can also access sensitive information traversing the home network and modify critical security settings within the network.

Enable automatic updates for all routers and modems. Software updates are extremely important as new security flaws are constantly discovered. Simply installing

updates from the device manufacturer mitigates many of these problems. This is best accomplished by enabling “auto-update” on the device’s administration page.

Turn off WPS and UPnP. Wireless Protected Setup (WPS) was initially designed as a user-friendly method for new devices to connect to a WiFi network. Unfortunately, it’s been found to allow attackers to connect to WiFi networks without permission. Universal Plug and Play (UPnP) is a network protocol suite that allows devices on a network to easily communicate but has been found to contain numerous and severe security flaws. Getting these two settings correct can have a large positive impact on home network security.

Turn on WPA2 or WPA3. Old and ineffective types of cryptography plague older network devices. Ensuring strong forms of cryptography are in use within home networks can thwart others from viewing sensitive information without authorization. At a minimum, configure WPA2 for home use.

Configure the router/modem firewall. Firewalls help prevent malicious network traffic attempting to enter a network from reaching specific devices. Firewalls generally come built-in to most home routers, but they must be properly enabled.

Change default passwords on your home router.

Enable anti-virus (like Windows Defender) on your computers. Setting it to auto-update every day. Don’t use computers for state work that do not have an anti-virus program running.

Only use VPN on State-owned computers to connect to the State network.

Do not let family members use your state-owned devices.

The “report phish” button is not in webmail. Notify your IT help desk if you suspect a phishing email. Do not forward the suspected phishing email to anyone.

Protect state-owned equipment. Don’t leave laptops in cars or unattended. Report lost or stolen state-owned equipment to your IT help desk immediately.

Be cautious of calls from “IT” asking you to give information or perform actions on your computers. Verify the caller is from your IT help desk.

Take care in storing, handling, and disposing of documents containing sensitive information. Don’t throw documents containing sensitive information away in your home trash unless you can shred it. Contact your agency information security officer for guidance on disposing of sensitive information at home.

Sources for this article

Center for Internet Security - Five Ways Teleworkers Can Improve Their Cyber Defenses

CISA - CISA Information & Updates on COVID-19

FTC - Coronavirus: Scammers follow the headlines; FTC: Coronavirus scams, Part 2

US-Cert - Avoiding Social Engineering and Phishing Attacks, Using Caution with Email Attachments