Judicial Council Information Technology

Technology Advisory and Best Practices for Security

May 15, 2020

Background

With the Coronavirus (COVID-19) health emergency, organizations are seeing an increase in phishing, scams, attempted security breaches, and identity theft. This bulletin provides tips related to security - including browsing securely / online privacy, password protection, securing your home network, as well as other topics. Recently, a joint alert was issued from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC). Remember, no one is immune to cyber risk, but by being cybersmart you can minimize your chances of an incident.

Phishing and Scams

Unfortunately, natural disasters and global health scares like the Coronavirus outbreak invite another opportunity to scam. Websites selling bogus products or fake emails, texts, and social media posts are examples of ways malicious people use to take your money and get your personal information.

Red flags to watch for in Emails

- Content: A strong sense of urgency rushing you into making a mistake.
- To: Generic greetings rather than using your name or title.
- From: Personal or non-business email address, such as @gmail.com or @hotmail.com.
- Hyperlink: Hover over hyperlink in message to verify destination.
- Attachments: Unexpected attachment or one that makes no sense.

Tips to avoid Scams

- Never click on links from sources you don't know.
- Make sure the antivirus software on your computer is up to date.
- Never give out personal or private information.
- Be wary of emails claiming to be from the Centers for Disease Control and Prevention (CDC), the World Health Organization (WHO), or experts saying that have information about the virus. For the most up-to-date information about the Coronavirus, visit the official website for the CDC and the WHO
- Don't click or call listed phone numbers that are included in pop-up ads.

Browse Securely / Online Privacy

The Internet touches almost all aspects of our daily lives. We can shop, bank, connect with family and friends, and handle our medical records all online. These activities require you to provide personally identifiable information (PII) such as your name, date of birth, account numbers, passwords, and location information.

Making certain your computer's antivirus software is up-to-date is critical. In Windows 10, updates can be checked and manually updated in six steps: 1) Type Settings" in the Windows search bar, 2) Select Update & Security, 3) Select Windows Security, 4) Select Virus and Threat Protection, 5) Select Virus and Protection updates, and 6) Check for Updates.

Finally, being alert for browser warnings (leave the site), checking for encryption (padlock of https next to address) to know the information is protected in transit, and making certain your browsers and plugins always have the latest patches and updates will help you browse securely.

Tips to Increase your Privacy

- **Increase your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.
- **Keep your software updated to the latest version available.** Maintain your security settings to keep your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates if you can and protect your devices with anti-virus software.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Consider disabling location services that allow anyone to see where you are—and where you aren't—at any given time.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Public Wi-Fi hotspots** Avoid sensitive activities. If you must use a public WIFI hotspots, ensure that you are positioned so that no one else can see your Active Directory credentials or authentication code being entered on to the screen. The VPN software on your laptop protects your remote connection. Your personal hotspot is often a safer alternative to free Wi-Fi.

- **Stay protected while connected.** Only use sites that begin with "https://" when online shopping or banking.

Strong Passwords and Passphrases

Creating a strong password is an essential step to protecting yourself online. Using long and complex passwords is one of the easiest ways to defend yourself from cybercrime. (Unfortunately, many of us don't because we are afraid of forgetting it.)

Tips to Secure your Password

Creating a strong password is easier than you think. Follow these simple tips:

- **Use a long passphrase.** Consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.
- **Don't make passwords easy to guess.** Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.
- **Avoid using common words in your password.** Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L."
- **Get creative.** Use phonetic replacements, such as "PH" instead of "F". Or make deliberate, but obvious misspellings, such as "enjin" instead of "engine."
- **Keep your passwords on the down-low.** Don't tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen. A best practice is to not keep a written record of passwords.
- **Unique account, unique password.** Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. It's important to mix things up—find easy-to- remember ways to customize your standard password for different sites.

Secure Your Home Wireless (Wi-Fi) Network

Securing your home Wi-Fi is important for your personal use, as well as when you are working remotely.

Tips for Securing your Network

- Change the default wireless router admin password to a strong passphrase of 20 characters or more.
- The password you create to allow people access to your wireless network (sometimes called the network security key) should be different from the admin password and should be at least 16 characters long. Users will only need to enter this password once and it will be remembered on their device.
- Ensure your personal or ISP-provided wireless router is using Wi-Fi Protected Access 2 (WPA2), if available.
- Disable the ability to perform remote administration.
- Contact your Internet Service Provider or router documentation for assistance.

Other Resources

National Cyber Security Alliance: https://staysafeonline.org/ncsam/about-ncsam/
Huge collection of tip sheets, videos, and articles on cyber security topics many of which are directed more towards IT and organizational leadership.

Department of Homeland Security: https://www.cisa.gov/stopthinkconnect-toolkit
This website includes tip sheets on twenty different cyber security topics

National Initiative of Cybersecurity Careers and Studies: https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019
In depth tip sheets on thirteen topics including phishing and scams, browsing securely, password protection, online privacy, and securing your home network.

Federal Trade Commission: https://www.consumer.ftc.gov/features/scam-alerts
Updated list and descriptions of online scams.