IT Annual Security Bulletin

CTC Information Technology Division

FALL 2020

National Cyber Security Awareness Month—Do Your Part, Be Cyber Smart!

Not everyone has good intentions. There are bad actors around the world that use the internet for cybercrime (any crime which is committed electronically), which can include theft and fraud. Most cybercrime begins with some sort of malware attack, and your personal information is at risk if a cybercriminal gains access to your computer or devices. Technological security measures can only protect you so much – YOU are your best defense. By knowing more about the threats that are out there, you can better protect yourself and your information. Such cybercrime include the following:

Malware Attacks – software intended to damage, disable, or give someone unauthorized access to your computer or other internet-connected device

Ransomware – malware designed to make data or hardware inaccessible to the victim until a ransom is paid

Physical Cyber Attacks – Anything connected to the internet is potentially vulnerable. Physical cyber attacks use hardware, external storage devices, or other physical attack vectors to infect, damage, or otherwise compromise digital systems

Social Engineering – Cybercriminals can take advantage of you by using information commonly available through social media platforms, location sharing, and in-person conversations

Phishing – Fake messages from a seemingly trusted or reputable source designed to convince you to reveal information, give unauthorized access to a system, click on a link, and/or commit to a financial transaction

Swatting – An attack centered around location sharing in which bad actors call the police claiming the victim has committed a crime, e.g. bomb threat, armed intruder, violent incident. These attacks can have physical and immediate consequences and arrest and serious injury can result

Other Avenues of Attack – Your network can be used to attack someone else. Any device that stores information or is connected to the internet (smart devices, mobile phone, thermostat, vehicles, printers, medical equipment) can be a vulnerability.

How can you protect yourself online?

- **Update** – The best defense against viruses and other online threats is to keep your devices, security software and web browsers updated with the latest patches.
- **Click Aware** – Be aware of email and online advertising links. Click baiting is a common way criminals gain access to your computer. Remember, if it sounds too good to be true, it probably is.
- **Delete** – When in doubt, throw it out. If a link, email, tweet, post, online ad looks suspicious, even if you know the source, it is best to delete, or if appropriate, mark it as junk mail.

5 Ways to be Cyber Secure at Work

Cybercriminals often rely on human error (employees failing to install software patches or clicking on malicious links) to gain access to systems. Cybersecurity requires the vigilance of everyone to keep data safe and secure.

1. Treat business information as personal information (any information that can be used to identify your or your accounts). Examples include your name, address, phone number, usernames and passwords, pictures, birthday, and social security number.
2. Don't make passwords easy to guess – Employees can do so by using a long passphrase (news headline, title of the last book you read). Don't make passwords easy to guess (don't include personal information (your name, pet's name). Avoid using common words in your passwords (substitute letters with numbers and punctuation marks or symbols). Get creative (use phonetic replacements, such as "PH" instead of "F"). Don't tell anyone your passwords, and watch for attackers trying to trick you into revealing your passwords through email or calls. Have a unique password for every account. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you;. Use a password manager to store all of your passwords.
3. Keep your software updated to the latest version possible.
4. Social media is part of the fraud toolset – Cybercriminals can gather information about you, your family, and your work through online searches and scanning your organization's social media sites. Avoid oversharing on social media and **NEVER** conduct official business, exchange payment, or share PII (Personally Identifiable Information) on social media platforms.
5. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual webpages, do not click on unknown links, and deleted suspicious messages immediately.

Identity Theft and Internet Scams

Did You Know?

- The average cost of a data breach for a US company in 2019 was $8.19 million?
- 7-10% of the US population are victims of identity fraud each year, and 21% of those experience multiple incidents of fraud.
- 70% of Americans feel that their personal information is less secure now than it was five years ago.
- 72% of Americans believe that most of what they're doing online is being tracked by advertisers, technology firms, and other companies.
- 52% of Americans say they have decided not to use a product or service because they were worried about how much personal information was being collected about them.

Remember to review HR policies 294 & 295 on Computer Security and Computer Usage!

Current Internet Scams

- COVID-19 Scams take the form of emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes.
- Imposter Scams occur when you receive an email or call from a person claiming to be a government official, family member, or friend requesting personal or financial information.
- COVID-19 Economic Payment Scam target Americans' stimulus payments.

Protect Yourself from Online Fraud

Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar – this signifies a secure connection.

- When you find yourself out in the great "wild Wi-Fi West", avoid free Internet access with no encryption.
- If you do use an unsecured public access point, practice good internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.
- Don't reveal personally identifiable information (PII) (e.g., bank account number, SSN, or birthdate) to unknown sources.
- Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from an email.

Telecommuting Safe Practices

With many institutions turning to telecommuting/teleworking this year, it's vital that employees keep their devices, home network, and all work-related information secure and up-to-date while working from home. The following tips can be used to strengthen the security of your home office.

- **Keep everything updated.** Keep your operating system (e.g., Windows), software programs/apps, anti-virus program, and browser updated. Don't put off a patch or update that is currently available. If possible, select to allow your software to update itself automatically as soon as there is an update ready.
- **Use only CTC IT approved collaboration tools.** Through the IT Division, users can use virtual meeting, instant messaging, and other collaboration software via Cisco (WebEx and Jabber) and Office 365 (Teams, Yammer, SharePoint, and Sway). Contact the IT Help Desk for access to or more information about these collaboration options.
- **Secure your wireless network.** Protect your home Wi-Fi network by enabling Wi-Fi Protected Access II (WPA2) or Wi-Fi Protected Access 3 (WPA3) on your Wi-Fi device/wireless router. (If you have the option, opt for WPA3.) These security features use certification and encryption to help protect your home network. Also, **ALWAYS** secure your wireless network with a strong password!
- **Avoid public Wi-Fi networks.** Assume that all public Wi-Fi networks are **NOT** secure. If you are working with confidential information, **NEVER** use a public network.
- **Use a virtual private network (VPN).** A VPN creates a private line that connects your personal device directly to another network. This is done to protect information that would otherwise be transmitted (and possibly extracted) across unsecure, public lines. The IT Division recommends Cisco AnyConnect, which is free, secure, and available through the IT Help Desk. You should **ALWAYS** connect to your work computer via a VPN, especially if you work with confidential or other sensitive information.
- **Follow CTC telecommuting and computer policies.** Comply with all HR policies and procedures while telecommuting. Specifically, telecommuters need to be most knowledgeable of HR Policies, 275, 294, and 295, located here.
- **If you need help or notice something suspicious, contact the IT Help Desk.** If you see unusual or suspicious activity on any device that you are using (*e.g.,* computer, mobile device, or home network) contact the IT Help Desk.
- **Protect your devices.** Password protect and lock your devices when they are not in use. Make use of personal identification number (PIN), fingerprint, multifactor authentication (also known as two-factor authentication, which requires two types of verification), or facial ID security features. Never leave your device in a vehicle. Make passwords and PINs hard to guess!
- **Protect CTC information. NEVER** store sensitive or confidential information on your personal device. Do **NOT** disclose confidential or sensitive data to unauthorized personnel, including friends and family.

Virtual Meeting Safe Practices

Many employees working from home have turned to using virtual collaboration tools to hold meetings, brainstorm together on projects, and keep in touch with other coworkers and managers. Meeting applications that have seen a lot of use this year include Zoom, Microsoft Teams, GoToMeeting, and Google Meet. However, employees making use of video conferencing still need to adhere to safe security practices in order to protect their content and virtual meetings from scammers and disrupters looking to hijack unsecure sessions. Employ as many of the following options as you can (options may differ, depending on the meeting application being used) to ensure a safer video conferencing environment:

Make meetings as private and secure as possible.

- Require the use of a strong passcode, pin, or password to enter a meeting. Do **NOT** reuse the same access codes, pins, or passwords. Provide the pin or password to attendees via a separate email or by phone, and remind attendees to not share the access code.
- Do not allow attendees to join a meeting before the host is present. Control the admittance of guests by enabling a waiting room.
- Prevent unauthorized access by locking the meeting after all participants have joined.
- Double-check the participant list against the invited attendees present, or have participants identify themselves as they join the meeting.
- Set appropriate attendee privileges/permissions as soon as possible.
- With reoccurring meetings, always check to ensure one-time guests are not included in on subsequent meetings.
- Avoid adding your meeting to any public calendars or social media posts.
- Be wary of unusual web meeting requests. If something looks out of place, call the host to verify the meeting request or contact the IT Help Desk.

Be aware of what is said, shared, and saved/stored.

- Remove any documents or notes that may be viewed on your desk before you start a meeting.
- Be aware that information (typed, spoken, or exchanged via shared documents) may be stored indefinitely within the application or another user's computer. Information can also be taken/stolen by outside sources/individuals if an unsecure video application is being used.
- **NEVER** share confidential information through a public or unapproved meeting application. (If you are unsure of what to use, ask the IT Help Desk.) Likewise, never list personal information (*e.g.,* location, phone number, or date of birth) on your profile.

Virtual Meeting Safe Practices Cont...

- Be aware that others may be recording the meeting. If confidential information is exchanged (through an approved meeting app), the recordings must be stored in a secure place.
- Share only the content you intend to share. If you need to share your screen during a meeting, close all unused windows and disable notifications to ensure that you do not share sensitive or confidential information. Hosts may want to disable screen sharing to prevent the accidental screen sharing.
- Be wary of shared links. If possible, hover over the link first to see where it goes.
- Turn off and/or cover your webcam when it is not in use.

RESOURCES AVAILABLE TO YOU

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. The list below outlines the government organizations that you can file a complaint with if you are a victim of cybercrime.

- FTC.gov: The FTC's free, one-stop resource, https://www.identitytheft.gov/ can help you report and recover from identity theft. Report fraud to the FTC at ftc.gov/OnGuardOnline or https://www.ftccomplaintassistant.gov.
- US-CERT.gov: Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov. Forward phishing emails or web-sites to US-CERT at phishing-report@us-cert.gov.
- IC3.gov: If you are a victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3) at http://www.IC3.gov.
- SSA.gov: If you believe someone is using your SSN, contact the Social Security Administration's fraud hotline at 1-800-269-027.

Remember to review HR policies 294 & 295 on Computer Security and Computer Usage!