This reference guide is a reminder and tool for you to use your day-to-day activities as we work together to build a culture of cyber security.

Definitions:

- **Breach:** An incident that results in the confirmed disclosure of data to an unauthorized party.
- **Encryption:** Encoding information, particularly document and customer data, to protect against unauthorized access.
- **Incident:** A security event that compromises the integrity, confidentiality, or availability of an information asset.
- **Insider Privilege and Misuse:** Any unapproved or malicious use of organizational resources. This is mainly insider-only misuse but also applies to outsiders (due to collusion).
- **Malware:** A general term used for software or computer code that is designed to disrupt computer systems and access information without permission. An example of malware is an exploit script (virus) that can replicate itself and spread to other computers in a network.
- **Miscellaneous Error:** Incidents in which unintentional actions directly compromised an attribute of a security asset.
- **Phishing:** A form of social engineering in which a message, typically an e-mail, contains a malicious attachment or link sent to a recipient with the intent of using fear or urgency to trick the recipient into clicking on the attachment or link.
- **Physical Theft and Loss:** Any incident where an information asset went missing, whether through misplacement or malice.
- **Ransomware:** Malicious software designed to either lock a victim's screen, encrypt their files, or destroy them unless a ransom is paid.
- **Web Application Attacks:** Any incident in which a web application was used as a vector of attack allowing a hacker access to the victim's computer.

Wire Fraud Prevention Tips:

- Implement call-back procedures utilizing a known, safe telephone number to confirm any instruction received through e-mail.
- Incoming telephone calls are not a substitute for proper identification due to the known risk of call spoofing.
- Closing professionals should confirm direct contact with the funds' recipient whenever possible. Funds have been lost when a closer relies on a call-back made to counsel for a recipient, but the confirming contact between the recipient and his/her counsel was via compromised e-mail.
- Many settlement professionals now require in-person, wet signature disbursement instructions from parties who have presented valid identification.

- Upon any indication that funds have or might have been misdirected, settlement professionals should initiate immediate, direct, outgoing contact with both the wiring and receiving banks. Never rely on an incoming call to confirm the contact.
- Safeguard your account number and verify account names.
- Be alert to e-mail spoofing red flags (poor spelling, grammar) or a change in payment.

Password Creation Tips:

- Change your passwords regularly. Make them complex and avoid using personal information within them.
- Don't use simple or easy to hack passwords like 'password', '123456', or 'abcdefg'.
- Create passwords using phrases or statements. Don't use easy to guess phrases like 'haveaniceday'.
- Protect your passwords! Make them long and complex. Never reveal them to anyone and use multi-factor authentication (also called two-factor authentication) wherever possible. Also, use different passwords for personal and work-related accounts.
- Don't create short passwords. Develop long passwords of 10 characters or more.
- Use special characters, numbers, and letters together in your password (for example: **!Lov3MyPi@n0).**

- Never write your passwords down but password phrases can be (be creative).
- Consider using a password manager if you work with multiple passwords.

E-Mail Protection Tips:

- Scrutinize e-mail content and be alert to anything suspicious.
- Carefully review the sender's e-mail address from unknown senders.
- Routinely maintain and update anti-virus and malware prevention software.
- Periodically check your e-mail configuration to ensure automatic forwarding has not been enabled without your knowledge. A quick internet search will show how to configure forwarding for most major e-mail providers.
- Enable two-factor authentication for account access. A quick internet search will demonstrate how to set this up for most major e-mail providers.
- Never trust phone numbers sent in e-mails unless they've been verified as legitimate.
- Always think twice before clicking on links or opening attachments. It only takes that extra split second to realize that you might be tricked.
- Before you click, hover your cursor over the sender's e-mail address along with any URLs in the message to verify they are legitimate.

Home Office Security:

- Install a Virtual Private Network (VPN) at home.
- Activate your home office operating system (Windows 7x – 10) firewall feature.
- Add a WiFi Router to your home office to beef up security for all home computers, phones and tablets. Create a strong WiFi password.
- For computer or laptop webcams, invest in a privacy shutter for your webcams.
- Consider home security upgrades such as security cameras and security systems which are remotely monitored at all times via a tablet or smartphone app.

Zoom Meeting Security Tips:

- Always use a meeting password. Passwords should be turned on for anything that isn't a public event.
- Keep passwords safe! Zoom sends meeting passwords out to all invitees when invitations are sent. If you're worried that someone unwanted may get the password, create the meeting without one, then update the meeting to add a password and send it out to invitees in a separate e-mail.
- Use Zoom's waiting room feature. When you set up the waiting room for a Zoom meeting, users that connect are put in a queue that the meeting host must approve them from. If you don't recognize someone in the waiting room, don't let them in.
- Mute audio and disable video for meeting attendees. Disabling video for everyone but the host will prevent any obscene content from being displayed on camera by attendees. This can be toggled off during the meeting. If anyone other than the host wishes to speak, request that the attendee use the chat feature to request speaking time, and then mute the person once they're finished.
- Turn off screen sharing for everyone but the meeting host or assistant host. Zoom bombers need to be able to visually take over a meeting to be effective and preventing anyone from sharing their screen aside from the meeting host stops them from being able to go on the attack.

Healthy Habits:

- Limit the personal information you store on any website.
- Implement anti-virus software, malware protection, and firewalls in your systems.
- Never open e-mail attachments or links unless you first verify they're from a trusted source.
- Never insert an unknown USB flash drive into your computer.
- Never leave your laptop unattended. If you leave it in your car, lock it in the trunk. For trucks, conceal it out of sight and never leave your laptop in your vehicle overnight.
- Never overreact to a fear-driven e-mail. If the e-mail generates fear, steer clear!

- Always verify requests for private information (yours or anyone's), even if the request seems to come from someone you know—fraudsters know how to fake an identity.
- Protect your stuff! Lock it up or take it with you before you leave, even if you'll only be away for a second and password protect all your devices.
- Keep your computer clean! Keep your devices, apps, browsers, and anti-virus/anti-malware software patched and up to date. Automate software updates and restart your devices periodically to ensure updates are fully installed. Find out what you need to do, if anything, for company devices managed for you.
- Back up your critical files. Store backups in a physically separate location from the originals and test them periodically.
- Delete sensitive information when you are done with it. Better yet, don't store it in the first place if you don't need to.
- If you have an encounter that you deem suspicious, report it!

Other sources:

The following links are available to review cyber security statistics and topics used during the training.

- **Accenture - 2019 Cyber Security Report**
- **Acronis - 2019 Cyber Security Report**
- **ALTA Wire Fraud Prevention - https://stopwirefraud.org**
- **CSO Online© - Top cybersecurity fact, figures, and statistics for 2019**
- **Cybercrime Magazine - Reports, Trends, and Information**
- **Digital Shadows - Reports, Trends, and Analysis**
- **Experian$_{tm}$ - 2020 Forecast Report**
- **ICSPA - Cyber Security Reports, Trends and Strategies**
- **Kensington - Impacts of Cybercrime**
- **Malwarebytes - Analyst Reports**
- **McAfee© - McAfee Labs Threat Report**
- **Phislabs© - 2019 Phishing Trends and Intelligence Report**

- **Ponemon© - 2019 Cost of a Data Breach Study: Global Overview**
- **Symantec© - Security Center, Reports, and Bulletins**
- **Verizon DBIR Report - https://enterprise.verizon.com/resources/reports/dbir/**

Law Enforcement Sources:

The following links are available to report cyberfraud or suspicious activities:

- **Internet Crime Complaint Center (IC3)**
- **F.B.I. 2019 Internet Crime Report**
- **Online Safety (USA.gov)**
- **The United States Department of Justice (Cybercrime Reporting)**