Cyber Security Literacy

Murray E. Jennex, Ph.D., P.E., CISSP, CSSLP, PMP
Professor, MIS, San Diego State University

Our online world is useful for conducting financial transactions at any time from any place. However, this flexibility has a cost with respect to new risks and threats that many of us are not prepared to face. These risks come in the form of social engineering, malware and browser attacks, physical security issues, and direct hacking attacks. Social engineering are attacks that attempt to get you to disclose information that helps attackers get into your accounts or to download malware that attackers can use to attack. Malware is software that is used by attackers to gather data/information or to conduct actual attacks. Malware varies from keyloggers which record all your keystrokes and then sends them to the attacker to software that allows an attacker to use your computer when they want. Malware is downloaded onto your devices either by getting the user to download infected attachments or to run infected executable files such as webpages and applications. Direct hacker attacks come from open public networks. Fortunately, there are many things that users can do to mitigate and minimize these risks. These best practices are listed below:

Best Practices and Behaviors with Laptops/Desktops:

1. If at all possible fun browse on a computer different than the computer with which you do banking. Most malware from browsers is found on online gaming, social media, and other fun and interesting websites. If you like to game or explore the web it is best to not use the device that you conduct your financial transactions on to do these activities.
2. If you do download a virus or malware do not use that device to conduct financial transactions until after it has been reformatted (best practice is to reformat up to three times before reinstalling software) and your software reinstalled from the original disks/source. Malware and viruses tend to install themselves into the operating system making them difficult to remove. While there are methods of removing malware and viruses many/most organizations do not trust them and will not trust a device until it has been reformatted and software reinstalled from original disks/sources.
3. Maintain physical security meaning keep the device in your possession and require a login to use the device. Do not lend it out, do not leave it in publicly accessible locations. The easiest way to install malware or viruses, to crack passwords, or to download data/information is to gain physical access to the device. An attacker can usually gain access to the use of the device by using an extraneous storage device like a self- booting USB drive to bypass login requirements and then use hacking tools such as John the Ripper or Loftcrack to crack passwords for accessing your accounts.
4. Don't plug unknown USB or flash drives into your device. Plugging in a drive results in the device running the installation software on the drive. This is dangerous if the drive was setup to install malware on the host device. This is a known attack method that resulted in the Department of Defense banning all USB drives for a period of time in 2008 when a contaminated drive was used to install spyware on defense computers. Many organizations no longer use USB drives and some have gone so far as to plug USB ports with glue to prevent them from being used.

Best Practices and Behaviors with Mobile Devices

1. Install a firewall. Phones and pads are just like computers and need to be protected. While iPhones and iPads are safer from attack through their applications (Apple verifies application providers before letting them into the Apple Store), browsing on a mobile device is just as dangerous and susceptible to malware as browsing is on a laptop or desktop. Most firewall vendors provide mobile versions of their products and these should be used.

2. Be careful of synchronizing the mobile device to your laptop/desktop. Email and browsing can be used to install malware and that malware can be passed to your laptop/desktop when you synchronize to the mobile device.
3. Password protect your mobile device just like you would your laptop/desktop. Attackers can easily gain access to your mobile memory simply by picking up the device unless it is password protected.
4. Install a tracking app on your mobile device. Mobile devices are easily lost or stolen and the tracking app can be used to locate the missing device. Also, these apps can be used to delete device memory and lockout attackers should the device be stolen.
5. Backup your mobile memory just like you should backup your important files.
6. Just like your laptop/desktop maintain physical security. It is always easier to attack a device if the attacker has it in their physical possession.
7. Do not store any data/picture/file that is potentially embarrassing on the mobile device. They have been known to be copied by service personnel when buying a new device; and it has been demonstrated many times that it is easy to hack into and copy these data/pictures/files.

Best Practices and Behaviors When Using Free Wifi

1. Do not perform any secure or financial transaction on free wifi. Public access to free wifi makes it easy for attackers to capture transaction packets off the free wifi network using packet sniffers. It is best not to perform any transaction that involves a login and password and/or account numbers.
2. Ensure you have no shared folders when using free public wifi as anyone on the network can access shared folders.
3. Do not set your device up to automatically log on to a free public wifi network. Logging into a free public wifi network must be a desired decision by the user that is made when the risks are understood.
4. Be aware of shoulder surfing. Someone watching you closely may be observing your log in process.

Best Practices and Behaviors When Using the Cloud

1. Know who owns data/information/knowledge stored on the cloud. Some cloud providers claim ownership of all data/information/knowledge stored on their cloud (for example Instagram). If this is the case with your cloud provider do not store intellectual property or proprietary data/information/knowledge on that cloud. Be particularly aware of storing documents.
2. Be aware of using collaborative documents on the cloud in particular with inter-organizational collaboration as ownership of these documents may be an issue. This is especially true for intellectual property documents such as patents where use rights may be very different than expected.
3. Be careful synchronizing cloud files with device files. Malware inserted into device files can be spread to the backup through synchronizing of files.
4. Know your Service Level Agreement, SLA. This document specifies terms of use for the cloud as well as expected level of availability, reliability, and security from the cloud provider. Not all clouds are equal. Some are very reliable and available and will protect your data/information/knowledge, others are not as good.

Best Practices and Behaviors When Using Email

1. Do not download/open attachments in an email unless the email sender is a trusted source and the email is in their character to send. The most common method of inserting malware/viruses into a device/laptop/desktop is to get the owner to do it by downloading and installing an attachment . Attackers are getting very good at making these emails seem legitimate. Spear phishing is a form

of attack where the attacker researches the victim and sends an email that they would likely accept as legitimate.

2. Do not open/click on links in an email unless the email sender is a trusted source and the email is in their character to send. The second most common method of inserting malware/viruses into a device/laptop/desktop is to get the owner to do it by running an executable file that will install the malware or virus. As stated earlier, attackers are getting very good at making these emails seem legitimate. Spear phishing is a form of attack where the attacker researches the victim and sends an email that they would likely accept as legitimate.
3. Never enter or send a password or log in information based on an email request. Asking customers to log in via an email is not an accepted business practice and in ALL cases is a phishing attack.
4. Scams, phishing, spear phishing is very common and you may get these attacks several times a day. If you do not know the sender or it is unsolicited email it is better to delete it then to take the chance of opening and responding. Taking any action on an email usually results in the attacker being able to determine that your email address is legitimate, meaning you will get even more email attacks.

General Best Practices and Behaviors

1. Auto update your device/laptop/desktop if possible. If not, update your device/laptop/desktop as soon as possible. Security updates acknowledge security flaws and fixes them. Attackers begin searching for non-updated devices/laptops/desktops as soon as the updates are released. Not updating creates a vulnerability in your device /laptop/desktop that has a known successful attack method making you easy prey.
2. Keep your malware and virus protection software up to date. This software runs off of a dictionary of known malware/virus definitions and is only effective if kept up to date.
3. Scan your device/laptop/desktop on a regular basis and after visiting other countries. Infections are more apt to happen when traveling due to increased use of public free wifi networks and other unknown networks. Do not perform financial transactions until you've scanned the device/laptop/desktop upon returning from a trip.
4. Change out electrical surge protectors on an annual basis as they wear out with continuous use.
5. Backup critical data/information/knowledge and practice recovering lost data/information/knowledge. Experience shows that backups that are not tested tend to not work.
6. Store backups in a safe location.