U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Some Cybersecurity Basics

Baiting

WHAT IS "BAITING?"

Baiting involves leaving a piece of portable storage media such as a CD, laptop or USB stick in an open location to tempt a victim into seeing what's on it. When the victim opens files opens on the media, executes a malware program that releases a virus or leads to personal and financial information being exposed to hackers. If the victim uses a network, the infection can spread throughout the network.

Because flash drives are rarely encrypted, the files on them are easily accessed. One study that looked at 50 USB drives found not one was encrypted, and none of the files on them were password protected.

Baiting is similar to phishing, but unlike other types of social engineering it promises an item or goods to entice victims. For example, baiters may offer free music or movie downloads if the victim shares personal information such as login data and passwords.

Baiting may also take place online, when cyber criminals post tempting offers or ads lead to malicious websites or get users to download malware-infected applications.

A 2016 report found that baiting is pretty successful. In one study 297 USB drives were dropped around the University of Illinois campus. Researchers verified that 45 percent were plugged into a device, but that 98 percent had been moved, so the number plugged in could have been much higher. The very first one dropped was found to be in use just six minutes later. In another study, 20 percent of 200 "finders" plugged in a drive found in public and opened files, clicked links or sent messages to an email address on the drive. Just 16 percent scanned the drive with antivirus software prior to use.

HOW DO I PROTECT MYSELF FROM BAITING?

Never plug an unknown piece of media into your computer. If you find a piece of media at your workplace, turn into your security officer. If you find it in public, it may be best to dispose of it.

The best way to protect yourself is to not open any files on media you find. But if you do, make sure your security software is up to date and scan all files before attempting to open them.

For more on baiting and other forms of social engineering, visit:

https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

Cookies

WHAT ARE COOKIES AND WHAT DO THEY DO?

A cookie is information a website saves to your computer using your web browser. A cookie allows sites to record your browsing activities –what pages and content you've looked at, when you visited each site, what you searched for, and whether you clicked on an advertisement. Data collected by cookies can be combined to create a profile of your online activities.

HOW CAN COOKIES BE USED MALICIOUSLY?

Cookies are a useful tool, but they come with a lot of potential for abuse. Not only will advertisers attempt to track your online activities, but poorly designed web applications inadvertently create security holes that malicious attackers can exploit to gain access to your account data. Since cookies are saved in plain text, and can be easily altered, cookies must never be used to store sensitive data. Poor cookie design can lead to exposed user information and financial loss.

WHAT CAN A USER DO TO STOP COOKIES FROM BEING USED MALICIOUSLY?

Web browser programs have different ways to let you delete cookies or limit the kinds of cookies that can be placed on your computer. When you choose your browser, you may want to consider which suits your privacy preferences best.

To check out the settings in a browser, use the "Help" tab or look under "Tools" for settings such as "Options" or "Privacy." From there, you may be able to delete cookies or control when they can be placed. Some browsers allow add-on software tools to block, delete or control cookies. And security software often includes options to make cookie control easier.

If you disable cookies entirely, you may limit your browsing experience. For example, you may need to enter information repeatedly, or you might not get personalized content or ads that are meaningful to you. However, most browsers' settings will allow you to block third-party cookies without also disabling first-party cookies.

Many browsers offer private browsing settings to keep your web activities hidden from other people who use the same computer. With private browsing turned on, your browser won't retain cookies, browsing history, search records or downloaded files. Privacy modes aren't uniform, though; it's a good idea to check your browser to see what types of data it stores. Although it won't keep cookies after the private browsing session ends, cookies used during the private browsing session can communicate information about your browsing behavior to third parties.

Geotagging

WHAT IS GEOTAGGING?

- Geo-tagging is adding geographic identification to photographs, videos, websites, and SMS messages. It's like tagging a precise map grid coordinate to everything you post on the Internet.
- Geo-tags may automatically be embedded in pictures taken with smartphones, but many people are unaware that those photos have been tagged before they post them online.
- Photos posted to photo sharing sites like Flickr may also be tagged with their locations.
- Posting photos tagged with an exact location allows others to track your exact location and correlate it with other information.

GEO-TAGGING PHOTOS

- Photos have used geo-tagging for quite some time. Some formats such as JPEG format allow geographic information to be embedded within the image that can be read by picture viewers.
- Owners should study their cameras' manuals to learn whether their devices automatically add geolocation metadata to pictures and understand how to turn off those functions.
- On photo sharing sites, people can tag a location on their photos, even if their camera does not. A simple search for "Afghanistan" on Flickr reveals thousands of location tagged photographs that have been uploaded.
- Soldiers deploy to areas all over the world. Some locations are public, others are classified. Soldiers should not upload geo-tagged photos. Publishing photos of classified locations can be detrimental to mission success, and in violation of the Uniform Code of Military Justice.

Juice Jacking

WHAT IS "JUICE JACKING"?

Juice jacking is a cyber attach in which a compromised USB charging station transfers malware to, or steals personal information from, a connected device.

Juice jacking is a cyber attack in which a compromised Universal Serial Bus (USB) charging station transfers malware to, or steals personal information from, a connected device. Juice jacking, also known as port jacking, is not limited to cell phones but any device capable of being charged via USB plug.

USB plugs are designed for two-way transfer of data. When a USB cable is connected between an electronic device and a charging station, there is a trusted relationship established. The connected device is receiving a charge while the charging station has access to the device's entire database, including sensitive data. Unless the charging station was compromised, charging stations are not concerned with what is on a person's device.

HOW DO I KNOW IF I'M A VICTIM OF JUICE JACKING?

Victims are often unaware that they have been "juice jacked", but there are some telltale signs that a device may be compromised. The device may:

- Consume more battery life than usual
- Operate at a slower speed
- Take longer to load
- Crash frequently due to abnormal data usage

HOW CAN I PROTECT MYSELF?

On many new devices, automatic two-way transfer of data is disabled. But if you really need to charge a device on the go, take some precautions:

Avoid using public USB charging stations

- Decline data transfer request
- Use two-factor authentication or biometric log-ins when available
- Carry a portable charger or battery pack
- Use electrical outlets with your own charging cable and wall plug-in charger
- Use a charge-only USB adaptor that allows your devices to be charged but does not transfer data
- Keep your software updated. Software updates are likely to have current security protection, patches and bug fixes. For example, many updated cellular phones now ask permission before allowing data to be transferred when they are plugged into an unknown station or device.

The bottom line: Be cautious where you charge your electronic device. Public charging stations at airports, hotels and restaurants are a prime target for cybercriminals to juice jack and collect your information or install malware to further criminal activity.

QR Codes

WHAT ARE QR CODES?

Originally developed in the mid-1990s for manufacturing and inventory control, QR codes most often appear as a small graphic that looks like randomly placed small black squares arranged in a borderless square (similar to the white square in the graphic above). But QR codes can be customized with different colors and different backgrounds.

When a QR code graphic is framed in the camera of a smartphone, the code can be read by the device and immediately trigger a response, such as opening a document or a web address.

WHY ARE QR CODES POTENTIALLY HAZARDOUS?

While QR codes make transactions fast and easy, cyber criminals and hackers can also misuse them for malicious activity or profit.According to cybersecurity experts and the Major Cybercrime Unit of the Army's Criminal Investigation Command, QR code fraud and theft are evolving and on the rise.

For example, QRs that have malicious code embedded in them can be placed in publicly accessible spaces, where curious passers-by scan them, only to be directed to websites that download damaging code on their devices.

The COVID-19 pandemic has also unwittingly aided the bad guys, because the codes' ability to provide a more hands-free transaction method has led to their greater use, to help prevent spread of the virus.

What are some things malicious QR codes can do?

Some of the nefarious things malicious codes can do include:

- Add unwanted and potentially dangerous contacts to a contact list
- Connect a device to a malicious network
- Send text messages to contacts in a user's address book
- Make calls to telephone numbers that impose charges on the user's phone
- Send payments to destinations where they cannot be recovered
- Compromise financial data and accounts

WHAT CAN I DO TO PROTECT MYSELF AGAINST MALICOIUS QR CODES?

In general, CID experts recommend the same kinds of vigilance and caution you would use to protect yourself from other online hazards:

- Be suspicious of unsolicited offers that seem too good to be true
- Don't open emails from unknown senders
- Ignore emails that ask you to provide identifying information such as usernames, passwords, dates of birth, etc.
- Do not access financial accounts by clicking links received in unexpected emails; use verified links instead

And they add some cautions specific to QR codes:

- Don't scan a randomly found QR code
- Be suspicious if, after scanning a QR code, you are asked for a password or login information

- Do not scan QR codes received in emails, unless you are certain they are legitimate
- Do not scan codes printed on a label that has been applied atop another QR code, unless you can verify its validity

Safely Disposing of Old Computers

WHY DO USERS NEED TO BE CONCERNED ABOUT DISPOSING OF OLD COMPUTERS?

Computers often hold personal and financial information, including:

- Passwords
- Account numbers
- License keys or registration numbers for software programs
- Addresses and phone numbers
- Medical and prescription information
- Tax returns
- Files created automatically by browsers and operating systems

Just deleting files or reformatting the hard drive will not remove this information. When you delete a file, the links to reconstruct the file disappear, but the bits and pieces of the deleted file stay on your computer until they're overwritten and they can be retrieved with a data recovery program. To remove data from a hard drive permanently, the hard drive needs to be wiped clean or destroyed.

WHAT CAN BE DONE?

Utility programs to wipe a hard drive are available online and in stores where computers are sold. These programs are generally inexpensive. Some are available on the internet for free.

These programs vary:

- Some erase the entire disk, while others allow you to select files or folders to erase.
- Some overwrite or wipe the hard drive many times, while others overwrite it only once.
  Consider using a program that overwrites or wipes the hard drive many times. Otherwise, the deleted information could be retrieved. Or remove the hard drive and physically destroy it.

Shoulder Surfing

WHAT IS "SHOULDER SURFING"?

Shoulder surfing is using direct observation, such as looking over someone's shoulder while they are using mobile computing devices or conducting transactions in public. Identity thieves may be watching or listening to get their personal information from people engaging in activities such as;

- Keying in passwords on their mobile devices or public-use computers (as in libraries or internet cafes)
- Filling out personal information on forms
- Entering a PIN code at an automated teller or point-of-sale machine
- Verbally confirming hotel, rental car, or credit card information on a cell phone

HOW DOES "SHOULDER SURFING" HAPPEN?

There are many ways eavesdroppers can nab personal information from unwitting victims. They may actually look over your shoulder, listen nearby, or shoot video with a cell phone as you enter your data or conduct a transaction. Shoulder surfing is particularly effective in public places where it is fairly easy to observe people in crowded, often chaotic, environments.

HOW DO I PROTECT MYSELF FROM "SHOULDER SURFING"?

There are several ways to minimize your risk:

- Be aware of your surroundings at all times
- Find a quiet spot at the outer fringes of a crowded area. A spot where you can sit or stand with your back to the wall is best
- Avoid engaging personal, business, or financial matters in public
- Never verbalize passwords or security codes
- Use a security screen or filter to obscure the visibility of your monitor