Phishing, Ransomware, and Other Cyber Threats

In our ever-increasingly connected world, we are all doing more on the internet. Whether it is shopping on Amazon, browsing the web, performing our banking, filling out forms, or whatever, we use the internet everyday for mundane tasks, and it is easy to forget that being that connected also puts us at risk. Every time we connect to the internet there is a chance that hackers, scammers or thieves will attempt to hack into our computers, steal our identity, pilfer our passwords, or perform any number of other nefarious deeds. While we put into place protocols to help keep us safe like firewalls, virus protection, stronger passwords, and more, our best defense is still knowledge and a critical mind. In this article we will talk about the latest scam circulating right now, but then we'll go into greater depth about other scams you should be aware of.

Recent Threats

One of the latest and most clever threats authorities are seeing right now is the use of malicious USB drives (sometimes called flash drives or thumb drives) to install malware onto a user's computer. The way this scam works is that a hacker will somehow get you a USB drive, which you then plug into your computer, and it will automatically install malware. This malware is usually either a trojan horse that opens a back door into your computer, allowing the hacker to access your computer and your personal files, or a key logger, which will capture all of your keystrokes (including usernames and passwords) which are then sent to the hacker allowing them to break into your accounts.

You might say, "If a hacker gave me a USB drive, I would never put it into my computer," but the scam is not usually as blatant as that. Hackers will use social engineering to entice you to plug the USB drive into your computer. For example, you may find a USB drive on the ground near your car while you are out shopping. Curiosity is a strong motivator, and many folks will plug that USB drive, which they found on the ground, into their computer to see what might be on it.

Another version of this is the Amazon or Best Buy scam. Hackers will mail what appears to be a large capacity USB drive and gift card to you through the US Mail. It all looks very official, and regardless of whether the recipient is enticed by the "free credit" on the gift card or the 256 GB USB drive (which is also likely mislabeled), they stick it into their computer which instantly becomes infected. In many cases, you as the user don't even have to run anything on the flash drive, it runs automatically when the drive is inserted. Don't be surprised to see this same type of scam using the branding from Walmart, Starbucks or other popular retailers. They key takeaway here is to never connect a USB drive to your computer if you do not know the person giving it to you!

Social Engineering

Social engineering, as it is called, happens in many forms, and it is not all computer based. You may have received a call from "Microsoft" telling you that your computer has a virus and asking you to walk through several steps to help remove it. This usually involves the fake "Microsoft" employee asking you to grant them access to your computer so that they can remove the virus. There are also scammers who will call you and tell you that your Amazon account or your bank account, or your credit card account has been hacked. In each case they will try to get you to grant them access to your account either by inviting them to connect to your computer or your account in question, or by asking you for your username and password, so they can log in directly. Don't fall for it… these companies will not call you and they certainly won't ask for your user credentials to log in to your accounts. If they really worked for these companies, they would already have access to your account!

The same can be said for calls you may receive from the Social Security Administration, Internal Revenue Service, or local law enforcement agencies. Most of these calls will have some flaw in the language, terminology, or grammar of their message which should raise a flag indicating to you that they are a scam. The calls are getting more convincing, though.

Ransomware

Ransomware is a type of malware that locks your computer, preventing you from gaining access to it. There is typically a countdown timer that provides a deadline after which your computer will be permanently locked or erased altogether. If this were to occur, you may lose cherished personal data such as photographs or videos, or critical business documents and data. This highlights the need for regular

and complete backups, so that you may recover from an attack such as this if you were to become infected. Ransomware can invade your computer innocently enough by opening an email attachment from someone you don't know, downloading software or PDF files from a questionable website, or even browsing to certain websites that may be known to distribute malware (your browser, in conjunction with your antivirus and firewall software, should warn you if trying to browse to a questionable site). We at the Archdiocese use an application called Trustwave to help keep you safe when you are at work or connected to our wifi via a mobile device.

Ransomware, or any type of malware for that matter, can be avoided by being a cautious and conscientious computer user. Malware distributors have become increasingly sophisticated, so you must be careful what you download and click on.

Other tips:

- Keep operating systems up to date. Ensure that anti-virus and anti-malware solutions are set to run regular scans and automatically update.
- Ensure that backups are done on a regular basis and recheck that they are completed.
- Ensure that the locations where backups are stored are not connected to the computers or networks they are backing up.
- In case you are attacked by ransomware, you should have a continuity plan set up in case your backups are compromised.

Keyloggers

Keyloggers are a legitimate form of software and can be used for many legal purposes such as parental control, business security, activity tracking, law enforcement, and civil disputes (think cheating spouses), they can also be built into malware that will capture and provide hackers with sensitive and/or private data that may be used to compromise your financial accounts and/or steal your identity.

Malicious programs that steal information via the keyboard do not pose a threat to the computer as a whole. However, they can pose a severe threat to users due to their ability to intercept passwords and other information entered by users via the keyboard. The result is that cyber criminals can get account numbers, PIN codes,

and passwords for electronic payment systems, email addresses, and user names for online accounts.

Summary

The key take-away is that we all need to be more thoughtful about how we interact with our computer and mobile devices. Every time we consider entering Personally Identifiable Information (PII) or passwords into a web page, email, text message or the like, you should consider who is asking for that information, and whether you trust them. Is this an action that you initiated (e.g. you calling tech support for assistance), or was the action initiated by a potential cybercriminal. As your parents always told you, "If it looks too good to be true, it probably is too good to be true." As always, if you have questions, we in the IT department at the Archdiocese of Denver are here to help. Feel free to call us if you have questions about a possible cyber threat or scam.