Computer and Internet Safety

The Internet and computing devices are a normal part of everyday life. We often use them without even thinking about it. The recent acknowledgement of the Meltdown and Spectre vulnerabilities brings security and safety concerns to light. The following is a general description of Malware and some guidelines to help protect your sensitive information.

History

Many years ago viruses were almost exclusively passes through altered programs that infected floppy disks. Anti-virus software would scan the disk when inserted into you computer and warn of any infection. Now the term Malware is more common and it is usually spread through email and malicious or compromised websites.

Malware

Malware generally has one of three purposes. Take over your computer and then use it to launch additional attacks. Encrypt your data and attempt to ransom it. Try and collect sensitive data like usernames, passwords, account numbers, etc. Malware can be stealthy and almost undetectable up through making your device unusable.

Meltdown and Spectre

These are different in that they exploit a vulnerability in the microprocessor. This vulnerability has existed for over 20 years but was only recently found and/or made public. However, the risk of Viruses and Malware has been around much longer.

Safety Tips, Do's and Don'ts

Do not open emails from someone you do not know and do not click on links in emails unless you know exactly what it is for.

Do not send usernames and passwords through email. Generally speaking, no one should ever ask you for a password.

Do not logon to applications when prompted through email. If you are sent a link to a website make sure it is actually the correct website. It is better to use your own bookmark or directly type in the URL. Even though it looks right in the email the URL the link takes you to could be different.

Do use two factor authentication whenever possible. Especially for sensitive accounts.

Do not save passwords in your Browser. If you device become compromised everyone one of those sites is also compromised.

Do use strong passwords and change them on a regular basis. Try to use different passwords and even usernames for different accounts. Again, especially for sensitive accounts.

Do keep security patches up-to-date on your devices. This includes cellphones and tablets as well.

Do use Virus/Malware detection software and keep it up-to-date.

Do not access sensitive information when using public or unsecure Wi-Fi. Example include transfering funds at the airport of logging into Infinite Campus when sitting at a McDonalds.

Informational Links

Internet Safety for Adults
http://safety.lovetoknow.com/Internet_Safety_Adult

How to Create a Strong Password (and Remember it)
https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

Meltdown and Spectre
https://meltdownattack.com/

AVG AntiVirus Free
https://www.avg.com/en-us/free-antivirus-download

Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites
https://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/

The Danger of Phishing
http://go.kaspersky.com/rs/kaspersky1/images/Dangers_Phishing_Avoid_Lure_Cybercrime_ebook.pdf