CYBER-SECURITY IN THE PRE K PROGRAM ENVIRONMENT

What is Cyber Security?

Cyber Security refers to the steps we take to make sure that all of our digital appliances are protected from any efforts to hack into them to make use of our devices for illicit purposes, or to collect data that might be used to steal our identities or extract payment from us, or attempt to remove money from our bank or other financial accounts.

Who are the main perpetrators of the attempts to hack our devices?

Unlike many years ago when most "hackers" were simply young individuals experimenting with their ability to break into computer systems, today's hackers are highly trained computer professionals who either work for criminal organizations, or work for nation state sponsored intelligence or military agencies that are opposed to democracy and America's involvement in world affairs, as well as members of home grown terrorist organizations in the United States.

What are the protection measures we typically use in Cyber Security?

First, we determine if our devices are capable of being connected to WIFI networks, Wired Networks, and/or the Internet.

Second, we determine whether we have enabled Connections to any of those networks on our devices. Devices not connected to a network and not using the Internet are typically not as hackable, but remember that even 4G and 5G channels can be hacked by the most sophisticated hackers in the world. They actually go after the hardware on the cell towers or the computers that manage the switching on those networks to gain access to our devices.

Third, we determine whether we have purchased or are using freely provided open source protection software on our devices and what features are part of the protection schemes for this software. Some free products only partially protect our devices. Most paid software has more feature protections than free version of the software. We should be using as many protection features that are available for the product.

Fourth, we determine if the main network connection devices are protected. These devices include our network server and switches, routers, and modems. These devices can be protected using specialized hardware and/or specialized network software that would be different from that which we use on our personal digital devices.

Fifth ,we determine if our passwords are strong (meaning that they have more than fifteen characters(including capital letter, numbers, and symbols) or a combination of five or more random words and that we make efforts to change passwords at least two to three times a year and never use the same password for multiple accounts.

Sixth, we determine if we are using two factor authentication on all accounts – meaning in addition to a password we are using some other form of authentication, email address, phone number, pin number, QR code, finger print, retinal scan, facial recognition, voice encoding, coded locking dongles, etc.

7. We determine if we have ever shared our secure passwords with anyone including members of our own family, or have ever asked our personal digital devices to save our passwords or allowed WEBsites we use to save our passwords. (These habits should be broken as soon as possible since they represent easy ways for others to access our devices).

8. Next we determine whether we have been using encrypted messaging and email, along with encrypted monetary transactions online, and whether those encryption methods use at least 128 key encryption. Just because a site seems to have the secure lock icon on the site doesn't mean it is actually secure. Remember there are lots of ways hackers can get into a network including WEBsite spoofing, which involves making what appears to be a legitimate WEBsite but is actually just a mock up of a real website that is being used to capture user ID data. Often hackers will collect company logos and other company identification information off of a legitimate WEBsite to use on the spoofing site.

9. We consider using secure VPN (Virtual Private Networks) services when working online with our digital devices. There are many VPN sites and services out there. You need to check reviews to see which are the most secure. You also need to realize that most of the free ones are not actually very secure, but most paid sites are. Still read the review information carefully. Hackers this year have attacked a lot of VPN services.

10. We make sure ot update all security products on a daily/weekly basis, or in accordance with the distribution of security updates provided by our hardware and software providers.

11. We use identity theft protection and account security protections provided by either third party services, or services from our primary account providers. Including notifications of unusual transactions.

12. We check regularly on our credit information and social security information to be sure it isn't being misused. Also check to make sure all 401K and Pension and

insurance policy information has not been hacked at least twice annually. Recently I experienced a retirement account hack in which my benefits were being paid to someone who was not on my account and whom I had no personal relationship.

13. Do not open emails from any party you do not know. Please note that all businesses and government agencies are not permitted to request personal information from you online and may only request this by sending you a certified letter. You may obviously submit personal information online, but be sure you are doing it on a trusted site only.

14. Do not click on email links to Word Documents or other Microsoft Office Files that have not been encrypted. Convert all documents to Plain Text and/or PDF files. Unfortunately Microsoft has a built in coding editor that allows hackers to embed malicious code into Microsoft Office products. Consider switching from HTML email delivery to plain text email delivery only. Hackers have a much more difficult time trying to break into plain text code and use it for malicious embedding than they do with HTML code and other Internet Based Coding tools. You won't see image information in Plain text emails unless you ask for it. One of the oldest hacking tricks is called steganography and is simply the ability to embed malicious code into pictures.

15. Do not click on WEB links to locations you are not familiar with. When visiting new WEBsites for the first time, try not to click on internal links until you have surveyed the site carefully. Hackers often find weaknesses in internal link pages that allow them to embed malicious code. Make sure that all WEBsite use the https:// protocol which is the secure hypertext transfer protocol.

16. Turn off your device camera when you do not need to use it. If you notice that the camera has been activated when you have turned off the camera, then you know your device has been hacked. Make sure to check on the camera being turned off when you are not using it at least once a day. Hackers can activate these including home security cameras without your knowledge and capture you working on your keyboard or your device screen, and capture images of your home if they can access your security camera system. If you have a home security camera system be sure to use two factor authentication to insure you devices are less vulnerable to hacking. You should also consider turning off your device microphone for the same reason when you are not using it.

17. Remember to choose Smart Home devices and appliances that can be secured with two factor authentication. This includes Smart TV's, Smart lighting, Smart Speakers, Smart Streaming devices, Smart thermostats, etc. The Internet of Things (IOT) is a vast array of computer controlled devices in many homes and businesses across this country. Unfortunately there are millions of these devices that are not secured in anyway and allow hackers into some of our most vulnerable systems, not only in our homes, but our

national electrical grid, our computer controlled cars and trucks, our water treatment facilities, and a host of other essential services.

18. Consider using at least two anti-malware products on each of your devices. No single malware software program is capable of stopping all malicious hacking or malicious software. The anti-malware product industry has to deal with upwards of thousands of new pieces of malicious software each week. They have to be able to detect this, find out how it works, and try to find a way to stop the code from executing. Even with the tens of thousands employees who work in this industry, working 24/7/365, they know there is no way any single product manufacturer is capable of handling the vast amount and variety of the cyber attacks that go on each day and each week.

19. No device or operating system is invulnerable to cyber security attacks. Some are less prone to these attacks than others. Currently two of the most secure operating systems in use are UNIX and LINUX. These products are based on a type of coding that does not lend itself easily to malicious coding. While Microsoft is gradually migrating a good bit of its product line to Linux, and Apple uses a modified version of UNIX neither Microsoft Windows nor the Mac OS or iOS are without significant vulnerabilities that hackers can exploit. They must be kept updated to avoid the most serious hacking attacks.

20. One of the newer concerns for all digital device users, is that hackers are now exploiting flaws in software that was often overlooked by them previously. Recently several key attacks have used flaws in printer driver software developed by the printer manufactures to make their printers work with different operating systems. Since many of these drivers were never updated to consider newer cyber attacks the hackers have found them to be easy targets and easy ways to access business and home networks. Similar driver software is made for most peripheral devices, so we need to make sure we are using the latest updated drivers for all of our peripheral devices. That includes, keyboards, mice, audio/visual devices, monitors, printers, scanners, etc.

21. App downloads – We all have downloaded a third party app at some point on our mobile devices. Often we fail to check for reviews that list problems with the apps including security problems and/or product stability and operational flaws before downloading. We often do this because someone else tells us how wonderful the app is. With young children there are a lot of times parents and teachers are downloading what they believe to be gaming apps made by responsible companies. Unfortunately what they may not realize is that these companies may not be meeting the COPPA requirements for ensuring that the software is not being used to collect data on children under the age of 13 or in some cases 18 years of age. Please review all apps carefully before deciding to download them for use in the classroom, and use the same careful

judgment when dealing with children or grandchildren at home. Be sure that any collaboration products can be used exclusively on a local network basis, rather than just on the Cloud (Internet). If the app allows for local collaboration that means you have better control over what the student users are doing than you would if they are using as cloud collaboration product. I am not saying you should never use a Cloud Collaboration product, only that you should be careful in reviewing and choosing these products.

22. Never leave a young child unattended when they are using a digital device. While we may feel that they are capable of using the device and the software product safely, and independently, children will take the opportunity to explore when we are not keeping an eye on them, unless the devices are set with parental controls. Some of the devices we use in the PreK program can be set to use Parental Controls, others cannot, so it is important we watch what the children are doing so they are not attempting to use an Internet based app that we don't provide oversight to here at the school.

23. Social Engineering to get you to reveal personal information including UserID's and passwords. Social Engineering is a term used in sociology to refer to strategies that are used to get groups of people to behave in a specific way without them realizing they are being manipulated to behave that way. This can be via a telephone contact and in-person contact, and more recently has become a large part of "Social Media" sites. This is often done by having you subscribe or join a site to follow the person or group you may be interested in. While this may only be a request for an email address to join, it may also be a request to provide a login for your access which would include you setting up a specific password to login. While you may think you are only creating this for your personal access, the site is actually collecting you login information which includes your UserID and password. They also may send you a verification email for you to confirm the information you have created for the account. While not all sites are doing this in a malicious way, remember that site operators often sell their site to other businesses and/or other site hosting organizations which may use this information in an inappropriate way.

Am I suggesting you or our students should never use a digital device or the Internet because it is too unsafe?

Not at all. What I am suggesting is the same thing I was taught in my NSA Cyber Security training. I am simply suggesting that you use the best practices above to protect you from falling victim to the hackers out there that are only interested in doing harm to you or to organizations in this country including our government. Using your devices and the network and Internet services available to you responsibly is all that anyone can ask of you.