CYBER OCTOBER

Week 1: Physical Security

Cybersecurity covers more than the domain of cyberspace and the intangibility of the internet. Threats lurk around every corner in the real world and people often forget the importance of physical security.

Not only should you be vigilantly aware of adversaries and threats on your network, but also be on the lookout for threats within the workplace or your surroundings as well.

" I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

Workplace Physical Security

- *Shoulder Surfing*: Cover your PIN or Passcode when utilizing a secure door's keypad, at an ATM machine, or typing your PIN on your computer's keyboard. Adversaries with prying eyes may try to gain unauthorized access to your systems by trying peek over and catch you while you type in that sensitive data.
- *Dumpster Diving*: Never throw away documents or paper material that contains Personally Identifiable Information (PII) or For Official Use Only (FOUO). People have been known to dig through dumpsters looking to find any relevant information they can use to perform attacks on AF personnel. Shred all of your paper documents: Receipts, E-mails, Sticky notes, etc.
- Always remove your CAC from your computer's card reader before leaving your workstation. Leaving a CAC in a workstation unattended is considered a CAT I security incident and leaves your computer vulnerable to malicious adversaries.
- Position your monitors and desks to be facing away from windows, doors, or openings. If possible, incorporate a screen protector on your monitors to ensure you have that extra level of privacy when performing your duties.
- Have a white-listed external hard drive for the AFNET? Ensure the data on the drive is encrypted! The 412 CS Wing Cybersecurity Office offers an encryption service through

Windows BitLocker. Send us an e-mail at 412tw.cybersecurity.office@us.af.mil for further information!

Personal / Home Physical Security

- Utilize Wi-Fi in your household? A few simple changes can increase the security of your home network.
    1. *Firmware Updates:* Most routers do not perform automatic updates to their firmware or for system updates. Ensure you access your router's configuration page and check for Firmware updates. These updates will help secure your device from the latest cyber threats.
    2. *Disable SSID Broadcasting*: Service Set Identifier (SSID) is the wireless network name you have chosen for your Wi-Fi. By disabling broadcasting, you will no longer be able to find it through normal means when searching for nearby networks. You'll still be able to connect with the known name, but this is will decrease the odds that your home network will be targeted.
    3. *Change default username/password:* Make sure to change your router's default administrator username and password. Most routers run a default log-on that attackers are well aware of. By changing your default log-on information you can prevent unauthorized individuals on your network.
    4. *Access Control:* If you want to take the extra step to securing your network, most routers come with the option of allowing Access Control via *white-listing* or *black-listing*. A *white-list* access control automatically blocks all new connecting devices even if they have the Wi-Fi log-on credentials. You can *white-list*, or allow, devices through their *Media Access Control*, MAC, address. *Black-listing* will allow new devices to connect, but you can target specific devices through their MAC address and *black-list¸* disallow, them from your network.
- To prevent malicious software from being accidentally installed on Windows you should create two user accounts. An administrator account for installing new software and system configurations, and a standard account for normal computer usage.
- Set a user or supervisor password for your UEFI / BIOS. If someone gains unauthorized access to your home computer and doesn't know your log-on credentials, they can still find their way in by working their way through the computer's UEFI / BIOS. Setting a Supervisor Password will prevent unauthorized changes to your computer's UEFI / BIOS.
- Disable / Turn Off Bluetooth on your devices when not in use. Attacks such as *bluebugging, bluejacking, bluesnarfing,* and more can target exposed Bluetooth devices on users not paying attention to their devices.
- Utilize a touch keypad for your household alarm or door entry? Perform regular cleanings of the touch screen so your finger prints do not leave behind a traceable pattern which may clue in criminals to your security codes.

Cyber October Team

SrA Brian Ison **Johnny Sniderhan**

A1C Joseph Parker **Anthony McCully**