IT'S CYBERSECURITY AWARENESS MONTH!

Updates from the Office of Internal Controls, Audit Compliance & Information Security (IAC/S)

Welcome to Week 3 segment for Cybersecurity Awareness Month. This week we will focus on **Mobile Device Security**, specifically for devices such as iPhones, Android, Google, or other small handheld smartphones. Laptops and Surface Pros are considered mobile devices; however, with the recently deployed secure Gold image these devices have these settings applied.

HOW CAN YOU KEEP YOUR MOBILE DEVICE SECURE?

Device security refers to types of software as well as behaviors that should be practiced to safeguard a mobile, tablet, laptop, storage device, or console against security threats. Cybercriminals are constantly looking for ways to take advantage of unsuspecting users and steal private information.

Device security starts the moment you open a new device and continues through the lifetime of the gadget. Often the factory default settings on mobiles and tablets are not configured with user privacy in mind.

The following are required at a minimum by both the State of Maryland and MDH Information Security Policy:

1. Screen lock enabled
2. Passcode to unlock screen and auto device wipe after 10 failed attempts
3. Encryption of device

Many of us have had our personal devices either lost or stolen. In the case where company information is stored on a device this represents a huge risk. Recently companies have received huge fines due to lost devices that contained confidential information. It is our responsibility to protect private information. MDH is currently investigating ways to further protect the devices of staff accessing email utilizing a MDM (Mobile Device Management) solution that is already deployed for other agencies by DoIT. More information on this will follow in the coming months.

More Ways to Secure Your Device

- Disable location services on all apps that do not require a GPS to function.
- Restrict all unnecessary apps from accessing your photos.
- Check which apps can access your microphone and camera.
- Block external companies from accessing your analytics data.
- Change default passwords.
- Use two-factor authentication.
- Install reputable security software.
- Beware of using unknown wi-fi connections.