WV Executive Branch Privacy Tip

As you know, the Privacy Office occasionally issues tips for the purpose of assisting you in making informed decisions in your "away from work" life. The following tip is reprinted with permission from the Privacy Rights Clearinghouse (www.privacyrights.org).

Mobile Device Security: Basic Tips to Protect Your Data from Thieves and Cybercriminals

Posted March 3, 2014

With the ever increasing presence of smartphones, tablets and other mobile devices in our lives, it is important to be aware of some common privacy and security threats. These are vast and varied, so the level of privacy and security you seek will likely depend on the information at stake.

Start by thinking about the information on your device. How valuable is this information to you? Would you be upset if someone accessed it without asking you? What would happen if it were lost or stolen? Below we've noted a few things you may want to think about, and some tips to help you get started!

Aside from physical theft, threats such as malware and spyware have become increasingly sophisticated. The good news is there are some EASY things you can do to reduce your chances of falling victim.

- **Password-protect your device (or use another means of authentication) and configure the device to automatically lock after a set period of time.** If you lose the device or it is stolen, this could buy you some time to remotely wipe the device. This also makes it a little more difficult for someone to physically install spyware.
- **Use strong, unique passwords and change them often.** You can use a random password generator if you don't want to go through the hassle of creating a new one for every account, and you can use a password manager to keep track of all of the strong passwords you create. Make sure to set a password for entry into your phone and unique passwords for every application utilized via your smartphone.
- **Turn off Bluetooth when you aren't using it.** If your device is always Bluetooth-discoverable, you expose yourself to the added risk of allowing malicious actors access to your device and communications.
- **Use trusted security software.** A lot of people think their mobile devices are immune to the risks that they diligently protect their home and work computers from. This is a myth.
- **Only download apps you trust.** Doing a little reading can save you the hassle of downloading an app that puts malware on your device. What are people saying about the app? Who is the developer? How many times has it been downloaded?
- **Install software updates (this includes your apps).** When vulnerabilities are discovered, the developer should issue an update to fix it. If you don't update the software, you continue to be vulnerable.

- **Err on the side of caution when someone messages or emails you a link or attachment.** Even if you recognize the email address, don't blindly click or download. The same is true with shortened links you see in social media. If you are questioning whether something is a scam, the Federal Trade Commission has comprehensive resources.
- **Be VERY cautious when using public Wi-Fi networks.** Yes, we know they are convenient and save you on your data plan, but you should assume that anything you do on an open network can be seen by others on the network (unless you encrypt your communications).
    - Make sure you are connecting to a legitimate network. For example, if you are in a coffee shop, ask them what their network is called before connecting to any open network.
    - Don't use public Wi-Fi for anything that involves sensitive information without setting up protections to encrypt your communications such as a VPN.
    - If you still decide to use the open network without other protection, think twice before entering ANY login information. Even if you simply want to log in to read the newspaper, assume that the log in information will be seen by anyone on the network. If you use that information (especially a password) for any other personal account--say to log in to your bank account--you could be in trouble.
    - **If you use your own device to create a Wi-Fi hotspot so you can get online, create a strong password.** Otherwise, you risk bad actors gaining access to your connection and communications.
- **Check your device's privacy and security settings, as well as app permissions.** Settings will vary by device and operating system, but feel free to ask us to point you in the right direction if you can't find relevant information. Parents often find these settings helpful when young children have access to devices.
- **Back up important data.** We can't emphasize this tip enough.

Please contact us if you have additional questions, or are looking for more resources!

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.