WV Executive Branch Privacy Tip

ON-THE-GO PROTECTION

Mobile devices make working on-the-go easier than ever, but they also offer new opportunities for hackers and thieves.

ACCORDING TO A RECENT WALL STREET JOURNAL ARTICLE, 50% OF SMARTPHONE USERS DON'T USE ANY PASSWORD PROTECTION.

Mobile devices are everyone's new best friend. We use them to keep in contact with friends, snap pictures, shop and bank online, and listen to music. Increasingly, we're also storing important (and sensitive) personal and company information on them.

Most people understand the need for security with their work and personal computers. Did you know that the same rules apply to mobile devices? In fact, when it comes to threats, there are a host of new ones that specifically target mobile devices.

Ready to get serious about protecting your mobile device? Here are a few easy-to-remember steps that can help mean the difference between sleeping soundly at night and disaster:

Don't leave your mobile device unattended.
The biggest risk to mobile devices isn't hackers or thieves, it's misplacing or losing the device. If you're using public transportation, check the seat before you leave. Make sure that when you aren't using your mobile device, it's either on your person or somewhere close.

Lock your device with a password or PIN.
This helps prevent authorized access. Also, make sure to set up your device to automatically lock after a specified period of time.

Keep your system updated.
Follow company procedures and keep your mobile device's systems current with the latest fixes and updates.

Check with IT before loading any new Apps or other freeware on a company-owned device.
Before you download a new App recommended by a friend, check with IT first. Just because your friend says it's okay doesn't mean the App is safe and free from viruses.

Always log off the corporate network.
If you need to access the corporate network using your mobile device, don't forget to log off after you're finished.

Turn off Wi-Fi and Bluetooth when not in use.
Just like you don't leave your house without locking the door, make sure you lock up access to your computer by turning off Wi-Fi and Bluetooth when you don't need them.

Avoid texting or e-mailing sensitive company or personal information.
Did you know that information sent via e-mail or text isn't secure? Think twice before sending sensitive information via text or e-mail using mobile devices.

Don't click on links or attachments in unsolicited e-mails or text messages.
You know you shouldn't click on links or attachments in unsolicited e-mails or text messages, right? The same rules apply with mobile devices.

More questions?
If you have any questions about using a mobile device for company business, make sure you check with our organization's policies and procedures or contact the IT department.

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

MEDIAPRO®