WV Executive Branch Privacy Tip

FREE WI-FI ISN'T ALWAYS "FREE"

Do's and don'ts for using Wi-Fi and remote access safely and securely.

WI-FI SNOOPING IS NO LONGER A RARITY: IN ONE THREE MONTH PERIOD OVER A MILLION HACKERS RECENTLY DOWNLOADED A PROGRAM THAT PROBES UNSECURED WI-FI CONNECTIONS.

Enjoying that free Wi-Fi at the corner café? You might have second thoughts if you knew that there could be a hidden cost. Cyber snoops and hackers enjoy preying on people just like you, using free Wi-Fi hot spots to hack into your unprotected mobile device.

Alarmed? You should be. But there are ways to stay safe and secure when working at home or off site. Here's a summary of common best practices:

1. **Choose secure connections.**
   When connecting to the internet while working off site, always try to choose a wireless network that requires a security key or has some other form of security.

2. **Approve access before you connect**
   Many mobile devices are set up to "sniff" for Wi-Fi access points and then connect automatically. How do you know if your mobile device is connecting to the "right" one? Easy. Just configure your device so that you must approve access before you connect.

3. **Disable your Wi-Fi adapter.**
   When you're not at work, a good habit to practice is to turn off your computer or mobile device's Wi-Fi capability when you don't need it.

4. **Make sure your firewall is always up**
   As the name implies, a firewall prevents unsecured access to your computer or mobile device. If you're going online off site, double check and make sure your firewall is on.

5. **Turn off file and printer sharing**
   It might be nice to let other colleagues on a network access resources on your computer. But not when you're working off site. When working away from the office, make sure you turn off file and printer sharing. When it's on, your mobile device is vulnerable to hackers.

6. **Encrypt … encrypt … encrypt**
   Okay, you get hacked. That means you're hosed, right? Maybe not. By encrypting your files, you add an additional level of protection in case you do get hacked. Encrypted files require a password to open or modify them.

7. **Too risky to lose?**
   This may seem obvious, but if the information on your mobile device is too sensitive to lose, maybe that's a good indication that it shouldn't be there in the first place.

More questions?
For more information about working remotely, make sure you check 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®