WV Executive Branch Privacy Tip
Public Computing – Risky Business!

KEEP IT COVERED…KEEP IT CLOSE…KEEP IT SAFE!

Learn how working on your computer or mobile device in public places can put company data at risk.

IN A TEST BY CBS NEWS, A HACKER WAS ABLE TO ACCESS A JOURNALIST'S LAPTOP OVER PUBLIC WI-FI FASTER THAN YOU CAN SAY *OPEN SESAME*.

The world is your office. Well, maybe not quite, but it's closer to being a reality than it once was. One of the benefits of today's mobile devices is that you can work almost anywhere—the park, the mall, a favorite book store, or the corner café.

But that kind of freedom doesn't come without risk. And we're not referring to the threat of a waiter dumping a plate of pasta on your notebook computer. Yesterday's pickpockets are today's hackers, looking to pluck personal and corporate information while you're out and about. In public, it takes little more than someone listening to your conversation or glancing over your shoulder to cause a serious security breach.

When working in public places, be on guard for the following dangers:

Eyes and Ears are Everywhere

- Don't talk about sensitive information when people can overhear your conversation.
- Don't access sensitive personal or company information if other people can see your laptop screen.

No Device Left Behind

- If you need to take a break or leave your seat, even for a second, always take your mobile devices with you.
- Want a guaranteed way to make the nightly news? Be the person who forgets a thumb drive loaded with confidential company and customer information on the plane. Always make sure to check your seat to make sure you aren't leaving anything behind.

Public Wi-Fi Can Be Too Public

- Whenever you can, use a Virtual Private Network (VPN).
- Take a second and turn off the wireless signal on your mobile device when it's not in use.
- Always use Wi-Fi Protected Access (WPA2) encryption.
- Keep your browser security settings on Medium or High security level.
- Ensure anti-virus software is running at all times, scanning both incoming and outgoing files.
- Don't connect to different networks simultaneously, or "dual home" (e.g., connect to the Internet and our organization's network at the same time.)

Remember the old Smokey the Bear warning? *Only you can prevent forest fires.* The same is true with security breaches. Only you can protect the integrity of our organization's information. Be smart. Working in public places can be safe … but only as long as you take the proper precautions.

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