This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

CYBERMINDFUL ON THE ROAD

Welcome back! By now, we're getting the hang of cybermindfulness in our normal computing locales. But when we travel, there are a few extra safe computing things to think about. Today we'll explore safe computing tips for travel, whether you're on the road to Miamisburg, OH or Miami, FL.

On the Road Again: Safe Computing Considerations for Travel

Hackers call the interception of computer messages a "man in the middle attack." Think of it as cyber-eavesdropping. The tips below will help you avoid being "overheard" when you're out and online.

Keep Your Connection Safe

If you partake of **FREE WI-FI**, how can you tell if the setter-upper has taken the right network precautions? Well, sometimes you can't. Here's what you *can* do:

- When possible, **use trusted Wi-Fi providers** that you know are secured. For instance, if you're in a hotel or conference center, use their official Wi-Fi, not some random open network you see listed as a nearby option.
- **Check that your sensitive online activity is encrypted.** Look for the "https://" prefix and the green lock icon in a web browser before entering your username and password on a site.

Keep Your Devices and Data Safe

If you lost your phone, tablet or laptop on the road, what info could someone get to? Before you head out, take a few easy steps to protect your stuff.

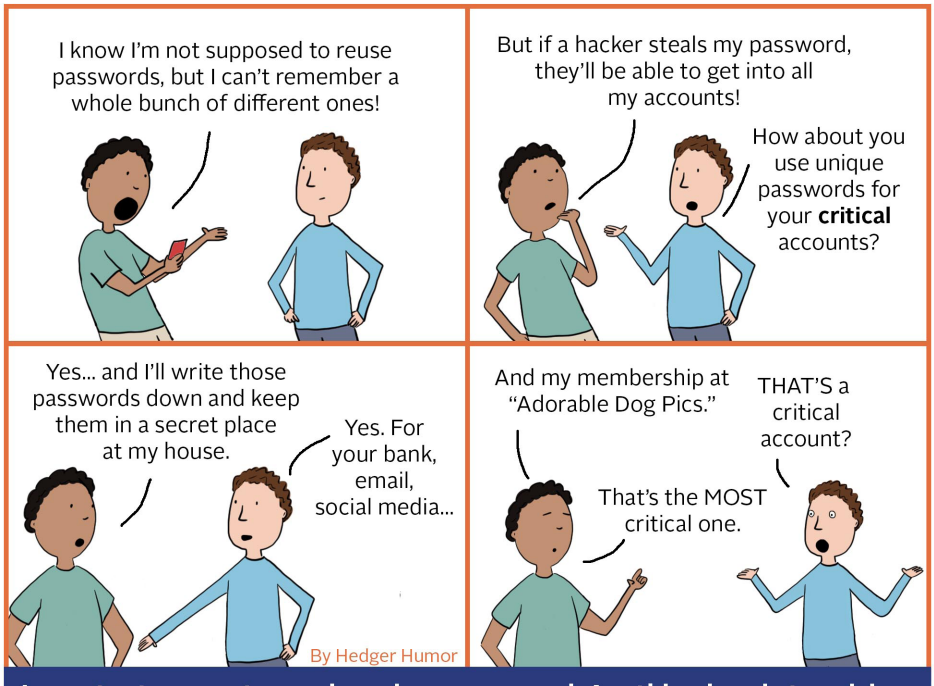
- **Clean your machine before traveling.** Make sure your

software, apps and operating systems are updated so you're not open to avoidable vulnerabilities.

- **Set an automatic screen lock.** Most devices have a setting to "lock" the device with your password or passcode after a period of time – find and enable this.
- **Encrypt your phone and laptop.** If you have a work laptop or phone, you likely have encryption software installed already (check with your IT support team), but encryption software is available for your personal devices as well. In fact, Windows and Mac OSX encryption are built into many of their operating systems, you just need to activate it. Your phone or tablet might also offer encryption as an additional security setting – and if not, you can add it.
- Regularly **backup and remove sensitive data** from your mobile devices. If it's not on there, no one can steal it.
- Remember that **if you're using a public computer** (like in a hotel lobby or internet cafe) your online activity could be tracked, so **don't visit sites that require your login info**.

BONUS TIP: Keep Travel Plans Off Social Media

Keep travel plans off social media. Don't post when you're traveling or going out of town on vacation. Letting criminals know that you're not home is an open invitation. Similarly, don't "check in" on social media everywhere you go. Save those beach and food pics to show off to friends when you return instead.



Important accounts need a unique password. Anything less is too risky.

Scam Self-Defense: Security Service Hoax

Here's another scam to watch out for: websites that spoof legitimate security software vendors' sites (like Symantec, McAfee, Kaspersky, etc.). Search results for these companies could turn up some fake sites along with the real ones.

Fake sites often tell you there's something badly wrong with your computer which needs to be fixed immediately and direct you to an 800-number for "support". The scammer on the other end of the line will likely demand remote access to your computer and charge you a hefty credit card fee to fix an imaginary problem.

Remember – only call toll-free numbers you know are legit, like on the back of your credit card, an account statement or an order confirmation email you received after a legitimate purchase. And never give out confidential information unless YOU have initiated the communication.

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE