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.

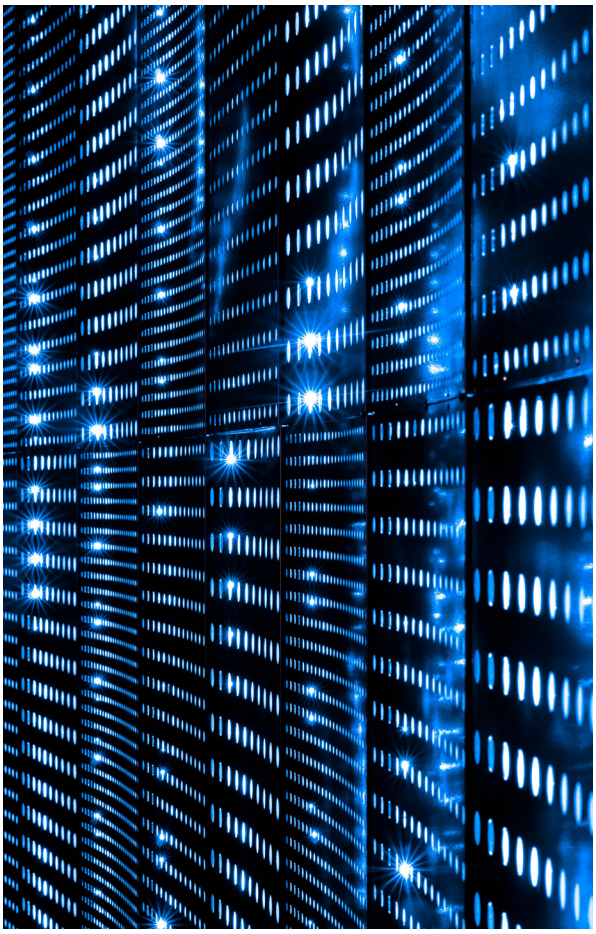
Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

THERE'S NO PLACE LIKE HOME ... FOR SAFE COMPUTING

Welcome, dear reader! So happy to see you back for another issue of **Becoming Cybermindful**. Today we're talking about safe computing in the ole' homestead. If you ever access the internet from home (you know, just in case you're ever online when you're not at work), there are some things to think about. Let's discuss.



Keep the Riff-Raff Off Your Wireless Network

A wireless network happens when you connect an internet access point – like a cable or DSL modem – to a wireless router. Going wireless is a convenient way to allow multiple devices to connect to the internet from different areas of your home.

However, unless you secure your router, you're vulnerable to people accessing information on your computer, using your internet service for free and potentially using your network to commit cybercrimes.

So take a few minutes to make sure your wireless router is secure:

1. **Change the name of your router:** The default ID – called a "service set idenstifier" (SSID) or "extended service set identifier" (ESSID) – is assigned by the manufacturer. Change your router to a name that is unique to you and won't be easily guessed by others.
2. **Change the preset password on your router:** When creating a new password, make sure it's long and strong, using a mix of numbers, letters and symbols. Troublemakers (or anyone, really) can often find these preset passwords online and crack into your device if you haven't changed it.
3. **Create a guest password:** Some routers allow for guests to

use the network via a separate password. If you have many visitors to your home, it's a good idea to set up a guest network.

4. **Use a firewall:** Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for attempts to access your system and blocking communications with sources you don't permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

Scammers can trick you by phone, too. Hang up on weird calls.

Scam Self-Defense: Tech Support Sabotage

"I just received a voicemail that said it was an emergency – the license key for Microsoft Windows was due to expire – and I should call 1-800-XXX-XXXX."

That's just one variation of the many phony tech support scare scams where a pop-up implores you to take IMMEDIATE ACTION to avoid CERTAIN DOOM and then directs you to a support line with phony techs ready to take your credit card number and fix the "problem".

There are several flavors of this scheme. You might receive a phone call from a "helpful" tech offering to fix a problem if you'll just allow remote access to your computer. Or you might be presented with an intimidating pop-up screen warning that something dire is about to happen ... unless you call their tech support line immediately.

The bottom line? Legitimate companies like Apple, Dell or Microsoft won't cold call you to fix problems on your computer. They're also not likely to harass you with a giant pop-up advertising their support number, either. If you suspect a problem, call your organization's tech support team instead. And if you'd like to learn more, check out the FTC's cheat sheet on tech support scams.

To paraphrase the immortal words of Nancy Regan, "just say no" to tech support offers that come out of the blue. And thanks for saying "yes" to these little doses of cybermindful education. We'll see you next time!

Learn more about Becoming Cybermindful at go.udayton.edu/cybersecurity

THIS PUBLICATION IS PROVIDED BY:

University of Dayton Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE