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.

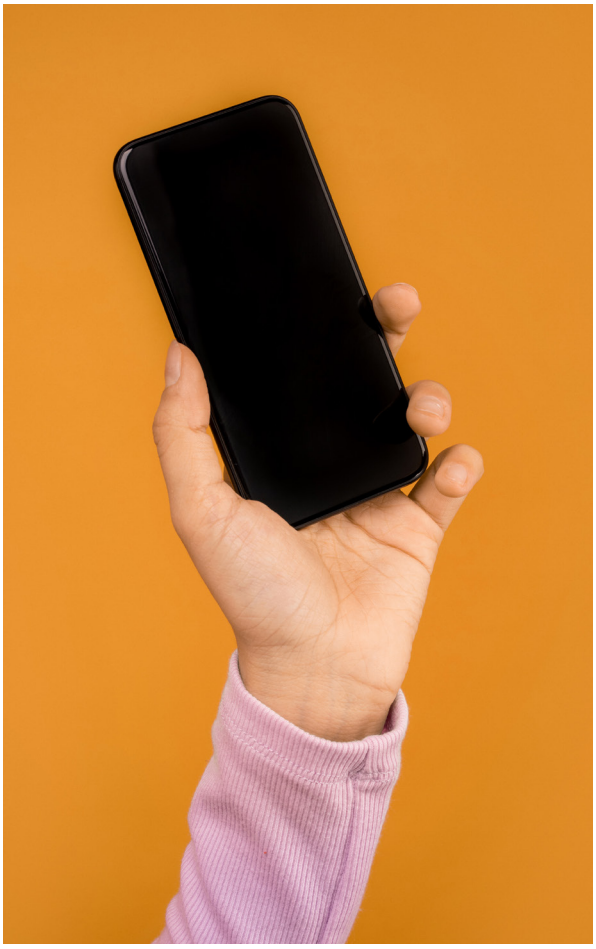
Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

CYBERMINDFUL HABITS FOR A LIFETIME ONLINE

If you're reading this, you've made it to the final newsletter of our **Becoming Cybermindful** series – congratulations! pefully you know a bit more than you did when we started out and feel more confident about facing the trials, treats and travails of online life. Before we part, let's review five habits of cybermindfulness.



Cybermindful Habits for a Lifetime Online

CYBERMINDFUL HABIT 1: Keep a clean machine.
Make sure your operating system, anti-virus and applications are regularly updated.

CYBERMINDFUL HABIT 2: Back up important stuff.
If you'd be sorry to lose it, make sure you've got a copy on some kind of offline storage (like an encrypted hard drive).

CYBERMINDFUL HABIT 3: Be aware of what you share.
When you put information online, think about where it's going and who can (or could) see it.

CYBERMINDFUL HABIT 4: Watch which Wi-Fi.
When you're out and about, only connect to recognizable wi-fi sources on your mobile devices. And make sure the websites you're using have that green lock icon if you'll be entering any sensitive information.

CYBERMINDFUL HABIT 5: Think before you click.
Look for the common, sneaky signs – was the message expected? Is it asking you to do something (click, enter info)? Is it trying to make you feel worried or curious? If it looks suspicious, ignore it.

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

Scam Self-Defense: With the Right Bait …

Frankly, most of us small potatoes aren't likely to be on the receiving end of a seriously targeted spear phishing attempt. But some of us, especially if we have highly-elevated system access or regularly traffic in confidential info, surely could be. It's helpful to keep a few things in mind.

Timing matters.

After work, hanging with the family, we may not be in "cybermindfulness" mode. Hackers know this and often time their messages to arrive when they suspect our defenses will be down.

Our phones aren't our friends.

We're less likely to double-check links from our phones (it's a "click and hold" move to do so on most devices), but that doesn't mean the links are less likely to be dangerous. Be on guard, even if you're not on your computer.

With the right bait, anyone might click.

Staying cybermindful lowers our odds, but if someone's really after us, directly and personally, there's a good chance we'll fall for it. Which is why our other defenses – updated anti-virus, spam filters, etc. – are still important.

The songwriter Joe South inadvertently offered some of the best advice ever about cybersecurity: "You better look before you leap." You don't have to agonize over every email that lands in your inbox, just stay aware of what you're being asked to do – and who's asking – before you comply with a request for action or info.

Some Final Words of Wisdom: The Secret of Cybermindfulness

It is easy to think that staying safe online is difficult, time consuming or a waste of time. The truth is much more encouraging: a little attention to a few simple protective measures has the potential to save you, your family and the organization you work for a whole lot of hassle.

We don't fall victim to social engineering because we're dumb or because hackers are so smart; we get ourselves in trouble when we forget the basics:

- **Keep your devices updated** (even if it means an inconvenient reboot)
- **If a communication asks you to take unexpected, but urgent action, think twice** (and don't be afraid to ignore or delete a weird message – a *real* correspondent will likely reach out again)
- **Whenever possible, use multi-factor authentication** (a passcode to your phone, a fingerprint verification) to extra-protect your online accounts
- **When in doubt, ask for help.** Contact the good people in your IT department for a second opinion or reach out to the sender directly (just be sure to look for contact info *outside* of the suspicious message you received) to verify if you're not sure.

And if you do get tricked (it happens to the best of us) and think you might have given up info to a cybercreep, contact your IT support team or the customer support line for the service the hacker tricked you with. **With quick action** (change your passwords for affected accounts!) **and a little extra attention** (watch for weird activity on your online accounts!) **there's an excellent chance that the damage done will be negligible.**

So what is the secret? The secret is that *right now* you have all the skills and knowledge you need to protect yourself from 90% of the attacks you will ever see!

And that's a wrap! Thanks for reading, friends. Now go forth and keep being cybermindful!

"With quick action and a little extra attention there's an excellent chance that the damage done will be negligible."

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE