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:

INFORMATION SECURITY IS EVERYONE'S BUSINESS

Greetings! Welcome to **Becoming Cybermindful**, a periodic publication that will provide you with the tips and know-how you need to keep yourself and your organization safe while you navigate life and work online.

Why should I care about safe computing?

That's a fair question. There's plenty competing for our attention – why spend some of it on Becoming Cybermindful? Well, here's the problem – we're doing stuff online all the time, for both our personal and professional lives. It turns out that all that online info is cash to criminals and they'll work hard to get it by any means possible: hacking into systems, downloading malware, or tricking you with smart-looking "phishing" emails. Your information, as well as your organization's data, is vulnerable – especially to our bad online habits.

But here's the good news: **by practicing safe computing habits, you help guard yourself and your workplace** from exposure of personal information, intellectual property or institutional information, loss of trust and reputation, and expensive remediation that results from data breaches. Habits are something we can work on together ... and they make a real difference.

Scam Self-Defense: That Link Might Stink

With all the email we get, it's no wonder we skim our messages, scanning for the meaningful bits. Hyperlinks jump out as something actionable, often presenting commands like "Log in to Your Account" or "Check the Status of Your Package". Even without imperatives, underlined, blue text just beckons us to click and obey: See link. Click link. Buttons are enticing too: Nice button. Click button. Habit. That's where it gets you.

But not all links deliver what they promise. In fact, a link can stink:

- By hiding a malicious download that infects your computer with malware, spyware or ransomware
- By taking you to a simulated website, like your bank, where you log in and the bad guys capture your credentials or account information

It's not always clear where a link is leading you. Look for these red flags:

- ☒ I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website.
- ☒ I received an email that only has long hyperlinks with no further information, and the rest of the email is blank.
- ☒ I received an email with a hyperlink that is a misspelling of a known website. For instance, bankofarnerica.com – the "m" is really two characters – "r" and "n".

If a link doesn't pass the sniff test, dump the email. And pat yourself on the back – you're Becoming Cybermindful already!

By Hedger Humor
Oh my gosh, this email says my account was hacked! NOOOO!
Hold on!
This is an unexpected email. It has an urgent tone. And it wants you to click on a link and enter login information. Those are signs of a scam!
Just check your account. Log in like you normally do.
My account seems fine. But I am NOT happy that this person tried to trick me!
How about I reply and say, "WHAT THE HECK?!"
Just delete it.
Then I'll say, "You need to re-examine your life choices!"

Know the warning signs in email. When in doubt, delete.

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