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:

WILL YOUR PASSWORDS BE UNBROKEN?

Good news – it's time for another dose of **Becoming Cybermindful**. This month's topic is near and dear to all our hearts: passwords. For a little extra fun, we'll talk about tax scams, too.

Password Wisdom 2.0

We know what you're thinking: "Strong passwords, change my passwords, don't Post-It to my computer monitor, blah-blah-blah ... I already *know* all that!" But, you may be surprised to learn that some "Password Wisdom" has changed over the years. These nuggets of password advice might surprise you.

You don't need different passwords for ALL the things, just the important things.
Work smarter, not harder. Think about your online services in terms of what requires the *most* security (like banking, work accounts) and what might be ok with a little less (like a Bengals fan forum or recipe sharing site). Stuff with financial or personal info should be protected with a strong, unique password (here's a quick video with A Few Words about Strong Passwords). For "junk" accounts, a little bit of password reuse is ok.

The goal is to reduce your vulnerability if something gets hacked – if your recipe account is hacked and you use the same password for online banking ... that's likely to go badly.

You can write passwords down.
Unless you're an elephant (they never forget, you know), chances are you can't keep every password in your brain. You *can* write them down, but protect them like your other valuables – maybe in your wallet or a locked drawer. Or, consider an online "password manager" like LastPass, Dashlane, or 1Password (these let you remember one *super secure* password to a site that safely catalogs all your others).

Passwords aren't enough to keep your data safe.
Sad, but true. A quick search on cybersecurity expert Troy Hunt's great site haveibeenpwned.com will show how many of your email addresses – and passwords – have already been exposed in data breaches. Your best bet is to use multi-factor authentication whenever possible to add an extra layer of security to your most important accounts. Read about MFA in this article by the National Institute of Standards and Technology.

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

Scam Self-Defense: Taxes, Death and Scammers – Always Sure Things

When tax season rolls around, don't let the drudgery of forms and schedules lull you into indiscriminate link clicking or freely sharing your adjusted gross income with the next pop-up that asks. Criminals may lure you with clever, timely ruses like:

- Phishing scams that promise links to your W-2 or other IRS-related information
- Phony tax return services designed to capture your personal information

The IRS and the state of Ohio both have websites to report suspicious information:

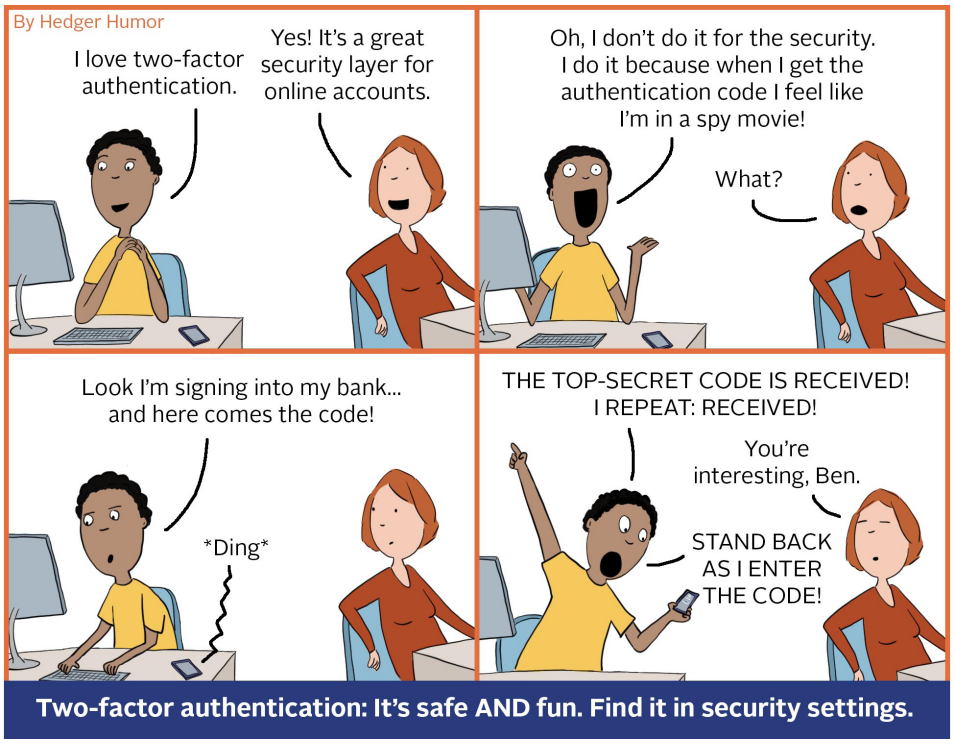
IRS – https://www.irs.gov/uac/Report-Phishing

OH – http://www.tax.ohio.gov/enforcement/Report_Fraud.aspx

Like taxes themselves, tax scams seem to stand the test of time. Keep an eye out, particularly if a message directs you to what looks like a login page (*always* question the validity of unsolicited links). When in doubt, open a separate browser window and type in the address of the website you're trying to visit directly.

Here are some ways to reduce your risk:

- Always use security software with firewall and anti-virus protections
- Use strong passwords on any site where you might enter your social security number
- Learn to recognize and avoid phishing emails *and* threatening calls or texts from thieves posing as legitimate organizations like your bank, credit card companies and the IRS
- Don't click on links or download attachments from unknown or suspicious emails
- Protect your personal data - don't routinely carry your social security card, store your tax records in a secure location



Contact the IRS if you get a notice indicating any of the following:

- You were paid by an employer you don't know
- More than one tax return was filed using your social security number
- Your attempt to file an electronic return is rejected with a message saying a return with a duplicate social security number has been filed
- You're entitled to a tax refund that you didn't request

In the good old days, the only certain things were death and taxes. With the advent of the internet, we're pretty sure you can always count on tax scams, too. But if we stay Cybermindful, we can really reduce the chances of being victimized by a phony email message from the IRS. Though it won't help avoid the Grim Reaper. On that cheery note, we'll see you next time! Keep thinking before you click!

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE