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.

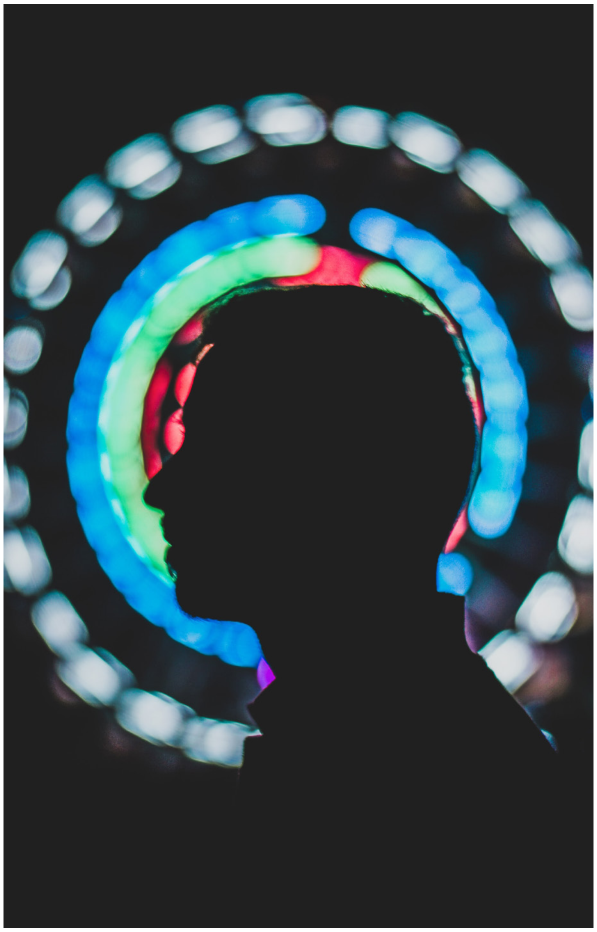
Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

ONLINE SHOPPING, BANKING AND GAMING – DON'T LET IT COST YOU

This month we're **Becoming Cybermindful** about shopping, banking and gaming online. We're betting you do at least one, maybe two (and if you're a millennial or younger, all three) of these things. Let's start with a quick refresher about Personally Identifiable Information (or "PII"), and why we want to protect it.



A Piece of the PII

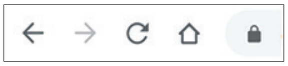
So what *is* PII, anyhow? It's any info specific to an individual that you don't want floating around freely in the cybersphere: Social security numbers, credit card numbers, banking info, your mother's maiden name … if it could be used to fake your identity or take your money, it's PII.

And the more PII you have in one lump, the more you want to protect it – if a crook has your DOB, that's one thing; having your address, home phone and SS# to go along with it is another, riskier ball of wax! In fact, a collection of your PII is so valuable it even has its own internet slang – a "Fullz" is a "full set of information." So where your credit card info might be worth $20, a Fullz with your physical address, date of birth and social security number might be worth $100 to a criminal engaged in identity theft. Crazy, right? (Might be a good time for A Few Words about Protecting Yourself from Identity Theft if you've got a few minutes, actually.)

Shopping and banking in particular rely on you sending some of your PII online. And that's ok, as long as you're paying attention. To that end …

Tips for Shopping, Banking and Gaming Online

✓ Make sure all transactions happen on secure websites, identified by an "https" prefix and (usually) a padlock icon in the URL bar.



✓ Exercise caution if you see an offer where the discount is way below normal (the bad guys know we're price sensitive when shopping online).

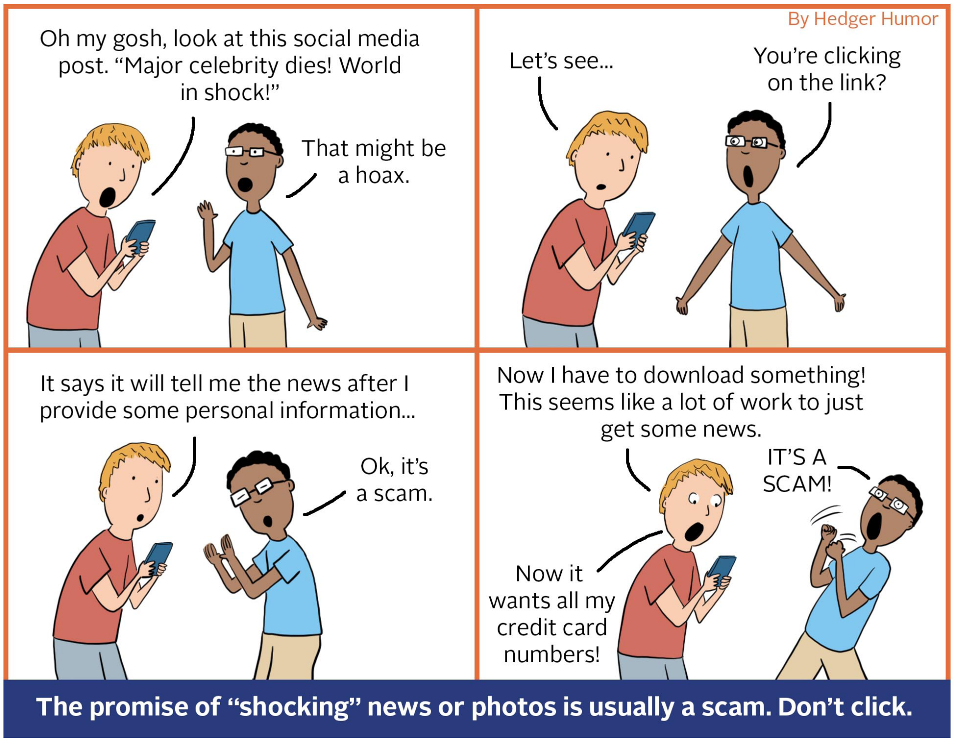
✓ Check your credit card transactions regularly (even daily) for unusual charges, especially small amounts.

✓ Use strong, separate passwords for bank accounts, credit card accounts, etc. – and turn on multi-factor authentication wherever it's available.

✓ Gaming? Beware messages that ask you to click something. Much like phishing emails, online games can trigger potentially malicious links and downloads.

✓ Keep your device's software and operating system up-to-date. A clean machine is a (more) secure machine!

Watch [A Few Words about How to Protect Your Data Online] for more suggestions!


By Hedger Humor
Oh my gosh, look at this social media post. "Major celebrity dies! World in shock!"
That might be a hoax.
Let's see...
You're clicking on the link?
It says it will tell me the news after I provide some personal information...
Ok, it's a scam.
Now I have to download something! This seems like a lot of work to just get some news.
IT'S A SCAM!
Now it wants all my credit card numbers!

The promise of "shocking" news or photos is usually a scam. Don't click.

Scam Self-Defense: Fake Apps

Many stores offer apps for direct online purchasing, so (to no one's surprise) scammers sometimes try to capitalize on this with fake retail apps. If you download one to your smartphone or tablet and load your credit card information, you can guess what happens next.

Your best bet? Be careful about what apps you download and how much information you give them. [AT&T recommends] paying particular attention to the name, the reviews and the number of downloads.

Alright, we've learned enough for today; go forth and treat yourself to some online gaming or shopping (cybermindfully, of course).

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