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:

GUARD YOUR PRIVACY ... AND SECURITY ... AND PRIVACY

You can't get too far into a convo about safe computing without the words "privacy" and "security" popping up. They're often used interchangeably, but they're not exactly the same thing. Since they're *both* important to **Becoming Cybermindful**, let's take a few minutes today to sort out what's what when it comes to privacy and security.

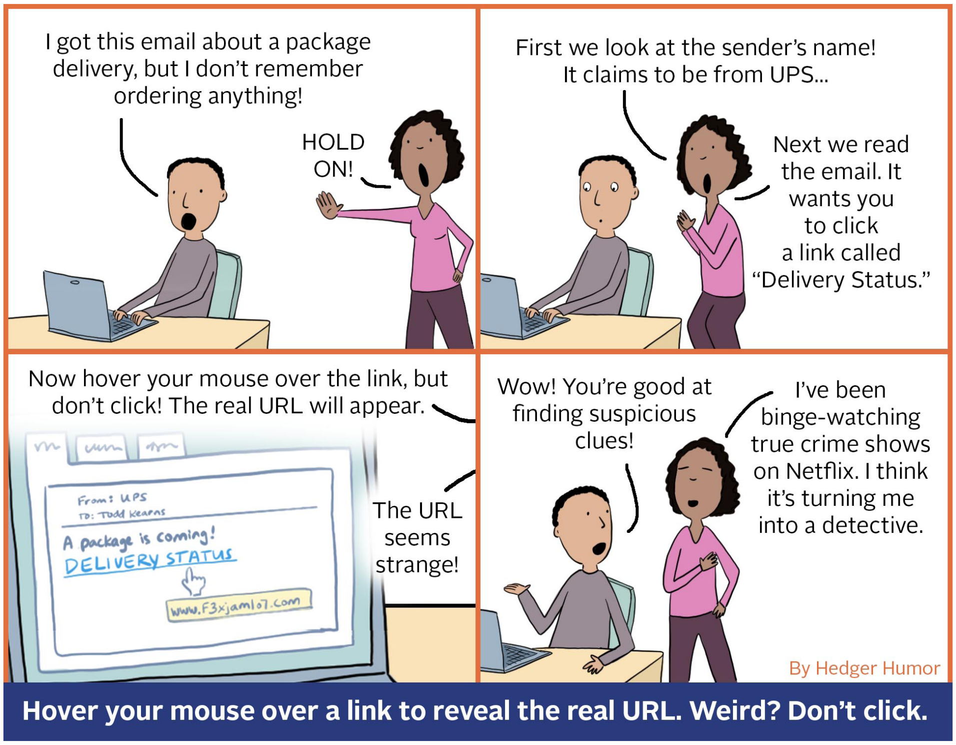
Security vs. Privacy

Ever heard that joke about involvement and commitment? "Think of a ham and eggs breakfast; the chicken was involved, the pig was committed." Security and privacy are similar – related, but not the same thing. This one gets a little deep, so buckle up.

SECURITY is about the technical and physical protections of your information – how data is guarded from unauthorized use. If you've got a firewall enabled on your computer, for instance, or you're storing information in a strongly password-protected system, we'd say that info is "secure".

PRIVACY encompasses everything done with data:

- Who collects it
- What they collect
- How they collect it
- Who they collect it from
- Who they share it with
- Where they store it
- How they transmit it
- What data is legally protected, what isn't


I got this email about a package delivery, but I don't remember ordering anything!
HOLD ON!
First we look at the sender's name! It claims to be from UPS...
Next we read the email. It wants you to click a link called "Delivery Status."
Now hover your mouse over the link, but don't click! The real URL will appear.
From: UPS
TO: Todd Kearns
A package is coming!
DELIVERY STATUS
www.F3xjaml07.com
The URL seems strange!
Wow! You're good at finding suspicious clues!
I've been binge-watching true crime shows on Netflix. I think it's turning me into a detective.
By Hedger Humor

Hover your mouse over a link to reveal the real URL. Weird? Don't click.

Privacy is about how folks with legitimate access to your information use it. Let's say you've voluntarily given your height and weight to your doctor along with a bunch of other health information. She can't give or sell that to the gym down the street – or *can* she? That's the kind of question we ask regarding data privacy. "You've got information about me. What rules govern your handling of that information?" Privacy is about the control you have (or don't) over where your information is going.

Being Cybermindful, we want to consider both. We want to make sure the systems we use to store and transmit our data are secure, but we also want to make sure the folks with legitimate access to our data will handle it responsibly.

And sometimes, *we're* those folks! As employees, we're often privileged users of other people's private information and need to be aware that there are federal laws (like FERPA for student data, HIPPA for health records) and industry standards (like PCI for debit and credit card information) that specify what kinds of data must be protected. With respect to our professional lives, here's our role in a nutshell:

> *As privileged users, we're responsible* for honoring data laws and guidelines and treating protected information with the utmost respect by *keeping our access to information locked* and *never storing protected information on personal devices or unsecured systems.*

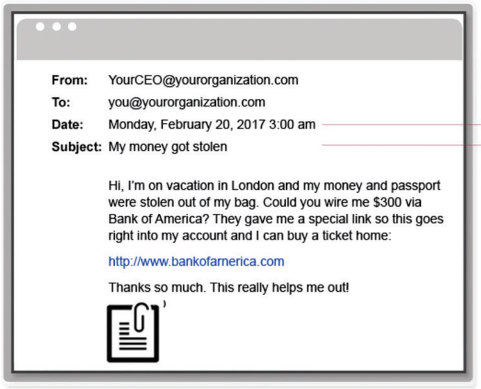
Share With Care

Outside of work, we also want to keep privacy in mind when sharing online:

- ✓ **Do your research:** Before posting information online, find out who can access the information, who controls and owns the information, and what is shared with third parties.
- ✓ **Keep your personal information private**: Assess whether it's *really* necessary to share sensitive information like your birthday, mailing address, phone number, e-mail, mother's maiden name, sexual orientation or Social Security number. When appropriate, make up answers only you would know or share partial information (like your birthday, but not the year you were born).
- ✓ **Own your online presence:** Set the privacy and security settings on web services and devices to your comfort level for information sharing.
- ✓ **Be cautious about accepting requests to connect online**: Connect only to people you trust who will not misuse the information or photos you post about your personal life, preferences, whereabouts.
- ✓ **Disable WiFi and Bluetooth when not in use:** Some stores and other locations look for devices with

Scam Self-Defense: Real People Don’t Email at 3 a.m.

Sure, some people do. But probably not your boss with a legitimate request for a list of salaries or a bank transfer. The “when” matters. Take a look at this red flags cheat sheet:



From: YourCEO@yourorganization.com
To: you@yourorganization.com
Date: Monday, February 20, 2017 3:00 am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

DATE/TIME

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time**, like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

Phew! That was a lot! Are you still reading? Great. Thanks. As a small reward for your continued attention, go take a walk, a nap or whatever kind of break will give your brain a breather. You’ve earned it. And whether you realize it or not, you’re becoming cybermindful – well done!

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

WiFi or Bluetooth turned on to track your movements while you are within range.

✓ **Think before you app:** Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value – just like money. Be thoughtful about who gets that information and how it’s collected through apps.

✓ **Delete when done:** Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterwards, or we may have previously downloaded apps that are no longer useful or interesting to us. It’s a good security practice to delete all apps you no longer use.

✓ **Secure your devices:** Use strong passwords, passcodes or touch ID features to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out.

✓ **Be aware of what’s being shared:** When you share a post, picture or video online, you may also be revealing information about others. Be thoughtful when and how you share information about others.

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton
Center for
Cybersecurity &
Data Intelligence

OHIO CYBER
RANGE INSTITUTE