Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

SOME THINGS ABOUT THE INTERNET OF THINGS

Greetings, Cybermindful friends! In our time together today, we're going to talk about some things. Some Internet Things.

Thinking about Things: A Safe Look at Smart Tech

The Internet of Things – or "IoT" – comprises every "thing" connected to the internet. Your smartphone and computer, of course, but plenty of other things, too: TVs, fitness trackers, your coffee maker … Almost anything with an on/off switch can be part of the Internet of Things these days. Think about what the following things can already do:

Wearables: Map your walk, monitor your heart rate and sleep, send alerts in an emergency

Appliances (e.g. thermostats, lighting, smoke detectors, refrigerators, entertainment equipment): Can be powered on/off or have settings adjusted remotely; learn and adjust to your use patterns; allow remote troubleshooting and repair

Home security: Allow you to lock/unlock doors without keys; control access via phone app; provide alerts

Cars: Send/receive via GPS to provide navigation, or send email when your car needs maintenance, unlock remotely, find you an open parking space, and even drive for you – yikes!
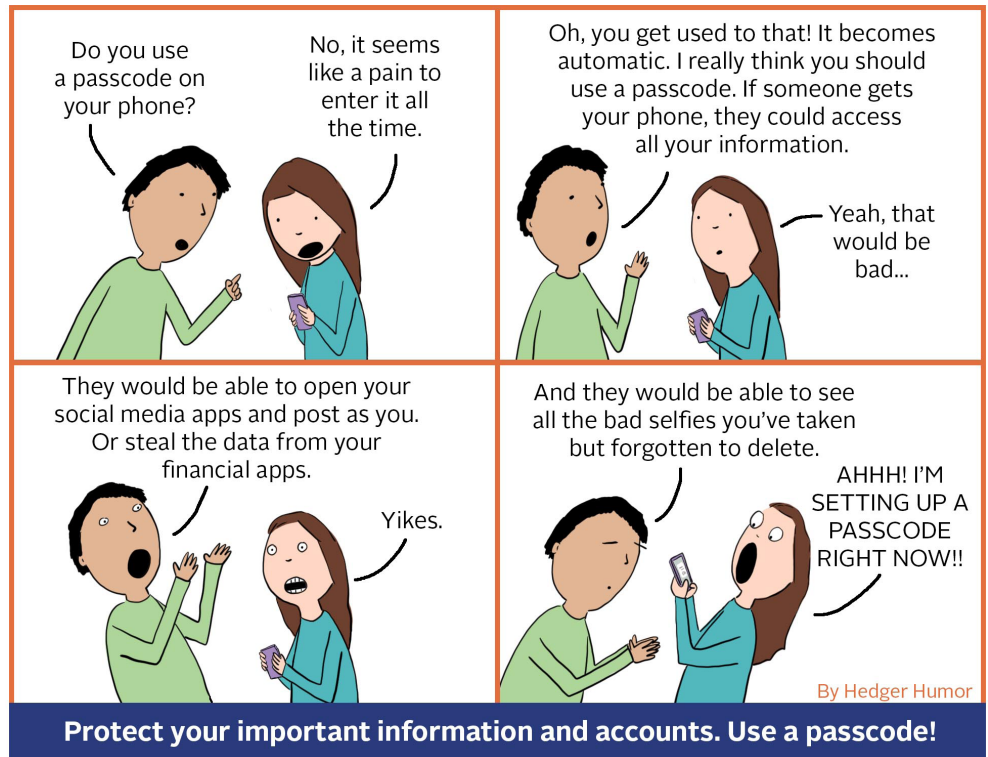
All of these things (over *20 billion* of them worldwide, according to Gartner.com) collect and share data to make our lives more convenient. But their power also holds potential for abuse by cyberslime. Regulations requiring secure transmission or use of the data generated by smart devices are still pretty inconsistent. And because the IoT is expanding so quickly, security concerns are growing too.

With that in mind, here's some quick advice for staying on top of your Internet of Things ... things:

- **Change the default passwords on all your connected devices**, *especially* your home Wi-Fi router! These "baked in" passwords can often be found online and are easy to exploit.

- **Check the default privacy and security settings** on your IoT devices and make sure you're allowing as limited access as possible.

Not sure how? Well, just so happens we've got a video for that: [A Few Words about Changing Default Settings for Networked Devices](#).
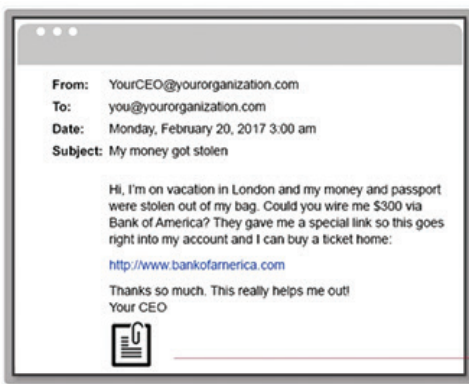
Less important, but still puzzling, we wonder about that non-descript word, "things," especially in a tech-proliferating world rife with ultra-trendy jargon and acronyms galore. Couldn't the clever cyber people coin a better term than "Internet of *Things*"? Oh well, some *things* we may never understand ...

Do you use a passcode on your phone?

No, it seems like a pain to enter it all the time.

Oh, you get used to that! It becomes automatic. I really think you should use a passcode. If someone gets your phone, they could access all your information.

Yeah, that would be bad...

They would be able to open your social media apps and post as you. Or steal the data from your financial apps.

Yikes.

And they would be able to see all the bad selfies you've taken but forgotten to delete.

AHHH! I'M SETTING UP A PASSCODE RIGHT NOW!!

By Hedger Humor

Protect your important information and accounts. Use a passcode!

Scam Self-Defense: Attachments Can Attack

Attachments are like candies: be wary about accepting them from strangers. That said, depending on your line of work, you might receive unsolicited attachments as part of your job. In this case, the best defense is a good ... defense. Keep your anti-virus (and other software) updated so your computer has the best self-protection tools at the ready.

And *if an attachment asks you to "enable macros," just say NO.* Malicious macros have become an increasingly common way of delivering ransomware. Here are a few other red flags to watch for:

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.bankofamerica.com

Thanks so much. This really helps me out!
Your CEO

ATTACHMENTS

• The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)

• I see an attachment with a possibly **dangerous file type.** The only file type that is **always safe to click on is a .txt file**.
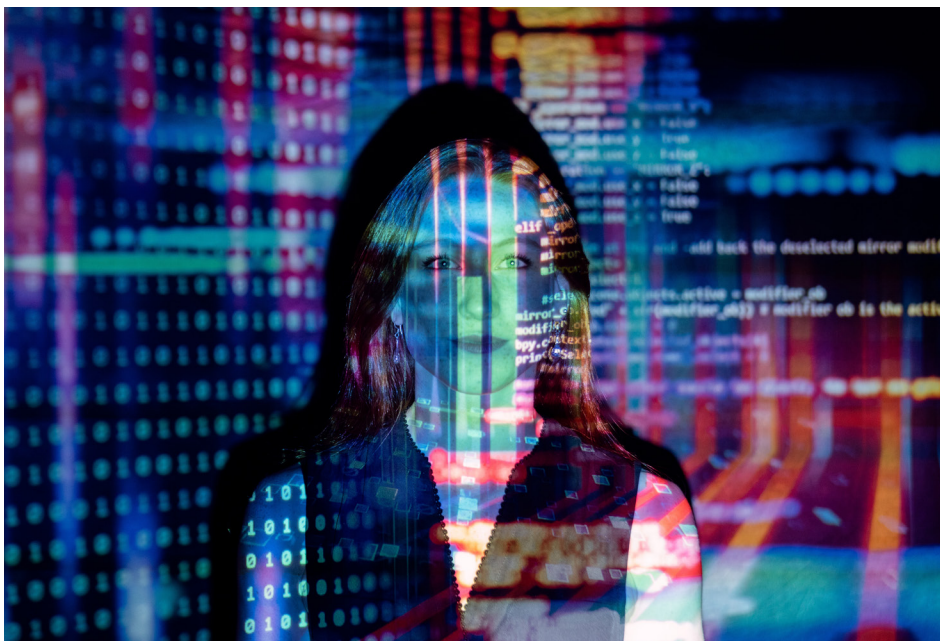
One final tip as we wrap things up:

You may have heard "if you're not paying for a service or a game online, you're probably the product." Access to small batches of your personal info is often the reason so many online services are "free" to begin with. That's not always a bad thing (data makes the world go round these days), but if you don't want the data from your Internet Things or phone apps making coin for someone else on the side, check your device's privacy settings and adjust accordingly when possible. That free internet stuff can be a fair trade, but be sure you're accepting those freebies with your eyes cybermindfully open!

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