

# Cybersecurity Awareness Month



TECHNOLOGY SERVICES



Thank you to Acadia Life Long Learning for having us present to you on this important topic.  
Thank you to National Security Alliance and its partners, and KnowBe4 for their resources.



**400+ Billion:** Annual cost to the global economy from cybercrime



**300:** Average cost per record associated with a data breach



**229:** Average number of days presence maintained before detection



**2.5 Million:** Spam emails blocked monthly by Technology Services



**50:** Percent of recipients open phishing emails and click on links within first hour of receipt



**99.9:** Percent of exploited vulnerabilities were compromised more than 1 year after breach was reported

Really should be saying, just a month – this is on our minds all the time and keeps me up at night

2.5 million is 80% of all emails that come into our network are spam; but some still get through



4<https://cofense.com/enterprise-phishing-susceptibility-report>

52017 Data Breach Investigations Report, 10th Edition. Verizon.

6Data Breach Digest. Verizon.

7<https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states>EDUCAUSE and REN-ISAC

Tell Facebook Story

According to AIG (insurance company giant) AIG Cyber Insurance Claims (2018)

Or in an IBM Ponemon Report, 2018: 28% Malicious intent; 27% Human Error; 25% System glitch



## EVERY CLICK, SHARE, SEND, POST YOU MAKE CREATES A DIGITAL TRAIL

### OWN IT.

Understand your digital profile.

Understand the devices and applications you use every day to help keep you and your information safe and secure.

### SECURE IT.

Secure your digital profile.

Protect against cyber threats by learning about security features available on the equipment and software you use.

### PROTECT IT.

Maintain your digital profile.

Be familiar with and routinely check privacy settings to help protect your privacy and limit cybercrimes.

TAKE PROACTIVE STEPS TO ENHANCE CYBERSECURITY AT HOME AND IN THE  
WORKPLACE

### **NCSAM 2019 Theme – Own IT. Secure IT. Protect IT.**

Over the month of October, we'll be exploring these themes and providing information on them. Watch for them.

Stay Safe Online – EDUCAUSE Connected; organization out of the US.

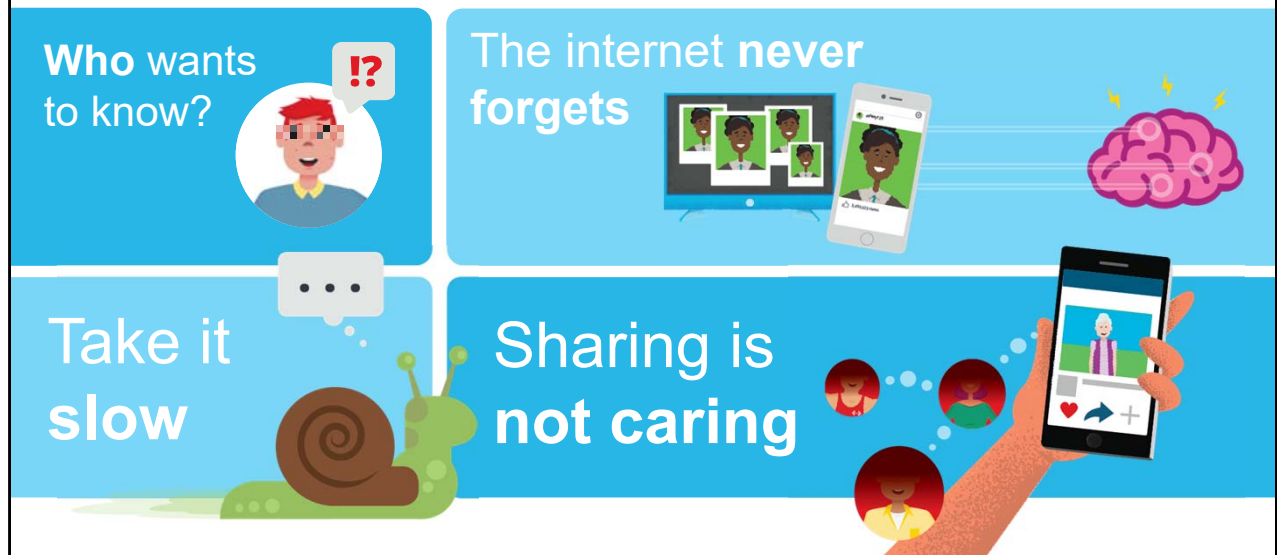
National CyberSecurity Alliance

Just give you some of the highlights...

# Themes Agenda

- Own IT
  - Social media
  - Privacy Settings
  - Best practices for device applications
- Secure IT
  - Passphrases
  - Multi-factor authentication
  - Shop Safely
  - Phishing
- Protect IT
  - Updating to the latest security software, web browser and operating systems
  - Wi-Fi safety
  - Keeping our data and information safe

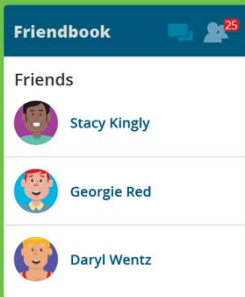
# Own IT: Social media



- There are 3 billion people on the internet and not everyone is who they say they are. Don't friend people you haven't met in real life. And consider that people may try to "friend" you based on information that's publicly available about you. Sometimes people friend or link to you in an attempt to defraud you; sometimes they're trying to target one of your contacts and they're just using you to get to that person.
- Everything is forever. Nothing on the internet ever really goes away forever so when you post, assume EVERYONE will be able to see what you're posting. Never presume privacy – that includes email
- The great thing about social media is sharing and staying in touch with people – the downside is that information can also be used to trick or impersonate you. Having a social media account increases the chance of ID theft by 46%. Also, 40% of consumers across the world have been targets of ID theft at least once, and 1.3 million children have their identities stolen every year
- Think before you click. Take a second to read and think before you click. The bad guys know that everyone is busy and working quickly, and they take advantage of that. One of the best tips to staying more secure with everything – social media, email, app permission, everything – is to slow down.

# Own IT: Privacy settings

## A few good friends



## Bad share day



## Location unknown



Sync and personalize across your devices

Turn off sync...

Sign out

## Syncing ship

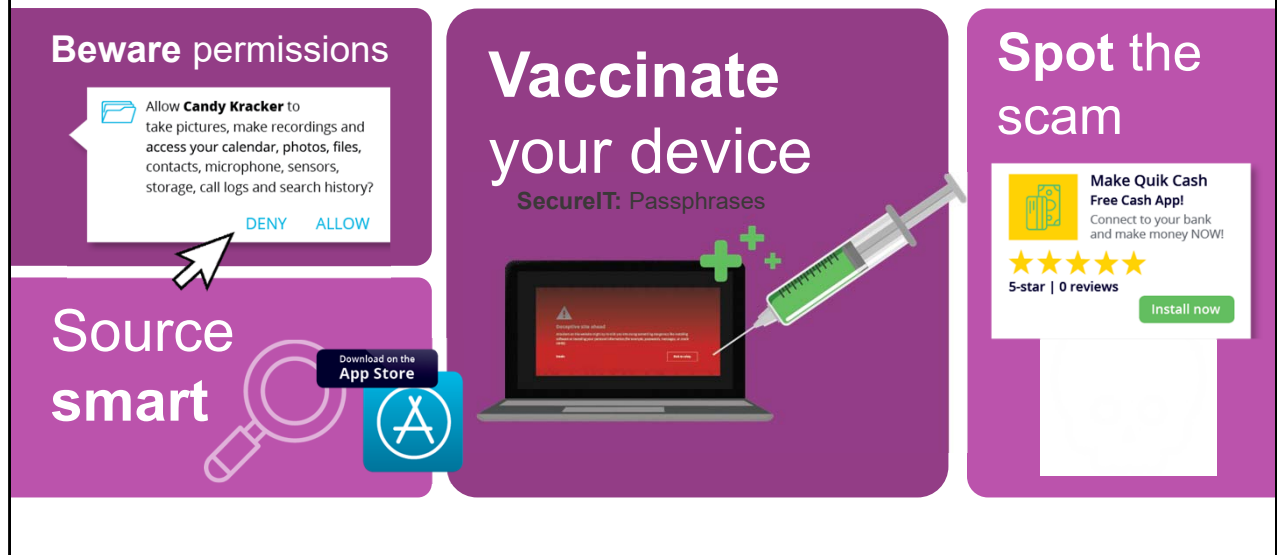
## Lockdown



### Talk track:

- Privacy on social media: limit your friends list to ACTUAL friends, and restrict what you post to friends only. Check under Settings on all your social media apps and change your privacy settings as appropriate
- Unique Account; Unique Password. Don't log into one app or account using another. Don't use FB or Google to create an account in another app. It means those apps are sharing data about you.
- If syncing is enabled on your accounts (between apps), and your device or account is compromised, you haven't just made life easier for yourself, you've also made it easier for the attacker. Consider syncing manually instead of enabling it automatically.
- Does every app and device you use really need to know your location? Allow this sparingly, like for maps and navigation only.
- Always use a lock screen on ALL of your devices, and enabling encryption will mean that even if someone gets past your lock screen, your data is secure

# Own IT: Device applications



- Pay attention to permissions you're granting when you install or use apps. Slow down and read the fine print. Do they really need to know your location, or have access to our photos or contacts?
- Only use apps from a reputable provider
- Apps that look too good to be true usually are – like all 5-star reviews
- Keep your antivirus up to date – it adds a layer of protection against malicious apps



# Secure IT: Passphrases

Longer and  
**stronger**



Mix and match

Irezumi

Coelophysis

**Ditch the digits?**



Thinking in **sentences**

jst4sm4llt0wngr!!lvnngn4l0nelyw0rld!!  
t00kth3mdnghttr4ng0ng4nwh3r3!!!\_

- Passwords and passphrases – the longer they are, the harder they are to crack
- Complexity is helpful – numbers, letters, upper and lower case, special characters – but length is key
- You can use passphrases or even sentences – and a password manager can help you keep it all straight
- Unique account; unique password
- Password safe
- Think of a password like a toothbrush – choose a good one; don't share it; don't reuse

# Secure IT: Multi-factor authentication

**Two locks are better than one**



**To have and have not**



**The eyes have it**



- Enable multi-factor authentication on every account possible (social media, email, etc.).
- Having two or more authentication steps makes it harder for an attacker to breach your account. Authentication just means how you prove that you are you. Multi-factor can be made up of something you have, something you are, something you know...like having an ATM card and knowing a PIN. Something you are includes biometrics, like your fingerprint, or an iris scan.
- If someone knows your password, but doesn't have access to a code texted to your phone, you are protected

# Secure IT: Safe shopping

Don't reuse passwords



Look for the S



Link and  
you'll miss it

Click here



<http://filledwithviruses.com/haxyouraccounts/>



Spot the  
scam



- When shopping online, create unique accounts for every shopping site and use a unique password for each (which you can manage with a password manager).
- Don't click on links in emails from merchants or shippers – navigate to the site yourself and use bookmarks for convenience instead of clicking on links in emails
- If something looks too good to be true, it probably is! Check the BBB and online review sites.
- The "S" in https stands for secure. Look for that on the sites you're shopping

# Secure IT: Phishing

Friend or  
foe?

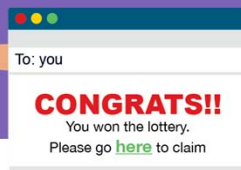


Hey I spoke to Lisa yesterday and she said I should contact you directly. send me a friend request so I can transfer you that money now



Slow and  
steady

Too good to be true



Phish fight



- The telltale signs of phishing: too good to be true, a sense of urgency, fake familiarity.
- Slow down and take the time to read before you click
- Remember, phishers use information that's publicly available about you to make you think you know them, or to make them seem more credible to you.
- Use caution- look closely at the sender's address. Don't download any attachments if the email seems phishy, and don't click on links. Attachments and links can lead to malware infections
- You can forward the email to see the from email address
- Read the URL – hover over the link; On your phone: hold and press to read the URL

# Protect IT: Updates

Always  
Update



Source matters

 **DOWNLOAD NOW YOU'RE INFECTED**

License to fail



Shield your system  
with **auto-update**



**Deceptive site ahead**

Attackers on this website might try to trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, messages, or credit cards).

Back to safety

Click  
attack



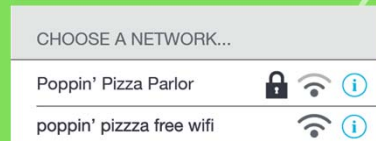
- Don't ignore updates! We get busy and they always seem to pop up at the most inconvenient times, but most updates are primarily security updates, so run them asap. Cyber security is an arms race with the cyber criminals constantly updating their attacks, so your technology providers are constantly updating their defenses. If you don't run those updates, you're lagging behind and are more vulnerable.
- Set your devices and systems to auto-update
- All your devices – anything you can think of – that is connected to the internet.
- Be on the lookout for fake update warnings. Bad guys use those too to try to trick us
- Never use unlicensed versions of software or an operating system – they frequently carry malware. Only download software updates from reputable sources.

# Protect IT: Wi-Fi

Public has **no privacy**



**Spot the copycat**



Auto-connect is **not correct**



**Password preferred**



- If you're using public wi-fi, use a VPN (virtual private network). If you don't have access to a VPN, avoid public wi-fi to access your email or important accounts like your bank account
- Hackers will often spoof a network name as a copycat without password protection to trick you into using them. Always confirm that you're using the network you're supposed to be using at a hotel or restaurant.
- Don't enable your devices to auto-connect to networks. Carefully choose the network you want to use.
- If you can't use a network that's password protected, use a VPN

# Protect IT: Data

Less is more



By the book



Sharing isn't caring



Lockdown



Who goes there?



Shred and buried



- Privacy legislation that affects us all – Nova Scotia FOIPOP and PIIDPA and federally PIDEPA.
- Collection, use, retention, disclosure, security,
- If you collect it, you are bound to protect it.
- The less data you have, the less you have to protect. This is true of storing your own information as well as anybody else's for which you are a steward.
- Physical and digital information should be stored, shared, and destroyed in accordance with company policy



## Resources

**Check your email breach status:**  
<https://haveibeenpwned.com/>

**KnowBe4:** <https://knowbe4.com>

**Stay Safe Online:**  
<https://staysafeonline.org/>

**Acadia Technology Services:**

- [hub.acadiu.ca](https://hub.acadiu.ca)
- <https://ts.acadiu.ca/home.html>; and
- <https://datasecurity.acadiu.ca/home.html>

**Twitter:** @TSAcadia

**Facebook:** Acadia Technology Services

16



# Thank You

Questions





# Domain Doppelgänger