Staying Safe Online

Brought to you by Digital Kitchener
Steve Asmundson – Supervisor Network Systems
Sarah-Beth Bianchi – Manager Digital Transformation & Strategy

Digital Kitchener

Connected

On Demand

Innovative

Inclusive

In a digital city, access is equality. By improving capacity to support digital literacy and increased access to tech, Kitchener can be a city where no citizen is left behind, ensuring that all citizens have equitable access to the benefits of a smart city.

Cybersecurity

- Q: What exactly is cybersecurity? Is it just for hacking, viruses, worms, trojans & the like?
- A: Cybersecurity is the practice of protecting the Confidentiality, Integrity and Availability of your information.

Passwords: Length

- Q: What are the best passwords to use?
- A: Longer is better!
  - Use pass phrases whenever possible - they're easier to remember and they're always long.
  - Self-affirmation works wonders as well - how fantastic is it if you type "I am beautiful.” or “Living my best life!” every time you log in?

Passwords: Variety

- Q: Do I have to have different passwords for everything?
- A: It's best if you do. If a service you totally forgot about is compromised and your password is out there, then it could be used to log into something else…
- Tip: Google released a new Password Checkup extension for the Chrome browser that will alert you when any credentials you use are known by Google to be unsafe.

Online shopping

- Q: More and more purchases are online. How do we know our credit card info will be safe? How do we know which companies and websites are real?
- A: Develop good online shopping habits
  - Don't click on links to visit shopping websites. Browse to the site directly, typing in the web address, then navigate to what you're looking for. This habit prevents you from being lured to an unsafe site.
  - Look for the lock or https:// in the web browser address bar. This shows that the communication between your computer and that website is secured from others.
  - Don't do sensitive or private transactions on public Wi-Fi. This protects your transactions from being monitored or disrupted by bad actors.
  - Use Google/Bing/Duck Duck Go to find out more about any company you're transacting with. If you can’t find much info about the vendor or website, trying doing your shopping elsewhere.

Online banking

- Q: How secure is online banking?
- A: Online banking sites are secure… but is your device?
  - Your banking transactions are only as safe as your device! It's super important to use good passwords/PIN/Fingerprint ID on your computer or smartphone before engaging in online banking.
  - Banking is heavily regulated, with strong practices to secure your money and their infrastructure. Stick to the apps provided by the major banks.
  - Never go to a banking site from a link provided in email. Always browse directly to the banking website to avoid being lured to enter your credentials in a fake site.
  - Use multi-factor authentication.

Zoombombing

- Q: Are you familiar with some of the security challenges associated with Zoom and the recent trend of "zoombombing" where people drop in on Zoom sessions uninvited?
- A: Zoom and other video chat apps can be vulnerable to bad actors joining or disrupting unsecured meetings. Develop good habits to help make your video chat sessions more secure:
  - Use a Unique ID for each meeting.
  - Require a Meeting Password.
  - Create a Waiting Room.
  - Create an Invite-Only Meeting.
  - Lock a Meeting Once It Starts.
  - Disable “Allow removed participants to rejoin”.
- Resources:
  - https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing
  - https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-preventing-zoom-bombing
  - https://www.nytimes.com/2020/04/07/style/zoom-security-tips.html

Video chat

- Q: How can I stay safe while connecting with family and friends on video calls?
- A: Develop good video chat habits
  - If possible, do direct person-to-person. (Facetime, Facebook Messenger, Google Meet). This habit prevents generating meeting links that bad actors can discover and use.
  - For group meetings, set unique meeting IDs and set meeting passwords. This habit makes it more difficult for bad actors to gain access.
  - When in doubt - hang up!
- Important: don't use Zoom for anything private or sensitive – like banking info or other personal details (especially the chat function). Even "private" Zoom chats can be transcribed.
  - Clicking on file or web links in Zoom or any other videoconferencing app carries the same risk as email!
  - Essentially, treat chats like email and don’t click on unfamiliar links or open unexpected attachments.

If you've been compromised

- Q: What do I do if I think I've been compromised?
- A: Don't let embarrassment or uncertainty prevent you from protecting yourself!
  - Yes, it might be uncomfortable to seek help. But it's better than losing money or peace of mind. In many cases, these are professionals who have a lot of experience scamming people.
  - Contact the police non-emergency number. (Depends on police agency. Waterloo Region Police Services has a cybersecurity division.)
  - Change all your passwords. Use different passwords for everything.
  - If you used a credit card number or released any banking info to a questionable source, contact your bank as soon as possible. They might be able to help block the transaction, recover the funds, cancel the accounts, etc.

Staying cybersecure

- Q: How do seniors stay abreast of developments to stay cyber secure?
- A: Find reliable, evidence-based resources to stay informed.
  - Get Cyber Safe https://www.getcybersafe.gc.ca/
  - Canadian Centre for Cyber Security https://www.cyber.gc.ca/en/
  - Canadian Anti-Fraud Centre https://www.antifraudcentre-centreantifraude.ca/
  - You can monitor your email address to be notified if it's been involved in any data breach via https://haveibeenpwned.com/.
  - Your local police service or OPP
    - https://www.wrps.on.ca/en/staying-safe/seniors_-safety.aspx
    - https://www.wrps.on.ca/en/staying-safe/prevention-and-awareness.aspx
    - https://www.wrps.on.ca/en/staying-safe/online-crime-safety.aspx
    - https://www.wrps.on.ca/en/services-reporting/online-reporting-.aspx
  - Watch the news - television, print, online… Cybersecurity is increasingly visible in the news. When you hear something, do more research to determine if it’s accurate and relevant to you.

Questions?

- We’ll send the slides so that you can see our content, click the links