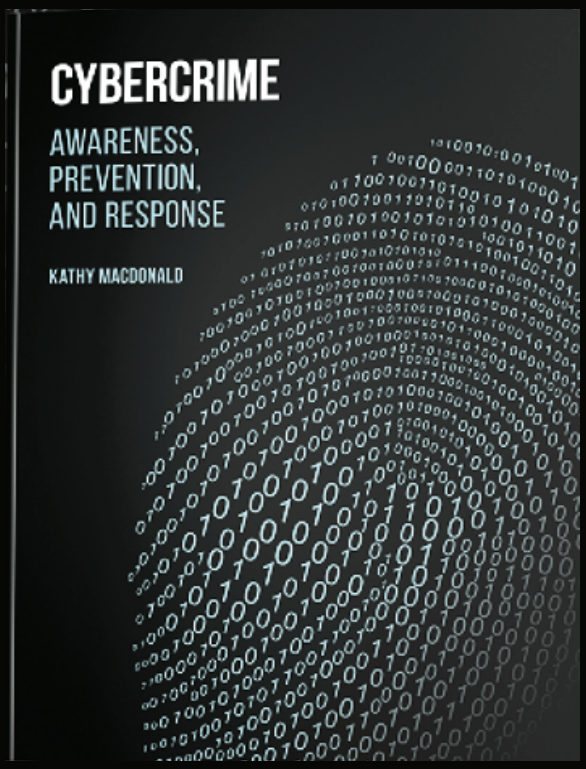


CYBERCRIME: Awareness, Prevention, and Response

The first Canadian resource of its kind to effectively address the role of technology in the criminal world.

Order Today
emond.ca/CAPR

This information sheet helps to keep you, your family, and your business safer, and more secure online

THREATS - PHISHING - SPEAR PHISHING - BUSINESS EMAIL COMPROMISE (BEC) - RANSOMWARE ATTACKS

These threats can contribute to personal, financial, corporate and intellectual property loss. The following indicators may help you recognize and avoid risk:

- The sender's email address may seem illegitimate.
- The email or text may be sent from a privileged person within a company that has never communicated with you in the past.
- The time and date may be suspicious, i.e. late in the day, in the middle of the night.
- The subject line may be suspicious, i.e. emotional tones, urgency, overtly friendly.
- The email or text may be unexpected, have an unusual request or seem out of place.
- The email or text may contain grammatical errors, inconsistent language and fonts, spelling mistakes, or syntax errors
- The email or text may seem to be adapted from a template.
- The email or text may infer threats related to you visiting illicit websites or viewing compromising images.
- The email may include visuals or logos of a legitimate company and may instruct you to click a weblink or ask you to download or open an attachment.
- The email or text may ask you to call a phone number, visit a specific website, complete a survey, purchase gift cards, or send a file.
- The email or text may generate an emotional response from you such as fear, panic, worry, urgency, sadness or excitement.

THREATS - PHISHING - SPEAR PHISHING - BUSINESS EMAIL COMPROMISE (BEC) - RANSOMWARE ATTACKS

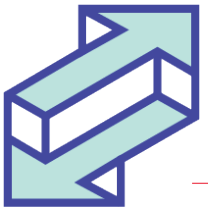
- The email or text may use the name of a company or mention an actual employee in your company. This name could have been easily found in an open source search.
- The email or text, may direct you to click on a web-link that you would otherwise use within your company, i.e. an association, union or supplier. If so, visit the website independent of the sent link.
- A person with authority in your company has asked you for help, or instructed you to do something important to them that seems out of the ordinary
- The email or text includes images or website URL's that are similar but slightly different from the legitimate business.
- The email or text includes a request for you to complete a form with personal information, a credit card number or a PIN number.
- When you hover your mouse over a link in the email or text (without clicking on it) you notice a different web page address or email address than referenced.
- You notice a spelling variation in the URL or in the domain name. It may be spelled slightly different from the name you know and trust i.e. a .net instead of .com.

REMEMBER: BE CAUTIOUS WHENEVER YOU ARE OPENING WEB-LINKS, CLICKING ON EMBEDDED LINKS OR OPENING ATTACHMENTS IN EMAILS.

How to respond if you believe the email or text is phishing or spear-phishing?

Report suspicious email and texts to your IT security department by following work policy. This is important particularly if it involves your company brand or if it imitates an employee within your company or anyone associated to your organization.

Don't respond to any email or text that asks you to provide confidential data unless you have initiated the request. Emails should be personalized to you in the body of the email only if you are expecting this communication. Block suspicious senders and report spam rather than simply deleting it. Be skeptical, take your time.



BEING PROACTIVE - VIRTUAL MEETING PLATFORMS

With the increasing use of virtual meeting platforms for meetings, IC3 has offered the following safeguards to help secure these environments.

https://www.ic3.gov/Media/Y2022/PSA220216

- Confirm the use of outside virtual meeting platforms not normally utilized in your internal office setting.
- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business/individual it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII of any sort via email. Be aware that many emails requesting your personal information may appear to be legitimate.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.
- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.

SOCIAL ENGINEERING

Social engineering attacks deploy tactics, techniques and procedures (TTP) that are meant to attack our state of mind. We are more vulnerable when our state of mind is stressed, distracted, disrupted and in a state of chaos.

- Anonymity - tactics that can hide an identity, a location or a device i.e VPN, Tor, temporary texting/emailing apps.
- Background noises - apps may be used to add content to support a fake story.
- Demeanour - the actor's attitude may appear friendly, forceful, generous or mean.
- Disguises - use of GAN photos, fraudulently obtained PII, & synthetic identification.
- Emotions - tactics that use fear, urgency, trust, excitement, love, hate, sadness to overpower rational decision making.
- Expert opinion - use of credentials i.e. doctor, scientist, to compel a target by following an actor that is perceived to be an expert.

- Herd mentality - use of multiple personas that may be orchestrated by a single actor to steer decision-making and critical thought.
- Pretext - use of a well crafted story that may be official-sounding, scripted and researched to include knowledge of schedules, locations and business concerns.
- Professional materials - use of business cards, uniforms, badges, brochures.
- Timing - this attack may coincide when the target is most distracted i.e. pandemics, weddings, funerals, mergers, disasters, political events, tax time, fires or floods.
- Volumetric attack - maximizing effectiveness by overwhelming a target and creating chaos. Using password cracking software, credential stuffing attacks, subscription bombing and phishing.

Actively defend against social engineering using this RISK model.

BE:

RATIONAL

INDEPENDENT

SKEPTICAL

KIND

DIGITAL SAFETY WHILE WORKING FROM HOME

- Contact your IT security department to learn about company policy related to devices, network access, and security protocols while working from home.
- Use a dedicated workspace to keep work and home life separate.
- Have the direct phone numbers to IT security, your work supervisors, and colleagues, in the event you need to contact them from home.
- Reduce and mitigate risk by making sure all your devices have been updated and patched, and that you have anti-virus software installed and activated.
- Check with your Internet Service Provider to have enough bandwidth to connect several concurrent devices remotely without adversely affecting performance.
- Remember to secure data and documents through the entire chain of custody including the collection, use and disclosure of personally identifiable information.
- Shred your sensitive data using a cross-cut or micro shredder.
- Transport sensitive documents back to the office for disposal, or use the services of a secure destruction company for electronic devices such as the Electronic Recycling Association.

https://www.electronicrecyclingassociation.ca/locations-ca/

- Be diligent when using your personal cellphone to make phone calls to people. Consider whether you wish to show your caller identification.
- Cover your web camera lens when you are not using it. This reduces the risk of a hacker accessing your webcam to surveil you.
- Turn off your video when joining conferencing platforms. Always behave on-screen like your microphone and camera are activated.

REMEMBER: VERIFY BEFORE YOU ALLOW ANYONE PHYSICAL ACCESS TO YOUR OFFICE, CONTROL OF YOUR COMPUTER OR PHYSICAL POSSESSION OF YOUR CREDIT CARD.

PASSWORD SAFETY

- Make passwords easy for you to remember but difficult for others to guess.
- A good password may be comprised by stringing three random words together then interspersed with numbers, upper and lower characters and special characters.
- Change your passwords frequently. Never reuse your passwords, even on different websites. This helps to prevent credential stuffing attacks.
- Change your passwords immediately if you split with your significant other, if you are a victim of a housebreaking or a car-prowling, or if you are compromised in any way.
- Use a 'Password Manager' to securely manage all of your passwords.
- Set up your 2-Factor (2FA) or Multi-Factor (MFA) authentication wherever it is available. For more information on 2FA visit, **https://twofactorauth.org**
- Passcode protect your mobile device with a complex passcode that activates immediately when your phone is not active.
- Don't use personal information in a password, or use easily guessed information that you may have posted in a public profile on social media.
- Monitor your email addresses and passwords to monitor and take action in the event that they have ever been breached. To check please visit: **HAVEIBEENPWNED.COM**

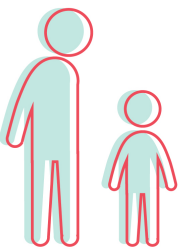
REMEMBER: MAKE SURE YOUR PASSWORD IS NOT READILY FOUND ON A DATABASE OR IN A DICTIONARY.

SOCIAL MEDIA

- Check your status on websites that you are currently using, or on websites that you have joined in the past. Delete and remove old accounts if you are no longer using or needing them.
- Delete posts that overshare too much personally identifiable information (PII), or that reveal sensitive data about your family or business.
- Take some time (at least once a month) to review and check the privacy settings you use on social media.
- Before deleting a social media account request an archive of past activity.
- Check your privacy settings on your mobile device to monitor the "Location Services." Turn off the metadata that is collected via microphone or camera on apps that you may be using.
- Post photos from a holiday after you return home.
- Ask for consent before posting other people's photos in social media. Strive to not overshare PII in social media.
- Know your friends and followers. Delete and unfriend at will.

ONLINE SAFETY

- Be cautious at free public WiFi hotspots to avoid unprotected public wireless connections, particularly when logging into a website with your credentials. Confirm a WiFi network with the host. When travelling, use a Virtual Private Network (VPN) service whenever possible.
- A lock icon or “https” in the browser address bar does not mean that a URL is 100% safe or secure.
- Retain physical control of your mobile device in public locations. If you are unable to carry your device, lock it out of sight in a secure location.
- Minimize the collection and the amount of data you carry on your mobile device.
- Make sure your laptops and mobile devices use a passcode.
- Back-up the data from your laptop and mobile devices on a regular basis.
- Install antivirus software with automatic updates and keep the operating system and all software up to date.



Resources: **getcybersafe.ca**
https://www.antifraudcentre-centreantifraude.ca

REMEMBER: DO NOT SEND COMPROMISING IMAGES OF YOURSELF TO ANYONE, NO MATTER WHO THEY ARE – OR WHO THEY SAY THEY ARE

LURING AND CYBERBULLYING

Responding to Internet Abuse and Predatory Behaviour.

- It is against the law in Canada to communicate online with a person under the age of 18 for a sexual purpose. Report incidents of this nature to police.
- It is illegal to distribute an intimate image without the consent of the person in the image. This person can be of any age, and at the time the photo/video was taken there would have been an expectation of privacy. cybertip.ca
- Be judicious, in most cases do not respond to inciting incidents directly. Take screenshots and gather evidence of offensive material, the date/time it was viewed and the URL. Retain offensive material for ongoing reference.
- If abuse continues, block and delete this connection.
- Change your passwords. If warranted, reduce your digital footprint.
- Seek help, file a report with police, call a HelpLine/HotLine, talk to family/friends, call a lawyer, young people may seek support from **Kids Help Phone**
- DO NOT PAY or NEGOTIATE with pornography websites to remove your images for a fee.
- Monitor the situation. Report Abuse: Contact the website in question, your Internet Service Provider, a school or a workplace.
- Consider hiring a DMCA Takedown service, reputation service or online investigator.
- Prevent ongoing risk by stopping your cellphone from automatically backing your photos to the cloud.

ADVISE YOUNG PEOPLE THAT IT IS SAFE TO TALK TO YOU ABOUT ANYTHING THAT HAPPENS TO THEM ONLINE.

ENDING A RELATIONSHIP? BE PROACTIVE.

- Immediately change all your passwords;
- Be suspicious if you have an increase in telephone hangups, unexpected text messages and emails;
- Check your mobile device for any spyware or hidden apps that may have been installed or uploaded without your knowledge.

DIGITAL ESTATE PLANNING

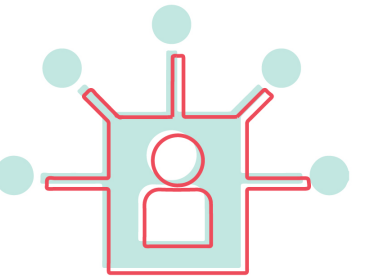
Consider naming a Digital Executor to remove your personal information from social networks if you are unable to do so. For example, Facebook, Twitter, or LinkedIn have created a link to set up a legacy contact. This is the type of information that should be removed by your digital estate planner:

- blogs and licensed domain names
- your presence in online communities or listserves
- music, photos, or other files that you store online
- seller accounts on Amazon, eBay, or Etsy, and access to financial accounts, PayPal or utilities.

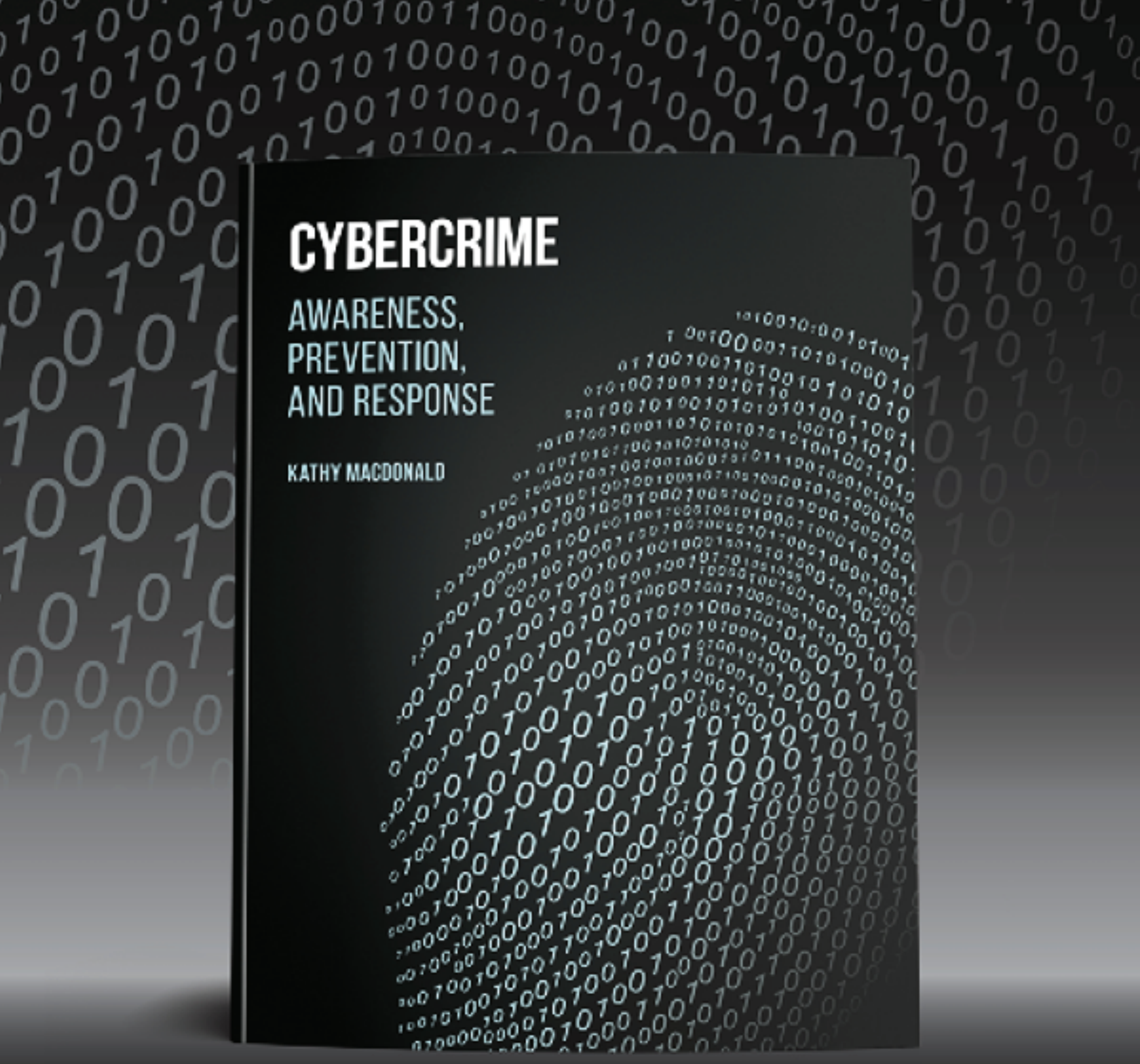
OWN YOUR ONLINE IDENTITY

- Set up “ALERTS” to monitor your brand, name & image at **www.google.com/alerts**
- If you find personal information on the Internet that you would like removed, identify yourself as the person in the picture/video and file a complaint about the posting of the content with the website.
- Request removal from a website through a "Contact Us" or "Report Abuse" link. Provide a police case number if you have one. Don't give up if they refuse.
- Check to determine if a photo can be located online by using a reverse image search such as tineye.com. Once located hire a takedown request service or serve a "DMCA Takedown Request" to help remove offending material from a website.

On an annual basis conduct a credit bureau review.
Canada: Equifax Credit Bureau, Fraud Dept.
Phone: 1-800-465-7166
www.equifax.ca
TransUnion Credit Bureau, Fraud Dept.
Phone: 1-800-663-9980
www.transunion.ca



REMEMBER: IF YOU HAVE BEEN A VICTIM OF A CAR-PROWLING, HOUSEBREAKING, IDENTITY CRIME OR A CYBERCRIME INCIDENT, PLACE A “FRAUD ALERT” ON YOUR CREDIT FILE.



For more information or to book a presentation
please contact:

Kathy Macdonald, MOM, MSc., CPP
kathy@kathymacdonald.ca
1.587.896.2801 ©

FAMILY AGREEMENT FOR THE USE OF TECHNOLOGY

Parents and caregivers often ask how to keep their child safe and secure. This agreement is a guideline. It is meant to help safeguard young children as they navigate the Internet and begin to establish their digital footprints.

WE AGREE:

I understand that being safe on the Internet is important to our family.
I wil try my best to be careful, respectful, and responsible whenever I am online.

I wil always try to be kind to people online, not fight, swear, or be mean to others.

I wil promptly ask for help by talking to my parent(s) or my caregiver(s) when:

I am asked to share my personally identifiable information (PII) online.
- I feel afraid or if I am being asked to do something that makes me feel unsafe.
- I need help to make my passwords long, strong and unique.
- I am asked to meet a person in the real world that I have only met online.
- I see something that I believe is unethical, illegal, or incorrect.
- I want to download an app that my parents or caregivers have not yet approved.
- I receive an email or a text from someone I do not know.
- I am sent a nude or semi-nude photo or video.
- I am asked for financial information, an account number or a credit card number.
- I am buying, selling, or registering for a product or a service.
- I am being asked to send a photo or a video of myself to someone.
- I feel I am being tricked or threatened.
- I receive a gift or a gift card from someone.

(Parent or Caregiver) I agree to help my child follow these rules. I agree to allow reasonable use of the Internet as long as these rules and other family rules are followed.

Signed (Child) _____

Signed (Parent/Caregiver) _____

Date _____