LE CENTRE Cummings CENTRE

SUMMARY PAGE – PROTECT YOURSELF - MARCH 16, 26 WEBINAR FEATURING ERIC OUIMET

PART 1: THAT DEVICE IN YOUR HAND IS A PORTAL

- The average adult in Quebec will spend over 3.5 hours per day on their phone.
- The device we carry around with us isn't just a phone anymore, it's a camera, our music library, how we order cars and food. It is also a multi-function tool for communication.
- This "Portal" allows us to communicate with anyone, instantly. At the same time, it also allows anyone to contact us directly.
- Fraud and scams are not limited by borders; anyone and everyone can be a target.

PART 2: SCAMMERS ARE TRAINED, SPECIALIZED AND EXTREMELY WELL ORGANIZED

- Scammers can range from one-person to a multi-level organization with hundreds of employees. They operate all over the world with some countries specializing in specific scams: tech support scams in India, romance schemes in Nigeria and the grandparents scam all across North America.
- 'Scammers' may be willing employees, others can be forced labour, working under stressful conditions.
- Scammers do not discriminate; they only see money.

The three basic methods used to scam people:

- WIDE TARGET: A widespread message sent to a random group of recipients - Example: a text message, email or automated call claiming to be Visa or the CRA.
- NARROW TARGET: A message sent to a group with a common link - Example: an email sent to everyone from a specific church group asking to buy gift cards.
- PINPOINTED TO YOU: A message or call targeting you personally - Ex: Romance Scams.

PART 3: LET'S TALK STRATEGY

- The most effective strategy to protect yourself from scams is the confidence in yourself to be skeptical and ask questions. Trust your gut and don't accept easy or dismissive answers.
- Remember the 3U rule to spot *Red Flags* (Warnings):
  - Unknown (Someone contacting you who you do not recognize).
  - Unexpected (A message out of the blue meant to pique your curiosity).
  - Urgent (Someone pressuring you to make a financial decision, can be good or bad).
- Be Aware of your emotions.
  - Scammers weaponize your emotions against you.
  - They will try to isolate you and keep you from telling anyone.
  - Scams rely entirely on your emotional commitment to their trick. Once you question the emotional component, the scam falls apart. Also, no real emergency requires secrecy!
- Good Digital Habits.
  - Have a strong password and don't ever share it. Your email password needs to be the strongest.
  - Digital Privacy: know what to share and what not to share online.
  - Don't follow random links, instead go through the source.
  - Two-Factor authentication is very effective, enable it when you have that option.
  - Run those updates! Especially on your mobile device and apps you use regularly.

PART 4: THE STIGMA WITH SCAMS

- The negative feeling attached to fraud. It's what makes us hide it instead of talking about it.
- Stigma can occur BEFORE or AFTER a scam has occurred.
- Scams need stigma: Silence helps fraud continue.
- If you have been a victim of an attempted or successful scam;
  - Talk about it.
  - Report it.
  - Learn from it.

RESOURCES

SOME USEFUL & HELPFUL LINKS

Reporting Scams, Fraud and ID Theft:

- Competition Bureau of Canada fraud reporting: **LINK**
- Canadian Anti-Fraud Centre (CAFC): **LINK**
- Sûreté Du Quebec Victim Guidance: **LINK**

Canadian Cyber Safety Guidance and Tips:

- Get Cyber Safe Canada: **LINK**

Check to see if your email address has been compromised:

- Have I Been Pwned: **LINK**

Check to see if a link is safe:

- Bitdefender Link Checker: **LINK**

Helpful tips to create a strong password:

- Government of Canada recommended tips to build a strong password: **LINK**

Facebook Privacy Checkup Information:

- A walkthrough on how to make your Facebook more private: **LINK**

Eric Ouimet Contact Information:

- www.anticipa.ca
- LinkedIn Profile