October was Cyber Security Month

Office of the Privacy Commissioner of Canada

- The Federal Government enacted a law requiring that companies report data breaches to OPC, it has been in effect since Nov. 2018.
- 19 million Canadians have been hacked in 446 breaches in the 8 months from November 2018 to June 2019
- Sources of violations
  - 59 % from unauthorized access by a hacker or “internal bad actor”
  - 22 % from accidental disclosure (info sent to wrong person or left behind)
  - 13 % from loss of data (files being left behind, USB or even paper files)
  - 6 % from physical theft of computers, thumb drives etc.
- Some public bodies exempt from reporting, so number probably higher

How These Hacks Happen

- Corporate breaches as discussed on previous slide
- Downloading of infected apps or files
- Email scams and phishing
- SIM card switching
- Juice Jacking – public USB charging ports can be hacked by having chips added that can install malware or access your machine contents

Recent Scams and Breaches

- Shoppers Drug Mart Text and Email Scam
  - Asks Shoppers customers to become Secret/Mystery shoppers
  - Warnings posted on Shoppers Website & Facebook page at https://www1.shoppersdrugmart.ca/en/news/secret-shopper-solicitation-fraud

- Apparent Government of Canada Scam
  - Scammers make it appear like real Government phone number is displayed
  - https://www.cbc.ca/news/politics/fraud-spoofing-canada-government-1.5348659

Recent Scams and Breaches

- Desjardin Credit Union Hack – June 2019
  - Updated to 4.2 million users impacted
  - Info taken includes names, addresses, birthdates, SIN nos., email addresses and information about transaction histories
  - Offering 5 years of Equifax monitoring for free to impacted clients
  - Source: https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216

Recent Scams and Breaches

- Phone SIM (Subscriber Identity Module) card switched without owner losing phone. This scam is on the increase.
- Canadian Bankers Association information: https://cba.ca/sim-swap-scam
- Example case:
- A woman had the same Rogers phone no. for 20 years & one day she noticed her phone had no signal, so she went to a Wi-Fi zone and found emails that her PayPal account had been connected to her phone & her credit card had been used to make purchases. She went to a Rogers store & eventually found out her SIM card had been switched remotely. All this happened in less than one hour.
- Source: https://www.insauga.com/a-new-and-terrifying-scam-can-steal-your-phone-number-and-clear-your-bank-accounts-in-mississauga
- https://www.cbc.ca/news/canada/toronto/ontario-provincial-police-sim-swapping-phone-number-porting-1.5354567
- https://www.cbc.ca/news/technology/phone-porting-extortion-1.5352300

In The Event of a SIM Swap

- Contact your service provider
- Find out which company is the new service provider and new number
- Contact new service provider and have new number deactivated
- Work to change all passwords on accounts or files that contain sensitive or sensitive personal information

Who is Right or Wrong or Liable?

- A small business owner used a legal service for his company.
- The lawyer's office invoiced him by email and said to send the deposit to Bank X.
- The business owner then received a second email from the lawyer's secretary saying she was attending the birth of her first grandchild & had to go out of town, please send the money to Bank Y instead.
- The business owner sent the $7000 dollars to Bank Y.
- The lawyer did not receive the money and took the business owner to Small Claims Court.
- The judge decided the business owner should pay the $7000 again. The lawyer's computer system had been hacked & neither party was aware of it.
- Source: https://www.theglobeandmail.com/canada/article-judge-urges-new-laws-in-assigning-liability-for-victims-of-cyberfraud/

Phone Apps with Malware Embedded

- Malicious apps are being hidden inside trivial apps that perform some service like QR reader, image editors, flash lights etc.
- These apps are invariably free and frequently have poor ratings
- The apps may disappear from view but will continue to run, disguised under a system name
- These apps deliver adware generating fraudulent revenue for their operators, unlike useful free apps that rely on adware in their unpaid versions
- Sources: https://www.forbes.com/sites/zakdoffman/2019/10/13/new-android-warning-these-15-malicious-apps-may-be-hiding-on-your-phoneuninstall-now/#295c9401ebe6

And https://www.forbes.com/sites/zakdoffman/2019/11/06/new-google-android-threat-these-7-malicious-apps-may-be-downloading-malware-onto-your-phone/#3971128275af

Package Names of Apps with Malware Embedded

- Free.calls.messages
- Com.a.bluescanner
- Com.bb.image.editor
- Com.cc.image.editor
- Com.d.bluemagentascanner
- Com.doo.keeping
- Com.e.orangeredscanner
- Com.hz.audio
- Cos.mos.comprehensive
- Com.garbage.background.cutout
- Com.hanroom.cutbackground
- Com.jiajia.autocut.photo
- Com.jiakebull.picture.background
- Com.fruit.autocut.photo
- Com.huankuai.autocut.picture

Phone Apps with Malware Embedded

- The apps listed on the previous page had more than 1.3 million installs, 7 more were documented last week
- The last 7 installed backdoors, not adware and then pulled in malware from elsewhere (details on next slide)
- The apps listed on the previous page and the 7 new ones have all been removed from the Google Play store
- There are probably many more out there that have not been discovered
- Malicious apps can hide more dangers than just unwanted ads

How to Check for Hidden Apps

- Tap -> Settings -> Apps & Notifications
  - The most recently opened apps appear in a list at the top of this page
  - If any of the Apps use the generic Android symbol (greenish blue pentagon with white Android silhouette) and generic sounding names then
    - Tap on the icon
    - Tap “Force Stop” followed by “Uninstall”
    - Real system Apps won’t offer an “Uninstall” option and will have a “Disable” option

Ways to Avoid Juice Jacking

- Use your own 110 Volt adapter and a conventional plug-in, not a public USB plug
- Carry a portable charge unit and charge from that
- Charge from your own computer, if feasible
- If using a public USB port directly,
  - Use your own cable, not a public one lying about
  - Use a “data blocker”, https://www.amazon.com/gp/product/B06XGJVHV8/ref=as_li_tl?ie=UTF8&camp=1789&creative=9325&creativeASIN=B06XGJVHV8&linkCode=as2&tag=culinarycasan-20&linkId=7f95b8ba1c38a741f19eaeefb562f45c
  - Say no if your device asks if you “trust this computer”

Resources

- Government of Canada Anti-Fraud Centre
  - http://www.antifraudcentre.ca/index-eng.htm

- OPP Resources
  - Follow the OPP on Twitter (@OPP_News), Facebook or Instagram and use the hashtag #KnowFraud
- CTV News Investigative Journalism
  - https://www.ctvnews.ca/politics/19-million-canadians-have-had-their-data-breached-in-eight-months-1.4572535

Topics to Cover on RCMP Site

- What to do if you experience a cyber incident – things like: cyber crime, spam, phishing, fraud, child exploitation, release of compromising photos
  - https://www.cyber.gc.ca/en/cyber-incidents
- Travelling exhibit
  - https://www.cyber.gc.ca/en/events/cipher-decipher-travelling-exhibition