The Great Cyber Caper

PROTECTING YOUR DATA

Cyber Crime is Soaring

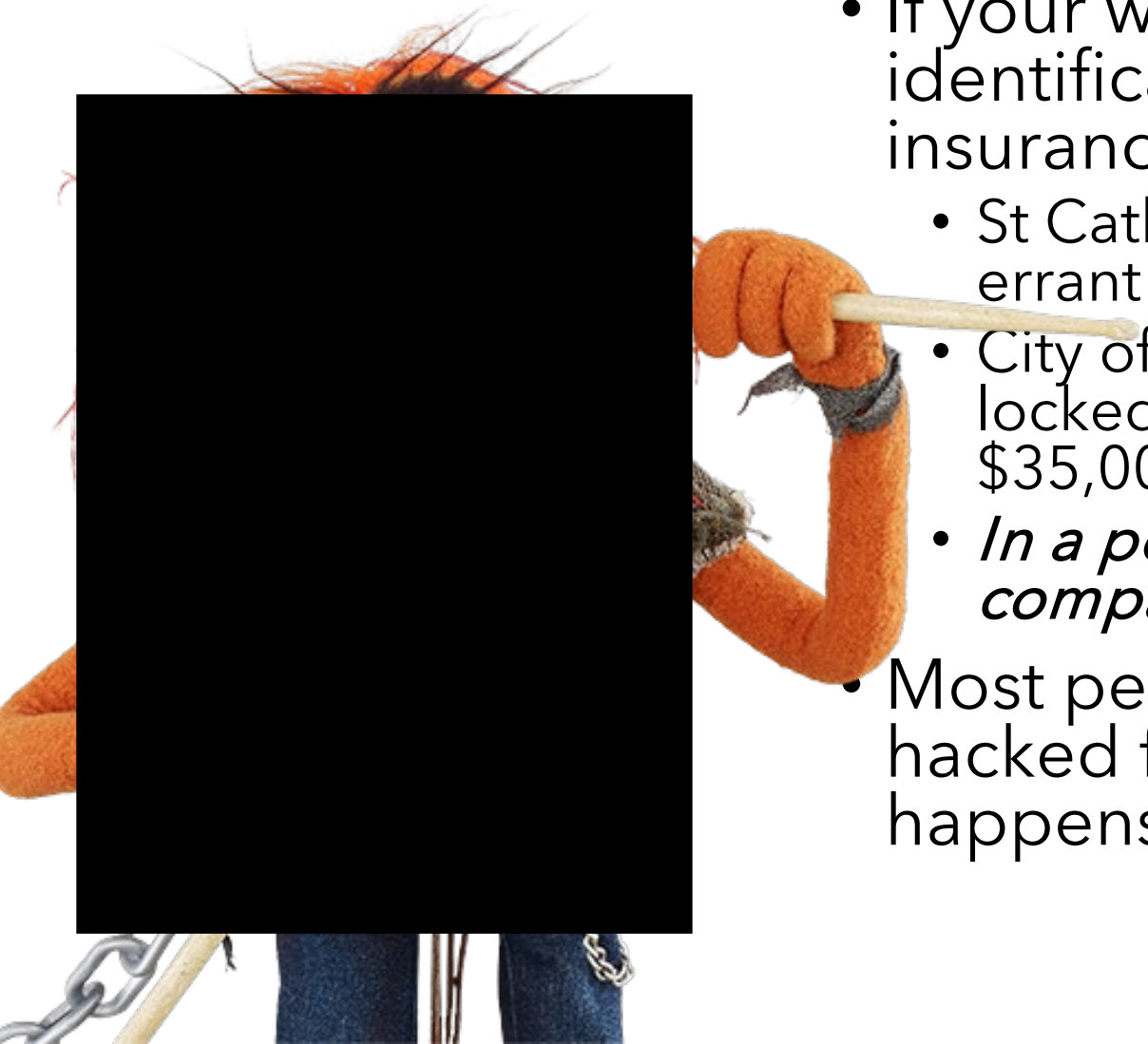
From November 2018 to June 2019

- 19 million Canadians (~ 50%) have had their data breached in 8 months
- 446 breaches were reported to the Office of the Privacy Commissioner of Canada
- 59% were unauthorized access such as hacker or internal bad actor
- 22% were accidental
- 15% due to loss of data (physical and 6% physical theft)

YTD as of October 2019

- Over 20% of Canadian businesses experienced a cybersecurity breach that affected their operations
- $43 Million in losses, and climbing
- Estimated that only ~ 5% of breaches reported
- Unreported ~ 95% represents ~ $1B

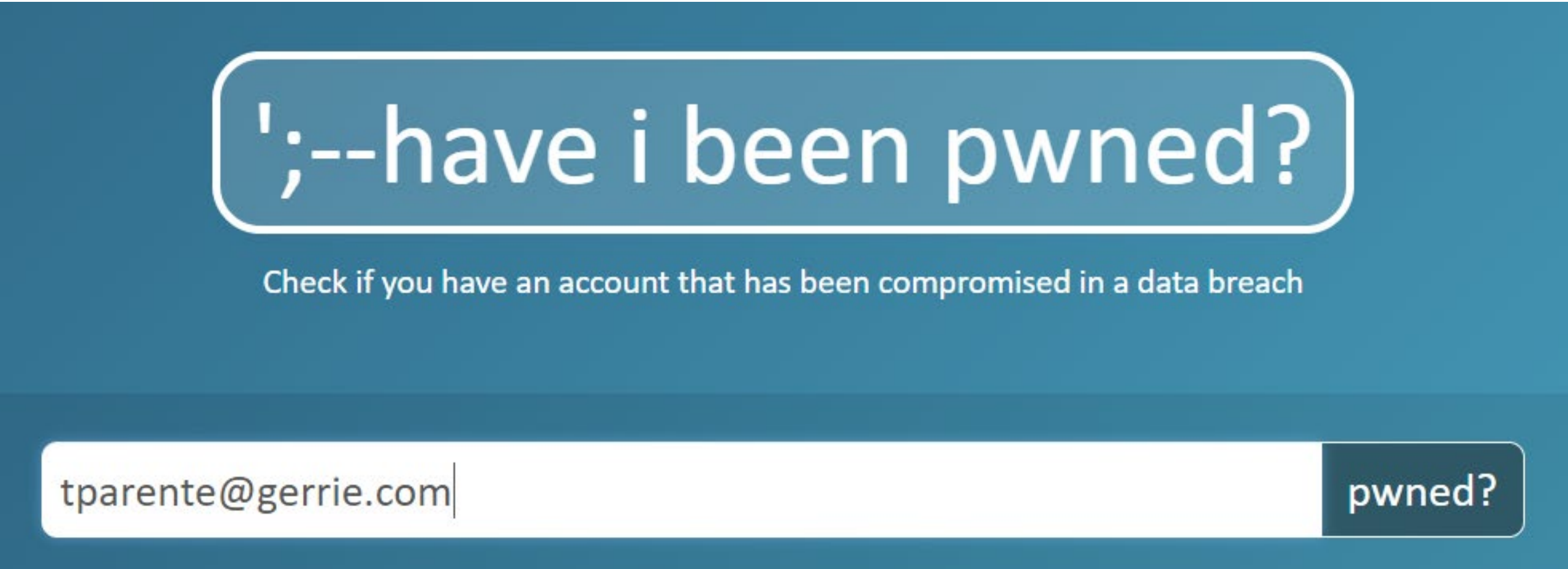
They're animals...



- If your work gets hacked, **<u>your</u>** personal identification could be at risk including social insurance information.
  - St Catharines Hydro lost over $655,000 due to an errant click on a phishing attack.
  - City of Wasaga had ransomware attack that locked everyone out for 7 weeks. Lead to $35,000 payment but over $250k in costs to fix.
  - *In a penetration test at a local Hydro company...*
- Most people that are hacked were initially hacked for at least 6 weeks before anything happens.

Most of you have been breached

- ***Here's who…from https://haveibeenpwned.com/***



What can you do to limit your attack surface?

Passwords!

- Use strong passwords ***over 11 characters*** long. The longer, the better. *Equifax was brought down by a default password.*
- ***NEVER*** re-use your passwords or keep them on sticky notes.
- Update your passwords regularly.
- If you can't remember passwords, use a password manager. You'll only need to remember 1 password.
  - https://www.lastpass.com/ - Free
  - https://1password.com/ - $5 a month
  - https://keepassxc.org/ – Free and local to workstation.
- While you're at it, disable auto-fill in your browsers and delete any saved passwords.

Clear your Cookies

- These little files hide in ***your*** computer so that ***your browser*** and websites can track ***your browsing*** sessions and save certain useful information, such as account names and passwords, for later retrieval.
- Stay away from most personality quizzes. *What Disney Princess are you?*
- ***https://www.ccleaner.com/***

Secure your devices…

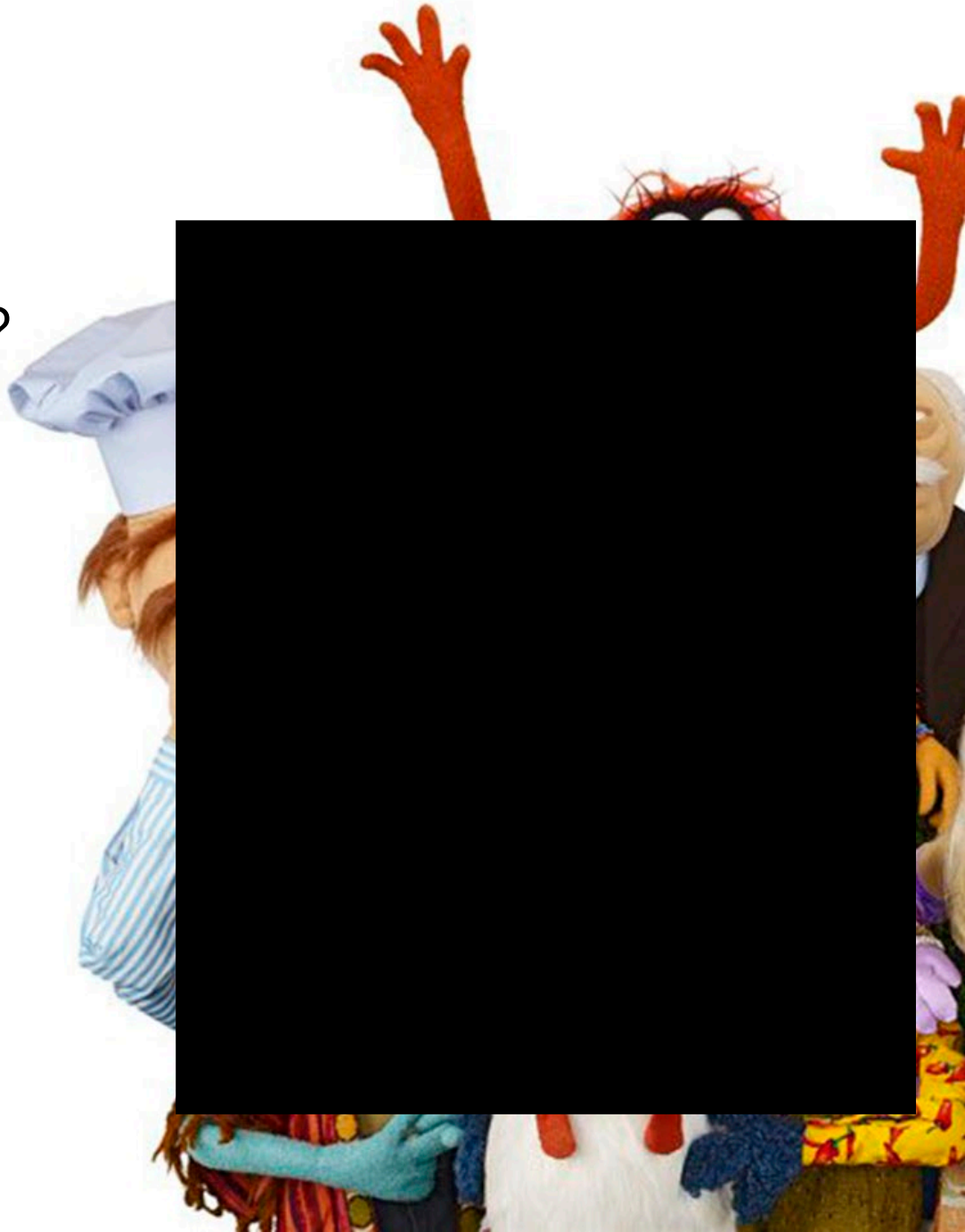
Hopefully you have an IT staff-member, but most of you won't.

- If you have a firewall, use the ***website filtering***. This will block out many questionable websites.

- ***Make sure your computers and phones have the most up to date versions (OS, software & AV):***
  - https://www.cyber.gc.ca/en/alerts-advisories
  - Windows 7 Microsoft support ends in January 2020.
  - Windows 8 ends in 2023, but it's crap anyways. Go to 10.
  - Run software updates often.
- ***Block USB memory devices.*** This can be done by a group policy.
- **Have back-ups and a recovery plan.**

Who has Access?

- When was the last time you had an audit of your access to your domain?
  - Do you off-board expired employees?
  - Do you verify vendor access has been removed?
- Do you track what 3rd parties staff access and ensure that access is reviewed frequently?
  - **Example**
- Does your staff workstations have local admin access? If yes, then they can install any software.



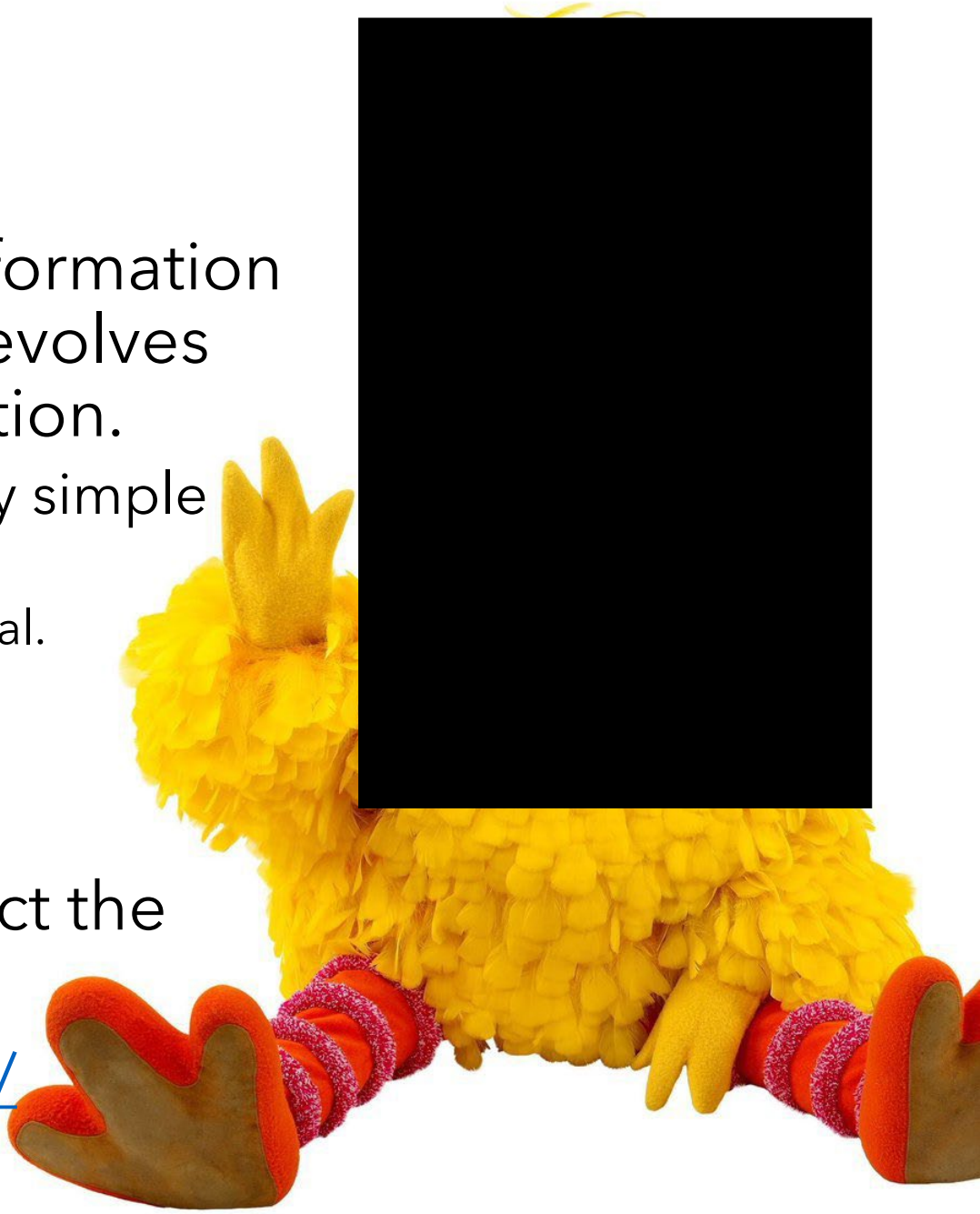
Here Phishy, phishy, phishy...

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. Look out for:

- Spelling mistakes or poorly written.
- If they ask for personal information they should have.
- Look at the email address.
- Hover over links to show the destination.
- Don't open an HTML/zip attachment in emails.
- When in doubt, do not click on the link. Go directly to the source (call sender to confirm or go to the website from a browser independently of the email).

Privacy

- We are all required to protect the information of our customers. Privacy primarily revolves around personal identifying information.
  - Information that can not be obtained by simple online searches:
    - Name and Address ***not*** considered personal.
    - Name and email ***is*** personal (combination)
    - Social Insurance and other information
    - Credit card or license information
- All businesses in Ontario must contact the Privacy Commissioner of Ontario:
- https://www.ipc.on.ca/organizations/



You haven’t been bad…

- You’ve all likely received an email indicating you were watching pornography as well as a comment on the videos.
- There is also likely an indication of an older password you used in the past that was hacked and sold.
- ***This is just a trick.*** If you still use that password anywhere…this is bad.

NIST Compliance

- You may eventually need to sign off on your cyber security preparedness if you ever need to connect with another network. You may be asked for an audit to prove it.
- NIST is the standard for cyber security: https://www.nist.gov/cyberframework

You will be compromised

Be Aware

Be Prepared