

Cyber Security Tips

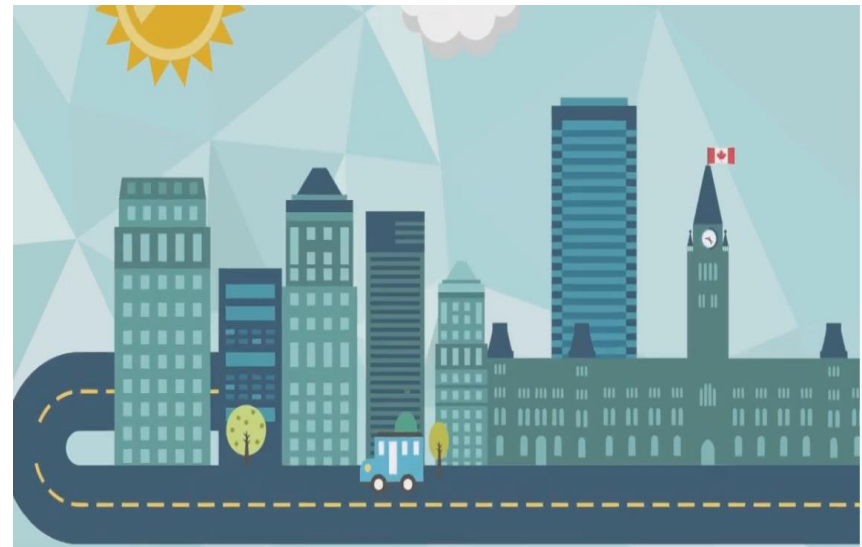
This tip guide on cyber security is based on a presentation by Frank Fazio given at FPEIM's Semi-Annual Meeting on October 26, 2019 and hosted by the Town of Souris.



FEDERATION
of
PRINCE EDWARD ISLAND
MUNICIPALITIES

Overview

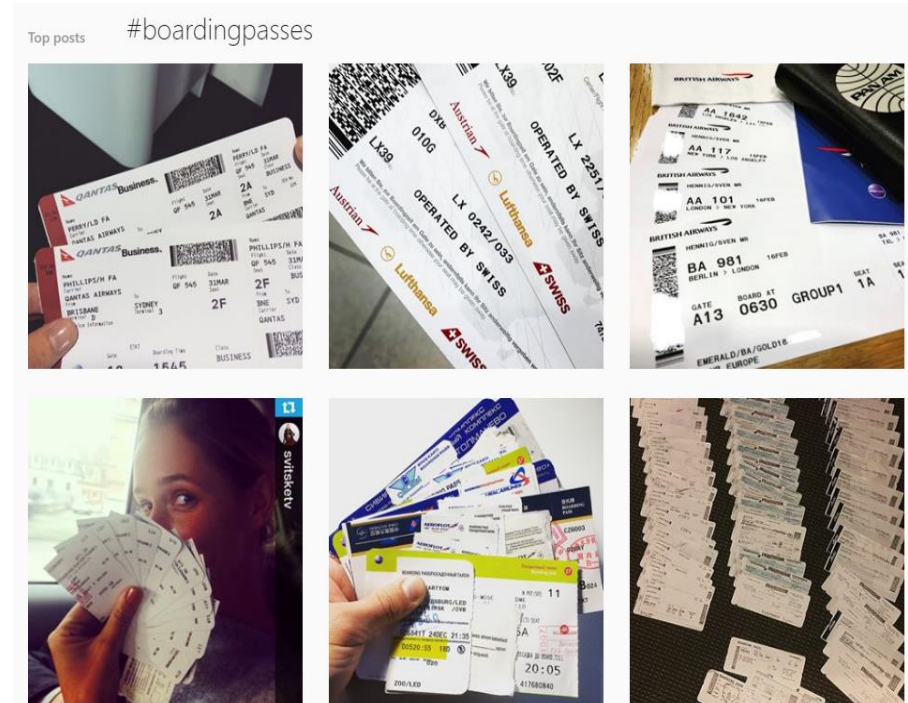
- Video to watch on why it is important for your municipal government to be cybersecure
<https://youtu.be/f7avmA8uHz0>
- What you throw out
- What you click
- How you create passwords
- What you post online
- What you plug in



Municipal government even small ones can be hacked, ransom your data, steal privacy or stop you offering services to residents.

What you throw out!

If you throw out your boarding pass, using your bar code **hackers** can get your **passport info, date of birth, credit card**, just by scanning your bar code! Don't post pictures of your boarding pass online goes without saying.



Shred, shred, shred.....

What you throw out

Your recycle bin – is it empty? physical and computer? does it contain valuable information? Shred documents.

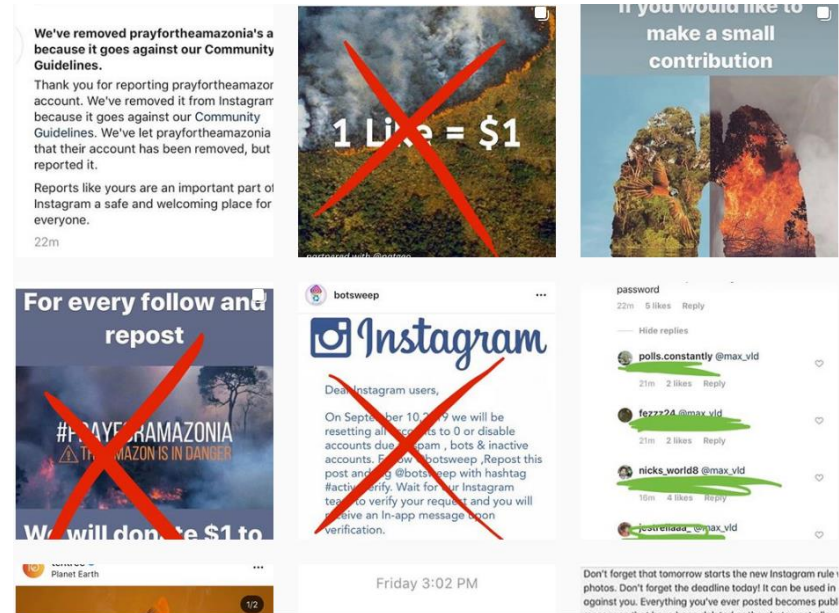
What do you leave in hotels, airports, hotel computers, rental car bluetooths, and on bulletin boards etc.?



Municipal government even small ones can be hacked, ransom your data, steal privacy or stop you offering services to residents.

What you Click – Click Bait!

- Trust no one, literally. Never open attachments in emails from someone you don't know. Cybercriminals often distribute fake email messages that mimic notifications from online stores, banks, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system.
- **Cyber Safe** <https://staysafeonline.org/stay-safe-online/online-safety-basics/spam-and-phishing/> will give you some tips to stay safe
- **Take the Phishing Quiz** (Can you spot which ones are scams?) <https://phishingquiz.withgoogle.com/>



Clicking allows access to your computer and computer networks to hackers.

Passwords

- **Don't use personal information** – programs that can come up with possible passwords with very little information
- **Don't reuse passwords** – Use a password manager
- Do use long phrases like songs or quotes
- Do use special characters
- Do use 2 factor authentication – use with all social media
- Check your passwords at www.haveibeenpwned.com



Municipal government even small ones can be hacked, ransom your data, steal privacy or stop you offering services to residents.

What you post online

- Don't put your debit and credit cards online or your license
- Don't post where it asked info about you – (what's your royal guest name), what's in your pocket challenge – hackers will spend months to get to know someone and then send file and ask them to open because they couldn't.
- Be careful about what information is in the background. i.e your password on a post-it note on your computer!
- Cover your webcam - Put stickers on camera and microphone – turn off microphone
- Social media issues –dog tag, phone number – be careful what you post
- Have an account for work and one for play



Municipal government even small ones can be hacked, ransom your data, steal privacy or stop you offering services to residents.

What you plug in

Be careful plugging your phone in to a USB where you can't see the other end – juice jacking

Use an electrical plug, shut off your phone, invest in a data blocker USB adapter only lets power through

USB drop – study 300 dropped and 299 picked up and 149 plugged in, be careful of plugging in USB drives that you found

You can be fooled – picture with hair on it – swipe up on Instagram



Municipal government even small ones can be hacked, ransom your data, steal privacy or stop you offering services to residents.