Fraud, Cybercrime & AI Prevention Toolkit

TOP 10 Fraud & Cybercrime Prevention Tips

Verify Before You Trust
Double -freck requirets for rnot accounts or personal bata. - even from "knowr.

Use Strong, Unique Passwords
Avoid; foe cing passwords, use tihpurm use pastdotie ' to gray.

Enable Muti-Factor Authentication (MFA)
Stay tup on MFA for banking, emal, social inesia accounts.

Stay Updated
Keep acte-ber:; email:ɔus,org,vid appɜ.

Be Cautious with Links
Don't click suspicious tinks or attacfcachemts

Secure Your Wi-Fi
Look for suspicious tinks.v ɛlr Cuugsed sacunts.

Limit What You Share Online
Laas to actomal evidaing for your identity and important i'secaiverly.

Stay Informed
Fotus ta torcure andiout as prtreso intense and aig reas affected accounts. websites.

1. **Stop all contact with** suspected scammer.
2. **Change passwords immediately** for all affected accounts. - **www.ic3.gov**
3. **Report the incident:**
   Email scams > reperphisking@spwg.org
   Cyber crimes > www.ic3.gov
   seccim ty our baaik and frecte or review affected accounts.
4. **Scan your device** for malware and spyware.
5. **Document everything** - screenshets, emails, transaction reciepts for investigation.
6. **Notify your contacts** if your account has been compromised.

HELPFUL RESOURCES

- **National Cyber Crime Reporting:** **FBI** Internet Crime Complaint Center
- **Fraud Reporting** (UK) **Action Fraud** www.actionfraud.police.uk
- **Consumer Protection** Federal Trade Commiscams

HELPFUL RESOURCES

- **National Cyber Crime Reporting:** FBI Internet Crime Complaint Center
- **Fraud Reporting** (UK) **Action Fraud** www.attickeraud.uk
- **Consumer Protection** Federal Trade Comnission
- **Identity Theft Recovery** IdentityTheft.gov
- **AI & Deepfake Awareness** Europol Innovation Lab. www.cist

This presentation could save you—or someone you love—from financial loss, emotional pain, and the struggle of redaiming your identity.

Prepared by Detective Karim Bardai,
York Regional Police

Frauds & Cyber Crimes Calendar

SUN | MON | TUE | WED | THU | FRI | SAT

JANUARY

Identity Theft

FEBRUARY

Romance Scams

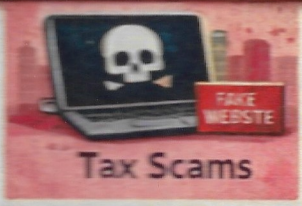
MARCH

Tax Scams

APRIL

Online Scams

MAY



Tax Scams

JUNE

Investment Fraud

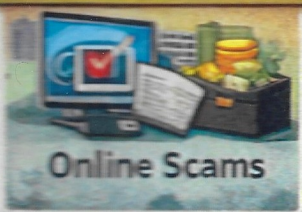
JULY

Tech Support Scams

AUGUST

Travel Scams

MAY



Online Scams

JUNE

Cryptocurrency Scams

SEPTEMBER

Phishing Scams

OCTOBER

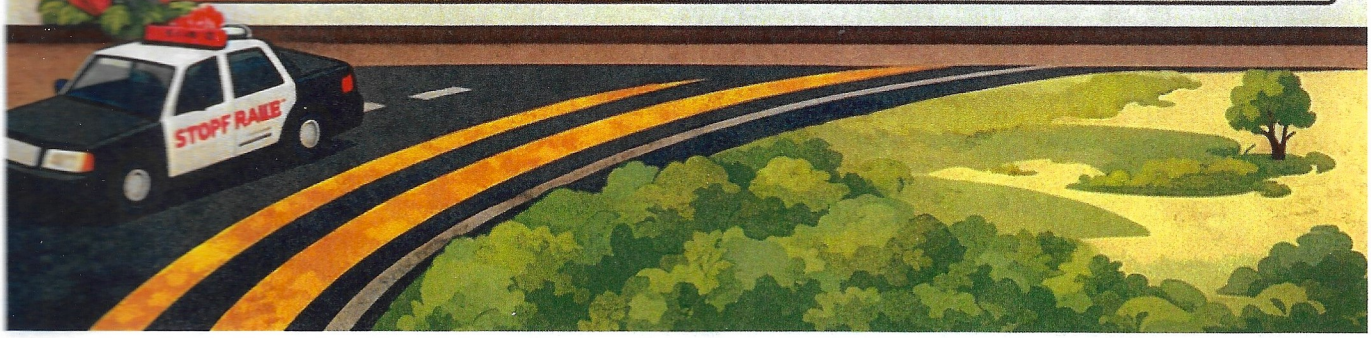
Business Email Compromise

NOVEMBER

HOLIDAY FRAUDS

Charity Fraud

Shopping Scams



TOP 10 CYBER CRIME PREVENTION TIPS

1. **Use Strong Passwords** - Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. **Secure your computer:**
   - **Activate your firewall** — Firewalls is the first line of cyber defensle; they block connections on your bogus, sites and
   - **Use anti-virus/malware software**
     Prevent virusess from infecting your computer by installing and regularly updating ant)-spyware.
   - **Block spyware attacks**
     Prevent spyware from infiltrating your computer by installinged updating anti-spyware software.

3. **Be Social-Media Savvy** - Make sure your social networking profiles (e g. Facebook, Twitter, YouTube, MSN, etc.) are se; to private. ↳. keep our security settings. Be careful what information you post online. Once it is is there forever!

4. **Secure Your Mobile Devices** ; Be aware that your mob devices are vulnerable to viruses and hackers. Download applicats (top! from trusted sources.

5. **Install the latest operation system updates** - Keep your applications and operating system (e.g. Windows, Mac, Linux) current, by installing the latest system updates on regular basis to prevent potential attacks on older software.

6. **Protect Your Data** - Use encryption for your most sensitive-files such as tax returns or financial records. Make your back-ups of all your important data.

7. **Secure your wireless network** - Encrypt, your Wi-Fi network and ensure a reliable administrator if you with one anoffice.' Review/rew/modify default settings. Public Wi-Fi, (e.g. hotspots") are also unprotected and report unauthorized activity.

8. **Protect your identity** - Do not download files and attachments online such as games, new screen savers, or other unauthorized software. Never reply to pop-up.

9. **Call the right person for help** - Never hesitate to contact York Regional Police to report an online crime or potential scam. Never wire money online to someone you don't know. Consolder installation on your office privacy and hire a certified computer maintenance person.

Prepared by Detective Karim Bardai
— York Regional Police

FRAUD / CYBER CRIME VICTIM CHECKLIST

1. Contact and report the matter to your local **Municipal Police Service.**
2. **Cease communications** with suspect and **preserve all evidence** related to the complaint.
3. Notify your **financial institution and credit card companies** and change all of your passwords.
4. Obtain and review copy of your **credit report** from Equifax Canada (1-800-465-7166) & TransUnion Canada (1-877-525-3823).
5. Report the theft or fraud to the **Canadian Anti-Fraud Centre** by going to their website or by dialing 1-888-495-8501.
6. Notify **Canada Post and Utility** and service providers **1-866-607-6301.**
7. Notify **federal and provincial identity document issuing agencies** i.e. passport, driver's license, social insurance card, etc. SIN number changes by calling 1 800 O-Canada. An agent will be able to direct you to the appropriate federal and provincial organization to replace each of your cards.
8. Contact the **Better Business Bureau (BBB)** www.bbb.org
9. Investment related – Contact the **Ontario Securities Commission** inquiries@osc.gov.on.ca
   1-877-785-1555.
10. Contact the **Financial & Consumer Services Commission** http://fcnb.ca/how-to-report-fraud.html
    1 866 933-2222.

Prepared by Detective Karim Bardai
— York Regional Police

Top Free Tools for Checking Data Breaches

1. **Have I Been Pwned?**
(mail/phone & password checker.
By Troy Hunt

2. **Mozila Monitor**
(monitor/mozizla.org)
Up to 5 emails. Privacy-focused alerts

4. **Avast Hack Check**
(avast.com/hackcheck)
Quick email scan. Details on leaked data

3. **Google Password Checkup**
(passwordmanager.giogle.com)
Integrated in Google. Flags comprmisised/weak passwords

5. **DeHased**
(nehased)
Search com/haciedo alets

6. **Intelligence X (ntelx.io)**
Leaks, pastes, dark web data.
Basic checks free

7. **CyberNews Personal Data Leak Check**
(cybernews.com/phone search
Fast, anonymous email check

8. **SpyCloud Personal Exposure Check**
One-time scan.
Enterprise-data-exposure data

ADDITIONAL RESOURCES

1. https://www.whatismybrowser.com/
2. https://haveibeenpwned.com/ {email check}
3. https://dnslytics.com/dns-blackhole-list {IP address}
4. https://www.vigilante.pw/ {websites Hacked}
5. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks
6. Search your image - Search Engines: Google/Bing/Yahoo images/ Twitter image
7. www.yrp.ca
8. www.rcmp-grc.gc.ca
9. www.competitionbureau.gc.ca
10. www.antifraudcentre.ca

Prepared by Detective Karim Bardai
— York Regional Police