An ***Equipping for...*** resource

Scams: A growing problem and how to be vigilant

Best Practices for Churches

Thousands of Canadians fall victim to fraud yearly, losing millions of dollars. Most people don't think it will happen to them, but fraudsters use increasingly sophisticated ways to target people of all ages. The impact of fraud on individuals, families and businesses can be devastating. The Canadian Anti-Fraud Centre reports that since the end of January this year, fraud reports totalled 6,610, with some $43.6 million lost to scams.

The Presbyterian Church in Canada (PCC) recently had to issue a warning about a phone scam targeting churches. A member of a Presbyterian congregation reported a call from someone claiming to be soliciting funds for Presbyterian World Service and Development (PWS&D). The caller insisted that the member provide banking information over the phone.

The PCC urges its members to be cautious and not fall prey to people using PWS&D's name or any other PCC ministry in attempts to solicit funds fraudulently. PCC ministries, including PWS&D, do not solicit funds over the phone, and they would never demand that donors share their banking information. The only time someone from the PCC will call a donor is to update credit card information used for monthly donations or to clarify information mailed to the church.

If it sounds too good to be true, it probably is. Don't be the victim of a scam.

Nkwuda Oke, Computer Systems Manager for the PCC, and Jim McDonald, the PCC's Development Manager, warn that such fraudulent activities are becoming more and more common. As scammers are duping people with increased efficiency, their tactics and methods have evolved and become much more refined.

continued

Be Aware

The best way to protect yourself from becoming a victim is to be aware of popular phone or text scams and how to avoid them.

THE CRA PHONE/TEXT SCAM

In this scam, callers impersonate Canada Revenue Agency (CRA) agents and threaten victims with arrest or legal action unless they pay a supposed outstanding tax debt. Other scammers pretending to call from the CRA demand personal bank information to facilitate bogus GST/HST or income tax refunds.

THE TECH SUPPORT SCAM

In this scam, a caller claims that a virus has infected your computer. Sometimes this scam begins with a startling website pop-up or email that demands that you call a number urgently. Scammers may even claim to be affiliated with well-known brands of computers. The scammer states that your computer is sending viruses or has been hacked and must be serviced. They request access to your computer or demand you pay a fee to fix the computer. This scam is particularly effective with less tech-savvy individuals.

THE EMERGENCY SCAM/GRANDPARENT SCAM

Emergency scams are a frighteningly convincing deception designed to prey on your fears that a loved one may be in danger. Using this tactic, scammers will call, claiming to be someone close to you, usually a grandchild, and plead for money, alleging that they are in urgent need due to an emergency. The tale of woe might be that they need bail money because they've been arrested (especially while travelling in a foreign country) or in a car accident. Victims are usually instructed to keep the money transfer a secret from the grandchild's parents, a tactic to prevent the story from being corroborated. The caller may ask the victim to send money via wire transfer or gift cards. According to the Canadian Anti-Fraud Centre, during the first three quarters of 2022, Ontario residents reported over 13,293 of these scams, resulting in over $118 million in losses.

THE BANK SCAM

Scammers impersonate representatives of lending institutions looking to give out fictitious loans. Victims are encouraged to pay upfront fees and share banking information, with predictable results. Banks will not call you and ask for your personal information.

continued

THE RCMP SCAM

Scammers impersonate RCMP officers and demand transfers of cryptocurrency to cancel an arrest warrant.

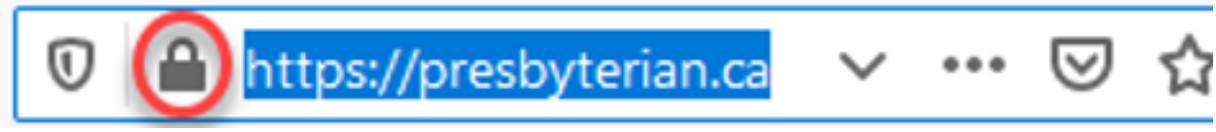
These are just a few examples of the types of scams that are targeting victims today. For a complete list of the frauds perpetrated most often in Canada, visit https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Popular email scams include phishing scams. This is the fraudulent practice of sending emails purporting to be from a reputable source to have you reveal private information. Some of the more common scams include emails that claim to be from Canada Revenue Agency (CRA) or various banking institutions.
Be extra cautious if you are ever asked to provide sensitive information, such as your name, password, account number, or SIN. A financial institution or government revenue agency will never ask for this by email.

Equally on the rise is the prepaid gift card scam. This is usually an email pretending to be from someone you know, such as a supervisor, a person in a position of authority, a co-worker, a business associate, a friend, or a family member. The scam usually starts with something like “Let me know when you are available,” “Can you do me a favour/favor,” or “There is something I need you to do,” and then asks for a reply. The initial email is often very vague and short on details. The person who responds is then requested to purchase the gift cards, most commonly Google Play, Amazon, Steam Wallet, Home Depot or Walmart cards, to scratch and send the codes to the fraudster by email.

Best Practice

- ·Don’t click on reply when verifying the authenticity of a suspicious email that appears to come from someone you know, as the “from” email address might be different from the “reply” email address. You should create a new email using the email address you have of the person.
- If you aren’t sure who sent you the email or something seems off, block the sender and report the email.
- Be suspicious of every link in an email. Only click on the link in an email if you were expecting it, even if it is from someone you know.
- Don’t open an email attachment you weren’t expecting or sent by someone you don’t know.
- Always be wary of emails from financial institutions, internet service providers and other organizations asking you to provide personal information online. Call the company directly and ask them to verify the email if in doubt.
- ·Always look for the "padlock" icon and an https:// to be sure you have a safe and secure connection when doing online banking, shopping or sending personal information.



- If you use webmail, make sure you use a secure connection, a feature available from all the primary services.
- Never use automatic login features that save your username and password. Take the time to re-enter your password each time.
- Clear your browser cache after banking or shopping online to ensure your personal information isn't stored on your computer.
- Keep your software updated (Operating system, anti-virus, browser etc.).
- If you are prompted to install something while you are on the Internet, please decline.
- When browsing the web, you might see a pop-up ad or a page warning you about a problem with your device. It may even look like the alert is coming from your device. It isn’t. These alerts are known as pop-ups, designed to trick you into calling a phony support number or buying an app that claims to fix the issue. Don’t call the number. Navigate away from that page. If you receive a pop-up that you can't exit, shut down your computer completely (push the power button).

continued

- Before sharing personal information, consider what you're putting out there through email and social networking sites. This can include information like your cell number, address, hometown, workplace, or status updates that let people know you're away, among other revealing details.
- Only use your credit card online if you know that the company you're dealing with is reputable and the website is secure.
- Public Wi-Fi in coffee shops, libraries, or airports is not secure. Never send personal information through public Wi-Fi.
- Don't be rushed. Scammers often use high-pressure tactics to create a sense of urgency to push people into making quick decisions.
- Hang up immediately if you receive a suspicious phone call or voicemail.
- You should never leave personal information on an answering machine or voicemail.
- Call Revenue Canada or your financial institution directly and ask them to verify the phone call.

By following these tips and being vigilant, you can help protect yourself from phone, email or internet scams and avoid falling victim to fraudulent activities. If you receive a suspicious call purporting to be from a PCC Ministry, the church advises its members to hang up **if they are ever in doubt and call the national office at 1-800-619-7301**. You can report any scam call you receive to the relevant authorities, such as local law enforcement. You can also contact the Canadian Anti-Fraud Centre (CAFC), which collects information on fraud and identity theft Canada-wide. **Contact the CAFC at 1-888-495-8501 or online through the Fraud Reporting System (FRS)**, even if a financial loss did not occur. Reporting helps prevent others from being defrauded. We must each remain vigilant and informed about these types of scams. By following the advice of the CAFC and other organizations, individuals can protect themselves and help prevent such frauds from becoming more widespread.