Protect yourself against financial fraud

Financial fraud cases have doubled over the past decade as fraudsters use more sophisticated tools and tricks to steal money and personal information. With news of our landmark settlement now public, First Nations communities are at greater risk of being targeted, so ensuring your financial security is very important.

THERE ARE MANY DIFFERENT TYPES OF FINANCIAL FRAUD, HERE ARE SOME COMMON ONES TO KEEP AN EYE OUT FOR:

MAIL/EMAIL SCAMS

- Unsolicited mail advising that you are either the beneficiary of funds or winner of a lottery, gift cards or some type of sweepstakes.
- Requires the victim to pay upfront fees before money can be released.

PHISHING

- The solicitation of personal or financial information from victims by impersonating reputable organizations such as the Canadian Revenue Agency or banks.

COMPUTER TECH SUPPORT SCAMS

- Fraudsters claim to be from a tech company such as Apple or Microsoft saying that your computer has been hacked and they need remote access to fix it, which can expose your personal information.
- They will also ask for credit card information to charge a fee for the repairs.

ROMANCE SCAMS

- Romantic attention via phone, mail, in-person, or by digital means with the aim of gaining access to and exploiting personal and financial information.

WIRE TRANSFER & CHECK FRAUD

- A unexpected wire transfer request arrives via mail/email or a check arrives in the mail with ia request to a portion or all of the money back.

HERE ARE SOME TIPS TO HELP YOU BE MORE AWARE AND PROTECT YOURSELF FROM FRAUD:

VERIFY CREDENTIALS

- Verify the credentials of individuals or organizations before sharing any personal or financial information. Legitimate entities will provide clear documentation and contact information. Be wary of unsolicited calls, emails, or messages asking for sensitive information.

REVIEW FINANCIAL STATEMENTS CONSISTENTLY

- Checking your banking and other statements for suspicious activity on a regular basis is a great way to detect fraudulent activity and protect yourself from identity theft.

BE SKEPTICAL OF HIGH-PRESSURE TACTICS OR THREATS

- Fraudsters often employ high-pressure tactics or threats to coerce individuals into making hasty decisions. Take your time to research and evaluate any financial opportunities or investments before committing your funds.

NEVER CLICK ON ANY LINKS RECEIVED FROM SUSPICIOUS SENDERS

- Clicking on links from suspicious senders can expose you to various cyber threats, including malware, phishing, identity theft, financial scams, and compromised security.

PROTECT YOUR PERSONAL INFORMATION

- Ensure that your personal and financial information does not fall into the wrong hands. Use strong, unique passwords for online accounts, and be cautious when sharing sensitive details online or over the phone. Properly secure documents containing personal information or shred before disposing of them.

ASK FOR HELP

- If you're unsure, ask for help! Trusted professionals, such as financial advisors, legal experts, and offices are at your disposal to help you offer valuable insights and help you verify suspicious requests.

Your First Nation Office will establish a process for collecting your personal and financial information so you can receive settlement payments. Please check their official platforms for accurate information. **Remember, if it looks suspicious or "too good to be true", then it likely is.**

Robinson Huron Treaty LITIGATION FUND

For more information, please visit www.rht1850.ca or send an email to info@robinsonhurontreaty1850.com

There are many scammers and financial fraudsters in the world—many of whom target our vulnerable populations.

Vulnerable populations are part of our communities. They include our elders/seniors, youth, and those living with physical, mental or financial challenges. Here are some of the most common types of scams and financial frauds and tips on how to protect ourselves and our vulnerable community members.

COMMON SCAMS AND FINANCIAL FRAUD

MAIL/EMAIL SCAMS

- Unsolicited email/mail advising that you are either the beneficiary of funds or winner of a lottery, gift cards or some type of sweepstakes.
- This scam will ask you to pay upfront fees before money can be released.

PHISHING

- The solicitation of personal or financial information from you by impersonating reputable organizations such as the CRA or a financial institutions.

COMPUTER TECH SUPPORT SCAMS

- Fraudsters claim to be from a tech company such as Apple or Microsoft saying that your computer has been hacked and they need remote access to fix it, which can expose your personal information.
- They will also ask for credit card information to charge a fee for the repairs.

ROMANCE SCAMS

- Romantic attention via phone, mail, in-person, or by digital means with the aim of gaining access to and exploiting personal and financial information.

ABUSE OF TRUST

- Family, friends and caregivers can also take advantage of you. In many cases, your personal and financial information is exploited for monetary gain.

TIPS TO HELP PROTECT FROM SCAMS AND FINANCIAL FRAUD

STAY VIGILANT

- Fraudsters come in many different ways, so you have to be aware of mail, email, text messages, phone calls or people that make suspicious requests that sound too good to be true.

DON'T EXPOSE YOUR PERSONAL AND FINANCIAL INFORMATION

- Be mindful about where you access confidential information and who you share it with. If you are unsure or suspicious about anything, please reach out to your local police service, First Nation office or other trusted organizations or persons.

BE SKEPTICAL OF HIGH-PRESSURE TACTICS OR THREATS

- Fraudsters often employ high-pressure tactics or threats to coerce individuals into making hasty decisions. This may look like them asking you to make a payment or provide information within a deadline or 'limited time' opportunity. Take your time to research and evaluate any financial opportunities or investments before you decide what to do.

NEVER CLICK ON ANY LINKS RECEIVED FROM SUSPICIOUS SENDERS

- Clicking on links from suspicious senders can expose you to various cyber threats, including malware, phishing, identity theft, financial scams, and compromised security.

ASK FOR HELP AND USE COMMUNITY RESOURCES

- Seek assistance from trusted advocates, support groups, local shelters, outreach programs, and support services that can offer assistance in verifying suspicious requests and help protect yourself from scams and financial fraud.

Robinson Huron Treaty LITIGATION FUND

For more information, please visit www.rht1850.ca or send an email to info@robinsonhurontreaty1850.com

What if you've been scammed?

It can be hard to accept that you've fallen victim to a scam or fraud scheme. However, it is important to remember that scams and cyber crimes can happen to anyone, anywhere, at any time. You're the victim so don't blame yourself for what has happened.

IF YOU ARE, OR THINK YOU MAY BE, A VICTIM OF FRAUD OR A SCAM, HERE ARE SOME STEPS YOU CAN TAKE TO PROTECT YOURSELF FROM FURTHER LOSS:

END ALL COMMUNICATION

- Scammers often target victims of fraud a second or even third time with the promise of recovering money; do not engage even if they use threats or coercion.

SECURE YOUR ACCOUNTS AND PERSONAL INFORMATION

- Update passwords and security protection for online banking, social media and computer profiles. Use multi-factor authentication where possible.

REPORT THE FRAUD

- Notify your band council, local police, bank, and social security office. Also, contact the Canadian Anti-Fraud Centre.

EDUCATE AND SHARE

- Share your experience with family, friends, and community members to prevent others from falling victim.

SEEK SUPPORT

- Falling victim to fraud can be a traumatic experience, talk to someone you trust or reach out to community support services for emotional assistance. Consider seeking legal advice if you need help navigating the aftermath of the scam.

1. Protect yourself.
2. Protect your community.
3. Stay informed.
4. Stay vigilant.
5. Stay connected.

Robinson Huron Treaty LITIGATION FUND

For more information, please visit www.rht1850.ca or send an email to info@robinsonhurontreaty1850.com