FRAUD ATTEMPTS ARE ON THE RISE

Anyone can fall victim to financial fraud. It never discriminates and comes in many forms. With reports of fraud dramatically increasing across the country, it's important to be alert and educate yourself. **Remember, if it sounds too good to be true, it probably is.**

HOW TO PROTECT YOURSELF FROM FRAUD

1) Use unique passwords containing a combination of numbers, letters, and symbols.

2) Never give out personal information over the phone, online, or through email or text message.

3) When on the phone, ask for full names and locations. Fraudsters will often hang up when confronted.

4) Check that email domains are from a legitimate source (ex. a financial advisor claiming to be from YNCU will have an email address that ends in yncu.com).

5) Monitor your accounts for any unusual activity and report discrepancies immediately.

6) Shred unwanted documents that contain personal information before throwing them out.

7) When browsing online, ensure the URL starts with **"https"** and your address bar contains a **closed** padlock. This combination means the site has taken extra measures to secure your information and is safe for shopping.

8) Update your devices and browsers regularly to protect your systems from potential threats and vulnerabilities.

If you suspect you are a victim of fraud, contact YNCU immediately at 1-888-413-YNCU (9628) and report it to your local police. Know that you are not alone. We are here to help.

COMMON FINANCIAL SCAMS

Fraudsters are savvy and target anyone from teenagers to grandparents to established corporations. New scams are emerging daily so it pays to educate yourself.

Here is a list of common scams:

1) **PHARMACY SCAMS –** you would receive a phone call from someone claiming to be from your pharmacy looking to update your information. Think before you act and ask questions.

2) **TECH SUPPORT –** you would receive a phone call, email, or website pop-up claiming your computer is under attack. Remember that tech support services do not send unsolicited email messages or phone calls requesting personal information.

3) **CANADA BORDER SERVICES AGENCY –** you would receive a phone call or email from someone claiming to be from CBSA regarding a package being held at customs. CBSA will never request your private information for an item being held. If you are unsure, contact CBSA directly to confirm the legitimacy of the call.

4) **GIVEAWAYS –** Entering social media giveaways seems harmless, but make sure you are keeping an eye out for impersonator accounts claiming you have won. These accounts will typically have subtle differences in their name and will often contact you outside the expected timeline. Do not give them any personal information and contact the original poster.

5) **ONLINE REVIEWS –** be wary of reviews claiming an employee helped them with their investment strategies. These fraudulent reviews will often include a Whatsapp number and email to contact their financial advisor. All of our advisors would have an email address that ends in yncu.com.

For an up-to-date list of scams, visit:
ANTIFRAUDCENTRE.CA