Fraud Prevention & Scam Awareness

PenFinancial Credit Union

1-866-866-6641 | PenFinancial.com
@PenFinancial

In today's digitally connected world, where technology has become an integral part of our daily lives, it's crucial to stay vigilant against the ever-growing threat of fraud. Deceptive individuals and cybercriminals are always on the lookout for unsuspecting victims, ready to exploit any vulnerability they can find. However, with a little knowledge and a dose of caution, you can protect yourself and your finances from falling prey to their schemes. It's important to remember not to give out your personal information to anyone over the phone or online. We've compiled a list of common fraud and scam themes to help you stay one step ahead and safeguard your hard-earned money.

1. CANADA REVENUE AGENCY (CRA) SCAM

The CRA will never contact you via text (SMS), phone, or email to request payment for taxes or fines. If someone asks you to buy gift cards in order to settle your taxes or fines with the CRA, **it is a SCAM!** Please be aware that government agencies do not accept gift cards as a form of payment. **Do not** reply to any texts, click any link in text messages or emails, or provide any of your personal or financial information.

2. GRANDPARENT SCAM

These scams usually involve a phone call or social media request/message from someone who pretends to be your grandchild or another close family member (son, daughter, niece, nephew, etc.) claiming to be in trouble and in need of immediate money for bail or hospital expenses. The scammer may try to convince you that they have been in a car accident, in the hospital, or have been arrested. You will be asked for payment right away in order to get your grandchild out of trouble. Payment may be requested through wire transfer, crypto currency, gift cards or by sending a courier to you home to pick up cash.

If you receive a call like this, **it is a SCAM!**

There are steps you can take to protect yourself:

- **Do not** sent money!
- Call your grandchild or another family member to verify the claims or requests.
- Always ask for proof of identification and call-back numbers.
- Set a safe word or phrase with family members that includes details only you would know, and ask for this word or phrase to confirm if the person calling is your relative.

3. DOUBLE PHISHING ATTACK

This scheme begins online, where a regular-looking, **but faked** login page now has a follow-up screen asking for your 2-step verification code. This allows the fraudster to bypass 2SV on login when you fall for the fake prompt and provide your login, password and then verification code to the fraudster.

While we have set up 2SV on certain transactions to help prevent the movement of money if fraudsters gain access to your account, it is crucial to remain vigilant. Fraudsters may call you, pretending to be a PenFinancial (or other Credit Union) staff member doing a follow-up or check-in call. They claim, to verify your identity, that you will need to share a verification code you will receive via text (SMS) or email. The fraudster will then attempt to move money via an e-transfer or bill payment, which will prompt a 2SV verification notice to you. If you receive a call where someone asks you do provide a 2SV code, **it is a SCAM! Do not share your 2SV codes with anyone,** as we will **never** ask you to share them.

4. PHONE, EMAIL & COMPUTER SCAMS

There are a number of telephone, email and computer scams that fraudsters may use to gain access to your personal and financial information. You may receive a text (SMS) message, phone call, or email from a fraudster claiming one of the following scenarios:

- *Your credit card has been compromised* and you're asked to provide personal information over the phone or click a link to verify or secure your credit card. **It is a scam!** Legitimate credit card companies **don't** ask for personal information over the phone or via email.
- *You missed a Canada Post delivery* and you're asked to provide personal information or click a link to reschedule the delivery, along with a fee. **It is a scam!** Canada Post **does not** charge a rescheduling fee.
- *Your missed an Amazon delivery* and you're asked to provide personal information or click a link to reschedule the delivery. **It is a scam!** Amazon will never send you an unsolicited message asking for personal or credit card information.
- *Someone claiming to be a representative from Microsoft, Amazon, CRA, etc. is requesting remote access to your computer* to assist with repairs, maintenance, or an online interaction. **It is a scam! Do not** allow anyone access to your personal computer, either through a remote connection or directly.
- *Someone claiming to be a Service Canada employee contacts you requesting personal information* such as a Social Insurance Number (SIN) or passport number. **It is a scam!** Service Canada usually sends mail in beige (or sometimes white) envelopes. **Do not** provide personal information over the phone or via email. You can contact 1-800-O-Canada (1-800-622-6232) and an agent will refer you to the program or service that attempted to reach you.

5. GIFT CARD SCAM

Typically, this involves fraudsters obtaining a gift card's PIN by peeling or scratching off the protective strip on the back of one card and replacing it with the protective strip from another card in their possession. The fraudster then waits to see when the gift card is activated, and as soon as the card is loaded with money, the fraudster quickly buys items online.

There are steps you can take to protect yourself:

- Buy gift cards from recognized brands and activate the card right away to monitor the balance right up to the day the card is gifted.
- Purchase gift cards online from the official store website. Digital gift cards come with full tracking and transaction details including a time stamp.
- Find out how to contact the company, so you're not scrambling if a card is compromised. You can even call the company ahead of time to find out how it will be handled if the card is empty.

IF SOMEONE IS TELLING YOU WHAT TO SAY TO THE TELLER...

IT'S A SCAM!

For more information and fraud prevention tips,
visit **PenFinancial.com/Fraud-Prevention**

Be sure to also follow us on social media
for news and updates:

@PenFinancial

PenFinancial
Credit Union

v.20231214.0001