

SCAM SENSE

Helping you to spot the fakes and stay safe - March 2026



SMISHING



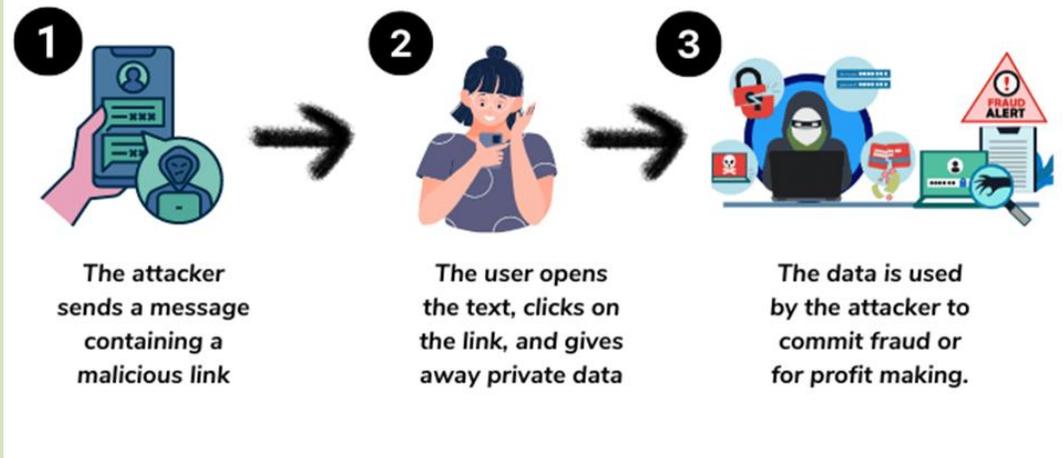
What is Smishing & Vishing?

- An urgent voicemail message from the tax department.
- A text message from Microsoft tech support warning you about a problem with your computer.
- A caller asking you to confirm your mailing address and credit card number so you can collect your free prize.
- A text message requesting your confirmation of an Amazon shipment.

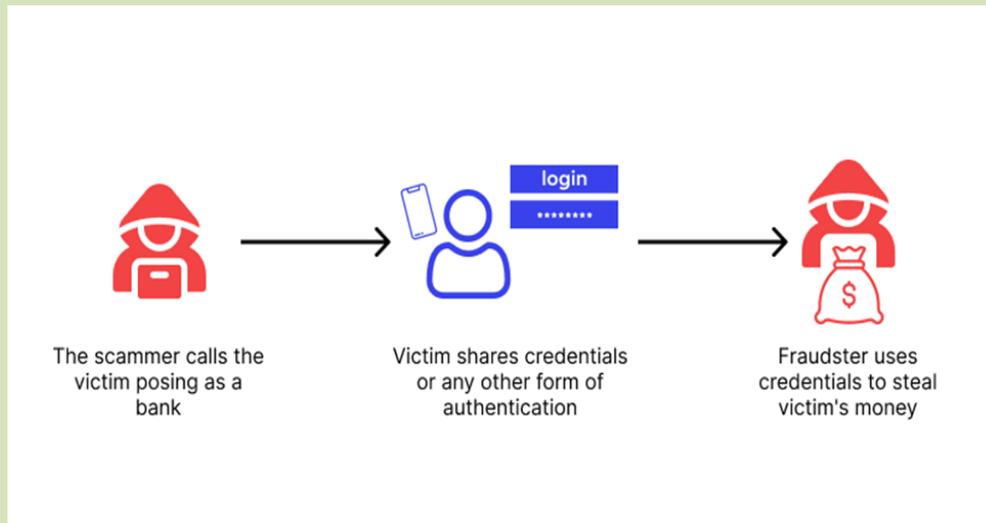
These are all examples of smishing and vishing cyber attacks. They have one thing in common: they happen over the phone. Phones are now an essential part of our daily lives. This is also why it has become one of the most popular contact methods for cyber criminals. Both smishing and vishing rely on social engineering to trick victims into giving up personal and confidential information.

Both use persuasive and often urgent language to manipulate victims into giving up information such as their bank account details, passwords, social insurance number, and mailing address.

SMISHING ATTACK PHASES



VISHING ATTACK PHASES



Protect yourself

- Verify the sender by contacting them through another medium, like the phone number on the official website
- Never click on suspicious links
- Delete smishing messages and block the number
- Ignore texts even if they ask to reply with "STOP" or "NO"
- Flag spam texts by forwarding them to 7726 (SPAM), helping your cellular provider investigate further
- Report suspicious texts. If you believe you've come across smishing, report it to Canadian Anti-Fraud Centre

From: <https://www.canada.ca/en/competition-bureau/news/2025/07/ding-scammers-are-hiding-in-your-text-messages.html>>



Fraud Prevention Month is a month-long crime prevention initiative aimed at educating and informing consumers and communities on how to recognize, report and stop fraud.

Trending scams

CRA Scams

Contact is made by way of an email, text message or phone call from a 'CRA agent' and typically follows the following pattern:

- Money is owed for current or back taxes and an arrest warrant has been issued.
- If they pay the amount owing and don't tell anyone about the phone call they will not get arrested.
- Directed to attend a specific store or a type of business and either purchase a gift card or e-Transfer the money.
- Directed to attend a specific Bitcoin ATM and deposit the money to a specific 'wallet'.
- In some instances of non-compliance they have another fraudster call the victim and pretend to be a police officer and tell the victim that they will come arrest them if the victim does not comply with the 'CRA agent' and send the money.
- Victim is kept on the phone at all times and told not to hang up or the police will come arrest them.
- The actual phone number is spoofed to read the Edmonton Police Service, the Edmonton Police Service complaint line number, Canada Revenue Agency or the phone number for Canada Revenue Agency.
- Message indicates "Your Climate Action Incentive Payment has not been claimed or processed yet" and you are asked to text or click on a link.
- **The CRA will never:**
 - pressure you to make an immediate payment.
 - threaten to arrest you, deport you, or send the police.
 - use aggressive or threatening language with you.

Buy and Sell Scams

Facebook Marketplace Scams

The Edmonton Police Service (EPS) is alerting citizens of a series of frauds occurring over Facebook Marketplace that target purchasers of Apple and Samsung products.

These frauds involve the purchase of 'new' products such as cellular phones and watches, only for unsuspecting buyers to discover that the items are fakes. In many instances, a receipt accompanies the fake item lulling the buyer into a false sense of security.

Citizens that are purchasing products on Facebook Marketplace are advised to look at the profile of the person selling the item. In most of these instances, the seller's profile is fairly new and has little to no activity.

Purchase Safety Tips

- Do not meet in a secluded place or invite strangers into your home. Suggest meeting during the day at a public location, ideally with video surveillance, such as one of the Buy and Sell Exchange Zones.
- Have someone come with you when you meet. If you cannot arrange for someone to accompany you, let friends or family know where you are going, what time you are meeting and all the details about who you are meeting, Let your contact know that everything is ok.
- Ask the buyer for photo ID. Take a photo of it for your reference.
- Buying or selling a vehicle? Offer to meet at an automotive garage where the vehicle's quality can be assured, instead of offering a test drive.
- Do not disclose to the seller how you will be paying – it could be an excellent opportunity for a personal robbery to take place.

Buy and Sell Exchange Zones

The Edmonton Police Service, in partnership with TELUS, have launched several Buy and Sell Exchange Zones across the city. Designated areas in police station parking lots are now equipped with video cameras to record the exchange of online purchases. This initiative originally began in 2020 as a pilot project at the Southwest Division but due to its overall success, the project has been expanded to the following divisions:

- **Northeast Division Station - 14203 50 Street**
- **Southeast Division Station - 104 Youville Drive East**
- **Southwest Division Station -1351 Windermere Way SW**
- **West Division Station - 16505 100 Avenue NW**

*Please Note: Although these stalls are surveilled by video cameras, **they are not monitored 24/7.**



Banking Courier Scam

A banking courier scam involves fraudsters posing as bank officials or police, claiming your account is compromised. They convince victims to hand over bank cards and PINs to a courier for a "secure" investigation. Banks will never send a courier to collect cards or ask for PINs, and victims often lose thousands of dollars.

Key Indicators and Tactics:

- **Impersonation:** Scammers pretend to be from well-known banks (e.g., RBC, CIBC, Scotiabank) or police.
- **Caller ID Spoofing:** The incoming call may appear to be from your bank's legitimate phone number.
- **Urgency & Fear:** Victims are told their card has been compromised or they are assisting in a secret investigation.
- **The "Cut Card" Trick:** Victims are instructed to cut their card, leaving the chip intact, and put it in an envelope for courier pickup.
- **Immediate Loss:** Once the card is collected, funds are immediately withdrawn or charges are made.

How to Protect Yourself:

- **Hang Up:** If you receive a suspicious call, hang up immediately.
- **Never Give Away Cards or PINs:** Banks will never send a courier to collect cards, nor will they ask for your PIN.
- **Verify Independently:** Call your bank directly using the number on the back of your card, not the one provided by the caller.

Spring cleaning? How to Dispose of Your Personal Documents Safely

Safe document disposal protects against identity theft by destroying sensitive information via cross-cut shredding (not strip-cut) or professional, certified destruction services. For maximum security, use services like The UPS Store, Shred-it, or AMA for secure, witnessed destruction of paper, CDs, and plastics.

Methods for Secure Document Destruction

- **Professional Shredding Services:** Companies like Papersavers, Roboshred, and Iron Mountain provide one-time purges or regular, scheduled, industrial-grade shredding.
- **Retail Locations:** The UPS Store offers secure, in-store shredding services.
- **Member Services:** AMA (Alberta Motor Association) offers secure document disposal for members and non-members.
- **Home Shredding:** Use a cross-cut or micro-cut shredder to prevent reconstruction of documents.

What to Shred - Anything with personal or financial information should be shredded:

- Bank statements and credit card offers.
- Old tax returns.
- Medical records.
- Pay stubs and utility bills.
- Old cheques

Digital Data Destruction

- **Delete and Wipe:** Simply deleting files is not enough; use software to securely erase or wipe data.
- **Physical Destruction:** Physically destroy hard drives, CDs, and USB sticks.

Local Edmonton Resources

- Shred-it Edmonton (18603 111th Ave NW).
- [Canadian Shredding](#) (311, 13548 97 St NW).
- [Access Information Management](#) (West Edmonton).
- AMA - Alberta Motor Association – They also host shredding events throughout the year

What to do if you think you've been scammed

If you think you have fallen victim to a scam, that you have given remote access to your computer to a suspected scammer, or that your computer has been hacked:

- Alert your financial institution. If you have provided your account details to a scammer, contact your bank or financial institution immediately and let them know.
- Get further assistance. Contact the [Canadian Anti-Fraud Centre](#) or call 1-888-495-8501.
- Get qualified computer help. If you have computer problems, seek help or advice from a qualified and reputable computer technician.
- File a complaint. You can report unwanted telemarketing calls at National DNCL or call 1-866-580-DNCL (3625).
- Contact law enforcement. If you think the call might be part of a fraud scheme, contact law enforcement authorities or the [Canadian Anti-Fraud Centre](#)) or call 1-888-495-8501.

Identity Theft and Fraud Victim Assistance Guide	
Service Canada (personal documents) 1-800-622-6232 or 1-800-OCanada	Canada Post 1-800-267-1177 canadapost.ca/postalsecurity
Social Insurance Number 1-800-206-7218 servicecanada.gc.ca/eng/sc/sin	Bills - contact your bank/credit and debit card/utility/phone service providers
Service Alberta 780-427-7013 servicealberta.ca	Equifax Canada 1-800-465-7166 consumer.equifax.ca
Passport Canada 1-800-567-6868 passportcanada.gc.ca	TransUnion Canada 1-800-663-9980 transunion.ca

Emergency Call 911

Non-Emergency
780-423-4567
Mobile Access
#377

Deaf or Hard of Hearing
780-425-1231
Crime Stoppers
1-800-222-8477

Connect on Social Media



Useful Websites:

www.antifraudcentrecentreantifraude.ca

www.standagainstscams.ca

www.edmontonpolice.ca/crimeprevention.ca

www.seniorfraudalert.ca