SCAMS TO WATCH OUT FOR

Smartphone Scams

Texts: Never click on a link in a text message sent from an unknown number. It may include a link to a scammer's website or app.

Apps: Beware of apps that, once installed, steal your information. Scammers might also create a nearly identical copy of an existing app and then make money from in-app purchases.

QR codes: Watch out for malicious QR codes created by cybercriminals that can take you to bogus websites designed to steal your personal information.

Cryptocurrency Scams

These scams often involve fake prizes, giveaways or early investment opportunities. The scammers may create bogus or lookalike cryptocurrency websites to trick victims into sending them money, sharing login information or "investing."

Online Purchase Scams

Cybercriminals sell products that you'll never receive on marketplace websites, social media or fake e-commerce stores. At checkout, you may not have the option to use a trusted third-party payment platform, which allows criminals to directly access your information.

Online Dating Scams

Fraudsters use online dating apps to cultivate a relationship and earn trust, which they then exploit in order to ask you to buy them something or send them money.

In 2021, people lost $547 million to romance scams – an 80% increase from 2020![1]

PROTECTING YOUR IDENTITY

Avoid sending money to someone you've never met in person, even if you feel a deep connection. Steer clear of sharing too much personal information through websites or apps.

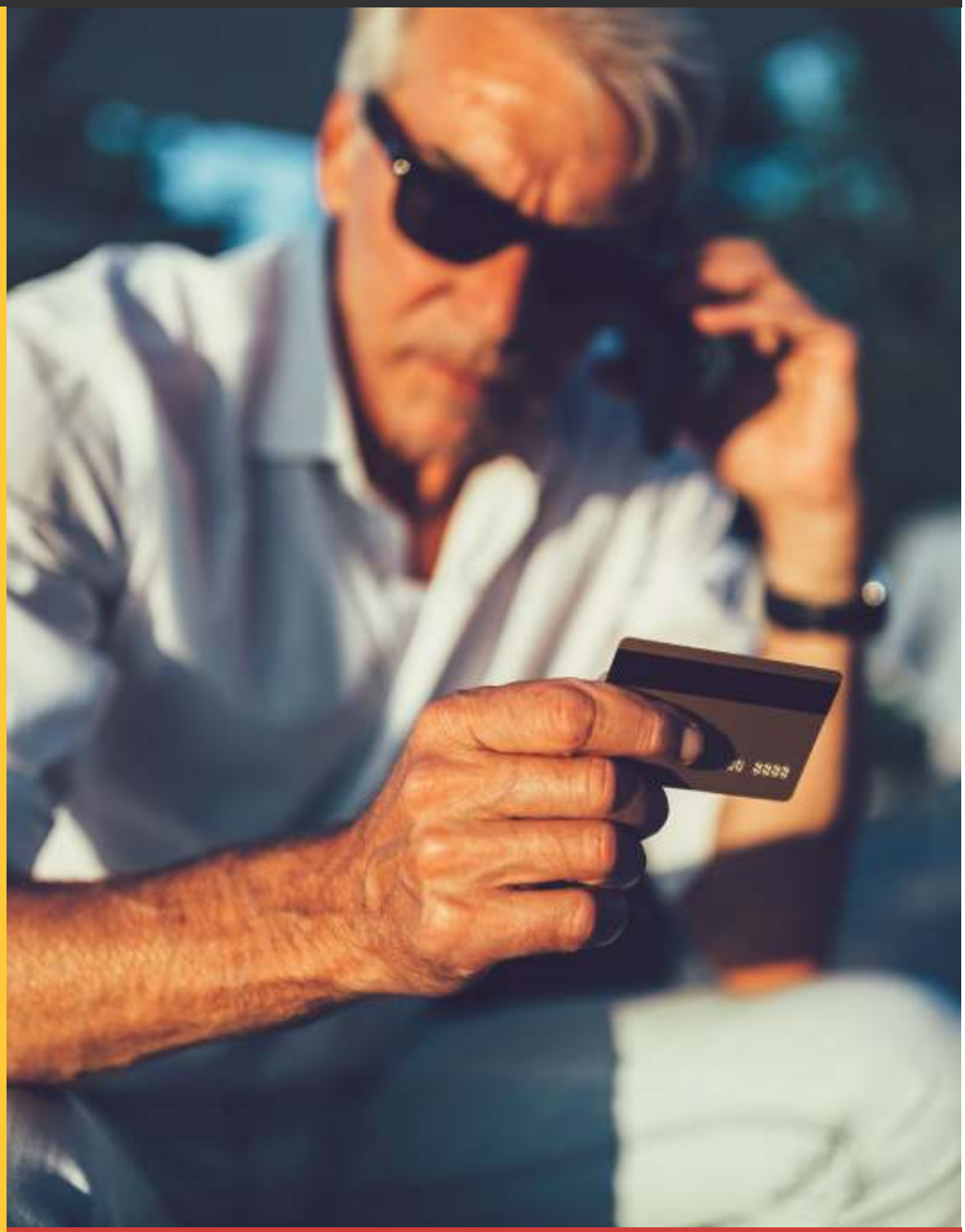
Before making online purchases, be on the lookout for too-good-to-be-true prices, lack of details or high-pressure sales tactics. You can also research the company through the Better Business Bureau.

Sign up for a credit monitoring service to get alerted when there are unexpected changes to your credit report or you've been compromised.

Never share your passwords or bank information. Call your financial institution directly to verify any suspicious texts.

Keep your smartphone safe by keeping your software up-to-date. Neglecting to install system or app updates can leave you vulnerable to cyberattacks.

SOURCE: 1. Canadian Anti-Fraud Centre



What to Do if You've Been Compromised:

- Report it to the Canadian Anti-Fraud Centre at www.antifraudcentre-centreantifraude.ca
- Notify your financial institution or card issuer.