

An aerial night view of a city, likely New York City, with buildings illuminated in shades of purple and blue. The lights create a vibrant, futuristic atmosphere. The text is overlaid on a dark blue, semi-transparent rectangular area on the left side of the image.

A COMPREHENSIVE

GUIDE FOR MODERN SCAMS

Table Of Content

CONTENTS

- 01 — How to Protect Yourself from Government Imposter Scams
- 02 — How Keylogging Works
- 03 — Identity Theft Scams
- 04 — Door to Door Scams
- 05 — How to Protect Yourself from Door-to-Door Scams
- 06 — How can I protect myself from Cheque scams?
- 07 — How to Avoid Job Offer Scams
- 08 — IRS TAX Scams
- 09 — Rouge Access Points
- 10 — How to Detect and Prevent Rogue Access Points
- 11 — Phishing Scams
- 12 — Craigslist Scams
- 13 — Charity Scams
- 14 — LinkedIn Scams
- 15 — Craigslist Scams
- 16 — Romance Scams
- 17 — COVID Scams

How to Spot, Stop, & Report Government Imposter Scams

Consumers reported more than **498,000** imposter scams to the Federal Trade Commission in 2020.

- Nearly 1 in 5 people reported losing money
- Overall, reported losses were nearly \$1.2 billion
- The median loss was \$850
- Almost one-third of the imposter scams reported involved someone posing as a government representative

Government imposter scams are a type of fraud in which scammers pretend to be government officials, such as representatives of the Social Security Administration (SSA), the Internal Revenue Service (IRS), or law enforcement agencies, to trick victims into providing personal information or making payments. These scams can take many forms and can be conducted over the phone, through email, or in person.



How Government Imposter Scams Work

Government imposter scams typically involve the scammer contacting the victim and posing as a government official or law enforcement agent. The scammer may use scare tactics to convince the victim that they are in trouble and need to take immediate action. They may threaten the victim with arrest, fines, or other legal consequences if they do not comply with their demands.

The scammer will then ask the victim to provide personal information, such as their Social Security number, bank account information, or credit card details. They may also ask the victim to make a payment using a prepaid debit card, gift card, or wire transfer. In some cases, the scammer may ask the victim to download and install software that allows them to take control of the victim's computer or access their personal information.

How to Protect Yourself from Government Imposter Scams

➔ Here are some tips to help protect yourself from government imposter scams:

Know How the Government Operates

Be aware of how the government operates and how they typically communicate with citizens. For example, the SSA will never call or email you to request your Social Security number or ask you to pay money to avoid losing benefits.



Don't Provide Personal Information

Never provide personal information, such as your Social Security number, bank account information, or credit card details, unless you are certain of the legitimacy of the request. If you are unsure, hang up and call the government agency directly using a phone number from their official website.



Don't Make Payments with Gift Cards or Wire Transfers

Government agencies will never ask you to make a payment using a prepaid debit card, gift card, or wire transfer. If a caller or email asks you to make a payment using one of these methods, it is likely a scam.



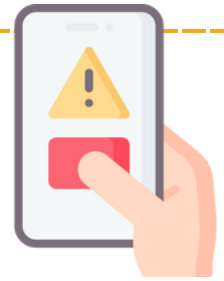
Be Wary of Unsolicited Calls or Emails

If you receive an unsolicited call or email from someone claiming to be from a government agency, be cautious. Do not provide personal information or make a payment until you have verified the legitimacy of the request.



Report Suspicious Activity

If you receive a suspicious call, email, or text message, report it to the appropriate government agency. You can also report government imposter scams to the Federal Trade Commission (FTC) at [ftc.gov/complaint] (<http://ftc.gov/complaint>) In conclusion, government imposter scams are a serious threat, and it is important to be aware of the tactics used by scammers to avoid falling victim to their schemes. By staying informed about the latest scams and taking steps to protect yourself, you can help prevent these scams and keep your personal information and finances safe.



How Government Imposter Scams Work

Keylogging, also known as keystroke logging, is a method of tracking and recording keystrokes made on a computer keyboard. Keyloggers can be either hardware-based or software-based and are often used for legitimate purposes such as monitoring employee activity or debugging software. However, they can also be used for malicious purposes such as stealing sensitive information like passwords or financial information.



How Keylogging Works

➔ Hardware-based keyloggers are physical devices that are installed between the keyboard and the computer. They record all keystrokes made on the keyboard and store them on an internal memory chip. The attacker can then retrieve the keylogger and extract the recorded data.

Software-based keyloggers are programs that are installed on a computer or device. They can be installed through various methods, such as downloading a malicious attachment or software from a fake website. Once installed, the keylogger records all keystrokes and sends the data to the attacker's computer or a remote server.

Types of Keyloggers

There are different types of keyloggers that vary in their level of sophistication and how they operate. Some of these types include:

Hardware Keyloggers

Hardware keyloggers are physical devices that are attached between the keyboard and the computer. They are small and discreet, making them difficult to detect.



Software Keyloggers

Software keyloggers are programs that run on a computer or device. They can be disguised as legitimate software, making them difficult to detect.



Wireless Keyloggers

Wireless keyloggers use radio frequency (RF) technology to transmit the recorded keystrokes to a remote receiver. They are often used in environments where physical access to the target computer is not possible.



Acoustic Keyloggers

Acoustic keyloggers use the sound of the keystrokes to record the input. They can be placed near the keyboard or computer and use a microphone to pick up the sound of the keystrokes.



How to Protect Yourself from Keyloggers

Here are some tips to help protect yourself from keylogging attacks:

Use antivirus and anti-malware software

Antivirus and anti-malware software can help detect and remove keyloggers from your computer.

Keep your software up to date

Keeping your software up to date with the latest security patches can help protect you from known vulnerabilities that attackers may try to exploit.

Be careful when downloading software

Download software only from trusted sources, and avoid downloading software from unknown or unverified sources.

Use two-factor authentication

Two-factor authentication adds an extra layer of security to your accounts by requiring a second factor, such as a code sent to your phone, in addition to your password.

Use virtual keyboards

Virtual keyboards allow you to enter your sensitive information using the mouse instead of the keyboard, which can help prevent keylogging attacks.

In conclusion, keylogging is a serious threat that can result in the loss of sensitive information and financial loss. By being vigilant and following best practices for online security, you can protect yourself from keylogging attacks.





Identity Theft

[ī-'den-tə-tē 'theft]

Stealing personal information and credentials to commit fraud.

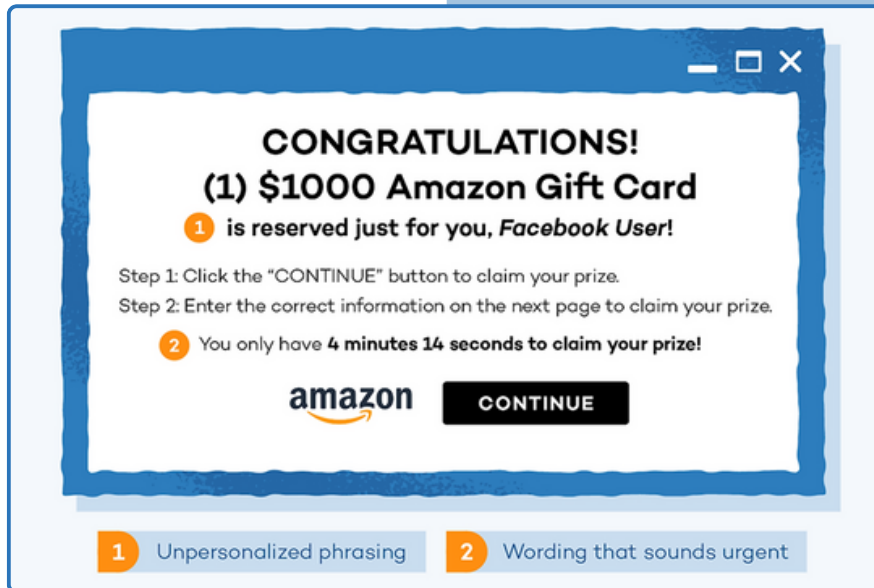
Identity Theft Scams :

Identity theft is a serious and growing problem in today's world. Scammers use various techniques to steal personal information, such as social security numbers, credit card numbers, and other sensitive data. Here are a few common identity theft scams to watch out for:

- **Phishing Scams:** Scammers send fraudulent emails or text messages, posing as legitimate companies, and ask you to provide your personal information, such as your username, password, or credit card number.
- **Fake Job Offers:** Scammers post fake job openings on online job boards and require you to provide personal information, such as your social security number, before you can apply.
- **Skimming:** Scammers install devices on ATMs or gas pumps that capture your credit card information when you use them.
- **Social Media Scams:** Scammers create fake profiles on social media platforms and use them to trick you into providing personal information or clicking on malicious links.

To protect yourself from identity theft, it's important to be cautious and vigilant with your personal information. Only provide your personal information to trusted sources, monitor your credit card and bank statements regularly, and be wary of any unsolicited requests for personal information.

Door to Door Scams:



Door-to-door scams are fraudulent schemes in which a scammer goes door-to-door, usually targeting elderly or vulnerable individuals, to convince them to purchase fake products or services, or to make a donation to a fake charity. Door-to-door scams can be carried out by a single individual or a group of scammers working together. Here are some common types of door-to-door scams:

● Home Improvement Scams

Home improvement scams involve a scammer offering to perform home repairs or improvements at a discounted rate. The scammer may claim to be a contractor, but in reality, they may perform shoddy work or use subpar materials. Home improvement scams can also involve advance payment for work that is never completed.

● Energy Scams

Energy scams involve a scammer claiming to be a representative from a legitimate energy company, offering to save the homeowner money on their energy bill by installing new equipment or making repairs. The scammer may ask for payment upfront or may offer to finance the work at an exorbitant rate.

● Fake Charity Scams

Fake charity scams involve a scammer soliciting donations for a fake charity or non-profit organization. The scammer may use a name that sounds legitimate or may claim to be raising money for a specific cause, such as disaster relief. The donations never reach the intended charity, and the scammer pockets the money.

● Magazine Subscription Scams

Magazine subscription scams involve a scammer offering magazine subscriptions at a discounted rate. The scammer may claim to be raising money for a school or charity. Once the victim has paid for the subscription, the magazines never arrive, or the subscription is canceled shortly after.

How to Protect Yourself from Door-to-Door Scams

➔ Here are some tips to help protect yourself from door-to-door scams:

Verify the Identity of the Salesperson

Ask for the salesperson's identification, and verify their identity with the company they claim to represent.



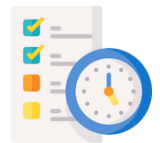
Research the Company or Charity

Research the company or charity before making a purchase or donation. Check with the Better Business Bureau or other trusted sources to ensure that the organization is legitimate.



Don't Rush Into a Decision

Take time to consider a purchase or donation, and do not feel pressured to make a decision on the spot.



Don't Pay Upfront

Never pay for products or services upfront, and do not provide payment information unless you are certain of the legitimacy of the transaction.



Report Suspicious Activity

Report any suspicious activity to your local law enforcement agency or the Better Business Bureau.



In conclusion, door-to-door scams can be financially devastating, and it is important to be aware of the tactics used by scammers to avoid falling victim to their schemes. By taking steps to protect yourself and staying informed about the latest scams, you can help prevent these scams and keep your money safe.



Money Scams:

Money scams refer to any fraudulent activity in which an individual or group tries to steal money from others. These scams can take many different forms and can target individuals, businesses, or even governments. Money scams often rely on social engineering techniques to trick victims into handing over their money willingly.

➔ **Here are some common types of money scams:**

● **Investment Scams**

Investment scams are a type of scam in which an individual or group offers fake investment opportunities with the promise of high returns or low risk. These scams may involve Ponzi schemes or pyramid schemes in which new investors are recruited to pay earlier investors, creating the illusion of profits. Investment scams can also involve fake companies, fake stock tips, or other tactics designed to trick victims into investing their money.

● **Lottery or Sweepstakes Scams**

Lottery or sweepstakes scams involve an individual or group notifying the victim that they have won a large sum of money in a lottery or sweepstakes. The victim is then asked to pay a fee or provide personal information to claim the prize, which does not exist. These scams often target vulnerable populations such as the elderly or those with limited financial resources.

- **Romance Scams**

Romance scams involve an individual posing as a romantic partner to gain the victim's trust and steal their money. The scammer may create a fake online profile and establish a relationship with the victim before asking for money under false pretenses, such as to pay for medical bills or travel expenses.

- **Employment Scams**

Employment scams involve an individual or group offering fake job opportunities that require the victim to pay a fee or provide personal information. These scams may involve fake work-from-home opportunities, fake recruiters, or other tactics designed to trick victims into paying money for a nonexistent job.

- **Tech Support Scams**

Tech support scams involve an individual or group claiming to provide technical support for a computer or other device. The scammer may contact the victim by phone or email and offer to fix a supposed problem with the device. They may then install malware or steal sensitive information from the victim's computer.

How to Protect Yourself from Money Scams :



Here are some tips to help protect yourself from money scams:

- **Protect Personal Information**

Protect your personal information, such as your bank account and social security number, and do not share it with anyone who does not need it.

- **Verify Information**

Always verify information before providing money or personal information. Check for legitimate sources and do not trust unfamiliar individuals or companies.

- **Be Skeptical**

Be wary of unsolicited messages for money, especially those that promise high returns or low risk.

- **Use Strong Passwords**

Use strong, unique passwords and two factor authentication to protect your accounts from unauthorized access.

- **Stay Informed**

Stay informed about the latest scams and techniques used by scammers to avoid falling victim to their tactics.

In conclusion, money scams are a serious threat to individuals and businesses alike. By staying informed and taking steps to protect your personal and financial information, you can help prevent these scams and avoid losing your hard-earned money.

Cheque Scams:

- **What are Cheque scams?**

Cheque scams are a common type of fraud in which scammers send fake cheques or money orders to their victims, then trick them into sending

some of the money back before the cheque clears. In the end, the victim loses the money they sent and may also have to pay the bank for any fees or charges associated with the bounced cheque. These scams can take many different forms. For example, the scammer may claim to be a foreign lottery or sweepstakes winner and offer to share the prize with you if you deposit their cheque and send them a portion of the money. Alternatively, they may claim to be a business or individual who owes you money and send you a cheque for more than the owed amount, asking you to return the excess funds.



How can I protect myself from Cheque scams?

To protect yourself from cheque scams, it's important to be vigilant and skeptical of any unsolicited offers that seem too good to be true.



Here are some tips:

- Be cautious of offers that require you to act quickly or provide personal information.
- Verify the legitimacy of any cheques or money orders before depositing them by contacting the issuing bank or financial institution.
- Don't assume that just because the funds appear to be available in your account that the cheque has cleared. It can take several days for a cheque to be fully processed, and if it turns out to be fake, you'll be responsible for repaying any funds you've already withdrawn.
- Don't send money to anyone you don't know or trust, especially if they're asking for it to be sent via wire transfer, Western Union, or other non-traceable methods.
- Report any suspected cheque scams to your bank and law enforcement immediately.

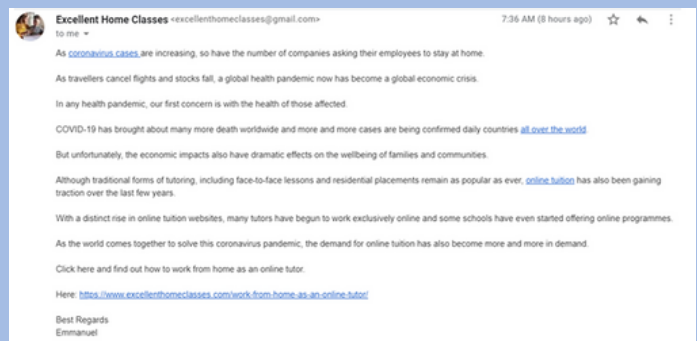
Remember, if something seems too good to be true, it probably is. Always exercise caution and common sense when dealing with unsolicited offers, and never give out your personal or financial information to anyone you don't know or trust.

Job Offer Scams:

What are Cheque scams?

Job offer scams are deceptive schemes where fraudsters pretend to be recruiters, employers, or job placement services with the aim to deceive job seekers.

These scams can take various forms, from promising high-paying jobs for a 'small' upfront fee, to 'recruiters' conducting fake interviews then requesting personal information for supposed background checks. Some scams may even involve sending the victim a counterfeit check as an 'advance' on their salary, then asking them to wire a portion of it back for 'work equipment.' Once the bank identifies the check as fraudulent, the victim is responsible for the funds wired. The objective of these scams can range from swindling money, stealing personal information for identity theft, to enlisting unsuspecting victims into money laundering schemes.



How to Avoid Job Offer Scams

Avoiding job offer scams involves conducting thorough research and due diligence. Always research the company, the recruiter, and the job posting. Legitimate companies usually post job openings on their official website or well-known job boards. Be wary of unsolicited job offers arriving via email or text message, particularly if you have not applied or posted your resume on a job search platform. Never provide sensitive information such as social security numbers, bank account details, or credit card information during the application process unless you have thoroughly verified the company and job offer. Additionally, avoid job offers that require you to pay upfront fees or invest your own money.

How to Recognize Job Offer Scams

Recognizing job offer scams can often be done by spotting various red flags. Poorly written job descriptions, frequent grammatical errors, and unofficial email addresses can be warning signs. Be skeptical of job offers that sound too good to be true, such as high pay for minimal work or work-from-home positions requiring no experience or skills. If the job offer is unsolicited and pushes for immediate action or requests payment or personal information, this should raise alarm bells. Real job offers are typically the result of an application process and interview. Always listen to your instincts; if a job offer feels suspicious or too good to be true, it probably is.

IRS TAX Scams



Claim Your Tax Refund Online

We Identified an error in the calculation of your tax from the last payment, amount to \$419.95. In order for us to return the excess payment, you need to create a-Refund Account after which the will be credited to your specified bank account.

Please click " Get Started below to claim your refund :

Get Started

We are here to ensure the correct tax is paid at the right time, whether this related to payment of texex received by the department or entitlement to benefits paid.

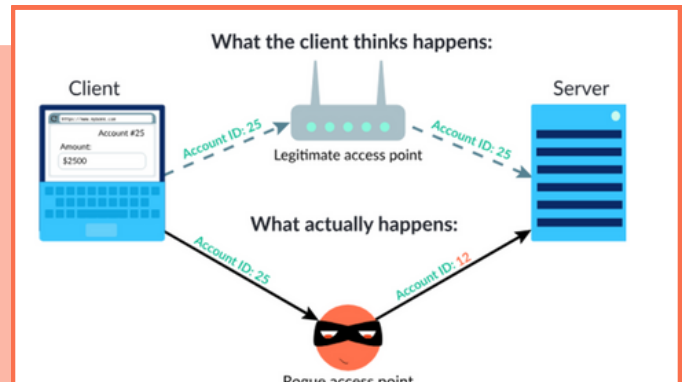
Scammers pose as IRS agents, claiming that you owe back taxes and threatening legal action if you don't pay. They ask for personal information or for payment in the form of gift cards.

There are 5 important things to keep in mind:

- The IRS will NEVER contact you by email, text, or social media
- The IRS will NEVER call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer
- The IRS will NEVER demand that you pay taxes without the opportunity to question or appeal the amount they say you owe
- The IRS will NEVER threaten to bring in local police, immigration officers or other law-enforcement to have you arrested for not paying taxes. Furthermore, the IRS also cannot revoke your driver's license, business licenses, or immigration status. (Any threats like these are used by scammers to trick victims into giving us valuable (information)
- The IRS will NEVER ask for credit or debit card numbers over the phone

Rogue Access Points

Rogue access points (RAPs) are unauthorized wireless access points that are installed on a network without the permission or knowledge of the network administrator. RAPs can pose a significant security threat to a network by providing unauthorized access to the network and potentially compromising sensitive information.



Network Congestion

RAPs can cause network congestion by competing with authorized access points for bandwidth. This can lead to slow network performance or even network downtime.

Unauthorized Access

RAPs can provide unauthorized access to the network, allowing attackers to steal sensitive information or launch other attacks.

Compliance Violations

RAPs can violate compliance regulations such as the Payment Card Industry Data Security Standard (PCI DSS), which requires that wireless networks be secured.

Malware Distribution

Attackers can use RAPs to distribute malware to network devices, potentially compromising the security of the entire network.

Risks Associated with Rogue Access Points

RAPs can pose several risks to a network, including:

How to Detect and Prevent Rogue Access Points

➔ Here are some tips for detecting and preventing RAPs on a network:

Regular Network Scans

Regular network scans can help identify unauthorized access points on the network. Tools such as wireless intrusion detection systems (WIDS) can help detect RAPs and other wireless threats.

Network Segmentation

Network segmentation can help prevent unauthorized devices from accessing sensitive areas of the network. By segmenting the network into different zones, the risk of RAPs affecting critical areas of the network can be minimized.

User Education

User education is an important part of preventing RAPs. Employees should be educated on the risks associated with RAPs and instructed not to install unauthorized access points on the network.

Wireless Security Policies

Wireless security policies can help prevent RAPs by defining the standards for wireless access on the network. Policies should include requirements for the use of secure wireless protocols and procedures for reporting and removing unauthorized access points.

In conclusion, rogue access points can pose a significant security threat to a network by providing unauthorized access and compromising sensitive information. By implementing best practices for network security and being vigilant for the presence of RAPs, network administrators can help protect their networks from this threat.

PHISHING SCAMS



From: [redacted] <[redacted]@MSVU.CA>

Sent: Friday, September 16, 2022 5:22 PM

Subject: We received a request from you

Don't trust an email just because it's from @msvu.ca

IT&S never asks you to click links to verify your account

Our record indicates that you recently made a request to terminate your Office 365 email and this process has begun by our administrator. If this request was made accidentally and you have no knowledge of it, you are advised to verify your account below [CLICK HERE](#) To verify. Please give us 24 hours to terminate your account OR verify your account. Failure to Verify will result in closure of your account.

<http://offfc4503032.sitebuilder.name.tools/>
Click or tap to follow link.

Watch for spelling, punctuation and grammar errors (highlighted)

The link goes to a suspicious website

Image from mcvu.ca

In conclusion, rogue access points can pose a significant security threat to a network by providing unauthorized access and compromising sensitive information. By implementing best practices for network security and being vigilant for the presence of RAPs, network administrators can help protect their networks from this threat.

How Phishing Works

Phishing attacks can take many different forms, but they usually follow a similar pattern. The attacker sends a message to the victim, either by email, text message, or social media, that appears to be from a legitimate source. The message often contains a link that takes the victim to a fake website that looks like the real one. The victim is then prompted to enter their login credentials, credit card information, or other sensitive data. Once the victim provides this information, the attacker can use it for fraudulent purposes.

Types of Phishing



Phishing attacks can take many different forms, some of which include:

Email Phishing

Email phishing is the most common type of phishing attack. The attacker sends an email that appears to be from a legitimate source, such as a bank or an online retailer, and asks the victim to click on a link that takes them to a fake website. The website then prompts the victim to enter their login credentials or other sensitive information.

Spear Phishing

Spear phishing is a targeted form of phishing attack that is aimed at a specific individual or organization. The attacker gathers information about the victim, such as their job title or employer, to make the phishing message appear more legitimate.

Smishing

Smishing is a form of phishing attack that uses SMS text messages instead of email. The attacker sends a message that appears to be from a legitimate source, such as a bank, and asks the victim to click on a link or reply with their sensitive information.

Vishing

Vishing is a form of phishing attack that uses voice calls instead of email or text messages. The attacker poses as a legitimate entity, such as a bank, and asks the victim to provide their sensitive information over the phone.

How to Protect Yourself from Phishing s of Phishing



Here are some tips to help protect yourself from phishing attacks:

- **Be skeptical of unsolicited messages**

Be wary of unsolicited messages that ask for your personal information. Legitimate companies will never ask you to provide sensitive information via email or text message.

- **Look for signs of phishing**

Phishing messages often contain spelling and grammar mistakes or ask for information that the legitimate company would not typically request.

- **Keep your software up to date**

Keeping your software up to date with the latest security patches can help protect you from known vulnerabilities that attackers may try to exploit.

- **Verify the sender**

Always verify the sender of the message before clicking on any links or providing any information. Check the sender's email address or phone number to ensure it is legitimate.

- **Use two-factor authentication**

Two-factor authentication adds an extra layer of security to your accounts by requiring a second factor, such as a code sent to your phone, in addition to your password.

- **Use a password manager:**

Using a password manager can help you create strong, unique passwords for each of your accounts, which can help prevent attackers from accessing your accounts.

In conclusion, phishing is a serious threat that can result in the loss of sensitive information and financial loss. By being vigilant and following best practices for online security, you can protect yourself from phishing attacks.

GRANDPARENT SCAM ALERT



WHAT IS THE SCAM?

Scammers are calling seniors claiming to be family members in need of immediate money for bail or hospital expenses.

The scammer will often send someone to the door to pick up payment.

BAIL FACTS:

- Police, lawyers, judges or jails do not call people to get money.
- Bail/fines are typically paid at a courthouse, police station or jail.
- Bail in Alberta is typically \$10-\$500.
- Bail can't be paid using gift cards.




“Court appointed” couriers don't exist. If someone asks to come to your home to pick up payment, it's a scam.



If it has to be now, it has to be no. Using fear or high-pressure tactics are usually a red flag.



Always ask for proof of identification and call-back numbers. Talk to family, friends or other people you trust to help verify claims or requests.



Grandparents scams, also known as grandparent fraud or emergency scams, are a type of scam that preys on the emotions of older individuals, typically grandparents. The scam often begins with a phone call or email from someone claiming to be a grandchild or a friend of the grandchild. The scammer may use a variety of tactics to convince the grandparent that their grandchild is in trouble or facing an emergency situation, such as being involved in a car accident, arrested, or in need of urgent financial assistance.

The fraudster might request money to be wired or sent through gift cards, claiming it's for bail, medical bills, or other emergency expenses. They often play on the victim's emotions and urgency to discourage them from verifying the information with other family members.

It's crucial for individuals, especially seniors, to be aware of such scams and to verify any unexpected requests for money or personal information by contacting other family members or the supposed person in need directly. Law enforcement agencies and consumer protection organizations often advise people to be cautious and skeptical of unsolicited calls or messages asking for money, especially when there's a sense of urgency or a supposed emergency involved.

AI Generated Phone Calls :



AI-generated scam calls involve the use of artificial intelligence technology, particularly voice synthesis or voice cloning, to create realistic and convincing automated phone calls. These calls aim to deceive individuals by mimicking the voice of a real person, such as a friend, family member, or authority figure. The scammers may use various tactics to manipulate recipients into providing sensitive information, making payments, or taking other actions that could lead to financial losses or privacy breaches.

➔ Here are some characteristics of AI-generated scam calls:

****Voice Cloning:****

AI can analyze and replicate a person's voice, making it sound remarkably similar to the target individual. This is often used to impersonate someone the recipient knows and trusts.

****Personalized Content:****

Scammers may use AI to gather information about the target, such as details from social media or other online sources, to make the scam call more convincing. Personalized content increases the likelihood that the recipient will believe the call is legitimate.

****Urgent or Emergency Scenarios:****

Similar to traditional phone scams, AI-generated scam calls often involve urgent or emergency situations. The caller might claim that immediate action is required, putting pressure on the recipient to act without thinking critically.

****Social Engineering Tactics:****

The AI may employ social engineering techniques to manipulate the emotions of the recipient, creating a sense of fear, urgency, or trust to elicit the desired response.

To protect against AI-generated scam calls:

- ****Be Skeptical:**** If a call seems suspicious or unexpected, be cautious, and avoid providing sensitive information.
- ****Verify Identities:**** If the caller claims to be a friend or family member, verify their identity by contacting them through a known and trusted method before taking any action.
- ****Avoid Immediate Actions:**** Scammers often create a sense of urgency. Take the time to think and verify information before making any decisions.

As technology evolves, it's crucial for individuals to stay informed about potential scams and employ security measures to protect themselves from deceptive practices.

Craigslist Scams

Craigslist, being a popular online marketplace for buying and selling goods and services, unfortunately, can be a platform for various scams. Here are some common Craigslist scams to be aware of:



Fake Rental Listings

Scammers may post fake rental listings for properties that don't exist or aren't available for rent. They might ask for a deposit or payment upfront, and once the payment is made, the victim discovers there is no rental property.



Ticket Scams

Scammers may offer fake tickets for events, concerts, or shows. After receiving payment, they may disappear, leaving the buyer with invalid tickets or no tickets at all.



Overpayment Scams

In this scam, a buyer or seller might send a check or money order for an amount higher than the agreed-upon price. They'll then ask the victim to refund the excess amount. The original payment is likely to be fake, and the victim loses money when the bank discovers the fraud.



Shipping Scams

Some scammers pose as buyers and offer to pay more for an item if the seller ships it to them. After the item is shipped, the payment is often fake or disputed, leaving the seller without their item and without payment.



Craigslist Scams

Identity Theft

Scammers may pose as legitimate sellers, asking buyers to provide personal information for a background or credit check. This information can then be used for identity theft.



Phishing Scams

Scammers may send emails pretending to be from Craigslist, asking users to update their account information. The emails contain phishing links designed to steal login credentials.



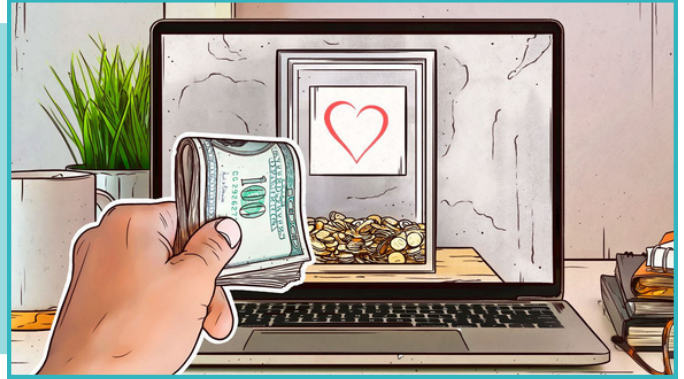
Tips to Avoid Craigslist Scams

- **Meet in Person** : Whenever possible, conduct transactions in person and in a safe, public location
- **Cash Transactions** : Use cash for in-person transactions to avoid payment-related scams.
- **Verify Identities** : If renting or purchasing, verify the legitimacy of the other party through reliable channels.
- **Trust Your Instincts** : If something feels off or too good to be true, it probably is. Be cautious and don't rush into transactions.

Always exercise caution when using online marketplaces, and report suspicious activity to the platform to help protect yourself and others from scams.

Charity Scams

Charity scams involve fraudulent activities where individuals or organizations falsely claim to represent charitable causes to exploit people's generosity. Here are common characteristics of charity scams :



Fake Charities

Scammers create fictitious charities or mimic the names of legitimate ones to deceive potential donors



Unsolicited Contact

Victims may receive unsolicited emails, phone calls, or direct messages from scammers claiming to represent a charity. Legitimate charities typically don't use aggressive or unsolicited tactics.



Pressure Tactics

Scammers often use high-pressure tactics, claiming there's an urgent need for donations. They may create a sense of urgency by describing a recent disaster or crisis.



Emotional Manipulation

Charity scammers play on emotions, using heartbreaking stories or images to evoke sympathy and encourage donations



Similar-Sounding Names

Scammers may choose names that sound similar to well-known and reputable charities to mislead donors.



Charity Scams

Fake Websites

Fraudsters create fake websites that mimic legitimate charity sites to trick people into making donations. These websites may look convincing but lack proper security measures.



Payment Requests

Scammers may request donations via unconventional methods, such as wire transfers, prepaid cards, or cryptocurrency. Legitimate charities usually provide multiple secure payment options.



Tips to Avoid Charity Scams

- **Research the Charity** : Before donating, research the charity independently. Verify their legitimacy through trusted sources, such as the Better Business Bureau, Charity Navigator, or GuideStar.
- **Check Contact Information** : Confirm the charity's contact information through their official website or contact details listed on reputable charity databases.
- **Be Skeptical of Unsolicited Contact** : Be cautious if you receive unexpected emails, phone calls, or messages requesting donations. Reach out to the charity directly through official channels to verify.
- **Look for Red Flags** : Watch for red flags, such as high-pressure tactics, requests for payment in unusual forms, or vague explanations of how funds will be used.
- **Secure Donation Channels** : Use secure and well-known donation channels provided by the official charity. Avoid making payments through unconventional or insecure methods.
- **Verify the Website** : Check the website's URL to ensure it matches the official charity's site. Be cautious if the site lacks security features like HTTPS.

By exercising due diligence and being cautious, individuals can protect themselves from falling victim to charity scams and ensure their donations reach legitimate and deserving causes.

LinkedIn Scams

LinkedIn, being a popular professional networking platform, is not immune to scams. Here are some common LinkedIn scams to be aware of



Connection Requests from Fake Profiles

Scammers create fake profiles and send connection requests to gather personal information or engage in fraudulent activities.



Phishing Messages

Scammers may send phishing messages posing as recruiters, potential employers, or colleagues, aiming to trick users into providing sensitive information or downloading malicious content.



Job Scams

Fraudulent job postings or messages offering lucrative opportunities may be used to collect personal information, conduct phishing attacks, or even request payment for fake job placement services.



Fake Endorsements and Recommendations

Scammers may create fake profiles to endorse or recommend other users for skills or services, attempting to build credibility for their own fraudulent activities.



InMail Scams

Scammers may use LinkedIn's InMail feature to send messages that appear to be from legitimate sources, luring users into clicking on malicious links or providing sensitive information.



LinkedIn Scams

Impersonation of Company Officials

Scammers may create profiles impersonating high-ranking officials within companies, attempting to trick employees into revealing sensitive information or transferring funds.



Premium Subscription Scams

Scammers may create profiles impersonating high-ranking officials within companies, attempting to trick employees into revealing sensitive information or transferring funds.



➔ Tips to Avoid LinkedIn Scams :

- **Verify Profiles** : Before accepting connection requests, verify profiles to ensure they are legitimate. Look for mutual connections, a complete profile, and relevant professional information.
- **Be Skeptical of Unsolicited Messages** : Be cautious with messages from unknown individuals, especially if they are unsolicited. Avoid clicking on links or providing personal information unless you can verify the sender's legitimacy.
- **Check Job Postings** : Investigate job postings thoroughly. Be skeptical of opportunities that seem too good to be true or require payment for job placement.
- **Review Privacy Settings** : Regularly review and update your privacy settings on LinkedIn to control who can see your information and contact you.
- **Report Suspicious Activity** : Report any suspicious profiles or messages to LinkedIn. The platform takes user reports seriously and investigates potential scams.
- **Enable Two-Factor Authentication (2FA)** : Enhance the security of your LinkedIn account by enabling two-factor authentication

By staying vigilant and following these tips, users can reduce the risk of falling victim to LinkedIn scams and maintain a secure professional presence on the platform.

Paris Olympics Scam

Criminals seek opportunities to exploit major events making headlines. With the upcoming Paris games this summer, there is a concern that the fake emergency scam, similar to the grandparent scam but with slight variations, might resurface. The modus operandi involves hackers compromising someone's email account. Subsequently, all contacts in that account receive a message claiming an emergency, such as a stolen wallet in Paris, and requesting assistance through gift cards or Venmo deposits.



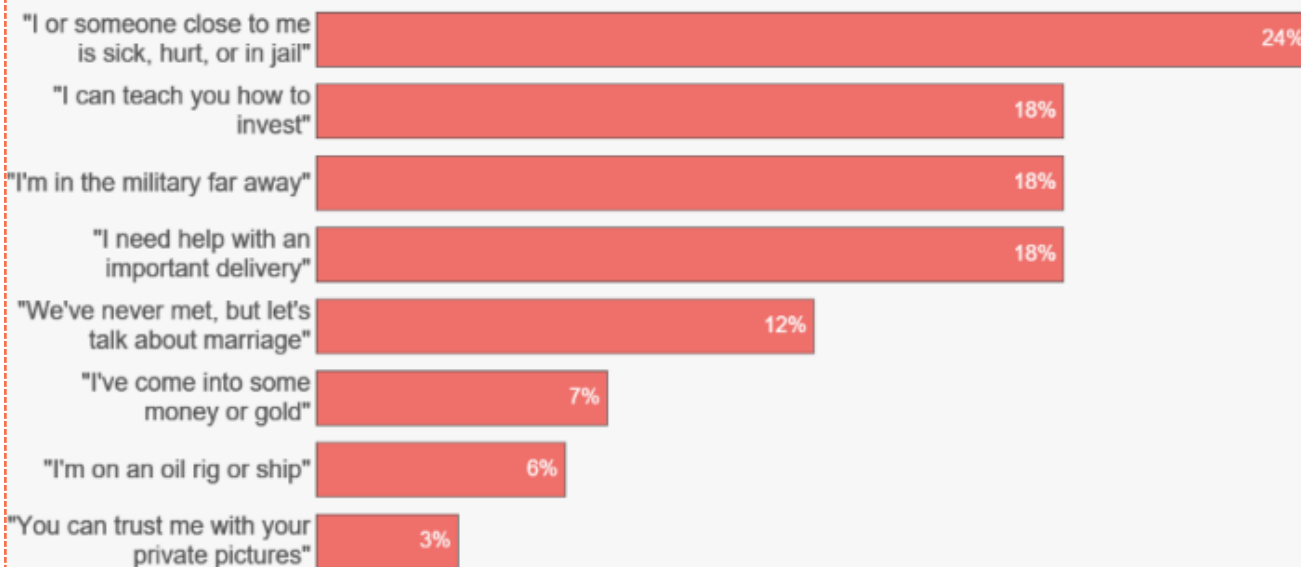
This scam could appear convincing to recipients who quickly associate the situation with the person's past experiences or interests. Olympics officials are cautioning ticket seekers about avoiding fraudulent ticketing sites and scam emails pretending to be from Paris 2024 or the Olympic committee.

To stay safe, it's advised not to react immediately to requests for cash from friends in Paris. Instead, follow the Federal Trade Commission's guidance and attempt to contact the person through alternative means, like a phone call. Verify the situation with a trusted source who knows the individual and can confirm their travel plans.

For those planning to attend the Paris Olympics, the official website for Paris 2024 emphasizes that legitimate communications will never ask for login details or banking information. It's crucial to scrutinize email addresses, as scammers often alter a single letter or number or use a different domain extension to create a fake appearance similar to the authentic address.

Romance Scams

Romance Scammers: Their Favorite Lies by the Numbers



Figures are based on 8,070 2022 romance scam reports that indicated a dollar loss and included a narrative of at least 2,000 characters in length. Lies were identified using keyword analysis of the narratives.

Romance scams involve fraudsters building fake romantic relationships with individuals to exploit their emotions for financial gain. These scams often occur online, where scammers create a false identity to gain the trust and affection of their victims. Here are common characteristics of romance scams:

Online Dating Platforms

Scammers often use dating websites, social media, or other online platforms to find potential victims. They create fake profiles with attractive photos and elaborate background stories.



Building Trust

Scammers invest time in building emotional connections with their victims. They may use fake personas, express love quickly, and claim to have common interests.



Request for Money

Once trust is established, scammers invent a crisis or urgent situation that requires financial assistance. They may ask for money to cover medical bills, travel expenses, or other supposed emergencies.



Romance Scams

Long-Distance Relationships

Many romance scams involve scammers claiming to be located in another country, making it difficult for victims to verify their identity.



Avoiding In-Person Meetings

Scammers often make excuses for not meeting in person, citing various reasons such as work commitments, health issues, or travel restrictions.



Use of Stolen Photos

Scammers commonly use stolen photos from real individuals to create a convincing online persona. Reverse image searches can help verify the authenticity of profile pictures.



Unusual or Rushed Declarations of Love

Scammers may declare love quickly, often faster than what would be considered normal in a genuine relationship. This is a tactic to intensify the emotional connection.



➔ Tips to Avoid Romance Scams :

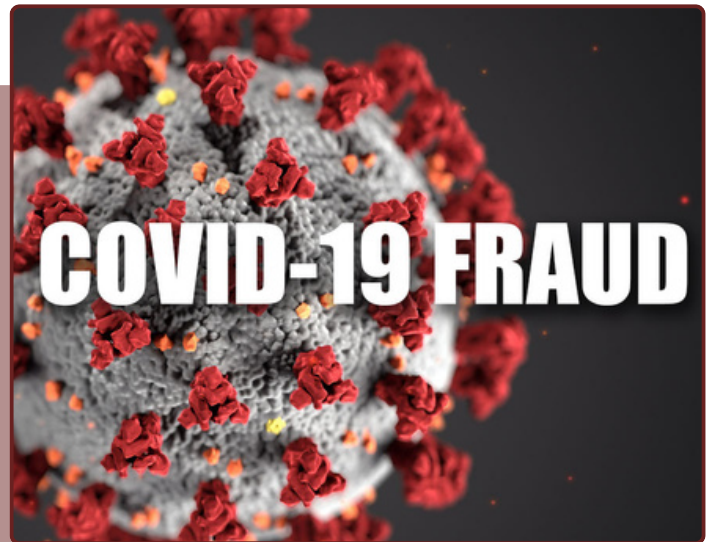
- **Be Cautious** : Exercise caution when developing relationships online, especially if the person seems too perfect or if the relationship progresses rapidly.
- **Verify Identity** : If you have suspicions, verify the person's identity through online searches or reverse image searches to check if their photos appear elsewhere on the internet.
- **Never Send Money** : Avoid sending money to someone you've met online, especially if you haven't met them in person. Scammers often use financial requests to exploit victims.
- **Protect Personal Information** : Be cautious about sharing personal information, such as addresses, financial details, or other sensitive data, with someone you've just met online.
- **Educate Yourself** : Stay informed about common tactics used by romance scammers and be aware of warning signs.

If you suspect you are involved in a romance scam, cease communication immediately and report the incident to the relevant authorities or the platform where you met the individual.

COVID Scams

Amid the peak of the COVID-19 pandemic, criminals exploited the situation by offering purported free coronavirus tests. Their aim was to collect individuals' Medicare numbers and other personal details, enabling them to file fraudulent claims in the victims' names.

During the COVID-19 pandemic, various scams emerged capitalizing on the situation. Common COVID scams include :



Phishing Emails

Scammers send emails posing as health organizations or government agencies, tricking recipients into revealing personal information or clicking on malicious links.



Fake Charities

Fraudulent charities claim to support COVID-19 relief efforts, soliciting donations that never go to legitimate causes.



Fake Testing or Treatment Offers

Scammers may offer fake COVID-19 tests, treatments, or vaccines, preying on individuals' fears and uncertainties.



Price Gouging

Sellers exploit high demand for pandemic-related items by inflating prices on essential goods like masks, sanitizers, and medical supplies.

