SCAMS

SCAMMERS DO NOT DISCRIMINATE

Scammers target people of all backgrounds, ages and income levels. Fake lotteries, Internet frauds, get-rich-quick schemes and miracle health cures are some of the favoured means of separating the unwary from their money. New varieties of these scams appear all the time.

LOTTERIES, SWEEPSTAKES AND CONTESTS

- You cannot win money or a prize in a lottery unless you have entered it yourself, or someone else has entered it on your behalf.
- You cannot be chosen as a random winner if you don't have an entry.
- A fake prize scam will tell you that you have won a prize or a contest. You may receive a phone call, an email, a text message or see a pop-up screen on your computer. There are often costs involved with claiming your prize, and even if you do receive a prize, it may not be what was promised to you.

PYRAMID SCHEMES

- In a typical pyramid scheme, unsuspecting investors are encouraged to pay large membership fees to participate in moneymaking ventures. The only way for you to ever recover any money is to convince other people to join and to part with their money as well.
- People are often persuaded to join by family members or friends. But there is no guarantee that you will recoup your initial investment.
- Pyramid schemes inevitably collapse and you will lose your money.

MONEY TRANSFER REQUESTS

- there is the scam email that claims to be from a lawyer or bank representative advising that a long-lost relative of yours has died and left you a huge inheritance.
- Scammers can tell such genuine sounding stories that you could be tricked into providing personal documents and bank account details so that you can confirm their identity and claim your inheritance.
- The "inheritance" is likely to be non-existent and, as well as losing any money you might have paid to the scammer in fees and taxes, you could also risk having your identity stolen.

INTERNET SCAMS

- Any email you receive that comes from a sender you do not know, is not specifically addressed to you, and promises you some benefit is likely to be spam.
- **Malicious software**—also referred to as malware, spyware, key loggers, trojan horses, or trojans—poses online security threats.
- Scammers try to install this software on your computer so that they can gain access to files stored on your computer and other personal details and passwords.
- **Phishing scams** are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate but in reality genuine organizations like a bank or a government authority will never expect you to send your personal information by an email or online.

MOBILE PHONE SCAMS

- Missed call scams start by scammers calling your phone and hanging up so quickly that you can't answer the call in time. Your phone registers a missed call and you probably won't recognize the number. You may be tempted to call the number to find out who called you.
- If it is a scam, you will be paying premium rates for the call without knowing. Text message scams work in a similar way, but through a Short Message Service (SMS).
- Scammers send you a text message from a number you may not recognize, but it sounds like it is from a friend—for instance: "Hi, it's John. I'm back! When are you free to catch up?" If you reply out of curiosity, you might be charged at premium rate for SMS messages (sometimes as much as $4 for each message sent and/or received).

HEALTH AND MEDICAL SCAMS

- **Miracle cure scams** offer a range of products and services that can appear to be legitimate alternative medicines, usually promising quick and effective remedies for serious medical conditions.
- **Weight loss scams** promise dramatic weight loss with little or no effort. This type of scam may involve an unusual or restrictive diet, revolutionary exercise or "fat-busting" devices, or breakthrough products such as pills, patches or creams.
- **Fake online pharmacies** use the Internet and spam emails to offer drugs and medicine at very cheap prices and/or without the need for a prescription from a doctor. If you use such a service and you actually do receive the products in response to your order, there is no guarantee that they are the real thing.

EMERGENCY SCAMS

- In the typical scenario of an emergency scam, a grandparent receives a phone call from a scammer claiming to be one of his or her grandchildren. Callers go on to say that they are in some kind of trouble and need money immediately. They claim to have been in a car accident, are having trouble returning from a foreign country or they need bail money.

DATING AND ROMANCE SCAMS

Scammers will try to build a friendship with you, perhaps even sending you flowers or other small gifts. After building a relationship, the scammer will tell you about a large amount of money they need to transfer out of their country, or that they want to share with you. They will then ask for your banking details or money for an administrative fee or tax that they claim needs to be paid to free up the money.

HANDY HINTS TO PROTECT YOURSELF

- Only give out your personal details and information where it is absolutely necessary and when you trust the person you are speaking to or dealing with.
- Destroy personal information: don't just throw it out. You should cut up or shred old bills, statements or cards—for example, credit cards and ATM cards.
- Treat your personal details like you would treat money: don't leave them lying around for others to take.

INTERNET BUSINESS

- Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.
- Beware of websites offering "free" downloads (such as music, adult content, games and movies). Downloading these products may install harmful programs onto your computer without you knowing.
- Avoid using public computers (at libraries or Internet cafes) to do your Internet banking or online shopping.
- Choose passwords that would be difficult for anyone else to guess—for example, passwords that include letters and numbers. You should also regularly change passwords.

WHAT TO DO IF YOU GET SCAMMED!

- Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to reduce the damage and avoid becoming a target for a follow-up scam.
- Report a scam. By reporting the scam to authorities, they may be able to warn other people about the scam and minimize the chances of the scam spreading further.
- If you sent money through an electronic funds transfer (over the Internet), contact your financial institution immediately. If they have not already processed the transfer, they may be able to cancel it.

General Internet and Smartphone Safety Tips

- Set strong passwords
- Combination of numbers, letters and symbols: ICARMP2 ("I CAN ALWAYS REMEMBER MY PASSWORD)
- Software upgrades for your device – get the most current upgrade that includes the latest security features
- Do not click on suspicious links and attachments
- Privacy settings for your social network accounts
- Think twice before connecting or posting (connect and share with people you know in real life)