Identifying a Scam: Do Your Research and Protect Yourself

1. Does the email, text message, or automated phone message claim to be from the CRA?

The CRA will never contact you via text message and will not ask for financial information via email. The CRA will also never use threatening language, threaten to arrest or report you. They may ask you for some information over the phone, but will never demand immediate action or payment. Do not let scammers scare you!

2. Is a company asking you for personal information over the phone or online?

People often receive emails or phone calls claiming to be a well-known company, such as a bank or a telephone company. They may ask for your full name or SIN. Never provide information via email or over the phone unless they are calling from a number you know and trust. If you are unsure, hang up, do some research and contact the company to yourself to confirm why they are calling.

3. Does the email or text message claim to be a legitimate organization and is asking you to click on a link to verify personal information?

Legitimate organizations will never ask you to verify information online. Do not click on links, even to unsubscribe. Contact the organization using the information on their website or in person to confirm if the information is needed.

4. Be careful when you are shopping online. Check to see if a link leads you to another website to buy the product.

Never buy a product from a link that is not associated with a legitimate website, such as EBay. If there is an issue with payment or you never receive the product, you will not be protected by the legitimate website. To check if a website is secure, make sure the link starts with 'https' and has a padlock symbol beside it.

5. Does a website prompt you to enter your credit card information for a 'free' trial?

Companies will claim that they will only start taking money from you if you do not cancel after the free trial. However, entering your credit card information is often an agreement to pay. Be sure to read the fine print and cancellation policy before signing up. Check out the company and product reviews.

6. Does an advertisement claim they can send supplements or medications without a prescription?

Products offered on websites claiming to be an online pharmacy may not be the real product or could even be unsafe to use. Remember that legitimate online pharmacies still require a prescription. Make sure to check out the company before you buy.

7. Does an advertisement encourage you to make a rushed decision?

Some advertisements, often online or email, use language that encourages you to buy the product right away. Advertisements will often claim that the price or offer is 'for a limited time only'. Do not sign up or buy without reading reviews of the company or product.

8. Does an advertisement claim to have a fast cure for a serious condition?

Advertisements often claim that they have a product that can cure a condition or produce fast results. This may include weight loss supplements and hair growth treatments. Never buy under pressure, especially if the payment plan is long term, and remember that 'miracle' treatments do not exist. Do your research!

9. Is a door-to-door salesperson pressuring you to buy a service or product that same day?

Scam artists often use high-pressure tactics to convince you to make major purchases that very that same day. This can include water heaters or other expensive products. You may never receive the product or you may receive a lower quality product. Legitimate salespeople do not pressure you. Make sure to ask for the person's name and company. Never give a door-to-door salesperson personal information, such as copies of bills. Take time to research a product before you buy.

10. Is someone you met on a dating site asking you to send money?

People can be very convincing when expressing their feelings for you especially online. Be careful, they may be claiming to be someone they are not. They might tell you they need money for some kind of emergency or to travel to meet you. Never send money to someone you have only met online.

11. Does a person you are communicating with claim to be the CEO of the company you work for?

This type of scam is common when you are an employee who has access to company funds. If you receive an email claiming to be from a senior manager or a CEO asking you to send money to a third party to secure a deal or contract, be careful. Confirm the transaction in person. Encourage your employer to have a standard process for transferring money so that scams are easily identifiable.

Connecting on Disability and Abuse
S'engager contre l'abus envers les personnes ayant un handicap

FIND OUT MORE

For more information on different types of scams/fraud and how to protect yourself, visit **The Little Black Book of Scams** site, **The Canadian Anti-Fraud Centre** site, or the **Canada Revenue Agency** site.