How to prevent wire fraud scams

One day, Josie (not her real name) receives an unexpected email from her aunt, explaining that a flood has occurred in the family home and they urgently needed an extra $3000 to help with the cleanup. Her aunt also mentions the family banking details have changed and provides instructions for a wire transfer to be sent to their new account. She doesn't hesitate and sends the money right away.

The next day, she calls her aunt and asks if she's received the money. Her aunt is shocked to learn about the wire transfer. She explains there hasn't been a flood, there isn't a need for an extra $3000, and she didn't send her an email in the first place.

By the time Josie and her aunt contact their banks and the appropriate authorities, a fraudster has already transferred the money to a new account. The money is long gone. Josie has just become a victim of a wire fraud scam!

What is social engineering?

Josie didn't think she could be scammed. She knows the tips on how to spot phishing scams, understands how to protect herself online, and has the highest privacy settings active on her social media. However, the fraudster didn't rely on common cyber tactics to trick Josie into sending money; instead they used social engineering.

Social engineering is the exploitation of human psychology to manipulate someone into performing a desired action. In Josie's case, the fraudster researched her financial habits and personal background.

They learned that Josie often sends money overseas and manipulated her by creating a sense of urgency and playing on her sympathy. The fraudster created a valid email address that looked identical to her aunt's, took advantage of the different time zones between Canada and Spain, and fabricated a scenario to convince her into sending the wire to an unfamiliar account.

Spot the scam

Josie's situation is not unique. There are many ways fraudsters lure victims into wiring funds. The initial hook can take many forms but, in every case, the scam ends the same way. You're asked to wire money and once you do, it's usually gone for good. Here are common types of wire fraud scams to look out for:

1. **Emergency scam**
   In this type of scam, a fraudster – maybe impersonating someone you know – will claim that there's some type of emergency and they need financial help. They'll often make the request by email, prey on your feelings of sympathy and create a sense of urgency.

   - **How to protect yourself:** If you know the person, always contact them to confirm that the story is true, using a phone number or email address you know to be genuine. If you don't know the person, delete the message. It is a scam.

2. **Romance scam**
   You receive a message from an admirer on social media or a dating site. This person strikes up a conversation and after chatting for several days, they seem like the perfect match for you. Sometime into the online relationship, the person makes up a sob story about how they need money for a personal tragedy, or that they want to visit you but can't afford the travel costs.

   - **How to protect yourself:** Don't send money to a stranger under any circumstance. Only send funds to someone with whom you've developed a long-term, trusted relationship. Keep in mind: when meeting someone online, do your research by doing an image search to see if their photos

belong to someone else. They may be stealing someone else's identity. Look out for inconsistencies in their profile and in your conversations, this may point to a big lie. Assume this is a scam.

3. **Investment scam**
   A fraudster claiming to be a stockbroker or portfolio manager offers you the chance to invest in an overseas company, product or property that will earn huge rewards with little risk on your part. The fraudster's offer seems legitimate and they have resources to back up their claims such as a fake website or call centre.

   - **How to protect yourself:** If the offer seems too good to be true, it is. Never invest in a company, product or property that doesn't have a solid & verifiable reputation. When in doubt, get a second opinion from your advisor.

Watch out for the red flags of wire fraud scams

The request is:
- Urgent or made right before the end of the business day
- Inconsistent with previous requests for funds, e.g. large amount, different recipient
- Too good to be true

The individual requesting money:
- Is someone you don't know
- Refuses using other common payment methods
- Insists on communicating via online platforms only
- Is unavailable by phone

The email:
- Has an incorrect return address e.g., 0 instead of o, 1 instead of l, extra underscore, altered domain name
- Contains odd or incorrect words, spelling, or phrases

The bottom line

As in Josie's case, a wire fraud scam can happen to anyone. Although she missed the red flags, she contacted her bank as soon as possible to report it, ensuring her remaining funds were protected, and avoiding future losses.

If you think you may be a victim of a wire fraud scam, contact your financial institution immediately. For additional resources, the Competition Bureau of Canada offers a great resource for **recognizing the latest types of fraud scams**.

Sources:
- *Ontario Securities Commission*
- *Canadian Bankers Association*
- *Alberta Securities Commission*

- *Government of Canada Anti-Fraud Centre*
- *Government of Canada Finance Department: Protection from frauds and scams*