Spotting Scams

These days, the increasing number of scams can make you want to sell your belongings and live off the grid. According to Franssen, there are easy ways to keep a little peace of mind, such as not answering unknown phone calls.

Phishing, by definition, is the act of sending fraudulent communications (emails, Short Message Service (SMS), phone calls) that appear to come from a legitimate or reputable source with the intention of stealing personal information and/or money.

These messages can appear like real communications from your bank, government, police, streaming service, or even gym membership. They can look like this:

Examples of Phishing.pdf

These messages will often include language that threatens to terminate your membership, pursue you for illegal activities, or bill you for false expenses. It will ask for credit card numbers and pins, passwords and your contact information so it can assign your information for other scams. **Some simple ways to spot phishing scams are:**

1. The legitimate source that the message is from isn't from the region or even a service you use. (i.e,. Netflix sends you an email saying your payment is overdue, but you don't have an account with them. Or you receive a call from Las Vegas, Nevada when you live in Oshawa, Ontario and don't know anyone there.)
2. The message seems pixelated or blurry. Often, scammers will copy and paste or send screenshots of messages but the quality will become distorted.
3. Upon receiving a message that seems suspicious, you call the source directly and confirm they've sent the message. (i.e. TD Bank sends you an email with information in regards to your account. Instead of replying, search for the number of your local TD Bank branch and have them confirm the information in the message. if they cannot, then it is a scam.)

In the instance that you've been called, do not pick up if you do not recognize the number. Another tip from Franssen is to not have an outgoing message on your cell phone. Some automated phishing scams done by machines can use your outgoing message to determine:

1. The number is active and in use.
2. Your gender.

3. Your age (roughly).
4. Your location (regionally).

It opens you up to a world of new potential ways to be scammed, all because you were trying to be polite and professional with a voicemail.