TELUS Keeping Yourself Safe Avoiding Online Scams

[TELUS Wise online basics 11. Keeping yourself safe: avoiding online scams]

[Female Narrator]

Many people worry about becoming victims of online scams. In these situations, scammers try to trick people into giving them money or personal information. There are a lot of scams to be aware of and they can cost you a lot of money if you aren't careful. Luckily, knowing what to watch out for can help you spot and avoid almost any online scam.

There are two main things that scammers try to get from you.

[Money, Personal Information]

Either they'll want you to send the money, or they'll want your personal information.

[Bank account information, Credit card information]

A lot of times they'll try to get your bank account or credit card information so that they can get money from you, or they'll try to get your passwords for your email or social media accounts

[Email passwords, Social media passwords]

so that they can pretend to be you.

Scams can come to you in different ways. Many come through email. So, you should be suspicious of email you received from someone you don't know. The same is true of text messages or messages on social media, like Twitter or Facebook. Sometimes though, scammers will pretend to be someone you do know. One of your contacts may have downloaded malware. That makes their computer send emails that look like they are coming from them and are meant to trick you in some way. One popular scam is to send a message that appears to be from one of your contacts saying that they are in trouble and need money right away. Don't answer these messages. If you think the person you know might really be in trouble, use verified contact information to get in touch with them to find out if they actually need your help.

Often scam emails ask you to send information, or money, update a password, or click on a link. They may also try to scare you by saying one of your accounts is about to be closed. These types of emails are called phishing scams, where a scammer will try to trick you into giving them information about your bank accounts or online activities.

[Phishing emails ask for: Information, Money, Password update, Account action]

Be cautious if you receive a message that appears to be from your bank, internet provider or Canada Revenue Agency asking you to provide or verify personal information. Instead of clicking on links in such emails go to the organization's website directly, find their contact information and call them on the phone to find out if there really is something they need from you.

Sometimes scammers may try to trick you by making you think they will give you money or even a free trip. You might get a message telling you that you have a tax refund, that you've won the lottery or that you might be able to benefit from taking part in a business deal. Sometimes they may just want you to click on a link that will enable them to either steal your personal information or install malware on your computer. No matter what remember that if something seems too good to be true, it probably is. If you got a message like this, just delete it. If you think there's a chance it might be true, go to the sender's official website to investigate the messages claim or call the sender on the phone.

[Official Website]

Don't use a phone number or web address from the message. Look it up.

How can you tell if an email you've received is a phishing scam? Imagine that you got an email, it's designed to make it seem as though your Netflix subscription is about to be canceled. While it's possible to get an email like this from a company you deal with, it's still a reason to be suspicious. Especially if you don't have any reason to think there's a problem with your Netflix account. Next, look at the “From” address. An email from Netflix should come from an address that ends in netflix.com. This one doesn't, so the sender is misrepresenting who they are.

[From: Netflix NetflixAccount@notice-access_273.com]

There is also a big restart membership button you're being asked to click on. That likely won't take you to Netflix, but instead to a website that looks like Netflix, where you will be asked for your credit card information.

Remember that it's pretty easy to make a fake website that looks real but it's a lot harder to fake a web address. If you want to confirm the web address, you can go to Google and search for Netflix or look for it on one of your receipts or invoices. You could also go to the Netflix site and check your account to confirm your subscription status. Another thing you can do is search for what the message is promising you. Suppose you get an email that says it's from Apple offering to enter you into a drawing for a free iPhone if you click on a link. If you search for “Apple” and an “iPhone contest” and add the word scam, for example, the top results may likely be warnings about the scam.

One last kind of scam that doesn't directly involve money is identity theft where someone pretends to be you so they can register for online accounts or apply for credit cards in your name. Identity theft usually happens when a scammer collects personal information about someone online or in other ways and then uses the information to pretend to be them. To keep this from happening, don't share any of these details in a public online space like a social media profile or post. Your full name, including middle names, your full date of birth, including the year, your social insurance number, your mother's maiden name since a lot of people use that as a security question, your credit card information or your driver's license or passport number.

[Don’t share: Full name, Date of Birth, Social insurance number, Mother’s maiden name, Credit card information]

[TELUS Wise]

For more information on online basics, check out the other videos in this series. Visit our website at telus.com/WiseOnineBasics