TELUS Wise®

Tips to help spot email scams.

Many online threats, including ransomware and viruses, make their way into our digital lives through scams known as phishing emails. Phishing emails appear to come from a legitimate source, but trick recipients into clicking on bad links, downloading malicious attachments or visiting fraudulent websites to provide personal and confidential information.

Tips to spot email scams:

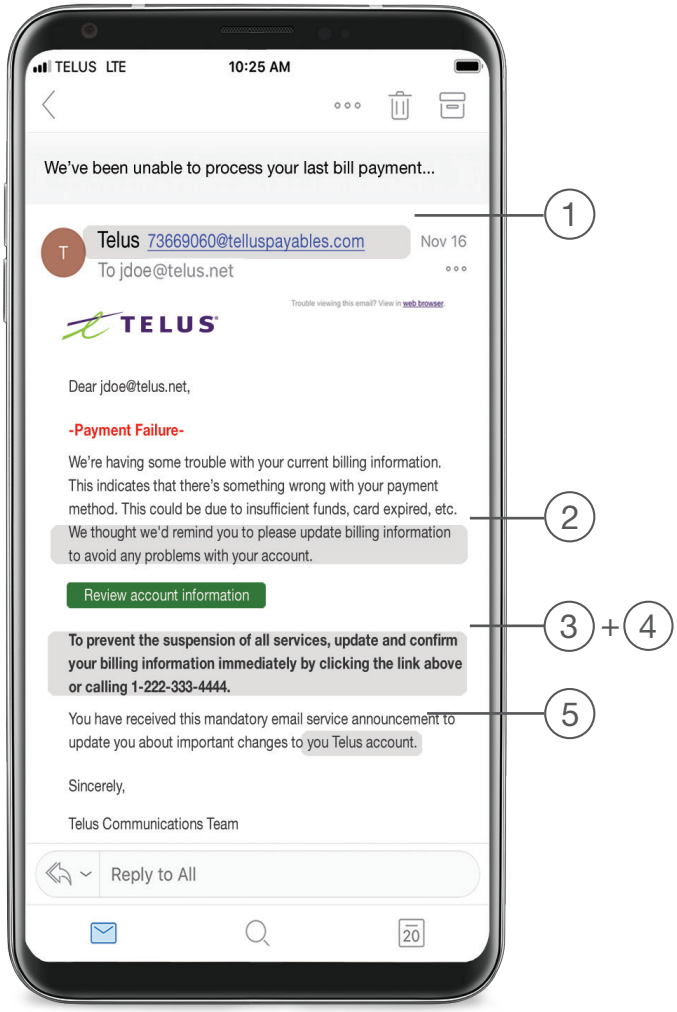
1. **Who is the sender?** Some phishing emails will have familiar domain names, but they are often misspelled or the sender's email address is a long string of letters, numbers and characters.

2. **Is the email asking for personal information?** TELUS and other reputable organizations and service providers (e.g. CRA, banks, etc.) will never ask you to provide personal or account information through unsolicited email.

3. **Scrutinize links and contact information.** When in doubt, call the organization and ask about the email, but first, look up the phone number on a statement or the company's website.

4. **Is the language threatening you to take action?** Warnings of police arrest, account disruptions and immediate deadlines can be another sign of a phishing attempt. Sometimes the body of the email will be intentionally vague, tempting you to click on a bad link.

5. **Does the email use poor grammar and spelling, or sound too good to be true?** If the answer is yes, it probably is! Read emails carefully and don't click on links claiming that you inherited money from a deceased relative or that you won a contest that you didn't enter.



When a suspicious email lands in your inbox, simply trust your instinct and do not click. All phishing emails can be forwarded and reported to **spam@fightspam.gc.ca**.

For more tips on how to stay safe in our digital world, request a workshop by emailing **wise@telus.com** or visit **telus.com/wise**.

Westminster Savings

TELUS