How to Spot Phishing Scams

Phishing attacks are one of the most prominent widespread types of cyber attacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact in order to scam you.

How To Recognize Phishing

Scammers use email or text messages to trick you into giving them your personal information. They may try to obtain your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they are often successful.

Scammers often update their tactics, but some signs will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they are from a company you know or trust. For example, they may look like they are from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. **They may:**

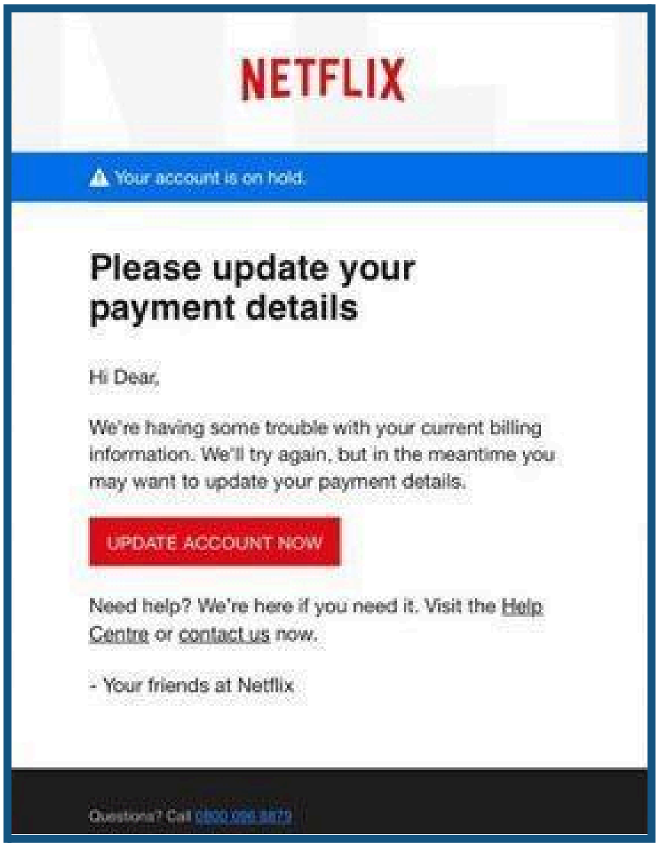
- Say they have noticed some suspicious activity or log-in attempts.
- Claim there is a problem with your account or your payment information.
- Say you must confirm some personal information.
- Include a fake invoice.
- Want you to click on a link to make a payment.
- Say you are eligible to register for a government refund.
- Offer a coupon for free stuff.

Here is an Example of a Phishing Email:

Imagine you saw this in your inbox. Do you see any signs that it is a scam? **Let's examine:**

The email looks like it is from a company you may know and trust (Netflix). It even uses a Netflix logo and header.

- ➔ The email says your account is on hold because of a billing problem.
- ➔ The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably will not use a generic greeting like this.
- ➔ The email invites you to click on a link to update your payment details.
- ➔ While, at a glance, this email might look real, it is not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can harm the reputation of the companies they are spoofing.



Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call 0800 096 8873

How To Protect Yourself from Phishing Attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it is good to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

Four Steps to Protect Yourself from Phishing

1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. The additional credentials you need to log in to your account fall into two categories:
    - Something you have — like a passcode you get via text message or an authentication app.
    - Something you are — like a scan of your fingerprint, your retina, or your face.
    - Multi-factor authentication makes it harder for scammers to log in to your accounts if they get your username and password.

4. Protect your data by backing it up. Back up your data and make sure those backups are not connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What To Do if You Suspect a Phishing Attack

- ➔ If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: Do I have an account with the company or know the person that contacted me?

    - ◆ If the answer is "No," it could be a phishing scam - report the message and then delete it.

    - ◆ If the answer is "Yes," contact the company using a phone number or website you know accurate before engaging with the message.

What To Do if You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security/Insurance Number, credit card, or bank account number, contact AntiFraudCentre-CentreAntiFraude.ca (Canada) IdentityTheft.gov (USA).

If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan.

Need More Help?

For more information, contact Cyber-Seniors at **844-217-3057** or visit **www.cyberseniors.org**.

*This lesson guide was made possible by a **CIRA Net Good Grant**. Learn more at **cira.ca**.*