Fraud Prevention Month

Phishing scams: What you need to know

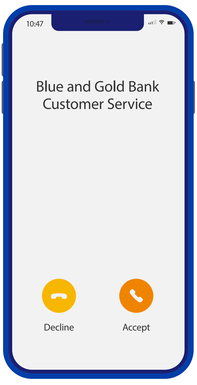
Cybercriminals are counting on us to be distracted and let our guard down. If we do, they can trick us into handing over our personal or financial information using one of their favorite tactics: phishing.

You might be familiar with email phishing but it's not the only type of phishing you can experience. Criminals will also use websites, text messages and phone calls to deploy a phishing scam.

Below are some common forms of phishing that you might encounter and the warning signs to look out for.

Phone-based phishing

Scammers might pose as a financial institution or credit card representative to trick consumers into providing your account number, expiry date, the three-digit security code on the back of their credit card or other sensitive information.



How to recognize phone-based phishing

1. A phone call from **"your credit card company"** or "financial institution", typically from someone who works in the "Security and Fraud Department"
2. You are told your card has been flagged for suspicious transactions and you need to **prove that you have the card** in your possession
3. You are asked to **confirm your account number**, expiry date or the three-digit security code, a one-time passcode that was just sent to you, or your PIN

Email phishing

Typically, you receive an email from a trusted organization (such as your bank), asking you to click on a link. Once you click on the link, you're taken to a site that looks identical to what you were expecting and you may download malware onto your computer, tablet or mobile device.

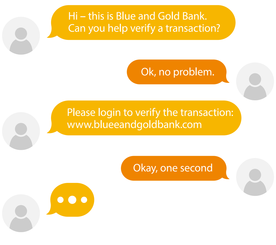
But in this case, it's a phishing site that can capture your log-in information and then use it to possibly drain your account or for other nefarious activities.

How to recognize a phishing email

- Formatting, spelling and grammar **errors** in the subject line or body of the email
- The email address **doesn't match** the organization
- **No contact information.** If something feels suspicious, contact your financial institution directly using the phone number on the back of your card
- **Deadline**. Scammers might include a deadline and threaten account suspension to add urgency to override your normal sense of caution
- **Suspicious hyperlinks.** Avoid clicking on hyperlinks if possible. A single click can cause your computer to become infected with malware
- **Suspicious requests.** Financial institutions do not contact cardholders to request their personal account information. However, if a cardholder calls a financial institution, they will be asked a series of personal questions to validate their identity
- The email does not address you by **name**

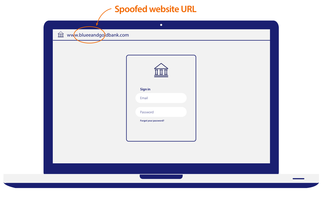
Text message phishing

With more companies using text messages to communicate with their customers, it can sometimes be a little tricky to figure out what's legitimate and what's a scam.



How to recognize a phishing text message

- There's a **link** instead of a phone number to call
- The text you receive may not contain the **name of the bank** or any other information
- The text requests that you **log in** to your bank account to verify a transaction, enter your PIN, or provide your three-digit security code



Website phishing

Scammers are getting better at designing websites that look legitimate. And sometimes, you might click on a link from a search or an email that seems safe, but instead directs you to a fake site run by a scammer.

How to recognize website phishing

- There's something **slightly off** about the web address or the actual page. Look for misspelled words, substitutions or dated logos
- An **unusual pop-up** on the site that requests that you enter your account information
- HTML links that **don't match** their destination

Have you encountered a phishing scam?

If you experience a phishing scam of any sort that uses Visa's name, please let us know by emailing us at **phishing@visa.com.** We appreciate your input and while we can't respond to each email, we fully investigate each claim to help stop fraud at the source.

For more information on phishing and other computer-based scams, visit the Government of Canada's Get Cyber Safe website at **www.getcybersafe.gc.ca/index-en.aspx**