

FRAUD ALERT: Credit card 'phishing' email scam

In an attempt to steal your identity, 'phishing' emails will request personal data or direct you to spoofed websites and phony customer support numbers that will prompt you to provide your valuable information. Be aware that the websites linked to these emails will often include official-looking logos taken from legitimate websites. One example purportedly from Visa states:

"During a recent checkout we detected suspicious activity and your Visa card may have been compromised. Fraudulent activity made it necessary to limit your card for online services.

*Your Case ID Number is: **AY09GP32DD06***

Conform to our security requirements and in order to continue online services with your card, we must validate your identity.

Please use our link below to proceed: [link redacted]"

The email then asserts "Visa"'s commitment to fighting fraud, and features Visa copyright information – otherwise fairly convincing elements in this type of communication. So, how can we determine a scam attempt from a legitimate email?

First and foremost, remember that financial institutions such as Visa do not solicit personal information via email, unless the cardholder initiates contact.

The Visa website [offers these tips](#) on how to protect yourself:

- When submitting personal or financial information on websites, look for the "padlock" icon on your browser's status bar. This signals that your information is secure during transactions. A secure web server should read **https://** rather than just **http://** at the beginning of the web address in your browser's address bar.
- Protect your computer, your sensitive files and your home network from hackers and viruses using tools such as anti-virus software, spyware filters, email filters and firewall programs.
- Do not respond to unsolicited emails asking for sensitive financial information such as credit card numbers, the security code printed on the back of your credit card, or your bank account number, driver's licence number or social insurance number. Be wary of emails that ask you to update or confirm personal information.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balance with your credit card company or bank.

To report or seek advice on dealing with fraud and scam attempts, contact Cynthia Nield at cnield@lians.ca, or 902 423 1300, x346.