Westville Police Service

"Committed to building a safe, healthy, friendly, and engaged community through a high level of policing"

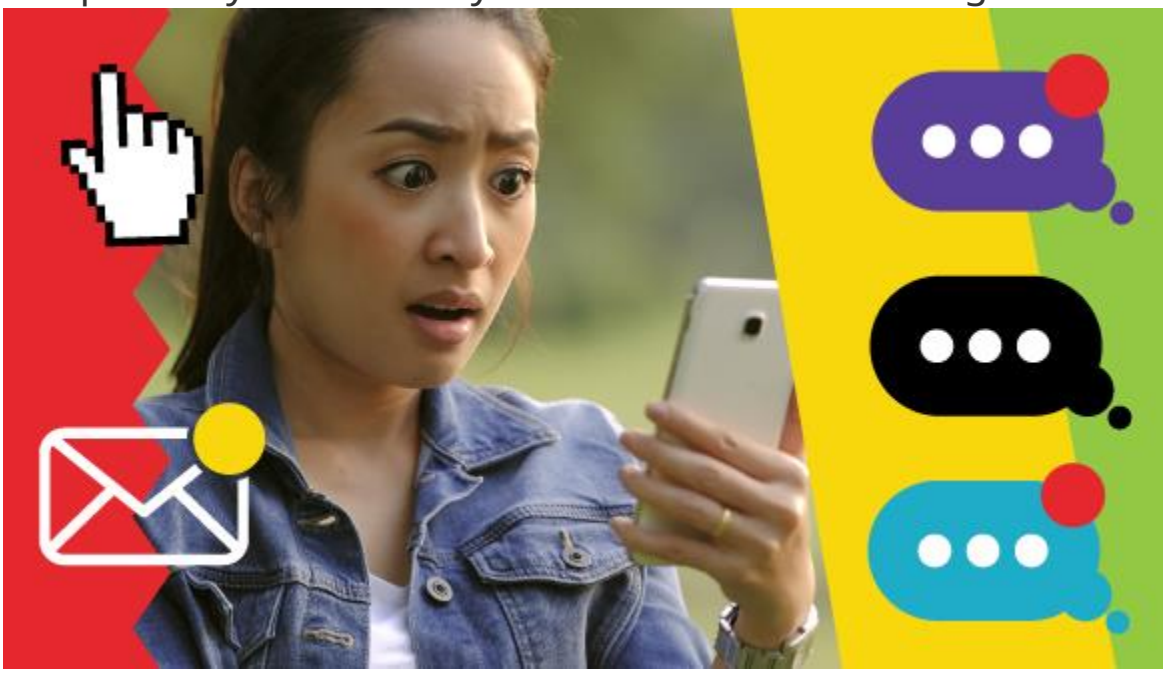
Westville Police Service members responded to 140 calls for service in the month of March 2022. Of the calls for the month, 62 criminal investigations, 16 other provincial statues, 11 municipal by-law enforcements, 13 are motor vehicles related and 38 are other calls to service.

Government of Canada / Gouvernement du Canada

Smishing: An introduction

Get Cyber Safe

Have you ever gotten a text warning you that your account has been compromised? Or that you're getting a refund on your taxes (just click here!)? These are usually signs of text message (SMS) phishing scams, also known as smishing . While using your phone to connect with friends and family might be second nature to you, it also presents unique cyber security challenges. Here's how you can protect yourself and your devices from smishing scams.



What is smishing?

Smishing is a type of phishing scam where cyber criminals try to trick you by sending fraudulent SMS or text messages. They often pretend to be a real business (such as a bank or delivery company), government department or person you know. During the COVID-19 pandemic, scammers have even pretended to be from assistance programs, like the Canada Emergency Response Benefit (CERB) and the Canada Recovery Benefit (CRB), to target vulnerable Canadians.

Smishing messages will often try to get you to click on a link , which may contain malware or lead to a spoofed website. If you click on the link, cyber criminals can then steal your data, your money or even your identity.

Signs of a smishing scam

There are a few easy ways to spot a phishing scam. The best way is to exercise caution whenever you receive a suspicious text message. Ask yourself, “Would this organization try to reach me by text?” Most legitimate organizations will never ask you to reveal personal information through an email or text message.

Most smishing attacks create a sense of urgency in the message and encourage you to respond right away. They may send threats, like claiming they’ll close your account, or offer a time-sensitive reward, such as a prize for a contest you didn’t enter. But no text is ever that urgent — take your time when evaluating a potential smishing message.

Many smishing messages appear to be from a trustworthy and reliable source, like your bank or another business you know.

Always be cautious, even if you think you recognize the business that the message is from.

How to protect yourself

There are many steps you can take to protect yourself and your devices from smishing scams.

If you aren't sure whether a text is real, check with the sender by contacting them through another medium, like the phone number listed on the business' official website.

Avoid clicking on suspicious links or responding to suspicious texts. Whenever possible, you should manually type the web address into a browser instead of clicking on a link in the text message. And fight the urge to click on a link just because you're afraid of missing out on something. Cyber criminals know how to create tempting messages and play on that emotion.

If you think you've received a smishing attempt, delete the message and block the number. Do not reply, even if the text tells you to text "STOP" or "NO" to stop receiving messages. If you reply, the spammer will know your phone number is active and may send more smishing messages.

You can forward any spam text messages to 7726 (SPAM on most keypads). This will let your phone provider block future texts from that number.

Conclusion

Smishing scams can have serious consequences. Knowing how to spot one is the best way to prevent yourself from becoming a victim.

If you suspect that you or someone you know has fallen victim to a smishing scam, don’t hesitate to contact the Canadian Anti-Fraud Centre to report it.