What is Smishing and How to Protect Yourself? Script

You've probably seen it and received it. A text scam from your bank or a government organization like the Canada Revenue Agency. These texts are designed to lure an individual into clicking a malicious link or calling a number posing to be from an official organization. These kinds of scams are known as smishing.

Smishing is a form of phishing that uses text messages instead of email to obtain an individual's information. These messages can arrive by SMS, iMessage, Facebook Messenger, WhatsApp, and other messaging platforms.

Smishing is a particularly common technique for cybercriminals to use. Individuals are more likely to trust the legitimacy of a text message compared to an email.

So how do you protect yourself from smishing scams?

1. **Don't reply to the text message, call the number, or click on any links in the message.** Clicking on a link could give cyber criminals access to your information.
2. **Conduct a web search for the phone number and the message.** Chances are you are not the first person to receive this message.
3. **Contact the organization directly to inquire about the message you've received.** If you believe the message is a scam, contact the organization through their official customer service number to inquire about the message you've received. If they confirm it is not from them, delete the message.

If you think that you may have been the victim of smishing, you should take the following steps:

1. **Change your passwords.** Ensure you have set up a strong and unique password.
2. **Report the incident to the Canadian Anti-Fraud Centre** toll free number. Visit the Canadian Anti-Fraud Centre's What to do if you're a Victim of Fraud page for more information.
3. **Report the incident to your local police**.

Thank you for watching!