What's the big deal if…

…I don't recognize the signs of phone phishing?

Why it is a big deal
• You are likely to fall for a phone phishing attack, and give cybercriminals the information or the means they need to gain access to our electronic network. This puts Canadian citizens' information at risk
Scenario
The "IT Service Team" calls to say your computer is infected with a virus. The agent wants to know what type of anti-virus software you have and asks for remote access immediately, so they can clean your machine before the virus infects everyone's computer. What are the clues that this is a phone phishing attempt?
Possible actions (vote on the correct answer)
• Option 1: The agent asked for remote access to clean your computer • Option 2: The agent asked questions about what anti-virus software is installed on the computer • Option 3: Used fear to motivate you to accept their help
Explanation
• All the options are clues that this is phone phishing • Somebody from the Department's IM/IT National Service Desk will never ask you what software you have – they already know • The National Service Desk does not require remote access to clean your computer of a virus
Key take-aways
• Do not answer any suspicious questions regarding the Department's computer system • Do not give remote access to your computer unless you're sure it's legitimate (legitimate requests come from the National Service Desk or a resolver group as a result of a service request from you) • When in doubt, hang up and tell your team leader/manager as soon as possible. Your team leader/manager must then contact the Regional Security Office to report the incident • Don't rely on your phone's caller ID. Phone numbers can be spoofed
More information
• Voice Phishing