Social engineering prevention - do's and don'ts

Take a minute to have a look at our list of do's and don'ts for dealing with social engineering attacks.

It's always a good idea to slow down, consider the communication you received, and think before responding, selecting links, or opening attachments.

Do

- Be suspicious of any email, text message, or phone call that requests personal or financial information.
- Use passwords that are hard to guess.
- Memorize your passwords.
- Develop passphrases for your passwords to help you remember them.
- Take the time to research any offers that sound too good to be true.
- If you receive an unexpected request from someone you know to share your personal information, contact them using a different communication method to validate the request.
- Hover over email addresses and links with your cursor to view the actual sender's email and URL destination
- Check for spelling and grammar errors, along with poor formatting, visual designs, or logos
- Be suspicious of unusual and high-pressure telephone calls appearing to come from Scotiabank
  - ~ If this happens, hang up and call us at **1-866-625-0561** to report it

Don't

- Don't open attachments or select hyperlinks in emails or text messages sent by unknown senders
- Don't call any number that appears on an email you think is fraudulent
- Don't share your banking passwords or PINs with anyone or any app or website that requires access to your finances, such as budgeting tools like Mint
- Don't use storage media devices, such as external hard drives or USB memory sticks, that you found in a public place
- Don't leave your computer, tablet, or mobile device unattended when you're logged into online banking
- Don't just close the browser when you've finished banking online — always log off
- Don't select a link in an email or pop-up window to go to a site
  - ~ Instead type the web address yourself in a new browser window to ensure you're connecting with the legitimate company

Scotiabank®