Phishing: Don’t Get Caught

Phishing is a type of fraud that uses deceptive e-mails, websites and/or text messages to gather personal, financial and confidential information for fraudulent purposes and/or unauthorized access.

Advice

- The impacts of phishing within a government context may include:
  - Unauthorized access to e-mail, shared drives, and personal drives
  - Accessing unsafe attachments or selecting links within e-mail from unknown sources may release contaminants such as viruses into the e-mail system, may damage your computer and/or impact network resources
- Learn how to spot the difference between legitimate versus potentially fraudulent e-mail messages, websites, and/or text messages - this is the best way to avoid jeopardizing the government network
- Contact the IT Service Desk at 709-729-4357 or email servicedesk@gov.nl.ca, if you have questions about phishing or suspect that you have received a fraudulent e-mail or text message in your government e-mail account

Other Information

Information on Phishing Campaigns

- Phishing campaigns are becoming increasingly difficult to identify as phishers are getting better at impersonating websites we know and trust. Visit the OCIO website to see some examples of phishing e-mails and websites
- Examples include e-mails that provide links to websites that are identical to legitimate service providers including financial institutions, utility services, personal services, etc. The website addresses may include:
  - Misspelled words in the address, such as tdcannadatrust.com, paypall.com, cra.gc.ca.xretal.net
  - Numbers, such as 72.241.13.118/www.bankofamerica.com/, or online.bank.com businessreport.ru/
- Sample content found in fraudulent e-mail messages include:
  - We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity...
  - During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information...
  - You have won a prize, contest, etc. please respond...
  - Someone you know needs a transfer of funds immediately because they are stranded...

What to do to avoid getting “caught”

- Only open attachments from known and trusted sources
- Verify the authenticity of the website address before you select it. You can do this by:
  - Moving your mouse over any link to reveal the actual address
  - Checking the spelling and other characteristics in the address
  - Using your search engine to research an unfamiliar website
- NEVER disclose your password

What to do if you suspect that you have received a phishing e-mail to your government account

- Do not respond, select any links or provide any information!
- Report your suspicion by phoning the IT Service Desk immediately: 709-729-4357 or email servicedesk@gov.nl.ca
- Do not forward the message around as a warning to the entire workgroup, division or department. This expands the number of e-mail accounts potentially affected