Phishing

Phishing is a social engineering method most frequently used by cyber criminals to capture personal and/or financial information from the unsuspecting public. It uses email with a spoofed address and takes the user to fraudulent websites. A 'spoofed' address is an e-mail address that has been forged to make it appear as if it originated from somewhere or someone other than the actual source, including from within your workplace. In phishing attempts, the e-mail may appear authentic with corporate logos, and falsely claims that it is from an established legitimate enterprise, such as a bank, a well-known online business or anywhere a personal account may be used.

A phishing email usually has a tone of urgency and asks the recipient to take immediate action – usually by clicking on a link or opening an attachment (recent phishing emails appear to be from CRA, PayPal, Canada Post, UPS, and Apple). The recipient must act now or there will be a negative consequence. Some offer a positive outcome, such as a prize. The goal is to trick a user into divulging personal and/or financial data such as credit card numbers, account user names and passwords or other valuable information. In some situations the fraudulent website may trick a user into downloading software containing malware onto their computer. Phishing is also used to infect the user's computer with malware (software with a malicious purpose) and use it to send out spam from the user's email address.

More Than One Way to Phish

Phishing has become an extremely lucrative business for cyber criminals. When the term Phishing was coined, it referred to the use of email to lure a person into becoming a victim. With time, the criminals have come up with better quality emails that look official, are well-written and have gone beyond using email. They have come up with other ways to Phish.

- **Spear Phishing** is the targeted version of phishing with attacks that are customized to the recipient of the email (corporate executives, for example). It will be unique in nature, usually contains personal information about the target or their work and is directly addressed.
- **SMS Phishing** or Smishing uses cell phone or smartphone text messages to convince people to divulge their personal information. The method may be a website URL but is often a phone number that connects to an automated voice response system with messaging that demands the target's immediate attention and action. Other tricks such as quizzes or questions will prompt the user to respond with the result being text spam as the user has unknowingly subscribed to premium services at a cost per text.
- **Vishing** scams make use of Voice over Internet Protocol (VoIP) which allows people to talk over their computer lines (e.g. Skype or FaceTime). The criminals call everyone they can and leave an automated message saying the person's credit card or bank account has been compromised, depleted or closed, and to call a phone number for information. (They can make the caller ID appear the way they want.) When people call the number, they are asked to enter their account number, and the damage is done.

Have you been spammed or phished?
There have been cases within government where employees received phishing emails asking for their IDIR user ID and password and have responded to these requests. The responses were used to compromise the employee's mailbox and send thousands of spam emails from their mailbox. What followed was an information security investigation to determine what happened and how much information was exposed.

How do you guard against Phishing?
Remember that legitimate businesses, financial institutions, and Help Desks should never ask you for personal or confidential information via email, voice or text message. Phishing messages are rarely expected, which is a clue in itself. Less sophisticated messages may set off alarm bells because there are misspelled words or faulty grammar. **You can 'hover' your mouse over a URL to see if it is identical to what is written; if they are different, this is an indicator that the source is probably not legitimate.**

In general:

- Be leery if the email was unsolicited.
- Be suspicious if the unsolicited email contains spelling errors or incorrect grammar.
- Best practice is not to trust supplied links, especially if received in unsolicited emails; use a reputable search engine to look up the address and/or company names and go from there.
- Do not reply with any personal, confidential or financial information to 'verify' your identity.
- Monitor your credit card and bank statements. If you believe you have been a victim of phishing contact your local police to get advice and to file a complaint.
- Do not click on "Unsubscribe" in a spam/ phishing email – this lets the spammers know they have hit a "live" address and you will get more emails of this type.
- If you believe the email communication to be valid, contact the company directly.
- If you are unsure what to do when a suspect email is received, best practice is to delete it.

When should I report spam/phishing email?

- When it appears to come from a government source.
- When it is threatening.
- If you have clicked on a link and/or provided your IDIR password.

In these cases, spam/phishing emails should be reported as a Security Incident by Calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866 660-0811 (available 24 hours a day); and selecting option 3.

For more information visit http://www.gov.bc.ca/informationsecurity