3 Key Tips for How to Spot and Avoid Phishing and Vishing Scams

A message from the Federation of Calgary Communities

FEDERATION OF
CALGARY COMMUNITIES

The word phishing comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users. Phishing is the creation of email messages and web pages that are replicas of existing, legitimate sites and businesses. These web sites and emails are used to trick users into submitting personal, financial or password data. You could be asked for information such as credit card numbers, bank account information, social insurance numbers and passwords. The goal of criminals using brand spoofing is to lead you to believe that a request for information is coming from a legitimate company. In reality, it's an attempt to collect your information for the purpose of committing fraud.

With vishing, criminals ask you place a phone call instead of asking you to click on links that direct you to a malicious website. When you call, a recording will ask for personal information like a credit card number. Criminals will then recognize any telephone keystrokes you type in, thus receiving your information. Do not use a phone number provided in an email. Use a phone number that you have independently found (like from your bank or credit card provider) instead.

1. Protect your computer with anti-virus software, spyware filters, email filters and firewall programs which are updated regularly.
2. Do not reply to any email that requests your personal information.
3. Look for misspelled words.

This information was taken from a pamphlet created by the Calgary Police Service and AMA. For more tips and the full pamphlet check out our website www.calgarycommunities.com and look for the Building Safe Communities resources list.