Digital Fraud Awareness

Updated January 2020

Recently, our association was targeted by a Spoofing scam. To our parent volunteers, please be on the lookout for fraudulent emails asking for personal or financial information, especially on behalf of our program. Below are some helpful details, as well as links for more information or reporting purposes.

Email Fraud

Spoofing (pretending to be someone else) and phishing (trying to capture personal info) are tactics used by cyber criminals as an easy way to produce results with very little effort (tricking into sending money/gift cards or into revealing login info; infecting computers by clicking on a link, etc.).

What it is:

- Email fraud is an online safety concern that involves fake emails, text messages and/or website links that are sent by criminals in order to steal personal and financial information (such as user names, passwords, SINs, account or credit card details) to obtain funds or install 'spyware' or malware.'
- The email or text received may seem as if it has been written and sent by a genuine person (a contact you might know) or organization (i.e., a bank).
- The purpose is to trick someone into: providing funds, give up personal or financial information, or allow unauthorized computer access using the following methods:
    - Respond/reply to an 'official' request to provide gift card/money, or update, validate or confirm account information.
    - Click on a web page link to provide user information in order to clear up an 'issue' or to obtain a product or service.
    - Click on a link or download, or send a reply, which may allow them to install malware in order to steal information, or infect associated computer networks, systems and databases to find ways to divert personal emails to them.
- Phishing can lead to financial losses, identity theft, and/or viruses.

http://www.calgary.ca/cps/Pages/Community-programs-and-resources/Crime-prevention/Phishing-and-email-safety.aspx

How to prevent becoming a Spoofing/Phishing victim:

- Practice 'smart-clicking'—think before you click. No matter who asks, you're under no obligation to offer info over email or text (or phone, if it's someone you don't know).
- Recognize that an email or text is requesting information focused on personal or financial details.

- Look for inconsistencies, spelling and/or grammatical errors.
- Check for an embedded hyperlink (or different reply-to address) by hovering your cursor over the link to verify the address.
- Do not **reply to, open an attachment, or click on links or downloads**, in any email that seems suspicious or the sender is unknown to you.
- If you have not clicked on links or replied, DELETE THE EMAIL OR TEXT.
- Keep your software up-to-date to ensure latest protection released by tech companies.
- Install or upgrade virus protection software; ask a professional for more information on how to secure your computer and devices.
- If you think your information or computer may have been compromised, contact your financial institution immediately and report your suspicions; banks will advise on what to do and how to monitor accounts.
- Contact Equifax and Transunion to place fraud alerts on your name if you suspect you are a victim of identity theft.

How to tell if you're a victim of a Spoofing/Phishing attack:

- Your computer runs more slowly than normal or behaves strangely. For example, it makes unexpected sounds, has lots of error messages or shows changes in files or folders.
- It 'freezes' frequently, runs slowly or completely stops responding.
- Computer applications do not work properly.
- Disk drives may be inaccessible or startup unexpectedly.
- There are unusual or unexpected error messages, images, or distorted menus and dialog boxes.
- Your contacts may tell you that they have received email messages from your address (but you haven't sent them anything).
- Your personal firewall may advise you that an application has tried to connect to the Internet although it is not a program that you are running.

For more information, and how you can inform or report:

For excellent information on cybercrime, please visit the Calgary Police Services (CPS) website, www.calgarypolice.ca, and The Canadian Anti-Fraud Centre (CAFC) website, www.antifraudcentre.ca.

- If a crime has occurred (money given or taken), immediately file an online crime report with Calgary Police Services, call 402-266-1234, or visit a District Office.
- The Canadian Anti-Fraud Centre (CAFC) is the central agency in Canada that collects information and criminal intelligence on cyber-fraud. Canadians are encouraged to report instances of fraud to the Canadian Anti-Fraud Centre at: http://www.antifraudcentre-centreantifraude.ca or by calling 1-888-495-8501.