Frequently Asked Questions about Phishing

What is phishing?

Phishing schemes are attempts to steal personal information through fraudulent email that looks legitimate. These email messages often provide links to fraudulent websites where you are asked to disclose credit card numbers, social security numbers, or other private information.

Phishing attempts often direct users to websites that have been "pharmed." Pharming occurs when hackers attack DNS servers and change IP addresses, redirecting users from a legitimate website to a compromised version of the original site.

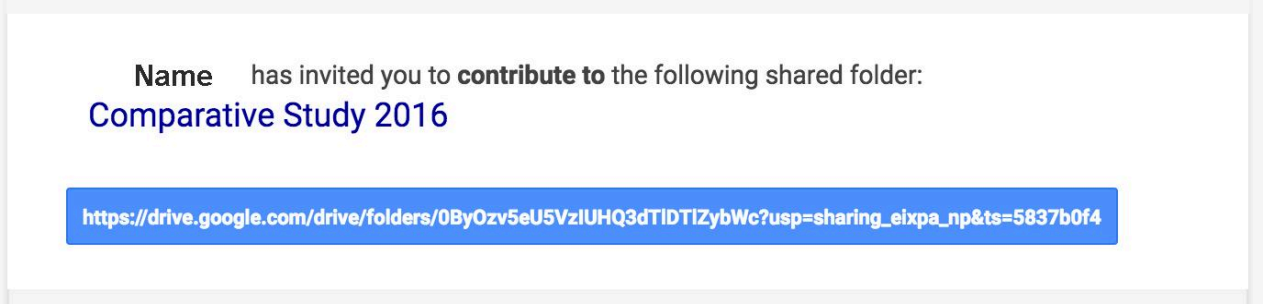
Although phishing is often easily recognizable due to poor grammar or bogus Reply-to addresses, some phishing attempts are relatively sophisticated. Always use caution when replying to unsolicited email.

Is there any easy way to identify fraudulent email?

Phishing email may include requests for the following:

- Sensitive personal information. Legitimate institutions will not request this kind of information through email.
- Lost personal information. Legitimate institutions keep back-up copies of data, so it is extremely unlikely that they would lose your information.
- Urgent action due to account changes that need your immediate attention. Be suspicious. Contact the business directly.
- Sharing of unexpected Google Drive folders or Docs (see example below)

Also, many phishing email scams will address you as Sir or Madam, or as Account Holder, rather than by your name.



How do I avoid becoming a victim of a phishing scam?

- If you get an email in which you are asked for financial or personal information, do not reply or click links within the message.
- Never provide sensitive personal or financial information through email. No legitimate business will ask for this kind of information through email.
- Do not click links in potentially fraudulent email. A link that looks like it points to a valid website could be forged or cause your computer to download malware.
- Use caution when opening email attachments, even if they appear to be from someone you know. Scan the file using your antivirus program before opening it.
- Always try to talk to a real person if you are in doubt.
- Keep your computer's security updated. Using the most recent versions of software can help protect you against phishing.
- Install and use a firewall program.
- Install and use antivirus software.

What do I do if I've been caught by a phishing scam?

- Call IST at 780-492-9400 or contact them through their website.
- Change your password (remember you'll need to update any other devices with the new password - phones, iPads, etc)
- Check your trash - often the scammers get your email to start routing legitimate messages to your trash, so you have several emails you've missed

If you received one of these suspicious emails and you unwittingly provided personal information or financial information, follow these steps:

- **Step 1** - Contact your bank/financial institution or credit card company
- **Step 2** - Contact your credit bureau and have fraud alerts placed on your credit reports:
    - Equifax Canada
    - Toll free: 1-800-465-7166
    - TransUnion Canada
    - Toll free: 1-877-525-3823