Cybercrime Prevention Messaging

Online Shopping

Phishing emails and Pop-Up Ads

Phishing emails are made to look like they came from a real company you know and trust, when in reality it was sent by a scammer. The intention is to trick you into going to a fake website that looks authentic where you're asked to input your personal information.

Similar scams may be sent through SMS messages to your phone, also known as Smishing Scams.

Some of the more common phishing and smishing scams:

- You're asked to validate your account by following a link.
- You're told there's a problem with your current account.
- You're threatened with action (i.e. closing your account) if you don't respond.

Prevention Tips

- Don't believe what you see. Business logos, websites and email addresses can easily be duplicated to look legitimate.
- Contact the business directly to legitimize the communication before you take any action. Search online to get contact information from an official source.
- Hover your mouse over links to check their true destination. If the URL doesn't match the link or seems suspicious, don't click on it.
- Beware of pop-ups.
- Be wary of unexpected emails that contain links or attachments from unknown senders.
- Update your computer's antivirus software.
- Ignore calls for immediate action or messages that create a sense of urgency.
- Watch for poor grammar and spelling.

Using Wi-Fi

- Make sure '**https**' appears before the website address in the address bar. The 's' stands for secure.
- Look for a lock symbol in the address bar.
- When using public Wi-Fi hotspots, avoid accessing sensitive information. Never input personal information including credit card data or complete financial transactions that are meant to be secure.
- Always keep your web browser, software and antivirus up-to-date.
- Set any mobile devices to manually select a Wi-Fi network instead of automatically connecting to unknown networks.

- To be the most secure, always log out of each website after each session, especially when using public Wi-Fi.
- Turn off your Wi-Fi when you aren't using it.

How to Secure Your Wi-Fi

- Your home Wi-Fi should be password protected. When you first set up your Wi-Fi, be sure to change the password to something other than what was provided by your service provider.
- If given a choice when setting up your Wi-Fi, choose WPA2 encryption as opposed to WEP or WPA

Shopping with Cryptocurrency (i.e. bitcoin)

- This type of currency isn't traceable and can be unregulated.
- Always make sure you are dealing with a legitimate company or person, as there may be no way to reverse the payment if there are issues with your transaction.

Online Banking Security

- Use strong passwords for financial accounts and keep them private.
- Create separate passwords for each of your online accounts so if one is compromised, the remainder are protected.
- Delete/clear your browser cache and history after you have finished your online banking.
- Ensure a firewall is active, antivirus software is installed on your computer and that all programs are up-to-date, especially web-browsers.
- Never use public Wi-Fi or public computers when banking online.
- Never allow the "auto-fill" or "auto-remember" feature for your passwords or personal information.
- Look for the lock symbol in the address bar or "https://" at the beginning of the website address (the "s" means "secure") to ensure the site is encrypted.
- Legitimate banks and businesses will never ask for your personal information in an email, be suspicious and contact your financial institution directly for such requests.
- When contacting a financial institution or business, use known verified contact information, not information provided by a suspicious email or link. Never reply to a suspicious email.
- Enter a website address into a browser yourself, never click on links.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (i.e. .com vs. .net).

- When disposing of a computer or device, ensure all personal data is permanently removed from the computer and hard drives. Use software or a hire a professional to wipe the hard drives clean, or physically disable/destroy the hard drive.
- Review your account regularly and report unusual activity to your financial institution.
- Make sure any online banking apps you download are authentic.

Creating Strong Passwords

- Change your passwords on a regular basis, at least once a year.
- Passwords should always been changed after a security breach with the company or if you know they've been compromised.
- Include a mix of uppercase, lowercase, numbers and symbols when creating your passwords. Using phrases is a good way to create a longer, more complex password that can be easily remembered.
- Avoid storing your passwords on your phone or computer.
- There are online sites available that will determine how long it would take a computer program to crack your password.

Tap Payment

- Contactless payments are extremely secure, however it is important to continue to check your bank statements and ensure there is no fraudulent activity.
- How does this work? And can thieves still get your information?
    - The payment portion is set up by Interac Flash. This form of payment allows the user to simply tap their card over the receiver (debit machine). The information that is transacted is the same information that is on the magnetic strip or chip portion of the card. No personal information is exchanged. This is strictly banking account information. The tap feature, however, encrypts the information each time, making nearly impossible to recreate for a secondary purchase with the same information. This feature however, is only good for purchases up to $100 at a time, with maximum of $500 in total purchases in a day. The risk to the consumer or primary user of the card is Zero as the banks take complete onus of missuses on the card if it is stolen or lost.
    - A payment feature that is becoming more and more popular is the use of Flash on your personal device or cell phone. This is the same as using the card, but is scanned by either a bar code or QR code displayed on the device screen. The same features apply to this as the tap feature on the physical card. However, people are starting to use the App's to avoid caring a physical card on them at all times. Also, if the person has their phones protected with a passcode lock, it provides an extra layer of security when it comes to the use of this payment option.

Online Scams

General Prevention Tips

- Do not feel pressure to respond to a request until you have a chance to verify the story.
- Never transfer money, or give out credit card or other financial information, until you can verify the person's identity and the story, and determine whether it is legitimate.
- Ask for call back numbers in order to confirm the legitimacy of any call you receive.
- Immediately report suspicious people to police.

Charity Frauds

Often in the wake of a catastrophe like a hurricane, flood or terrorist act, scammers will set up illegitimate "relief funds" to help survivors and solicit donations from victims.

- You can check with the Canada Revenue Agency to ensure your donations go to recognized registered charities.
- Do not feel pressure to provide money urgently. Take the time to do your research before you make a decision to donate money.
- Watch out for copycat charities that may be posing as a reputable charity or have a similar sounding name.

Grandparent Scams

Scammers contact victims claiming to be a grandchild in some sort of trouble. They ask the grandparent to send money and not to tell anyone.

- Never provide money to anyone unless you have confirmed their identity and that the story is legitimate.
- Have the contact information of all of your children and grandchildren on file. Call them directly, as well as other family members, to verify the story.
- Ask the caller questions that only your family member would know the answer to.
- Do not feel pressure to respond or give money until you've been able to verify the story.

Vacation Rental Scams

- Verify the existence of a property using the 'Street View' function of an online mapping site when available.
- Request the advertiser to provide ownership documents and ensure the name on the lease matches public property records.
- Request additional images of the property and ask to view the property via video-conferencing when possible.
- Avoid cash transfers as they are untraceable.

Online Classified Scams

- If available, use the “Report Ad” link for suspect advertisements.
- Beware of large discrepancies in price compared to similar items advertised.
- Check that the picture in the advertisement matches the geographical location of where the item is being sold.
- It’s best to deal locally and in cash. Avoid accepting payment via money transfer and never wire money to anyone.
- Never wire or transfer excess funds to anyone.
- Avoid purchasing e-tickets or box office tickets that can’t be verified, of any kind, from online classifieds.
- If it looks too good to be true, it probably is.

Mobile Devices

Securing Devices

- Ensure the wireless networks used are secure before accessing sensitive information.
- Do not store personal information or passwords on your device.
- Conduct regular back-ups of your device and install device tracking apps that will help you locate it if it goes missing and remotely wipe personal information from the device (such as Find My iPhone).
- Regularly check that your apps and device software is up to date.
- Ensure there is a password to access your device, and that it is ‘locked’ when you’re not using it.
- It is possible for malware to infect a mobile device. Make sure you are using safe internet practices.
- Be aware of which apps are using and storing your location data. Some devices also geotag any photos taken. Make sure you know if your device is doing this and turn it off if you are not comfortable with sharing your location information with your photos.

Device Advice for Kids/Teens

- Make sure you know what your kids are doing on their devices and understand what the apps they are using are.
- Be able to recognize all of the app icons on your kid’s device and know what they link to.
- Often it is your name on the account and plan, anything they do could affect you.
- Set up a contract (link to S4 contract) with your children that outline your expectations before giving them access to the device. Include things like:

    - Who will have access to the device and any passwords associated?
    - Which apps they are allowed to use.
    - How to interact with other people online and through social media and what to do if they experience inappropriate behaviour.
    - What information is personal and should not be shared with anyone.
    - General safe internet practices.
    - Usage restrictions.
    - Explain why restrictions have been put in place.
- Know the age restrictions that exist for many social networking sites.
- Teach your kids how to create strong passwords.

Reporting Cybercrime

- You should contact the police if you've lost money or property, or when legitimate threats have been made.
- If you believe you have been the victim of a crime, please contact the Calgary Police Service at 403-266-1234, or 9-1-1 in an emergency.

Additional Resources

https://www.serene-risc.ca/en/cybersecurity-tips/wi-fi

Smart Cybersecurity Network

http://computercrimeinfo.com/

FBI computer Crime Specialist

http://keepass.info/

Password Storage

https://lastpass.com/

Password Storage

http://www.pcmag.com/article2/0,2817,2407509,00.asp

Smartphone Apps

http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html
Little Clack Book of Scams

https://www.protectchildren.ca/app/en/
Canadian Centre for Child Protection

https://www.cybertip.ca/app/en/
Online Safety

http://www.prevnet.ca/
Bullying/Abuse Resource