PERSONAL DIGITAL SECURITY

LLO CONFERENCE – June 13, 2019
Rick Doelle – rixsite@hotmail.com

INTRODUCTION

As more people use the internet to shop online, there is a greater risk that users will lose personal and financial information to cyber-criminals.

This report deals with security considerations at different stages of the online shopping experience.

SECURITY FOR THE USER

PASSWORDS

Many web sites have you enter an account name or UserID and a password.

The account name identifies you as the user and it stays the same.

The password prevents others from accessing your account and you can change it whenever you want to.

You should use a strong password for your account. It should be difficult for someone to guess.

The strength of a password depends on its length, complexity and unpredictability.

Some web sites show the strength of your password when you create it.

FEATURES OF A STRONG PASSWORD

If allowed by the web site:

1. Use at least 12 -14 characters, preferably more;
2. Use a mixture of capital letters (A – Z) and small letters (a – z);
3. Include numbers (0 – 9) and symbols (@, #, $, etc.).

Avoid using passwords based on:

- Repetition (e.g., aaaaa, 55555);
- Dictionary words (English or foreign language);
- Letter or number sequences (e.g., qwerty, 12345);
- Usernames;
- Names of relatives or pets;
- Romantic links (current or past);
- Biographical information.

Video: "How to Create a Strong Password" (3:30) by Safety in Canada
https://youtu.be/aEmF3Iylvr4

PASSWORD MANAGER

Use a password management app to keep track of passwords and to generate strong passwords when necessary.

The password manager stores the passwords for the web sites you visit.

You only have to remember one strong master password or passphrase to open the app.

There are both free and paid subscription versions of password managers.

Highly rated free password managers for 2019 (PC Magazine):
www.pcmag.com/roundup/331555/the-best-free-password-managers

- LastPass (4.5*)
- LogMeOnce (4.5*)
- MyKi Password Manager (4.5*)
- 1U Password Manager (3.5*)

Highly rated paid password managers for 2019 (PC Magazine):
www.pcmag.com/roundup/300318/the-best-password-managers

- Keeper (4.5*)
- LastPass (4.0*)
- Dashlane (4.5*)
- Password Boss (4.0*)
- Sticky (4.0*)
- LogMeOnce (4.0*)

TWO-FACTOR AUTHENTICATION

This is one of the best ways to protect your account from being hacked.

Access to your account is based on something you know (a password) and something you have (a smart phone or e-mail).

When you log into your account from a new device or browser, a verification code is sent to your smart phone or e-mail.

If the correct verification code isn't entered, the login attempt will be blocked.

You can arrange to skip this step when signing in from a trusted device.

Does a web site support two-factor authentication? Find out at:
www.twofactorauth.org

Type the company name to see if it supports two-factor authentication.

USER ACCOUNT DATA BREACHES

A data breach is an incident where information has been exposed unintentionally to the public.

In December of 2016, Yahoo announced it had uncovered a massive data hack, compromising more than 1 billion user accounts. This was in addition to an earlier 2014 data breach, which had affected over 500 million users.

User Account Database

Has your user account been compromised in a data breach? Find out at:
https://haveibeenpwned.com/

Enter your user account and click on the **pwned?** button.

If your account information has been exposed, then change your password.

Password Database

Has a password been reported in a data breach? Find out at: https://haveibeenpwned.com/Passwords

This site has over 500 million real world passwords that were previously exposed in data breaches.

This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts.

PASSWORD SECURITY MEASURES

1. Generate and save a unique, strong password for each web site.
2. Don't give out your password.
3. If you write down a password, keep the paper in a secure location.
4. Use a password manager to manage your passwords.
5. Use two-factor authentication when it's available on a web site.
6. Subscribe to a service to notify you of any data breaches.
7. If your data has been breached or if you think someone knows your password, then change the password for that site.

PHISHING

Phishing occurs when someone sends you an electronic communication and:

a. pretends to be a trustworthy company; e.g., a bank, credit card company, and

b. attempts to get personal, sensitive information from you; e.g., username, password, bank account or credit card information.

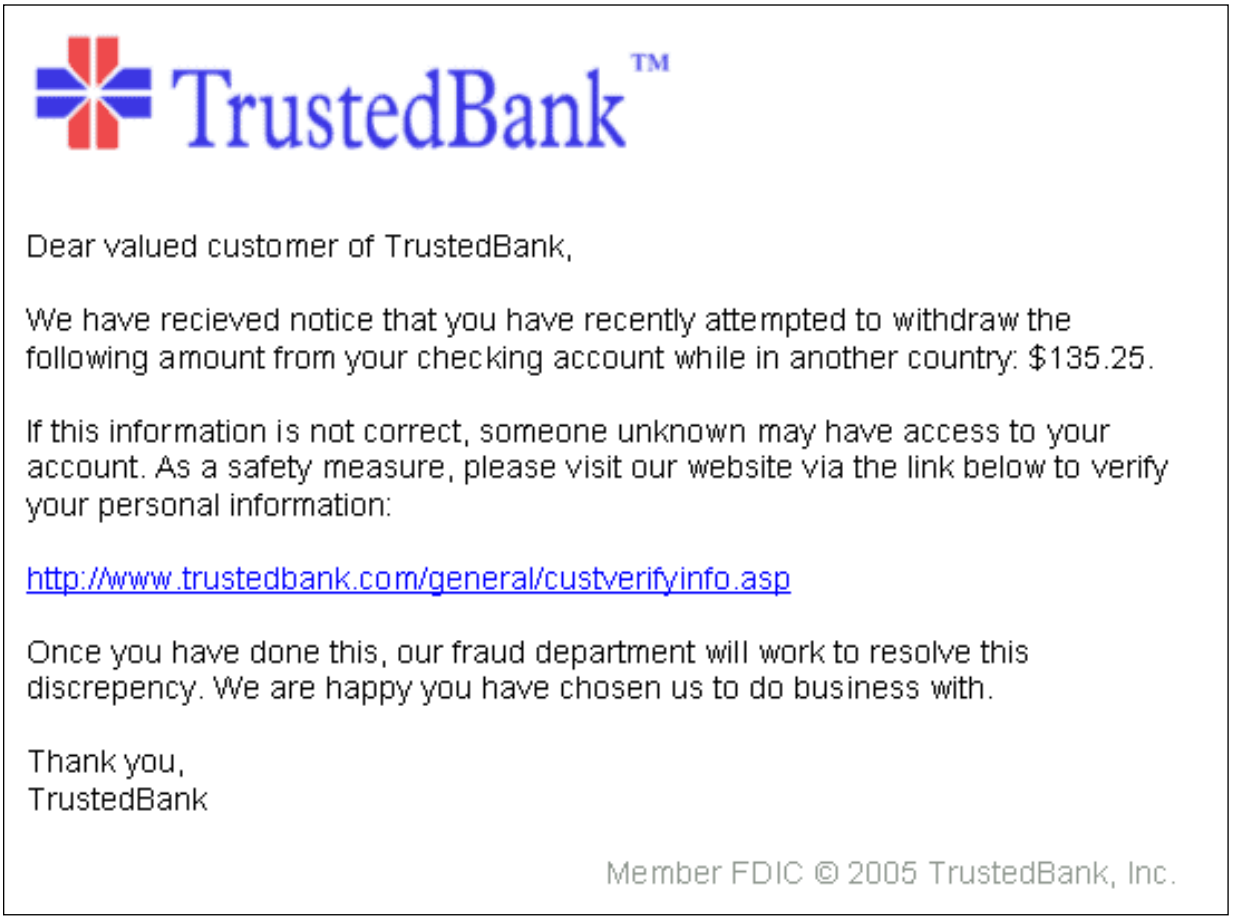
The notice looks official and usually it has some urgency associated with it.

Usually there is a generic greeting and there might be spelling and grammar errors in the text.

The sender attempts to trick you into revealing confidential information by having you click on a link inside the message.

The link goes to the phisher's website, not to the true website of the organization.

Here's an example of a phishing e-mail, disguised as an official e-mail from a (fictional) bank:



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Be suspicious if your name is not included in the message or if only your user account name is given.

Hover the mouse pointer over the link to inspect it. It should lead to a secure, logical address starting with https://

It's best to ignore the message and delete it.

If you want to respond or confirm the message, then contact the organization directly; don't use the link in the message.

Phishing is widespread and many people respond to it.

An approximation of global phishing totals in 2012 from getcybersafe.ca
www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/_mgs/nfgrphcs-2012-10-11-eng.jpg

156,000,000	phishing e-mails are sent out each day.
16,000,000	make it through spam filters.
8,000,000	are opened.
800,000	links are clicked.
80,000	fall for a scam and share personal information (~0.05%).

Can you spot if you're being phished? Take the phishing quiz at Google:
phishingquiz.withgoogle.com

SECURITY FOR YOUR DEVICE

SCREEN LOCK

If you leave your device unattended, then lock the screen.

Use a password to unlock the screen. This prevents unauthorized access to your device.

DEVICE OPERATING SYSTEM

Keep the operating system of the device up-to-date.

Allow the device to automatically update the operating system and install security patches.

ANTI-VIRUS SOFTWARE

Install anti-virus software on your device.

Without it, you risk losing your personal information and your files.

The software ensures that you're protected against viruses, spyware, ransomware and other malware.

Many of the antivirus apps can be used on multiple platforms: PC, Mac, Android, iOS.

Highly rated free PC anti-virus protection for 2019 (PC Magazine):
www.pcmag.com/roundup/267984/the-best-free-antivirus-protection
Avast Free Antivirus (4.5*) AVG Antivirus Free (4.0*)
Kaspersky Free (4.5*) Bitdefender Antivirus Free Edition (4.0*)

Highly rated paid PC anti-virus protection for 2019 (PC Magazine):
www.pcmag.com/roundup/256703/the-best-antivirus-protection
Webroot SecureAnywhere AntiVirus (4.5*) Kaspersky Anti-Virus (4.5*)
Bitdefender AntiVirus Plus (4.5*) McAfee Antivirus Plus (4.0*)

Highly rated Android anti-virus apps for 2019 (PC Magazine):
www.pcmag.com/article/358984/the-best-android-antivirus-apps
Symantec Norton 360 Deluxe (4.5*) Kaspersky Security Cloud (4.5*)
Bitdefender Total Security (4.5*) McAfee Antivirus Plus (4.0*)

Highly rated Mac anti-virus apps for 2019 (PC Magazine):
www.pcmag.com/roundup/355173/the-best-mac-antivirus-protection
Bitdefender Antivirus for Mac (4.5*)
Symantec Norton 360 Deluxe (for Mac) (4.5*)
Kaspersky Internet Security for Mac (4.5*)
Webroot SecureAnywhere Antivirus (for Mac) (4.0*)

SECURITY FOR THE INTERNET CONNECTION

HOME NETWORK ROUTER

Set up secure WPA2 encryption on the home router with a strong password.

Only devices with the correct password can connect to the home network.

This prevents unsecured wireless connections to your network.

PUBLIC WI-FI NETWORKS

There are many security dangers when using public Wi-Fi networks.

Data sent through public Wi-Fi can be intercepted by cybercriminals.

A common danger is fake public Wi-Fi networks. These have similar names to legitimate networks and they are meant to trick you.

Once you connect to the fake network, everything you do online can be monitored.

Your activity can be scanned to look for banking and social media login information.

Malware and viruses can be planted onto your computer over an unsecure Wi-Fi connection.

Video: "Easy Ways to Stay Safe on Public Wi-Fi" (2:31) by Safety in Canada
https://youtu.be/X87MJEsJ91A

TIPS TO STAY SAFE ON PUBLIC WI-FI

1. Enable your firewall and keep your anti-virus app up-to-date.
2. Verify the proper Wi-Fi address, to avoid connecting to a bogus network.
3. Check for a secure connection, with either "https" or a closed padlock icon in the browser screen.
4. Watch for shoulder surfers, especially when entering passwords.
5. Turn off file sharing.
6. Avoid checking sensitive data, unless it's absolutely necessary.
7. Avoid credit card or personal transactions when on Wi-Fi.
8. Use a Virtual Private network (VPN).
9. When done, log-off all your open services and turn off your Wi-Fi.

VIRTUAL PRIVATE NETWORK (VPN)

Video: "My Private Network - Introduction" (1:45) by My Private Network
https://youtu.be/t8Es_ymjjHM

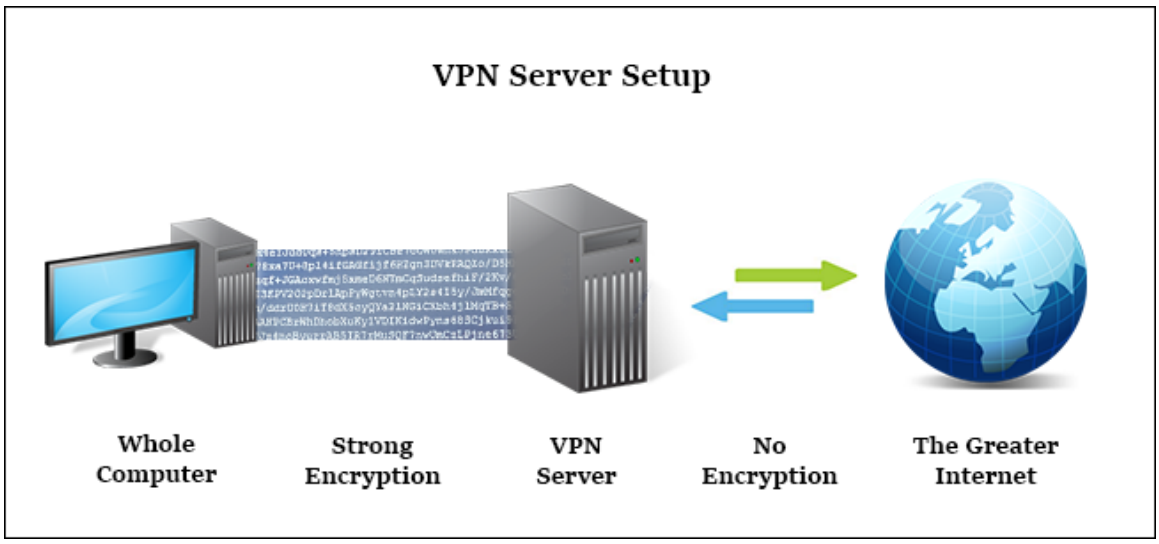
If you do nothing else, using a VPN is the best way to ensure your online privacy.

They make networks more secure, especially free public Wi-Fi networks.

The VPN creates a secure tunnel through which your data travels to the VPN servers, where it's sent to the internet. It also results in location spoofing.

The VPN works in the following way:

1. You start the VPN service on your device.
2. The software encrypts your data using a secret code, before the Internet Service Provider sees it.
3. The encrypted data goes to the VPN server where it's decoded.
4. The unencrypted data is sent on to the internet.
5. Data from the internet is sent back to your device in the reverse order.



The online destination sees your data as coming from the VPN server and its location, not your computer and your location.

No one can easily identify you or your computer as the data source, nor what activities you're doing on the internet.

The data is encrypted so that if anyone intercepts your data, they only see encrypted information, not raw data.

Without a VPN, your location is known and your data can be read by anyone intercepting it.

Highly rated free VPNs for 2019 (PC Magazine):
www.pcmag.com/roundup/285788/the-best-free-vpn-services

TunnelBear VPN (4.0*)	Hide.me VPN (3.5*)
ProtonVPN (4.0*)	AnchorFree Hotspot Shield VPN (3.0*)
Avira Phantom VPN (3.5*)	Kaspersky Secure Connection VPN (3.0*)

Every VPN listed here restricts its free version.

Some services limit the amount of bandwidth you can use in a given period.

Some keep the number of devices you can connect simultaneously low, generally to one or two.

Highly rated paid VPNs for 2019 (PC Magazine):
www.pcmag.com/roundup/296955/the-best-vpn-services

NordVPN (5.0*)	CyberGhost VPN (4.0*)
Private Internet Access VPN (4.5*)	ExpressVPN (4.0*)
Proton VPN (4.0*)	IPVanish VPN (4.0*)
TunnelBear VPN (4.0*)	TorGuard VPN (4.0*)

SECURITY FOR THE WEB BROWSER

When using a public or shared computer, use the private browsing mode of the web browser.

This is known by different names for different browsers; e.g., Private Browsing, Incognito, InPrivate Browsing, Private Tab.

Using private browsing disables the browsing history and the web cache (temporary storage of web documents).

Traces of activities could still be left behind, so that the user's browsing activities are not fully hidden.

On a public or shared computer, if private browsing is not used, clear the browsing history, the web cache and cookies before closing the web browser.

See this web page for more details: "Clearing Browser Cache and Cookies"
https://kb.wisc.edu/page.php?id=12384

SECURITY FOR THE DESTINATION WEB SITE

Video: "How to Know if a Web Site is Secure" (3:15) by Safety in Canada
https://youtu.be/F-J6sRhtRuU

For any financial transactions, ensure that you use a secure web site. Look for "https" in the web address and/or a locked padlock icon.

For non-financial transactions, try to use secure web sites.

Avoid saving your payment card information on multiple web sites.

If possible, use a third-party payment service; e.g. PayPal, Apple Pay, Google Pay.

Pay with a credit card instead of a debit card or direct bank transaction. The credit card provides more protection against fraud.

For extra safety, use a dedicated computer for financial transactions. Don't use that device for surfing or social media.

When finished with a web site, log out of your account at that site.

MONITORING YOUR FINANCIAL ACCOUNTS

Regularly monitor your financial online accounts (bank, credit card) for unauthorized transactions.

Report suspicious activity to the financial institution.

If you have financial losses because of fraudulent activity, report this to the police.

If you think you or someone you know has been a victim of fraud, contact the Canadian Anti-Fraud Centre at 1-888-495-8501.

TIPS ON STAYING CYBER SAFE WHILE SHOPPING

Elizabeth Weise, The Hamilton Spectator, Nov. 24, 2016.
www.thespec.com/living-story/6984825-tips-on-staying-cyber-safe-while-shopping

In the rush for holiday online shopping, it's too easy to take shortcuts that raise your risk for a cyber attack.

1. Don't Use Sketchy Wireless Networks

Watch out for free Wi-Fi hot spots that could be false.

Public Wi-Fi is not secure and it might be monitored.

2. Who Really Sent You That Online Greeting Card?

Electronic greeting cards are popular, but do you know who sent the card?

Be careful about clicking on any links inside the card.

3. Use A Different Password for Each Account

Criminals have records of data from hacked accounts.

They can use this information to try to access stores and banks online.

4. Watch for Typo Squatters

Check the spelling of web site addresses that you type.

Hackers have registered typo web site names to fool you into releasing personal information.

5. Change Your Coffee Pot's Password

Connectable devices have easily hacked passwords.

Change the password to reduce the chance of the device becoming part of a zombie botnet.

6. Don't Hand Over Your Credit Card Number

Don't save credit card information online.

If the web site is hacked your data could be stolen.

7. Read Through Your Credit Card Statement

Look for unusual or unfamiliar purchases.

Call the credit card company to check out those charges.

8. Be Careful of Package Delivery Notices

Online delivery notices could be phishing emails.

Don't click on any links within the notice.

Go to the web site directly to check the information.

THE INTERNET OF THINGS

This is a group of smart devices that connect to each other and to the internet; e.g., thermostat, alarm system, TV.

Many of these devices connect to the internet through your home network.

Ensure that your network has a strong password and set up a separate, secure "guest" network for your smart devices.

Turn off geolocation when not in use.

Disable microphones and cameras on smart devices when not in use.

Create usernames that don't contain identifying information.

ONLINE AND TELEPHONE FRAUD

Warning Signs – How to Protect Yourself

1. Never give anyone remote access to your computer. If you are having problems with your operating system, bring it to a local technician.
2. Beware of scammers advising you of an unauthorized charge on your credit card account and requesting your credit card number.
3. Verify any calls with your credit card company by calling the phone number on the back of your credit card.
4. Never provide personal information or banking details over the telephone unless you initiated the call.
5. Beware of solicitations for products or services offering lower energy bills.
6. Do your homework before hiring a company.
7. Don't be afraid to ask questions, and if you feel pressured, never hesitate to hang up.

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501.

LITTLE BLACK BOOK OF SCAMS

https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

Descriptions of 12 different types of scams attempted online, on the phone or in person.

GOVERNMENT WEB SITES

Get Cyber Safe
www.getcybersafe.ca

Canadian Anti-Fraud Centre
http://www.antifraudcentre-centreantifraude.ca/index-eng.htm