DIGITAL SAFETY

FOR THE NON TECH SAVVY

WINDSOR POLICE

wfcu CREDIT UNION

CRIME STOPPERS WINDSOR & ESSEX COUNTY

A Community Initiative for Online Safety

CANTERBURY ElderCollege SERVING SOUTHWESTERN ONTARIO

THE CITY OF WINDSOR ONTARIO, CANADA

DIGITAL SAFETY FOR NON-TECH SAVY

by
KEVIN COSGROVE
Certified I.T. Technician,
Civilian Security Advisor,
Technology Instructor

Dedication to the Memory of
1st Class Constable John Atkinson
1968 – 2006
Windsor Police Services
6744
Heroes in life, not death

Published by Canterbury ElderCollege
2500 University Avenue West, Windsor, Ontario, Canada
N9B 3Y1

Canterbury ElderCollege,
Canterbury College,
2500 University Avenue West,
Windsor, Ontario, Canada, N9B 3Y1

ISBN 978-1-7778179-0-9

WFCU Credit Union is proud to support the printing of this handbook. The information contained in this handbook is provided by Canterbury College and is for informational purposes only.

Printed by Lacasse Printing

Cover Design:
Visual interpretation of digital data containing frauds and scams

Canterbury ElderCollege and Why We Believe This Publication is Important for our "Aged 55 and Better" Community

When ElderCollege was formally launched with is first semester of courses offering a unique continuing educational opportunity for persons age 55 and better, it was clear very early on that many prospective ElderCollege participants were relatively new to their computers. Indeed, many did not have emails or, in many cases, were so concerned about fraud through computers and emails that they did not wish to share an email address with ElderCollege.

Initially, this posed a problem as the least expensive way for a "grassroots" organisation such as ElderCollege to communicate with its participants was via email. "Snail mail" was simply too expensive for a small volunteer based limited funds organisation. That was in the autumn of 2011.

Ten years later, not only do many more ElderCollege participants communicate via emails, but many have also taken advantage or ElderCollege's course offerings online. We are both proud and excited as ElderCollege has reached out to our ever expanding community not only in southwestern Ontario but across Canada and in the United States.

Yet through it all, we continuously learn of more and more diverse attempts to deceive and effectively steal from those of us who are older and perhaps more vulnerable to the attempts by so many wretched people to scam us.

Kevin Cosgrove initially produced the basic contents of this booklet as hand-out for the many courses he has volunteered to offer ElderCollege. When we realised what a gem, he had prepared for his classes we suggested that if we could find sufficient funding and he was prepared to expand his initial

class handouts into a coherent booklet, we would publish it and distribute and make it available to as many seniors as possible.

On behalf of ElderCollege, I thank Kevin Cosgrove for his contribution to an improvement in the overall safety that many of us seek in our daily encounters with the digital age.

In addition, I thank all those businesses, organisations and individuals who saw in this publication a worthy contribution to public safety and thereby provided the funds we needed to bring this valuable booklet to fruition.

LBJ

---Lloyd Brown-John, Founder and Director,
Canterbury ElderCollege

Our Sponsors

With heartfelt appreciation we thank our wonderful sponsors whose generous support made the publication and distribution of this book possible

Our Donors

We sincerely thank these individuals for their kindness and personal support of this project

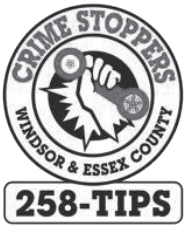
Pamela Hines
and
Royal Lepage Binder – Ondeko Commercial Advantage

Special Thanks

for their continued support, content review or program endorsement

In Canada, victims of cybercrime and fraud have benefited from seeking assistance and support from the **Canadian Anti-Fraud Centre** since the early 2000s. While anyone can be the target of these crimes, it is often the most vulnerable that falls victim. Whether it is individuals, organizations, or agencies, the CAFC is dedicated to providing a victim-centered approach, giving victims empathetic and compassionate support as they seek to recover from the financial and psychological devastation these crimes can cause. The CAFC is a national centre of excellence and has been modeled internationally.

Anyone who has been the target of cybercrime or fraud is encouraged to report to the CAFC either through their website **www.antifraudcentre.ca** or toll-free line **888-495-8501**



Crime, unfortunately, affects us all. Crimes affect our feeling of safety and security within our homes, parks, workplaces, or schools. Crime Stoppers is an anonymous reporting system that offers rewards for information to help the police solve crimes. Since its inception in Windsor-Essex County, the Crime Stoppers Board of Directors has authorized over $1,000,000 in reward payouts that have led to solving crimes.

YOU REMAIN ANONYMOUS – Crime Stoppers does not want to know your name or where you live. We just want the information you have, and then we will go to great lengths to protect your anonymity. **THERE IS NO COURT** - The Supreme Court of Canada has ruled that anonymous tipsters are protected. **YOU COULD EARN A CASH REWARD** - Tips that lead to an arrest for seizures of stolen property, illegal drugs or weapons, or information that is deemed valuable in an investigation could get you rewarded.

Crimes **you** may help solve include, but are not limited to, break & enter, homicide, assault, robbery, sexual Assault, domestic violence, arson, fraud, drugs, or impaired driving. You may report **online crimes** as well, involving human trafficking, the sale of stolen goods, posting illegal/explicit/abusive material, or exploitation.

www.catchcrooks.com
519-258-TIPS (8477)

Youth Diversion provides timely and effective prevention and intervention services to children and youth ages 6 –18. Services hold youth accountable for their actions and offer opportunities for them to address underlying issues contributing to their at-risk behavior. Youth Diversion's programs focus on assisting youth in developing self-respect, responsibility, and appropriate problem-solving skills while empowering children and youth to create, maintain, and positively improve upon their decision-making both off- and online. Parents are also supported in navigating digital safety through **#parentingunplugged** webinars and podcasts, Youth Diversion's **Digital Drivers e-Presentation series**, and other free resources available to view and download from the Youth Diversion website: **www.ecyouthdiversion.ca**

1821 Provincial Road Windsor, ON, N8W 5V7
(519) 253-3340
Email: info@essexcountydiversion.com

Windsor Police Community Service Branch is responsible to proactively interact with the community in crime prevention techniques, children's traffic safety issues and substance abuse. The goal of the Windsor Police Community Service branch is to raise community awareness of policing issues to gain greater community support and involvement.

3312 Sandwich St., Windsor, ON N9C 1B1
Tel: 519-255-6173

Table of Contents

Preface 12
Introduction 14
Securing Your Devices 15
Digital Declutter 19
Backup Your Files 21
Password Management 23
What is 2FA? 25
Credential Stuffing 27
WiFi Security 29
Understanding Internet Addresses 32
Email Security 34
Junk Programs 38
Free! Free! Free? 38
Fraud Phone Calls & “Scareware” 42
Online Shopping 48
Online Banking 49
Social Media 51
Reduce your Digital Footprints 53
Romance Scams 56
Leaving a Computer On 60
Disposal of Devices 61
Legacy Access 62
Conclusion 62

Preface

The international nature of many frauds and financial scams can make prosecution difficult. Digital crime is often highly anonymous; when a crime is committed, the “trail” is usually only a temporary web address or phone number. The criminals can shut down and quickly re-appear at another address or even another country. As you can imagine, international laws don’t allow extradition for individual minor crimes. With that said, reporting electronic crimes is still essential. It enables local law enforcement to dictate where more resources may be required and maintain documentation when large-scale electronic crimes are committed. The scam emails or phone calls that you receive may already be part of a more extensive investigation. Joint law enforcement with other countries does occur, but it requires mass reporting to bring these problems to light.

Throughout the following pages, we hope to assist you and your family in using safe practices and to keep you from becoming victims of computer-related crimes. Please keep in mind that this booklet provides practical but brief information on a variety of topics.

If you have been a victim of online fraud or your identification has been compromised, you should:

• Contact any affected financial institutions/credit card companies.

• Contact law enforcement (on a non-emergency phone number) and the CAFC either through their website **www.antifraudcentre.ca** or toll-free line 888-495-8501

• Contact credit record companies to report the fraud and possibly set up credit monitoring e.g., Equifax and TransUnion (fees might apply).

• Keep an eye on accounts for unusual activity or unrecognized charges, or “tests” of $0.01 to check if an account is working. Unfortunately, there isn’t a time limit of when you can finally let your guard down; some scammers will even keep information for several months to years before acting upon it to avoid detection. Existing or new hackers can gather information from online lists and databases from years ago that still contain relevant information like passwords that are still in use, or unchangeable information such as S.I.N., name, birthdates.

• Have your computer or electronic devices checked by a professional to remove any threats.

• Change any online passwords that may be affected. Focus first on primary accounts that other accounts refer back to for password reset or identity verification.

It is common for users to feel ashamed for falling for a scam or getting hacked. Keep in mind that, in many cases, you are up against criminals that may spend a significant amount of time and effort on the crimes they commit. Even some of the world’s biggest companies, with professional computer departments, can also affected by scams and hackers.

Introduction

The ***Security/Convenience Balance*** theme is at the core of how professionals use and maintain their devices to avoid getting viruses, hacked, or scammed.

Let's make some comparisons to your non-digital life. If you choose the convenience of not locking doors at night, you may be increasing the risk of a break-in. If you choose the convenience of paying for gas by waving your keychain at the pump, you are running a risk should that keychain be lost or stolen. In your digital life, if you don't want to use security features to log in, then you are risking someone accessing your devices and accounts...quite easily. Suppose you choose to have your internet browser remember passwords for convenience. In that case, your accounts are in jeopardy if your computer is infected/hacked, or info will be lost if your device is stolen/crashes.

Law enforcement often refers to easy access crimes as "crimes of convenience," and many computer crimes are similar. Frequently real-world security problems can be traced back to adding some form of convenience without considering the adverse effect on security. While it is true that nothing can stop a determined or skilled thief who wants to bypass the security of something like a locked door, a standard lock stops most thieves and prevents "*crimes of convenience."* Similarly, in the digital world, standard, basic security measures will take care of *most security* problems.

So, without going to extremes or causing computer paranoia, unplugging your entire home, and wearing tinfoil hats, there

are simple steps that anyone can take to improve online security. Fortunately, you don't have to be a computer genius or read long, boring information to keep safe. This booklet keeps it simple and narrows down to only the information that you need. Some steps may require further exploration, requesting help, and implementing new procedures. In the long run, taking these steps is much easier than repairing a damaged credit rating, recovering from financial theft, dealing with an account hijack, or even contending with issues when problems cross over into a threat in the physical world.

Securing Your Devices

When home computers became a norm for many households back in the '80s and '90s, computer viruses were widespread. Early viruses mainly focused on causing damage to a computer, its files, or the networks to which they were attached. Initial viruses were akin to vandalism and malicious acts. Viruses are still relevant today but are now more focused on financial gain and gathering information. Although many people use the term "virus" to describe anything in a device that is dangerous or causes unwanted behavior such a spyware or malicious programs, technically that is not the correct use of the terminology. Currently, even though home users encounter less actual viruses (by definition) and are more likely to be caught up in user participated scams, viruses still can cause problems.

Here are some quick fixes to protect your device:

1) Always use the most current version of an operating system (O.S.) Windows, OSx, iOS, Android, Linux.
Some people dislike change, and sometimes updating may mean a difference in how your device or software "looks." Staying with an older operating system or software simply due to appearance is never worth being exposed to security flaws when using a device online. (Security/Convenience Balance). Some O.S. upgrades may disable specific obsolete software or hardware such as printers or scanners when they are no longer supported. If this is the case, and it is still a necessity to continue running an older O.S. then it is recommended to take the device offline before continuing use and instead use a secondary updated device for internet use.

2) Check for software updates regularly or allow for automatic updates.
It is normal human behavior only to remember incidences of when issues occur and forget the other times, because of this some people develop the opinion that updates cause problems. Updates can occasionally cause unexpected problems, but the overall risks are minimal compared to leaving the computer without updates or "unpatched". Support programs, such as web browsers, PDF readers, Java, Adobe Flash Player, etc., must also be checked regularly for updates or uninstalled since they can be a major source of security flaws and device exploitation. Make sure to only obtain software updates from the originating company. Search online, get help, or hire a computer service if you cannot find the source of updates.

3) Keep antivirus/anti-malware protection on your computer.
These two types of programs scan for different problems. They can work independently, or they may be part of a single program or security suite. Standalone antivirus programs may

only handle viruses and ignore other threats such as possible malware, potentially unwanted programs (P.U.P.s), or unwanted browser behavior. Whether using two standalone programs or a combined program/suite, make sure that you can scan for viruses as well as malware threats.

TIP: Only install one antivirus software at a time, as multiple programs can severely slow down your device or prevent it from working correctly.

The bottom line regarding whether or not you need to have an antivirus/malware scanning program is - it depends. In deciding which program(s) to use, you only need to make sure that it has the features that you require, and it protects from problems that you may encounter, regardless of price, aggressive sales, or marketing. For example, compare computer security to having a security alarm on your home, you may have an excellent system, but if you invite a burglar in and they subsequently rob you. The solution is not that you now need a more expensive security alarm. Having improperly chosen security software may not protect your devices from threats that you actually encounter. In day-to-day experiences, many computer services can tell you that their customers are often confused why their computer gets “infected” or is not running correctly, despite the money that the user pays every year for a particular security program.

Security and antivirus software companies commonly offer a free or “trial” version of their software, as well as a paid subscription version. This is a good way for users to decide if the product meets their needs. Many computer manufacturers pre-install trial versions of security software that may pester you to purchase upgrades or subscribe annually to their full service so that your “security doesn’t expire”. Despite their sales pitches, it may not be necessary to buy these ongoing subscriptions and is more a matter of decisions based on your specific needs. Some paid versions of security programs may

offer helpful advanced features, but you may also find free, reputable alternatives that fit your needs just as well. For example, the last few versions of Microsoft Windows include a built-in virus scanner, ransom-ware protection and a firewall, which works automatically, is free, and doesn't expire.

If you are buying additional security products, it is best to choose a solution that matches your unique usage and behavior, such as needing virus scanners for downloads or email, checking for safe websites, or providing safe cloud storage and backups. Look up current reviews and examine the different features that a program or suite offers and ensure it fit your needs.

Keep in mind that the overall security of your device or computer shouldn't rely solely on antivirus/malware scanners and firewalls etc. Allowing someone to remote access your computer, intentionally/accidently accessing dangerous websites, improper password habits, or divulging important information online can undo anything that security software can protect you from. For example, even the most prominent companies can be made vulnerable by an employee choosing abc123 as their password.

The user's behaviour is the ultimate key to computer security.

You can be as effective as a security program or team of I.T. professionals simply by making the right choices and practicing secure behaviours.

Digital Declutter

#1 Rule of computer security: it can't be hacked if it's not there in the first place.

1) Remove programs that are no longer used or supported.
If unsure about whether it is safe to remove a program, you can ask someone knowledgeable, lookup up the program name on the internet or have a computer service do a cleanup for you.

2) Clean up old files and documents.
"Digital hoarding" is a significant and often overlooked problem for many people. If your computer is hacked, then old files, receipts, resumes, emails etc., serve as a treasure trove of information that criminals can exploit. While cleaning up, safely store backups of files that may be needed in the future. Physically destroy unneeded backups (like C.D.s or hard drives) if they are no longer useful, or keep them in a safe place, just as you would with old tax receipts, banking documents, etc. If you are unsure of how to safely dispose of hardware or data, contact a computer support service for secure deletion before getting rid of or donating a device.

3) Clear out cookies and browsing history regularly.
Cookies can be helpful, such as when they are used to save items in an online shopping "cart" until you complete your purchase. They can also be used to store logins, save the history of where you have been, or store information for companies to decide which ads to show you depending on

your online behavior. Since cookies may store login info for your convenience on a return visit to the site, this is information that can be hacked from your browser so the value of storing them must be weighed. (Security/Convenience Balance) Many cookies are from 3rd party marketing companies that are hired to gather info on your browsing habits, where you go, what you search for, and what you click. Getting your behavioral info is the new “gold rush” as information gathering explodes in our digital world. Cookies are the reason why, after a web search or online purchases, suddenly all web pages you visit seem to have similar ads. Learn to locate browser settings to control how long a cookie is kept, whether to accept cookies, or whether to block third party/advertising cookies. “Favorites” and “Bookmarks” of frequently visited websites can also be an “info give-away” if a scammer gains access to this information; For example, you could become the target of a phishing email if a scammer notices which bank you have bookmarked.

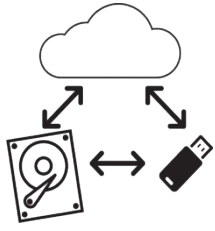
Additional Note: Some websites stop a user from visiting if cookies or advertising are blocked and may request that you unblock the site to continue. It is up to you to decide if you wish to unblock a site in trade for this access.
(Security/Convenience Balance)

4) Clear out old emails and cloud services.
For the same reasons as clearing old files, de-cluttering online storage also makes inboxes and cloud services easier to manage and backup. Most email and cloud storage services have a capacity limit, so keeping old useless emails and files may unnecessarily fill your account.

5) Shut down old/unused accounts and services.
You should always make sure that you shut down unused accounts properly using the account controls. If you have forgotten a login to an old/unused account, you should not just

abandon it; instead, go through recovery steps, contact the website/company if necessary, and then shut down the account properly. Any info left behind in old accounts may be used by scammers in the event of a hack or info leak (see section on credential stuffing). An online service like *Just Delete Me* which can be found at **www.justdeleteme.xyz** can provide helpful information on deleting accounts.

Backup Your Files



Backups are of course essential in the event of computer failure, but they are also an important security feature in case of problems such as virus infection, especially from a crypto or ransom virus. Crypto/Ransom viruses are a type of virus that encrypt and lock your files until you pay a ransom to get a password to decrypt them. These types of viruses have become a significant computer threat because at times people or businesses have no other choice than to pay the ransom when proper, timely backups are not in place to restore damaged files. Remember, even when a ransom is paid, there is no guarantee that you will get your files back. These are criminals that you are dealing with, so there is no “complaint department” to call.

Ransom viruses commonly arrive from an email written directly to a business that has been targeted due to their finances or the importance of their computer files, such as a hospital or financial company (this type of targeted phishing is called “spear-phishing”). In 2021, the Colonial Pipeline company in the U.S. was the target of ransomware, and as the largest petroleum pipeline in the country this attack

affected the east coast fuel supply until it was resolved days later. Ransomware is not only targeted at businesses, it can infect home users as well via a random email (phishing) or a virus-infected download of illegal programs and media. If your files are backed up properly, then even a catastrophic computer failure or crypto-virus will be a troublesome but temporary problem.

The industry standard for the *best* backup procedure is the "3-2-1 rule": at least **3** copies of data (including the original) existing on **2** different types of media (CD, DVD, USB stick, external drive, cloud storage), **1** of which is stored away from the device location. Even following these standards, a backup doesn't have to be complex. It can be as simple as a copy and paste of essential pictures or files to a memory stick or external drive. Be sure to remove any external drives when not used to avoid damage from electrical surges or virus infections. There are many programs available to perform scheduled backups of files or even back up the entire computer. Most of these backup programs are designed with ease of use in mind. In the past few years, online backups (cloud storage) have become more popular and affordable and allow easy, secure access to your backed-up files

When deciding on a backup plan, consider what would happen if you lost all of your data right now; which lost files would cause the most problems? Then, take some steps to back these files up. Keep backups up to date and store them in a secure place (possibly off-site or in a fire-safe box). Then, when a problem happens, you won't regret the minimal effort it took to secure the information.

Password Management

It's likely for the average person to have dozens of accounts and logins – for banking, emails, social media, even a password to get into a device itself. It can often feel overwhelming to retain all of this information. For some it seems inconvenient to type a few characters to access something that *needs* to be secure. (Security/Convenience Balance). Ask most technology users if they have a hard time memorizing passwords and you will likely get a resounding yes, but when you ask who told them to do this; you will probably be met with blank stares. The reality is that it feels complicated and overwhelming because you are trying to do something that is not reasonable to do. It is a **false belief** that memorizing account information is how to manage passwords properly. Because of this belief, many people develop negative and very dangerous habits like using only one password for everything or using easy to guess passwords and variations. To avoid problems and unreliable habits professionals use some type of management to keep track of them.

Here are some tips to help keep you on track:

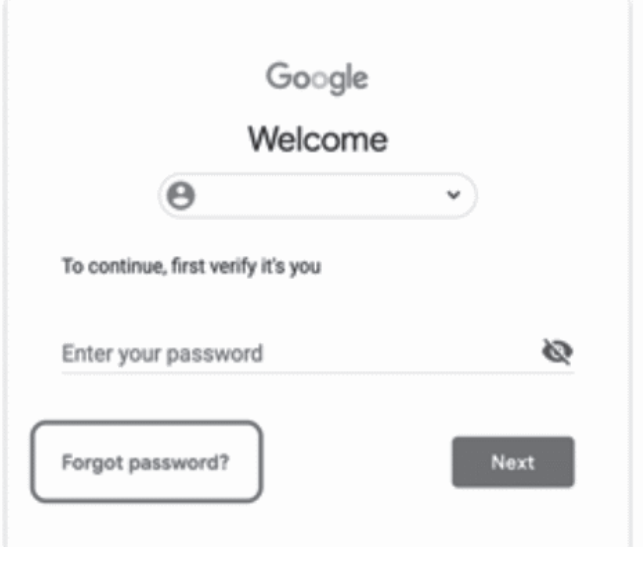
1) Keep a written/digital updated password document. If it is digital, you should preferably keep it outside of the device, and password protected. If it is printed, then you should store it in a safe, secure place.

2) Always use unique complex passwords for each website or service. Each additional character in a password multiplies the difficulty of hacking it. Using passwords such as ABC123, pet names, family names, favorite sports team etc., is a common choice and is thus easily exploitable, <u>especially</u> when the password is re-used for multiple accounts.

3) Set a calendar date to review accounts, update contact recovery information, and change passwords.
   You can decide how frequently to do this; quarterly, semi-annually, or yearly. Record and date your changes.
4) Despite advances in browser security, we have not reached a point where it can be recommended to authorize web browsers to remember login information for you. Passwords stored in a browser can be retrieved, copied, or hacked. (Security/Convenience Balance). It is also a common experience for people to lose passwords stored in their browser or auto login due to a device failure or theft and then not have any other record of the information.

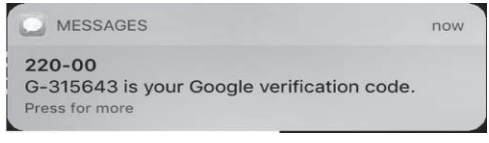
Keep in Mind: You are not expected to memorize account names or passwords.

If you are still experiencing difficulty when managing your passwords/accounts, you can use a password management program. There are well-respected companies that offer security solutions for keeping records of logins and accounts. Research current reviews of password management software or ask a trusted computer service for advice.



A lost password can usually be recovered or reset. For example, your email service may send recovery instructions to a secondary email account, text a cell phone, or even call your home phone with a recovery code to allow you to regain access to your account. Account Recovery options only work if your contact information and phone numbers etc. are **up to date**. Make sure you review your recovery/backup options on your accounts, especially after moving to a new home or a phone number change.

What is 2FA?



Second or Two Factor Authentication (2FA) adds another layer of account security in addition to requiring a password. This second factor could come from one of the following categories:

1) Something you know
This could be a personal identification number (P.I.N.), a one-time code sent to a phone or email, answers to "secret questions," or a specific keystroke pattern.

2) Something you have
Typically, a user would have something in their possession, like a credit card CVD, a smartphone, or a hardware token/security USB key

3) Something you are
This could be a biometric pattern of a fingerprint, facial recognition, voice print, or even an iris scan. Some devices and cell phones include fingerprint scanners, voice or face recognition.

With 2FA in place, a potential compromise of just one security feature (like a password) will still require more information to access the account. So, even if your password is compromised, the chances of someone else having your second-factor information become less likely. Many Canadians will be relieved to know that Canada Revenue Service now offers 2FA for their online login. Be sure to secure your Canada Revenue account with the new security features, as well as your other accounts.

In the **Something you have** category, a brand of secure USB key called YubiKey is a device that is commonly used among law enforcement and government personnel that when plugged into a device that you are using, will authenticate that it is *you* that is logging in at that device. Another type of 2FA may be an “authenticator app” on your smartphone linked to your account that provides temporary codes that expire if not used quickly. Check to see if your email provider, social media account, or online banking has 2FA available. Services like Gmail, Hotmail, and Facebook all provide some type of 2FA.

Additional Note: With or without 2FA enabled, some services offer to send a login notification when an unusual or *new* login occurs, such as receiving an email or SMS text message from your bank. Take advantage of using these notifications wherever they are available, as they can alert you to unauthorized access to your accounts.

Credential Stuffing

123456	111111	1234567	1234
123456789	123123	qwerty	iloveyou
picture1	12345	abc123	aaron431
password	1234567890	Million2	password1
12345678	senha	000000	qqww1122
qwertyuiop	asdfghjkl	zxcvbnm	football

Figure: Common password examples

Credential stuffing is rapidly becoming one of *the most significant security threats worldwide*. This threat consists of finding "useful" information, especially passwords, from one source and trying to "stuff" them into another unrelated account or website. Hackers are able to prey upon people's bad habits of using the same or similar passwords for multiple sites and accounts, such as using login information from a simple cooking recipe website as the same login information for their bank or tax accounts. Simply put, this threat is enabled by the user's bad habits that are usually derived from the false assumption that user's must memorize their account credentials.

Various estimates from the I.T. security industry show that over 50% of people reuse passwords on multiple accounts, and approximately 13% use a single password for everything. **Please stop trying to memorize passwords**. This habit leads to many security problems, and as most people can tell you, bad password habits are not even easy to maintain as it often results in lost accounts, or constantly needing to reset your password to get back in. Instead, write information down somewhere safe, or use password management software on your device. A unique, strong password combined with 2FA/notifications will protect your account and alert you when someone tries to login.

Personally identifiable information (**PII**) and security details available on the web or in hackers' databases may still contain information and passwords that you have used several years ago. Whatever password lists scammers have may not work currently, but different hackers will keep finding, and using this information over and over, *literally for years*, until one of them eventually succeeds. If information has been leaked or hacked that contains non-changeable information, such as you date of birth, social insurance number or your full legal name, then you may experience problems for years to come, requiring constant diligence and credit monitoring. This long-term high alert is **not easier** than just writing your unique passwords down. Common password "tricks" that many people use are not effective, like changing from "password1" to "password2" or "password!". There is no password "trick" that hackers have not encountered before. Keep in mind that the internet has existed for many years and hackers ***also*** gather information to analyze people's online habits.

It is not uncommon for small company networks or websites to have lax security due to a lack of knowledge, staff, or the finances to consistently maintain and update their networks. Frequently, these small companies are targets for hackers simply to gather *reusable* account information, even though the company or website may not contain any financial information. Data gained from easy access targets can leave an open door to more secure websites or accounts. Credential stuffing is the same as any other crime of convenience - like trying the handles on every car on a street just to see if they'll open, but with much more devastating consequences than losing spare change in your cup holder.

You can *easily* defend against this crime of convenience simply by using unique account details that are useless anywhere else.

WiFi Security

Always keep a strong password on your WiFi access as well as your router's administration settings. Many WiFi routers come pre-installed with a login name as "admin", and a password as "password" or even just a blank space to access the router's internal settings. Login information may also be printed on the bottom of the router or in the router's documentation. It is always recommended to change the factory-installed password on your devices.

Internal settings on many routers can usually be accessed by typing one of the following in the address bar of a web browser:

192.168.0.1
192.168.1.0
192.168.1.1

These are called I.P addresses, which for the internet, is the number version of a web address. Think of this in phone terms, when you tap "mom" on your phone, it doesn't dial the letters M-O-M, instead it translates that word to the appropriate phone number to connect the call. Similarly, when you type google.ca it gets translated to an IP address. All network devices have an IP address, but for home users the IP address for your router is probably the only one you would ever have need of knowing.

TIP: scam callers sometimes try to scare victims with technical terms by using the phrase "your IP address has been compromised", this phrase is meaningless and is just "techno babble"

When setting up a router, it is recommended to avoid using personally identifying information for the name of your WiFi network (referred to as a SSID or Service Set IDentifier), like your name, address, or phone number. Instead use recognizable but non-identifying names for you SSID.

WiFi communications are scrambled (encrypted) to protect your network and passwords. You should set the encryption type within the router to the current recommend level as hackers learn to bypass older encryption types. As of 2021 the recommended encryption setting is WPA2 with AES. If your router or device cannot use the current recommend encryption, then it should be replaced.
Keeping the internal software (called firmware) for your router or network device up to date is **very** important. Most modern routers have settings that will access updates for you but may require you to activate this feature manually. If you are not sure how to keep your router or WiFi device up to date with the latest firmware or encryption, the manufacturer-provided documentation or website may contain instructions, or you can ask a local computer service for help.

WiFi-enabled devices like cameras, smart T.V.s, even smart kitchen appliances called **I.O.T.** devices (“internet of things”) are often forgotten about when it comes to updating the internal software. It is not uncommon for off-brand devices to provide lower quality support or lack updates as often times the manufacturer may be difficult to contact. Replace non-updateable or obsolete I.O.T. devices or remove these devices from internet access if you cannot keep them updated with the latest security features. Stories or news that you my hear of hacked baby monitors or security cameras are frightening and real events as these devices often get overlooked for keeping up to date security.

Many WiFi routers can create a secondary “guest” WiFi network. Use this when available to provide WiFi access to others as a guest network as it is isolated and secured from accessing the rest of your home network. For the same reasons, the guest network is also recommended for use with any I.O.T. devices you may have, such as wireless cameras, fitness trackers, or home appliances.

Since WiFi itself is a convenience technology and is susceptible to security problems, using wireless connections on a device or printer when it is already in close proximity to other devices isn’t the best practice. Connect devices by wire instead of using WiFi whenever possible. (Speed/stability of a wired connection is also considerably better than WiFi) Disable the WiFi feature on devices if wireless will not be used, including turning off WiFi on laptops that remain plugged in with a network wire.

Free WiFi hotspots, such as at a coffee shop, are convenient but can also present a security risk if the location does not have proper security protocols or encryption in place (Security/Convenience Balance). In addition to a hotspot’s potential security flaws, the WiFi signal name (SSID) can be faked by a hacker. It is easy for anyone to rename their WiFi SSID to display “Coffee Shop Guests”. When using any free hotspot remember to ask an employee to verify the correct name of a guest connection. Be cautious about transmitting private or financial information such as account logins or credit card purchases on a public WiFi. Finally, make sure your system security is functioning and up to date while using hotspot connections.

Additional Note: It is common for some routers and internet-connected devices to have a “quick” set up button called WPS, so that you don’t have to use a password to connect (Security/Convenience Balance). Not surprisingly, since this is a convenience feature, WPS has been shown to have

security flaws and creates a risk that is easily hackable. Disable the WPS feature on your router if possible.

Understanding Internet Addresses

A website's address or "URL" (Uniform Resource Locator) contains information about "where" your web browser is connected. Understanding it may help you stay safe. The URL can usually be found along the top section or address bar of your web browser. Let's consider each section of a typical URL:

1. ***https***://www.google.ca/

The first portion of an internet address is called the scheme; HTTP stands for hypertext transfer protocol, otherwise known as communication for a standard web page. *HTTPS* is "HTTP Secure". This should be used when accessing secure websites like banking or sites that require a login. Other schemes you might see are mailto://, which can open your computer's default email service provider to help you draft an email to the email address you entered in the URL, and ftp://, which is a standard protocol for transferring computer files between a client and server on a computer network.

2. https://***www***.google.ca

www stands for "world wide web". Sometimes you may see *www2* or *www3;* This is used when websites are "off-loading" traffic to an alternate web server; This is *rarely* a security issue. Some web browser software may not display this part of an address.

3. https://www.***google***.ca

This portion refers to the “domain name” or website name. Words in front of the domain name are still owned by the same website and are called subdomains.
e.g., www.***security.google***.com. Separated words behind the *intended* domain name are NOT from the same website and are a common scam technique. For example, www.google.security.com wouldn’t be the “security” page of google.com; it instead would be the “google” page of security.com.

Other examples of fake/misleading sites:
www.cibc.login.com
www.adobe.flashplayer.update.com
www.security.com/cibc
www.acounts.com/appleID

4. https://www.google***.ca***

This is called the country code or ccTLD (top-level domain), and it is *not mandatory* for a website to use a matching TLD when originating from a specific country such as:
.ca (Canada), **.uk** (United Kingdom), or .**cn** (China). The TLD may indicate a type of business such as: **.com** (commercial), **.edu** (school or university), or **.org** (organization).

Since it is not mandatory to use a specific TLD it may only help to determine where a website is from but is more likely just to be of use to make sure you are at the intended version of the website that you were looking for, such as amazon.ca instead of amazon.com.

Other information shown after these elements is information that is relevant or required by the specific webpage you are on.

Email Security

Spam (junk mail), scam (fraudulent mail), or phishing (information seeking mail) emails are all too familiar for anyone who has an email address. Regardless of which email service you use, you should learn how to use the available blocking or "filters" to get rid of unwanted email. Well-known services often have online help or even how-to videos on sites like YouTube to learn how to use additional settings in your email.

Scam emails are often written to elicit a sense of urgency by claiming that you have account problems with a service, such as pretending to be an email from Amazon, eBay, Netflix, PayPal, credit cards, or popular banks. For Canadians the scammers also target us with fake emails pretending to be from Shoppers Drug, Canada Post, Tim Horton's and Canada Revenue. These emails may try to convince victims to provide personal details, fill out phony surveys that lead to dangerous websites, may offer rewards, prizes, or cash. The more popular the service is then the more likely scammers will try to exploit their brand name with fake emails.

Never reply to emails claiming loss of service or account problems, have offers that seem too good to be true, or ask you to verify account details.
Here are a few simple rules that can keep you safe, as well as protect the people that you have online contact with.

1) Don't forward email without a person's permission.
When you forward an email, it will contain the original sender's address as well as your own; If the next person does the same and forwards the same email, then both your address *and* the

originating address are sent along again, and so on, just like old-fashioned chain letters. Without any doubt, this can eventually lead to security problems at some point. For example, someone who receives this email gets infected with a virus, which begins sending emails that falsely show *your name* as the sender. If you are resending anything in an email, you should copy only the needed content or "body" and then paste it into a new email.

2) When sending an email to multiple people, use an option called B.C.C.:
"B.C.C." stands for "blind carbon copy", which simply means that each person receiving the email cannot see the names and addresses of any other people who receive it. When sending out "group emails," not using B.C.C. can easily cause the same security problems as the above notes on forwarding emails. If you're not sure how to use B.C.C. when addressing an email, take some time to look it up online with an internet search such as "how to use B.C.C. in Gmail", or ask someone knowledgeable for help.

3) Never respond to or use an "unsubscribe" feature for unsolicited junk email.
When you reply or unsubscribe to unknown junk mail that you didn't subscribe to in the first place, you are validating to spammers that your address is "live," which means your email address can be sold to other junk mail lists, which in turn will result in you getting more junk mail. Delete junk mail and take steps to set up blocking rules.

4) Learn how to spot scam emails.
A company logo and official appearance are very simple to imitate and can be easily added into an email to fool you into clicking a link or providing secure details. Scams or fraudulent emails can usually be spotted due to:
a) Improperness wording, poor grammar or spelling errors
b) The use of impersonal greetings like "dear client" or using

your email address as the salutation name such as “dear bunnyslippers@hotmail.com”

c) A threat of loss of service or account termination unless action is *taken immediately*

d) Origination from an unrelated email address or an address that appears similar to the actual company, but not correct. (i.e., m**1**crosoft.com instead of microsoft.com)

e) ANY requirement to click a link within the email to provide further details about your identity or account.

f) The email is addressed to multiple people

5) Do not open attachments from sources that you aren’t expecting. Email attached documents can be a source of viruses.

Scammers may try to bypass policies of not opening email from unknown sources by using emails where the sender can’t be anticipated, for example, a job resume sent to your workplace or a fake invoice prompting curiosity of why you are being billed for something. In these situations, where you may need to open attachments, you should download the attached file first and scan for viruses before opening it.

These are just some of the methods you can use to identify email problems – While we have come a long way from the old “Nigerian prince scam”, always keep in mind that scammers are likewise getting more sophisticated and are inventing new techniques all the time.

Surprisingly, spelling errors or other small noticeable mistakes may be a tip-off to the savvy, but mistakes are at times included intentionally in scams. They weed out users that are more knowledgeable or those that may easily become suspicious, thus allowing the scammer to focus efforts instead on the more vulnerable victims. So, if you are able to catch these red flags, please make sure to help others to avoid falling victim whenever possible.

TIP: On a computer, if you move your mouse over a link (without clicking) in an email, the browser or email program will show the link's destination. If the actual destination of the link does not match the text, then there is definitely a problem – for example, the link text says "amazon.ca" but hovering over the link displays lkjuasdfbligaihaagf.com. On portable devices (phones, tablets, etc.), displaying the destination of a link can be a bit more complicated, therefore reserve the handling of important emails to when you are using a regular computer instead.

If you have been using email for many years, you may have noticed the trend in using online webmail for *home use* instead of email programs like Outlook Express. Many of these email programs are no longer available, supported or recommended. Overall, webmail does provide a more secure environment for email, as an online service can be continuously updated, secured, and maintained. In contrast, an email program requires all of its users, on a variety of devices, to constantly update or download the different versions, updates and to maintain proper device security levels.

Some email platforms allow you to flag an email as phishing, in addition, Canadians can forward scam and junk email to: spam@fightspam.gc.ca

Visit **www.fightspam.gc.ca** for information on Canada's anti-spam legislation.

Junk Programs

There are many programs available that claim to make your computer usage *better*, run *faster*, enhance your internet experience or offer dozens of other “snake-oil” claims. Without any doubt, the majority of programs are junk. They are a waste of money at best, a security threat, or a means to harm your device at worst. You do not need optimizing programs for your devices. Simple maintenance like updates and clearing out junk is all that is recommended to do to keep your machine running well.

Useless or damaging programs include all types of junkware such as driver-updaters, web-optimizers, “special” media players, registry cleaners, browser add-ons, or browser toolbars. Your device will run better and safer without them.
In general, if you are not sure if you need a program or app that is installed on your device, then you can research the software name to decide if you can safely remove it.

Free! Free! Free?

There are almost unlimited free websites, services, email providers, games, programs, and apps on the internet. Free software or support can exist at times as a “bonus” for existing customers, such as a printer company offering photo software to manage your pictures. But unfortunately, often free programs are loaded with intrusive advertising or may be

“spyware” that gathers data on you in trade for your “free” usage.

Many websites offer free access to information or programs to generate revenue from a *reasonable* level of advertising which pays for staff and equipment, which is a similar business model to public access television showing commercials every 15 minutes. For example, using this business model services from Facebook, which users don’t *directly* pay for, were able to generate revenue of over $17 billion in 2018.

Apart from advertising, another way to generate revenue for many digital products is to gather data about you and your habits and sell that information to third parties. Most “legitimate” free services or products have an “end user license agreement” (EULA) often authorizing their gathering of data about you in trade for your “free” use of their product or service. Sadly, many companies exploit the fact that the average person can’t be bothered to read these long legal documents before clicking on the “I agree” button.

Laws are slowly starting to be put in place to protect people from data gathering that is *too intrusive*. However, it’s a complex problem to solve by legislation since most people *willingly agree* to these agreements in trade for a free service, the latest game or to watch the newest movie on the internet. One fix for intrusive data mining is to be more cautious when choosing to install a free app or game and use diverse or alias information when signing up for services. (see section Reduce Your Digital Footprint for more help)

As dull as they may be, you should read license agreements (EULA’s) before you click “I agree.” Companies know how valuable your information is, and this is why they are so willing to offer you something for *free*. Whether it’s a store’s “loyalty card” or a free game on the web, take a better look at what

you have to give back to receive something for “free” and decide whether or not it’s worth it. (Security/Convenience Balance). Also look into a service or company’s “security track record” and their policies on protecting the information that you provide, before agreeing to provide your valuable data to them.

Figure: a bundled Java installer

Another related area of potential problems with *free* software*/*apps is commonly called “*bundleware*”, which installs multiple programs along with the intended software. Usually, someone will encounter bundleware when trying to find *free* software for a specific use, like cropping a video, recording music, or managing downloads. Bundleware can originate from legitimate software companies that in return receive revenue for promoting another company’s software.

In these cases, there is *usually* an option for the user to choose not to install this additional software. However, as many people habitually quickly click through install options, they can unknowingly "agree" to install the extra software. For years the program "McAfee Security Scan" used the method of installing via bundleware; thus, due to quickly clicking "ok" people often had no idea what the software was or how it even got on their computer.

Bundleware can also come from less reputable sources that have modified the original software package to install several other harmful programs simultaneously, with no options for the user to decline the extra software installs. Commonly, dangerous bundleware can be found when downloading programs from a website other than the originating company (Adobe Flash Player is a great example that should only be downloaded from Adobe.com). The offending website or programmer will take the original legitimate software (without permission) and add on other programs. Usually, after installing these types of "free" programs, you'll will find several other new junk programs on your computer, your browser may be *hijacked* to use a different search site, you may find that you have a dangerous fake security program on your computer, or an actual virus infection. Many times, these bundled programs are intentionally hard to un-install and may require special software or professional cleanup. Downloading of "pirated" software, programs that bypass a software's license called 'cracks', or programs for downloading illegal content often contain harmful bundleware since the source of these programs are often hackers themselves. Without discussing the legality or morality of downloading unlawful software, they are often dangerous and include serious security threats to your device.

If you notice programs on your device that you don't recognize and that you didn't intentionally install, or you notice that your browser behavior/home page suddenly changes, then you

should take some steps to look up the problem on the web, uninstall the programs, or get some help removing them and restoring your settings. A Google search of a program name or looking it up on **shouldiremoveit.com** may help.

Fraud Phone Calls & "Scareware"

Fraudulent support phone calls or fake pop-up messages on your device are intimidating but straightforward scams. The only difference between these two types of scams is whether they call you or you are convinced to call them. Many scammers will often claim they work for, are partnered with, or are authorized by well-known company names to gain your trust. They will often state that they are calling to help you because one of your devices is having problems or is infected. Phone support scammers rely on the basic fact that day-to-day computer problems are very common. Due to this, their call seems to coincide with actual issues on your device. Just hang up on these phone calls. Companies like Microsoft, Apple, Google, Facebook, McAfee, Norton/Symantec or any other computer or software company never call you at home and do not authorize anyone to call you or tell you that your computer is infected/having problems. These types of scammers will request remote access to your computer where they may quickly copy security information and passwords, install dangerous software or leave your device working improperly.

NEVER allow anyone to remote access your device unless you can verify who they are.

In addition to the security threat of what may be copied or viewed on your device, these scam phone calls may also result in the scammer asking the victim for payment for their fake support by requesting the wiring of payments or using gift cards such as Amazon, Google Play, iTunes, Steam account cards, or pre-paid credit cards, as many of these types of gift cards are not linked to a bank account and the funds are not insured.

“Scareware” is another method that phone scammers use. This is a term for a fake security program that shows dire security warnings on your device which provides a phone number for the victim to call the scammer. As most antivirus/malware programs will catch scareware installed in your device, many scammers now resort to using fake websites with similar messages that usually will “lock” your browser to prevent you from closing the warning page. Easy ways to spot these scams are claims that your computer has a very serious problem! you must not shut down! and you must call 1-800- now! or else something *serious* will happen!. Scareware tries to create a sense of urgency intended to get you to pay to fix the fake problem. As a bare minimum, when a warning on a device includes a phone number to call, you can be confident that it is a scam, as legitimate software companies rarely provide a support phone number pop-up on your device.

If a fake warning message persists on the computer even after rebooting or re-opening your web browser, you may need a security scan or a professional cleanup to remove any threats on the device. Regardless of how convincing they look, which company logos they use on the warning, or how persuasive/aggressive they are on the phone, these phone numbers and phone calls are just scams.

Figure: Fake security warning with scammer phone number

Similar to the above-mentioned support scams, while looking on the internet for computer support, you may find false phone numbers or 3rd party companies *claiming* they are authorized to support a specific company's product or offer support for general computer problems. At times it can be difficult to find the proper phone number from searching online for a company's support, so be aware of which website is offering the phone number. For example, only rely on a phone number for Microsoft support that is provided on the Microsoft.com website. These fraudulent support companies will always request remote access to your computer; and will then claim your device is full of problems and viruses, for which they offer to clean up, or install phony security software for a *considerable fee*. These fake support companies are usually easy to check out online by typing in the "name of company+scam" or "phone number+scam".

To bypass law enforcement, some of these companies offer real, but “weak”, support for very expensive fees, such as doing nothing more than installing a free antivirus for hundreds of dollars. At times it can be difficult to punish or get a refund from these companies as the victim agrees to the service, similar to if someone offers to mow your lawn for $500 and you agree to it, there is no technical crime committed other than user being naïve or non tech savvy.

If you feel that your device may have real issues or that a warning message might be valid, initiate a security scan or contact a local computer service for help or advice. Most local computer service/stores would happily answer a quick phone call to ask if a pop-up warning message is legitimate.

There may be an exception to phone calls for a computer security problem. If your computer is infected in a manner that is sending out dangerous traffic over the internet, then your internet provider company *may* contact you to advise you to get the computer cleaned up. (be careful though, scammers claiming to be from large or nationally recognized internet providers can also use this type of call to offer a “cleanup” …for a considerable fee, of course) As soon as fees are mentioned with **any call**, this should put you on alert that it may be a scam. Trust your instincts, and don’t be intimidated. As in many types of scams, this call is similar in that you will be able to verify a caller’s authenticity by calling your internet provider yourself. Alternatively, in this situation, an internet provider may not necessarily initiate contact with you; instead, you will notice that your internet service has been shut off, which will undoubtedly prompt you to call them.

The **fake email extortion** or **sextortion scam** is an email that the scammer sends with a *claim* that they have infected your device and can see your “adult” browsing history as well as record you from your webcam. To make this threat seem real the scammer will include an actual piece of personal

information in the email. (this is usually just information that has been gathered online or from hackers lists as mentioned in the credential stuffing section). This scam will state that you have to pay them, or they will send the pretend compromising information they gathered on you to your family or workplace.

Another prevalent computer-related phone scam worth mentioning here due to its increase in popularity is the **refund scam**. Sometimes this scam originates through a fake email notifying or thanking you for an item/service purchase, or it may also start with phony support and the processing of the payment for it. Regardless of the initiating method, the scammers offer a refund to the user. Then, to show this *refund* happening, they request access to your device to process this refund. During the call, the scammers shows you on your screen that they *accidentally* provided you too large of a refund, usually in the thousands of dollars; Then, through various stories like being fired for the error, becoming homeless, etc., they prey on people's sympathies and convince the victim to send them the difference of the refund amount to them in **cash** so they won't get in trouble. The victim is instructed to courier the money *quickly* to an address, which in actuality is a short-term rental apartment or "Airbnb", rented under a false name. It is then gathered by "money mules" working for the scammer. Cash deposits are untraceable, so with this scam, the victim is unlikely to ever have their money recovered. Furthermore, a bank or financial institution will not insure loss caused by a customer withdrawing their own money.

Other types of fraud may not be computer/internet related. However, they should still be avoided, such as calls or texts claiming to be from a government revenue office, law enforcement, or immigration service, often threatening arrest unless you pay fees immediately. With the global pandemic, covid-related scams have also been added to scammer's

methods. Scammers sometimes may even use a fake "spoofed" phone number and seem very convincing and intimidating. If you are concerned there may be a legitimate problem, hang up and call the government agency, police, or health agency etc., through alternate means. Keep in mind that law enforcement wouldn't be very effective if they called people ahead of time to warn them of an impending arrest, and that this intimidation is just another fear tactic used by scammers.

Phone calls, scam web pages, fake email, and fraudulent phone texts are an easy, inexpensive way for scammers to target the maximum number of people effectively. According to TechRadar, "For every 12,500,000 emails sent, spammers receive one reply." For each scam, or fake email this figure would amount to an incredible number of scam emails sent every day to generate billions of dollars every year for the scam industry.

According to the Canada Revenue Agency, about 55 Canadians a day were victims of a scam last year – 'Listen to Your Voice of Reason Before You Act!' Beware of scammers posing as Government of Canada employees. You can learn what to expect if the CRA contacts you by visiting the official Government of Canada website: Canada.ca/be-scam-smart

If you or someone you know has allowed remote access to any of these scams. Especially if it involves payments or compromise of your identity, you should contact local law enforcement, any affected financial institutions, and a trusted local computer service for further help. Any financial loss or identity theft should also be reported to the Canadian Anti-Fraud Centre.

Never give out identifying information or allow remote access to your device before adequately identifying the source.

See the Canadian "**Little Black Book of Scams**" online at **www.competitionbureau.gc.ca** for more information about scams covered herein, as well as others.

Online Shopping

Online shopping has become commonplace in today's market. Businesses like Amazon and eBay and others have changed the retail landscape. When buying online, make sure to check a company's or seller's reviews and history before making an online purchase.

Services such as PayPal can be used to make a payment by acting as a middleman that can insulate your credit cards from direct contact with the seller; this works by paying the funds to PayPal, and then PayPal sends the money to the seller. Other payment types may be available, always choose a type that provides some protection.

If possible, use a separate credit card for online shopping with insurance, purchase protection, and a set limit on the amount spent online or during a single purchase (with 2FA if available).

For local online classifieds such as Kijiji, always arrange to meet in person, inspect the product, and exchange funds. Whether buying or selling, never go alone. Arrange to meet in a public place, like a coffee shop or even a police station. Be wary of cash "up-front" requests and be sure to get a receipt. Never wire funds. If a seller asks you to wire payment via

Western Union or MoneyGram, you are likely to be dealing with a scammer.

In Southern Ontario, the Essex County O.P.P. has implemented a program to provide a camera monitored “safe purchase location” for exchanges set up online. We are proud that this program has caught on with other agencies. Check with your local detachment for availability in your area.

Online Banking

The banking, credit card industries and many online retailers spend millions of dollars every year to keep electronic transactions secure. For the billions of transactions occurring worldwide every day, this has become a cornerstone of modern society. The communications that are used for online banking are very secure and security problems are *usually* caused by the user’s actions or something interfering within the user’s device. If your computer is infected with malicious software or a virus, has weak passwords, or you allow remote access allowing someone to see what you are doing or access your files, that is usually where the security problems with online banking exist.

If you use online banking, simply make sure that:

1) You use an updated and secure web browser and operating system

2) You login using only secure websites with HTTPS in the address (keep in mind that even a HTTPS can be faked, but if a site *doesn’t have* HTTPS then it *definitely* is not properly secured).

3) You use secure and unique passwords for every individual account.
4) If you keep financial records on the computer, ensure that both the computer and the documents are secured, and password protected. Many word processing & document programs can be used to password protect a file. Search online for help or instructions on how to do this.
5) You regularly scan for viruses or malware.
6) You check your accounts regularly for unrecognized transactions

Some online banking services offer 2FA security features or even options to send notifications by phone, text or email whenever there is a login. See if 2FA or alerts are available from your bank.

Important Note: If you use a web browser program, always open a new browser session when beginning online banking. Do not conduct financial transactions with multiple tabs open on your browser. Instead, use only one tab, then log out and close the browser when done. A website can access information regarding other websites that are open simultaneously in your browser, which website you recently came from, and which website you go to next.

Social Media 

Social media is just a tool, and how it is used determines if it has any value to you. Whether you're a journalist using social media to report in a war zone or you're taking photos of your lunch and posting cat videos, what you do with social media is up to you. Regardless of the platform, here are a few things that you should keep in mind from a security standpoint if you are going to use social media.

It is *your responsibility* to understand the security and privacy settings available for any platform. This includes:

1) Whether or not your postings are private or public
2) Whether your contact information and personal details are private or public
3) Who can message you and who can contribute to your posts.
4) Reducing your digital footprint (See next section) by being cautious about posting identifying details that can be used to exploit you by
5) Treat all of your posts with the permanence of getting a tattoo. Once you post something and it is *let loose* on the internet, there is no control over where it ends up from there or who will see it. *Even if a post is deleted afterward,* it may have already been copied, forwarded to someone else, backed up, or a screenshot may have been taken. So please choose what you post online wisely, and treat it as permanent.

A common scam with social media is attempting to access your information by sending a "friend request" while posing as someone you know, regardless of whether you already have that person as a contact. It is easy for scammers to make a new account with the name of someone you know and simply

copy their publicly accessible profile photo. If you have doubts about the identity of a friend request, contact that person from other means, or ask a question *only they could answer* before accepting the request. An extreme example of unwanted online sharing occurred around 2018 (and fortunately was publicly exposed). U.S. military personnel that were stationed at undisclosed and secure bases were using Fitbit like activity trackers. Online fitness tracker Strava made a publicly available map posted online showing the paths of its user's logs as they run or cycle. For military users that didn't turn off data sharing the map was able to show the shape/structure of foreign military bases in countries including Syria and Afghanistan as soldiers moved around them as well as which roads nearby were well patrolled. Other leaked data showed activity routines disclosing exact patrol times.

Important Note: Some cameras or cell phones have settings that "tag" additional information into a photo such as location of where the photo was taken. It is highly recommended to disable this feature, especially when dealing with digital images of children.

For parents trying to guide their children's online usage and avoid internet dangers, the task can seem to be overwhelming. Issues such as sexting, sharing inappropriate

photos, accessing adult content, cyber bullying, sharing inappropriate personal details or encountering online predators may require new parenting skills and assistance. For help with social media usage by children or teens, refer to the Youth Diversion's #KYPP program which stand for #KeepYourPrivatesPrivate. Also refer to the Digital Drivers e-Presentation. **www.ecyouthdiversion.ca**

If you or someone you know is experiencing Mental Health challenges as related to use of social media or technology, please visit **https://211ontario.ca/.** Found on that page is an online directory of local supports. You can also call, text, or email your concerns and receive a personalized response.

Reduce your Digital Footprints

Avoid answering questions/polls on social media about your favorite teacher's name, name of your first pet, first car, etc. Questions and polls like this may seem harmless and fun, but they are the exact same questions that a secure website or bank may use to validate your identity. A Google image search for examples of "security questions" may shock people who have answered these polls. Whenever possible, suggest to the poster to remove dangerous posts like these when you see them.

Posting information, pictures, or "check-ins" that show your location or daily schedule when you are away from home or vacationing can be used to commit a crime. Watch out for

revealing details in the background of photos like landmarks, addresses, and license plates; Information like this can easily be used for planning break-ins or other crimes such as stalking or child abduction. Wait till posting vacation pictures until after you get home. It is common for users to view the internet in “global terms”, but information can just as easily be found about someone locally.

Be mindful when posting or sharing of information that contains any personally identifiable information. To use a spin on a popular phrase, feel free to dance like no one is watching, but post like everyone is.

Use different emails and usernames (you should already be using different passwords, of course). Be careful not to create an easily traceable “trail” across the internet. For example, one social media website may have posts of your birth date, another may have family photos and names, and another may have info of where you or relatives live (including children), there may even be info of which bank gets a “thumbs up” from you. With social media, blogs, forums, and chatrooms, there is no limit to what type of info may be divulged in simple conversation without regard to how it may be exploited, so using a different username and email can leave this information disconnected from each other.

Many people are unaware that is unnecessary to always divulge accurate or complete personal information when signing up for accounts or services; you can create an alias or alternate data such as a throw-away email address or fake date of birth for non-essential accounts or mailing lists.

It is only legally necessary to enter exact personal information when stated and legally required, such as for financial/gov’t accounts.

What could alternate emails/usernames look like for someone named John/Jane Doe?

jodo-shipping ▪ jo.do ▪ Amazon-Jane ▪ jEbay ▪ JoMovies ▪ JayneDee ▪ JDspambox ▪ JayOnline ▪ Jdo-junkmail ▪ j.d.soho ▪ TheDoeMail

Get creative, use information for only one account; record your info somewhere safe.

There are services and browser-plugins that can provide functional but disposable emails and passwords for this purpose. Many internet providers and online email services offer the ability to make several **alias** names under one account that can be used to diversify your contact information. Check with your internet provider or search online for how to setup aliases for your online email such as Hotmail or Gmail.

Digital security is a constant arms race between security professionals and hackers. As developers continuously secure software and hardware, hackers probe for weaknesses and exploits, and easy to discover information to gain access. Despite having users follow safe practices and using secure devices, companies are still subjected to a constant barrage of hacking attempts that puts **your** data at risk. Data leaks and hacking of user information is unfortunately out of your control despite your own safe habits, so taking steps to reduce and diversify your data online is your best option to keep your personal information secure.

TIP: By using alias/alternate data, it also provides a way to track which companies leak your information or sell your data, such as when you begin to receive emails from a third party that is using your alternate information that was only used for one account.

Romance Scams

Online dating sites and social media are common ways to meet people in our modern internet society. Still, they are also a potential source of online fraud. Romance scams are one of the most common types of online fraud, costing hundreds of millions of dollars every year and, unfortunately, is one of the most under-reported scams. It is estimated that only 1% of victims report this type of fraud as people are usually ashamed of falling for a scam or, because of the personal nature of romantic communications, they are too embarrassed to discuss with family, friends, or law enforcement.

With millions of people turning to online dating apps or social networking sites to meet someone, seniors, both men and women, are a major target for this type of scam. But instead of finding romance or companionship, many find a scammer trying to trick them into sending money. In large operations it may not even be just one person that you may be 'chatting" with, as you are groomed into the relationship; it is passed on to "higher ups" who are more skilled at completing the money part of the scam. **Never send money or gifts to a "sweetheart" you haven't met in person.** Scams are constantly evolving, but romance scammers usually use a few techniques and storylines in common regarding who they claim to be, why they need your money, and how they ask for it.

Who: Usually someone who claims to be from a financially gainful career that happens to be in a remote area. Commonly used stories claim to be a doctor overseas, deployed military

personnel, or an oil rig worker. This inaccessibility of their job is part of the lie of why it's difficult to see you in person.

Why: The scammer will ask for funds to cover "urgent" problems such as travel expenses, emergency medical bills, border customs fees to retrieve something important, a travel visa or legal fees for documents, and even to cover gambling debts. Of course, they promise they will repay, but never do.

How: As with other types of scams, they will request money in forms that are hard to trace or refund. Common methods that a scammer may request money is by wiring the funds or using gift cards such as Amazon, Google Play, iTunes, Steam account cards, or pre-paid credit cards, as many of these types of gift cards are not linked to a bank account and the funds are not insured.

If you suspect you're involved in a romance scam:

1) Stop communicating with the person immediately.
2) Talk to someone you trust, don't ignore advice or warnings from your friends, family, staff at financial institutions, or even a store clerk if they have valid concerns about a relationship, money withdrawals or transfers, or gift card purchases.
3) Search the type of job the person claims to see if other people have heard similar stories. For example, you could search "oil rig scammer" or "U.S. Army scammer."
4) Try a reverse image search of the profile picture that the scammer is using to see where it may have originated from or where else it is used. **www.tineye.com** is a valuable site that may have results for this type of search
5) Report it to law enforcement on a non-emergency number and/or the Canadian Anti-Fraud Centre at: **www.antifraudcentre.ca** 1-888-495-8501
6) If gift cards were used, contact the company that issued the card as soon as possible. Tell them you paid a scammer with the gift card and ask if they can refund your money.

Regardless of the type of fraud, scammers focus on methods of payments that are non-refundable. Using a courier for cash may be an obvious red flag but using a wire transfer is also a form of 'final payment'; funds are not recoverable after a wire transfer has been sent. An EMT (Electronic Money Transfer) is also very difficult to recover funds from. If fraud is suspected there are times the receiving financial institution may place a hold on incoming EMT funds and the sending financial institution can request a return of funds. However, in most instances of fraud the funds are gone before anyone identifies that the fraud has even taken place. Just like cash or gift cards, one should expect that when a wire transfer or an EMT is sent, the funds are not recoverable.

Other scams that often target seniors are the **'grandparent'** or '**inheritance' scams**. With the grandparent scam there is usually a call requesting immediate money for some type of emergency from a grandchild. Bad phone connection or infrequently speaking to the "grandchild" may be excuses used to explain away not recognizing their voice. A sense of urgency is created by claiming an accident, fines or bail, or other immediate emergency. Verify identity with questions only a family member could answer, contact the "grandchild's" parents, or even local authorities from where the claim is coming from.

If you are unable to verify their identity or the occurrence, you should contact your own local police for assistance.
The **inheritance scam** may be one of the older scams and though most people are already familiar with it, there are many people who are still victims of it every year. The story with the scam may vary but it is usually claiming an inheritance from a deceased person or distant relative who has left an estate or funds to the intended victim. The scam is usually sent from someone claiming to be from a law firm that is trying to find relatives to give the inheritance to. The scammer begins by requesting small amounts of money like $50 to cover

administrative fees. The victim will then be told everything seems in order, and the scammer now requires their banking information to complete transferring the inheritance to the victim's bank account. This banking information allows the scammer to empty the bank account, possibly steal the victim's identity or use the information to sign up for credit cards or loans.

This type of scam gains effectiveness from a few factors. The scammers may use names or logos of legitimate law firms, which of course is easily copy-able from the internet. The letter may contain valid information about the intended victim from sources mentioned previously in the section on "credential stuffing". Lastly, in real events of an estate inheritance, actual law firms have been known to seek out relatives.

As with other scams, you should talk to someone you trust, and don't ignore advice or warnings from your friends, family, staff at financial institutions if they have valid concerns.

See the Canadian "**Little Black Book of Scams**" online at **www.competitionbureau.gc.ca** for more information about scams covered herein, as well as others

Did you know? Not all scammers are just individual criminals, some are associated with large operations, organized crime and even forced labour situations where rows of callers are patrolled and watched over by armed "soldiers" to make sure calls are being placed. As a multi-billion-dollar problem it reaches into the darkest corners of society.

Leaving a Computer On

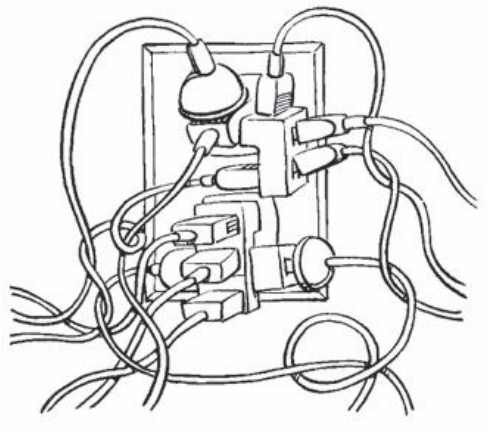
Most people wouldn't think that leaving a computer on while in a safe place could be a security risk. When a device is shut down, it is removed from any network virus or remote access threats, clears any information stored in memory cache, and allows for any updates to complete, (which are often security-related). In addition, most modern devices have become fast enough that turning it on only when needed is no longer an *inconvenience.*

TIP: In addition to security factors, keep in mind that electronic circuits, hard drives, routers, modems, and cooling fans have a limited lifespan, and this lifespan is also reduced by heat generated during normal usage - and of course, shutting down protects against power surges, storms and saves electricity.

Additional notes regarding power:

Low voltage devices such as phone or tablet chargers can still cause fire hazards, be careful charging devices near bedding or blankets, especially when unattended. Always replace frayed or damaged wires.

Surge protectors only protect in the event of a large electrical surge such as a lightning strike. Smaller day to day fluctuations and "brownouts" are not stopped by a surge protector, and these small fluctuations can still damage computer components. Use a protector with "voltage conditioning" if you have electrical issues.



Using a power bar or surge protector as a way to bypass a wall plug's limits and use *more* items than you would normally plug into a single wall socket is dangerous and can create a potential fire hazard. Be aware of safety limits and proper usage. Check online for tips and help from **windsorfire.com** and **esasafe.com**

Disposal of Devices

When disposing of or donating old computers, backup drives, or cell phones etc., always have the *storage* memory **securely** deleted, or restored to factory settings with any personal or account information properly erased or destroyed. Some devices have storage drives, with important data that may be needed in the future, that can be removed from devices and kept for safekeeping. Seek help from a trusted source if necessary.

Legacy Access

In addition to recording login information to assist and secure your own day-to-day online use, lacking legacy access is also a common security problem. Planning procedures in case of an accident, medical issue, or death is understandably an often overlooked or difficult topic. Keeping account records and discussing security with loved ones will make a difficult time easier by allowing access or allowing accounts to be closed.

Conclusion

Taking online security seriously is a necessity in the modern world. Many people still think that they are not at risk of being hacked because they don't have a lot of money or feel that they don't have important information. But even people who do nothing "special" on their devices definitely do have something worth hacking - information like their identity, contacts, access to friends and family, or details about them, etc. If you keep your digital life secure, it can help provide security not just to yourself but also to the people connected to you.

Switching to secure behaviors may take some time to break existing bad habits, especially when it comes to password use and trying to memorize them. However, with a bit of practice being safe can quickly become second nature.

With any future reading on anti-phishing or anti-scam information you will quickly discover that whether through email, phone, website, or other, that the majority of scams

require a user's active participation to succeed, so being even a little more *tech savvy* is a good defense.

To find more information on any of these topics many people are surprised to find out that search sites like Google can be used to find answers simply by using everyday language in plainly worded questions, such as "what is 2FA?" or "how do I secure my Facebook?". With approximately 7 billion people on the planet and decades of online usage, there is likely someone asking or answering the same question as you. Often, the "whiz kid" down the street who seems to know so much, is just somebody who knows how to effectively search for answers on Google.

Remember that despite the threats associated with digital devices and the internet, our modern digital world also provides access to unlimited amount of useful information and keeps us connect to one another.

After learning *safer* security practices, you can go to existing online accounts to update your details with secure personal information, remove unsafe posts, and provide unique passwords.

All of the included information has been developed with the assistance of law enforcement personnel and a computer technician/instructor with more than 20 years of professional experience and is carefully compiled from real day-to-day problems and encounters with the average computer user. Even though this booklet only briefly covers essential information on various security topics, this information can be a solid foundation for securing your devices, identity, finances, and keeping your family safe. While it is true that each matter covered herein can be expanded into an entire field of study, even knowing the basics is a good start.

Remember! - If you have been a victim of a crime, fraud, scam, or extortion, don't feel ashamed.

Report problems as soon as possible.

Please Be Safe
K.C. ☺

Windsor Police Service
Non-Emergency: 519-258-6111
150 Goyeau St. Windsor, ON N9A 6V2

Windsor Police Financial Crimes Unit
519-255-6700 ext. 4330

Amherstburg Police Service
Non-Emergency: (519) 736-3622

Ontario Provincial Police
1 888 310-1122

Please note that crimes cannot be reported via email, texting, or social media. Online reporting from appropriate websites may be available.

Always Call **911** in any EMERGENCY situation where immediate police, fire or ambulance assistance is required.

Further support is available from:

Canadian Anti-Fraud Centre
www.antifraudcentre.ca
1-888-495-8501

Essex County Youth Diversion
www.ecyouthdiversion.ca
(519) 253-3340

Canadian Anti-Spam Legislation
www.fightspam.gc.ca

www.windsorfire.com

www.esasafe.com

Computer Logon	name	pasword	date
Router Administration	name	pasword	date
WiFi Access	name	pasword	date
Wifi Guest Access	name	pasword	date
Internet Provider	name	pasword	date
Email Account	name	pasword	date
Email Account	name	pasword	date
Email Account	name	pasword	date
	name	pasword	date
	name	pasword	date
	name	pasword	date
	name	pasword	date

NOTES:

Investing In Your Financial Future.

For more than 25 years, we've been providing our members with the best investment, estate, insurance and retirement planning services under the WFCU Investment Services name.

With access to a wide range of income and growth-based investments, including **mutual funds and GICs**, we will take the time to understand what's important to you to provide a tailored investment approach, optimize your investment opportunities, and assist in managing your retirement portfolio through consistent and experienced advice.

Experience **Avanti Wealth** – your premier, locally operated, wealth management partner.

Schedule an appointment with us today!

Sandy Kosak
WEALTH CONSULTANT
Avanti Wealth

Michael Middleton
WEALTH CONSULTANT
Avanti Wealth

INVESTMENT SERVICES	ESTATE PLANNING	INSURANCE SERVICES	RETIREMENT PLANNING

7041 Tecumseh Rd. E., Windsor, ON
519-974-1181 • avantiwealth.ca

avanti | Wealth

AVAILABLE THROUGH wfcu CREDIT UNION

Avanti Wealth is a program provided by Credential Financial Strategies Inc. offering financial planning, life insurance and investments to members of credit unions and their communities. Trademark(s) of Avanti Wealth are used under license by Credential Financial Strategies Inc.