Cyber Security Toolkit

Protecting yourself from online threats

CANADIAN BANKERS ASSOCIATION

In partnership with

GETCYBERSAFE.CA

A toolkit from the Canadian Bankers Association and Get Cyber Safe to help you understand cyber security threats and develop a cyber hygiene routine to protect yourself.

We are all in this together. Banks in Canada are working around the clock on the prevention and detection of cyber security threats. They are working closely with each other and with bank regulators, law enforcement and all levels of government to protect the financial system and their customers from cyber crime. There are also simple steps you can take to recognize cyber threats and protect yourself and your money from financial fraud.

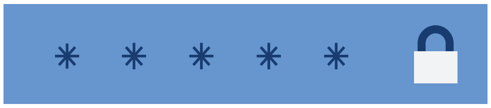
Contents

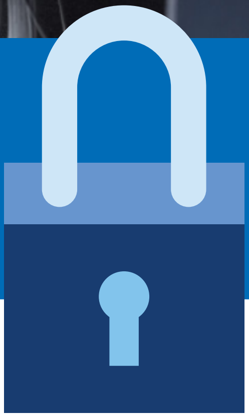
Cyber Security 101

The Internet has made it easier than ever to stay in touch with family and friends, conduct business and manage your finances with greater speed, efficiency and convenience.

Unfortunately, criminals also use the Internet to try to gain access to personal information such as passwords, personal banking and credit card details and social insurance numbers to commit fraud.

Our increasingly connected world means that your personal information is exposed to security risks. Criminals take advantage of the absence of strong cyber security safeguards. The good news is, you don't need to be a computer expert to implement strong cyber hygiene practices.





What is cyber security?

Cyber security is the set of practices that you have in place to protect your devices and personal and financial information. Cyber criminals target individuals to gain information they can exploit to steal money from you.

Cyber Hygiene Checklist

Protecting your devices and information from cyber attacks

Cyber hygiene is a great way to think about the importance of taking regular steps to proactively protect your connected devices, such as our mobile phones, laptops, desktop computers and smart appliances from cyber threats.

While banks in Canada use sophisticated technology and layers of security to help protect customers from fraud there are steps that you can, and should, take to protect yourself.

1. Protect your devices

Install anti-virus and anti-malware software on all your connected devices and keep this software up to date.

2. Install software updates and patches

Install software updates as soon as they're available for all of your connected devices. Don't delay as these updates have important security patches and fixes that will protect against the known vulnerabilities. Research shows that 42%[1] of smartphone owners update their operating systems as soon as an update is available and 56%[2] of Canadians update their anti-virus software at least once a week.

3. Create unique, strong passphrases and passwords

Ensure that you create strong and unique passwords for each website. This is important since a security breach at one site means your password could be handed to criminals who may try to use it at other sites. If you suspect or know that your password has been compromised, be sure to change it on the affected account and any accounts where you have reused it.

4. Schedule regular back-ups of your data

Back up your files frequently to a secure location and consider also saving critical files offline, for example in an external hard drive or on a USB flash drive. This practice helps protect your critical data from exposure to cyber threats like ransomware. Also ensure that you have clear procedures on how to restore your files from backup and a schedule in place to ensure backups are happening regularly. Always be sure to test your backups to make sure they work.

[1] Pew Research Centre, 2017

[2] Public Safety Canada, 2018

Cyber Hygiene Checklist
Continued

5. Disable file sharing networks

File sharing networks, often called “peer-to-peer” (P2P), are popular because they allow users to upload and download music, movies, games, documents and other computer programs across global networks. However, accessing these sites is considered a high-risk activity since peer-to-peer sites are commonly used by criminals to distribute objectionable or illegal files and viruses that are disguised to look like innocent downloads of popular songs, movies, etc.

6. Be wary of downloading free apps, files, programs, software or screensavers

Malicious code, like ransomware (that locks you out of your devices and files), spyware (that secretly monitors what you do online) and keystroke loggers (that secretly track what you are typing) can be hidden in the downloaded file or app and used to access personal information, such as passwords and financial information.

7. Limit sharing of sensitive personal information online

Cyber criminals only need a small amount of your personal information to impersonate you online and commit financial crimes. Be careful what personal data you share online. Don’t provide your birthdate, PIN or any personal or financial information unless you have initiated the contact or know with whom you’re dealing.

8. Strengthen social media security and privacy settings

Review the privacy and security settings available for all your social media accounts and tighten the default controls. Limit who can access your social media accounts and remember what you post online lives forever.

And be sure to only accept requests from individuals you know and review your contacts regularly to ensure all your contacts are relevant.

Your Cyber Hygiene Checklist

□ Protect your devices

□ Install software updates and patches

□ Create unique, strong passphrases and passwords

□ Schedule regular back-ups of your data

□ Disable file sharing networks

□ Be wary of downloading free apps, files, programs, software or screensavers

□ Limit sharing of sensitive personal information online

□ Strengthen social media security and privacy settings

Spotting Common Scams

There are several common scams you should be aware of including:

- Email Fraud or Phishing Scams
- Phone or Voicemail Scams
- The SIM Swapping Scam
- Online Gaming Scams
- Identifying Fake Websites and Applications

Many scams are variations on a set of tactics cyber criminals use to attempt to trick you into revealing sensitive personal information.

SOCIAL ENGINEERING: understanding how cyber criminals might try to trick you

Social engineering is the process criminals use to exploit our basic human urge to respond to urgent requests, be useful or help out a friend in need, to lure us into providing information that can be used to commit financial fraud. Social engineering tactics lure us into clicking on malicious links and attachments or into providing sensitive information that can be used to launch cyber crimes or commit financial fraud.

When it comes to cyber security, even the strongest information security systems are vulnerable when the people accessing those systems are tricked into giving away their login credentials and other personal information.

Rather than using technical hacking techniques to conduct a cyber attack, social engineers use manipulation and human psychology to spin a story that they hope we'll believe.

3 ways to spot social engineering techniques

01 Using fear as a motivator. Sending threatening or intimidating emails, phone calls and texts are techniques social engineers will use to scare you into acting on their demands for personal information or money.

02 Suspicious emails or texts that include urgent requests for personal information are major red flags that someone is trying to trick you.

03 Too-good-to-be-true offers or unusual requests. If an online contact offers you free access to an app, game or program in exchange for login credentials or personal information, beware. Similarly, free online offers and links can often contain malicious code.

Protecting Against Phishing Scams

Phishing scams are as old as email itself. It's no longer true that spelling and grammatical mistakes in an email are a common sign of a phishing scam. The increasingly sophisticated nature of these scams means that you need to be on your guard.

Here are a few red flags that the email that just landed in your inbox is a phishing scam:

Demands and threats

Is the request for information from a legitimate source? Your bank will never send you a threatening email, or call you on the phone, demanding information like your password, credit or debit card number, or your mother's maiden name.

Suspicious senders

Check the "from" address. If you hover your curser over the sender's name, you can see the actual email address. Some phishing attempts use a sender email address that looks legitimate but isn't – one red flag is when the email domain doesn't match the organization that the sender says they are from.

Suspicious links or attachments

Always be wary of links or attachments that you weren't expecting. Scam emails often include embedded links that may look valid, but once you hover over them, the real link will be visible.

Warnings

Warnings that your account will be closed or your access limited if you don't reply are telltale signs of a phishing scam.

Protecting Against Phone Scams

Phone scams, also called "vishing" and text scams, also called "smishing," can take several forms, but these scams have a few tactics in common.

How the scam works

You receive a call or a voicemail from a criminal who is posing as a government agency or member of law enforcement. The message says you have an overdue balance or outstanding debt or that there is a warrant out for your arrest. In a variation of the scam, sometimes the criminal poses as a bank employee asking you to assist them with an investigation into fraudulent activity on your bank or credit card account.

The calls, voicemails, and texts sound authentic, but there are often red flags that the communication is a scam:

Very often these calls, texts or voice messages use threatening and aggressive language to frighten and bully you into paying the phony debt or providing your login credentials. Or the message might claim that you've won a prize or have qualified for a special deal.

The calls or messages include warnings that they'll contact police if you don't reply.

The caller demands that you pay your outstanding debt in gift cards, bitcoin or by wire transfer.

How to protect yourself

Banks take extensive steps to protect the personal information you entrust to them and to help you protect it as well. Banks and government agencies will never request gift cards or prepaid cards in payment of a debt or bill.

If you receive a call from a scammer, hang up or delete the voicemail message.

You can also block the caller's phone number and report the calls to the Canadian Anti-Fraud Centre.

Understanding the SIM Swapping Scam

You might know that a subscriber identity module (SIM) card is the small, removable card inside your mobile device that identifies you and gives you access to your mobile provider's network. But did you also know that criminals can now swap your SIM card through their cellphone provider, gain access to your phone, and steal information they could use to access your bank accounts?

SIM swapping is a relatively new type of fraud targeting your personal information so that criminals can impersonate you and access your bank accounts. Most victims won't know they've been compromised until they try to place a call or send a text message which doesn't go through.

How the SIM swapping scam works

SIM fraudsters start by trying to find information about you like your name and phone number. Then try to trick you into providing this information by sending you a phishing email or by searching your name and your phone number if you've published it on social media sites.

Once they have enough personal information, they call your cellphone provider or use the online chat option pretending to be you and request a new SIM card in your name.

Once they have gained the new SIM card connected to your phone number, they'll have access to all services you've linked to your phone: bank accounts, emails, pictures, phone calls, text messages, etc.

How to protect yourself

- Set up a passcode/PIN with your service provider to access your phone for any online or phone interactions. Do not use the same PIN as you use for other accounts, like your bank account.

- Don't publish your phone number on any of your social media profiles. Limit the amount of personal information you post online like your birthday, elementary school names, or your pet's name. Fraudsters can use these clues to answer common identification questions and impersonate you.

- Don't use the same passwords or usernames across multiple accounts. Always create a strong, unique passphrase or password for your sensitive accounts. Check out the tips in the next section for the CBA's recommendation on how to choose a strong password.

- Don't click on links or attachments in suspicious emails or text messages. Remember that your bank will never send you an email, or call you on the phone, asking you to disclose personal information such as your password, credit or debit card number, or your mother's maiden name.

Avoiding Online Gaming Scams

Cybercriminals are taking advantage of the popularity of online sites, apps and games to create convincing scams that are hard for adults and kids to recognize and avoid. There are several best practices that you can adopt and, as a parent or guardian, use with your children to avoid online gaming frauds and scams:

Never use Personally Identifiable Information (PII) in an account profile

Real names, addresses and phone numbers should never be used to set up a gaming profile. Information in a profile may be publicly available so use fictional names or skip the profile-building process completely if possible.

Beware of fake websites and mobile apps and only make purchases on official gaming platforms

Many games offer in app or in game purchases to enhance the gaming experience. The extreme popularity of online games makes creating game scams very attractive to cyber criminals. Scam websites can look very professional but often contain malicious code or of offers to provide game currency in exchange for personal information. Avoid all offers for "free" game currency that you might receive on social networks or through in game chats.

Protect account information

Always choose a strong, unique password for your each of your accounts and, if available, enable two factor authentication to help protect your accounts from unauthorized access.

Be wary of suspicious links and do not click on them, even if they look like they're from "friends" in the game

Suspicious links that are on websites or sent by text, through in game chats and by email can download malicious software on your devices and steal your login details and passwords, which can allow a cyber criminal to access your personal information and gaming assets and put them up for sale.

Resources

The Canadian government's Get Cyber Safe websites lists a number of resources to help parents keep their kids safe online.

The Office of the Privacy Commissioner of Canada's graphic novel, Social Smarts: Privacy, the Internet and You, can help older kids better understand and navigate privacy issues.

For Parents and Guardians:

Use parental controls for devices, websites and gaming platforms that your child accesses

Many devices, websites, gaming platforms and Internet service providers provide tools to help you protect kids online. Take advantage of the protection features available to help you manage your children's online access, including which kinds of websites they access, who can contact them and how they can make purchases.

Explain that account information is private

Explain to your kids that they should never share account information with anyone except you, not even with their friends. Your child's account may contain sensitive personal information, including your credit card account information. Game companies would also never ask for sensitive personal information like bank account numbers and passwords or social insurance numbers. Demands for any kind of personal information is a key warning sign of a scam.

How to Spot Fake Websites and Apps

Scammers create online shopping websites and apps that have a similar look and feel to genuine retailers under an intentionally misleading, legitimate-sounding name.

These websites and apps are more often than not just a front to steal your credit card details and sensitive personal information.

Here are a few clues to help you identify a fake online shopping site.

Signs of a fake shopping website:

- the site looks poorly designed, unprofessional and has broken links,
- you can't find an address or phone number for the business,
- sales, return and privacy policies are hard to find or unclear,
- the back button is disabled - you get stuck on a page and can't go back,
- you're asked for credit card information anytime other than when you are making a purchase.

Major app store platforms like Apple's App Store and Google's Play Store monitor content and routinely remove malicious apps. But you still need to be vigilant about the apps you download.

Signs of a phony app:

- the name of the app publisher (typically displayed under the app's name) is close to the retail app you're looking for but isn't quite right,
- the app has a poorly written description or doesn't have any user feedback,
- the app requires an excessive number of permissions for installation,
- the app has a lot of pop up ads or you are constantly being asked to enter personal information.

Protect yourself while shopping online

- Shop with reputable and trustworthy retailers that provide a street address and a working phone number.
- When looking for the shopping app of your favorite retailer, visit the retailer's website and look for the link to their legitimate app there – don't just search through the app store.
- Look at the URL of the website to see if it starts with "https" and displays a tiny padlock icon in the address bar. If it begins with "https" instead of "http" it means the site is secured using an SSL Certificate (the s stands for secure).
- Never respond to pop-up messages on a website or app that asks for your financial information.
- Use your credit card and avoid websites and apps that request payment by wire transfer, prepaid debit or gift cards, cash only or through third parties.

Protecting Against Ransomware

Ransomware is a type of malware, or malicious software.

Once the malware is on your computer, it can lie dormant until the hacker takes control and encrypts your files. When files are encrypted, it is very much like the files are locked, and scammers will demand a ransom payment to decrypt and unlock the files. Keep in mind that even if you pay the ransom, there are no guarantees that they will unencrypt your files or that they won't sell or leak the information online.

How you can avoid downloading ransomware

Install reputable, up-to-date anti-virus and anti-malware protection software on all your devices and keep on top of updates.

Take the time to install the latest version of your operating system and applications.

Backup your files frequently to an external source, such as an external drive or cloud-based storage, that is not linked to your computer. If they are linked, your backed-up data could be encrypted too.

Be careful to not click on links or open attachments from unknown addresses and disable macros in documents – you could unknowingly download malware by enabling a macro, clicking on an email attachment, link or online pop-up window.

What to do if you are a victim

It can be very difficult to decrypt your files and remove the ransomware from your computer. If you are the victim of ransomware, you can consider the following:

Check with your anti-virus provider
If you are familiar with data recovery, you may try to remove the malware yourself. Some anti-virus providers can detect this malware and may have instructions and software to help.

Consult an IT security specialist
A professional may be able to help you remove the ransomware and restore your files if you have them backed up.

Change your passwords
Change your online passwords, particularly for your bank accounts. That will stop the criminals from accessing your accounts if they were able to access your passwords.

Report the scam
Alert your local police and the Canadian Anti-Fraud Centre.

Tips on choosing strong passwords for your online accounts

CANADIAN BANKERS ASSOCIATION

Choosing strong unique passwords for your sensitive online accounts like your main email account and your financial accounts is important since a security breach at one site means your password could be handed to criminals who may try to use it at other sites.

Why are unique passwords so important?

These bad actors then use a technique called credential stuffing. They use automated tools, such as account checker apps, to "stuff" your credentials into as many login pages, such as your bank account, as possible until a match is found. If you're using the same username and password for many different websites, it's more likely that fraudsters will be successful in accessing your accounts.

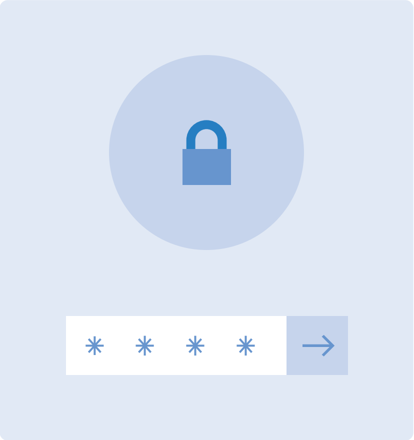
Your financial institution will have its own specific requirements for secure passwords, but here's an easy way to choose a unique password that's hard to crack and easy to memorize.

Use a passphrase instead of a password

Using a passphrase that you associate with that website makes it easier to remember. For example, if you're logging into a photo sharing site, the phrase could relate to images of your friends and family:

Phrase:
absence makes the heart grow fonder

And you can turn that phrase into a complex password to meet the security requirement to use letters and numbers and special characters as follows:



Step 1: Determine phrase:

absence makes the heart grow fonder

Step 2: Take the first letters of the words in the phrase:

amthgf

Step 3: Add uppercase letters:

AmthgF

Step 4: Expand words, substitute and/or add numbers and special characters and ensure that your password is at least eight characters in length.

Amth3G+F1!

Take additional steps to protect yourself

Strong and unique passwords are the first step in keeping your sensitive personal information protected. Also consider taking advantage of multi-factor authentication for your online accounts when available and keep your computer and device software up-to-date by installing the latest operating systems and security updates.

Working From Home Safely

When working from home, it's important to protect against security weaknesses you might have in your home office set up.

Here are some simple tips to ensure you are maintaining good security protocols at home, even if your home office consists of a laptop and your couch.

Be sure to regularly refer to your company's internal portals or communications for guidance regarding the latest threats, as well as company safeguards, practices and processes to keep your work devices safe.

Protect your devices

If you are working from your personal computer and mobile phone, make sure you take precautions to protect your devices:

- If you can, try to work only using the devices assigned by your employer. You will benefit from the security measures they have in place to protect you and the privacy of your work-related information.
- Protect your devices and various accounts with strong and unique passwords.
- Protect your software. Install anti virus and anti spyware software on all your connected devices and keep them up to date. And don't delay on software updates and patches - install software updates as soon as they are available so you're protected against the latest threats. Even better – automate the updates so they're installed regularly.

Tip: Keep Support Within Reach

Keep a sticky note of your company's help desk phone number close by so you can easily contact them to get help or report incidents – even if all your work devices are compromised.

Working From Home Safely
Continued

Protect your privacy and the privacy of others

It's important to separate work from home to protect your privacy, adhere to the privacy guidelines of your employer and protect the privacy of the members of your household.

- Separate work from home. Don't save work related documents or data on your personal devices and don't let other members of your household use your work devices.
- Only print what you must and securely shred all documents with personal information about you, your clients or your employer.
- Back up your personal files frequently to an external, secure source. Test your backups to ensure they worked properly and to make sure you know how to restore your backed up files. Have a schedule in place to ensure those backups are happening regularly – very often you can schedule them to happen automatically.

Secure your home Wi-Fi

Scammers know that many people are now working from home and will take advantage of this.

- Change the default name and password for your home router to something strong and hard to guess. And be sure to auto-install any updates and patches for your router to protect against threats.
- Set-up a guest network for visitors.

Resources

Find more tips at
https://cba.ca/staying-safe-while-working-from-home

Protect your devices

Secure your Wi-Fi

Separate work and home

Additional Resources

Canadian Bankers Association
Fraud Prevention website:
www.cba.ca/fraud

Canadian Bankers Association
Free fraud prevention newsletter.
Subscribe online.

Government of Canada
Get Cyber Safe website
www.getcybersafe.gc.ca

Financial Consumer Agency of Canada
www.canada.ca/en/services/finance/fraud.html

Your bank is also a great resource for cyber security tips and information. Check with your financial institution to learn about the security services, guides and advice they have available to you as a bank customer.

CANADIAN BANKERS ASSOCIATION

The Canadian Bankers Association is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. www.cba.ca

GETCYBERSAFE.CA

Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. The campaign is led by the Communications Security Establishment, with advice and guidance from its Canadian Centre for Cyber Security, on behalf of the Government of Canada. Getcybersafe.ca