Tips for Protecting Privacy Online

Consumer Reports Magazine

https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now/

When signing up for services, like an app or social media, we are willing to give up personal information and agreeing to terms of use without understanding the consequences.

“If you not paying for the product, then you are the product” Is this true? Facebook is particularly adept at building user profiles.

Check Your Data Breach Status Go to **Haveibeenpwned.com**, submit your email address or username against lists from 120 known breaches at companies like Adobe, LinkedIn and Snapchat.

Haveibeenpwned.com You will need to register to check the full data base. If your name pops up, change your password.

WiFi Imposters

Laptops, smartphones, and laptops can automatically connect.It is convenient but risky.

Why an issue? A hacker can set up a rogue WiFI with same name or similar one as the legitimate one. It can trick your gadgets into joining.

Solution: Once in awhile, it is good to prune all or some of the networks you join.

Using 10-Minute Mail

You are often asked for a functioning email address when accessing a website or sign up for a loyalty card..

Solution: Go to **10minutemail.com** You get a functional email address for about 10 minutes. When time is up, the email self destructs.

See Who Shared Your Private Data

When you need to to use your real email address such as site that you need to log in to repeatedly, how can you know what companies share your data? **If you have a gmail account: Type”+” before the @ symbol and add the websites name.**

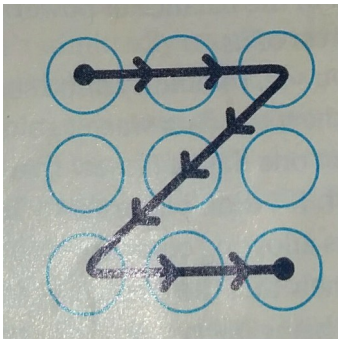
YourName+Websitename.com@gmail.com e.g,brom.churchill+microsoft.com@gmail.com

Email addressed to YourName+Websitename.com@gmail.com will go to your regular inbox YourName@gmail.com. But now it will carry an extra crumb of data, and if you get spam from a company you've never heard of, you'll know who to blame.

Screen-Lock PIN. Go Long Using a six digit lock pin is much more secure than a 4 digit one.
4 digits 10x10x10x10 =10000

6 digits much harder to break. 10x10x10x10 x10x10 =1000000

Finger Locks
77% started in a corner and 1 in 10 formed a letter. Digital pins are more secure.



Shred These 5 Documents
Social Insurance Number (SIN) Credit Card Numbers Financial Account Numbers Birth Date
Medical Insurance Numbers

Shut off the Flow of Credit Card Offers

Unsolicited mailings can be intercepted and filled out by identity thieves who can have credit cards sent to their own address. Debt can pile up in your name.

Your full name Your address Your social security number Your complete bank account number (if you have direct deposit Your employer and its address Your rate of pay

Credit Card Fraud
Phone the company to stop offers.or phone credit report companies to freeze accounts.

Equifax (free 30 day trial) **Transunion**

Does **Credit Karma** work? Is it reputable?

In order to receive a report, you have to send in photocopies of two pieces of identification, along with some basic background information. The reports will come back in two to three weeks. Free if mailed

in. If you sign up for the 30 day trial period, make sure to cancel within 30days or they will continue to debit your credit card each month for $16.95.

Receive Less Mail **CMA Do Not Mail Service** (Canadian Marketing Association) is a private association funded by members and is free to use..Similar to the National **Do Not Call List** operated by the Canadian Government Go to **https://cornerstonewebmedia.com/cma/submit.asp** to remove your info from many mailing lists.

Password Strategies

About 20% of those currently in use are:

0000, 1111, 1212, 1234 Avoid birth dates, phone number, Social Insurance Number

Good Password Policies

8 or more characters, Combination of letters,numbers,symbols A good site has a meter showing password strength, Locking out account after several attempts, 2 factor identification, Different password for each account

Worst Offenders Netflix, Pandora, Spotify, Uber, Pinterest, Instagram, Dropbox, Evernote, Walmart

WASHINGTON

Netflix subscribers target of email scam

An email scam targeting Netflix users aims to gather personal information from the streaming service's 110 million subscribers. The suspicious emails tell recipients that their Netflix billing information needs updating and takes them to a fake Netflix website where they are asked to log in and enter information including credit card numbers. On its website, Netflix says that it may email users asking them to come to website to update information. "If you're unsure about a link in an email, you can always hover your cursor over the link to see where it directs in which you can see the real linked web address at the bottom of most browsers," the company says.

Common Passwords

Equifax,,a credit reporting company was hacked in September. Nearly half the US population had sensitive information stolen. Data breach was announced 5 months after the hack took place. Not clear as yet how many accounts in Canada were breached.

Nearly 60 percent of Canadian businesses surveyed suspect or know for certain they were hacked.I(psos poll taken last Feb.)

Yahoo was the most blatant example of hacking (3 billion accounts)

Make up complicated, non sensicle passwords with letters, numbers, special characters or

pick 5 long, random words and string them together into a nonsense sentence you can remember. or lengthy password phrases that are easy to remember. At least 64 characters.

PasswordManagers Password managers such as **LastPass, 1Password and Dashlane** can generate a complex, unique password for each account. **Lastpass and 1Password** most common ones and easy to use. Drawbacks. Still need a good password for your password account. **Lastpass** was hacked last year but users passwords apparently remained safe .

Write Down Passwords Writing down vital passwords and storing in a secure location a good idea. Keep in a sealed envelope that is to be opened if one is incapacitated.

Be Password Loyal

Change password periodically - only when account is compromised. Not always necessary to change a password unless there is a data breach but how do you know that this is occurring.If you switch often, you may end up with a weak password or something that is hard to remember each time.

Identity Theft After Death
Make sure death certificate is sent to Revenue Canada and cancel drivers licence,credit cards financial accounts and insurance.

Two Factor Identification It gives you an added level of security if someone steals your password. An added piece of information (usually a set of numbers sent by text to your phone)
Go to **twofactorauth.org** for a list of sites that offer 2FA

Scanning Files using Google Drive Suspicious documents? Save it to Google Drive and open it there. If malware present, it will be isolated in a virtual environment.

Google will scan files for viruses. Not as good as your antivirus protection but adds an extra layer of protection.

Smart TV Smart TVs can transmit data to analytic companies that may use it through ACR (Automatic Content Systems) Turn **off** Live PLus or SynPlus which allows ACR to operate.Keeping these on simply allows the TV to transmit your info to marketing companies.

Webcam Creeps Malicious actors can turn on a laptop's camera without your knowledge.
Best solution.Put a piece of tape or Post-it note over it.

Firewall for Public Connections Make sure this is **on** for public connections.
Settings - Network & Internet - Status - scoll down to windows firewall

Network Discovery Turning **Network Discovery** off makes it more difficult for other devices on the network to find your laptop.
In windows, go **WiFi** and then scroll to **Change Advance Sharing Options** and select to turn **off Network Discovery** **If it is on, you can see other networks(good). But it can also allow other computers to see you (bad).** Also, turn **off File and Printer Sharing** when on public WiFi.

Fake Information Some companies, such as toymakers ask for personal information to register them. Use fake information whenever possible.

USB Drive Buy one that has a built in security encryption.Lexmark has one along with Apricorn (but a bit pricy)

HTTPS "Https" means your data is encrypted as it travels back and forth between computer and website. The "s"stands for secure Usually more secure and more trustworthy than the more common HTTP.

HTTPS site require a security certificate that illegitimate sites don't bother with. Especially make sure payment page is an "https" page. Look for the green padlock icon to the left of the address bar. You can click on the padlock icon to verify the details of the website(e.g., the type of encryption used.)

Checking for Suspicious Links First, hover over the suspicious link. Full address will appear in bottom corner of your browser. Right click to access the drop down menu. Select **copy.**
Go to Sucuri Site Check at **sitecheck.sucuri.net**
Paste the URL into the link checker to get a report. Not always foolproof.

You can also check for reviews about a site on google.

Add HTTPS Everywhere Some sites use HTTPS inconsistently where only part of the site is encrypted or may switch to another unsupported HTTP site.

Solution: Add the HTTPS Everywhere extension from the Chrome Store.**www.eff.org/https-everywhere**

If a site or web mail provider does not support HTTP already, HTTPS will not make you more secure.
It will simply activate the security features on the individual website. **Not perfect, but provides an added level of security**
Transparency Report from Google https://www.google.ca/search?q=Transparency+Report+Google&oq=Transparency+Report+Google&aqs=chrome..69i57.14020j0j8&sourceid=chrome&ie=UTF-8

Fake Email Addresses. Call Customer Service
Any email from a bank or social site that asks you to logon should not be clicked.

Open a new browser window and type in the correct address of the company website or alternately, phone the company.

Vishing The term, which blends the word ‘voice’ with ‘phishing,’ refers to a telephone scam to trick people into revealing critical financial or personal information that can be used for identity theft.

Attackers use a technique called caller ID spoofing to make it look like calls are coming from a legitimate or known phone number.There are several companies offering commercial spoofing services, such as SpoofCard.

Directly call the institution named, using a number that is known to be valid. Never give out personal information. Review recent activity to detect tampering.
Don't trust caller ID. Ask questions. Ask them to identify who they work for, and then check them out to see if they are legitimate As, in an email scam, directly call the institution named, using a number that is known to be valid. Never give out personal information.
Review recent activity to detect tampering.
Report incidents to fraud bureau if suspicious.

Checking Phone Number
yp.ca, for example L1-647-694-0203 for reverse lookup

Good for checking local calls

Encrypting Computer Files For windows, download GPG4win (Gnu Privacy Guard)
What is Gpg4win?
Gpg4win enables users to securely transport emails and files with the help of encryption and digital signatures. Encryption protects the contents against an unwanted party reading it. Digital signatures make sure that it was not modified and comes from a specific sender.

Holiday Scams **Shipping Confirmation Ploy**

Canada Post phone call informs you a package is waiting for you and you need to confirm its you by submitting personal information

Fake Retail Site or Classified Ad Come-On A super low price for something you really want. Address and phone number not usually provided. Goods may never arrive or of inferior value or counterfeit.

CBC Marketplace check this site to examine a marketing ploy.

http://www.cbc.ca/news/business/marketplace-skin-cream-trials-1.4349777
Some may have a return policy but in very fine print hidden away.

Summary

Staying Safe Online
Update Everything
Strengthen Passwords
2 Step Verification if possible

Avoid shopping & banking on Public WiFi

CCTS

www.ccts-cprst.ca/abductor/ CCTS is an independent organization dedicated to resolving customer complaints about telecommunications and TV services.

Future Topics

Home WiFi Privacy Simple distinction between a modem and router:

A modem connected to your Internet Service provider and to a Mac or PC is what makes it possible for you to go online.A router connected to your modem is what allows you to share your Internet connection with others in your home, with built-in security against hackers.

Use of a VPN

Turn on your company's VPN, even for personal use. Use a private service such as IVPN, NordVPN or VPN (free) used by Opera Browser