

CYBER SAFETY FOR THE PEOPLE

If your **DATA** hasn't been **LEAKED** yet, it will.
You can **CONTROL** what info is accessible.

What is Cybersecurity?

The World Wide Web

The Internet

WiFi

Cellular

The digital sphere is like the Wild West. There are no guarantee of safety online. Almost everything we do today requires being online. This is how we access information and have information hacked, leaked, exposed, accessed, blocked or deleted.

CYBERSECURITY is how to protect information or communication online. All of your activity is valuable. Sensitive or Personally Identifiable Information is even more valuable. Don't leave your valuables visible or in the car. Don't leave your sensitive **PPI** either!

Term Definitions

USER

The consumer using the product

COMPANY

Who made the product

BAD ACTOR

Any person or company with negative intentions to access your information

PPI

Personally Identifiable Information: Full name, birth date, social security #, Face ID scan

DATA BROKER

A company that collects or purchases user data to sell to other companies.

ALGORITHM

A set of rules a computer follows for a specific outcome.

AI

Artificial Intelligence. Can reproduce simple tasks & collect lots of data.

SPYWARE

Malicious software that collects your information.

RANDOMWARE

Malicious software that blocks access to your data in exchange for money.

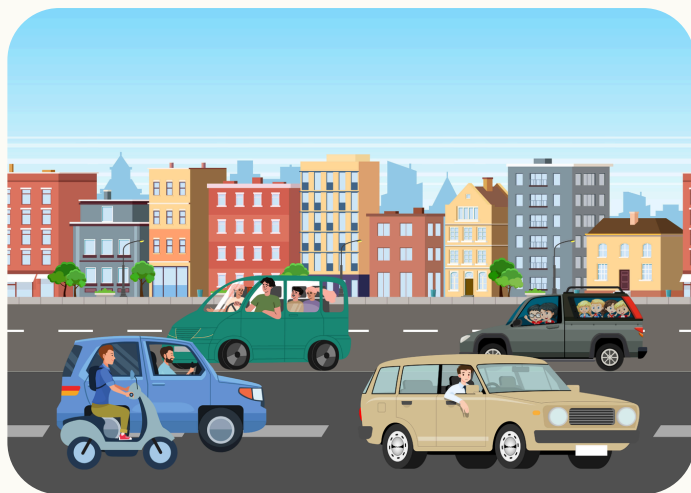
DARK WEB

Websites that don't appear in search engines often for illegal activity.

COOKIES

Information about your online activity, websites, shopping carts, log in credentials.

Personal cybersecurity is similar to defensive driving.
Be alert. Be aware.
Always wear your seat belt!



DEFAULT device and application settings leave you exposed.
Good **PRIVACY** practices keep you safe.

Default Settings

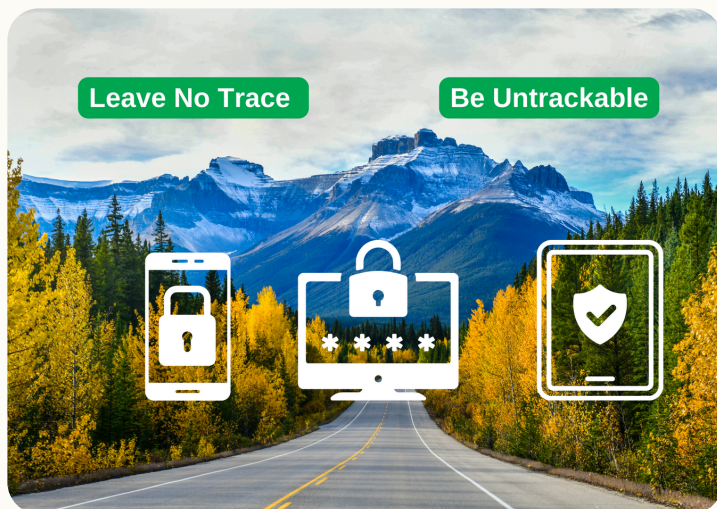


Privacy Settings



Leave No Trace

Be Untrackable



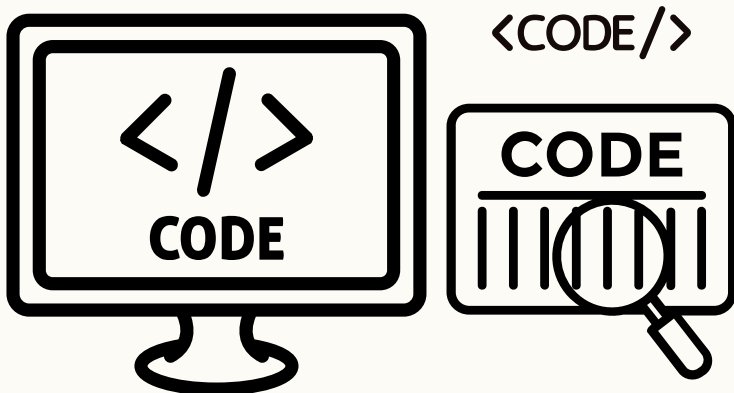
Like visiting a National Park, leave no trace, leave no tracks, don't bring anything back home with you.

Keep your information **SAFE** with a few simple tips and tricks. Unfortunately it's a matter of **WHEN** not *IF* your data gets leaked. Identifying **SECURE** privacy focused applications, use of security apps and daily practices of **DIGITAL HYGIENE** protects your identify online.

DIGITAL PRIVACY BASICS

OPEN SOURCE

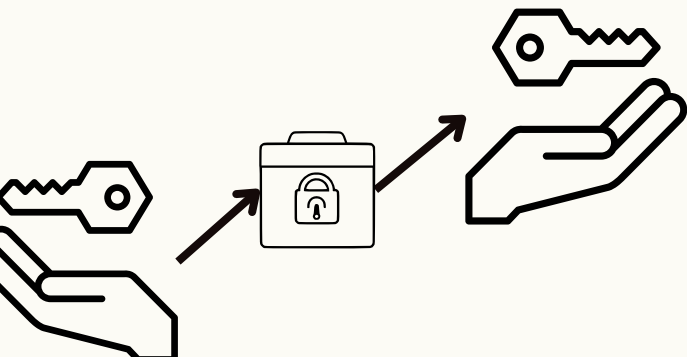
Open Source is a program or application where the code used to create it is available online for anyone to inspect. This transparency allows users to identify any issues. Like the blueprint for a building.



PROXY

In technology proxy often means a 'proxy server' which acts as an authorized intermediary between digital communications. This can be for sending emails, logging on or just connecting to the Internet. Instead of you the connecting end sees the PROXY

END-TO-END ENCRYPTION



E2EE is when information transferred online is **ENCRYPTED** (scrambled and hidden) so only the sender and receiver can access it. Some companies use encryption where a third party can't see or intercept your information, but company employees can. End-to-End Encryption means **ONLY** sender and receiver can see the information, the company has zero access.

Personal

Find the important parts of your life and create separate online space for each. PPI websites (taxes, payroll), friends and family should communicate with you through separate platforms than the other parts of your digital life.

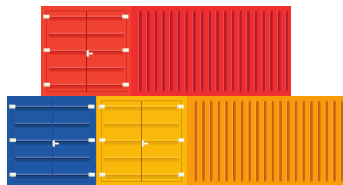
COMPARTMENTALIZATION

Professional

Business emails are the most commonly hacked. Keeping your work, academic and other professional information separate keeps other areas of your life being affected by a business hack/leak.

Public

Emails and user names for subscriptions and areas you find less important. Streaming platforms, news subscriptions and other non essential websites.



DATA LEAK

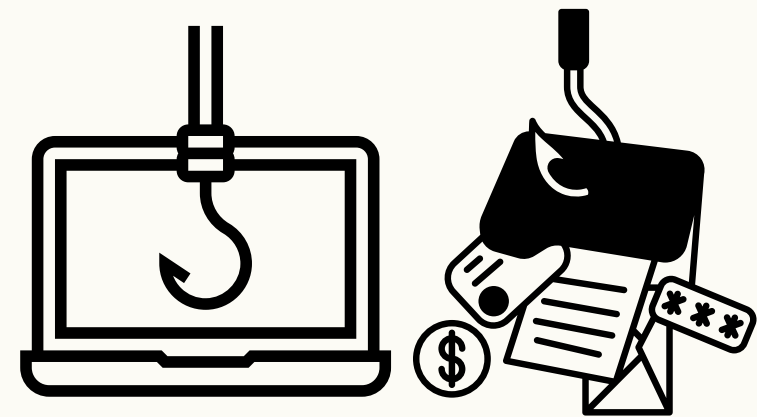
This can happen in any number of ways. Your information can be anywhere online. Most commonly this happens through a company that is hacked. Signed up for a news letter from that company at any point? Congrats! Any info they had on you is now leaked.

PHISHING

This is a common trick. Fake emails that look legitimate, spam emails with malicious spyware or anything that requires you to "take the bait." These require you to click, download or enter your information. You give away your information unknowingly.

AI CLONING

Advanced software can copy an image, voice and even live video of an individual. These AI cloning scans tend to involve urgent requests for large sums of money.



DAILY DIGITAL HYGIENE

- Always use a **VPN**
- Turn off **BLUETOOTH** when not in use
- Use **MFA** for most important accounts
- Create **STRONG** passwords
- Use a **SECURE** password manager
- TURN OFF** your phone once a day

PRIVACY FOCUSED BROWSER

Default browsers that come with digital devices have settings that favor the company. This means all your information is easy to see and automatically tracked. With a SECURE browser your information is not saved and trackers are blocked.



DuckDuckGo



Brave



LibreWolf

BEFORE YOU DOWNLOAD / SIGN UP

Check the **PRIVACY POLICY**

Make Sure They **DON'T SELL** Your Data

Check For **E2EE** For Any Communication

AFTER YOU DOWNLOAD / SIGN UP

Turn **OFF** Location Data

Ensure Tracking Is Off

BLOCK Cookies

PROXY
PLATFORM

MySudo is privacy focused but not secure. Create proxy emails, phone numbers and credit cards.

SECURE + PRIVATE EMAIL
PLATFORMS

Companies that use end-to-end encryption, are open source with secure communicator transfers. Create alias emails. Connect to secure calendars.



Proton Mail



Tutanota®



StartMail

PASSWORD MANAGER

These password managers can connect to browsers and used on multiple devices. Safely store strong passwords. Only remember one.



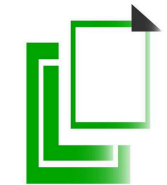
bitwarden



1Password

SECURE CLOUD &
DOCUMENT STORAGE

Open Source. End-to-end Encryption. Privacy Focused. Create & Collaborate. Compatible with Microsoft & Google



LibreOffice



ONLYOFFICE

SECURE TEXT / CALLS

Open Source. End-to-end Encryption. Privacy Focused. Create & Collaborate. Compatible with Microsoft & Google



Signal



Threema.

MFA



DUO

Trusted MFA



YUBICO

Physical Security Key



FREEOTP

Open Source

Privacy focused MFAs with different specialities. RFID. Physical. Open Source.

VPN



NordVPN®



Surfshark



BRAVE

These VPNs are privacy focused and don't sell your data.

Make sure your MFA and Password Manager are two separate apps.