How to Protect Yourself from Identity Theft Online

Online cases of identity theft have run rampant over the years as more people increase their digital presence. Nearly everyone is using digital interfaces – not just for entertainment and social media, but for accessing financial and healthcare services.

Here's an honest admission of facts: if you don't carefully manage your digital presence, including your privacy and cybersecurity, you leave yourself vulnerable to identity theft. It's more common than you think: in 2021, there were 27,531 reported cases of identity fraud in Canada.

Most people lack knowledge on how to protect critical information whilst using online services. The more information you leak, the more severe your risk of identity theft. There are the most common forms of identity theft that you could fall victim to:

- Account takeover
- Credit identity theft
- Synthetic identity theft
- Medical identity theft
- Taxpayer identity theft

As you can imagine, there are multiple gateways for cybercriminals to breach into and access your information. Here are some of the most common ways:

- Spying on your screens
- Phishing attacks
- Man in the Middle attacks
- Accessing your mail and reading the contents of physical letters addressed to you

Information that You Should Protect at all Times

There are certain pieces of information that you should never leave unprotected or share with anyone unless absolutely necessary. These include:

01 Social Insurance number (SIN)

02 Business Number (BN)

03 Insurance policy number

04 Bank account number

05 Credit and debit card number

06 Driver's license number

07 Employer identification number

Steps You Can Take to Prevent Identity Theft Online

While there is no ironclad solution to prevent identity theft online, you can take steps to minimize the risk. Here is a roundup of steps you can take to protect your data and identity.

Only Conduct Transactions on Secure Platforms

Before buying any product or service, make sure that the online platform provides a safe and secure environment for conducting financial transactions.

As a rule, do not buy from a site that doesn't have a secure socket layer (SSL) encryption. Websites with SSL encryption have their addresses starting with the URL "HTTPS://" instead of "HTTP://". In addition, secure websites have a padlock next to their address. The padlock indicates that the website has SSL encryption enabled.

Your browser may also block connections to unsecure websites. It is good practice to read the vendor's privacy policy to see how they store your personal information. We recommend using only one credit card for online purchases.

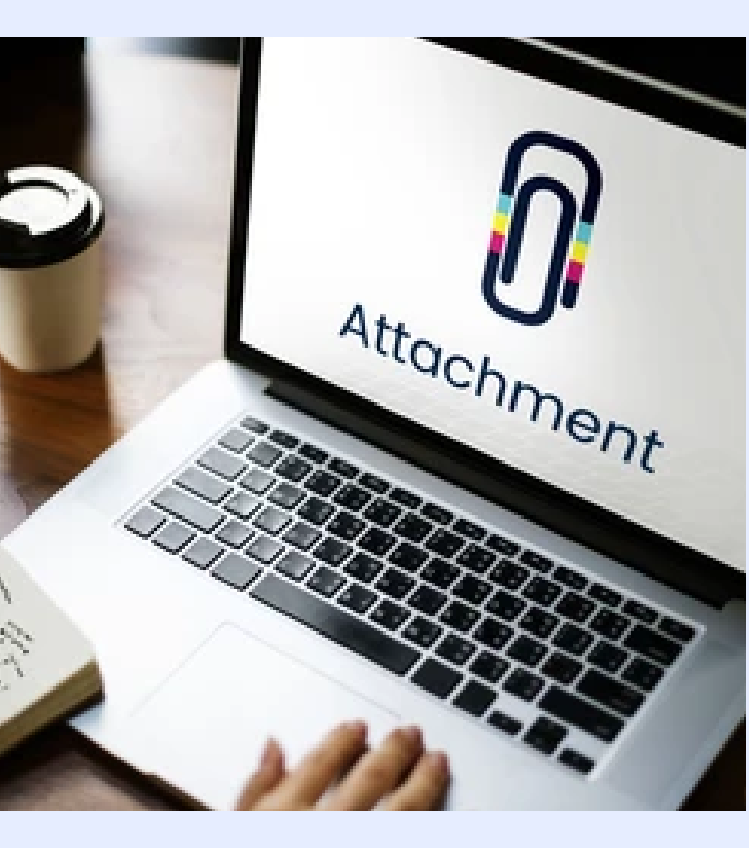
And always read your credit card statements to see if you have been charged for fraudulent or unknown charges.

Pro tip: Want to buy a product but don't trust the vendor? You can purchase a virtual credit card to protect your real financial information. You can use the virtual credit card to run trial versions of the product without giving up your banking information. This will also protect you from unauthorized charges to the credit card.

Email Attachments

Never send sensitive information via email. This is because once the email is sent, its protection is no longer under your control and may be intercepted by cybercriminals.

It also goes without saying that you should never click on email links that originate from untrustworthy sources. Only accept email attachments if:



- They originate from an address you trust
- They originate from someone you already know
- You are expecting them
- They are cleared by your antivirus program
- Do not contain unusual spelling errors or characters

Try not to sign into your email accounts from an untrustworthy computer because there is a risk of someone intercepting your data. Change your passwords if you have used your email accounts on another computer or network.

Use Stronger Passwords and 2FA

Make a habit of using different passwords for different accounts. The password should be strong with at least 12 characters and combine special symbols including lowercase and uppercase letters, numbers, and punctuation.

The password should be extremely random and unique. Simple passwords are prone to dictionary attacks and can be easily broken into with the help of brute force attacks.

Never use your birth date, name, or street address in your password. Longer passwords take millions of years to crack and are simply not worth the effort.

Besides using strong passwords you should use two-factor authentication (2FA) on all your accounts. 2FA eliminates the risk associated with compromised passwords. If an intruder hacks, guesses, or phishes your password, that's no longer enough to breach your accounts.

Beware of Phishing Attacks

Most online security systems are nearly bullet-proofed and not worth the hassle of breaking into. This is why cybercriminals resort to social engineering tactics such as phishing attacks to get the information directly from the victim.

Examples of these may include phishing emails that seemingly originate from your employer, you might get a call from a so-called tech support expert from Microsoft, or someone claiming to be from the CRA.

They may come up with a terrifying story about you being in trouble unless you provide them with specific information. Ignore such emails and callers and take steps to block them.

Lock Your Phone

Smartphones are playing a central role in our lives and have almost completely replaced desktop PCs. The average smartphone contains a treasure trove of data about its owner - data that makes online identity theft a walk in the park for cybercriminals.

Despite the risks, some people don't lock their phones. A simple four-digit PIN is no longer sufficient to lock your phone. Your best bet is to use fingerprinting and biometric authentication, backed by strong passcodes that use various characters and numbers.

Wrapping Up

Remember the more steps you take to protect your data, the lower your risk of online identity theft. You should also sign up for a reputable cybersecurity service provider for monitoring, detecting, and preventing identity theft online.

For more information, get in touch with our cybersecurity service providers at Microsys Inc and embrace top-down cybersecurity practices.

Get In Touch With Microsys