PROTECTING YOURSELF FROM IDENTITY THEFT ONLINE

JANUARY 2021 ITSAP.00.033

A **digital identity** is information about a person, an organization, or a device that represents that entity uniquely within a domain. When you post or share information about yourself or your organization, you are building and adding to that identity. Your digital identity contributes to your reputation and credibility when engaging with people, products, and services online.

Identity information is a high-value target for cyber threat actors looking to sell this information or use it for fraud. Threat actors can steal identity information using unsophisticated techniques, like mail theft or more sophisticated techniques, like phishing or carrying out attacks on databases or online services. Once a threat actor has sufficient identity attributes, they can create fraudulent identity credentials, or take control of existing credentials.

YOUR DIGITAL IDENTITY

Your **digital identity** includes all the personal identity attributes that are available about you online (e.g. date of birth, social insurance number, medical information, phone number, login credentials).

This data is collected and shared when you interact with your social media accounts, online subscriptions, financial accounts, and other service accounts. Your data is also collected when you use Internet browsers, online databases (e.g. health sector, academia), and cloud services. Your digital identity attributes grow as you interact with more online services and as organizations you connect with in the physical world put more of their data online.

THREATS TO YOUR IDENTITY

Any personal information shared online is at risk of being compromised or stolen. Some main threats to your digital identity include the following examples:

PHISHING

A scammer calls, texts, or emails you, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information.

SOCIAL ENGINEERING

A scammer uses a more personalized phishing attack to target you specifically. Social engineering attacks often include personal details about you or your organization to trick you into sharing further personal details.

DEEPFAKES

A threat actor uses synthetic media (e.g. video, audio, photos) to impersonate you or your organization, as a form of authentication (e.g. biometrics) or misrepresentation, to steal sensitive information or spread misinformation.

THIRD-PARTY DATA BREACHES

Your vendor's network and sensitive data is compromised by threat actors. External networks and information (e.g. client data, credentials) handled by the compromised vendor are at risk. Compromised credentials may be used to access other accounts, further spreading the attack.

AWARENESS SERIES

PROTECT YOUR IDENTITY

To protect your digital identity, you should implement security best practices, such as the following:

USE WI-FI SECURELY

Secure your Wi-Fi network by changing the default network name (SSID) and password that came with your router and account. Avoid using public Wi-Fi networks, especially if sending sensitive information or logging into sensitive accounts. If you must use a public Wi-Fi network, use a virtual private network (VPN) to protect sensitive information.

USE SECURITY TOOLS AND SOFTWARE

Install a firewall to filter and block malicious traffic, protecting your network from external threats. Install anti-virus software to scan your devices for malware and anti-phishing software to block phishing content. Ensure to update all software and applications regularly.

SECURE YOUR ACCOUNTS

Use strong passwords and passphrases with multi-factor authentication (MFA) to secure all accounts. MFA adds a layer of security by protecting your account if your password is compromised.

Keep personal social media accounts private to restrict those who can see what you share (e.g. reduce the risks of deepfakes). For business social media accounts, remind employees who manage the accounts to be cautious about the information they are posting.

SHARE WISELY

Before signing up for services and accounts, you may want to research who you are sharing data with. Review company privacy policies to find out how third parties handle your personal information.

If you get an unsolicited request, think twice before sharing personal information. Don't click on links included in text or email messages. Verify the identity of the person or company asking for this information and the legitimacy of the request. When in doubt, contact the company (e.g. your bank) by using the contact information posted on the official website.

MANAGE AND MONITOR ACCOUNTS

Review your accounts regularly and monitor financial accounts for suspicious activity. If you no longer use an account (e.g. online shopping account), be sure to remove any personal information and delete the account.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**

ADDRESS IDENTITY THEFT

If your digital identity has been compromised, take immediate action:

1. Report the incident to the account source, as well as other associated or connected accounts (e.g. login through partnered sources).
2. Determine which information could be affected (e.g. financial information, social insurance number).
3. Change passwords and security questions on all accounts that are related to the compromised account (e.g. partnered accounts, emails) or that use the same password.
4. Use Equifax and TransUnion to analyze your credit report and enable alerts to notify you of unauthorized inquiries.
5. Report your incident to the Canadian Anti-Fraud Centre online or at 1-888-495-8501.
6. Notify law enforcement of the incident.
7. Report organizational identity theft activity to the Cyber Centre (**contact@cyber.gc.ca**).

LEARN MORE

Visit the Canadian Centre for Cyber Security website (**cyber.gc.ca**) to learn more about cyber security and our services. You can find our catalogue of publications, including:

- *ITSAP.00.071 How to Shop Online Safely*
- *ITSAP.00.080 How to Use Online Banking Securely*
- *ITSAP.80.101 Virtual Private Networks*
- *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication*
- *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi*