Protecting yourself from identity theft online

CANADIAN CENTRE FOR CYBER SECURITY

May 2024 | ITSAP.00.033

A digital identity is information about a person, or an organization 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.

Personally identifiable information (PII) is a high-value target for cyber threat actors who look to sell this information or use it for fraudulent purposes. Threat actors can steal PII using unsophisticated techniques, like mail theft, or more sophisticated techniques, like phishing or 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, such as your:

- 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, cloud services, and online databases, like health or academic platforms. 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 digital 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 you, sends you a texts, or emails you, or uses social media to trick you into:

- clicking a malicious link
- downloading malware
- sharing sensitive information.

Further reading: Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101), and What is voice phishing (vishing) (ITSAP.00.102).

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.

Further reading: Social engineering (ITSAP.00.166), and Spotting malicious email messages (ITSAP.00.100).

Third-party data breaches

Third part breaches occur when a threat actor compromises your vendor's network and sensitive data. External networks and information, like client data and credentials, handled by the compromised vendor are at risk. Threat actors may use compromised credentials to access other accounts, further spreading the attack.

Further reading: Protecting your data and information when using applications (ITSAP.40.200).

Deepfakes

A threat actor uses synthetic media, like video, audio, and photos, to impersonate you or your organization. They can also use it as a form of authentication or misrepresentation, to steal sensitive information or spread misinformation.

Further reading: Biometrics (ITSAP.00.019), How to identify misinformation, disinformation and malinformation (ITSAP.00.300), and Generative artificial intelligence (AI) (ITSAP.00.014).

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Cat. No. D97-1/00-033-2024E-PDF
ISBN 978-0-660-72034-0

Canada

Protecting yourself from identity theft online

CANADIAN CENTRE FOR CYBER SECURITY
May 2024 | ITSAP.00.033

Protecting your digital identity

To protect your digital identity, you should implement basic cyber security best practices.

Use a secure Wi-Fi network

Secure your Wi-Fi network by changing the default network name, known as the service set identifier, and password that came with your router and service 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 to protect sensitive information.

Use security tools and software

Install a firewall to protect you network from external threats. A firewall filters and blocks malicious traffic. 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) and phishing-resistant 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. This can 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 your personal information 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 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, be sure to remove any personal information and delete the account.

Address identity theft

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

- Report the incident to the account source, as well as other associated or connected accounts
- Determine which information could be affected, such as financial information or social insurance number
- Change passwords and security questions on all accounts that are related to the compromised account, like partnered accounts and login emails, or that use the same password
- Use Equifax and TransUnion to analyze your credit report and enable alerts to notify you of unauthorized inquiries
- Report your incident to the Canadian Anti-Fraud Centre online or by phone at 1-888-495-8501
- Notify law enforcement of the incident
- Contact the Cyber Centre to report organizational identity theft activity

Learn more

- How to shop online safely (ITSAP.00.071)
- How to use online banking securely (ITSAP.00.080)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Protecting your organization while using Wi-Fi(ITSAP.80.009)
- Digital footprint (ITSAP.00.133)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Identity, credential, and access management (ICAM) (ITSAP.30.018)
- Security considerations when using social media in your organization (ITSM.10.066)