DIGITAL FOOTPRINT

JANUARY 2022 **ITSAP.00.133**

Your organization uses the Internet to carry out business activities, provide employees with remote work capabilities, and offer services to clients. As your employees and partners carry out activities on different online platforms and applications, consider the digital footprint they leave behind. Digital footprints contain sensitive information that is valuable to cyber threat actors. Through the use of tracking and monitoring techniques, threat actors can access and exfiltrate this sensitive information, jeopardizing its confidentiality and security.

WHAT IS A DIGITAL FOOTPRINT?

A digital footprint is the trail of data you create while using the Internet. This trail of data comes from the websites you visit, the emails you send, and the information you submit or download online. You build your footprint both actively and passively.

- **Active digital footprint:** Data left through intentional actions, such as posting on social media, filling out online forms, or agreeing to browser cookies.
- **Passive digital footprints:** Data left unintentionally or unknowingly. This data is often collected by monitoring tied to your IP address. Websites and applications may install cookies on devices without disclosure, use location tracking, or log your activities.

Consider who can contribute to your digital footprint and take the appropriate security measures to protect it.

WHAT ARE THE RISKS?

Your organization is responsible for protecting the sensitive information (e.g. client names, financial data, personal identification information) it collects. Cyber threat actors look for vulnerabilities that they can exploit to gain access to sensitive information. Handle sensitive data with the appropriate safeguards to prevent privacy and data breaches.

Be cautious when sharing information about others online. Some people are very concerned about their privacy and their digital footprint.

Keeping your clients' information secure is extremely important for the security of sensitive information and the reputation of your organization. Compromised digital footprints can lead to issues with background checks, identity theft, and reputational harm. Ensure appropriate preventative measures are in place to protect the confidentiality and integrity of your sensitive information.

WHAT ARE THE THREATS?

Threat actors try to exploit vulnerabilities and access sensitive information using techniques that collect data through active and passive footprints.

Phishing attacks or website spoofing are common techniques. By clicking on a link, downloading an attachment, or sharing sensitive information, you are making your digital footprint more accessible to threat actors.

Bring-your-own devices (BYODs), smart devices, and unsecure Wi-Fi networks are vectors that threat actors can use to collect data. With the increase in remote work, sensitive data may be shared through devices and networks that do not have the appropriate security measures in place.

If your business handles online orders through a website, there are further considerations for keeping sensitive data secure. Refer to *ITSAP.40.016 Using Encryption to Keep Your Sensitive Data Secure* on details regarding encryption and secure browsing.

AWARENESS SERIES

Cat. No. D97-1/00-133-2022E-PDF
ISBN 978-0-660-41484-3

HOW DO I PROTECT PRIVACY?

Privacy is important. To reduce the risks of sensitive data being exploited, consider the following measures.

Train your employees and raise awareness. Train all employees to keep them aware of cyber security and privacy topics and issues. Your training should cover proper information handling and protection measures, as well as other cyber security best practices.

Read privacy policies and terms of use. Before downloading an application and using a service, read and understand the types of information being collected, the ways in which it can be used, and the security measures in place to protect personal information.

Disable cookies, if possible. Even if you are not actively sharing information on applications and websites, your data is still traced through your device, IP address, and network.

Configure default settings. Some applications have their default settings open for public access. Configure your privacy and security settings with the highest and most restrictive settings available.

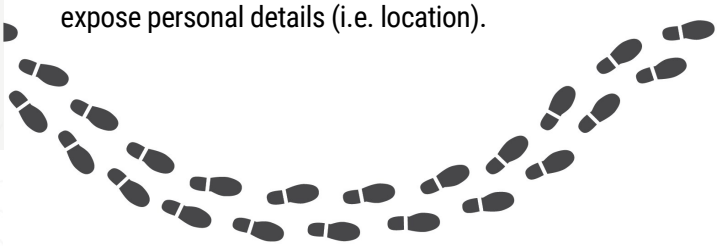
Disable monitored settings. Refrain from using unnecessary applications that require access to locations, calendars, and contact lists. Disable settings that run analytics and monitor your actions for targeted advertising.

Stay up to date with any changes with application's terms of agreements, updates, and privacy settings.

WHAT ELSE SHOULD I CONSIDER?

To secure your actions online from cyber threat actors, consider the following preventative measures:

- Install anti-virus software and a firewall to reduce the risks of data being passively shared.
- Enforce the use of strong and unique passphrases or passwords for all accounts.
- Use mobile device management or mobile application management to monitor BYODs.
- Restrict unencrypted website browsing and install privacy enhancing web browser extensions (e.g. ad-blocker).
- Remove old accounts and any privileges from employees who no longer need access.
- Permit access to only those with a need to know and classify data based on the level of sensitivity.
- Create a social media policy to clarify expectations on what can be shared on organizational accounts.
- Remove metadata from photos before sharing and posting online. This information is stored in the image file and can expose personal details (i.e. location).



LEARN MORE

Visit the Canadian Centre for Cyber Security (CCCS) website (**cyber.gc.ca**) to find our publications, including:

- *ITSAP.00.070 Supply Chain Security for Small and Medium Organizations*
- *ITSAP.00.100 Don't Take the Bait: Recognize and Avoid Phishing Attacks*
- *ITSAP.40.016 Using Encryption to Keep Your Sensitive Data Secure*
- *ITSAP.00.012 Internet of Things for Small and Medium Organizations*
- *ITSAP.70.013 How is Your Smart Device Listening to You?*
- *ITSAP.70.002 Security Considerations for Mobile Device Deployments*
- *ITSAP.10.093 Offer Tailored Cyber Security Training to Your Employees*
- *ITSAP.00.033 Protecting Yourself from Identity Theft Online*
- *ITSAP.10.003 How to Protect Your Organization from Insider Threats*

Visit the CCCS Learning Hub website (**cyber.gc.ca/en/learning-hub**) to explore our training courses, including:

- *Course 110 – Cyber Security in the GC and Online Exposure (1/2 day)*
- *Course 152 – Protecting Digital Privacy (90 minutes)*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**