Digital footprint

February 2024 **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, and take the appropriate security measures to protect it. Digital footprints contain sensitive information that is valuable to threat actors. Through the use of tracking and monitoring techniques, threat actors can access and exfiltrate this sensitive information, jeopardizing its confidentiality and security.

About digital footprints

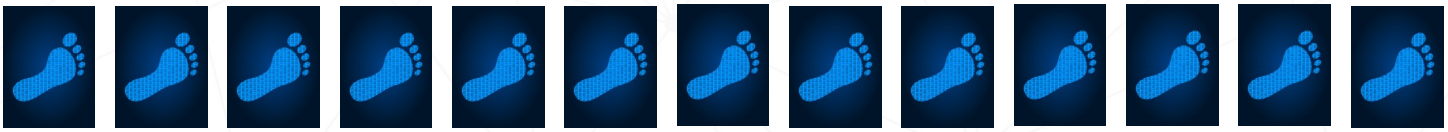
A digital footprint is the trail of data you create while using the Internet. This trail of data comes from the websites you visit, the emails you send and the information you submit or download online. You build your footprint both actively and passively.

- **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 through monitoring tied to your IP address. Websites and applications may install cookies on devices without disclosure, use location tracking or log your activities.

Understand the risks

Your organization is responsible for protecting the sensitive information it collects, like client names, financial data and personal identification information. Threat actors look for vulnerabilities that they can exploit to gain access to sensitive information.

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



Know 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.

Artificial intelligence (AI) algorithms can also pose a threat to your digital footprint. They can analyze your digital footprints to track your behaviour online. This data could be used by a threat actor to steal your identity.

Bring-your-own devices (BYOD), smart devices, and unsecured Wi-Fi networks are vectors that threat actors can use to collect data. With many people now working remotely, 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. For details about encryption and secure browsing, read Using encryption to keep your sensitive data secure (ITSAP.40.016).

AWARENESS SERIES

Cat. No. D97-1/00-133-2024E-PDF
ISBN 978-0-660-69844-1

Protect your privacy

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

Train your employees and raise awareness. Your employees should be 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.

Deactivate 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.

Deactivate monitored settings. Refrain from using unnecessary applications that require access to locations, calendars and contact lists. Deactivate 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.

Other cyber security considerations

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
- implement multi-factor authentication (MFA) and enforce the use of strong and unique passphrases or passwords for all accounts and devices
- avoid using public Wi-Fi and instead use secure networks and a virtual private network (VPN)
- deploy mobile device management or mobile application management to monitor bring your own devices (BYODs)
- restrict unencrypted website browsing
- install privacy-enhancing web browser extensions like ad-blockers
- implement allow lists or block IP addresses, domain names and file types that are known to be bad
- 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 such as your location

Learn more

For more information, consult the following publications:

- Supply chain security for small and medium organizations (ITSAP.00.070)
- Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)
- Internet of things (IoT) security (ITSAP.00.012)
- How is your smart device listening to you? (ITSAP.70.013)
- Security considerations for mobile device deployments (ITSAP.70.002)
- Offer tailored cyber security training to your employees (ITSAP.10.093)
- Protecting yourself from identity theft online (ITSAP.00.033)
- How to protect your organization from insider threats (ITSAP.10.003)
- Virtual private networks (ITSAP.80.101)
- Application allow list (ITSAP.10.095)
- Protective domain name system (ITSAP.40.019)
- Use of personal social media in the workplace (ITSAP.00.066)
- Artificial intelligence (ITSAP.00.040)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)

The Cyber Centre's Learning Hub also offers related training courses:

- Course 110 – Cyber Security in the GC and Online Exposure (1/2 day)
- Course 108 – Cyber security best practices (1 day)