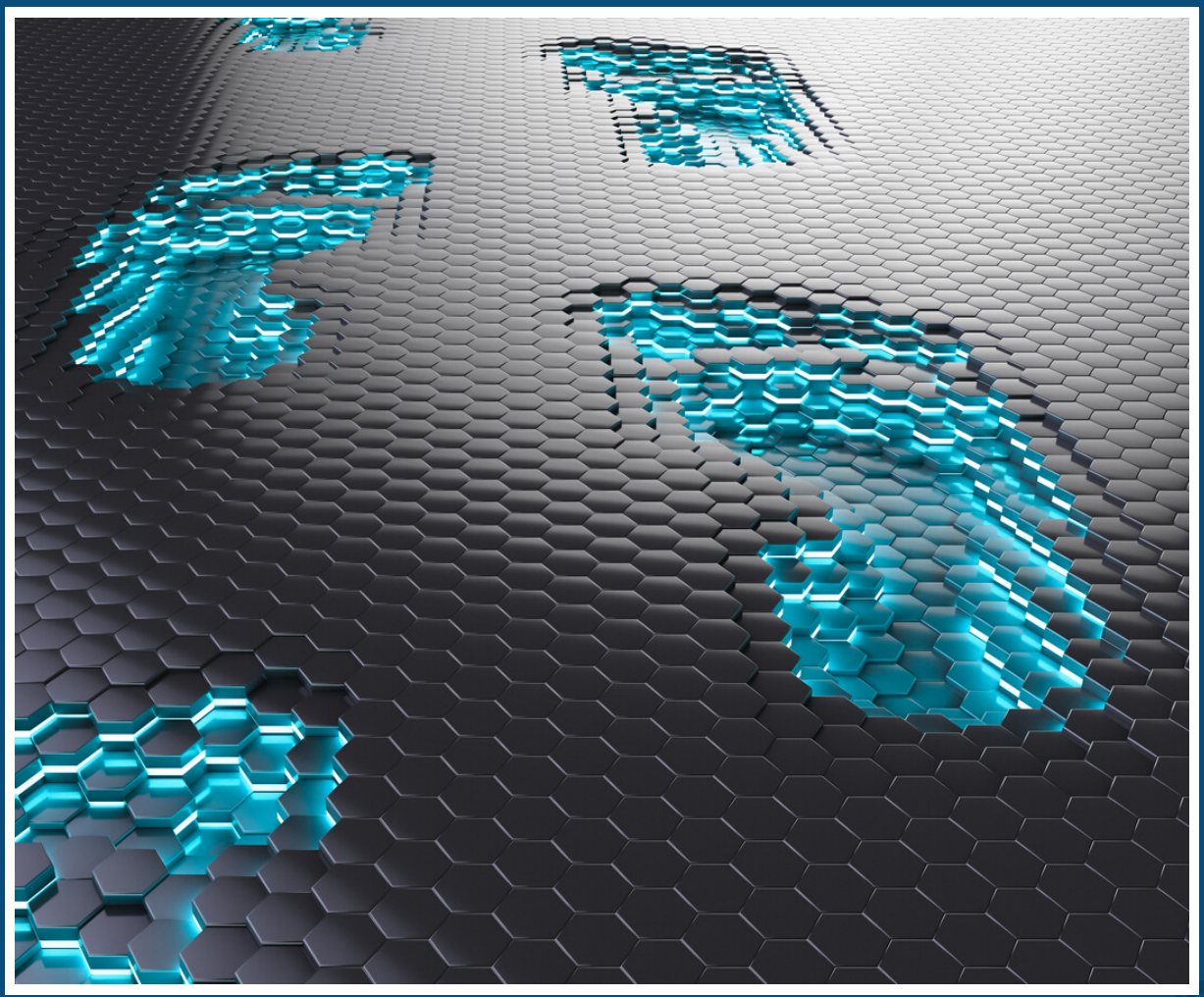
The most **Frequently Asked Questions** about Digital Footprint



THE
CYBER
RESILIENCE
CENTRE
FOR THE NORTH WEST

What a **Digital Footprint?**

Your digital footprint is the digital data left behind when browsing online, via an app or a digital service, posting on social media or having your bio on a website.

Having a digital footprint is a normal part of day-to-day life, and it's becoming impossible not to have some form of digital footprint.

Current privacy and data protection legislations are still new, and many digital footprints are publicly available, looking back many years.

You may have seen in the news previously the digital footprint of someone's historical tweets making headlines, such as a historical racist tweet that resurfaced after many years.

What is the **Digital Footprint** of my business?

Investigating digital footprints is a delicate task and requires trained investigators.

Trained digital footprint investigators use various tools and techniques to discover an individual's/corporate's digital footprint. This can require searching the dark web for any leaked or unwanted sensitive data exposure.

One simple task that any individual or business can do is a google search for their name or their business name. You should review any historical data or images you no longer wish to be visible.

The Google advanced search is a simple interface to carry out this task.

What could my business' **Digital Footprint** reveal?

A simple google search will show your business's general online presence — including reviews, location and contact details.

From here, you can see how your company ranks on Google or what others will see when looking for your business (often used for competitor research).

A thorough security-focused digital investigation will look for data leaks, sensitive data exposure, identity theft and cyber attack angles on the business. This requires investigating staff members and their digital presence. If compromised staff credentials are found, this can lead to the compromise of your directors.

Additionally, be aware of directors'/staff's personal details that could be used for impersonation and identity theft.

What could my business' **Digital Footprint** reveal?

If the findings of your investigation surprise you, it is crucial to learn from them and adapt your behaviours for the future.

For example, a construction business may want to share completed project details on its website. However, oversharing and providing sensitive data (project start/end dates, cost, client names, client contact names, locations etc.) about the project can be used against you by an Attacker through Invoice Hijacking attacks or Spear Phishing attacks etc.

We discuss how dangerous it is when employees use their work email addresses for personal accounts in this recent article.

Why is my **Digital Footprint** important?

Any high-profile individual or business needs to be aware of its online presence.

For example, a high-profile director or executive with a sensitive job title should make an extra effort to reduce their footprint and online presence as much as possible. In addition, a business's competitors may use fake review accounts to bring down their competitor's web traffic or damage their reputation.

When planning a cyber-attack, cybercriminals perform digital investigations into a company and use their findings to their advantage. They will work to explore your business' online data, all in search of any vulnerabilities.

Why is my **Digital Footprint** important?

For a spear-phishing attack, for example, a company's public data would be used by cybercriminals to craft their way into a company.

Using any staff names, email addresses or job titles they find online will play a vital role in a spear-phishing attack. In addition to this, if there are any confidential documents (such as company memos) that are accidentally public, an Attacker could steal signatures and use them to make their Spear Phishing emails look more legitimate.

Can someone track your **Digital Footprint**?

Only some things we do online are publicly visible.

Therefore, your social media privacy settings must be set correctly so that your; location, photos, date of birth and many other details can't be tracked.

When an Attacker performs a Digital Investigation, it's often a case of connecting the dots between their findings before they can act on what they have found.

How to check your privacy settings - Whatsapp, Instagram, Facebook and Twitter.

How can I delete or manage my **Digital Footprint**?

You can carry out your digital footprint investigation. Once you have determined your digital presence, you can manage where you need to tighten your security, delete sensitive information or tighten your privacy settings on accounts online (such as social media). Then, follow the experts' advice to maintain and protect your future.

Having a Digital Footprint is inevitable. However, you need to manage it rather than reduce it.

Want to reduce your digital footprint? We recommend undertaking a Digital Footprint Investigation; this investigation can help manage potential business threats.

Contact us today to learn more about how this can help protect your business and your digital footprint.

Talk to us

Whether you just want informal advice, to learn more about your digital footprint or our services and membership. We are happy to help.

Get in touch with our expert team who can help you on your journey towards cyber resilience.

CALL US: 0161 706 0940

INFO@NWCRC.CO.UK

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

info@nwcrc.co.uk
www.nwcrc.co.uk