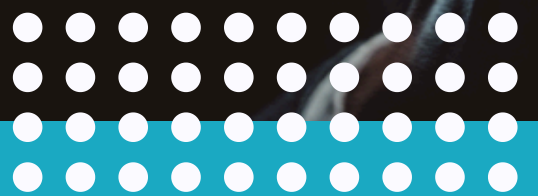


Protect Your Digital Footprint

Practical steps to reduce cyber risk in a GenAI world



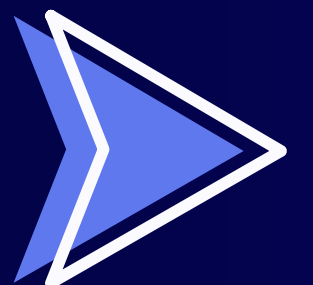


Your Digital Footprint

Every action online leaves a trail.

From social media posts and emails to images, voice recordings, and AI-generated content, your digital footprint continues to grow. This information can be copied, reused, and combined to create detailed profiles that scammers use to impersonate people and exploit trust.

Cyber security is not just about systems. It is shaped by everyday behaviour.





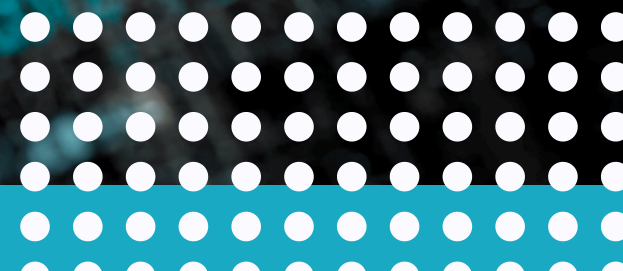
PRACTICAL WAYS TO PROTECT YOUR DIGITAL FOOTPRINT

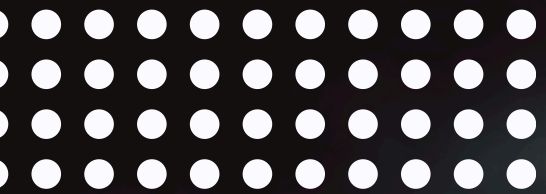
Control what you share

Information shared online is often permanent.

- Set social media profiles to private where possible.
- Avoid oversharing personal or professional details.
- Review old posts, images, and tags.
- Remove accounts you no longer use.

Less public information means fewer opportunities for misuse.





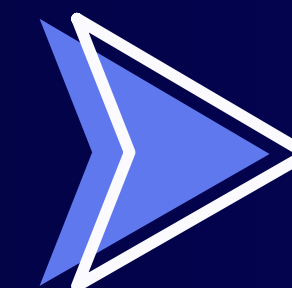
PRACTICAL WAYS TO PROTECT YOUR DIGITAL FOOTPRINT

Connect with caution

Not every connection request is legitimate.

- Review profiles before accepting requests.
- Be cautious of vague or unexpected invitations.
- Verify identities using trusted channels.
- Personalise connection requests you send.

Trust should be verified, not assumed.





PRACTICAL WAYS TO PROTECT YOUR DIGITAL FOOTPRINT

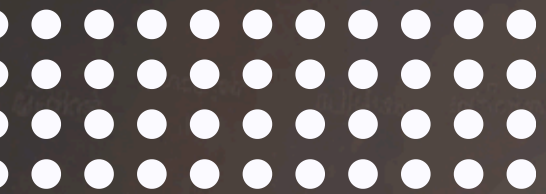
Protect your digital identity

Your identity is one of the most valuable targets.

- Use a password manager with unique passwords.
- Enable multi-factor authentication (MFA).
- Lock physical mail and documents.
- Regularly review financial and account activity.

Strong identity habits reduce the impact of breaches and scams.





PRACTICAL WAYS TO PROTECT YOUR DIGITAL FOOTPRINT

Be alert to AI-powered risk

AI has made scams and impersonation more convincing.

- Pause if a message feels urgent or unusual.
- Verify requests using known contact details.
- Ask verification questions only the real person would know.
- Avoid sharing personal or sensitive information online or with AI tools.
- Treat AI-generated content as a draft and apply human judgement.

Slowing down and verifying protects both you and your organisation.





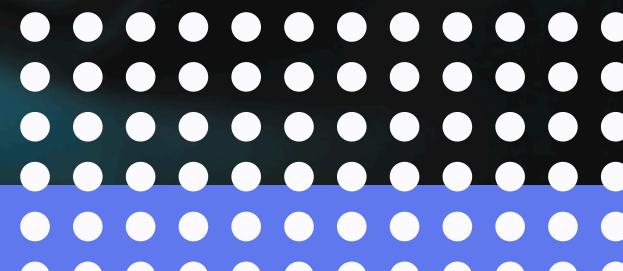
PRACTICAL WAYS TO PROTECT YOUR DIGITAL FOOTPRINT

Maintain good digital hygiene

Digital safety requires regular upkeep.

- Review app permissions and remove unnecessary access.
- Check if your email address has been exposed in a data breach by [clicking here](#).
- Delete unused accounts and apps.
- Update passwords and enable MFA.
- Avoid sharing personal information with unfamiliar platforms.

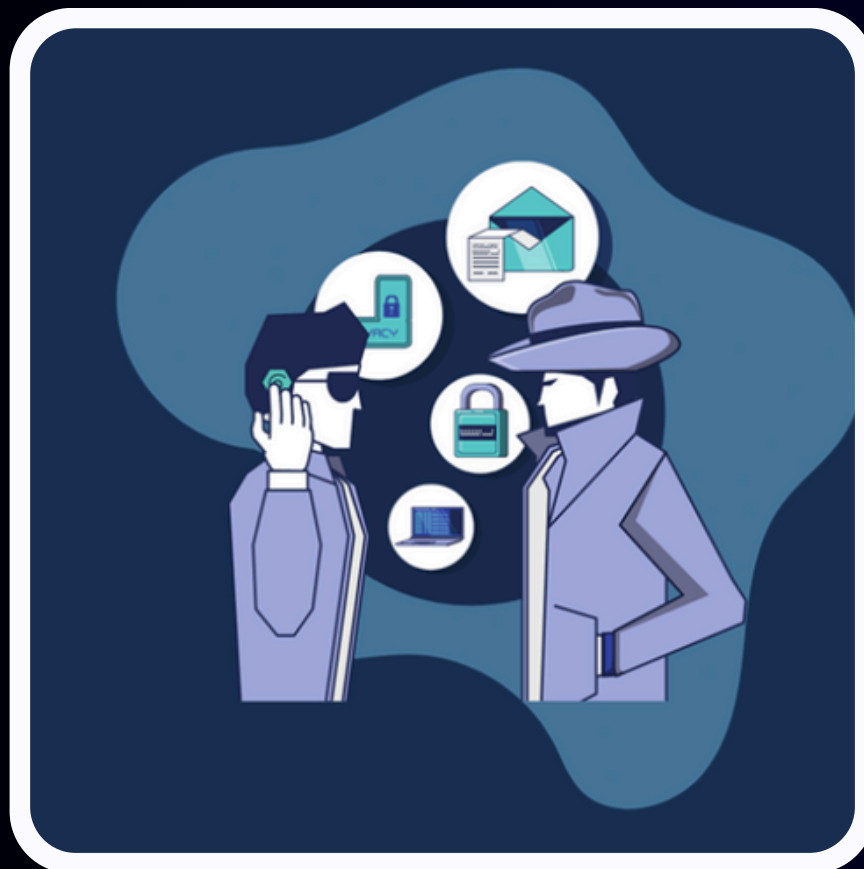
Small actions, done regularly, reduce long-term risk.



Reinforce safer digital habits across your organisation

To support the behaviours covered in this eBook, consider scheduling the following courses as part of your ongoing cyber awareness program.

These modules align with the practical guidance in this resource and help embed safer digital behaviours across teams.



PROTECTING YOUR DIGITAL IDENTITY



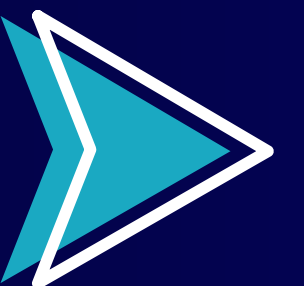
AI-POWERED SCAMS



SAFE USE OF GENAI



[Discover additional cyber awareness and security courses.](#)





Phriendly
Phishing