Your digital footprint.

Tread with care

GET SAFE ONLINE .org

www.getsafeonline.org

Every time you use visit a website, send or receive a message or email, buy or book anything online, comment on a post, upload a photo or find directions on your phone, you're adding to your digital footprint. When you stream music, make a video call or use a smart speaker, that adds to your digital footprint too.

And when you post a photo of your children or friends, you're also adding to *their* digital footprint, even though they may not have agreed to it.

One of the commonplace consequences of having a digital footprint is seeing an ad for something you've searched for online on your social media feed, or as a pop up. But there can be other, more serious outcomes too. Like when you don't make the shortlist for a job because a prospective employer has seen something you posted five years ago. When you're scammed because you've inadvertently shared some confidential details. Or when somebody sells on your personal information to a third party.

We could probably all benefit from thinking more about the trail we leave online. And how it could affect us and others now and into the future.

#DigitalFootprint

What happens when you have a digital footprint?

Your digital footprint is part of your online history and can potentially be seen by other people, or tracked and held in multiple databases, however careful you are with your privacy settings. Here are just a few examples of what can happen:

- Prospective or current employers can look into your and family members' background.
- Applications for schools, colleges, universities, scholarships, clubs or even sports teams could be rejected.
- You, family members or friends could fall victim to fraud or identity theft … or both.
- Your children could be at risk of criminal activity threatening their online or physical safety.
- Records of your online activity could fall into the wrong hands, including organised crime groups.
- Tech companies such as browser and search engine providers can track and record what you've searched and viewed. This, in turn, could be shared with other parties including law enforcement agencies.
- You could be refused life, medical, property or vehicle insurance based on information you have shared online.
- Advertisers can track your movement from site to site to gauge your areas of interest.
- Companies can target you with specific marketing content on social media and other websites. You could also receive emails, letters or phone calls from these companies.
- Entertainment providers (such as music or films) could target you with unwanted recommendations for content based on what you download or stream.

Your top tips

- Think twice before sharing information about yourself, family members or friends that would be better kept private. That goes for social media, forms on websites and apps, responding to texts and messages and when taking part in surveys and quizzes.
- Think before you post. Even if your social media privacy settings are set up correctly, there's no guarantee that your posts or photos won't be shared beyond those who you want to see them.
- Be aware that every time you visit a website, your activity is visible to tech companies like website owners, browsers and search engines.
- Read terms and conditions and data privacy policies on websites and apps before providing any personal data or making transactions. What can the providers do with your data, and why would you agree to it? If you're not comfortable with the information being requested, don't provide it.
- Check geolocation settings on mobile devices, apps and cameras. If you don't want anybody to know your whereabouts – or where you've been – disable them.
- Never stop enjoying the many excellent benefits of using the internet, but always bear in mind the digital trail you may be leaving, who may be able to access it and how they may be able to use it.

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to **Action Fraud** at **actionfraud.police.uk** or by calling **0300 123 2040**. If you are in Scotland, contact **Police Scotland** on **101**.

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

HSBC
first direct
LLOYDS BANK
HALIFAX
BANK OF SCOTLAND
ARMY BE THE BEST
TESCO
M&S BANK
NatWest
Royal Bank of Scotland
creativevirtual The science of conversation™
CITY OF LONDON POLICE National Policing Lead For Fraud
NPCC National Police Chiefs' Council
NATIONAL TRADING STANDARDS eCrime Team
cifas The UK's Fraud Prevention Community
TO STOP FRAUD
EUROPOL EC3 European Cybercrime Centre
ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk
METROPOLITAN POLICE
Ofcom
VS VICTIM SUPPORT
NEIGHBOURHOOD WATCH
neighbourhood ALERT
Llywodraeth Cymru Welsh Government