HM Government

My Digital Footprint

A guide to digital footprint awareness and management

2017

This publication is available at www.gov.uk/government/publications

Introduction

Having a digital footprint is normal – they're very difficult to avoid.

A digital footprint is the data that's left behind whenever you use a digital service, or whenever someone else posts information about you online.

Given that your footprint can be publicly accessible, it's important that you know what it looks like - **you don't always know who's looking at it, how it will be protected, or who it might be shared with.**

The aim of this guide is to help you understand how you can manage your own digital footprint.

This guide is in four parts:

1. **My digital footprint:** an overview
2. **Managing my digital footprint:** reducing the risk of your data being misused
3. **Monitoring my digital footprint:** researching your digital profile
4. **Internet safety:** useful sources to help you stay safe online

Please feel free to share this booklet with your family and friends.

Part 1: My digital footprint

What is it?

A digital footprint is the data that's left behind **whenever you use a digital service.**

Whether you access the internet using a mobile phone, tablet or laptop, you're leaving a trail of information behind you.

For example

- Emailing
- Social media
- Messenger
- Banking
- Dating
- Photo sharing
- Gaming
- Shopping
- Location services
- Applications
- Professional networking
- Using a travel card or paying with a credit/ debit card when travelling

All these activities add to your digital footprint.

It could include information about you, your home and your work that others, including those with malicious intent, can easily gain access to. So, it's important you know what it comprises.

Who contributes to it?

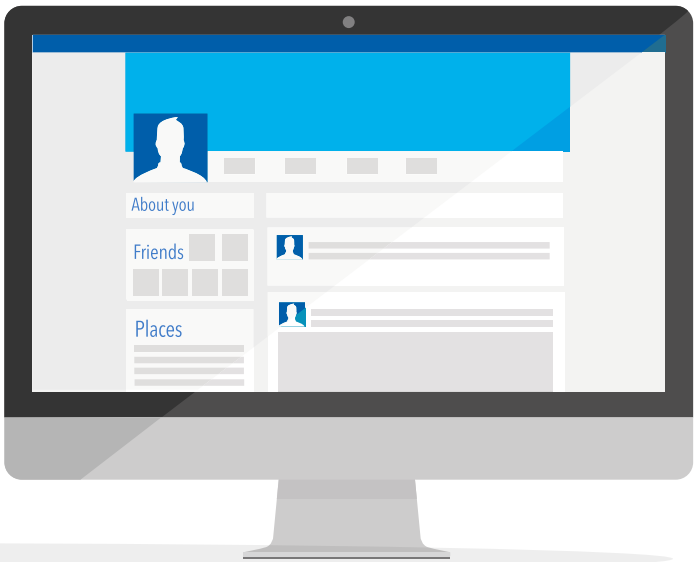
Everything you do online can contribute to your digital footprint.

But it's not only you who can influence your digital trail.

Your friends, family, colleagues and the clubs and societies you're a member of can also add to it, every time they mention you online.

This means that the personal messages, information and data that we post online can end up being viewed by far more people than we ever intended.

And even people you don't know can contribute to your digital footprint. For example, corporate and public sector bodies can add to it as well, when they list public information about you on the internet.



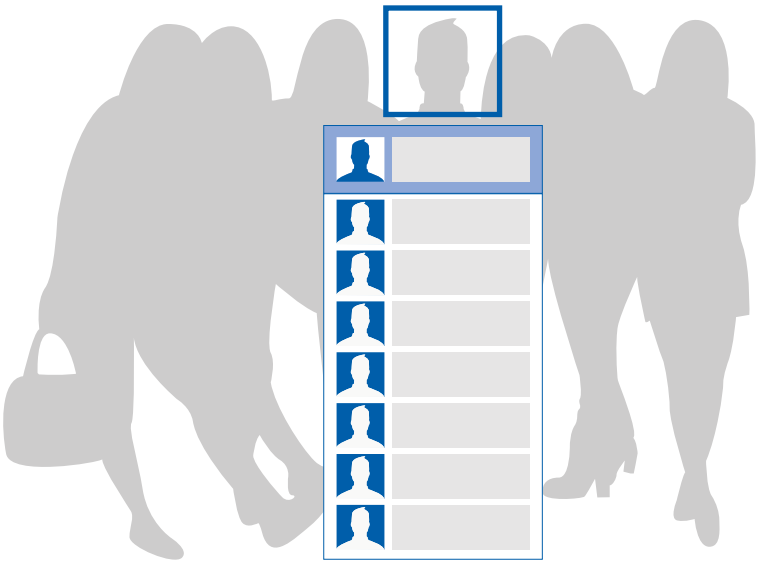
Why is it important?

Once something is shared online, it's there forever – and what happens to this information may not always be under your control.

And for those of us who work for organisations where our roles give us privileged access to sites, information or assets – be it organisational processes, systems, finances, technology, staff data, public data, intellectual property or intelligence – we need to be extra vigilant.

Our digital footprint may be of interest to those with malicious intent. Criminals, protest groups and even foreign intelligence services can all benefit from gaining access to information about us, our work and who we associate with.

Looking after your digital footprint is an ongoing job, so monitor it regularly.



Part 2: Managing my digital footprint

Below are some useful pointers that will help you to manage your digital footprint and reduce the likelihood of your data being misused.

Decide what your stance is on information being published about you or your family online

Everyone should have a view on how information about them and their immediate family is shared online. Do your friends know your views? Do the schools that your children attend know your views?

Once you've decided where you stand, let those who may share this information know.

While online, if you notice something posted about you by a friend or family member, consider asking them to remove it if you don't want it to be there. If that's not possible, understanding what others know about you is still a positive step towards dealing with any unintended consequences.

Regularly review what information about you and your family is available online

Look for information that is publicly available as well as information available to restricted groups, such as followers or friends.

Think about how comfortable you are with this information being available online and any potential security risks it may pose.

Where possible, reduce or remove any information posted on sites you no longer use. It's not enough to make your profile on

one social media site completely private if another account is still accessible and lists all your personal details.

If you see anything posted online that you would prefer was kept private, ask the site administrators to have it removed. As a precautionary measure, consider removing yourself from direct marketing databases.

Avoid sharing for sharing's sake

Enter the minimum amount of authentic information into online registration forms. Do you really need to enter genuine information in every field if there's no legal reason to do so?

Remove metadata from pictures before you post them online

This is especially important for pictures taken with a mobile phone. Metadata commonly stored in exchangeable image file format (EXIF) can reveal details about the location of the device the photo was taken with. This information can be used over time to build up a pattern of your life that can ultimately make you a target for criminals or stalkers.

There are various apps and services freely available that you can use to remove EXIF data.

Think before you post

Try to maintain a positive digital footprint. Always think before posting something online and take time before responding to something negative.

Think about the accumulation of information online relating to you or your family. Anyone who finds out enough could potentially impersonate you or use the information to your detriment.

Think about what you are posting or reposting about others. Put yourself in their shoes – would you like the same being said about you? What would someone you respect think about what you are posting?

And even a seemingly innocuous post can be risky - a burglar could use information posted on social media sites about holidays to establish when properties are left unattended.

Check privacy settings regularly and change them from their default settings

Your information is a revenue source to many social media sites. Privacy settings for such software are often changed, exposing your personal information during upgrades or when new features are added.

Visit the privacy settings pages to check what your external profile looks like on social networks. Take positive action to find out what photos you are tagged in.

Always re-check the configuration settings on your device after every operating system upgrade and review what personal information, like location and contacts, certain applications have access to when they are installed or upgraded.

Compartmentalise your digital life – consolidate on your phone

Use different email addresses for different activities. For example, use one for online banking and another for online shopping. This allows you to close any email accounts that might be problematic without it impacting other parts of your online life.

Most smartphones let the user view multiple email addresses on one device, avoiding the need to log in and out of different email accounts.

Consider using email addresses that don't contain your real name. Doing this helps to make identifying your email accounts more difficult if one of them is compromised.

Hand over personal information wisely

When handing over personal information, make sure it is being transmitted securely.

When entering personal data onto a website always check to see if there is an "https" connection (shown alongside the website address) or a padlock symbol on the site you are using.

These indicate that the site has a good level of security and that other people cannot easily see your personal data.

Ultimately, any information you supply to a website becomes the corporate asset of that site. Check that you are happy with how that company will protect and share your information by reading their terms and conditions.

Make a plan for what to do if you lose your device

Have you backed up everything that's important to your digital life, in case the originals are lost or damaged? It's worth considering a range of back-up solutions, from paper-based to cloud-based services (but consider your digital footprint with the latter). It may also be worth configuring your device for remote wiping in the event that it's lost or stolen.

Part 3: Monitoring my digital footprint

Regularly reviewing your footprint is an essential part of maintaining your online safety.

The following websites can help you do this.

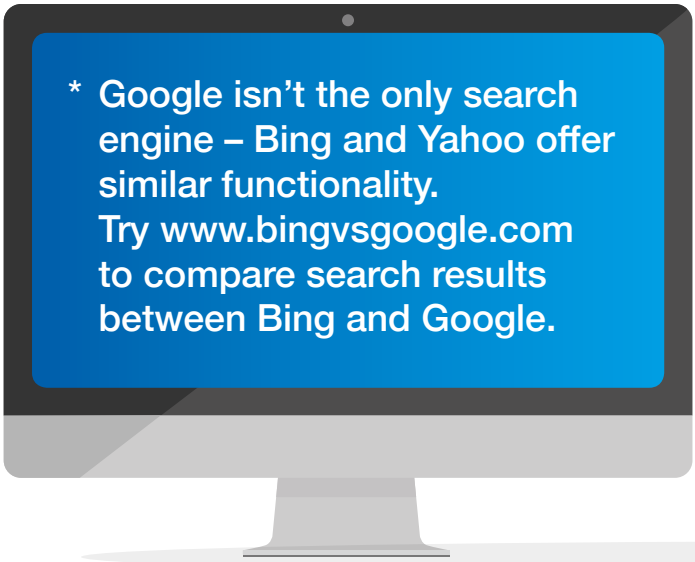
Website checklist

Website	What can you search for?	Search criteria
google.com*	General search against specified criteria – will include information hosted on a range of websites e.g. LinkedIn	• Forename and surname (e.g. Amy Smith) • Forename initial and surname (e.g. A Smith) • Email address (e.g. asmith@gmail.com) • Email address and location (e.g. asmith@gmail.com Bristol

Website	What can you search for?	Search criteria
google.com/images*	Search specifically for images against search criteria	• Forename and surname (e.g. Amy Smith) • Forename initial and surname (e.g. A Smith)
google.com/groups*	Search specifically for returns by a social media group against search criteria	• Forename and surname (e.g. Amy Smith) • Forename initial and surname (e.g. A Smith) • Group name (e.g. Bolton Chess)
google.com/blogsearch*	Search for blog entries about a specific individual – either posted by them or by others	• Forename and surname (e.g. Amy Smith) • Forename initial and surname (e.g. A Smith)

Website	What can you search for?	Search criteria
pipl.com	Search specifically for personal information (refine searches using geographic location, or leave blank to see how many people in the world share your name)	• Forename and surname (e.g. Amy Smith) • Forename initial and surname (e.g. A Smith)
192.com	Search for personal information – specifically who else may live in the same area/town/city	As per search fields, try any combination of name, home address, telephone number and try to include name variations/initials
whostalkin.com	Search for information regarding websites run by individuals	Names of websites
whois.com	Search for information regarding websites run by individuals	Names of websites

Website	What can you search for?	Search criteria
alexa.com	Search for information regarding websites – particularly useful for those people that run/own websites	Names of websites
tineye.com	Search for images rather than text	Upload an image or URL of an image that you want to search for



Google Alerts

Google Alerts is an automated service that emails you whenever the Google search engine indexes information about you or your family, or whenever criteria you provide, such as your name or address, is searched for.

If you choose to use this service, set up a dedicated email address as it will create a degree of separation from your other online accounts. You should only create or access these accounts from home IT systems, otherwise you may be in breach of your organisation's security procedures.

Search **"Google Alerts"** in Google for details on how to set up your account.

Part 4: Websites with information about staying safe online

Online – general

www.cyberaware.gov.uk

Guidance and videos on how to behave safely online.

www.getsafeonline.org

Get Safe Top 10.

www.thinkuknow.co.uk

Guides on understanding and dealing with the different forms of cyber bullying. Also, guides to staying safe online for people of all ages (five to adult).

www.chatdanger.com

Staying safe online with advice largely targeted at parents, carers and children, referencing real-life examples.

www.teachingprivacy.com

Guide to staying safe online with real-world stories and useful discussion questions.

www.internetmatters.org

Advice on how to help children use the internet safely.

Phone

www.knowthenet.org.uk

Provides advice for staying safe online. Also covers mobile safety and gives top tips for mobile security.

Computer

www.us-cert.gov

Security publications, 10 ways to improve the security of a new computer.

Social networking

www.knowthenet.org.uk

Privacy advice for social networks.

Anti-fraud tips

www.actionfraud.police.uk

Provides anti-fraud advice and ways to report fraud incidents online.

Direct marketing removal

www.tpsonline.org.uk

The Telephone Preference Service provides a free service that helps you avoid UK-based telemarketing calls (N.B. isn't 100%) by removing your information from direct marketing databases.

www.mpsonline.org.uk

The Mail Preference Service provides a free online service that maintains a list of all those people that do not wish to receive direct marketing.

www.phonepayplus.org.uk

The website of the premium phone number regulator. Useful if you spot any premium numbers that you haven't dialed, on your bill.

www.192.com/misc/privacy-policy

This page of 192.com displays information on how the website gets the data it publishes. Also includes a link to the CO1 record removal form, which will allow you to remove your details from 192.com.


HM Government