Tracking my Digital Footprint

A guide to digital footprint discovery and management

CPNI
Centre for the Protection of National Infrastructure

DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

"Every day most of us contribute to an evolving public presentation of who we are that anyone can see and that we cannot erase. We might think we are at home on our laptops, cell phones or iPads communicating with just a few people on our friends list. But in reality we are in a huge auditorium speaking into a public address system to a world that can record and distribute everything we say."

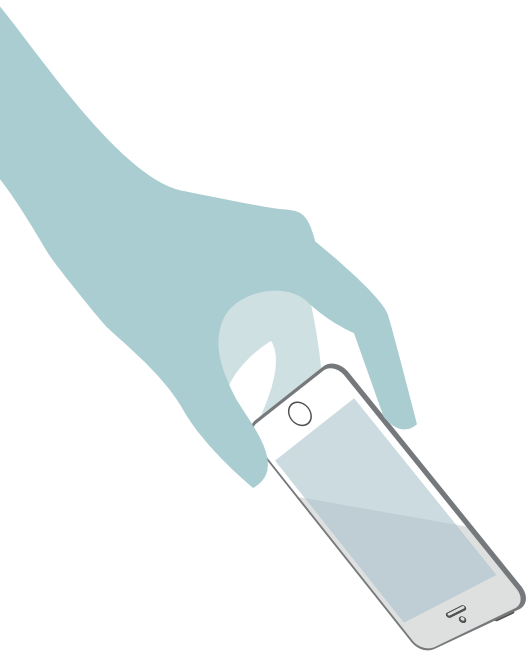
* [Online source] Digital Citizenship Adventures (2015), accessed 30 January 2015 https://sites.google.com/site/digcitizenshipadventures/managing-your-digital-footprint

Introduction

A digital footprint is the data that's left behind whenever you use a digital service, or whenever someone posts information about you onto a digital forum, such as a social network.

Having a digital footprint is normal – they're very difficult to avoid. Given that your digital footprint is publicly accessible, we recommend you know exactly what it looks like and how to actively manage it. This is a brief guide to help you do that.

This booklet demonstrates what others can easily discover about you via a few quick internet searches and suggests some simple ways to obstruct anyone attempting to target you or attack your online accounts.



This guide is in three parts:

1. **General principles:** promoting a positive digital footprint and methods to reduce the likelihood of your data being misused.

2. **Website checklist:** sites to use when researching your digital profile.

3. **Internet safety:** useful sources to help you stay safe online.

If you find this guide useful, please feel free to share it with your family and friends – often it's these groups of people who put information about you online when you would rather they didn't.

Part 1: General principles

In this section we've listed some general principles that will help you to manage your digital footprint securely and reduce the likelihood of your data being misused.

1. 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. Do your friends know your views? Do the schools that your children attend know your views?

Once you've decided where you stand, if it's practical, spend some time talking to those who may share information about you or your family to let them know your views.

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 it needn't be a drama; understanding what others know about you is a positive step towards dealing with any unintended consequences.

2. Find out what information about you and your family is available to the public

Find out what information is available online about you, your family, your work and your interests. Look for information that is publicly available as well as information that is available to restricted groups such as designated contacts or friends.

There are several ways in which you can determine your digital footprint. For detailed guidance, refer to Part 2: Website checklist on page 13.

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

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, take screenshots as evidence to use when approaching the site administrators to have it removed. See Part 3: How to take a screenshot on page 20.

As a precautionary measure, consider removing yourself from direct marketing databases. You will find more advice on this in Part 3 as well.

3. My favourite pet is "the Eiffel Tower"

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?

4. Remove metadata from pictures before you post them online

This is especially pertinent 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. The easiest way to remove Exif data is to simply re-size and re-save the photo before you post it online.

5. Protect your phone number

Payments can be charged to your mobile phone bill, so treat your phone number like a bank card PIN – only disclose it online if you really need to.

6. Think before you click

In some employment sectors, you're now expected to create and maintain a positive digital footprint. Always think before posting something online and take time before responding to something negative.

Even a seemingly innocuous post can be used against you. There have been instances in which burglars have used information posted on social media sites to establish when properties are left unattended.

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?

7. 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 (e.g. location, contacts) certain applications have access to when they are installed or upgraded.

8. Keep passwords safe

With your passwords, you must always remember to:

- Keep them out of sight
- Change them regularly
- Don't let anyone else use them

In addition, make email passwords more complex than the ones you use for website logins or social media accounts. The email address that you supply to websites for account resets make such email accounts the front door to your digital life.

Making the password to your email address as strong as possible contributes to the security of accounts hosted on other websites you might use, such as online shopping or banking sites. And don't use the same password for everything. Otherwise if one of your accounts is compromised there's a good chance others could be too.

9. 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 'burn' any email address that might be problematic (e.g. constantly being sent 'spam') without it impacting other parts of your online life.

The good news is that most smartphones let the user consolidate and view multiple email addresses on one device, avoiding the need to log into different email accounts.

When compartmentalising your digital life, don't use email addresses that contain your real name. Doing this helps to make identifying your email accounts more difficult if one of them is compromised.

10. Do not give social media apps access to your phone or email address

Some social media software will prompt you to share information stored on your phone, then attempt to harvest and link people in your contact list to others in their databases. You might find your colleagues being prompted by these sites to make contact with your friends or family without your knowledge.

Please be aware that other apps will try to do the same, but will include this as part of their terms of use – consider the contents of your contact lists before you install such apps. It is good practice to always research an application before you install it.

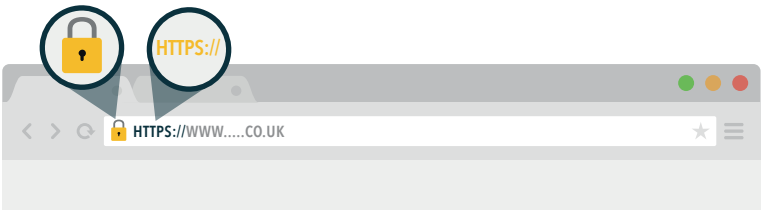
11. If it sounds too good to be true then it probably is

It might sound obvious, but if you're sent an email or text with an unsolicited offer from someone you haven't heard of, or an invite to click on a link, don't click on that link.

If an offer sounds too good to be true, then it probably is. Look at the content of the email or text – does the grammar hang together? Are there spelling mistakes? Has it been sent at 3.00am? If the text or email is from someone you know but the message was unexpected, consider confirming with that person via telephone.

12. 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 connected to. 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 the terms and conditions.

13. 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? For example, contact information, apps and device configurations?

It is 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.

14. Don't make your device easy for others to access

Consider using passwords for all your devices and always secure your voicemail with a PIN code. Make sure to change passwords and PINs from their default settings. This sounds obvious, but it will help defend against unauthorised access (including remote access to your voicemail).

Protect your device from malware as much as you can. Malware is malicious software that exists in several forms, such as:

- **Spyware –** designed to gather the personal information you enter into websites and then pass it on to criminals.
- **Viruses –** that shut down your entire system and can spread to other machines.
- **Ransomware –** that will restrict access to your computer system and demand you pay a fee to unlock it.

Useful tips to help keep your device safe from malware include:

- **Use appropriate antivirus software –** this will scan websites, incoming emails and files you open for known viruses. But it's important you keep this software regularly updated.
- **Make sure firewalls on your devices are turned on.**
- **Ensure your device's operating system (OS) and apps are kept up to date –** set your OS to automatically check for software updates when connected to the internet. Install updates as soon as you get a reminder.
- **Avoid connecting to public WiFi as much as you can –** not all public WiFi is encrypted, even if you are asked to enter a password. If you need to use public WiFi, try to send or receive private information from a secure web page and only use well-known, commercial hotspot providers.
- **Be mindful of those around you when using the internet in public places –** don't make it easy for others to see your password or personal information. Treat your information like it's the PIN to your bank card.

Part 2: Website checklist

In this section we've listed websites that help you to understand and monitor your digital footprint. We recommend checking your footprint regularly.

Things to bear in mind when searching online

Always search the internet from a safe location, such as your home, and with a computer you are authorised to use. Not every computer is well maintained and entering personal information online with one that isn't completely secure could make your accounts vulnerable.

If you have a more commonly occurring name – John Smith, for example – then you might find that the search engines listed below return a lot of information. This means you are less likely to be found by your name alone, and that's good!

You can choose not to be listed on the publicly available electoral roll by simply ticking the relevant box on the registration form. If you've not done this, your current address will be identifiable via 192.com.

Consider requesting your details be removed by completing a CO1 record removal form, which can be downloaded online. If you live in shared accommodation, you may want to talk to your housemates about 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)
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)
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)

**N.B. Google isn't the only search engine – Bing and Yahoo offer similar functionality. Try www.bingvsgoogle.com to compare search results between Bing and Google.*

Website	What can you search for?	Search criteria
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 specifically for comments made in blogs, etc.	Phrases, text (e.g. company names)
whois.com	Search for information regarding websites run by individuals	Names of websites
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 3: Websites with information about staying safe online

Online – general

www.cyberstreetwise.com
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.

How to take a screenshot

Screenshots are useful as evidence when seeking to have information about you removed from websites. Here we've listed the different ways you can take a screenshot on some of the UK's more popular devices.

Apple iPhone/iPad (iOS 7.0 and above)
Hold down the home and power button at the same time until you see the screen flash and you hear a camera shutter sound. The snapshot can be found in your photo roll.

Google Android (4.0 and above)
Hold the power and volume down button at the same time until you see the screen flash and you hear a camera shutter sound. If successful, you will see the details sent to the notification panel where you can tap once on the image to open it. The snapshot can also be found in your gallery.

Windows/Linux
Use the PrtScn key and then paste the screenshot into Paint or another image or word processing program and save it.

Apple Macintosh
Press the following keyboard combination, holding the keys down together: Command, Shift, 3. The screenshot will be added to your desktop.