E-Safety – Your Digital Footprint

1 of 16 – Introduction

Welcome to this session on your digital footprint.

By the end of this session, you will be able to:

* Understand what is meant by the term digital footprint
* Identify some of the activities which add to your digital footprint
* Understand privacy issues relating to your digital footprint
* Explain how to build a positive digital footprint

2 of 16 – What is a digital footprint?

A digital footprint is the name given to the trail of data and information you leave while using the Internet. This information is specific to you, and everyone who uses the Internet leaves a digital footprint of some kind.

There are two types of digital footprint:

**Passive:** This sort of footprint is generated by browsing the Internet, and users are often unaware data on them is being saved. Websites save information on you as cookies when you visit them; search engines store your search history, and most websites log your IP address when visiting a website.

**Active:** This sort of footprint is generated when you share information online. For example, if you send an email, sign up to an online service, or post something on social media, this information can all be linked back to you.

3 of 16 – Adding to your digital footprint

Most websites will ask you to accept their terms of use and cookies when you initially visit them. A cookie is a small piece of data which the website saves about you and includes information such as your location, device used and your IP address.

The following activities all add to your digital footprint in passive or active ways:

* Online Shopping
* Posting on social media
* Playing videogames online
* Paying with a debit/credit card
* Geolocation services, such as tagging somewhere you visit on Instagram

4 of 16 – How others affect your digital footprint

A digital footprint is made up of things to do with you but can be influenced by others too. For example, a family member tagging you in a photo will link your name to that image. This goes for things like tagging posts with geolocation information too.

It is not just friends and family members that can add to your digital footprint, but also any societies you are a part of, businesses you may have used, and public sector bodies. Information shared by these organisations might be more detailed and contain your full name or parts of your address depending on the type of organisation sharing the information.

5 of 16 – How your information is used

Your digital footprint acts like a trail which other people and companies can use to find out more information about you. Depending on how much information you have been actively putting online, it can be very easy for employers or organisations to find details of your life.

Employers often conduct an online search for prospective employees to learn more about that person before they are interviewed or hired. They will want to see that you have views in alignment with their company values, how you talk to others online, if you have good written communication skills, and that you don’t appear irresponsible. People whose online profiles show them taking drugs or drinking alcohol have been shown to be less likely to be hired over someone who appears to be a good cultural fit for the company.

This same investigative technique is also being adopted by universities, who want the best candidate possible to represent them.

Additionally, law enforcement agencies have started to look at people’s digital footprints to find information which would otherwise be unattainable. This has led to police locating and arresting criminals who have posted pictures or videos of themselves bragging about the amount of money they have made from committing illegal activities.

6 of 16 – Risks associated with your digital footprint

Privacy is the biggest risk associated with your digital footprint. Social media specifically collects an extensive amount of data about a user which is then used for a variety of purposes. For example, Facebook will track the websites you have visited as well as things you click on or post on their platform.

This information can be used to identify things such as:

* If a person is an introvert or an extrovert
* A user's level of education
* Location
* Race
* Full date of birth
* Political or religious beliefs
* Sexuality

Most social media sites collect information by default, and many users don’t realise they can opt-out of this by adjusting their user profile settings.

Once a social media site has built up a profile about you as a person, it can sell different pieces of this information to various businesses which will affect the types of things you are advertised, or the types of media you are recommended.

7 of 16 – Security risks of your digital footprint

As well as privacy concerns, the amount of information available for anyone to find out about you can lead to an increased risk of being hacked, doxed, or targeted for a scam.

If you need to reset an online account, you will usually have to provide answers to security questions. Common security questions are things like the name of your first pet, or your mother’s maiden name.

You may have seen an image which says something like “your superhero name is the name of your first pet and the road you grew up on”, encouraging people to post their superhero names in the comments. This is most likely to have been made by hackers who want to trick people into sharing their security question information so that they can gain access to their online accounts.

This is a good reason to never fully fill out forms online with personal information, unless it is legally required.

8 of 16 – Managing your digital footprint

The following steps show what to do to manage your digital footprint as it currently exists.

**Step 1 – Decide**

When it comes to managing your digital footprint, you need to decide how much information you are comfortable with having available about you online. Consider how the information available may impact your life. Will it help or hinder future educational or career opportunities?

**Step 2 - Search**

The second step is finding out how much information is available about you online. To start with, you could simply Google your name and see what information appears. Make a note of what websites appear as we will need those for the final step.

[Click here](https://www.192.com/) visit 192.com where you can search for additional information.

[Click here](https://www.social-searcher.com/) visit social-searcher.com where you can search for additional information.

**Step 3 - Curate**

Finally, you can start to curate your digital footprint. This third step varies depending on the service you are using, or the search you are appearing in. For most social media sites, you can change your privacy settings to stop appearing in search engines, hide important information from people outside of your network, and simply delete posts you wouldn’t want others to see. For websites which you used to use but no longer do, it is worth closing them using the settings on the platform. For specific sites like 192.com, you can visit their help section and ask for information to be removed.

9 of 16 – Additional ways to protect yourself online

There are many other things you can do to reduce your digital footprint and protect yourself online.

**Use a password manager:**

Set up a free password manager such as BitWarden and use one unique password to enter it. You can then save all your other passwords to the app which means you don’t have to store them in the browser or on any websites.

**Remove photo metadata:**

Every photo you take contains metadata. This metadata contains a date and location the photo was taken, and much more. [Click here](https://www.canto.com/blog/photo-metadata/) to visit a website with instructions on how to remove these details before uploading a photo online.

**Remove your phone number:**

If a social media account displays your mobile number, you should consider removing that link. If the site is ever hacked, or if your settings show your mobile number to others, criminals can charge services to that mobile number without you knowing.

**Use a VPN:**

The best way to control your privacy online is by using a VPN. These Virtual Private Networks re-route your Internet traffic and make it harder for online services to track your activity. It is not advisable to use a free VPN as these services have been found selling the data, they get from providing this service to you, defeating the purpose of a VPN.

10 of 16 – Building a positive digital footprint

We have seen how your digital footprint can be used by employers and other organisations in negative ways, but it can also be used to shine a positive light on you as an individual.

Portray yourself online by limiting how much people can find out about you if they are not connected with you. You can ask friends or family members to remove any tags of you to photos which you might be in which you don’t think show your best interests. This can also apply to checking work-related information and asking your employer to remove anything which you find personal.

Lastly, be mindful of how others can perceive you online. Think about the things you share online, and how they might be perceived by others as you don’t know who is looking at your posts, or who it might be shared with. Even if choose to delete a post you have made, there are many ways that post can be recovered, or even simply screenshot and saved by others.

11 of 16 - Question 1

Which of the following defines the term digital footprint?

Choose one

* A digital footprint is the name given to specific purchases you make online.
* A digital footprint is what is remains online once you have deleted your social media.
* A digital footprint is the trail of data and information you leave while using the Internet.
* A digital footprint is the location of the last Wi-Fi hotspots you used

**Answer:**

A digital footprint is the trail of data and information you leave while using the Internet.

12 of 16 - Question 2

Which of the following are ways you add to your digital footprint?

Choose all that apply:

* Posting on social media
* Playing videogames online
* Online shopping
* Browsing the Internet

**Answers:**

Posting on social media, playing videogames online, online shopping and browsing the Internet are all ways you add to your digital footprint.

13 of 16 - Question 3

What are cookies as used by websites?

Choose one:

* Information about the media you consume
* Your full name and phone number
* Information about your social media accounts
* Your IP address and location

**Answer:**

Your IP address and location

14 of 16 - Question 4

Put these in the correct order to match each step taken to manage your digital footprint.

* Search various websites to check what others can see
* Delete posts you don’t want available to anyone, and update your privacy settings
* Decide how much personal information you want available to others online

**Answer:**

Step 1 – Decide how much personal information you want available to others online

Step 2 – Search various websites to check what others can see

Step 3 – Delete posts you don’t want available to anyone, and update your privacy settings

15 of 16 - Question 5

What are some additional ways you protect yourself online?

Choose all that apply:

* Use a password manager
* Use online banking
* Remove photo metadata
* Remove your phone number
* Create a torrent
* Use a VPN

**Answer:**

* Use a password manager
* Remove photo metadata
* Remove your phone number
* Use a VPN

16 of 16 - End

Well done, you have completed this session on your digital footprint.

You should now be able to:

* Understand what is meant by the term “digital footprint”
* Identify some of the activities which add to your digital footprint
* Understand privacy issues relating to your digital footprint
* Explain how to build a positive digital footprint

If you have any questions about anything covered in this session, speak to your tutor for more help. ​