CYBER WORKS

Social Media: How to Stay Safe

Social Media Security, Privacy & Footprints

Audience: General **Reading Time: 10 Mins**

Social Media opens up a whole new audience for businesses, and enables people to keep in touch with friends and families virtually. However, as social media becomes even more popular, we need to ensure that we retain our privacy and don't reveal too much.

Key Points

- Strong passwords and two-factor authentication should be used for all social media accounts
- Try not to answer security questions truthfully and instead use random answers
- Social media needs to be used with care as one mistake can easily lead to your personal information being released to the entire world.
- Your social media footprint is the data contained about you on social media
- Social media posts can inadvertently reveal a huge amount of unintended personal information
- Metadata and reverse image search can both be used to identify where photos were taken

Social Media: Stay Safe

Social Media is used by almost everyone, and businesses of all sizes also tend to have a social media presence. Social media can be a great way to connect with our friends and share what we are doing. Businesses can easily reach huge, targeted audiences with advertising tools for different social media sites; Facebook claims 1.6 billion people worldwide are connected to a small business on their site.

A huge number of different social media sites are used, with the most popular in the UK being Facebook, Instagram, and Twitter. Snapchat, YouTube, TikTok, Reddit and Discord are also popular. We reveal a huge amount of information to these websites, and this information can easily become public if care is not taken. We need to ensure that we secure our accounts and be careful about what information we share on these websites.

Securing your Accounts

A strong password should be chosen for all of your social media accounts, use the longest password the site permits and ensure that this contains a mix of uppercase and lowercase characters, along with numbers and punctuation. It is much easier to guess phrases that are common (such as song lyrics or sayings) or even what you consider a 'random' sentence, that still makes grammatical sense. e.g. "dogseatbones" makes sense, therefore is easier to guess. An alternative approach is to use the "three random words" method; choose three or more words at random - ones which do not fit together in a sentence, and connect these together. This now becomes your password. For example "correcthorsebatterystaple".

Never use any personal information, or information tied to you, in your passwords. This includes information such as names (including those of your pets), addresses, special dates or any kind of your favourite things (sports teams, places, food etc.) Furthermore, ensure you choose a password that has not been seen in a data breach before. Someone trying to gain access to your account will likely use a huge list of passwords seen in previous data breaches and try using these passwords for your account. Troy Hunt (@TroyHunt on Twitter), an Australian Cyber Security researcher who runs the website haveibeenpwned.com. The website allows you to check and see if a password you have used has been seen in a data breach before. Ensure you use a password that hasn't: https://haveibeenpwned.com/passwords

Most social media sites offer an extra layer of security: Two-factor authentication (2FA). This requires you to provide another piece of information before you are logged into your account; a second factor, your password is the first.

Two-factor methods can vary between

Definitions

Data Breach - An event where someone who does not have permission to access certain data does so. Usually associated with hackers stealing data from websites. These can contain a huge amount of sensitive data about people.

Metadata - Metadata is data about data. This is data often added to photo files or documents. This may contain extra technical information, but will usually also contain data about who created it, when it was created, and where.

3rd Party App - An app or website that you sign into using one of your social media accounts, instead of creating a new account on the website. It may have access to some of the information from your social media.

Two-Factor Authentication (2FA) - A system in which two different methods are required to authenticate the user.

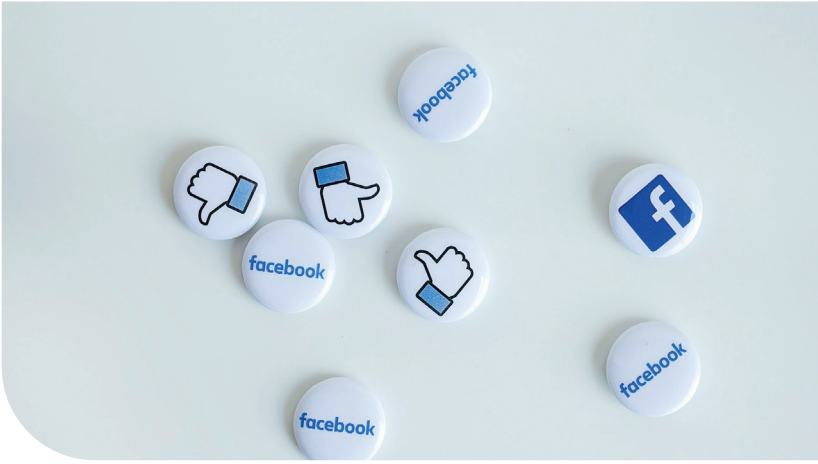
websites, but are usually one-time passwords. These are either sent to you via email or text message when you want to login, or are generated using an app. Some websites also allow the second-factor to be a security key – this looks like a USB stick that you plug into your computer when logging into the website. Security keys can also be contactless, so the same security key can be used when logging into websites on your phone or other devices that lack USB ports. However, not all devices support the use of security keys. Yubico, makers of the YubiKey, a leading security key manufacturer, list Facebook, Instagram, Reddit, and Twitter as supporting its security keys.

However, if you lose your 2FA key or method you will lose access to your account. To ensure that you can maintain access, it is advisable to keep your backup codes in safe place. These are normally given to you when you setup two-factor authentication and can be used to login if you do not have access to your usual two-factor method.

Furthermore, some websites use security questions that you must answer in the event you forget your password. However, these questions usually have answers that people other than you may know, or information you may have revealed on social media. Common answers include information such as: *your place of birth, mother's maiden name, favourite food, or football team, etc*. There is, however, no harm in answering these with incorrect answers – the website will be none the wiser. This will ensure that even if someone were to know the answer to your security questions, they will not be able to get the question correct. Choose a random word instead – just make sure you remember it!

Social Media and Digital Footprints

A social media footprint is the information that is available about you on social media, this includes information posted both by yourself and by others. It includes social media posts, who you are connected to and any activity you perform on social media. This forms a subset of your digital footprint, which is records of any interaction with any digital service, including online shopping, credit card or travel pass activity (Oyster card, etc.), and information that apps on your phone collect.



A huge amount of information can be divulged on social media, sometimes accidently, and we are not always aware of the implications of this information being shared. Each different aspect of social media can divulge different pieces of information; profile pictures, posts, the accounts we connect with, 3rd party apps, and profile information can all reveal a wealth of information.

What are the risks?

The main risk of social media is that your highly personal information is exposed on the internet to strangers. Even if you quickly delete this information, it may still be available on the Web Archive: a project aiming to archive the internet. Sharing certain views on social media may lead to abuse, bullying, stalking or even financial loss or identity theft depending on the information you post. The information you post may, in extreme circumstances, lead to you being blackmailed.

Social media is not inherently bad, or dangerous, but it needs to be used with care. One mistake can easily lead to your personal information being revealed to the entire world.

Profile Pictures and Usernames

People tend to choose a good picture of themselves, or a favourite image to use as their profile picture; wanting to show off to the world. Whilst seemingly innocuous, it can be used to link different accounts across different social media platforms. Depending on the picture, if two accounts on different social media platforms use the same profile picture – they likely belong to the same person. Likewise, using the same username across different platforms can also be used to link accounts to the same person.

If you wish to keep your social media accounts separate, use different profile pictures and usernames on each.

Posts

Social media posts are the main source of information on social media sites, people publish an extraordinary amount of their lives on social media – both their highs and lows. Posts vary by platform but can consist of almost anything: photos, check-ins, reviews, and nearly everything else – anything. However, you should be wary of what you post online. Would you feel comfortable saying what you are going to post to everyone who will see it in person? There are numerous cases of employees being dismissed for inappropriate social media posts.

Have you ever replied to a friend's post which was asking you something to the effect of *"How to make your Movie Star Name - Post the following: Mother's Maiden name, Street your grew up on, and name of first pet"*. Just a bit of harmless fun, right? Except, do you remember your "Security Questions" from earlier? You may have inadvertantly revealed a whole lot of personal information about yourself.

Every photo that you take has metadata attached to it, this is information about the photo, this includes the date and time it was taken, details about the camera that took it, and where it was taken! Some social media sites remove metadata when you post photos, but others do not. Someone who can view the photos you post has the ability to easily see where the photo was taken. Reverse image search can also be used to identify the locations of images. This is done by uploading an image and searching for similar images; these similar images may reveal the location of the original photo.

Exercise apps that you may use on your phone which track your workouts, such as running or cycling, can reveal your precise location to the public if you post on social media. These apps can track your precise location during your workout and produce a map at the end displaying the route you took, along with timing information. There is often an option to share your workout either on social media, or with other members using the same app. This shows the map of your workout, including your precise location of your start and finish;

often these are your home. If you share your workouts, be aware that you may also be sharing your home address. This has been used to expose the positions of US military bases in the Middle East, as those stationed there shared their workouts with other members of the apps they used.

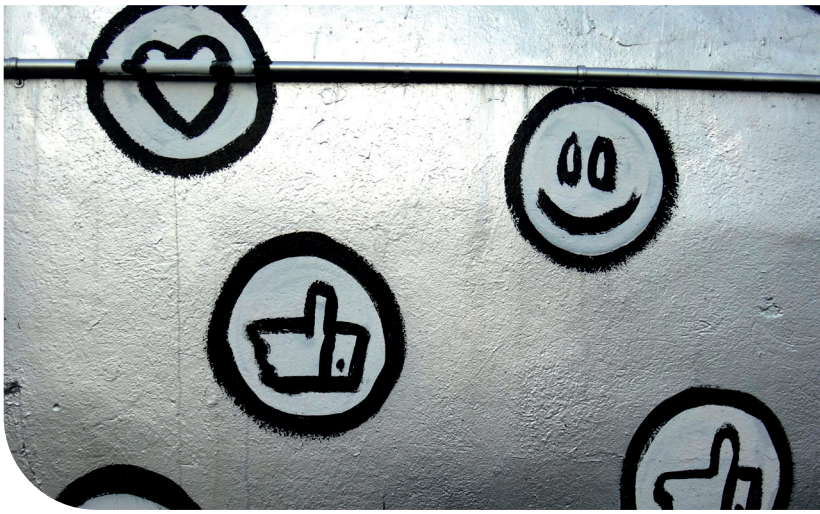
Furthermore, be aware of what may be in the background of photos or videos you share online. There have been numerous examples of photos being posted by celebrities or organisations where passwords written on post-it notes taped to computers have been visible.

Many people post photos of airline boarding passes on their social media when going on holiday, being unaware of the information these contain. These contain a barcode that is scanned when boarding your flight. However this barcode can contain a wealth of information such as your full name, date of birth, dietary requirements or allergies if you get a meal on your flight, along with information about your flight source and destination.

Former Australian Prime Minister Tony Abbott posted a picture of his boarding pass on Instagram, and using the information from the boarding pass someone was able to find his passport number. If you do decide to post a picture on your next holiday of your boarding pass, be aware of the information it contains and try to hide any barcodes or information on it.

Friends, Followers and Likes

The accounts that you are connected with on social media, terminology varies by platform but includes the accounts you are friends with, follow or like. These accounts can reveal a huge amount of information, including your location, education, employer, and political views – some of which you may not want to be public.



Some accounts of organisations that you are connected with may have a global presence, such as celebrities or large sports teams, however some only operate in a small area, or have a small following. Accounts for small sports teams, or local organisations which only operate in their locality, such as local councils, or small businesses will generally only interact with those in their vicinity. If you are connected with a small business – you probably live near it.

Furthermore, if the accounts you connect with belong to your friends or family, the information they have on their profiles can reveal information about yourself. If they have information on their profiles indicating where they live, who they work for, where they went to school, college or university, some of this information probably applies to you, too.

If other people can see the accounts you interact with, they may also be able to determine your political views based upon who, or what you interact with, such as accounts who post their political views or belong to political parties. On

many platforms, you can restrict who can see the accounts you are connected with. This is usually split into categories: everyone, other accounts you are connected with, only certain

accounts or only yourself. Check your privacy settings of the information on your profile.

3rd Party Apps

3rd party apps are applications or websites that you have signed into using a social media account, instead of creating a new account on the website. This streamlines using new apps and websites as you just click the "Sign in with ..." button. However, doing so shares your information that you have submitted to that social media platform with the 3rd party. These 3rd party apps may store this information for an unlimited period, the data they are able to access is not always relevant to their purpose. However, not all 3rd party apps wishing to access your information are malicious, a confirmation is usually required to share your data, ensure that you only agree if the data they wish to access is appropriate.

The Cambridge Analytica – Facebook scandal involved data gained through a nefarious 3rd party application on Facebook.

Profile Information

Social media platforms, particularly Facebook, prompt users to enter a wealth of information when they register an account, this can be used to suggest people you may know and improve your overall experience on social media. For example, it may ask you to enter where you have lived, which school you went to and where you work, it will then suggest people who provided the same answers. This can, however, reveal a huge amount of information about yourself, and this information may accidently be left public. If you wish to keep work out of social media, do not provide that information.

Information that you used to sign up to social media platforms can be used so that other people who have this information can find you. For example, most social media websites allow you to upload your contacts to find people on that platform that have either email addresses or phone numbers in your contacts. If you don't wish to be found, use a different email address for each social media website, and don't link your phone number. Twitter shared phone numbers of users with advertisers without permission.

There is no line in the sand as to what information you should or should not share on social media, the information you share on different social media platforms is a highly personal decision. However, you should ensure you are aware of the information available on your social media profiles. Ensure that you check the privacy settings on the information available on your profiles and limit this information to what you feel comfortable with. Furthermore, respect the privacy of others, ask your friends if it is ok to post pictures of them online.

READ MORE

1. Facebook. Facebook for Business. [ONLINE] at: https://www.facebook.com/business/ads [Accessed 25th September 2020]
2. YouGov The most popular social networks in the UK. [ONLINE] at: https://yougov.co.uk/ratings/technology/popularity/social-networks/all [Accessed 25th September 2020]
3. Troy Hunt. Haveibeenpwned.com [ONLINE] at: https://haveibeenpwned.com/ [Accessed 25th September 2020]
4. Yubico. Works with YubiKey Catalog. [ONLINE] at : https://www.yubico.com/works-with-yubikey/catalog/ [Accessed 25th September 2020]
5. Alex Hope. 2020. When you browse Instagram and find former Australian Prime Minister Tony Abbott's passport number [ONLINE] at https://mango.pdf.zone/finding-former-australian-prime-minister-tony-abbotts-passport-number-on-instagram [Accessed 25th September 2020]
6. NCSC. Social Media: how to use it safely. [ONLINE] at: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely [Accessed 25th September 2020]
7. BBC. 2018. Fitness app Strava lights up staff at military bases [ONLINE] at: https://www.bbc.co.uk/news/technology-42853072 [Accessed 25th September 2020]
8. Jeffrey Friedl. Jeffrey's Image Metadata Viewer. [ONLINE] at: http://exif.regex.info/exif.cgi [Accessed 25th September 2020]
9. Miller-McCune. 2010. On Facebook, You Are Who You Know. [ONLINE] at: https://web.archive.org/web/20120325032734/http://www.miller-mccune.com/culture-society/on-facebook-you-are-who-you-know-10385/ [Accessed 25th September 2020]
10. New York Times. 2018. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. [ONLINE] at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [Accessed 25th September 2020]
11. Fitzgerald HR. 2020. Social media: 3 noteworthy employment law case studies. [ONLINE] at: https://www.fitzgeraldhr.co.uk/social-media-and-employment/ [Accessed 25th September 2020]
12. Business Insider. 2018. A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note. [ONLINE] at: https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1?r=US&IR=T [Accessed 25th September 2020]
13. CNET. 2020. Twitter faces class-action privacy lawsuit for sharing security info with advertisers. [ONLINE] at: https://www.cnet.com/news/twitter-faces-class-action-privacy-lawsuit-for-sharing-security-info-with-advertisers/ [Accessed 25th September 2020]
14. Wayback Machine. [ONLINE] at: https://web.archive.org/ [Accessed 25th September 2020]

About the Author

Henry Clarke is currently studying at Lancaster University. Henry has completed his BSc in Computer Science at Lancaster and is now studying his MSc in Cyber Security. Henry is part of Lancaster's Cyber Security society **LUHack**, his interests are cyber security and programming.