



Fresh start

Take a look at your online identity and reclaim ownership of your personal privacy.



Online, we are defined by what we do and what we leave behind.

Everything we do online leaves a trace, whether it be what we've bought, events we've attended, sites we've visited or people we've connected with. We may have dispensed opinions on every possible kind of subject or freely given away our social connections, holiday plans, current and past income, or relationship status (also current and past). All of that data, and much, much more, persists - long after the details of our daily life, or the substance of our personal beliefs, may have changed.

Because we cast these digital shadows it's possible to reach into the internet and retrieve a composite 'snapshot' of each of us. Although that picture may not always accurately represent us, it may well contain more personal information than we would be entirely comfortable sharing. What may be even more concerning to some people is that there are companies, organisations and individuals who trawl the internet pulling out these snapshots - and trading on the information they hold - *all the time*.



Your digital trail.

Every time we go online we inevitably reveal information about ourselves; whether it's a tiny thing, like up-voting a comment on a message board, or a major life event, like planning a wedding, it leaves a trace, and all that data is valuable. Even if it's just a list of websites we've visited or items we've purchased, our digital trail is a hugely attractive asset to brands, advertisers, and organisations who may want to use our data to try to sell us products or services, interest us in their causes or influence our political thinking. It's

also a potential magnet for hackers and criminals who are adept at using the information we may have inadvertently shared to access our private accounts, hijack our identity and steal our data.

The trail we leave can be described as *active* or *passive*. Active trails occur when we take an obvious, deliberate action online, like posting to our Instagram feed or subscribing to a mailing list. Our passive trail is altogether more subtle: it's assembled without our approval or knowledge and includes things like; the invisible alert a company receives every time we open a 'special offer' email link, or the location tag we leave as we move from place to place.

In fact our mobile devices are one of the top contributors to our individual digital trail as they constantly share vast amounts of information about us.

Who has our data.

The main contenders for capturing our personal data are the massive online players like Google, Apple and Microsoft, shopping sites like Amazon and Alibaba and the social media giants Facebook, Twitter and their like - along with our respective governments. In addition many 'informational' websites like *Mashable*

”
 We accumulate
massive amounts
of digital clutter,
and some of it can
be harmful if it gets
lost or is stolen.

Michael Kaiser
 National Cyber Security Alliance



or *Mentalfloss* want our personal details and require us to use them to open an account.

But there is another group who's job is solely to search through internet sites and traffic collecting everything they can find about us: *data brokers*. Data brokers (or *information-brokers*) are companies which collect information about us in order to sell it on

to other organisations or individuals. The information these data brokers collect can be comprehensive and include; credit scores, police records, social media posts, search histories, census data, birth certificates, marriage licenses, voter-registration information, and so much more. In countries with less restrictive online-privacy laws it is true to say that many data brokers hold more personal and private information on a citizen than their own government does.

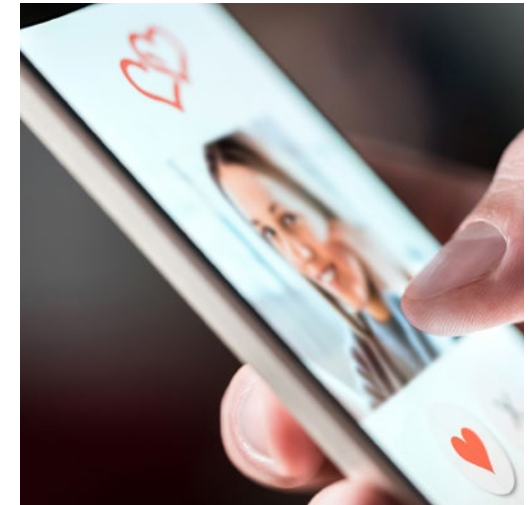
Many people are not really aware such companies exist, but data brokerage is now an extremely lucrative industry generating in excess of \$200 billion revenue yearly. While we may not feel comfortable with the fact that there are organisations whose whole business model is to capture as much personal information about us as possible, in order to sell us shoes or influence our

democratic votes, there are other, more immediate threats to our safety and well-being. *Hackers* and *cybercriminals* are all desperate to get hold of our most private and secure information.

What could someone do with your data?

Once our accounts get hacked, or our identity becomes compromised, the possibilities for malicious actions performed either against us, or in our name, can be terrifying. We could fall victim to bank theft, have loans taken out in our names, lose our social security benefits or even see future careers and personal relationships jeopardized by unsanctioned postings or comments online.

If our data is lost as part of a massive data-breach it could be 'pasted' to dark-web sites designed to share stolen credentials or sell them to the highest bidder. Due to the ease of anonymity associated with these kinds of sites they are hugely popular with criminals and hold vast quantities of information. In fact there is so much stolen data available whole private lives and online identities can be purchased, as part of a database, for as little as \$5 each.



FRESH START



Be cyber-smart! Make a fresh start.

It's impossible to navigate the internet, or any part of online life effectively without leaving *any* kind of digital trail behind. No-one wants to go through life never posting anything or signing up to any free services or accounts.

Most people are prepared to give up *some* privacy for the extra-functionality that digital transactions and mobile apps offer. The good news

is that by taking some precautions, and changing our approach a little, we can all achieve a much better balance between privacy and convenience *and* reduce our digital trail in the process.

If we can achieve that we'll not only be protecting our most important accounts we'll be going a long way to reclaiming our privacy and securing our identity. So let's make a start.



Step One. De-clutter your digital life.

Many of us have old, half-forgotten email accounts, unused online services we've signed up to and years worth of data in folders we haven't opened for years, so start out by turning your whole online life upside-down and giving it a good shake. There is nothing to be gained by holding on to old accounts and files that you don't want anymore. Pretty much all the major free-email providers, for instance, have suffered a data-breach at one time or another.

Why allow your credentials to be among those stolen if you are no longer even using their service? By only keeping the files and services that you can't bear to part with, and actively use, you'll be reducing the amount of information which is just lying around waiting to be compromised.

Look through your photo library

Of all the clutter filling up the memory allocation of our devices, accounts and cloud-storage, digital images must be the primary offenders. It's so easy to take and store photos that we all do it, all the time. But how often do you actually end up looking through them all? And when you do, how many do you actually want to keep?

Now is the time to go through and delete all those multiple versions of the same scene (or 'burst-mode' shots), pictures of sunsets that seemed great in real life, but just look disappointing on a smart phone, and not-quite-Instagram-worthy snaps of restaurant meals.

To help you out, Apple allows you to search for pictures by who's in them, what they are of, or where they were taken. Google Photos uses its Face Grouping function to make 'sets' of images categorised by facial similarity. If you have concerns about privacy then, after you have used the grouping utility to find and delete what you need, go back into your Google account settings and disable the Face Grouping service.

Delete downloads and sort through folders

Our computers downloads folder can become like those cupboards some of us have where we just store all kinds of stuff we never look at, have forgotten about or didn't want to deal with at the time. Full of things you didn't really mean to download, stuff copied over or duplicated 'for safety', old installer

FRESH START

applications and attachments from emails saved by accident. Have a good look through, get rid of what you don't need, and save the rest to a password-protected external archive.

Do the same for all those 'Desktop Stuff', 'Miscellaneous' and 'To-Clean-Up' folders that we all drop files into to deal with later. The chances are they will be at least 50% full of screenshots anyway, and do you ever actually need those?

Doing all that may make you *feel* better but deleting unneeded credit card statements, medical files, tax forms and invoices will actually keep you safer. The goal is to help ensure that if your hardware is ever lost or stolen, and your data becomes compromised, hackers are limited in the personal information they can freely access. Consider backing up sensitive documents that you *do* want to keep onto password-protected drives or cloud services secured with multi-factor authentication.

Secure old and unused devices

Old external storage media like CDs, thumb drives, and removable hard drives that you don't use or need anymore (or that don't fit current computers) are a source of potential data breach if they get lost, thrown away or stolen. And the same is true for unused and out-of-date hardware. Personal computers with defunct operating systems, unsupported wifi routers, old gaming consoles can all store personal data about you which could be highly valuable for someone with criminal intent.

Even if you are simply thinking of buying a new computer, tablet, or smart phone to replace a fully working one it's essential you keep whatever sensitive information there is on your old device from falling into the wrong hands. The National Cyber Security Centre recommends using your device's

Clean up your digital debris.

Once you have decided what apps and accounts need to go and what can stay there are a few steps you can take to make sure you are starting out with a fresh approach.



Remove
unused data

Now is the time to delete any emails, photos and documents you don't need.



Clear your
browser

Clear your history and remove old cookies and unwanted extensions.



Archive
files

Relocate your most important files to a separate hard-drive.



Delete
old apps

How many apps do you have on your device? Are you still using them all?!



Disable push
notifications

Some notifications are useful, others are just a nuisance so get rid of them.



Scan for
malware

Start off with a thorough check for potentially harmful viruses.

Fig.1. Starting fresh with your mobile devices.



Erase all Content and Settings or Factory Reset features. Modern data-recovery software is highly efficient and easy to use, so take the time to make sure you have fully erased all the information before parting with unwanted hardware.

Before you start, back-up any relevant content you want to keep and then check your device for any removable storage. For computers, that means checking any internal drive ports like DVDs and USB ports for old or forgotten media, while gadgets, phones and digital cameras may have microSD

memory cards and SIMs hidden away inside them. Some older devices, particularly older digital cameras, may have internal storage too, so connect them to a computer one more time and delete (or better yet - overwrite) any existing files.

If you decide to use freely-available online software make sure it comes from a reputable company or trusted source. To be sure your devices are clean before parting with them the best option for most people is to either obtain some specialist data-wiping software from an IT security firm or take your hardware to a specialist who will clear it for you.

Clean up and clear out your email

Next, turn your attention to the applications, online services and cloud utilities you use every day - foremost among these will almost certainly be your email account. Your primary email (the one you use most often and/ or the 'recovery address' you have set-up to receive password reset emails) is, for many, their single most important online asset. It's also the account which, if compromised, would leave you the most vulnerable to hacking and identity theft.

”
The past can come back to haunt you... old online accounts can be weaponised against you if you forget about them.

Matt Burgess

Deputy digital editor, Wired UK



Primary email accounts usually contain information, not just about you and the businesses and services you use but about your friends, family members, colleagues and contacts too. Sorting through your hundreds of old emails and deleting what's unnecessary is a great way to manage the risks you'd face if your email was ever hacked. Use your email search features to hunt through old messages for anywhere you may have shared things like bank account details, social security numbers, tax forms or payment invoices. Consider tactically deleting everything from before a certain date, or everything from a particular contact.

If you need to archive and save any important, old messages onto a secure, password-protected external drive or hard disk most email clients and account providers (including Gmail, Yahoo, AOL and iCloud Mail) provide users with ways to export account data, so you can hold it locally while it is deleted from the company's servers.

Cancel notifications

When you install a new application you're probably eager to get it up and running to see what kind of job it can do, and how it could help or entertain you. At that early stage it's all too easy to just go ahead and give it the notification access it asks for, but it's not long before you have dozens of pushes every hour offering all kinds of discounts and special offers. Not only does this get distracting and irritating but it can create the kind of environment where you just don't bother checking properly everything that your apps are trying to alert you too. It can make it too easy to miss something important, like a security warning or authentication request, so open up your notification settings and select the apps you actually want to hear from. A good general-principle would be to only allow notification access to apps that will send you genuine messages from real people, or services that you need and use every day.



Step Two. What you don't need, delete.

Don't ignore all the old, unused accounts and apps you may have installed or signed-up to just because they may be difficult to find or annoying to delete. Dormant accounts can be a serious security threat. Don't forget - *your* data isn't usually saved on *your* device - it's more often located on the app or site-creators servers and, if they are hacked, it could be *your* identity that's in danger. Why risk a potential compromise of your personal data, financial information, or private files by leaving it lying around in forgotten places?

Managing old, unused accounts

Fashionable sites and services come and go (MySpace anyone?) and we probably all have expired, free-trials to streaming platforms and one-off accounts hanging around. Listed below, you'll find some useful resources and helpful tips designed to allow you to find, recover, and delete your unused, forgotten and unwanted accounts.

Finding everything you have signed up to

Start with the obvious ones; go through all the services you can easily remember. All those apps you can still see on your devices' home-screen or accounts that send you email reminders and push notifications.

Once you have done that use your email's search function to help find dead accounts. Searching for '*verify your email address*', '*welcome to*' or '*forgotten password*' and similar phrases found in the '*Welcome*' emails that many services send, may well reveal a few sign-ups you have forgotten about.

Then try searching in your web browser. Most search engine applications save the log-in details for websites you access and you should be able to find any accounts you've saved from the settings menu.

A good look through the *saved passwords* on mobile devices will perform a similar function and should serve to jog your memory as to what accounts you have opened in the past. Similarly, if you use a *password manager* (and you should definitely consider using one if you don't already) to help keep track of all your login details you will have a very effective database of all your current accounts. Finding old services this way has the added benefit of providing you with the necessary login details, too, in the (probably quite likely) event that you've forgotten them.

Below is a quick checklist of where to find the list of sites and services you may have signed-up to using a few of the most common third party accounts.

Apple ID On your iPhone or iPad go to Settings/ Password & Security/Apps Using Your Apple ID.

Facebook Go to Settings/Apps and Websites.

Google Go to myaccount.google.com/Security/ Third-party apps with account access + Signing in to other sites.

Instagram Go to Settings/Security/Apps & Sites

Twitter Go to Settings and privacy/Account/Apps and Sessions/Connected Apps.

Many websites and apps let you sign in with your Apple ID, Facebook, Google, Instagram, Twitter accounts, or similar third-party service. If you've used this feature check through the each of your sign-in services to see a list of sites linked to your account. Please be aware that simply 'disconnecting' the link between the two won't clear your data or terminate your account.

On a similar theme - please note that '*unsubscribing*' from a site or service is not the same as removing your account! Lastly, check through your physical journals, personal organisers, documents and secret stashes of notes for any login credentials, usernames or passwords you may have recorded.

Removing profiles and moving on

Now that you have found all your old accounts it's time to start closing down the ones you no longer want, use or need. It probably won't come as a surprise to learn that this is often a more difficult operation than the initial signing-up process. This is particularly evident when trying to remove yourself from mobile app accounts and subscriptions. You may think it's as simple as deleting the app from your device but you'll often need to use the browser on a desktop computer and log-into a company's main website to delete your profile.

Deleting old accounts. Why should you care?

You may well be asking yourself what could really happen if an old account you made gets hacked? You may have only used it once to watch a video or post a comment. Here are some of the top reasons why you should never leave forgotten pieces of your data lying around online. **Source:** techrepublic.com

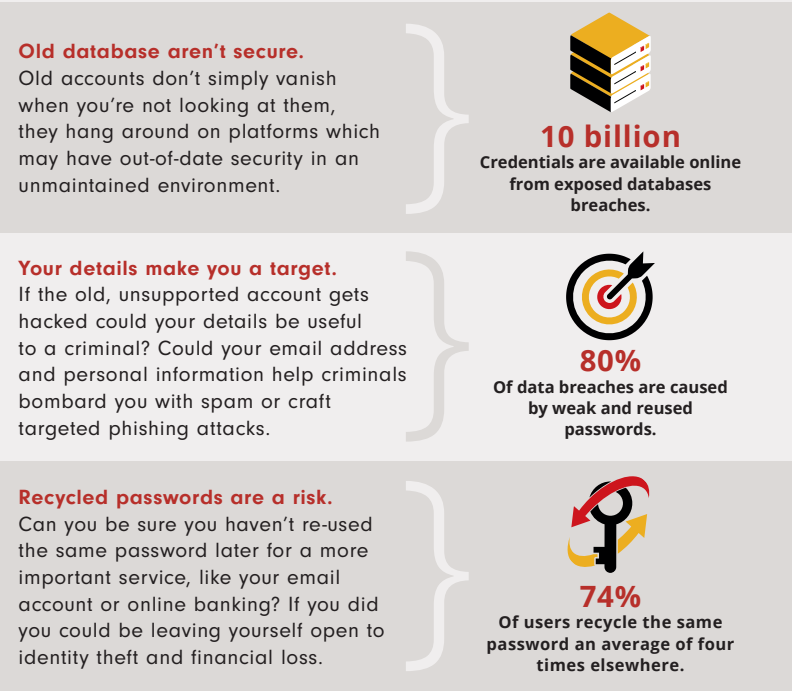
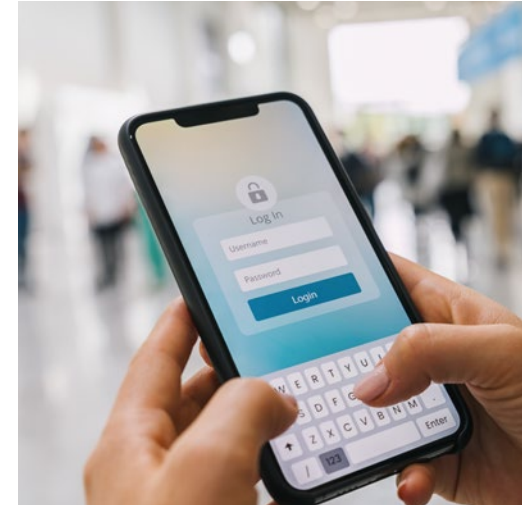


Fig.2. Why you should always delete old accounts.



Don't skip the 'zombie' accounts too!

The less data you have on corporate databases scattered across the internet, the more protected you are from the criminal or negligent misuse of your personal information. Even some obsolete platforms, like Myspace and Google+, have suffered data breaches that have affected millions of users who may not have used in years. An app or service that is discontinued or out-of-fashion is still live, so don't skip hunting down and deleting any profile or personal information you may have stored on it.



Read any instructions carefully, specifically when it comes to policies on data retention and privacy. It's possible you'll need to take some extra steps, like sending a follow-up email, before a company will completely remove your profile and accompanying data.

Deleting accounts

In each instance try the *Settings* page first as this is often where a site will put the *Edit* or *Delete* controls. If you can't find anything there and the process to remove your account still isn't clear then it's time to explore the *Help* menus and *FAQs*.

Do young people take online privacy seriously enough?

In a survey a group of 11-16 year olds born and raised with digital technology were asked about their confidence accessing and controlling a range of account settings on their social media profiles. Below are percentage breakdowns of some of their answers, along with an insight into prevailing attitudes to privacy and sharing. Source Market Research Society.

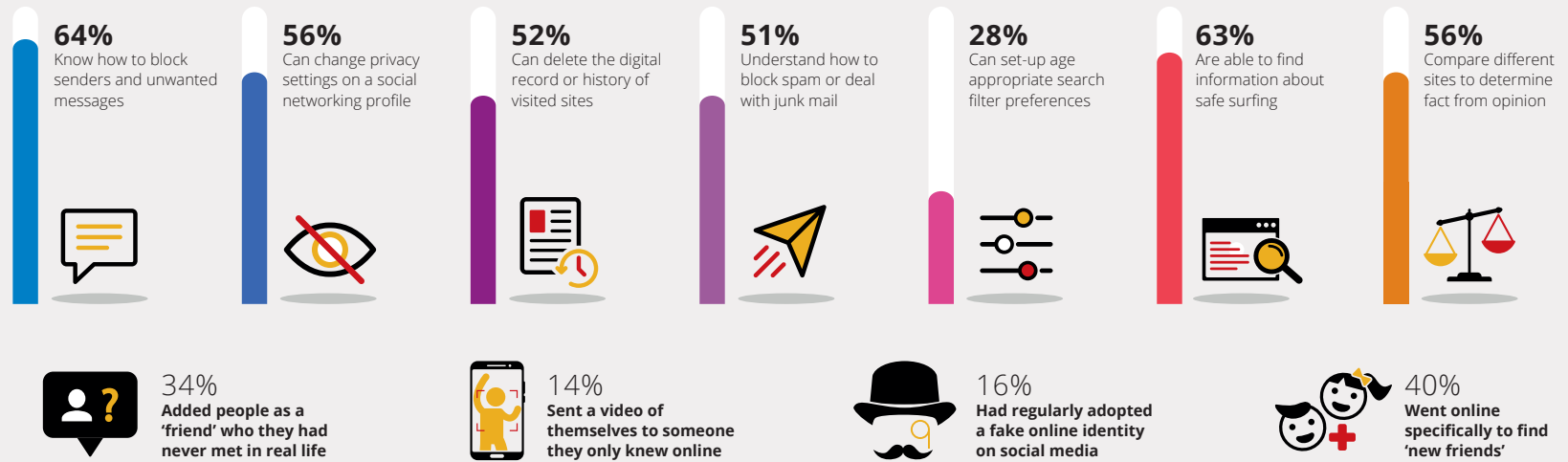


Fig.3. Do young people know how to stay safe on social media?

If all that isn't useful then try launching a text chat through the sites customer service links. They are often faster and more efficient than phone calls or emails.

If all else fails then take a look at the excellent online resource **JustDeleteMe**. It hosts direct links to the account cancellation pages on all of the most popular services. Click on the relevant link on JustDeleteMe,

sign-in to your account, and you'll be taken straight to the unsubscribing process. It has a large database of step-by-step manual instructions too.

Do be cautious if you're considering using a fully automated, online-tool to unsubscribe from services and apps as they can be untrustworthy. The site *Unroll.Me.com* was recently convicted of collecting users data and then selling it on to third-party companies...



Take advantage of local privacy laws.

Hopefully this won't be necessary, but if you are finding removing your information impossible you may have specific, local laws which are there to ensure your data is treated in accordance with your wishes. In Europe, for instance, The *General Data Protection Regulation (GDPR)* gives individuals the right to have their data permanently deleted, but each location has different rules and requirements so check the law where you live.

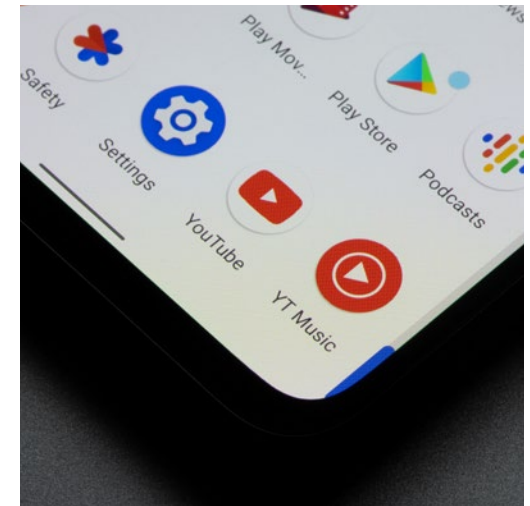
Step Three. Protecting your privacy.

Putting aside a short time to make a few simple changes to your devices and accounts will help strengthen your security against unwanted attempts to access your data and protect your identity. Companies and websites track everything you do online. Every ad you click on and website you visit is constantly collecting information about your location, browsing habits, and more. Where this data ends up is often outside of your knowledge and control so here are some tips on reclaiming your online privacy.

Is Google tracking your every move

If you are an account-holder and regular user of Google's products and services you may be one of the people who is increasingly unsettled by the idea that the company knows almost everything about your online life. The good news is there is a way to erase everything you have ever searched for on its site and stop it tracking your data.

Start by erasing your Google search history; open up the Google home page and log in to your account. Click on the circle in the upper corner (with your image or initials inside) and access *Manage your Google Account* from the menu that



Privacy, marketing and your data

Which companies are taking the best care of your personal information? The following is a breakdown of four of the top social media sites and what they deliver to their users in terms of data privacy. **Source** infographicjournal.com.





				
User can turn off location tracking	✓	✓	N/A	✓
Automatically support a secure connection	✗	✓	✓	✗
Limits profile visibility on start-up	✓	✗	✗	✗
Control how users can search for you	✓	✓	✓	✗
Control who can connect with you	✓	✗	✓	✗
Prevent users from tagging you in posts	✓	✗	✗	✗
Opt out of search engine indexing	✓	✗	✗	✓
Set log-in alerts	✓	✗	✗	✓
Automatically support a secure connection	✓	✓	✗	✓
Limit data-sharing with third party apps	✓	✗	✗	✗
Delete location information	✓	✓	✗	✓
Select advertising	✓	✗	✗	✗
Opt out of all advertising	✗	✗	✗	✗
Block other users	✓	✓	✓	✓
Chose who can see your photos	✓	✗	✓	✗

Fig.4. How is your data treated by four social media companies?

appears. Under the *Privacy and Personalization* category tap the *Manage your data and personalization* section and navigate to *Activity Controls*. Scroll down to *Activity and Tmeline*, and click *My Activity*. On the menu to the left of your screen you can now click *Delete Activity*. You can now choose how far back through your browsing history you would like to go.

Once you are done, head back to *Activity Controls*. From here you can choose to pause *Web and App activity tracking*, *Location History*, *YouTube History* and more. Turning these settings off will prevent Google from targeting you with personalised ads and stop it recording your search history. Follow this procedure every few months just to be sure further searches are not being archived.

Protecting yourself on social media

Sites like *Instagram*, *Facebook* and *Twitter* have made it easier than ever to share things online. But the act of sharing on social media is fundamentally different from using other types of digital communication. Unlike instant messaging or emails, which are designed to be privately distributed between a select group, things you share on social media are, by definition, much more public and easy to access.

All social media sites offer specific ‘privacy tools’ to help you limit who can see the things you post. Ignoring those settings means everything you share can be seen by anyone with an internet connection. You may feel that you have nothing to hide, so why should you limit your audience, but there are some good reasons for being a bit more selective.

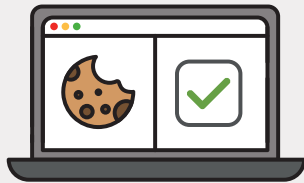
Are you sharing too much?

By ‘oversharing’ online you could be allowing identity thieves access to some very important personal information. Data as seemingly simple as the

What is **microtargeting**?

Electronic tools, like **Cookies**, track your browsing habits, likes and social interactions across the internet in order to build up a profile about you.

This profile is used to tailor advertisements to your specific interests in order to influence your actions or to sell on to data brokers.



school you attended or your pet's name could be enough information for a criminal to answer your 'security questions' and take control of your accounts. Once hackers have this information they can go on to potentially access bank accounts, set up credit cards, and carry out many other types of fraud, all in your name.

Using social media to hack accounts and

identities is now so common that it has its own name - *social engineering*. Rather than requiring a high level of computing skill, like the stereotype of 'traditional' hackers, social engineering relies on using your freely available personal information to win your trust and manipulate your behaviour.

The truth is that our accounts have been targets since the first social media sites were created in the early 2000s. We all hand over 'personally identifiable' information, like our date of birth and email address, in order to create a profile but should we be so complacent?

Setting privacy levels

Many users don't read the privacy policies on social media sites but you should research what, when and with whom your data is being shared.

Each of the major social media sites, like Facebook, Twitter, LinkedIn, and Instagram, provide ways to protect your account. By default they are usually set to the lowest confidentiality level so it's up to you to go in and customise them to be sure you are only sharing with the people you really want and mean to. To help you get started, here are some easy shortcuts collated to help walk you through the basics on three of the biggest platforms.

Facebook

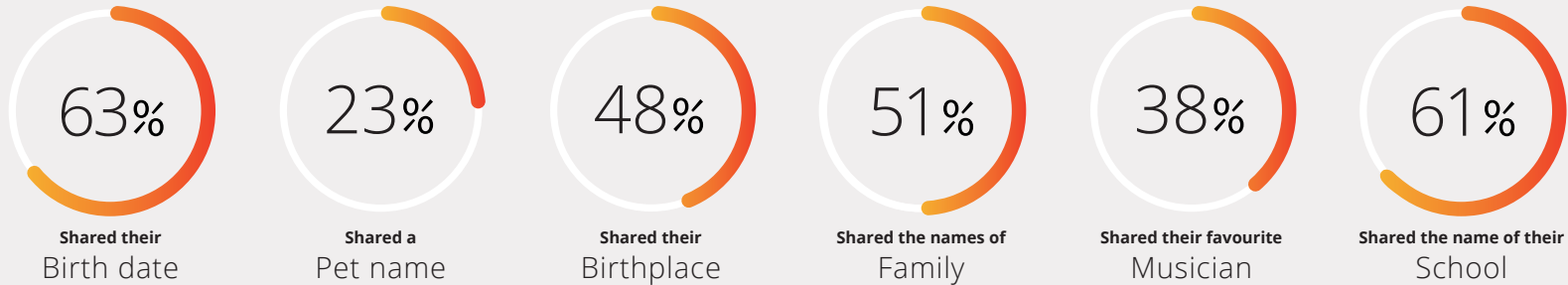
Log into your account and click the triangle in the top left of your screen to access '*Privacy & Settings*' and then '*Settings*.' In your settings menu, click '*Privacy*' on the left navigation list to bring up the management menu where you will find a number of options designed to help manage who gets to see what. To prevent strangers or hackers from gathering information about you, ensure only friends can see your posts by changing the settings in the '*Your activity*' section. You should also think carefully about turning off the '*How people can find and contact you*' option, which controls whether you appear in search engines. Turning this off will make tracking down your personal information much harder for scammers and hackers.

”
Google knows me even better than my best friend, because Google has perfect memory in a way that people don't.

Bruce Schneier
 Cybersecurity expert

Are you giving away the answers to your security questions?

Without being aware of it you may be sharing way too much personal information. Details of which could be used to answer many of the most commonly used security questions needed to access - and take control of - your online accounts. **Source** TrendLabs.com



Hackers who get access to this kind of personal information are in an excellent position to be able to leverage it for criminal purposes. The following statistics were gathered from a poll asking respondents about their own use of social media and also whether they, or those they know, had experienced crime because of it.



Fig.5. Could your security questions be answered by viewing your social media accounts?

Instagram

Instagram allows you to control who gets to see your profile. If you set your account to private, you will need to approve a person’s follow request before that user can see your photos, or see information about who you are following and who follows you. Your Instagram Stories are also affected by your profile’s privacy settings. For private accounts, only approved followers can see your story in their feed and from your profile. To access your settings,

log into your Instagram account, click on your *profile*, then on ‘*Settings*,’ and finally on ‘*Privacy and Security*.’

Twitter

The most important decision to make for Twitter users is whether you set your account to *private* or not. Private accounts only allow approved followers to read your posts.

Best advice for freshening up your social media.

Here are our top tips for cleaning up your social media presence, strengthening your privacy and getting ready to post more securely.

Find and remove spam, fakes, trolls and bots

Have a good look through your followers and delete any that don't adhere to the site guidelines, are abusive, look fake or are obvious advertising or spam bots.

Secure your accounts

If you have used any passwords on multiple accounts or sites then create fresh, new ones unique to each account. Enable two-factor authentication for added security wherever possible.

Make sure your posts reflect who you are

Many of us will have been posting and sharing for some time, and over that period it's likely we, and our views, will have changed. Check for, and delete, old posts that no longer accurately reflect your current opinions.

Update your privacy

You can decide what goes public and what stays private! Ensure you review the privacy settings on each of your accounts to limit exactly who can access what.

Create a social-media specific email address

If you are using the same email address you use for internet banking and online shopping for your social media accounts you may be making things easier for criminals. Consider making an email just for your social platforms.

Set yourself a standard for posting in the future

Make the messages you're putting out there positive and real.

Fig.6. Spring clean your social media accounts.

While this option may not be feasible for an organisation or business it's much safer for private individuals than having an open account.

The next set of options deals with advertising. Twitter is quite upfront about the fact that, by default, it will read your private information to target you with specific ads. If you don't want your data shared with advertisers keep this settings disabled. To reach and adjust all these settings just log into your account and click '*More,*' then '*Settings and privacy.*' In the new menu that appears simply click on '*Privacy and safety*' and the full list of preferences will be revealed.

Securing your social accounts

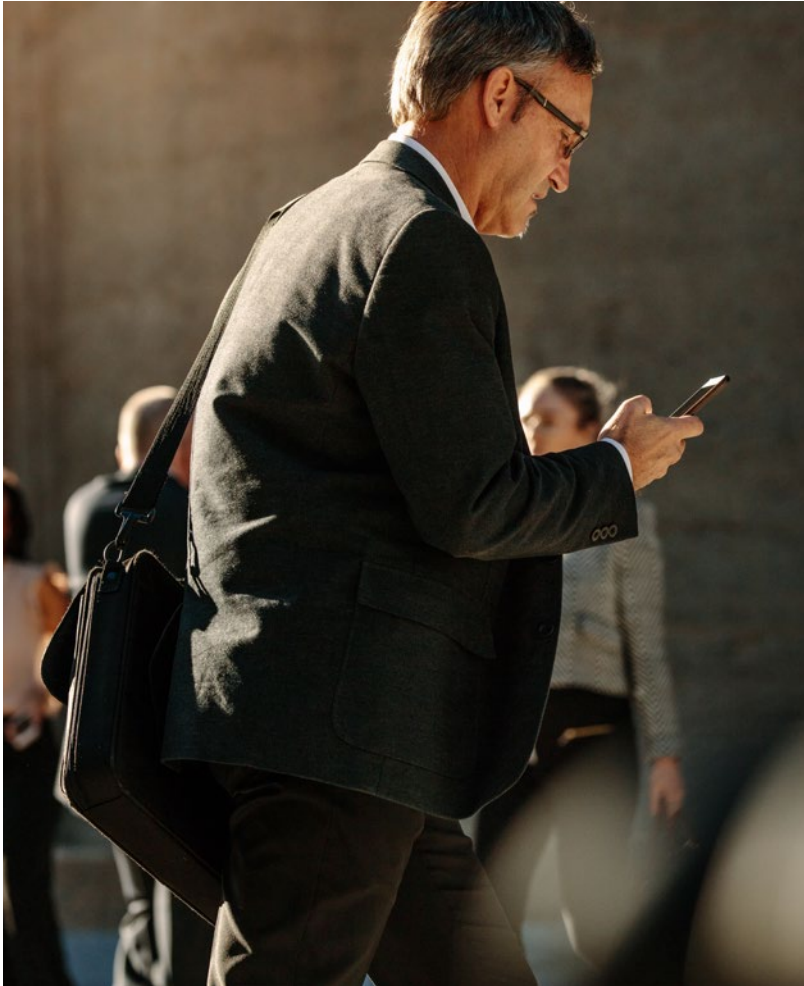
The best ways to protect your personal information when using social media are to use a unique, secure password, and set up two-factor authentication wherever possible. This will help prevent unauthorised access and also alert you if anyone does somehow manage to get hold of your password. Be cautious who you add as a 'friend' too. Don't forget - anyone you add becomes an 'insider' and will be able to see, and comment on, your feed.

You may be judged by what you post

Whether or not you are conscious of it, how you speak and act on social sites will affect how you are perceived by others. That's why you should always think carefully about what you share and post online.

Check third-party access to your accounts

You may well have allowed some online services like social media, music streaming, and online shopping, permission to connect to your Google, Facebook, Twitter, Dropbox, or Microsoft accounts. For example, you may



download an app that helps you schedule workouts with friends. This app may request access to your Google Calendar and Contacts to suggest times and friends for you to meet up with.

Sharing access like this can make your life easier and faster and, as companies like to say 'improves your experience', but may come with enhanced

privacy concerns. It's important to remember, for example, that every application you have ever allowed to connect to one of your key services keeps that authority forever, or at least until you revoke it.

You should only allow access to applications you trust and regularly use. If you don't use a service or application anymore, remove its access, just to be safe. The same is true if the company that owns an app changes hands, the new owners could have a very different attitude to your data and how it is stored and used than the model you initially signed-up for. If you learn that one of your favourite services has been sold, check the privacy record of the buyers and see if your terms and conditions have been altered.

You may have been using a single-sign-on service (like Microsoft) as a way to access third-party services for a few years. If so, it's more than likely you'll

”
Citizens would rebel if it were mandated that everybody carry a tracking device, but that's what is happening.

Stuart A. Thompson & Charlie Warze
 New York Times



have a long list of 'connected' apps that you no longer use. It's possible you don't really remember what reading and editing capabilities you may have granted those apps so, to secure your privacy, it's time to do some cleaning up.

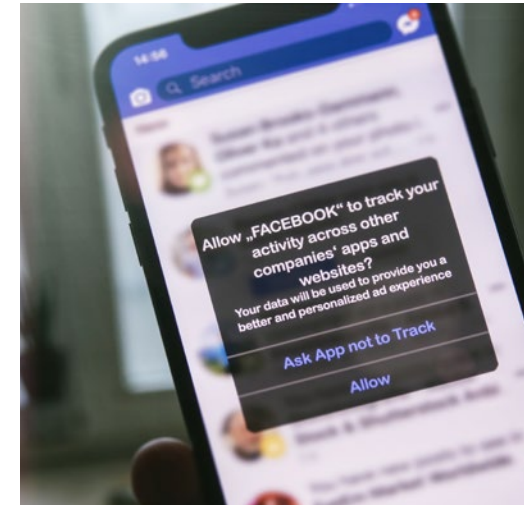
Again - this is something you are probably going to need a desktop computer for as some account options aren't available in the mobile environment. To secure your accounts visit the main website of the apps you use, log-in and check your list of connected services; viewing and managing these

permissions is generally done through the *Settings* and *Privacy* menus. Once in you can hunt through the list of connected services and revoke access to the ones you no longer want or need.

Mobile privacy

A recent *Statista* survey showed that average smartphone users have approximately 80 apps on each device. Almost all of these apps will request some sort of information about you and the device you are using. They may want to know your name, your email address or your exact location, some will even request access to your device's microphone and camera.

Whenever you install new apps, your device will ask you to confirm the app's exact access requirements. Think carefully about exactly why each service will be enhanced by allowing it to share your personal details. While you may be happy for a health tracking application to count your steps using GPS it may not make as much sense to allow the Android '*Brightest Flashlight*' app to know your location too! If you have doubts about the access an app is requesting search for a similar one with more reasonable requirements.



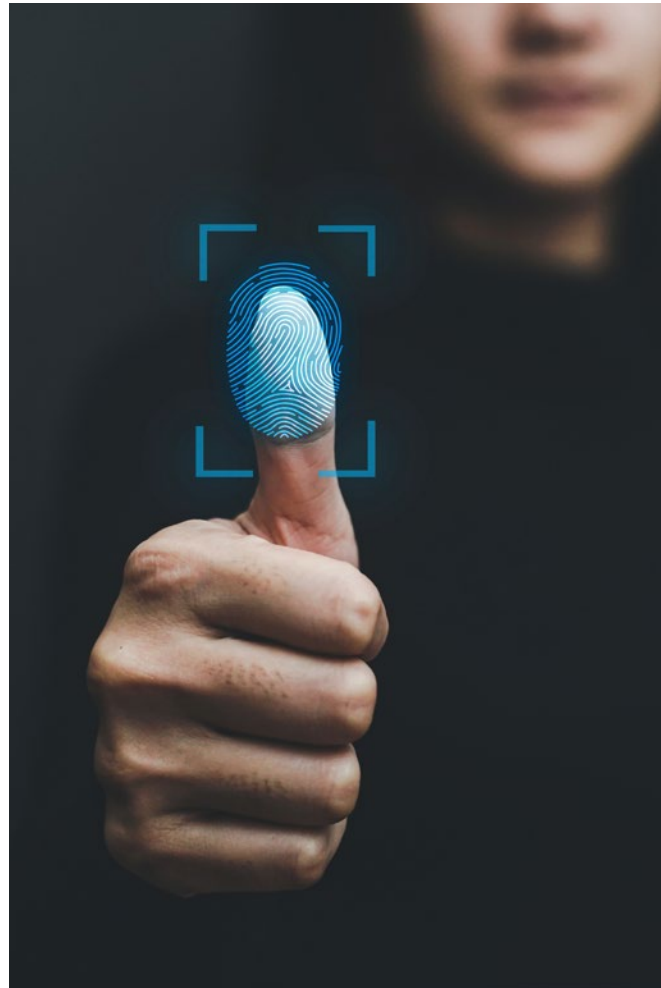
Step Four. Securing your future.

Hopefully the steps we've outlined will be of some use to you in protecting your identity and reclaiming some online privacy. If you have managed to work through even half of them you are well on your way to controlling how your personal data is collected and managed in a much more assertive way. In this last step we'd like to briefly discuss how you can keep the momentum going by performing a few simple actions that will help secure your online life as you move forward.

Use a password manager

The average person has 70-80 passwords to remember, and, as a result, many of us end up reusing the same old passwords or relying on passwords that are easy to remember, but equally easy to guess. And, while most people probably know that it's not a good idea to use 'password' as your password, or your birthday, it doesn't stop many of us from doing it.

But the worst thing you can do with your passwords is to reuse them across multiple sites. Many genuine hacks are due to what is known as '*credential stuffing*' - using stolen login names and password combinations



from one site to breach another. To combat these bad practices you should definitely look into getting a password manager.

Password managers will generate a complex, unguessable password for you whenever you need one and store all of them in one place - protecting them with a single master password. All you need to remember is your master password and the password manager will remember everything else.

Set up multi-factor authentication

If you are serious about strengthening your digital security and protecting your identity adding multi-factor authentication is one of the most important steps you can take. While no security measure can guarantee you never fall victim to a hacking attack enabling multi-factor authentication wherever possible is going to go a long way to locking down access to your most important accounts.

Multi-factor authentication works by adding an additional element to the log-in process. This requires two or more pieces of information (like a password and a one-time code sent by SMS) for successful entry to an account.

FRESH START

Consider using a virtual private network (VPN)

VPN networks anonymise your internet traffic (searching, uploading and downloading, email and so on) by layering it in encryption and routing it via a random relay. This makes it extremely difficult for sites to track you or to see where you're actually located. Some people may want to use a personal VPN as it adds a layer of security to your browsing. It can also provide some privacy from your Internet service provider and help minimize tracking based on your IP address.

Have you been 'pwned'?

Data leaks happen. It's an inevitable side-effect of our modern, always-connected world, and often these have nothing to do with you doing something wrong. Companies make mistakes, organisations get their servers hacked, individuals let information slip through human error and, unfortunately, that's just how it is. Due to no fault of your own, and in the face of your own best efforts, your data may be compromised (or 'pwned'). That being the case we are all fortunate that there are a few organisations in the world who make it their life's work to help mitigate the negative effects of cybercrime. One such entity is behind the website *haveibeenpwned.com*.

This site is an online resource which collates the stolen records recovered from thousands of known, mass-hacking events. Enter your email addresses into the sites searchable database regularly to reveal if your credentials have ever been hacked. If they have, take action immediately. Change the passwords and recovery information for relevant account as quickly as possible.

The last word

In the information age getting a handle on your own privacy and security matters more than ever. Your identity belongs only to you - so take care of it. ■





THE END.

© FIL Limited 2023.

Information contained in this booklet has been obtained by Fidelity International from public sources. Care has been taken by the staff of Fidelity International in compilation of the data contained herein and in verification of its accuracy when published, however the content of this booklet could become inaccurate due to factors outside the control of Fidelity International and this booklet should, therefore, be used as a guide only.

This booklet is published and distributed on the basis that Fidelity International is not responsible for the results of any actions taken on the basis of information contained in this booklet nor for any error in or omission from this booklet. Fidelity International expressly disclaims all and any liability and responsibility to any person in respect of claims, losses or damage, either direct or consequential, arising out of or in relation to the use and reliance upon any information contained in this booklet. Fidelity International means FIL Limited and/or its subsidiaries.

