



Resilience

Staying safe online

Contents

- 4** Types of Cyber Threats
- 5** Ransomware
- 6** Anti-Virus
- 7** Passwords
- 8** Updates
- 9** Windows 10
- 10** Public Wi-fi
- 11** Mobile Devices Tips & Tricks
- 12** Downloading apps
- 13** Social Media Security
- 14** Facebook
- 15** Twitter
- 16** LinkedIn
- 17** Instagram
- 18** Snapchat

Types of Cyber Threats

Cyber-attacks can come in a variety of forms. Targeted attacks are often more sophisticated, and it is harder to identify the attacker(s). Understanding the different types of attacks is key to defending against them.

- ❓ The identity of the attacker(s) is often unknown.
- 🕒 Users often do not know they have been attacked until it is too late.



Ransomware

Ransomware is a form of malicious software (malware) which aims to extort money by encrypting computer files and demanding a ransom for the decryption password.



- ₿ Usually, the ransom will be a few hundred pounds in bitcoin, a cryptocurrency.
- ⊘ Never pay the ransom. There is no guarantee you will get your files back!

Distributed Denial of Service Attack (DDoS)

A DDoS attack is a frequently used technique designed to flood the target with connections in order to overload a website or network. This brings down the service and causes a great amount of disruption, as the service cannot be accessed by clients or users. These attacks can lead to negative repercussions for a company as it can often prevent key business infrastructure from operating effectively.

Spear Phishing

Be wary of emails and documents asking you to send sensitive information such as usernames and passwords. If an employee falls for the “cat and mouse trick”, malware can infect a company's infrastructure and cause lasting damage to IT systems. It is important to educate your employees in identifying the key markers of a phishing email and what to do if they find one. Many phishing emails will have errors in them, which is done on purpose, to filter out the smart from the gullible. However, spear phishing attacks utilize target-specific details to make emails seem more legitimate. This technique is only applicable to a few targets at a time, as the process does require research into the target for it to be effective.

Malware

Malware is one of the most common threats to businesses and home users alike and can cause devastation if it successfully infects and spreads through a network. Malware is a computer programme purpose-built to damage infrastructure, spy on users, steal sensitive files, or lock all data and hold its owners to ransom. The latter is called Ransomware. Malware can infect devices in many ways, including: emails, malicious sites, infected documents and adverts on websites.

Web Application

Serious weaknesses or vulnerabilities in web application design can allow hackers to gain direct access to databases in order to manipulate sensitive data. This is one of the many damaging attacks that can be used to exploit a website. Many databases contain valuable information, including personal and financial details, making them a frequent target for hackers.

The identity of the attacker is often unknown. Users often don't know they've been hit until it's too late.

Attacks can come in a wide variety of forms. They can be very targeted towards a handful of individuals, or extend across a whole business, or even multiple businesses. Understanding these attacks is the first step towards securing yourself and your customers.

How can I protect myself?

Ransomware usually exploits known security vulnerabilities. Upgrading to Windows 10, and keeping it and your applications up to date, reduces the risk of malware infection.

Ransomware normally arrives via phishing. Take steps to reduce the chances of phishing emails reaching your staff. Implement technical countermeasures, like DKIM, SPF & DMARC. Train staff to be aware of phishing and how to spot it.

All staff should not be able to access all files. By limiting staff access to the files required to do their jobs, you can limit the impact of ransomware attacks.

Have a back up strategy

The best protection against a ransomware attack is a good back-up strategy. Remember to test your back-ups! The only thing worse than having no back-ups is thinking you have back-ups and discovering you have none or they don't work. We recommend backing up at least weekly. The back-up device should not be permanently connected to the device it backs up. Copies should be held off-site to insure against your office burning down or other man-made or natural disasters.

What to do if your systems are infected with ransomware?

Do not pay the ransom. There is no guarantee that you will get your files back. Report the incident to the police via 101 (ask for the cybercrime team) or via actionfraud.police.uk.


The website nomoreransom.org may be able to help you identify the strain of ransomware and provide the password for your files.

The police will not be able to help you with incident response, however the NCSC website (ncsc.gov.uk) has a list of certified incident response companies who can help you.

Anti-Virus

Anti-virus software is computer software which is designed to prevent a computer from malicious software, detect it and remove it if identified. Anti-virus software will attempt to quarantine or delete any file it deems to be malicious/suspicious.



 Anti-virus software will alert you to malicious files – it is, however, not perfect!

 Only download files/programmes from trusted sources.

Why do we need Anti-Virus?

Anti-virus software is very important as, in most cases, it is the only line of defence against harmful files/programmes.

Anti-virus software defends users against the likes of viruses, malware and other suspicious files which can be downloaded to their computers. These threats employ numerous techniques which can result in file theft/deletion, the downloading of further malicious material and even destruction of computer hardware in extreme cases.

It is crucial that, to maintain protection, anti-virus software is kept up to date in order to detect and remove new strains of viruses and malware. Most anti-virus software will automatically update as programmes may release updates as often as daily. It is always best to ensure that any anti-virus programme being used is configured to automatically check for these updates.

Anti-virus recommendations

In terms of protecting Windows users, the most readily available anti-virus software is “Windows Defender”. It is free and comes pre-installed on computers running Windows 7, 8 or 10. It should be noted, however, that “Windows Defender” is a rather basic piece of

of anti-virus software which does not offer a complete set of tools. This means that “Windows Defender” may not be able to protect users against all varieties of malicious files.

Users are therefore recommended to use “Windows Defender” alongside another third-party piece of anti-virus software to ensure maximum protection. These third-party options often come in both free and paid tiers, with the latter offering more comprehensive protection to users. Free anti-virus software includes AVG and Avast, whilst Norton and Kaspersky are among those which must be paid for.

Like “Windows Defender”, these third-party offerings are not perfect and can sometimes let suspicious and harmful files/programmes slip through unnoticed. As such, users should always be aware of what is happening on their computers and ensure that they are downloading files/programmes from reliable/trusted sources.


Equally, other operating systems, such as macOS, also have integrated security features to protect from viruses and other malicious software. macOS provides features such as ‘Gatekeeper’, which prevents the accidental execution of malicious software through validating downloaded applications before allowing them to run. Similarly, there are third-party offerings available from all popular vendors previously listed which can be used in conjunction with the pre-installed tools.

Passwords

Passwords are often our only line of defence against an attacker. Unfortunately, most people re-use the same password for most of their accounts. This re-use can have catastrophic consequences for the security of your online accounts.



 Use a different password for every account.

 Use a password manager to help you store and create passwords.

How do attackers obtain your password?

The most common method is finding it in data dumps from websites which other hackers have compromised. Attackers can also research you via social media and attempt to guess your password. Your dog's name followed by your year of birth (e.g. patch1969) is not a good password. An attacker can easily find out your dog's name and year of birth.

Password re-use

This is our biggest problem. Re-using the same password across multiple accounts will result in you having an account compromised. For example, you use the same password on your iCloud account and a travel forum. When the travel forum is compromised, your password is now public knowledge. The attackers will take the email address and password from the travel forum and try to log in to any service they think you use. Now, because you re-used your password, the attacker has access to your iCloud account.

Generating secure passphrases

A long passphrase is better than a short complex password. Rather than a single word with your year of birth after it and some special characters randomly thrown in, take 4/5 words and create a phrase or sentence. This will be much easier to remember. You can still meet complexity requirements by using punctuation which will naturally fit into phrases/ sentences.

Password managers

Password managers are special pieces of software which store all your usernames and passwords. Think of them as bank vaults. We store all our valuables in one very secure place, protected with a strong vault door. In this case, the vault door is your “master password” which unlocks your password manager. Anytime you need to log in to a site, you unlock your password manager and copy/paste the password into the website. Much more convenient than trying to look up the password in your little black book or trying to remember which variation of your password you used for a specific site. While this is an “all your eggs in one basket” approach, the basket is very secure. It is highly likely that you will be compromised because of password re-use. It is far less likely that your password manager will be compromised.

Updates

There are two kinds of updates. Those which fix security vulnerabilities and those which add new features. Sometimes these two are combined into one update. It is much harder for attackers to break into up-to-date software.



↓ Updates are free and easy to install.

🔒 Installing updates is the easiest thing you can do to keep yourself safe.

Windows 10



Windows 10 is the current version of the Windows operating systems. With Windows 10, there are different options available and to be considered when setting up a user account.

👤 Child accounts can be created to control which websites can be viewed.

💻 Windows 10 will be the last major version of Windows for 5 to 10 years.

Why do we need to keep our devices up-to-date?

Updates require very little effort to apply whilst providing protection against all current and publicly known vulnerabilities in the software. However, having the latest update does not mean that the software contains no vulnerabilities, only that all publicly known vulnerabilities have been fixed.

There are two kinds of updates: those which fix vulnerabilities and those which add new features of functionality. Usually, the updates which add features are released on an annual or biannual basis; updates which fix vulnerabilities are released sporadically, usually when vulnerabilities are reported.

The easiest way to stay updated/patched is to enable automatic updating whenever possible!

Updating desktops and laptops

We encourage all users of Windows computers to move to Windows 10 as soon as possible. It will be the last major version of Windows for five to ten years. As for Mac users, Apple supports the last two releases of macOS (10.13: High Sierra and 10.14: Mojave). If possible, 10.14 should be used, as updates will be rolled out for this operating system for a longer period.

Updating mobile devices

We advise that, if your Android device cannot be updated past Android 4.4.4, you upgrade the device immediately, and, if it cannot be upgraded to Android 7 or 8, you upgrade the device within nine months. The most up-to-date version of Android is version 9, with version 10 currently in development.

To update Android devices, open the 'Settings' app then:

System > Advanced > System update (Android 9)

For iOS devices, it is recommended to use iOS 12 - the most up-to-date version of the operating system.

To update iOS devices, open the 'Settings' app then:

General > Software Update

What options are available?

When creating a user account, there are two available options: a local account (an account that can only be used on the PC on which it is created) and an account tied to a Microsoft account. The latter lets users synchronize their settings between their various devices; simple tweaks made by users are often saved e.g. backgrounds and logged-in services such as Skype. The Microsoft accounts also allow for the use of family settings to be used on that account - this is not available on a local account.

Administrator accounts

Administrator accounts provide complete control of the operating system to the user and are only recommended for users with knowledge of advanced system settings such as Local Security Policies and Local Group Policies. not available on a local account.

Family settings

With creating a new profile, it can now be set as a children's profile. Once done, settings can be modified by logging in with the Microsoft account at:

<https://account.microsoft.com/account/ManageMyAccount?refd=account.microsoft.com&destrt=FamilyLandingPage>

This gives account holders the ability to control the amount of time that the account can be used for, what websites that can be viewed by the child account, being able to view the recent activity of the account (web browsing) and all of the apps and games that can be installed from the account via the Windows Store.

Public Wi-Fi

None of us likes being detached from the internet, especially when it's free! Public Wi-Fi can be a curse as well as a blessing. It is a potential gold mine of information from which attackers can gain information about you or your devices.

⚠ The security of public Wi-Fi should never be trusted.

👤 You have no idea who else will be on the network with you.



Mobile Devices Tips and Tricks

Mobile devices are a key part of our everyday lives, and so often contain a huge amount of personal data such as emails, texts, photos, and social media messages.

↓ Install any device or app updates as soon as possible.

☁ Back up device contents and enable encryption.



Turn off your Wi-Fi when not in use.

When your Wi-Fi is enabled on your phone or laptop, it will constantly be broadcasting information about wireless networks to which it has previously connected. Using this information, it is possible to track where a device has been. It is also possible for an attacker to sneakily connect to your devices by impersonating any of the networks to which you have previously connected, e.g. your home Wi-Fi. From this, an attacker could now monitor any internet communication from your phone or laptop: email, instant messaging and downloads.

Don't access sensitive data

Do not access any sensitive information (like online banking or work emails) on public Wi-Fi. If an attacker can gain access to the same wireless network as you, it is easy for them to then view a large majority of websites you visit; they could also redirect you to other - more malicious - sites.

Consider using a VPN

A "Virtual Private Network" (VPN) can also be used for extra protection on public Wi-Fi and mobile data networks. A VPN creates an information tunnel between your device and the VPN server, which then forwards your data to the websites you wish to visit. This means that everything you access over the internet will be encrypted and secured from public Wi-Fi; even if the site doesn't use HTTPS.

VPN providers charge for this service, however there are comparison charts available to find the best deal. Ensure, when looking for a VPN service, not to use the free alternatives, as they could do more harm than good.

What if I must use public Wi-Fi?

If using public Wi-Fi is an absolute must, ensure websites have a padlock at the address bar. This sends everything encrypted over a protocol known as HTTPS (where the S stands for "secure") and makes it much harder for an attacker to read on your end. Remember also to check the URL for each website you visit to ensure you are on the correct, official sites.

Use strong passwords and passcodes

Always use strong passwords that do not contain memorable dates or names. Adding a passcode such as a password, PIN, or pattern lock, to your device's lock screen helps to prevent someone else from gaining access to your device. Setting up your device's fingerprint reader or face recognition scanner (if your device has one) also allows for additional security.

Keep devices and apps updated

Ensure updates for mobile devices and apps are installed as soon as possible. These protect against security vulnerabilities and may also include additional performance and feature updates.

Back up device contents

If your device has a fault, or is lost or stolen, then it is easier to get a copy of your data if it is already backed up. Both iOS and Android offer built-in back-ups for saving a copy of your contacts, calendar and photos in the cloud, which can be enabled through device settings.

Enable remote tracking

Android and iOS both have built-in options for remotely tracking devices which can be enabled in device settings. This means that if your device is lost or stolen, it can be remotely tracked and erased.

Android:

<https://www.google.co.uk/android/find>

iOS: <https://www.icloud.com/find>

Enable encryption

Encryption prevents someone else from reading your data if your phone is lost or stolen. On Android, encryption can be enabled through the device settings via Settings > Security > Encryption. (Note that this varies slightly by device and version of Android.) Encryption is enabled by default on iOS and cannot be disabled.

Downloading Apps

As there are various mobile device manufacturers and each device often has its own operating system, app stores vary depending on the device. This means that the way in which apps are downloaded and the permissions are subject to change.



- ✓ Apps will ask for permissions to access different areas of your device.
- ✗ If you are unhappy with any app, remember you can always uninstall it!

Android

Android is an open-source operating system owned by Google which uses the Play Store to download apps. Android is the only operating system of the top three which runs on many manufacturers' devices (Samsung, Sony, HTC etc.).

After downloading an app from the Play Store, it will ask for various permissions on your device. These permissions allow the application - from that request until permissions are later changed - to access different areas of the device. The Play Store, although governed by Google, is not as secure as it seems.

iOS

iOS is a closed source operating system owned by Apple which makes use of the AppStore to distribute applications. The AppStore has stricter policies regarding what applications can be added to it; although the fact that the security is greater does not make it perfect. This must be kept in mind when apps are being installed.

If an app requests more permissions than are granted by default, a pop-up screen will appear. From there you can choose which permission(s) you want to enable or disable.

Windows

On a Windows mobile, apps are kept in a sandbox environment. This technique isolates apps and prevents them from interacting with one another unless you have given permission for them to do so. Apps are available to be downloaded from the Windows App Store.

App permissions

Application permissions that may be asked for include:

- Camera
- Microphone
- Contacts
- Send and/or receive SMS texts
Reads and/or writes to Storage (This one is common, allowing applications to create log files)
- Full Network Access (Allowing for Internet access over Mobile data or Wi-Fi)
Keeping the device active (Not allowing the device to sleep for extended periods of time when inactive could do damage to the battery.)
- Access to device accounts (This may also mean that they can access data stored in that account which may not be something you want.)

Many of these permissions apply to both Android and iOS but less so to Windows devices. When keeping track of app permissions, it is important to be conscious of what the app is meant to do. It is good practice, when apps need to ask for permissions, that they inform you why they need said permissions. This should help with the decision on whether or not to accept them.

It is also important to note that there are free and paid versions of apps available. Ads are common with free apps and are one of the main causes for malware to be downloaded onto the device. Reading the comments section before

Social Media Security



Social media allows us to create and share information, ideas, our career interests and other forms of expression through virtual communities and networks. Whilst it allows us to connect on a global scale, social media can also allow your information to get into the wrong hands.

- 🔍 New employers may research you via your social media.
- 💬 Think before you share. Too much information can make you vulnerable to hackers.

Posting in isolation

When you post on social media, it is typically a small update. Over the years, all these small updates start to add up. Attackers can piece together all these individual posts to build up their understanding of a person or business. Some of the biggest platforms, like Facebook, have been around for ten years. That is a lot of small updates!

Know what is public

Most platforms will allow you have a public or private account. Private accounts let you control who can see what you post. Facebook will let you share updates with everyone ("Public") or only with your friends. Review your privacy settings to ensure that you are only sharing updates with your friends. You can act like a stranger by using your browser's "Private Browsing mode" and navigating to your social media profile. Whatever you can see on your profile is what the public can see.

Multiple accounts

Most platforms now have the option of having a dedicated business account. You should utilise this feature to keep your personal profiles separate from your business. Business accounts usually have more powerful features for marketing and engaging with customers.



Facebook is the largest social media platform in the world with 2.32 billion monthly active user accounts. The idea behind Facebook is to allow users to share their events and experiences with an audience of their choosing.

+ Facebook also own WhatsApp and Instagram.

There are privacy settings. You just have to use them!



Facebook Messenger

Facebook also have their own messaging service. This service can still be used without an active Facebook profile. Users can choose to deactivate their accounts but still utilise the company's messaging service without a publicly accessible Facebook page.

Default settings

Every user on Facebook has his/her own profile. By default, people you are not friends with can view a preview of your profile. This includes: a limited selection of your photos, an overview of your profile information, your relationship status and your friends list.

Things to consider

Facebook is a great way to connect with friends and to share content online. However, your Facebook profile can also expose personal information to unintended recipients. This can range from current/future employees discovering inappropriate content to a malicious attacker using your profile to uncover personal details.

Posts

Posts made by a user can only be seen by "friends". Facebook allows users to alter this default setting, enabling them to configure each post's audience individually. This is a great feature, as it means you can alter the privacy settings of each post relative to its content.

Control your privacy settings

To configure your privacy settings on Facebook, navigate to the account settings. This can be found by selecting the tab to the right of the notifications icon. Within the settings page, there are several areas which can be adjusted to suit your privacy needs.

Who can see your posts?

The four main options that Facebook provides are: "Public", "Friends", "Only Me" and "Friends Except". For personal and private pages, you should use the 'Friends' or 'Friends Except' options to prevent any unwanted parties from viewing personal content. This ensures that only people you have chosen to connect with and share with can see what you post.

Who can look me up?

There are several ways to keep your Facebook account private. One of these is to prevent people from finding it in the first place. Facebook allows you to decide whether you want people to be able to find you by email address, phone number and search engines. Limiting these settings can help keep your account private.



Twitter is a social networking service that allows users to express their thoughts and opinions with 280-character posts known as 'tweets'. Twitter allows you to follow other users, tweet publicly or privately and send private messages to other users. Security settings dictate how much of your content other users can see and should be checked before using the social media platform.

Tweets are public to everyone by default.

The platform is used for discussing popular topics worldwide.

Profile

Each user has a unique profile that consists of their name, username, following/followers list, as well as a collection of the user's tweets, likes and retweets. Account usernames are used to directly 'mention' someone within a tweet; '@CyberCentreGM' for example. By default, Twitter profiles and tweets are public, therefore everyone has access to the content within them.

Tweets

A tweet is a 280-character post which appears on your followers' timelines. Users can respond to tweets in three different ways; retweet, like or reply. Retweeting shares a particular tweet on to your own tweet timeline, liking a tweet shows appreciation and replying allows users to respond to the tweet directly.

Hashtags

One of Twitter's main features is the use of the hashtag. The hashtag or '#' is used within tweets in order to relate the tweet to a certain topic; for example, '#CyberSecurity'. This feature allows people to follow specific events or discussions as well as being able to join in with their own tweets.

Posts

Users can decide to what extent their account is public or private. The three main options which should be addressed from the 'Privacy and Safety' tab in the settings menu are: 'Tweet Privacy', 'Tweet Location' and 'Direct Messages'.

Tweet Privacy decides on whether to reduce tweet visibility only to users who you follow back on Twitter instead of allowing everyone to view your account's tweets. Keeping tweets public is the default and, when changing back to a public account, please keep in mind that previously hidden tweets will be made visible to all.

'Tweet Location' will, as the name suggests, add a current location to your Tweets. This can be a precise location allowing anyone who can see the tweet to find you; vulnerable users should disable this feature. After disabling this feature, you are also able to remove existing location information from all existing tweets with the button situated below the tick box.

Finally, regarding Direct Messages, it is recommended that users should not allow these to be received from anyone, as is the case when this tick box is unticked. When this option is enabled, only users you follow can message you.



LinkedIn is a social media platform on which professionals can display their skills, connect with other professionals and search for jobs. "Connecting" with someone is similar to a Facebook "friend" request. This allows you to view greater detail about each other and to share private messages.



LinkedIn is the world's largest professional network, with 260 million users logging in each month.



Be careful who you connect with on LinkedIn!

Who do you connect with?

Do you know who all your connections are? Do not accept connections from users you don't know or do not wish to interact with. Avoiding these unknown connections will help keep you safe from potential online scammers. You may also want to examine your current connections and remove those that you don't know.

Multi-factor authentication

Multi-factor authentication can help protect your account. If an attacker is able to guess your password, they won't be able to successfully log in without the second log in step. This involves LinkedIn texting a unique code to you every time you log in to the service. To set this up, access the "settings" tab, under the "Me" option (on the right of the notifications icon on the navigation bar). This will take you to the "settings" page. From there, select the "Account" tab and you will find the two-factor authentication settings under the "Login and security" section.

Do you know what you're sharing?

By going to [linkedin.com/public-profile/settings](https://www.linkedin.com/public-profile/settings) you can choose what sections of your profile are available to users who aren't signed into LinkedIn. You can further check this by signing out of LinkedIn and navigating to your profile page, or by opening your profile in an 'incognito' or 'private' tab.

Phishing

It can be common for malicious users to send you private messages to phish you. Before accepting or reading them, ask yourself the following questions:

- Do I know the person?
- Do I trust them?
- Are they acting out of character?
- Why might they be asking these questions?

If you are unsure about the validity of the message coming from the user, contact them through a verified means of communication (call, text or meet in person). Double-checking the validity of a message will prevent you from falling victim to a phishing scam from a hacked or fake account.



Instagram

Instagram is a photo-sharing platform which can be accessed on multiple devices, the most popular being smart phones. Instagram provides users with the functionality to apply filters to alter the characteristics of their photographs.



Uploaded photos are public by default.



Users often apply filters to change how their photos look.

Getting started

To utilise the service, a user must sign up with their email address or phone number. From here, they can choose to "Follow" accounts of interest. On following another member, you'll be prompted with their "posts" in the feed sorted in chronological order. By default, a user's privacy settings are set to "public", meaning that any user accessing the platform, with an account or not, can view user profiles. A user may change this to "private", meaning that people who they accept to be followed by can access the content on their account.

Instagram for business

Having an Instagram account can aid your business' marketing reach by keeping the public up-to-date with your company's current affairs. If a company wishes to sign up as a business account, this must be enabled in the "settings" section of the user's profile in order to access more business features, such as advertising, statistics and more. To aid the cross-posting of content that may appear on Instagram, a business may also wish to link their other social media such as Facebook, Twitter or LinkedIn.

Businesses may use Instagram's "moderation" feature to block a series of given phrases they may deem inappropriate to be displayed in the comment's section.

Be aware that anyone posting anything to Instagram grants Instagram and Facebook a royalty-free, transferable licence to use that content in any way they choose. This includes the right for them to distribute, modify, translate, copy, perform and create derivate works of your content.

Privacy and settings

When using Instagram, the platform will automatically collate data regarding behaviour on the platform, along with the access of device-specific content such as contacts and pictures. Instagram states, when a user begins using the platform, that their data will in fact be collected and used for marketing purposes.


You can set your account to be a 'private account', meaning that only users you approve can see the content you post. Be aware this only effects users going forward, as existing followers will still be able to view content available on previously public profiles. If you do not want existing followers to have access to posts, you must block them.


Business profiles cannot make their accounts private.

For added protection, you can enable Two-Factor Authentication on your account, either through SMS message or through an Authentication App, such as Google Authenticator. Payments through Instagram can be further protected by adding a Security PIN which can be used when making purchases.



Snapchat is a photo-sharing social media site built for mobile phones. It encourages instant or "as it happens" sharing, with photos taken throughout a person's day. This appeals to younger people, and to businesses targeting a younger demographic.

 Snaps are meant to be temporary.

 Snaps can be saved without your knowledge!

Temporary Images?

Snapchat's USP is that images are "temporary". When a 'snap' is sent to someone, it has a timer on it and the recipient may only view the image for a few seconds.

Snapchats last for 30 days in the app before they are deleted and at least 30 days from the time they are opened on Snapchat's systems. Snaps added with the 'our story' feature can remain viewable for up to 90 days.

If the receiver screenshots a snap, the sender will receive a notification. However, there are multiple ways to capture a sent image without the sender even knowing.


Who can snap me?





By default, only people in your friends list can, so be careful who you accept as a friend. Additionally, anyone with your username or your phone number can add you on Snapchat. Snapchat will also suggest people you may know based on your "friends".

Snap Map

Snap Map is a feature on snapchat where you can see all your friends' locations. This feature is off by default. You can also add a story using a feature called "'our story'", which ties a snap to that location, and anyone viewing the map can click on your location to view the story. If enough people add to this, then it is more visible on the map.



 Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

 01786 447 441
 enquiries@sbrcentre.co.uk
 www.sbrcentre.co.uk
 @SBRC_Scotland

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27