ONLINE SAFETY

Rotherham ageUK

THE SAFER ROTHERHAM PARTNERSHIP

RNN GROUP

NHS

Voluntary Action Rotherham

Rotherham Federation

Believe in children Barnardo's

ROTHERHAM DIGITAL

Rotherham Metropolitan Borough Council

USING THE INTERNET

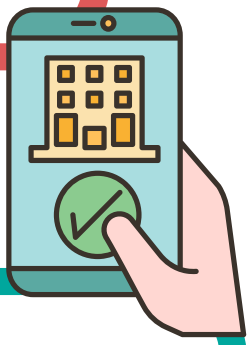
Looking at how the digital world is changing the way we live and with the emergence of new apps and games every day can make the internet feel overwhelming, but there are actually only a limited number of functions apps can have.

VIEWING
Such as streaming movies on Netflix or watching YouTube

SOCIALISING
Such as messaging or using social media such as Facebook or forums

PLAYING
Such as online games or going online through gaming consoles

LEARNING
Such as online courses for learning new skills or hobbies



SHARING
Such as social media sites like Instagram or online blogging

HOUSEHOLD ADMIN
Such as online banking, ordering the weekly shopping, etc.

What are the top 3 things you do online, or would like to be able to do?

1 _____

2 _____

3 _____

ONLINE RISKS

The Internet is one of the greatest inventions in the world and provides people with instant access to endless possibilities – you can buy your weekly shopping, stay in touch with friends across the world, learn new skills, search for a job, book a holiday or just play a game or catch up on your favourite TV shows.

It's important to remember the positives of the world online and not allow the potential pitfalls to put you off.

It can be difficult identifying and managing online risks as there is so much information and it can feel overwhelming - hopefully this will give you some practical tools to help you feel confident in using your judgement on any app or site.

DIGITAL FOOTPRINT

Your digital footprint is the data that is left behind when you have been online.

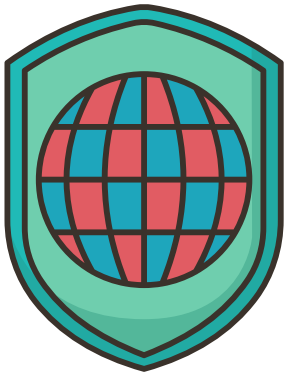
With every new profile, photo or comment you post, you add to a trail of information about yourself which stays online.

When you see an advert on social media for a product you were looking at the day before - that's your digital footprint that has led you there.

In recent times, several celebrities have been in trouble now for things they have posted on social media, even if it's a long time ago. More and more employers are also looking online to see what a potential employees digital footprint shows.

It's important to remember when posting anything online, it has the potential to be seen by anyone, as clearly as a footprint in the snow.

PROTECTING YOURSELF ONLINE



Whilst there are specific ways to protect yourself when carrying out certain activities such as gaming or shopping online, there are also some general ways in which you can minimise the risks of the internet.

CREATING STRONG PASSWORDS

One of the ways in which you can protect your online interests is to create strong passwords. It can be difficult to keep track but many devices will store passwords for you such as Apple Keychain. The key is to make your passwords memorable but not so obvious that they can be guessed, such as using a name and date of birth.

- Don't use the same password for multiple websites
- Include a mixture of upper and lower case letters, symbols and numbers
- Don't share your password with anyone
- Change your passwords regularly

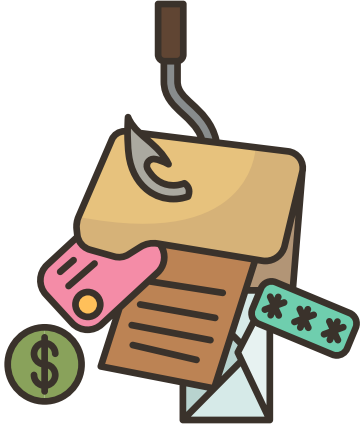
KEEPING YOUR DEVICES SECURE

You can minimise online risks by adding security programmes, keeping your device up to date and only downloading apps from the official iOS and Android app stores.

Make sure your devices are up to date – older computers/devices are more vulnerable to hacks and viruses

Install security updates as soon as possible – you will usually receive a notification that an update is available

Look at installing additional security programmes such as anti-virus to further reduce risks



ONLINE SCAMS
WHAT TO LOOK OUT FOR

Online scams are becoming harder to spot and can often catch out even the most savvy internet users. Unknowingly sharing personal or financial information sees millions of people lose money in the UK alone every year.

Some of the most common scams include:

Email scams
Bogus emails sent in the hope that you will enter personal or financial information which may include links or files that could harm your device or direct you to fake websites.

Computer viruses
Sometimes called malware, these are rogue programs that spread from one computer to another and may be sent to you as a link or email attachment which will release a virus when you click on it.

Phone scams
Criminals impersonate legitimate organisations as a reason to contact you and use this to trick you into making payments and accessing your personal and financial information.

Fake websites
Created by scammers to look official, requesting personal or financial information or offering a service for a fee which is available free elsewhere.

Health scams
False and misleading claims may be made about medical-related products, such as miracle health cures, and fake online pharmacies may offer medicines cheaply but may be poor quality and potentially harmful.

Relationship scams
through social networks or dating sites, scammers may try to gain your trust and then use this to extort money from you.

NOTES

ONLINE SCAMS
HOW CAN YOU PROTECT YOURSELF?

There are ways in which you can make it more difficult for fraudsters to get away with online scams

- Be wary when opening emails from senders you don't recognise
- Don't click links in emails unless you are sure they're legitimate – if in doubt, open a webpage and google the site you need to visit
- Don't give personal details over email – banks will never ask you to confirm your personal details or account details via an email
- Ask yourself if this could be fake, take a moment to stop and think before parting with your money or information – it's ok to reject, refuse or ignore a request received online, only criminals will try to rush or panic you
- If you receive a request through a friend or an organisation then use other means to contact them and verify the legitimacy of the request before you pass on any personal or financial information

SHOPPING SCAMS

Only make payments using secure payment options.

Check the URL of the website begins with https instead of http. This means the site is secured using a TLS/SSL certificate which secures your data as it is passed from your browser to the websites server.

Look for trusted payment options such as PayPal, Apple Pay and Google Pay.

Where possible, use a credit card when making purchases over £100. This provides protection under Section 75 of the Consumer Credit Act and could help you get your stolen money back.

If you think you have been a victim of a scam then contact your bank immediately and report it to Action Fraud

Visit: www.actionfraud.police.uk Telephone: 0300 123 2040

SOCIAL MEDIA

Social media is a great way to stay in touch with people, catch up with long lost friends and make new contacts - adults who use social media have been found to have increased social support and greater life satisfaction. But there are risks, particularly in terms of what you might see and how much personal information you might share.

Any app that allows you to message and interact with others is classed as social media - Do you know these popular social media apps?

What are the risks on social media?

Cyberbullying
Although this is often associated with children and young people, it can happen to anyone.

Cat Fishing
When someone sets up a fake online profile to trick people, often through dating sites, usually to get money out of them.

Online Grooming
The presence of strangers online means there is a risk of grooming, this could be for exploitation or radicalisation.

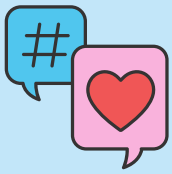
Identity Theft
There is a risk that someone could clone your profile or use your personal information to impersonate you or misrepresent you online.

Seeing offensive or upsetting images or messages
Most social media apps use algorithms to decide what content you see and this can make it difficult to manage what you see online.

Invasion of Privacy
Social media platforms can be vulnerable to data breaches which could expose your personal data or some may allow third-parties to access user data.

Phishing
When criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer or steal your personal information.

Misinformation, misused information or malicious content
There is a lot of information circulated via social media and it can be difficult to know what is real and what is either fake or displayed out of context.



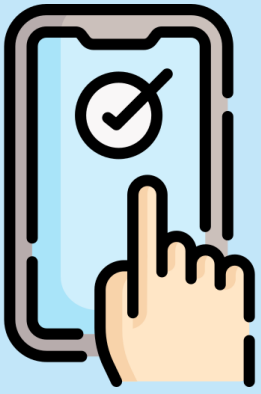
There are many positives to social media - don't be put off by the potential risks, there are ways in which you can manage your settings and minimise these risks.

Keep social media profiles private – only allow friends you have accepted to see your posts and be aware of other people tagging you in social media content, you can amend automatic tagging in the settings on most social media apps.

Avoid sharing personal information like your phone number or address and check the background of photos – does it show people where you live or where you work?

Remember that anything you post has the potential to be seen by anyone so if you're going on holiday you might not want to let the whole world know your house will be vacant for a week.

Check your settings on social media apps for filters which will allow you to modify what content is automatically shown – particularly important when children and young people are using social media.



How to report a problem on social media

If you see something online which you find upsetting or harmful then you can report it.

Most social media sites offer you the tools to report posts which are offensive or upsetting. This can usually be found by clicking on the post

Report Harmful Content is a website which helps guide you through making reports to certain apps or websites on any of the 8 harms (Threats, Impersonation, Bullying & Harassment, Self-harm or Suicide, Online Abuse, Violent Content, Unwanted Sexual Advances, Pornographic Content).

There is also a way to make the report direct to them if you are not getting a response to a report you have made.

https://reportharmfulcontent.com/

NOTES

ONLINE GAMING

Playing electronic or video games on devices such as Xboxes, smartphones or computers is known as online gaming. Online gaming appeals to people of all ages and whilst it can be a fun and sociable activity, there are some risks to be aware of and measures you can take to minimise these risks.

What are the risks of online gaming?

Talking to people you don't know
Many games allow users to interact with others online through competitive or cooperative play, as well as communication features to allow more sociable interactions.

Online bullying
Can happen across any kind of app, game or website where there is interaction with others

Griefing
Deliberately spoiling other players' enjoyment of a game by playing in a way that is intentionally disruptive and aggravating

Trolling
Sending malicious, abusive or derogatory messages to another user online with the intention of upsetting or harassing them or damaging their reputation

Risk of losing money
Scammers can target online games and there can be hidden costs through in-game purchases

Online gaming can be addictive
You might be concerned about how much time you, or someone you know, is spending on gaming.

There are also benefits for online gaming

Can develop critical and creative skills

Is available to all audiences and family members

Is an accessible way to socialise with others

Can bring educational benefit and awareness

Minimising the risks for online gaming

Use strong passwords on gaming accounts

Don't share any personal information while gaming, stick to usernames

Only download and play games from trusted sources

Pick an anonymous username – this can avoid having your online games linked to the digital footprint associated with your real name

Enable Multi Factor Authentication (MFA) – this is usually a code sent to your phone to verify it is you when logging in

Keep your gaming software updated as these can include security patches that fix known vulnerabilities

Use a credit card to make purchases if possible as these offer more protection from fraudulent charges

If someone is acting suspicious or aggressive – block them!

Some of the most popular online games

The Sims, Apex Legends, Call of Duty, Minecraft, Fortnite, Roblox

How can we help young people stay safe gaming online

Whilst online gaming appeals to all ages, it is especially popular with younger people and there are certain risks which they can be more vulnerable to. There are ways in which you can help children and young people stay safer while gaming:

Reporting, or encouraging them to report harmful or offensive content online

Have active and open discussions around gaming and socialising online

Learn about in-app purchasing and check if there are hidden costs

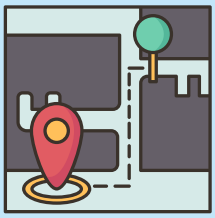
Look at the age restrictions on games and see if they are appropriate

LOCATION SETTINGS

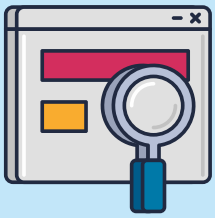
Your location refers to where you are and devices often track this in the background even when you don't have internet or reception using GPS. These location-based services are found on most smart devices including phones and use technology to pinpoint the location of your device, and therefore you!

Your location can be used in lots of different ways

Checking in on social media



Using maps to get directions



Online searches for things nearby such as shops

Risks of sharing your location

Some apps will allow you to share your location with friends and family but this could also mean you're sharing this information with people you don't know.

Checking in at home tells people when you are home but also where your home is, which can be dangerous. This is the same for checking in at a friend's house or at school.

Some apps will also reveal your live location (where you are at that moment) and if you often check in at the same places it could allow someone to know your usual movements.

It's important to also remember the positive side of the internet and this includes the positive ways in which location settings can work.

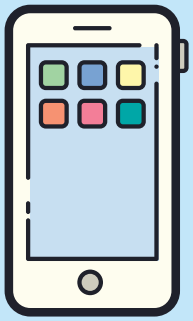
Your location can help you find something nearby or check the weather before you head out just be sure you are very clear on why and how your location will be used, how long for and who can see it.

How can you manage what you share?

Some apps, like map apps, will need to know where you are to work properly, but others (social media and most games) do not need this information. You can manage how your location is used and shared in your privacy or general settings on your device and on some apps.

Device settings

You can disable location settings completely or switch location settings on or off for individual apps – usually found under general settings on mobile devices



App settings

You can manage privacy settings on social media sites such as Facebook and on gaming accounts to check how your location might be shared

Social media and other accounts are often linked which can mean your location is available on a public account – make sure all your social media accounts are only visible to trusted friends!

What if someone else shares my location?

The best thing to do would be to ask them politely to remove the post or the location information or you can remove your tag so you're not linked to the post.

You can also use your own privacy settings to manage how visible you are in other peoples posts and require them to be approved by you before they are public.

- **Use privacy and account settings on devices, apps and games to manage your location sharing.**
- **If you want to tag a photo or event in a particular location do it later so you're not sharing a live location.**
- **Avoid checking in regularly from the same locations or marking tagged locations as things like 'work' and 'home' as this can give people a picture of your movements and lead to safety concerns.**
- **Watch out for friends who may accidentally post your location information or use privacy settings to limit or prevent tagging entirely.**
- **Make sure all linked accounts are only visible to friends you know in real life.**

QR CODES

You might have noticed these black and white codes popping up more and more. They work like a barcode and are a scannable image that can instantly be read using a Smartphone camera.

When your camera scans the QR code, you'll see an icon or web address on your screen near the code. When you tap that, you'll automatically go to the associated website via your phone's web browser. They can be very handy and save time when you want to look at something without having to type in a long website address.

Where might you see a QR code?

on adverts, in magazines or newspapers and any place where you can make contactless payments such as car parks and restaurants

Have a go at scanning this QR Code

SCAN ME

(Don't worry, we've checked this one out)

NOTES

QR codes are convenient and easy to create and scammers can potentially replace legitimate ones with their own fraudulent codes. These "fake" QR codes redirect you to malicious websites designed to steal your sensitive information.

What to look out for to minimise the risks of QR codes

Check that the QR code hasnt been tampered with, replaced or covered up by a fake code on a sticker.

If you do visit a link via a QR code, check the site is authentic before giving any details - such as looking for bad grammar, poor design, an odd or misspelled website address or missing the websites branding.

Be vigilant about codes located in an unusual place, on an item that can be easily moved or stuck to the table, possibly covering the genuine code.

Only use your phones camera to scan a QR code - scammers have created fake “scanning apps” that install malware on your device when you download them. This malware is designed to steal users' credentials and access their accounts.

Be cautious of any QR code that is sent in an email. While most email services can detect and warn you of malicious links and attachments, they can’t do the same for malicious QR codes. Even if you receive an email from a friend or contact with a QR code embedded in it, be wary. Scammers can use hacked email accounts to launch phishing attacks from recipients who you’re more likely to trust.

This is also true for QR codes sent via social media messaging which may look like they’re from a friend but could be a hacked account. One of the most common ones you may have seen is the message that starts ‘I found this photo of us..’

ONLINE SHOPPING

Online shopping can be a convenient way to find better deals, shop from the comfort of your home and find products that might not be available in local stores. For some people, online shopping is a necessity. There are risks when online shopping but you can protect yourself.

Risk of fraud

If you're shopping online, there's a larger risk of fraud and this is a key concern for most people. Credit card scams, phishing, hacking, identity theft, counterfeit products, bogus websites, and other scams are common but you can minimise these risks by ensuring you use secure websites when submitting personal information.

Protecting yourself online shopping

Look out for the following things to help protect yourself from online fraud

The address starting with 'https'

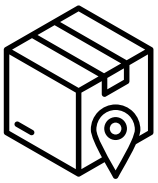
A padlock symbol in the URL bar at the top

An up-to-date security certificate

Ensure that the online shops you're visiting are genuine - be on the lookout for 'copycat' sites

Read online reviews of the site and avoid anything that seems too good to be true.

Other potential risks of online shopping and how to minimise them



Shipping Problems

Most websites have a help section which will allow you to contact them to discuss any issues with shipping and for more expensive items you can usually select protected postage such as signed delivery.

Returning Items

Sometimes items need returning and it can be an easy or a complicated process. It's always worth looking at return policies on the website before you place an order.

USEFUL INFORMATION

The internet is always evolving and as it does there are new risks emerging and new security measures that you can put in place.

Lots of websites offer useful information and are updated regularly, these are a few we can recommend

UK Safer Internet Centre

Safer Internet Centre
https://saferinternet.org.uk/

internet matters.org

Internet Matters
www.internetmatters.org

age UK

Age UK
www.ageuk.org.uk

STOP! THINK FRAUD

Stop! Think Fraud
https://stopthinkfraud.campaign.gov.uk/

GET SAFE ONLINE .org

Get Safe Online
www.getsafeonline.org

National Cyber Security Centre

National Cyber Security Centre
www.ncsc.gov.uk

NOTES

GLOSSARY

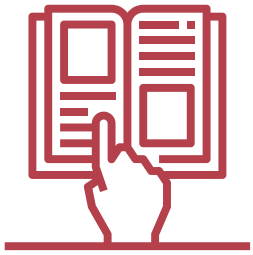
There’s lots of jargon on the internet - these are some of the key words and phrases

Apps (applications)

A type of computer program that you can download for your computer, tablet, or smartphone. You should only download apps from trusted places such as the Google Play Store if you have an Android phone or tablet, or the App Store if you have an Apple device.

Bluetooth

Bluetooth is a type of wireless technology used to connect one device to another – for example, connecting your phone to a speaker to play music.



Cat Fishing

When a person takes information and images, typically from other people, and uses them to create a new identity for themselves, usually to trick people and get money out of them.

Cookies

A cookie is a small piece of data that's stored on your computer, smartphone or tablet when you visit a website. Most websites pop up with a message asking you to 'accept cookies'. Cookies allow the website to track information about your activity on the website, such as how many times you've visited and how long you spent on the website. You don't have to accept cookies, but it might mean that you can't access some websites.

Cyberbullying

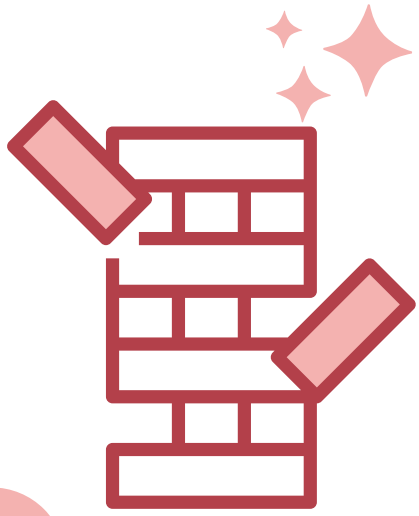
This describes lots of different kinds of online abuse including but not limited to harassment, doxing, reputation attacks and revenge porn.

Cyber Stalking

This is the act of repeatedly sending messages that include threats of harm, harassment, intimidating messages, or engaging in other online activities that make a person afraid for his or her safety. The actions may be illegal too depending on what they are doing. Similar to harassment, cyberstalking involves the perpetrator making persistent efforts to gain contact with the victim, however this differs from harassment – more commonly than not, people will cyberstalk another person due to deep feelings towards that person, whether they are positive or negative. Someone who is cyberstalking is more likely to escalate their stalking into the offline world.

Doxing

When an individual or group of people distribute another person's personal information such as their home address, cell phone number or place of work onto social media or public forums without that person's permission to do so.



Flaming

This is when someone is purposely using extreme and offensive language and getting into online arguments and fights. They do this to cause reactions and enjoy the fact it causes someone to get distressed.

Griefing

Online gaming term - deliberately spoiling other players' enjoyment of a game by playing in a way that is intentionally disruptive and aggravating

Hacking

Using a computer to access information stored on another computer system without permission, or to spread a computer virus

In-app Purchases

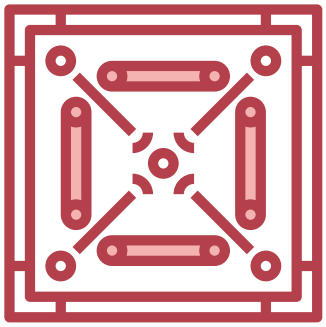
Extra content or subscriptions that you buy inside an app.

Malware

Malware is short for 'malicious software'. A general term describing software that can cause harm to your computer through spreading computer viruses or accessing your personal information.

PII – Personally Identifiable Information

Including names, middle names, date of birth – any information that can identify you



Spam

A commercial email that you didn't request, also known as 'junk mail'.


Rotherham
ageUK

THE SAFER ROTHERHAM
PARTNERSHIP

RNN
GROUP

Rotherham
Metropolitan
Borough Council

Voluntary
Action
Rotherham

Rotherham
Federation

Believe in
children
Barnardo's

ROTHERHAM
DIGITAL

NHS