How to reduce your chances of becoming a victim

There are a number of steps you can take to reduce the risk of cybercrime:

- when creating passwords, use three unrelated words, eg fishbooktable; and think of three different words for each account. This means that if one is compromised the others are safe
- never give personal or sensitive details out online or over email
- make sure all devices have up-to-date anti-virus software and a firewall installed
- keep software and apps regularly updated
- only download from legal, trusted websites
- only open emails and attachments from known and trusted sources
- only ever use websites that start with https://, however make sure that you're on the correct site by sense-checking the full website address
- avoid using public WiFi hotspots that are not secure, use your mobile data. If you have no choice but to use Public WiFi, then only use it with a Virtual Private Network enabled on your device
- regularly back up your data
- control your social media accounts – regularly check your privacy settings and how your data is being used and shared
- be cautious of internet chats and online dating – there's no guarantee you're speaking to who you think
- be extremely cautious if you're asked for money

Passkeys

Where supported, consider using passkeys instead of passwords. They are secure and protect against common crimes, like phishing. This is because passkeys don't use passwords. That means there's nothing for criminals to steal.

Many organisations now support passkeys. This includes the NHS, Google, Apple and Microsoft. You can usually find out how to set up a passkey in the Help or Support section of the company where you have your account.

Email and text scams

Be careful when opening emails and texts, especially if you don't know the sender. If an email or text is unexpected or seems unusual, even if it’s from someone you know, ignore it and contact the sender directly to check if they sent it.

Your bank, the police and reputable companies will never ask for sensitive or financial details via email, phone or text.

To protect yourself from scams, known as 'phishing':

- don’t open attachments or click on links in emails or texts from senders you don’t know
- never give out personal information, financial details or passwords in response to an email, when you receive an unexpected phone call or in response to a text message
- set up spam filters on all of your accounts
- don’t respond to emails or texts from unknown sources
- always go to a website directly, by typing out the address yourself, when logging into an account

Social networking

Social networks are a great way of keeping in touch with friends and family, but be careful about how much personal information you share.

Once you post or share something on any social media platform it’s out of your control and could be shared and used by others, even if you delete it.

Make sure you:

- set your privacy settings to the highest level and check them regularly as updates can affect settings
- don’t add or accept ‘friend’ requests from people you don’t know
- where possible, block apps and social media sites from tracking and showing your location, to stop people you don’t know from following you
- think carefully about the images, videos and content that you share
- remember that if you wouldn’t do or say it in the real world, don’t do it online

How to spot a fake website

If an online offer looks too good to be true, it probably is. To help spot a fake site:

- sense check the domain name
- are the prices too good to be true?
- never pay by bank transfer – legitimate sites will accept payment via usual methods, such as bank card and PayPal
- read the terms and conditions, and policies, to check they're clear and fair

Back up your data

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless they pay a ransom.

Regularly back up all your documents and photos in at least one other place to minimise the risk of losing everything if you get a ransomware virus. You can back up data onto:

- a USB stick
- an external hard drive, making sure that the drive isn't connected at all times, as ransomware can infect devices connected to your network
- a cloud server, making sure that the password you use for cloud servers and backups is a strong password and one you don't use anywhere else

Tips for parents and guardians

The internet lets children connect with friends and learn new things. But there are also dangers to going online, and children can be particularly vulnerable.

Talking to your child is one of the best ways to keep them safe online. By understanding the risks and keeping yourself up-to-date on the latest technology, websites and social networks you can help your child enjoy the internet safely and securely.

To help protect your children online:

- keep computers and games consoles in family rooms where you can monitor activity
- install parental control software or activate parental controls through your Internet Service Provider (ISP) to prevent access to inappropriate content
- 'friend' or 'follow' your child on social networks, so you can see how they're using them
- check age restrictions for websites or social networks to make sure your children are allowed to join
- advise your child not to post personal information or any images they wouldn't want everyone to see
- check their social media accounts' privacy settings, so their posts are only seen by friends and their location isn't tracked
- avoid using webcams unless talking to close friends or family, and consider covering it when not in use
- monitor how your children use the internet and watch for any secretive behaviour
- encourage your child to be open about what they do online and who they're talking to
- insist you go with them if they wish to meet online friends
- ensure the games your children play online are age appropriate

Protecting yourself from Cybercrime