

What is cyber security?

Cyber security is how individuals and organisations reduce the risk of cyber-attack.

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

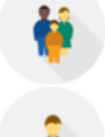




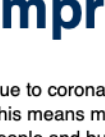
Why is it important?

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

National Cyber Security Centre (NCSC)

Helping to make the UK the safest place to live and work online.

They Provide Information for...

- 
Individuals and families
[Click for more info.](#)
- 
Self Employed and Sole Traders
[Click for more info.](#)
- 
Small and Medium Sized Organisations
[Click for more info.](#)
- 
Large Organisations
[Click for more info.](#)
- 
Public Sector
[Click for more info.](#)
- 
Cyber Security Professionals
[Click for more info.](#)

Improve your Cyber Security

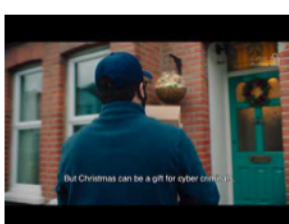
Due to coronavirus, more people will be doing their festive shopping online this year. This means more opportunities for hackers to carry out cyber-attacks. They often do this by targeting people and businesses using:

- email and website scams
- malware - software that can damage your device or let a hacker in

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

You can improve your cyber security by taking six actions:

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data



Improve your Password Security

Hackers can get access to your account by using software to crack your password, by trying one password in lots of places or by trying to trick you into disclosing your password through scams.

Creating strong, separate passwords and storing them safely is a good way to protect yourself online.

Action 1: Use a strong and separate password for your email!

If a hacker gets into your email, they could:

- reset your other account passwords
- access information you have saved about yourself or your business

Your email password should be strong and different to all your other passwords. This will make it harder to crack or guess.

Using 3 random words is a good way to create a strong, unique password that you will remember. You should also protect your other important accounts, such as banking or social media.

How to change your password in:

You should search online for advice from your provider (Gmail, Yahoo! Mail, Outlook, BT, AOL Mail) on how to change your email password.

Advice on passwords for sole traders and small businesses

Did You Know?

If a hacker gets into your email, they could reset the passwords for your other accounts using the **'forgot password'** feature.



Action 2: Create Strong Passwords using 3 Random Words

When you use different passwords for your important accounts, it can be hard to remember them all. A good way to create strong, memorable passwords is by using 3 random words. Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if you need to. For example, "RedPantsTree4!" Saving your passwords in your browser will help you manage them.

Test Your Knowledge

Which one of these passwords does not appear in the top 100,000 most compromised passwords?

arsenal22, 1v7Upjw3nt, p@55w0rd, RedPantsTree, victoria!, 20111977

Action 3: Save your passwords in your browser

Saving your password in your browser means letting your web browser (such as Chrome, Safari or Edge) remember your password for you.

This can help:

- make sure you do not lose or forget your passwords
- protect you against some cyber-crime, such as fake websites

It is safer than using weak passwords, or using the same password in more than one place. Make sure you protect your saved passwords in case your device is lost or stolen.

How to protect your saved passwords

Someone who gets access to your device may be able to use your saved passwords to access your accounts.

This kind of cyber-crime is much less common than remote attacks over the internet, where passwords are cracked using software.

To make sure you are protected, you should:

- turn off or lock your device when you are not using it
- use a strong password to protect your device
- turn on two-factor authentication for all your devices and accounts
- turn on biometrics (Face ID or Fingerprint recognition) if your device supports this

You should also back up your data regularly. This will help you recover your important information if your device is lost or stolen.

How to save your passwords in your browser

You should search online for advice from your provider (Google, Chrome, Microsoft Edge, Firefox, Safari) on how to save your passwords in your browser.

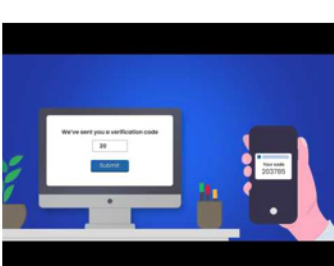
Did you know?

You can access your saved passwords from any device where you are signed into the same browser.

Add extra protection

Once you've set up strong, separate passwords for all your devices and services, there are other things you can do to reduce your risk of being hacked.

Action 4: Turn on two-factor authentication (2FA)



Two-factor authentication (2FA) helps to stop hackers from getting into your accounts, even if they have your password.

Some online banking uses 2FA automatically. It does this by asking for more information to prove your identity, such as:

- a PIN, password or code
- Biometrics - a fingerprint or face ID

How to turn on two-factor authentication (2FA)

You will need to manually turn on 2FA for most of your accounts. Not all accounts will offer 2FA. Online banking uses 2FA automatically. 2FA is also known as two-step verification or multi-factor authentication.

You should search online for advice from your provider (Gmail, Yahoo, Outlook, AOL) on how to turn on 2FA for email. You should search online for advice from your provider (Instagram, Facebook, Twitter) on how to turn on 2FA for social media.

Action 5: Update Your Devices

Out-of-date software, apps, and operating systems contain weaknesses. This makes them easier to hack. Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out. Turn on automatic updates for your devices and software that offer it. This will mean you do not have to remember each time. Some devices and software need to be updated manually. You may get reminders on your phone or computer. Do not ignore these reminders. Updating will help to keep you safe online.

How to turn on automatic updates

You should search online for advice on how to turn on automatic updates for:

Apple - Mac, Apple - iPad, Microsoft Windows 10, Android smartphones and tablets, Android apps.

Test your knowledge

How do companies fix weaknesses in their software?

Bandage, Patch, Repair

Make sure you can recover quickly

A cyber-attack may mean you lose some or all of your data, such as pictures, documents, or financial or client information. Backing up regularly will help you get back on track.

Action 6: Back up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online). Backing up regularly means you will always have a recent version of your information saved.

This will help you recover quicker if your data is lost or stolen. You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.

If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done. You should search online for advice on how to turn on automatic backups for: Apple MacOS, Apple - iPhone and iPad, Android, Microsoft Windows 10 and Windows 8 OneDrive.

Advice on backups for sole traders and small businesses

Backing up your data will mean your business can continue to operate if a cyber-incident does happen. Start by identifying the data that is most important to your business. This could be financial, contract, customer or supplier information. Make sure it is backed up regularly.

You should also know how to restore a backup in the event of data loss.

Did You Know

You should always back up your data before updating your device. This is because updates can sometimes remove or change files. For more tips on how to stay safe online visit [CyberAware](#).