

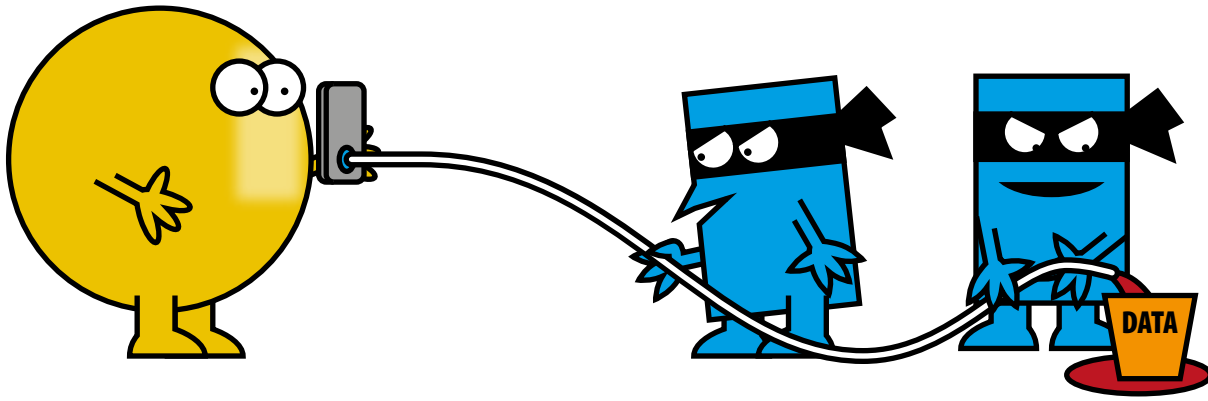
**Stay safe online – protect your tech
and know how to spot a scam**



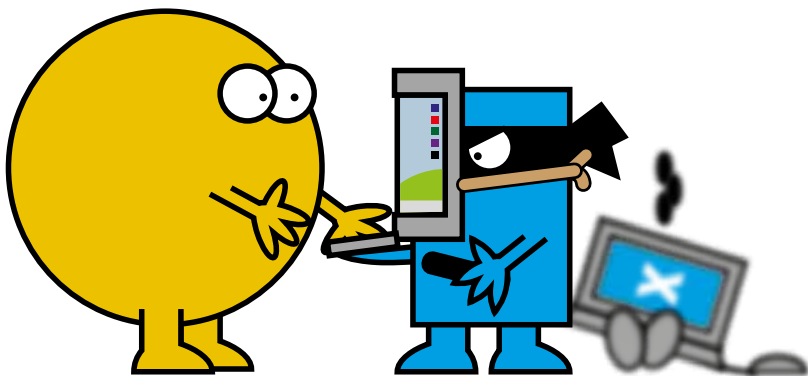
Accessing the internet is easier now than ever before, whether you use a computer, tablet or mobile device. Keeping your information safe online can also seem quite daunting, when you hear about computer viruses, malware, cyber-crime and digital scams – but there are some simple steps that you can take to protect yourself from becoming a victim.

**Know the risks and set up your technology securely to
protect against automated attacks**

Malware and computer viruses



Malware is a type of malicious software designed to harm or deceive your computer, tablet or phone. Cybercriminals can use it to obtain data – from financial, healthcare information, personal emails, and passwords. The possibilities of what sort of information can be compromised have become endless.



A **computer virus** is a type of malware that aims to disrupt systems and result in data loss, through damage or theft. A computer virus will attach itself to other programs, files or documents. It then duplicates itself, and spreads from one computer to another.

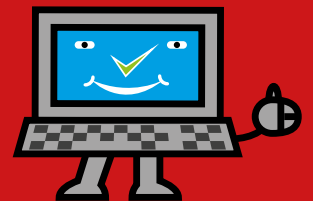
For example, you could receive an email with a malicious attachment, open the file unknowingly, and then the computer virus runs on your computer.

Unusual behaviour, such as unexpected pop-up windows, reduced system speed, crashes and other unexplained behaviour are a sign of an affected device.

Top tips to protect yourself from malware and computer viruses

Always:

- keep your computer software updated;
- think twice before clicking links or downloading anything;
- be careful about opening email attachments or images;
- use antivirus software and keep it up to date (antivirus software also protects against malware).

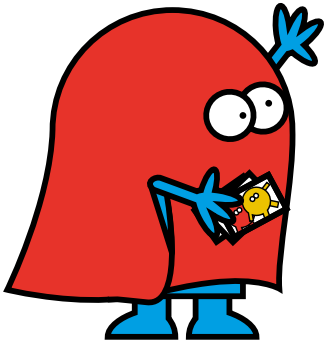


Never:

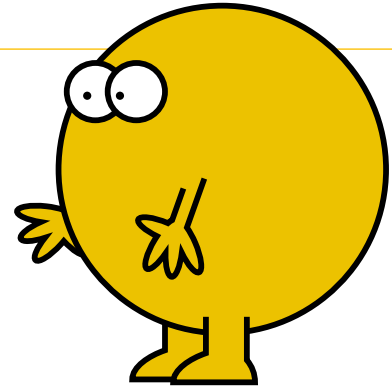
- install software at the request or guidance of someone over the phone;
- trust pop-up windows that tell you to download or install software;
- give account details, such as your password to anyone over the phone.



Phishing



Phishing is when scammers (pretending to be someone else) send fake emails, text messages or WhatsApp messages, usually to thousands of people at once. Scammers can pretend to be your friends, by making it look like it came from a trusted email address.



Phishing communications are getting harder to spot. Some will still get past even the most observant user. Whoever you are, if you use email, you'll receive phishing attacks at some point and you may receive text messages or WhatsApp messages as a mobile telephone user.

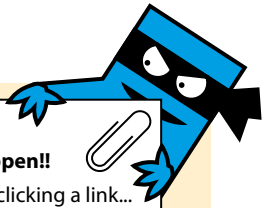
The goal of these scammers is most often to get you to:

- reveal sensitive information such as bank details or personal details;
- click on links to unsafe websites;
- send money to them.

Because they have political or ideological motives for accessing your information. Some examples include:

Email messages

- Messages from a friend's email address urging you to click the attachment to look at some amazing photos.
- A message from your bank advising that you have been offered a £1,000 free overdraft, asking you to click a link to log in and accept it.



From: Your.friend@somewhere.com
Subject: **Click this link and amazing things will happen!!**
You won't believe how much money can be made by clicking a link...

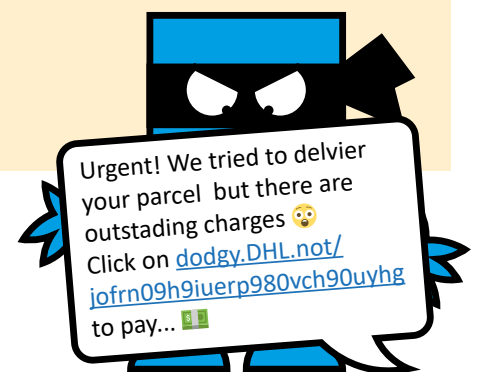
Text messages

Examples include:

- Parcel delivery texts asking you to click on a link to pay for delivery.
- Messages claiming to be from your bank.

If the message looks suspicious **do not click on any links**. You can check authenticity by contacting the alleged sender by telephone to confirm if it is real.

You can report suspicious scam text messages by forwarding them to **7726** where it will be used as intelligence.



WhatsApp messages

Examples include:

- Supermarkets offering vouchers if you forward the message to 10 contacts – this is a phishing exercise.
- Messages that pretend to be one of your children or a relative claiming they have lost or broken their mobile phone and are using a temporary replacement – these may ask you to make an online payment for them. If you receive a message like this ring the child or relative and confirm with them.

Emails

Examples include:

- A message from somebody that you know saying that they have a problem – can you help them out. If you aren't sure, ring your friend and ask if all is OK – at the very least you will notify them that their account has been hacked and they can change their password to protect themselves.
- Emails that can look very official and genuine such as TV licence renewals, Driving Licence renewals. **Always check the senders email address** – if it is genuine it will end in the organisations' genuine address. Scam emails are generally random/personal email addresses so you can tell that they aren't genuine quite easily.

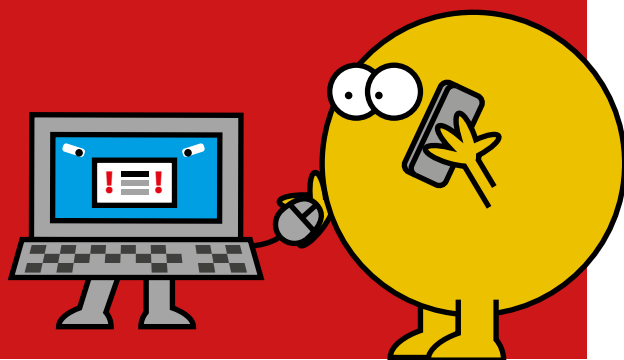
Scam emails can be forwarded to report@phishing.gov.uk where they can be used as intelligence.

Often a phishing attack is easy to spot, but sometimes they can be more sophisticated. If in doubt, act as if it is definitely a phishing email, don't click on or open anything, and delete it.

Top tips for spotting phishing scams

Phishing messages often:

- have a generic or incorrect greeting rather than being specifically addressed to you;
- request personal information such as passwords, bank details, date of birth, personal ID numbers, etc;
- are short, vague and look or sound a little odd – even if they apparently come from someone you know;
- contain unexpected attachments, or unexpected links to online documents. Even if the email comes from a trusted sender;
- contain poor spelling or grammar. Or incorrect references to banks, Amazon, antivirus subscriptions or other services;
- try and create urgency – “your account will be disabled in 24 hours”, “this needs to happen by 5pm today”, in the hope you'll act without thinking;
- come from someone that you would not expect to be contacting you. Not just because you don't know them but also perhaps you do not normally have any communication with the kind of contact that they are claiming to be;
- try and claim false authority, for example, government agencies, police forces, your bank, fraud departments, etc;
- ask you to do something that you would not normally do.



Reduce the impact of phishing attacks by limiting access

Where you can, always set up two factor authentication (2FA) on your important accounts such as email or financial accounts. This means that even if an attacker gets your password, they still won't be able to access your account, as they would need the second piece of information, such as the code which would be sent to your phone, which they cannot access.

Other online scams

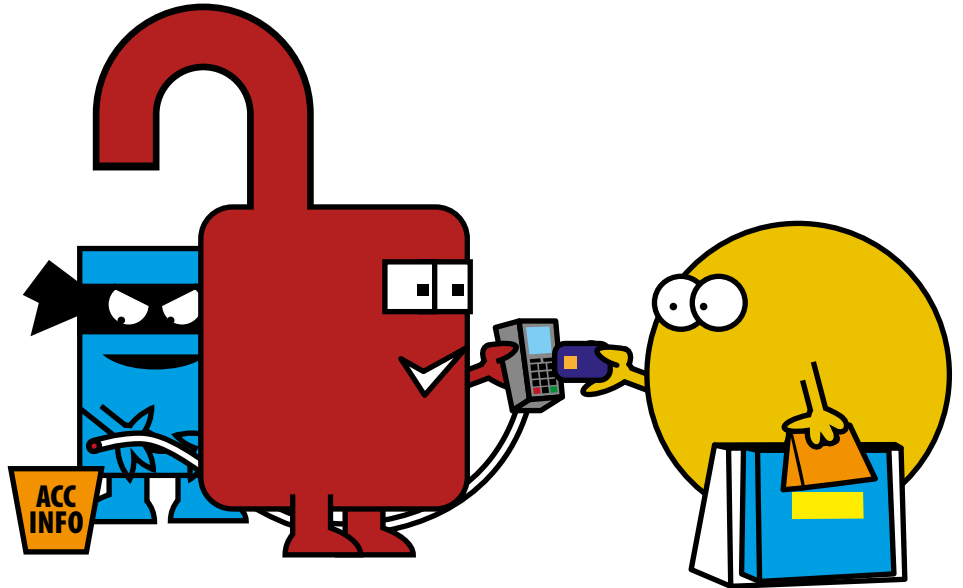
Social media

Scammers can clone Facebook accounts then messaging everyone in their account to either ask for money or to advise about an amazing financial opportunity. Contact your friend by another means (call or text) and ask them if it's really them – again you will have alerted your friend that they have been hacked and prevented yourself from losing money to scammers. You and your friend should both change your passwords.

Online shopping

Always use a trusted website – while it's tempting to go for the cheapest option you can find, many of these websites don't operate in the UK and aren't subject to our consumer laws. If there are problems, this can make exchanges and refunds difficult.

Always check the URL for a green padlock or https when paying – these both denote that your payment and personal details are secure



Be aware of copycat websites, these can appear at the top of a web search such as applying for a passport, driving licence, blue badge. Always check that you are engaging with the correct official website (in these cases) that it is the genuine Gov.uk site.

Online dating and gaming

These are easy scams for criminals with patience; playing on your emotions. Scammers might engage on dating sites and online gaming sites where they will communicate in the chat rooms, moving the conversation to a private messaging site such as texting or Whatsapp to gain your trust. They may then ask for money for an emergency and of course they will pay you back. NEVER give money to somebody you haven't met in person.

Online questionnaires, surveys and quizzes or social media 'tell me about you' type status posts

Scammers can use these to find out basic information about you which could lead to them deciphering your passwords or at the least give them background for a later scam. Be really careful about what information you share online.

What else you can do to protect yourself from online threats

Back up your data

Safeguard your most important data, such as your photos and key documents, by backing them up to external storage, be it an external drive or a cloud-based storage system. Also, leave this storage disconnected from your system when not in use, so that it cannot be attacked.

Set strong passwords

This process shows how to have an unlimited number of passwords without writing any of them down:

First, choose three random words

For the purpose of this example, I will use: **triangle**, **house** and **spanner**

Using three random words is a government approved method of creating a highly secure password, which while long – 20 letters in this example – is easy to remember.

So my initial password is:

trianglehousespanner

Second, add a capital letter

Many websites and computer systems require the inclusion of a capital letter, so choose at least one letter, and capitalise it.

I am going to capitalise the Ns in spanner, to give me:

trianglehousespaNner

Third, add a number

We have already created **trianglehousespaNner**, which is a great three random words password, but some websites require a number in their password, so let's add one. It might be that you have a number that you like, such as a favourite number. We do want to make it easy to remember after all. I am a fan of the number 4, so that's what I will add. This gives me:

trianglehousespaNner4

Finally, add a special character

Many websites and computer systems also require the inclusion of a special character. Special characters are any of these punctuation symbols:

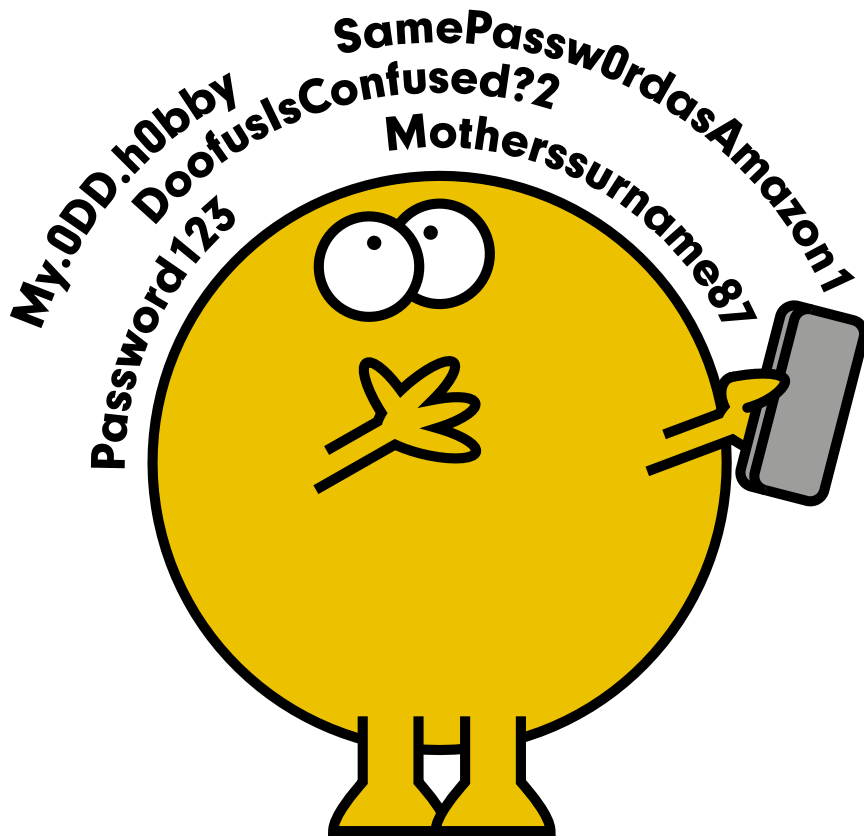
!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

Although there are more symbols, those listed here are the ones that systems commonly accept, and for this example I am going to use a comma.

So my password now looks like this:

trianglehousespaNner4,

We have used three random words, added at least one number, capital letter, and special character. While **trianglehousespaNner4,** seems like a lot to remember, after a few uses, it will be easy to remember.



So what's this about remembering lots of different passwords?

This is the bit where you choose a rule that works for you.

Let's consider these websites and see how easy it is to make unique passwords for them:

- www.spotify.com
- www.amazon.com
- www.gmail.com

It could be that you choose to include the last two letters of the website name, giving you:

- **trianglehousespaNNer4,fy** for Spotify;
- **trianglehousespaNNer4,on** for Amazon; and
- **trianglehousespaNNer4,il** for Gmail.

or you could use the last three letters read backwards, giving you:

- **trianglehousespaNNer4,yfi** for Spotify;
- **trianglehousespaNNer4,noz** for Amazon; and
- **trianglehousespaNNer4,lia** for Gmail.

Use your imagination. Whatever you decide to do, base it on the name of the website, or system that you are creating the password for. And use that same rule for all passwords.

Then when you next want to log in, you simply type in your first bit – **trianglehousespaNNer4** – in this example, then apply your rule to remind you what the last part of the password is.

By adding this final step, you have created a method that gives you highly secure and unique passwords, that never need to be written down.

Frequently asked questions

If three random words are so secure, can't I just use the same password for everything?

No, as if one website is hacked, the attacker will have access to all of your accounts

I have a system that will only take up to nine character passwords. What should I do?

Choose a short nonsensical word such as plut and use it for all short passwords in place of your usual three random words, then make the other changes as normal e.g. **pluT,4** followed by the last rule you chose, e.g. for a last three letters backwards rule, a Spotify password would be **pluT,4yfi**

Can I use this method for home and work passwords?

Yes, however you must use a different three random words, to separate passwords for work stuff from passwords for personal stuff.

If through hacking a system, a hacker discovers my password, won't the hacker be able to figure out my method?

No, due to the final bit being different. As hackers only try other systems with the password that has been discovered. That's said, they might be targeting you for a specific reason, e.g. because of your job in childcare, or as a finance manager etc.

So, if you are notified about a successful attack on a system you use, immediately change your three random words and update to the new password on all of your accounts.

If you have difficulty understanding this document, please contact us on 01983 821000 and we will do our best to help you.