Your local independent charity supporting older people in Camden since 1965

Camden Age UK

Charity No. 293446

Online Safety Workshop

Building your foundational understanding of the world of digital

Websites

Spotting the difference between a legitimate website and a suspicious website can be easier than you think

1. Is the URL web address secure?

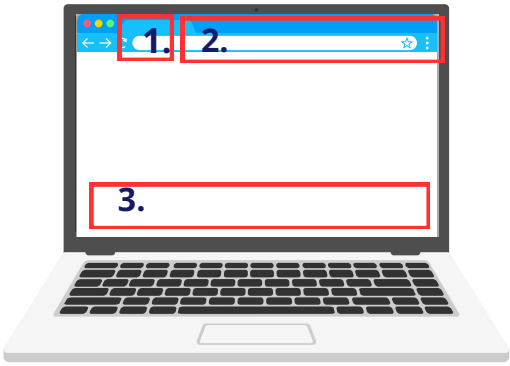
Does the website URL (the web address) start with the code: **https://**

2. Does the URL look suspicious?

A suspicious URL (web address) might not match a normal web address from trusted companies.
For example : most websites we access here in the UK will end in either **.com** or **.co.uk**

3. Does the website contain clear, consistent information about the company or organisation it claims to be?

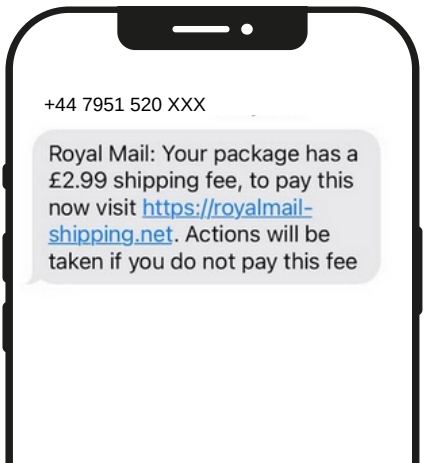
A suspicious website might not have consistent information, missing details like a business address or missing its legal terms and conditions (these can be found at the very bottom of the home page

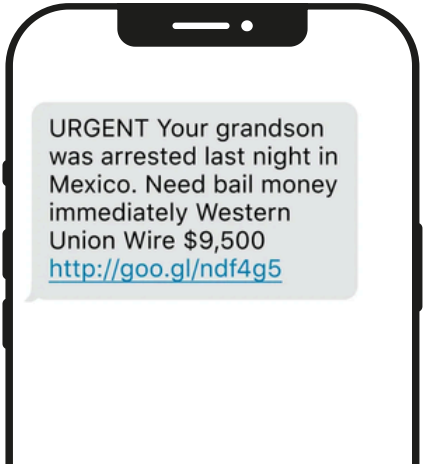


Text Messages

Got a strange text message out of the blue? It could be a 'phishing' message

- Scam artists pretend to be legitimate companies and organisations like Royal Mail, HMRC, Apple
- These messages will often contain a **URL link** with instructions to click on it.
- Look critically at the number that has sent the message AND the URL link
- Does the URL link match the official web address of the legitmiate organisation. For example: **https://www.royalmail.com/**
- Is the phone number just a number? legitimate organisation's will usually show with a name of the company or organisation
- Does the text message contain false urgency?

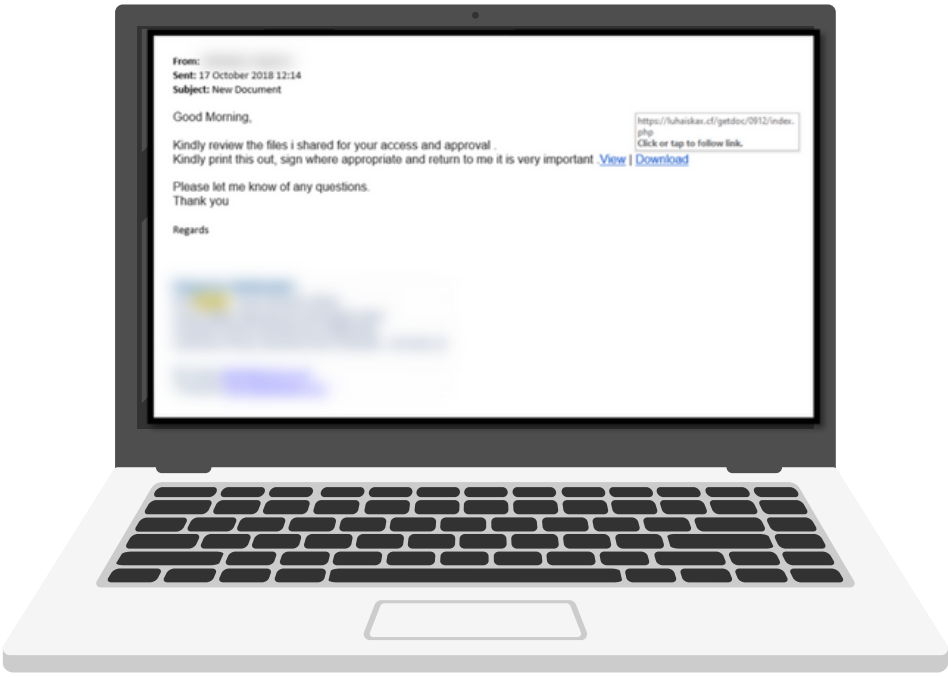




Emails

Emails from scammers use similar tactics to a scam text message

- Targets of email scams sometimes recieve 'phishing' emails that pretend to be one of their email contacts
- If the email is seemingly from a personal contact remember to think whether the email is out of context
- Does the email ask you to click on a strange URL link? OR download an unknown file?
- IF you have receive one from a personal contact or business, try to contact them using their phone number to check and verify it is them



Wi-Fi Connections

Wi-Fi is a great way to connect to the internet and not use your mobile data, but not every WiFi network is safe

- Wi-Fi is a short range radio signal that allows you phone, tablet or computer to connect to the internet, you can either access public or private networks
- Private networks are owned and paid for by the home or business venue that you are in proximity to and usually have a password
- These are open Wi-Fi networks that cover larger areas - these DO NOT have a password or padlock symbol next to the Wi-Fi name
- Public Wi-Fi networks can be provided by your local council or in a business premises but can also be set up to steal personal information

Be cautious when joining a 'public' Wi-Fi connection as they can be unsecure and allow the providers to see your online activities and any personal details you put into your phone while using their internet connection

Passwords

Keeping strong passwords in a safe place is a sure way to keep safe online

- A strong password contains at least 8 characters, numbers, capitol letters and special characters **&?!***

Here is an example: CAmd3n2023!

- Keep your passwords safe in a small booklet, make sure to right what the password is for and the date you created it - this will come in handy if you ever change them in the future
- A small book in your home will be safer than saving your passwords online
- Do not use the same password for every online account - if you don't want to make one that is totally new try to make variations of the same password with different numbers and characters

Top Tips for Online Safety

Be a detective! Learn the indicators for suspicious messages, email or phone calls

Be wary of any unknown numbers or email address
If you are the message or call seems out of context then go with your gut feeling and be cautious - Your bank will never call you and ask you to move your money to a 'safe' accoun

Many scam messages (phishing messages) will pretend to be respectable organisations or businesses
Scammers pretend to be trustworthy by impersonating Natwest, Royal Mail or HMRC or one of your email contacts

Look closely at the email address or web address
Do they end in **.com** or **.uk** or a region that you have recently bought a product from? If not then they may be false!

Do your own research before clicking on any links
Try to contact the business/organisation though other contact lines and check that the website addresses match up

Check that the Wi-Fi connection is safe
Always make sue your know or trust the provider of the Wi-Fi network, is it your friend's? Family member's? Local business'? Verify the source

If you're unsure ask a friend, colleague, or family member

Useful Websites For Online Safety

https://us.norton.com/blog/how-to/how-to-know-if-a-website-is-safe

https://www.ncsc.gov.uk/

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online

https://www.citizensadvice.org.uk/consumer/scams/check-if-something-might-be-a-scam/

Contact us

If you would like to learn more or receive digital support then please send us an email on:

- digitalinclusion@ageukcityoflondon.org.uk

Or visit our website:

- www.ageukcityoflondon.org.uk