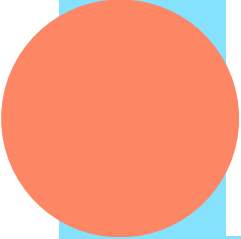


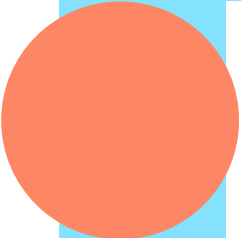


# Online Scams

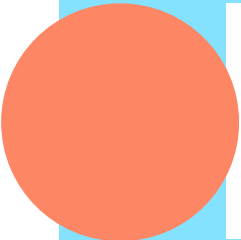
Online scams are becoming harder to spot and can often catch out even the most savvy internet users. Unknowingly sharing personal or financial information sees millions of people lose money in the UK alone every year.



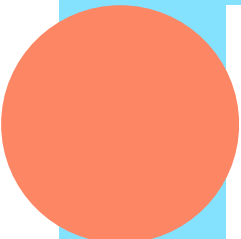
Email scams - Bogus emails sent in the hope that you will enter personal or financial information which may include links or files that could harm your device or direct you to fake websites.



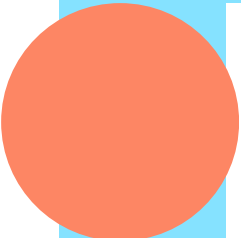
Fake websites - created by scammers to look official requesting personal or financial information or offering a service for a fee which is available free elsewhere.



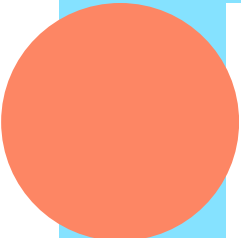
Computer viruses - sometimes called malware, these are rogue programs that spread from one computer to another and may be sent to you as a link or email attachment which will release a virus when you click on it.



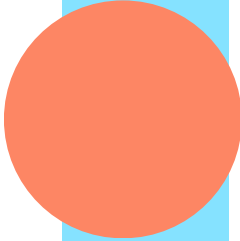
Relationship scams - through social networks or dating sites, scammers may try to gain your trust and then use this to extort money from you.



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.



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.



Shopping scams - Only make payments using secure payment options. Check the URL of the website begins with https instead of http as 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. Also look out for trusted payment options such as PayPal, Apple Pay and Google Pay and where possible, use a credit card when making purchases over £100 as this provides protection under Section 75 of the Consumer Credit Act and could help you get your stolen money back.

Take a moment to stop and think before you provide any personal or financial information online, only criminals will try to rush or panic you.

Ask yourself if this could be fake? – it's ok to reject, refuse or ignore a request for information, legitimate organisations will not ask in this way

If you receive a request for personal or financial information and you're unsure, use other means to contact the organisation and verify the request.

If you think you have been a victim of fraud or cyber crime then contact your bank immediately and report it to Action Fraud.

#### Further information on online scams:

Age UK - [www.ageuk.org.uk](http://www.ageuk.org.uk)  
Citizens Advice - [www.citizensadvice.org.uk](http://www.citizensadvice.org.uk)  
Take Five - [www.takefive-stopfraud.org.uk](http://www.takefive-stopfraud.org.uk)

If you think you may have been a victim of fraud or cyber crime then you can report this to Action Fraud on 0300 123 2040  
[www.actionfraud.police.uk](http://www.actionfraud.police.uk)