Fraud Awareness

What to look for:

Unsolicited — Did you contact them? If not, ask yourself why (and how) they are contacting you.

Unprofessional — Are there misspellings, poor grammar, a strange email address or number? Are they rushing you? Verify your contact.

Unusual — Is this a usual occurrence? What are they asking for? Is it suspicious, too good to be true? Ask someone.

What they want

- **Money** or items with monetary value like vouchers or crypto currency
- **Card details** (to withdraw money)
- **Personal information** (for ID theft or sale of contact details)
- **Account access** (to gain information, restrict access for ransom, or to piggyback on your device)
- **Ad delivery/click harvesting** (scammers will harvest your activity so companies can pay to boost traffic)
- **Personal gain** (some people release viruses just to sow chaos or may be an individual with a vendetta)

Take your time.....

Scams rely on you not noticing until it's too late. Mistakes are inevitable so the aim is to rush you or make something too enticing, convenient or important to ignore.

Limited time offer!! ~~Was £150!~~ Now £60! 00d 03h 42m 58s

Delivery delayed. Pay fee now.

Me: It's an emergency, please send £££!

Login Now or Lose Access to your Account.

Free Movies & TV Shows!

Your account has been hacked! Click here to secure.

Disconnect. Report

Turn off, unplug, disconnect. Shutting off can interrupt malware and you owe no politeness to scam callers. Hang up.

Report immediately to your bank if money has been taken or seek advice if a computer or phone has been compromised.

Be Sceptical

Who are they?

Most ‘scammers’ aren’t people at all but lines of code that can operate on their own and seem harmless. It targets as many people as possible to get the highest return and relies on people underestimating how often they are at risk, how easy it is to trigger and making mistakes.

Know the risks. Be sceptical.

It’s scarily simple!

It is easy to spoof a link. It’s just one line of code!

www.definatelynotascam.co.uk

It is easy to mimic a website. *Anyone could do it in <1min.

It is easy to impersonate an account, and AI is making it easier.

Hi, it’s Dave! Could you do me a favour...

Do’s and Don’ts

- **Do** turn off message preview on lock screen.
- **Don’t** just call back numbers you don’t recognise. This can confirm you as a potential target. Look up the number online first to see if it’s already been reported.
- **Do** turn off auto connect Wi-Fi on mobile devices.
- **Don’t** give out your email, phone number, name or work role to cold callers or untrusted sites who may use this information to seem more credible for targeted scams.
- **Do** turn off auto loading images. Viruses can be hidden in image files which gain access to your device when loading, making opening emails and messages dangerous.
- **Don’t** write down your password digitally or otherwise. Short phrases with special characters are more secure and easier to remember. *Password: Keys2MyDesktop!_*
- **Do** use Trustpilot before buying from a new online store.
- **Don’t** click on links or download files without verifying.

Stay Safe

Scams are meant to trick you; impersonating people you know, authorities, brands you trust, exploiting habits, shortcuts. Be sceptical. Disconnect. Report. Stay safe.

*How to be a scammer in <1min:
Go to amazon, view page source, copy and paste to wordpad. Convert txt to html with a quick google search and save. Now you have your very own working amazon homepage to use however you like. You can use ctrl+f to find and replace links, you can track activity like login details and then have access to delivery information and any connected cards or funds.