

# Don't become prey for a fraudster



## Think **twice** BEFORE YOU ACT



[www.getsafeonline.org](http://www.getsafeonline.org)



Gloucestershire Constabulary

Do you think twice before you click on links in unexpected emails, posts or texts, or open email attachments?

Or before you reveal your confidential details to a total stranger who's called claiming to be from your bank, your credit card company or the police?

If not, you could become easy prey for a fraudster. They get you on the hook, reel you in, and before you know it, you've given away your PINs, passwords ...everything they need to steal your hard-earned money, never to be seen again.

Millions of people in the UK get defrauded in this way every year, and we'd like to help you protect yourself against becoming one of them.

*It's easy – start by reading these expert top tips from Gelly.*



**#SaveGelly**

[www.getsafeonline.org](http://www.getsafeonline.org)

 [@GetSafeOnline](https://twitter.com/GetSafeOnline)

 [www.facebook.com/getsafeonline](https://www.facebook.com/getsafeonline)

## Gelly's top tips to avoid online and phone scams

- **Never give out personal or financial data** including usernames, passwords, PINs, ID numbers or memorable phrases.
- **Be very careful that people or organisations who you're supplying payment card or other confidential information to are genuine**, and even then, never reveal passwords. A bank, HMRC, retailer or other reputable organisation won't ask you for your password or PIN via email, phone call or any other means.
- **If you're asked by a caller to cut off the call and phone your bank or card provider, call the number on your bank statement or other document from your bank** – or on the back of your card. But be sure to use another phone from the one you received the call on or leave it for five minutes before you make the call, in case the sender number has been spoofed or the line left open.
- **Don't open email attachments from unknown sources** as they could well contain malware. Delete them, and take the details to report if appropriate.
- **Don't click on links in emails from senders you don't know**. Instead, roll your mouse pointer or finger over the link to reveal the actual sender. If they're different, it's a scam. Even if you get an email that seems to come from someone you might know – but it seems unusual – the sender may be a fraudster who's spoofed their address. If in doubt, call (but don't email) the sender.
- **Don't attach external storage devices like USB sticks or hard drives** – or insert CD-ROMs/DVD-ROMs into your computer – if you're uncertain of the source. This is a favourite way for fraudsters to spread malware.

But most important...

**Think twice** BEFORE YOU ACT



If you have been a victim of banking fraud or spot irregular activity on your account, contact your bank straight away.

**Remember**, it's important to report any fraud to Action Fraud by calling **0300 123 20 40** or at **www.actionfraud.police.uk**

Also report fraud to any **website** or **ISP** where you've been defrauded. This applies however large or small the amount: it could protect others, and the proceeds of fraud are often used to fund activities like terrorism and human trafficking.



And remember, always

# Think **twice** BEFORE YOU ACT



[www.getsafeonline.org](http://www.getsafeonline.org)



Gloucestershire Constabulary

Supported by:



OFFICIAL PARTNERS

