

Safer Online



BE SAFER WHEN SHOPPING ONLINE

Preventing online fraud



ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk



**POLICE & CRIME
COMMISSIONER**

Serving
Hampshire
Isle of Wight
Portsmouth
Southampton

Be safer when shopping online

DONT BE CONNE

SCAM AWARE



D O N L I N E

THINK YOU HAVE BEEN A VICTIM OF FRAUD?

Details stolen?... Money taken?...

Report it to your bank and report to Action Fraud by calling:

0300 123 20 40

or via the Action Fraud website:

WWW.ACTIONFRAUD.POLICE.UK

BE SAFER WHEN SHOPPING ONLINE



BE SURE IT'S **SECURE**

Avoid using public Wi-Fi for your online purchases & transactions.

Wait until you get home or to a location where you can be sure it's secure, or even better, use a VPN app.



DON'T JUST **SEARCH**

Only use trusted, well known or recommended sites.

Search results can be rigged to lead you astray.

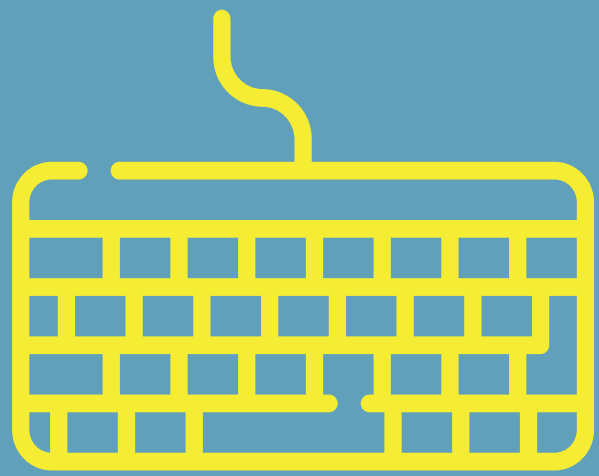


PICK YOUR **PASSWORDS**

Using the same password for all of your online shopping accounts is the same as using just one key to open your front door, your office, your car. If you lose it, you lose all. Always use different passwords, 10+ characters, or a passphrase that only you will know.

A close-up, slightly blurred image of a computer keyboard. The keys are visible, with some text like 'MONTH/YEAR' and '19' partially legible. A semi-transparent text box is overlaid on the right side of the image.

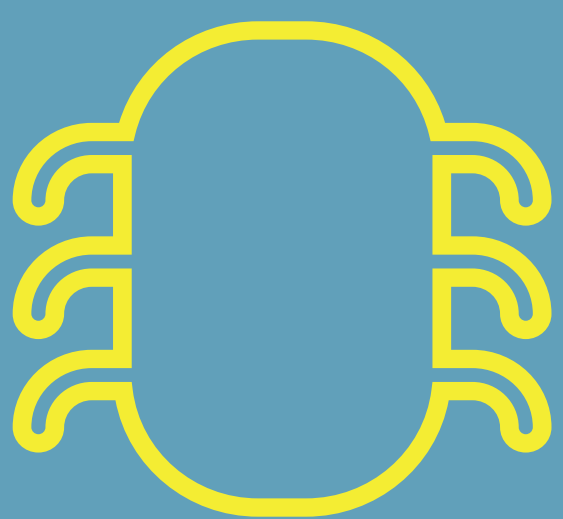
**Always use different passwords
each with 10+ characters**



CHECK YOUR **TYPING**

Typo-squatting is a technique where a mistyped web address leads to a perfect replica of a website, except it's not legit...

Would you notice www.amaazon.co.uk? Take your time, double-check.



AVOID A NASTY **VIRUS**

Never open attachments or click on links in emails you're not expecting. And be careful if you receive an e-card as they can be fraudulent too.

Always install anti-virus or anti-malware software on all of your devices. Some forms of malware such as the nasty Banking Trojan can sit dormant in your device, intercept and steal payment details when you complete an online purchase.



Always install anti-virus or anti-malware software on all of your devices



PRIVATE **PASSWORDS**

Never save your passwords or financial data to your phone or mobile device and ensure your phone is password protected.



TOO GOOD TO BE **TRUE?**

Deal sounds too good to be true? Then it probably is. Research carefully. Look for references and feedback (Trustpilot, user reviews etc). Always approach with caution.

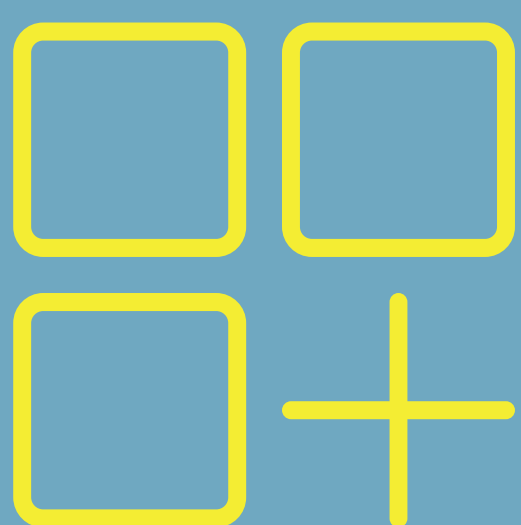
*Be safer when
shopping online*

WWW.ACTIONFRAUD.POLICE.UK



If it sounds too good to be true,
it probably is

IT'S QUICK AND EASY TO BUY ONLINE ON YOUR MOBILE PHONE, BUT MAKE SURE IT'S ALSO CYBER SAFE



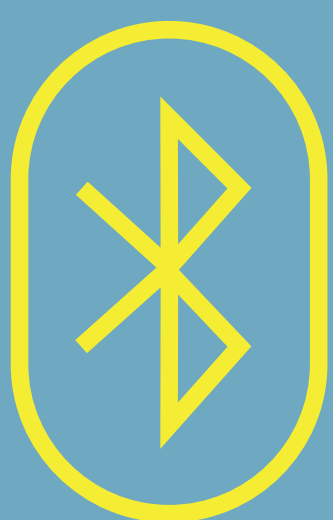
BE 'APP'Y

Use dedicated apps on mobile devices and smartphones. Be sure to download the app from an authorised app store (iTunes, Google Play etc) and make sure the app is secure. Always keep your apps updated to ensure they are as secure as can be.



BE READY TO WIPE **YOUR PHONE**

If stolen most mobile devices have the software to wipe all data from their memory - learn how this works so you can do it in case of emergency so your data isn't stolen.



CLOSE THE **BLUETOOTH DOOR**

Do not leave your Bluetooth open or in the on position on your phone - as this leaves the door open for the crafty hacker.



Learn how to remotely wipe your
phone in case of emergency

CARDS ARE QUICK AND EASY TO USE FOR PAYING ONLINE, BUT BE CAREFUL WITH THE INFORMATION YOU GIVE OUT



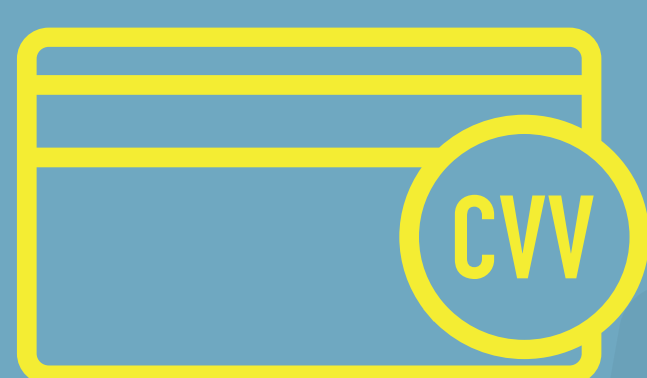
S STANDS FOR **SECURE**

If you're sending your credit card or other personal information online, make sure you see the HTTPS in the browser & see a padlock. S stands for secure.



CARD **CONTROL**

Use credit cards for shopping? Consider getting a pre-paid card or card just to use for online purchases and set a very low credit limit on it so that even if it does fall into the wrong hands, damage is limited. Credit cards offer greater consumer protection than debit cards. If you use a pre-paid card - check it has fraud protection.



CVV **ONLY**

Remember: when purchasing online, you'll be asked for your CVV (3 digit security on back of card) but you should never be asked for your card's PIN or any internet banking passwords.

A close-up photograph of a person's hand holding a gold-colored credit card. The card features a silhouette of a person and the text "5065 STANDARD MasterCard". The hand is positioned over a laptop keyboard, which is visible in the background. The person is wearing a grey long-sleeved shirt. The image has a soft, slightly blurred aesthetic.

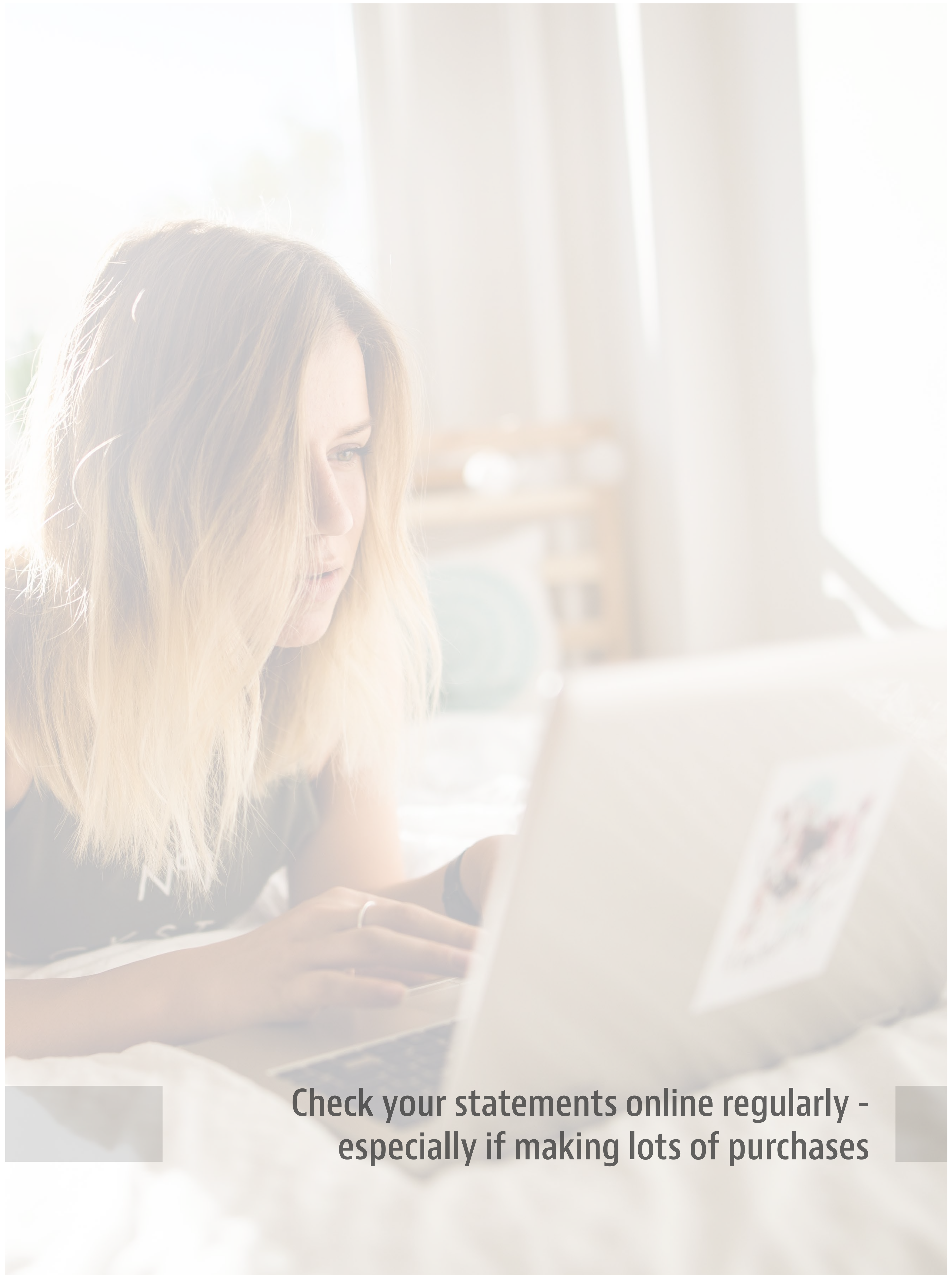
**You should never be asked for your card's PIN
or any internet banking passwords**



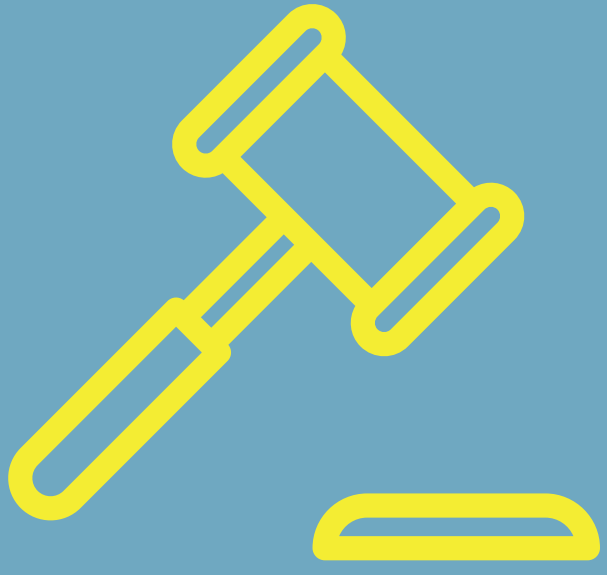
SWIFTLY SORTING STATEMENTS

Check your statements online regularly - especially if you're making a lot of purchases. Make sure what you have bought matches your statement. The quicker a problem is identified, the swifter it can be sorted.

*Don't be conned
when shopping online*



**Check your statements online regularly -
especially if making lots of purchases**



PRIVATE SALES & AUCTION SITES

01

Buying from an auction site such as eBay? Pay on the site every time – never click on a link a seller sends to you and never pay via bank transfer.

02

Never pay by money transfer – use a recognised service such as PayPal or Sage Pay which protects your money until you've resolved any problems with a seller.

03

Research the seller before you bid. Check their feedback and be mindful that this can be faked.

04

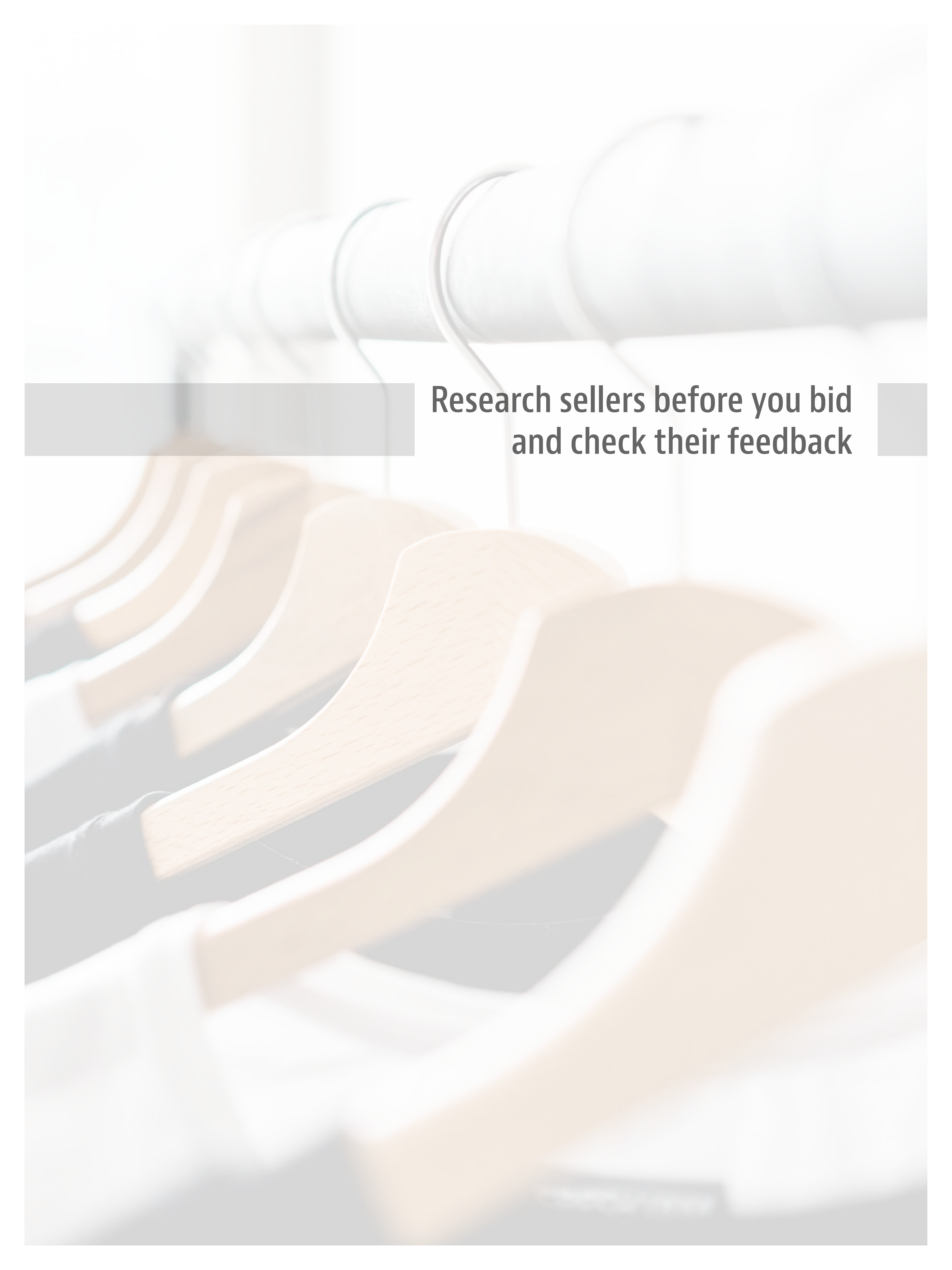
If you are collecting something you have bought from a private seller online, take someone with you or make sure that someone knows where you are going.

05

Are you selling? If someone has sent you money via PayPal, check that it has cleared before you despatch the goods. Wily fraudsters can exploit the chargeback facility to grab their money back from PayPal, and you will lose your goods and your money. They can't grab money back from your bank.

06

Never provide your banking details to people or businesses that you don't know.



**Research sellers before you bid
and check their feedback**

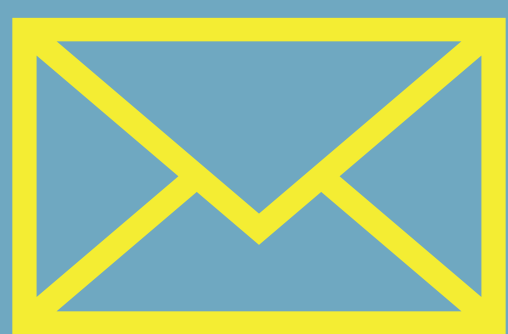
ALWAYS BE CYBER AWARE.

BE SUSPICIOUS IF:



.....

The buyer or seller has bad feedback history or a very recently set up account.



.....

You get a private message or email offering to buy below the current bid or reserve price or to sell a similar item after an auction has ended.




.....

You find an expensive item for sale at an incredibly low starting bid. If it sounds too good to be true – it probably is.



Scam Aware



A top-down view of a workspace on a light-colored wooden surface. In the upper right, a white tablet is held by two hands, displaying a website with a '50% SALE' banner and a 'GO+SHOP' button. To the left of the tablet is a white mug with a lemon slice, sitting on a brown woven coaster. Below the mug are several white envelopes and a roll of orange tape. In the lower right, a brown paper bag is partially visible with a 'Thank You' tag. In the lower center, a silver laptop is open, with hands typing on the keyboard. The laptop screen shows a website with a 'NEW COLLECTION' banner and a 'SHOP NOW' button. To the left of the laptop are a pair of scissors, a roll of yellow tape, and a pair of glasses.

**Be aware if you get a private message
offering the item at a lower price**

FACEBOOK MARKETPLACE



Approach Facebook marketplace purchases with caution. Unlike rival sites such as eBay, it doesn't always offer a secure payment facility.

Never transfer money directly into someone's account in response to a photo you have seen online. If they want to sell – ask them to do it via PayPal, so that if there is a dispute and the goods never show, you can raise it with PayPal.



Never transfer money directly into someone's account



THINK YOU HAVE BEEN A VICTIM OF FRAUD?

Details stolen?... Money taken?...

Report it to your bank and report to Action Fraud by calling:

0300 123 20 40

or via the Action Fraud website:

WWW.ACTIONFRAUD.POLICE.UK

