

Fraudsters try to get rich by conning honest people out of their hard-earned cash.

We all need to know when and where to look out for fraud. Here are some simple steps to help protect yourself.



## You can help beat fraud

Remember, the only people who don't want you to be suspicious are the fraudsters.

- Stay alert when you switch on your computer, open your post, answer the phone, or go to a cash machine
- Be aware and stay safe from fraud.

## Find out more

[cifas.org.uk](http://cifas.org.uk)  
[cityoflondon.police.uk](http://cityoflondon.police.uk)  
[consumerdirect.gov.uk](http://consumerdirect.gov.uk)  
[getsafeonline.org](http://getsafeonline.org)  
[met.police.uk/fraudalert](http://met.police.uk/fraudalert)  
[moneymadeclear.fsa.gov.uk](http://moneymadeclear.fsa.gov.uk)

## The National Fraud Strategic Authority

Working with partners across government and business to help protect you from fraudsters and the harm they cause.

[attorneygeneral.gov.uk](http://attorneygeneral.gov.uk)



# Keep clear of **fraud**

Who's eyeing up  
your money?



## Keep clear of **fraud** and protect your personal information

Fraudsters are greedy and enterprising. They often adapt their approach to match what's going on in our day-to-day lives. From emails asking for your bank details following a bank merger, an employment agency asking you for money upfront to start a new job, or an investment opportunity that's only available now. So stay aware!

### On your **computer**

Do you have protection from computer viruses?

- Software that blocks viruses and dodgy emails is essential, cheap and can save a lot of trouble
- Don't use one password for everything
- Change your passwords regularly. Don't let anyone persuade you to share your passwords for any part of your computer or online accounts
- Think about what kind of information you want to offer the whole world through social networking sites – and what unscrupulous people could do with it
- Your full address, date of birth and mother's maiden name are valuable information to a fraudster interested in impersonating you.

### By **email**

Seen an official-looking email requesting information about your bank account?

- These emails often claim to be part of a security check. Your bank will never ask for this information. Keep your bank details safe
- Got an email that seems to be from your bank suggesting you download some software or click on a link to a website?
- That site is false. It will steal personal data from your computer.

### In the **post**

Opened a letter claiming you've won an overseas lottery but need to pay some money up front before you can get your prize?

- The prize does not exist, and honest lottery companies don't ask for money upfront
- Ignore scam letters and emails offering rewards for help in transferring money out of a foreign location.

### On the **phone**

Taken a phone call from a stranger inviting you to buy shares that offer a huge profit and pushing you for a quick decision?

- The shares don't exist, or are totally worthless. You won't see your money again if you hand it over.

### In the **home**

Keep personal identity documents, passports and bank cards out of sight, so they're not visible to strangers.

- Make the effort to read your bills and bank statements. You may spot evidence of someone else spending your money
- Throwing out bills or bank statements with the rubbish provides fraudsters with a mass of information about you. Get a shredder and destroy them for good.

### On your **person**

Having trouble remembering Personal Identification Numbers (PIN) for credit and debit cards?

- Don't write these numbers down where people might see them. Never leave your PIN in the wallet or purse where you keep your plastic cards
- When at the cash point, always stand in front of the keypad and cover it when you put your number in
- Keep your credit card in sight at all times.