The true cost of scams

(and how to avoid becoming a victim)

Scams are big business – the average amount lost by Which? readers who have fallen victim to one is almost £1,500. We investigate the most common scams and show you how to protect yourself against them

A knock at the door, an email, a phone call or a click of a button on your computer – scammers exploit every route they can to trick you out of your money. And with good reason – scams are big business. New Which? research has found that our members who fall foul of one lose £1,488 on average. The Office of Fair Trading estimates scams cost UK consumers £3.5bn a year.

Our survey of 5,200 members (in June 2013) revealed that two thirds of you have been exposed to a scam in the last three years, or know a family member or friend who has. And around the same number say they're getting more scam correspondence than three years ago.

Scams are now so sophisticated that even the most savvy consumer can fall foul. Some 30% of people we surveyed are worried about friends and family members being taken in.

Which? members are most likely to fall for online shopping scams, which typically involve goods you've ordered failing to arrive or not being as described. Just 5% have come into contact with these, but when you do, 73% have been fooled. For more shopping scams, see p18.

The most common scam Which? members have faced is phishing emails – emails that pretend to be from organisations, such as your bank, trying to obtain personal details.

You're getting good at spotting scams. 94% of those who'd come into contact with phishing emails and 91% of those who'd come into contact with lottery/sweepstake/prize draw/competition scams didn't respond. In each case, nearly nine in 10 of you said it was because you could tell it was a scam.

But tricksters are inventing new scams. Based on your feedback, we've picked some to watch for and show you how to protect yourself.

GO ONLINE For more expert advice on your consumer rights, a video revealing the hallmarks of a scam, and advice on how to get your money back, visit **www.which.co.uk/scamclaim**

Which scams are most likely to fool us?

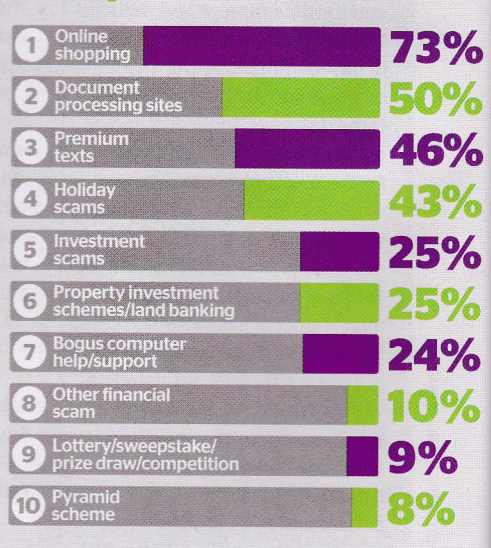


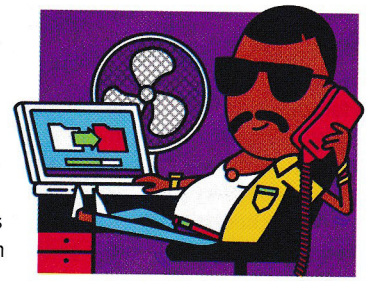
ILLUSTRATION BY: SPENCER WILSON

Bogus computer support scam

Which? members have lost: £215 on average, but Microsoft reports the average victim loses £745

Spotting the scam Typically, you'll receive a phone call out of the blue from someone claiming to be from Apple or Microsoft. They'll point you in the direction of harmless computer code or information on your computer, and tell you it is evidence of virus infections and impending system crashes. These 'computer support' services then offer to clean up the computer remotely, for a fee. We've also heard from readers about malicious software or viruses being installed, while others say they have had personal details stolen.

Is it legal? There's nothing illegal about offering services to clean up someone's computer and install software in return for money if there is a genuine problem. However, falsely claiming to be from a particular company and lying about viruses on your computer to obtain custom is fraudulent.



What you can do Legitimate companies will never call out of the blue claiming to have information about your computer (see panel, right). If you think you've been a victim of this, run a virus scan using your security software. Make sure it's up to scratch by reading our security software reviews, **www.which.co.uk/securitysoftware**. If you think your account or card details are at risk, tell your provider. Also tell Action Fraud, the UK national fraud reporting centre, at **www.actionfraud.police.uk/report_fraud** or call 0300 123 2040.

The illustration, left, shows the proportion of people exposed to a variety of scams in the last three years who said that they had responded to them.

The results are based on a survey of 5,200 Which? members we carried out in June 2013.

MEMBER VIEW
PC problems

Carolynne Jollye, Kent

Carolynne was using her computer when someone claiming to be from Microsoft called her out of the blue saying that they'd noticed problems with her PC.

She said: 'I was told to press three buttons and up came what looked like thousands of errors.' The caller offered to fix them for £153.65, which Carolynne paid on her credit card.

The 68-year-old from Sevenoaks, Kent, then watched as the caller took remote control of her computer, downloading and installing software and files.

Afterwards a friend at her local computer club told her that she'd been scammed, so Carolynne tried to cancel the payment but it had already gone through.

After calls and emails to the 'computer help' company were ignored, her credit card provider agreed to refund her money.

Carolynne, who paid another £70 so that a qualified computer expert could check and restore her PC, said: 'I now know every computer has got the "errors" that came up on my screen and they're harmless, but at the time it looked scary. Alarm bells should have started ringing when they said that they needed the money before doing anything.'

She has since received another call from someone claiming to be from Microsoft, but this time she just hung up.

How to avoid the computer support scam

PC support scams can leave victims out of pocket and at risk of having their personal details stolen. Here are the essentials to stay protected:

WHEN THE PHONE RINGS...

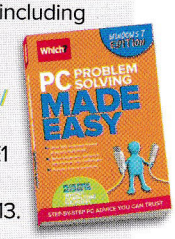
They say: ***I'm calling from [eg Microsoft] to talk about a problem with your computer***
What to do: Hang up. Legitimate computer companies say they will never call customers directly offering to fix computers, or send unsolicited emails requesting personal or financial information.

They say: ***Your computer is running slowly***
What to do: Hang up. Even legitimate computer companies can't tell this remotely, as any error report data sent from your computer is always anonymous.

They say: ***You have a virus on your computer***
What to do: Check this yourself using up-to-date, quality security software.

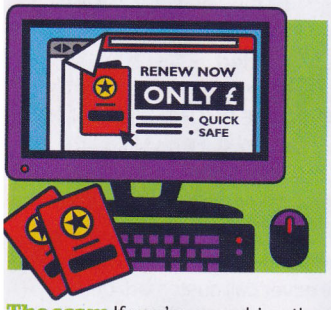
They say: ***Can I have remote access to your computer?***
What to do: Never allow a cold caller remote access to your computer. At best, they'll waste your time and money. At worst, they'll infect it with malware and potentially steal personal details.

Learn how to stay safe online and protect your identity – buy our book ***Computer Problem Solving Made Easy*** with a 20% discount for just £8.79 including UK p&p (RRP £10.99). Call 01903 828557 or visit **www.which.co.uk/books** and enter discount code ONLINE1 at the checkout page. Offer ends 30 Sept 2013.



Devious document processing sites

Which? members have paid £34 on average to sites that charge you for services you can get for free elsewhere



The scam If you're searching the internet for the right website to use to apply for or renew official documents such as a passport or European Health Insurance Card (EHIC), you'll likely come across some official-looking websites that offer to process your applications for a fee. All the sites we looked at claimed to offer a service that goes above and beyond what official bodies can deliver, such as form checking and application updates.

However, we don't think that they do anything important you can't do yourself for free on official sites.

Is it legal? Yes, but they must be upfront and honest about what they do. While all of the sites we looked at explained that they weren't affiliated with official government bodies or processes, disclaimers can be hard to spot – which is shown by the large number of people who had come into contact with these sites and ended up paying a fee. Indeed, we believe that one website's claims and the web addresses of other sites may breach consumer protection regulations.

What you can do We think these services are a waste of money, so be wary of sponsored links on search engine results – on Google these are highlighted in a grey box on the results page – as they're unlikely to be the official applications channel.

The official EHIC application service is at **www.nhs.uk/ehic** or on 0300 330 1350, while the official passport site is at **www.gov.uk/renew-adult-passport** or on 0300 222 0000.

Shopping scams

The average loss for a shopping scam is £112. Here are a couple to watch out for

1/ The selling scam

The scam You post a classified ad for something that you want to sell and are contacted by a 'buyer', who often claims to be overseas. The buyer 'accidentally' pays over the odds for the item, often by cheque. They then ask you to refund the difference, often by money transfer, only for the payment or cheque to bounce leaving you out of pocket.

Is it legal? No. This is fraudulent.

What you can do If you pay by money transfer you may struggle to get your money back. However, you can try contacting the service that you used, report the matter to the police and to your local trading standards. If you are concerned at all about a buyer you are dealing with then don't sell to them.

2/ The delivery scam

The scam You receive a delivery card through your door suggesting that a courier was unable to deliver a parcel. The card asks you to call what turns out to be a premium rate number – these have been known to charge hundreds of pounds for connecting to a recorded message.

Is it legal? No. This is fraudulent.

Other delivery scams In a variation, a 'courier' arrives unexpectedly at your home with a package. The label has your address on it but no name. You're asked to pay a nominal delivery charge by card using a device that 'skims' (records) your details. Or scammers, using stolen card details, buy a product and get it sent to your address. After you've signed for it, scammers posing as the company or courier say the delivery was mistaken and ask to collect it. Once handed over, you get demands to return the product.

Is it legal? If someone skims your details they're committing fraud and theft. If you're caught up in the 'mistaken' delivery scam, while theft and fraud relating to stolen cards has occurred further down the line, this is nothing more than a nuisance for those affected.

What you can do If you're not expecting a delivery, be suspicious – you can refuse to accept it. If you are worried that your details have been taken, call your bank and card provider straight away.

MEMBERS' TIPS
HOW TO AVOID BEING SCAMMED

"Never click on links in emails claiming to be from banks, PayPal etc. Instead, go to the official website in a new browser window/tab and log in to your account there.

"Nothing is so urgent that you need to commit a financial transaction immediately or without seeking a second opinion. Phone scammers always say by not committing you'll lose a discount; nonsense.

"If I don't know whether it's a scam or not, I go to the company's website or put the heading of the suspicious email into a search engine. This normally tells you if it's a known scam, and often says how to report it.

"If suspicious, never call the telephone numbers they provide to check if they are who they say they are – call the numbers listed for that company or organisation.

"Wherever possible, report scams to the relevant authorities or organisations to ensure they're aware of them.

ILLUSTRATION BY: SPENCER WILSON

Holiday horrors

When Which? members have fallen foul of holiday scams, it typically costs them £3,677. Here we put two of the most common types under the microscope

1/ Fake emails for help

The scam You receive an email from a loved one who is abroad, asking for urgent financial help. Which? member Michael Dawson received an email from a couple who he knew were on holiday in the Philippines, asking for money because they'd been robbed. Suspicious, he delayed answering until the next morning. Later that day he saw the couple, just returned from holiday, in the street, and found that the email had just been a plausible scam.

Is it legal? No. Obtaining money by deception is fraudulent.

What you can do Be very wary of urgent demands for money from loved ones by text or email – it's possible their phone has been stolen or their email account has been hacked. If in doubt, try contacting them by other means first, such as on their mobile or at their accommodation if you know where they are staying. One Which? member suggested agreeing a codeword or phrase with loved ones should a real emergency happen.

2/ Cheap holiday scam

The scam Watch out for holidays advertised at incredibly low prices as you might only get part of what you paid for, such as flights but no accommodation, or nothing at all.

Is it legal? There's nothing wrong with companies offering a discounted holiday, as long as they can provide the flights, transport and/or accommodation they say they will. If they obtain custom by deception then this is fraudulent.

What you can do If a company selling cheap holidays claims to be a member of a trade body such as Abta, check it's genuine (for example by visiting the trade body's website), and report anything untoward to it. Never pay for a holiday using a money transfer service, such as Moneygram or Western Union. If you paid on credit card and encounter fraud, contact your card issuer so it can investigate.

EXPERT VIEW

Vigilance is key

David Paine | Which? money expert

It's easy to think scammers only trick the most vulnerable and naïve, but our latest research shows that even the most switched on and careful consumer can fall foul if circumstances conspire against them.

Half of Which? members have been directly exposed to a scam in the last three years, which shows just how prevalent they've become. And, surprisingly, some of these scams are completely legal. In one area, document processing sites, we're raising our concerns with the government.

The vast majority of people who took part in our survey didn't respond to the scams, but even one response is too many. For those who have been scammed, it is encouraging to hear that some victims get their money back.

And while it's important to be vigilant, you shouldn't fear answering the door, picking up the phone, opening emails and surfing the internet. We can't let the scammers win.

Couple tricked by holiday club scam

Which? member David and his wife were coerced into attending a typically lengthy but plausible holiday club presentation, while they were on holiday in Spain.

The couple, from Cheshire, asked some probing questions before they hesitantly paid about £3,000 in return for the promise of luxury holidays at knockdown prices.

But when they were asked to attend another presentation and had no success in trying to book a promotional free week's holiday, they became suspicious. After being tricked into paying an £80 membership renewal fee a year later, the couple started getting cold calls from a company offering to sell their membership for an upfront payment.

David then found a Spanish consumer website that indicated he had fallen for a common scam. 'I felt such a mug for being taken in,' he said. He wrote to the holiday club to cancel membership and request a refund, but got no response. He also contacted trading standards and his credit card company.

After supplying detailed evidence, David got his money back from his credit card provider under Section 75 of the Consumer Credit Act. For more on your rights when paying by card, see **www.which.co.uk/s75**.

TAKE ACTION While some holiday clubs are reputable and trade in good faith, others may have sharp practices and mislead you about what you will get – and this is fraudulent. If you attend a holiday club presentation, remember you can leave at any time. Read the small print in a contract carefully, ask about your cancellation rights, and get all verbal promises in writing. If you have problems, call the UK European Consumer Centre (ECC) on 0845 604 0503 or visit **www.ukecc.net**, or report the club to Action Fraud at **www.actionfraud.police.uk/report_fraud** or on 0300 123 2040.