Young Friends Against Scams

Scams Fact Sheet

The all-in-one guide on how to spot scams, how to protect yourself and others from scams, and what you can do to help scam victims.

NATIONAL TRADING STANDARDS
Scams Team

Buckinghamshire&Surrey trading standards

SURREY

www.FriendsAgainstScams.org.uk

Scams and young people

Anyone can be targeted by a scam, regardless of age, gender, education or economic background.

Younger people are especially likely to be targeted through online scams such as fake websites which are used to get people to give them personal information such as bank account numbers or credit card numbers and pin codes.

Younger people often think they are less likely to be hit by scams, however there are many common scams specifically targeted to this age group. Common types of scams targeting this age group include subscription traps, social media, gaming, ticketing and job/rent scams.

Half of young people say they would never respond to an online scam.

PHISHING

Phishing is a way that criminals get sensitive information like usernames and passwords. This is usually done by an urgent email which will take you to a fake website which may look real or familiar to you. They are fake sites set up by criminals to gain your personal details. Phishing can also happen by phone via text messages known as smishing or by a call which is called vishing.

GAMING

Games that contain virtual money such as Fortnite have become an avenue of exploitation for criminals. There are many websites that are offering free virtual money for different games, provided you pass on your personal details. This could result in criminals having access to yours or your parent's bank accounts.

As games are being turned into mobile versions, criminals have started to create fake downloadable versions of the game. This is another way to get you to give your personal data to criminals.

FINANCIAL EXPLOITATION

Financial exploitation is abuse. It can take many forms, using different types of money including crypto. It might seem harmless, but is often linked to fraud, and it can be dangerous.

Young people are being encouraged, coerced or forced to:

- Open a bank account for some else to use
- Accept money (from crime into their account to transfer to someone else (money laundering)
- Let someone else use the bank card to buy things which they plan to fraudulently return (a type of fraud).

Young people may be approached:

- Using messages or fake job adverts online, including apps, social media, and gaming
- At cashpoints or in places like school, college or university
- Or by family, friends, boyfriends, girlfriends or partners

Financial exploitation can happen to anyone. It is not your fault.

Laundering money is illegal. In some cases, people go to prison. When someone manipulated or forced to commit a crime, this is called criminal exploitation, and financial exploitation is one form of it.

If you are worried that you or someone you know may be being exploited, you should talk to an adult you trust, such as a parent or carer, teacher, youth worker, or police officer.
.

SOCIAL MEDIA

Social media scams usually appear as enticing promotional deals and competitions.

- They may have genuine links, use official brand logos and/or links to enter your personal details.
- Clicking on these links sends your personal information to the criminals and potentially shares features and status messages from your own personal account for all your friends and family to see which could lead to them responding to the same scam.

How to spot them:

- You may be seeing a high volume of the same/similar status updates from people on your social media.
- Always check the branding for irregularities from what you believe it should be.
- Stay vigilant when you see new companies, organisations or brands pop up on your social media.
- It may be a criminal pretending to advertise.

Scams in the wider community

Scams are uninvited contact from another person(s) making false promises to manipulate people (victims) out of money. They come in many forms:

- email -letter -telephone -in person(doorstep) -websites

Average age of a person the criminals target is

75

53%

of people aged 65 and over have been targeted by criminals.

Estimated that only

5%

of victims report the crime.

Anyone in your community could be a victim of a scam, however, it is more likely to be someone like your elderly neighbour or a grandparent. This is because older people tend to be more vulnerable and therefore more likely to be deceived by the criminals.

Criminals get their victims hooked and keep responding to them because they target people who tend to be:

- Lonely
- Socially Isolated - many live on their own without family nearby or visiting regularly and are unable to get out of their home on their own due to disabilities and frailness.
- Feel shame about falling for another person's lies.

Because of the above, they may not report that they have been a victim.

The criminals have their details and will sell it onto others so they get bombarded and targeted continuously by numerous criminals.

The majority of scam victims suffer in silence, and don't tell even their closest friends and family.

You may be able to tell if someone you know is a victim when:

- There will be lots of post and clutter on all the tops of their furniture and on the floor.
- Their house will be in a general state of untidiness & probably not very clean as things are getting on top of them and they can't cope with what is going on.

And once they have responded

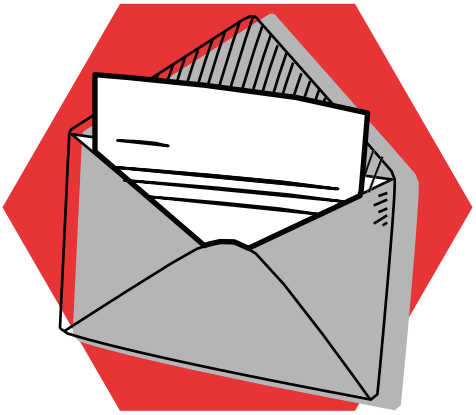
Scams cost the UK economy between

£5-£10,000,000,000.00

(Billion) a year

Types of scams

POSTAL



How can you spot them?

- Someone making frequent visits to the post office.
- Receive lots of mail everyday.
- Use lots of stamps.
- Receiving worthless or useless products in the post.

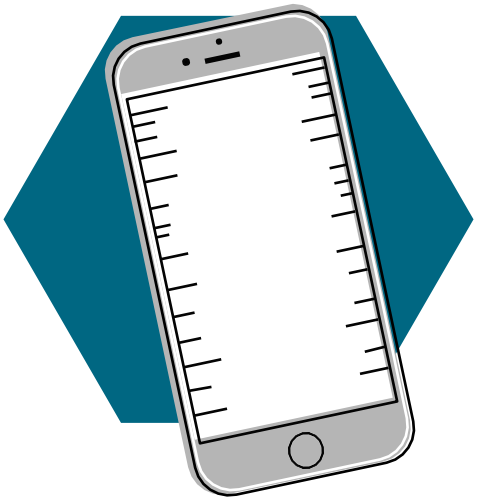
What can you do to help?

- Encourage them to put them directly in the recycle bin.
- Help them sign up to the mail preference service.
- If a major issue, get a relative to have all mail redirected to them so they can filter scam mail.

How can you stay safe?

- Do not respond to them. Put them in the recycle bin.
- Sign up to the mail preference service.

PHONE



How can you spot them?

- Make regular payments over the phone.
- Receive a high number of phone calls each day
- Speak of a helpful caller - someone who helped fix an issue.
- Speak of friends who call regularly.

What can you do to help?

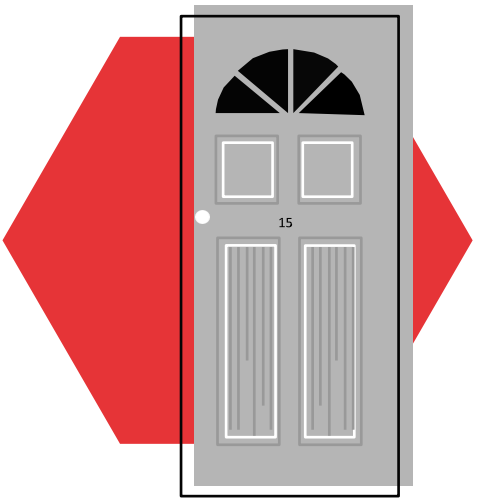
- Help them to block unknown calls.
- Encourage them to sign up to the telephone preference service.
- See if they can get a call blocker from a reputable supplier.

How can you stay safe?

- Block calls from unknown numbers.
- Sign up to the telephone preference service. Get a call blocker from a reputable supplier.

Types of scams

DOORSTEP



How can you spot them?

- Have had poor quality of work carried out.
- Had unnecessary work carried out.
- Feel under pressure to agree with doorstep callers.
- Make large cash withdrawals to pay doorstep criminals.

What can you do to help?

- Get them to display a No Cold Callers Sticker on their door. Suggest they could get more quotes if you know they are having work done.

How can you stay safe?

- Have a no cold callers sticker on your door.
- Don't be afraid to say NO.
- Get a second opinion.
- You have 14 day cooling off period on any contracts made in the home over £42. This means you are allowed to change your mind.

ONLINE

How can you spot them?

- Receive suspicious emails.
- Receive notifications about false final demands.
- Speak of a new relationship which is perhaps online.
- Make payments online via email or SMS text links.

What can you do to help?

- If they go online and use email, ask them if they've turned on a filtering system that sends unknown email addresses direct to a junk mail folder.
- Tell them about 2 factor authentication for extra security.

How can you stay safe?

- Do not respond to phishing emails asking for logins and passwords.
- Have a filtering system that sends unknown email addresses direct to junk box.

In your community

Be observant when out and about in your own neighbourhood. Rogue Traders come in various forms.

Typical work includes:

- Roof washing
- Roof repairs
- Tarmacking
- Tree cutting.

If you see vans and trucks **without proper company information** or **just a name and mobile number** then tell a parent or guardian that you think there might be rogue traders working on a neighbour's house and that you think they need to be reported.

There are approved trader schemes which should be used if your family ever needs a trader:

Trust Mark: This is the government-endorsed quality scheme for tradespeople working in or around the home. Members have been checked to ensure they meet government standards and comply with a code of practice.

www.trustmark.org.uk/homeowner

Which? Trusted Trader: Every trader you find on this site has passed the rigorous assessment set by trading standards professionals, and every customer review you read here is verified genuine by moderators.

trustedtraders.which.co.uk

Buy with confidence: Established by trading standards authorities, this scheme nationally recognises traders who have been vetted and approved to ensure they are trustworthy and operate fairly. It is by many local councils.

www.buywithconfidence.gov.uk

How to protect yourself

As well as protecting your community against scams, there are also ways you can protect yourself from scams that are targeted more at young people. Some of these may not apply to you now but they are great to know for your future:

1. If you think you have become a victim of a scam or of cyber crime, contact Report Fraud or Citizens Advice to report it. Contact victim support if you or someone you know has been affected.
   - Report Fraud: 0300 123 2040
   - Citizens Advice: 03454 040506
   - Victim Support: 08 08 16 89 111
2. You can report spam texts from your mobile phone by forwarding the message to 7726 for free!
3. Do not download anything unless a parent approves it.
4. If you get any suspicious emails or messages with links, asking for your personal details, report it and then delete it!
   - If you are not sure get a parent to look over it.
5. If you're suspicious of a link in your email, hover over it with your mouse and you can see the real URL.
   - On mobile phones you can do the same by tapping and holding your finger on the link.
6. Only visit parent-approved websites.
7. Always check you are on genuine, secure websites. You can do this by looking at the website address.
   - Does it look suspicious?
   - Does it match the website address of the company?
   - If you are logging onto a website, make sure it is the genuine login page.
   - HTTPS - S stands for secure - look for this.
8. Be careful of strangers or people you are not sure about contacting you through social media or in person.
9. Do not share personal information on social media or with people you do not trust.
10. Never give your bank details to anyone in person or over the internet.
    - Your bank will never ask you for all the details - they should already know some of them!
11. If you're under 19. You can confidentially call, chat online, or email Childline about any problem, big or small. Call them on 0800 1111. **https://www.childline.org.uk/get-support/contacting-childline**
12. Youth Access provides information about local counselling and advice services for young people aged 11 to 25 at **https://www.youthaccess.org.uk**