Avoiding Scams

Saying "No" or hanging-up is not rude

Produced by the Neighbourhood Watch Plus Project

Isle of Wight age UK

Need to know about scams?

Isle of Wight Trading Standards 01983 823000 visit www.iwasp.org.uk
Friends Against Scams - 20 minute e-learning www.friendsagainstscams.org.uk
Action Fraud www.actionfraud.police.uk 0300 123 2040
Neighbourhood Watch Scams toolkit
www.met.police.uk search for "Little Book of Big Scams" and "Little Book of Cyber Scams". Advice from Hampshire and Isle of Wight PCC.
Visit Take Five Campaign takefive-stopfraud.org.uk
Advice on fraud at Hampshire Police www.hampshire.police.uk
Age UK have advice and downloadable booklets on scams.
Investments - Financial Conduct Authority (FCA) www.fca.org.uk/scamsmart
For online security visit getsafeonline.org and www.cyberaware.gov.uk

Want to report a scam?

If a suspect is present at your door, dial 999
National fraud reporting Centre www.actionfraud.police.uk 0300 123 2040
Bogus or unfair traders Trading Standards 01983 823000

Want to avoid doorstep scams?

Fit a spy-hole and chain on your door - remember to use them.
Display a Trading Standards no cold-callers sticker.
Rogue traders can be attracted by an untended garden, or a home needing maintenance. Age UK IoW's Home Safe Service can assist with these issues.
Do not buy anything from cold-callers, request they leave.
Do not give to charities or anyone else at the door.
Agree a password with your utility companies.
Check the ID of all utility company employees who arrive unexpectedly, do not use the phone number on their ID badge to check.
Sign-up to Neighbourhood Alerts to find out about local scams.
Use trades people approved by Trader Approval Scheme, get several quotes.

Never employ a cold-caller.

Want to avoid postal scams?

Sign-up to the Mail Preference Service www.mpsonline.org.uk
Sign-up to the Fundraising Preference Service.
Sign-up to avoid un-address mail from Royal Mail 0345 2660858 optout@royalmail.com and the Direct Marketing Association for other providers on 020 7291 3300 at yourchoice@dma.org.uk.

Letters that say you have won a lottery, are from a love interest you have not heard of, offer amazing products or that request funds before you can get winnings or an inheritance, or can read fortunes are scams.
Postal offers that appear too good to be true are exactly that.
Look out for poor grammar, bad spelling, a PO Box, a foreign address or Request that you not to tell anyone about your good fortune are usually scams.

Never purchase anything from unsolicited mail.
Never send money or vouchers to enable someone to send you money.

Want to avoid online scams?

Using a mobile phone, a tablet or a personal computer can expose you to scams, malicious software, identity theft, hacking. There are some simple steps you can take to help prevent this.

- Keep your device updated and when security updates are no longer available, upgrade.
- Use appropriate up to date security software to help prevent malicious software.
- keeping a separate backup of your data will help to mitigate ransomware blackmail attempts.
- Use different strong passwords for different websites and avoid obvious passwords.
- Never trust that an e-mail is from your bank and do not click on links to your bank.
- Unsolicited e-mails requesting that you verify your logon details via a link, or that you need to send your personal or banking details, or transfer or receive money are most likely scams.
- Anyone you met online who requests money or vouchers, is going to be a scammer, even if you have a relationship with them. When messaged by someone new, check if their profile picture is obtained from elsewhere, image search with tineye.com to find where else it appears.
- Never trade off an auction site and always use the payment method in there terms & conditions.
- Check with the FCA if an investment is genuine register.fca.org.uk or www.fca.org.uk/scamsmart
- Avoid public WiFi hotspots for online banking, your details can be stolen, use 3G, 4G or 5G.
- When disposing of documents with your personal details on, shred them first to avoid ID fraud.
- Be mindful of holiday, recruitment, software, ticketing, pension, identity and investment fraud.
- The Age UK Isle of Wight Digital Inclusion Project can assist with IT competence & avoiding scams.

Need to tackle scams targeted at older people?

Older people are specifically targeted because criminals perceive them to be both trusting and vulnerable. When someone has given their details to a scammer, they are often put on a "sucker's" list, which leads to increased contact from scammers. When someone is isolated or lonely, a scammer can be the only person who regularly calls them. Communities and charities can tackle isolation.
Advice is available from Age UK Isle of Wight 525282, who offer befriending volunteers.
The Silver line is a 24hr support & chat line for older people www.thesilverline.org.uk 0800 470 8090
For dementia specific support and advice www.alzheimers.org.uk 0300 222 11 22
Protecting older & vulnerable people from fraud www.thinkjessica.com

Want to avoid telephone scams?

Fit a home phone call blocker with TrueCall technology, or buy a BT phone with TrueCall technology.
Some call blockers can be administered remotely by technology minded relatives.
Sign-up to the Telephone Preference Service www.tpsonline.org.uk 0345 070 0707.
If you are unsure who is calling, allow your answerphone to take the call or hang-up.
Sometimes, larger telephone providers can provide a blocking service.
Do not give out personal details on the phone to **ANY** cold caller - even if they say they are your bank, an IT company, your internet provider, or even claim to be the police - caller ID's can be faked. Verify who they are by calling them back on a published number. Fraudsters want to confirm your details, so may give you incorrect details and invite you to correct them, just hang-up.

Never give out banking or card details on your phone, even if it is your bank cold-calling you.
Never reveal your card PIN number to anyone, your bank will never request this.
Never click on a link in a text message from your bank, the sender's details can be faked.
Never give out personal or banking details on the phone to ANY cold-callers.
Never agree to buy any goods or services from a cold-caller on the phone.
Never visit a website or download any software if requested to do so by ANY cold-caller.