East Hunsbury Parish Council

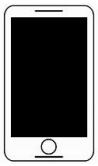
East Hunsbury Seniors
STAY ALERT – STAY SAFE
How to Avoid Scams

In conjunction with information from the **Age UK Scams Awareness** and **Avoiding Scams** online guides and information, please follow these helpful tips and have them 'ready' for when you need them. www.ageuk.org.uk

WHAT IS A SCAM?

Scams are a way of cheating people out of their money. A scammer may try to approach you on your doorstep, by post, over the phone or online. They'll often pretend to be someone they're not or make misleading offers of services or investments. New digital ways of communicating have led to an increasing number of scams and more people being tricked by them. But you can protect yourself by knowing what to look out for, and what to do if you suspect a scam. There are different types to look out for:

PHONE SCAMS



Scammers often try to trick people over the phone, so be wary of *uninvited* or *unexpected* calls.
What to watch out for:

- **Calls supposedly from your bank or police about fraudulent use of your credit or debit card, or bank account**.
  A scammer will ask for your PIN number and may tell you to give your bank card to a courier. *Neither your bank nor the police would ever do this.*

- **Pushy sales calls** or investment opportunities that seem too good to be true.

- **Calls about your computer**. The person calling may say your computer has a virus and ask you to download software to fix it. This is actually 'spyware' that will give them access to all your online information.

- **Be wary of any cold calls or texts from strange numbers** offering products or services, such as pension or debt management.

- Calls claiming to be about correcting your **Council Tax band or giving you a Council Tax rebate.** Your council would never call you about a rebate out of the blue.

- Calls asking you to **pay to renew your membership of the Telephone Preference Service**. The service is free and calls asking you to pay for it are scams.

WHAT DO YOU DO?

- **SAY NO.** Ignore a caller that asks you for personal information such as your PIN number or tells you that your computer has a virus.

- **REPORT ANY SCAMS**. Forward unwanted texts to 7726 (this is free) so your mobile phone provider can flag potential scams.

- **CHECK THE LINE.** Be aware that scammers can keep your phone line open even after you've hung up. Use a different phone, call someone you know first to check the line is free, or wait at least 10 to 15 minutes between calls to make sure that any scammers have hung up.

- **USE AN ANSWERPHONE**. If you have an answerphone on your landline or voicemail on your mobile, use it to screen your calls.

- **CHECK YOUR CALLS**. Get a caller ID device to see who's calling. Be aware though that some scammers appear as a legitimate number, for example, your bank or utility company.

WHO DO YOU CONTACT?

- Contact Action Fraud to report a scam 0300 123 2040

- Contact your bank if you receive a call about your bank account or credit card that concerns you.

DOORSTEP

A scammer may knock on your door pretending to be a trader, charity collector or simply in need of help. They may seem polite and friendly, but that doesn't mean you can trust them. Things to watch out for:

- **Traders** who say they've noticed something wrong with your property that they can fix.
- **'Police officers'** who ask to see your bank cards and PIN numbers. The *real police* wouldn't ask for this information.
- **Pushy sellers** with *large discounts* or *time-limited offers.*
- People who claim to be from **gas and electricity companies** but *don't have an official ID badge*.
    - **Deliveries** of any goods or products that *you didn't order.*
    - **'Charity collectors'** who seem pushy or can't supply a registered charity number (a legal requirement).
    - People who ask to come into your home because they say they need help, for example to use your phone, or because they feel unwell or want to use the toilet.

WHAT DO YOU DO?

You don't have to open the door to anyone you don't know. If you do, always think:

- **STOP** Are you expecting anyone?
- **LOCK** If not, lock any other outer doors before answering the front door. Some scammers work together – one keeps you chatting while another gets in through a back door.
- **CHAIN** Put the door chain on (but remember to take it off again or people with a key, like home help, won't be able to get in). Look through the window or spyhole to see who's there.
- **CHECK** Ask for an ***identity card*** and examine it carefully. If you're still unsure, phone the company the person says they're from. Get the number from a bill or your phone book. Don't worry about leaving someone waiting – if they're who they say they are, they won't mind. If you're being pressured or feel unsafe, contact friends, family or the police.

MORE TIPS TO AVOID DOORSTEP SCAMS

- Never buy from doorstep sellers.

- Ask for a '**No Cold Callers'** sign from your local council or get a printable version online and put it in the window.

- Set up a password with your utility providers to be used by anyone they send round so you can be sure they're genuine.

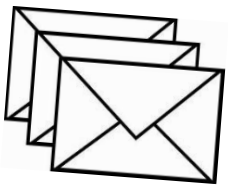
- Don't be embarrassed to say 'No' or ask people to leave.

- Never sign anything on the spot – take the time to think about any offer, even if it seems genuine. Where home improvements are concerned, it's always best to get several written quotes before deciding.

- Don't accept deliveries of anything you didn't order that's addressed to you. If you accept them without realising, contact the company they were sent from or your local police.

- **THINK**: if it sounds too good to be true, it probably is.

MAIL SCAMS



Mail scams are sent by post and may be addressed to you directly by name. They contain fake claims or offers that are designed to con you out of your money.

WHAT TO WATCH OUT FOR:

- **Lotteries** including foreign lotteries, or **prize draws** claiming you've won a fortune. These often look legitimate, with barcodes or ID numbers. The letter will ask you to pay an administration fee, buy a product or call a premium-rate phone number to claim your winnings.

- **Psychics and clairvoyants** who claim to have seen something in your future.

- **'Pyramid' investment schemes**, which ask you to pay a fee and recruit friends or family members to get a return on your investment.

- **People asking for money** because of unfortunate circumstances, like illness or poverty.

- **Letters from a 'solicitor'** about an unclaimed inheritance, often from a 'relative' overseas that you've never heard of.

WHAT DO YOU DO?

- **REJECT**: If you receive a letter you think is a scam, ignore it and throw it away. Never reply.
- **IGNORE**: Don't call any premium-rate phone lines mentioned in these letters. These numbers start with 09 and can cost up to £4 per minute to call.
- **VERIFY:** If you're unsure, check the details of the solicitor or organisation.
- **OPT OUT:** Try to avoid being added to mailing lists. For example, when you register to vote, tick the box to opt out of the 'edited register' (also known as the 'open register') as this can be used to send unsolicited marketing mail.
- **REDUCE:** Register with the Mailing Preference Service. This will stop many direct mailing companies from contacting you, but not all of them. Ultimately, it's not always easy to control what people send you. What you *can* control is your response.

WHO DO YOU CONTACT?

- Tell Royal Mail if you think you've received scam mail and send it to them with a covering letter.
- Report details of overseas scams to the Citizens Advice consumer service on 0808 223 1133.

EMAIL AND ONLINE

Email and online shopping can make our lives a lot easier, but they also create opportunities for fraud. Digital scams are becoming increasingly common and sophisticated, so it's good to know how to keep yourself safe.

WHAT TO WATCH OUT FOR:

- **Fake websites**
  These often look like a trusted organisation's real site to get you to give personal information. For example, you could get an email claiming to be from your bank, which directs you to a fake website and asks you to enter your account details.

- **Any emails from abroad asking for money**
  This may appear to be a stranded friend or relative asking for help but could actually be a scammer who has broken into ('hacked') that person's email address. Or it could be an email asking you to transfer a sum of money abroad in return for a larger reward later.

- **Emails with attachments**
  Some attachments contain viruses that 'infect' your computer. These could seem to be from someone you know, but their account may have been hacked.

- **Tax refund emails**
  An email claiming to be from HM Revenue and Customs (HMRC) offering you a tax refund if you enter your details. The real HMRC would never email to give you a tax refund. This is a common scam and many people have fallen victim to it.

- **Invoice emails**
  These appear to be from companies that you deal with regularly, or even a solicitor, and can seem genuine.

WHAT DO YOU DO?

- **STRONG PASSWORD**
  Always create a strong password for any online accounts, as this will help prevent your account being hacked. Aim for 7-13 characters. Choose a combination of letters, numbers and ideally some punctuation marks. Don't use obvious information about you, like your name or date of birth.

- **IGNORE ATTACHMENTS**
  Don't open any attachments to an email unless you know they're safe and from a trusted provider.

- **LEAVE THE LINKS**
  Don't click on any links within emails that claim to direct you to your bank, utility company or HMRC. Always search for the website yourself instead.

- **REPORT AND DELETE**
  Report scam emails to Action Fraud then make sure you delete them.

- **DON'T REPLY**
  Never reply to scam emails, even to say 'No'. This will let the scammer know that your email address is active and they'll send you more emails.

- **DOUBLE-CHECK**
  If you get an unexpected request for payment from someone claiming to be a trusted company or your solicitor, look up their phone number and give them a call to double-check.

- **FILTER JUNK**
  Check your email account is set up to filter junk (or spam) mail. This may help remove some suspicious emails from your inbox automatically.

- **STAY VIRUS-FREE**
  Make sure you have anti-virus software installed on your computer to protect it from viruses.

- **CHECK YOUR PREFERENCES**
  When shopping online, you may be asked if you want to receive mail or emails from the company. Make sure you tick or untick the correct box. You can also *unsubscribe* from any mailing lists you have signed up to.

WHO DO YOU CONTACT?

- To report scam emails, contact Action Fraud 0300 123 2040