SUFFOLK NEIGHBOURHOOD WATCH ASSOCIATION

MARCH 2018 NEWSLETTER

HMRC scam still doing the rounds

A member wrote in to advise that his wife received an email from HMRC, stating that a refund of £333 was due and that they were having problems refunding it.

Although the email looked very genuine, the reader was alert to the request to provide them with bank details, as the transfer had to be done within a day or would be time barred.

Scams are created to trick you into handing over money or personal details.

As well as leaving people out of pocket – Trading Standards estimate that £5-10 billion is lost to scams each year in the UK – victims are often left feeling a sense of shame and social isolation - but don't feel embarrassed - it can **happen** to **anyone**.

And we are sure you get the message - but you can still help by reporting scams.

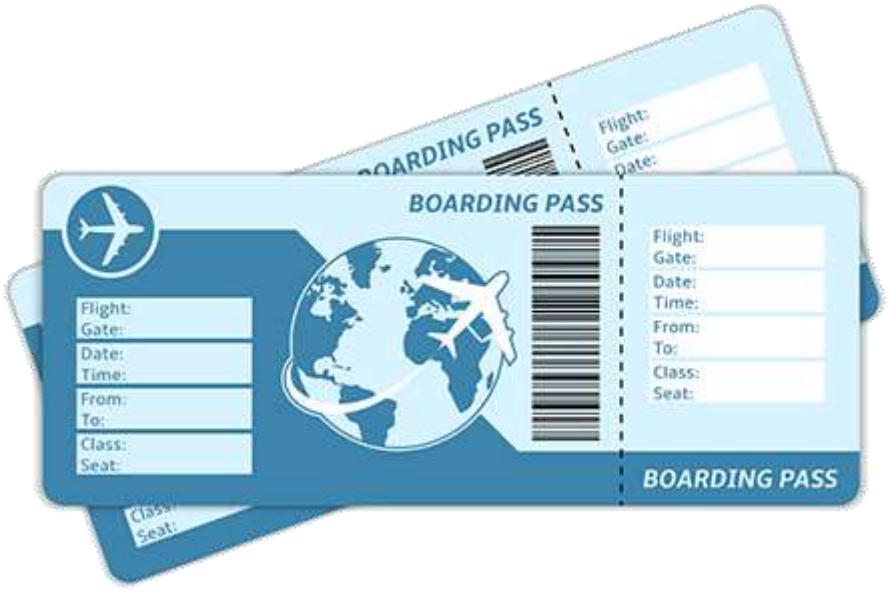
You can report scams to:
The Citizens Advice consumer helpline Telephone: 03454 04 05 06

scams to look out for.

Action Fraud, the UK national fraud office Online: via their online fraud reporting tool Telephone: 0300 123 2040

You can also join **Suffolk Trading Standards** and 'Take a Stand Against Scams' to help share information about different types of scams and how to support victims of scams in Suffolk.

Flight Ticket Fraud Alert



Fraudsters are attempting to entice victims who are looking for cheap flights abroad.

Victims have reported booking tickets via websites or a “popular” ticket broker, only to discover that after payment via bank transfer or electronic wire transfer, the tickets/booking references received are counterfeit. In some cases, all communications between the company or broker and the victim have been severed.

Fraudsters are targeting individuals who are seeking to travel to African nations and the Middle East, particularly those wishing to travel in time for popular public and religious holidays.

Prevention Advice:

- Pay safe: Be cautious if you're asked to pay directly into a private individual's bank account. Paying by direct bank transfer is like paying by cash – the money is very difficult to trace and is not refundable. Wherever possible, pay by credit card or a debit card.
- Conduct research on any company you're considering purchasing tickets from; for example, are there any negative reviews or forum posts by previous customers online? Don't just rely on one review - do a thorough online search to check the company's credentials.
- Check any company website thoroughly; does it look professional? Are there any spelling mistakes or irregularities? There should be a valid landline phone number and a full postal address so that the company can be contacted. Avoid using the site if there is only a PO Box address and mobile phone number, as it could be difficult to get in touch after you buy tickets. PO Box addresses and mobile phone numbers are easy to change and difficult to trace.
- Be aware that purchasing tickets from a third party, particularly when initial contact has been made via a social media platform can be incredibly risky.
- If tickets to your intended destination appear cheaper than any other vendor, always consider this; if it looks too good to be true, it probably is!
- Look for the logo: Check whether the company is a member of a recognised trade body such as ABTA or ATOL. You can verify membership of ABTA online, at www.abta.com.
- If you have been affected by this, or any other type of fraud, report it to Action Fraud by calling 0300 123 2040, or visiting www.actionfraud.police.uk.

A message from ACTION FRAUD

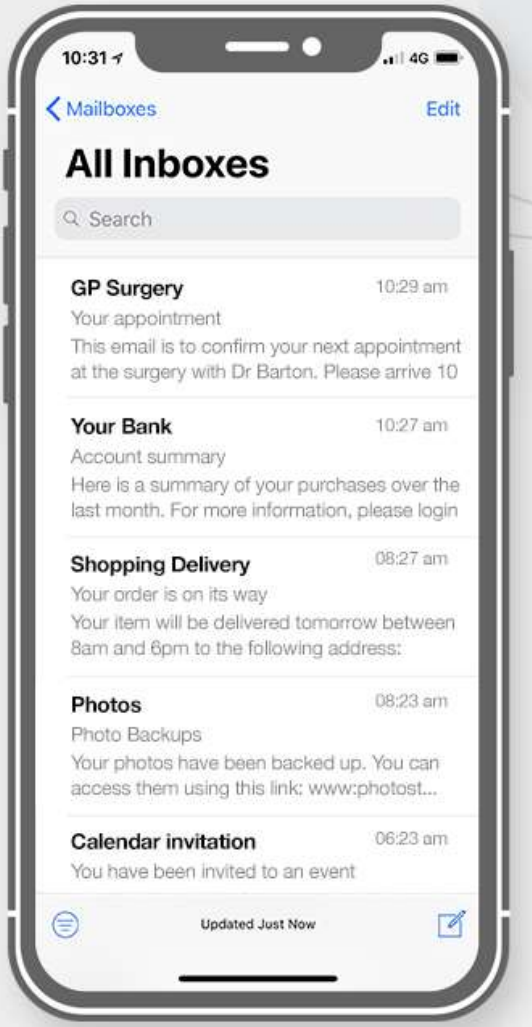
How to protect your email against criminals

@cyberprotectuk

Secure your email account in 2 simple steps

Why are email accounts so important?

Email accounts contain a wealth of sensitive information. Criminals can use your email to reset passwords or obtain personal and financial information, such as your bank details, full address or DOB, leaving you vulnerable to identity theft and fraud.



What you need to do:

- ☑ Use three random words to create a strong, separate password for your email account.
- ☑ In the security settings of your email account, enable two-factor authentication.