

Scam Marshal Newsletter

April 2023

Total Scam Marshals across the UK: 2,428

Andrew Judd
Police Station
Tufton Street, Ashford
Kent
TN23 1BT



**NATIONAL
TRADING
STANDARDS**

Scams Team

Ofcom study: Nine in Ten adults in the UK have come across content they suspected to be a scam

Nearly half of the participants in the study (**46%**) said they had been personally drawn in by an online scam, while two in five (**39%**) knew someone else who was a victim.

A quarter of those who said they'd encountered online scams had lost money as a result (**25%**) - with a fifth (**21%**) being scammed out of **£1,000** or more.

More than a third (**34%**) of all victims also reported that the experience had an immediate negative impact on their mental health, increasing to nearly two-thirds (**63%**) among those who had lost money.

If you think you've been a victim of some sort of online fraud – or even if you've spotted a fraud but not been caught out by it - report it to Action Fraud straight away on **0300 123 2040**

Scam letters from 'People's Postcode Lottery'

People are being told to watch out for a fake letter, which claim that recipients have won thousands on the People's Postcode Lottery.

This scam letter includes the People's Postcode Lottery logo and branding. It claims that your postcode has been randomly selected from the electoral roll database and says your 'win' is part of a programme to award money from previously unclaimed prizes. The letter asks you to call a number to claim your prize. At this point the criminal will ask you to provide personal information, which will likely include your bank account details.

The advice is to always contact the People's Postcode Lottery directly via a verified phone number (08081 098765), e-mail address or postal address if you genuinely believe that you may have won a prize.

To report a potential fraud, please contact Action Fraud on **0300 123 2040**.

Return address: FREEPOST, NTSST, MAIL MARSHALS

How to spot the signs of a fake HMRC tax refund email

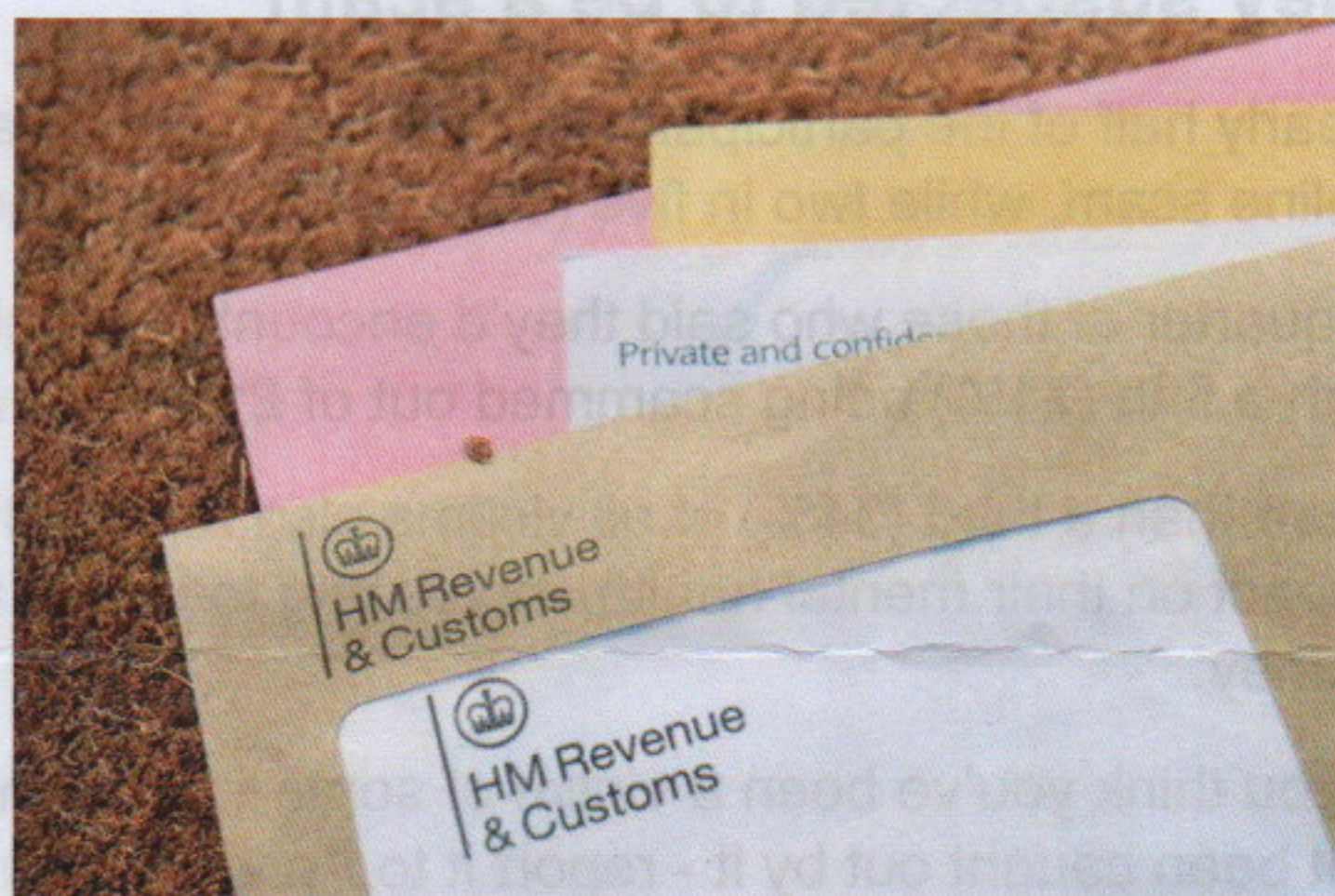
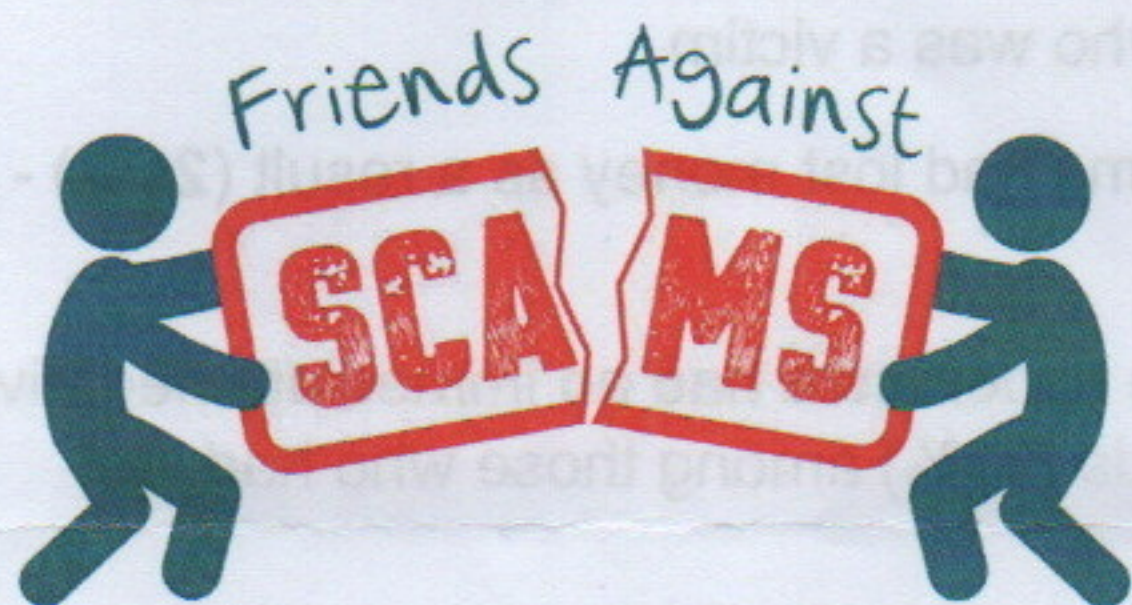
Criminals are sending people fraudulent emails pretending to offer people a 'tax refund' from HM Revenue & Customs. The Government has issued a warning about the scam which criminals use to try and steal personal details, otherwise known as phishing.

Included in the emails is a link which says the recipient can claim a tax refund. Once the link is clicked, a website opens with forms to fill in personal details.

One example of these emails used HMRC branding to try to appear legitimate, while stating: "After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund."

HMRC will never send notifications by email about tax rebates or refunds.

Criminals may spoof a genuine email address or change the 'display name' to make it appear genuine. If you receive an email like this, forward it to report@phishing.gov.uk and Action Fraud.



Useful tips to protect yourself:

Passwords: Use a strong and different password for your email using 3 random words. Your email password should be strong and different from all your other passwords. Your emails contain a lot of information about you that criminals can use to scam you or people you know. So it's crucial you use a strong password for your email account that you don't use for other accounts.

Use your browser's password manager: If your web browser offers to save your password when you're logging in or creating an account, always do so. These 'password managers' will help you create and store strong, different passwords for all your different accounts.

2-step verification (2SV): If you're offered '2-step verification' to protect your email and social media accounts, always use it. 2-step verification (sometimes called 2SV) helps to keep criminals out of important accounts, such as your email and social media, even if they have your passwords. It works by sending a code or PIN to a device only you have access to, such as your phone. Typing in this code or PIN helps to prove your identity. Never give that PIN out to anyone else.