Scam Marshal Newsletter

January 2025

Total Scam Marshals across the UK: 2,618

Address box

Welcome to your fourth quarterly Scam Marshal newsletter for 2024

In this edition we'll examine how the year of 2024 saw a rise in Police impersonation scams, explore the ever-growing use of deepfake videos, and delve into how sim card swap fraud nearly doubled in 2024.

Phoney Police

Criminals are again impersonating the police and using telephone calls to scare people into revealing their financial details. Typically, you're told that you're being defrauded, and the police are trying to help you, but the calls can sometimes be accusatory, claiming you have been reported for a crime.

Fraudsters impersonate the police to scare you into action by pretending to be a voice of authority. Some statements they typically say are: **'You've been a victim of fraud', 'Someone reported you'** and **'You're going to be arrested'.** If you receive a call like this, make sure to not give away any personal information, and maybe consider installing a call blocker to reduce the chances of these calls happening again.

Deadly Deepfakes

Elon Musk, Martin Lewis and Holly Willoughby were all featured in videos where they appeared to promote lucrative investments. However, the celebrities never actually agreed to promote these products and never said what they appeared to say.

That's because these videos were the work of deepfake technology fuelled by accessible online artificial intelligence (AI) tools.

Sometimes, deepfake videos use cloned voices to create the impression that someone said something that they never said. Other times, real footage of someone was manipulated and put together to make it seem as if the person was promoting something they weren't.

Always make sure to check when receiving or watching a video which looks slightly suspicious whether it be from a celebrity or anyone. **Think before you act**!

Return address: FREEPOST, NTSST, MAIL MARSHALS

When you send us your scam mail, please keep the letter/s in their original envelope and write the date received as it will help with our investigations. If you need more Freepost envelopes, email us at friendsagainstscams@surreycc.gov.uk.

Sim-Swap Situation

Reports of criminals hijacking phone numbers via sim cards to steal bank security codes have doubled since 2023. Criminals are doing this is by posing as the victim over the phone to convince their phone provider to switch the number to a new sim card that the criminal is in possession of. Once the number is linked to their own Sim, the criminal can attempt to access the victim's online banking, email and social media accounts as the one-time passwords (OTP) would now go the number on their Sim card.

Action Fraud state that reports of Sim-card fraud have reached over 2000 at the end of November 2024, having doubled from 2023. There are many reasons for this, such as an aging population and technological advancements. Action Fraud believe that the surge in fraud reports is likely due to an increase in public awareness of Sim swapping.

5 steps to prevent Sim-swap fraud:

- **Secure your mobile account:** Ask your network provider about any additional security
- **Turn on Multi-Factor Authorisation**: Most email, social media and online bank accounts can be secured with multi or two-factor authentication. Avoid SMS-based checks if you can (although they're still better than no MFA at all)
- **Clean up your online profile:** Restrict who can see your social media profiles and avoid sharing details such as your date of birth and phone number
- **Recognise the signs and act:** Call your network immediately if you receive an unexpected message about your Sim being ported or a PAC request
- **Tell your banks:** Warn any financial organisations so that they can freeze your accounts, and keep a close eye on your bank statements, email and social media accounts for unusual activity. Change your passwords and disable SMS as an authentication method

Friends Against Scams

The National Trading Standards Scams Team raises awareness of mass marketing fraud through the Friends Against Scams initiative. Anyone can access the free online training at **www.FriendsAgainstScams.org.uk**, or attend a face-to-face meeting organised by one of over 2,500 SCAM champion volunteers throughout the UK, and join the over 1 million friends against scams!.

www.FriendsAgainstScams.org.uk has a free short (15min) scams awareness course that can help you protect yourself and loved ones from scams. Anyone completing this session becomes a Friend. So far, over 1,100,000 people have completed this training, helping to take a stand against scams. You can complete the training at **www.FriendsAgainstScams.org.uk/elearning/coop.**

Action Fraud – 0300 123 2040 – www.Actionfraud.police.uk

Police Scotland – 101 (from within Scotland) - www.scotland.police.uk

Citizens Advice – 0808 223 1133 – www.citizensdvice.org.uk

Citizens Advice Scotland - 0800 028 1456 - **www.cas.org.uk**