

Consumer Alerts – October 2026

Sim swap telephone scam

Beware receiving a cold call from an individual claiming to represent your mobile phone network provider. The caller falsely informs the victim that their current SIM card is outdated or broken and must be replaced at no cost to the mobile user. To process this fictitious upgrade, the caller triggers a security text message to the victim's handset and requests that they read the one-time passcode (OTP) aloud to verify their identity.

This security code allows the fraudster to perform an unauthorised SIM swap, transferring the mobile number to a criminal device causing the victim's phone to instantly lose connectivity and display a permanent "No Service" status. By hijacking the telephone number, fraudsters can intercept text-based two-factor authentication codes and security alerts, granting them possible access to online banking platforms and personal accounts.

Remember, one-time PINs and verification texts are strictly confidential and must never be read aloud to any caller.

Beware military romance scams

Beware romance scams involving alleged American military personnel. The scammer will pretend to be a soldier or service member, building an online relationship overtime, gaining the victims trust to then exploit them financially. The soldier or service person will use a fake online profile and will often claim to be deployed overseas. Deployment overseas provides a believable reason

why they can never meet and why live calls are difficult. The alleged deployed soldier may begin asking for money, saying they need money for leave, flights, medical bills or due to a frozen bank account.

Once the scammer has gained your trust, which may be over weeks or months of communication, they can introduce a crypto investment opportunity, a fake platform that shows made up profits.

Beware bank impersonation scams

Beware receiving a text message claiming to be from your bank about a new payment that has allegedly been set up on your account, providing a number for you to call if you do not recognise the transaction. The person on the other end of the line will tell you your bank account has been compromised by scammers. They will request your bank details to help protect your money and may ask you to transfer your money into a 'safe account' or hand over your debit card so it can be replaced.

Ignore any message that is from a mobile number and not your bank, use the telephone number on the back of your bank card to contact the bank to check if concerned.

Report it to Report Fraud via www.reportfraud.police.uk or on 0300 123 2040.

Contact the Trading Standards Service via the Citizens Advice consumer Helpline on 0808 223 1133.

Check out our Facebook page, www.facebook.com/StanleyDards/

