

I have listed below 4 alerts/scams. They refer to persons impersonating Police Officers, a scam lottery letter, a new phishing email and a new smishing scam. At the bottom my email is my normal advice on how to avoid becoming a victim.

Scam 1 – Scam calls impersonating Police.

Please be aware of scammers impersonating Police.

3 people were called in the Folkestone area yesterday by scammers impersonating Police Officers. In one call they asked if they knew a person who had been arrested using their Barclay Card and in the other 2 calls, they stated that people had been arrested for Fraud. None of those called were taken in by this and disconnected the calls and contacted Police.

If you receive a call from someone claiming to be the Police and you are not sure if it is a genuine call. Then obtained their details and call 101. Never call a number that they supply and try to use an alternative telephone to the one that you were called on. If you cannot use an alternative telephone, then either wait 5 minutes to call using the same phone or before ringing 101, call a family member to make sure that the line has been cleared, as Fraudsters will stay on the phone and you could yourself speaking to them again.

Remember, the Police will never ask you for passwords, Pin numbers or ask you to remove cash to give to an investigator or courier as part of an investigation

Scam 2 – Lottery Scam Letter

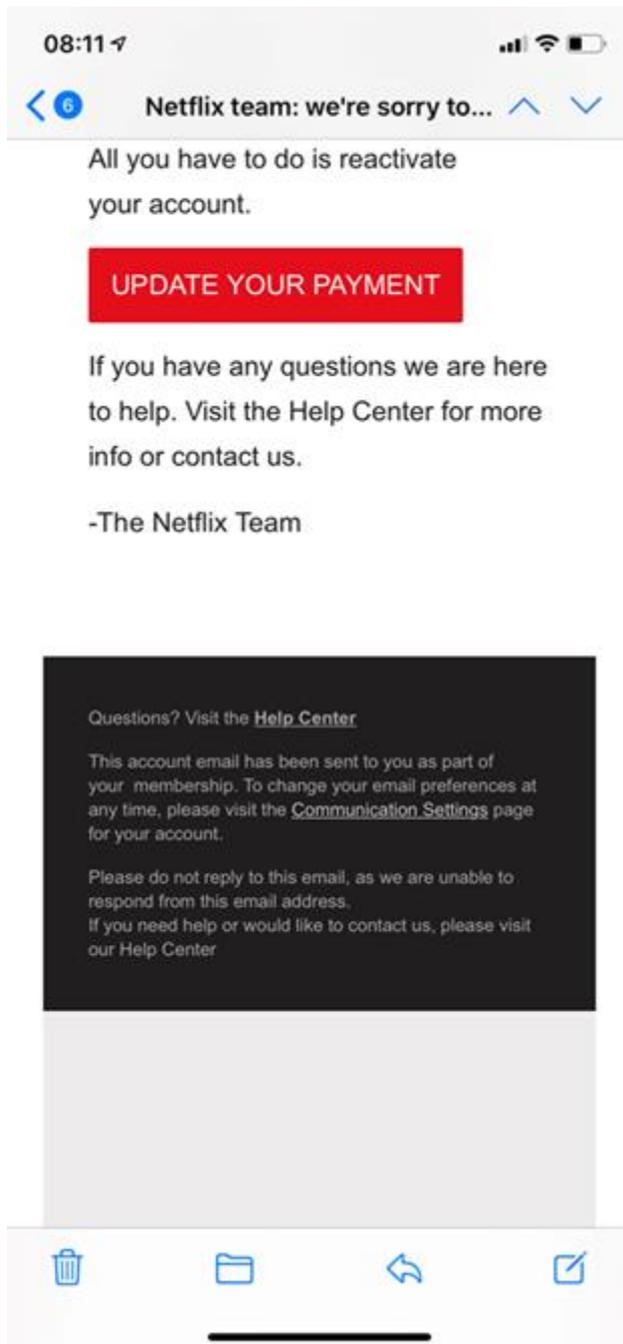
The below letter was received by a person in Ashford and states that this is from the Covid-19 Relief Lottery. This is a new scam. If you receive this please do not respond and report to Action Fraud Action Fraud by calling 0300 123 2040, or by using their online form.



SCAM 3 – NETFLIX Phishing email

The below email was received this week and is a new phishing email with scammers impersonating Netflix. It asks you to click on a link and takes you to a long scam email to try and obtain your personal data.

Please be on the lookout for this and if received, do not click on the link and please forward to report@phishing.gov.uk who are dealing with these types of phishing emails.



Scam 4 – Revolut Card Smishing Text message

If you are the owner/user of a Revolut Card, which is a type of pre-paid card that can be used in the UK or abroad without charges, please be aware of a scam text message that is being sent out to card holders impersonating the company. It will state that your account is frozen and that you need to click a link to verify your ID. Revolut are aware of the scam and are taking steps to stop this but in the meanwhile, if you get this message please do not click on the link. If you are unsure if it is a scam, then contact Revolut using a trusted number.

If you believe a text message is a smishing scam, then you should report it to the company who allegedly sent you the message. This'll give them the chance to alert other users to the risks. Some organisations even have a dedicated email address for you to report potential

scams to. If you've been a victim of a smishing scam, then you need to report it to Action Fraud by calling 0300 123 2040, or by using their online form.

Please remember the following advice -

Take Five -

Stop -Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge -Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect - Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

And use our own A, B, C of scam awareness:

A- Never **Assume** a caller, email or text is genuine.

B- Never **Believe** a caller, email or text is genuine.

C- Always **Confirm** by contacting a trusted number, family member, friend, your bank's fraud department or the police to check if it's genuine.

Report scams at www.actionfraud.police.uk

==

Steve Kelly

Prevent & Protect Fraud Officer

Intelligence | Essex & Kent Serious Crime Directorate