Kent Fraud Alert System

TAKE FIVE TO STOP FRAUD™

More AI (Artificial Intelligence) Scams to be aware of

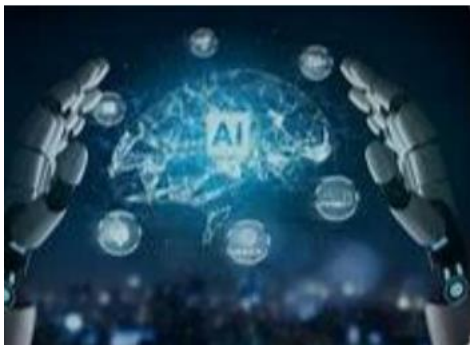
Deepfake videos

A deepfake video is where the person in it has been digitally altered to appear as a different person. Criminals use this technique to make it appear as if someone, usually a popular celebrity or trusted person, is saying something they are not. For example, they can make it seem like a celebrity is promoting a fraudulent investment scheme with words from their own mouth. However, the video is fake.

Deepfake videos can also be used to steal people's identities or to pass verification checks and access victims' accounts as well as to create images of completely non-existent people.

How to spot these scams:

- Some deepfake videos use lip-syncing, so watch the video carefully for lip-syncing that is slightly off.
- Pay attention to details in the quality – does the hair, lighting and skin tone of the person look believable? Is there any blurring in the video?
- Listen out for strange background noises or robotic voices.
- Look for unnatural expressions – it is hard to mimic natural blinking and AI often lacks facial emotion and AI body movements can seem off.
- Where does the video come from? If it is not an official account or if it is an account you have never heard of and you have not seen the video anywhere else, be wary.



If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police

Kent Fraud Alert System

TAKE FIVE TO STOP FRAUD™

Investment Scams

We are still seeing a number of reports of victims for this type of criminality. Often the victim will only become aware that they have been scammed when they either to try to encash or withdraw part of their investment.

How to protect yourself from Financial Investment fraud:

Investment opportunities: Do not be rushed into making an investment. Remember, legitimate organisations will never pressure you into investing on the spot.

Seek advice first: Before making significant financial decisions, speak with trusted friends or family members, or seek professional independent advice.

FCA register: Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that is not regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police

Kent Fraud Alert System

TAKE FIVE TO STOP FRAUD™

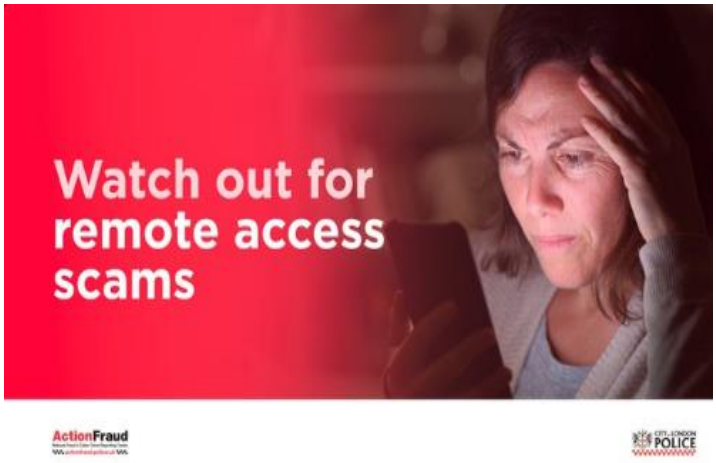
Remote Access Scams

Another Fraud reported all too often is remote access scams.

Remote Access scams will often begin with a browser pop-up saying that your computer is infected with a virus or a call from someone claiming to be from your bank saying that they need to connect to your computer in order to cancel a fraudulent transaction on your account. Regardless of the narrative that the fraudster's use, their goal is to steal your money or access your financial information by tricking you into allowing them to remotely connect to your computer.

Remember -

- A tech company, telecommunications provider, bank or service provider will never contact you out of the blue requesting remote access to your device.
- Only install software or grant remote access to your computer if you are asked by someone you know and trust, such as a friend or family member, and never as a result of an unsolicited call, browser pop up, or text message.
- Your bank will **not** ask you to reply to an e-mail with personal information, or details about your account. If you contact them, use a phone number/email address that you know to be true, rather than one sent to you in an email – it may be false.
- It is okay to reject, refuse or ignore requested. Only criminals will try to rush or panic you.



If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police

Kent Police

Report a non-urgent crime online **www.kent.police.uk/report**
Talk to us on LiveChat – available 24/7 **www.kent.police.uk/contact**
In an emergency, if crime is in progress or life is in danger call **999**
If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.
www.kent.police.uk

Kent Fraud Alert System

TAKE FIVE TO STOP FRAUD™

Advance Fee fraud

A Kent resident has reported receiving a call from a person stating that they worked for an advisory group on behalf of the Government and that they had overpaid their mortgage and were owed more than £4,000 and that they had a cheque ready to post to them. They then stated that they need to pay some admin fee's first and needed to send £300 to an address via royal mail. It was a scam and the intended victim disconnected the call.

This is a variation of various types of telephone scams that we receive reports of each day and is known as an Advance Fee Fraud. This is when fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise.

Remember the ABC of fraud awareness –

- A – Never Assume that a caller is genuine.
- B – Never believe that a caller is genuine.
- C – Always confirm by disconnecting the call and calling back via a trusted number, no one supplied by the caller.

If they call out of the blue with offers of money in return for a fee, then STOP, it is a SCAM.

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police

Kent Police

Report a non-urgent crime online **www.kent.police.uk/report**
Talk to us on LiveChat – available 24/7 **www.kent.police.uk/contact**
In an emergency, if crime is in progress or life is in danger call **999**
If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.
www.kent.police.uk

Kent Fraud Alert System

Fake McAfee emails

If you get an email like the below, it is a scam and please do not click on the link, as it will take you to a realistic looking website designed to steal your personal and financial data.

Having just checked my personal emails, I have found that I have received these every day this month. If you look at the email below you can see straight away that the email has an incorrect spelling of McAfee and the email address that this has been sent from, has no links to McAfee.

Always be wary of clicking on links in emails and text messages, as they are likely to be a scam.

Report suspicious emails by forwarding them to: Report@phishing.gov.uk

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police

Preventing fraud

Together, let's stop scammers.

Remember, ABC:

never Assume

never Believe

always Confirm

Get the latest scam advice: @KentPoliceECU

------ Original Message ------
From: info+dfwdvyvct@bibliotecadaterra.be
To: XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Sent: Tuesday, July 30th 2024, 13:27
Subject: RE: ⚠ Your Account Will Be Removed Today:07/30/2024! All Are Unprotected)

YOUR SUBSCRIPTION M.cAfee MAY HAVE EXPIRED!

Your subscription of M.cAfee Total Protection may have expired Today Tue, 30 Jul 2024 08:27:10 -0400 (EDT)
After the expiration date has passed your devices will become vulnerable for Hackers.

reference code	47126UK
Name	XXXXXXXXXX
account-ID	10681

Keep your Devices Safe NOW >>

Available (-85%) Renewal Discount Today : 4 min 19 sec
Renew your subscription by clicking the button bellow.

RENEW NOW