

#### **Courier Fraud ALERT!!! - Please share**

We have seen an increase in reports of courier fraud across the county during February.

Last week we received 6 reports in one day in the Dartford area.

Those 6 attacks have been using various ways to target individuals but the most popular has been to call stating they are an officer from a London Police Station and that someone has either been arrested with the victim's card or that they have arrested a family member with their card. They will then ask for money or the victim's cards as evidence, which they will collect by courier. The criminals may even ask you as part of an investigation to purchase gold/gold bullion for them to collect!!!

Another call impersonated HMRC stating the victim owed Tax and that they need to pay a courier by that evening or they face being arrested by Police.

All of these are scams, the Police and HMRC will never contact you like this.

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.

Have you been asked to withdraw cash by the police?

### This is a scam.

The police or your bank will never:

- · ask for your bank details or PIN
- ask you to transfer or withdraw and handover sums of money
- send a courier to collect your bank cards, cash or PIN

If you are unsure about a call or visitor you have received:

- Don't give out any personal or financial information.
- Hang up or close your front door to check the caller's identity.
- If they phoned you, wait 10 minutes before you use the phone again (or use a different telephone) in case they stay on the line.
- Contact their company yourself or dial 101 for the police do not call a number they have provided.
- Report suspicious activity straight away.



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,
was too a contact of the service and the service 1800.











#### **Life Insurance Fake Emails**

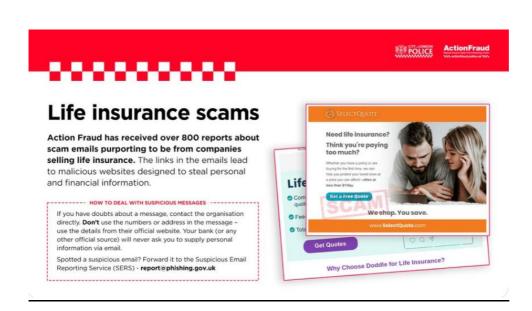
Watch out for these FAKE emails claiming to sell life insurance. Action Fraud has received 800 reports of these scam emails, designed to steal your personal information.

Always 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.

You can also obtain extra advice by visiting the Home Office website -

Stop! Think Fraud - How to stay safe from scams (stopthinkfraud.campaign.gov.uk)















#### **Email Account Take Over – URGENT FRAUD ALERT**

TO STOP FRAUD

Last week I received several reports of people's emails being compromised. The criminals will take over the victims account and then impersonate them. They will email people within their friends list stating that they are ill or injured and cannot get out of the house and need to get a gift card for a family members birthday and ask them to do this for them and to email the gift card code. However, it is a scam. If you get an email like this apply ABC and never Assume or Believe a message asking for money is genuine and Confirm by calling the person and speak to them.

Additionally, you can check to see if your email address has been compromised by checking on the below publicly available website –

<u>Have I Been Pwned: Check if your email has been compromised in a data</u> breach

You just need to type your email address in and the website will tell you if criminals possibly have access to your email account.

The following is advice from National Cyber Security Centre on how to create a strong password –

#### Three random words - NCSC.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.

### **Preventing fraud**

Together, let's stop scammers.



Remember, ABC:



never Assume



never **B**elieve



always Confirm

Get the latest scam advice: **@KentPoliceECU** 











#### **Shoulder Surfing at Cash Points**

I have recently been speaking to colleagues in the banks who have informed me of a rise in shoulder surfing incidents in Kent. This basically involves when you go to use a cash machine and the criminal then looks over your shoulder to see your PIN number. They will then follow you away and distract you, whilst an accomplice steals your Bank Card.

When using a cash machine always be aware of anyone standing too close behind you and shield your hand when inputting your PIN Code. If you think that someone is standing too close or acting suspicious, then do not carry out the transaction and report it to Bank Staff or the Police.

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.



#### **Preventing fraud**

Together, let's stop scammers.



Remember, ABC:







Get the latest scam advice: @KentPoliceECU











#### Fake Email – Mystery Box with free prizes

Watch out for these FAKE emails claiming to give away a mystery box with free prizes. Action Fraud has received 7,902 reports of these scam emails, designed to steal your personal information.

Always 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.

You can also obtain extra advice by visiting the Home Office website –

Stop! Think Fraud - How to stay safe from scams (stopthinkfraud.campaign.gov.uk)



### **Preventing fraud**

Together, let's stop scammers.



#### Remember, ABC:







Get the latest scam advice: @KentPoliceECU











#### **Fake TV Licensing Emails**

Watch out for these FAKE emails claiming to be from TV Licensing and stating that your license is about to expire and that you need to click on a link to update your details. However, it is a scam and it is designed to steal your personal information.

Always 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.

You can also obtain extra advice by visiting the Home Office website –

Stop! Think Fraud - How to stay safe from scams (stopthinkfraud.campaign.gov.uk)



### **Preventing fraud**

Together, let's stop scammers.



Remember, ABC:





always Confirm

Get the latest scam advice: @KentPoliceECU







