Employment Scams

We have had a number of reports recently where people have been victims of employment scams which have been a combination of applying for a job that

they have seen on social media or being approached directly, as a result of the victim has placing their CV on line.

The Fraudsters will normally state that they are an agency and as such work on a commission basis and in order to secure you the job, will request you pay various fees. They may also ask you for bank account details to arrange setting up salary payments.

However, there is no job and any fees paid go straight to the fraudsters.

The following will take you to the Action Fraud web site which has more information on how these scams work and how to protect yourself.

Employment fraud | Action Fraud

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

TO STOP FRAUD

Together, let's stop scammers.



Remember, ABC:

never Assume

never Believe

🔟 <u>always</u> Confirm

Get the latest scam advice: @KentPoliceECU

Contacting 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 deaf or speech impaired, text **`police**' and your message to **60066**



Latest PayPal Phishing Scam

Watch out for the latest PayPal phishing email, that exploits their "Request Money" feature and attempts to frighten you into calling a malicious telephone number so that the fraudsters can obtain your financial data.

To find out more about this and other PayPal scams, visit the below site for further details.

Learn to Recognize Scams and How to Avoid Them | PayPal TC

Forward this or any suspicious email 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.

.....

PayPal 'request money' scam reported 275 times

The scam exploits PayPal's 'request money' feature to try and scare people into calling a malicious phone number and giving away their personal information. The emails arrive from a legitimate Paypal email address, often claiming that the recipient's PayPal account was used for a fraudulent transaction. The goal of the email is to get the recipient to call the phone number provided in the email.

If you have doubts about a message, contact the organisation directly. **Don't** use the numbers or address in the message – use the details from their official website. Your bank (or any other official source) will never ask you to supply personal information via email.

Spotted a suspicious email? Forward it to the Suspicious Email Reporting Service (SERS) - report@phishing.gov.uk



ActionFraud Cyber

Preventing fraud

TO STOP FRAUD

Together, let's stop scammers.



Remember, ABC:

🕛 <u>never</u> Assume

<u>never</u> Believe

🕛 <u>always</u> Confirm

Get the latest scam advice: @KentPoliceECU



Contacting 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 deaf or speech impaired, text **`police**' and your message to **60066**



BT Phishing Scam

Another phishing email to look out for, this time BT. Action Fraud have received numerous reports of these emails, which state your bill is ready to pay and requests you click on a link. This will take you to a genuine looking website, where not only will it steal your personal and financial information but also your BT log in details.

If you are unsure always contact the organisation directly using a trusted number but not one provided in their email.

You can visit the below BT website for further information.

How to report abuse and phishing | BT Help

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.

ActionFraud Cyber Aware

.....

BT SCAM EMAILS

Action Fraud has received 676 reports in two weeks relating to fake emails purporting to be from BT. The emails commonly use the subject line "Your bill is ready" and provide a link that can be used to make a payment. The links in the emails lead to genuine-looking phishing websites that are designed to steal BT login credentials, as well as personal and financial information.

If you have doubts about a message, contact the organisation directly. **Don't** use the numbers or address in the message – use the details from their official website. Your bank (or any other official source) will never ask you to supply personal information via email.

Spotted a suspicious email? Forward it to the Suspicious Email Reporting Service (SERS) - **report@phishing.gov.uk**



Preventing fraud

Together, let's stop scammers.







Contacting 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 deaf or speech impaired, text **`police**' and your message to **60066**



Disney+ streaming service phishing Email

Lookout for phishing emails offering a "98% discount" on subscriptions to the Disney+ streaming service, it's a scam. You will be asked to click on a link that is designed to steal your personal and financial data.

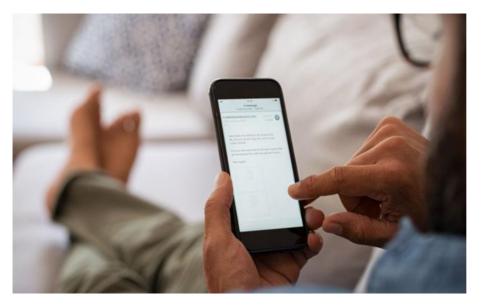
98% discount!! Remember if it sounds too good to be true then it probably is.

For further details visit the following by Which,

Beware of this fake Disney+ phishing email - Which? News

Forward this or any other suspicious email 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.



TO STOP FRAUD

Preventing fraud

Together, let's stop scammers.



Remember, ABC:

🛄 <u>never</u> Assume

never Believe

🕛 <u>always</u> **C**onfirm

Get the latest scam advice: @KentPoliceECU

Kent Police

Contacting 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 deaf or speech impaired, text **`police**' and your message to **60066**



TO STOP FRAUD"

Puppy/Kitten Scams

We have had several reports recently in Kent of people buying puppies and kittens online, only to find out that it is a scam.

Are you thinking about getting a new puppy or kitten? If so, do you know the signs of this scam? If not, visit the below Action Fraud website with information on how to protect yourself,

Paws for thought when buying a pet online | Action Fraud

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:

🕛 <u>never</u> Assume

never Believe

🕛 <u>always</u> **C**onfirm

Get the latest scam advice:



Contacting 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 deaf or speech impaired, text **`police**' and your message to **60066**

