



Protecting yourself from cybercrime and fraud

AIMEE PAYNE

CYBER PROTECT & PREVENT OFFICER

KENT POLICE – SERIOUS CRIME
DIRECTORATE



**Kent
Police**

Crime has gone digital

KENT

FRAUD PROFILE



20,318

TOTAL CRIMES REPORTED
APR 2018 TO MAR 2019



+11.4%

£41.6M

TOTAL VICTIM LOSSES
APR 2018 TO MAR 2019



+44.2%



62%

OF REPORTS WERE
FROM BUSINESSES



38%

OF REPORTS WERE
FROM INDIVIDUALS



| CYBER DEPENDENT |

Kent

CYBER PROFILE



758

REPORTED CRIMES
APR 2018 TO MAR
2019



£374K

LOST BY VICTIMS
APR 2018 TO MAR
2019

328

HACKING (SOCIAL MEDIA AND EMAIL) -
TOP CYBER DEPENDENT CRIME BY
VOLUME

APR 2018 TO MAR
2019



£113K

LOST BY VICTIMS OF HACKING
(SERVER) - TOP CYBER CRIME BY LOSS

APR 2018 TO MAR
2019

REPORTED VOLUMES & LOSSES



11%

OF REPORTS WERE
FROM BUSINESSES



89%

OF REPORTS WERE
FROM INDIVIDUALS

Two types of cybercrime

Cyber-dependent

Crimes that can only be committed by using a computer to attack another computer

Eg: Hacking, Spread of Viruses, Ransomware, DDOS

Cyber-enabled

'Traditional' crimes which are increased in their scale by the use of computers

Eg: Fraud, identity theft, harassment, romance scams

The attraction

Traditional Crime

- ▶ Offender required to be present at crime scene
- ▶ One offence at a time
- ▶ Evidence/ Forensics/ CCTV
- ▶ Witnesses
- ▶ HIGH RISK/ LOW REWARD

Cybercrime

- ▶ Not present at the scene
- ▶ Multiple offences at the same time
- ▶ Commit offences from anywhere in the world
- ▶ Co-operation required between law enforcement internationally
- ▶ LOW RISK/ HIGH REWARD

Key Message

80% of all Cyber Crime is easily preventable by adopting basic measures and being aware.

Remember A, B, C

A – Accept nothing

B – Believe no one!

C – CONFIRM EVERYTHING!

Are you aware of exactly how much you are sharing?

<https://www.youtube.com/watch?v=yrjT8m0hcKU>

Social Engineering



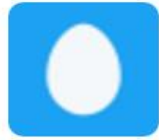
CONVICT QUOTES

Facebook lets you find things like a person's first school, birthday, their pet's name, and answers to all the other usual security questions. A lot of the info I need to guess your password is right there on your profile page.

Convicted Criminal

This quote was obtained by detectives in the National Fraud Intelligence Bureau.

What could someone do with this information?



John Smith
@johnsm1th123

Hey [@BudgetAirlineUK](#) - your gate at Manchester Airport should have opened 15 minutes ago. Whats happening? [#NotGoodEnough](#)

5

RETWEETS

9

FAVORITES



1:50 PM - 19 Oct 2016 - via Twitter · Embed this Tweet

↩ Reply 🗑 Delete ★ Favorite

Subject: RE: Your Delay at the Gate
From: info@BudgetAirlineUK.com
To: john.smith123@email.com

Dear Mr Smith,

We are sorry to hear that you were delayed at the airport when checking in at Manchester Airport on the 19th of October, for your flight number BUDNY1910 to New York. We hope it didn't spoil your trip!

As an apology Budget Airline UK would like to offer you a discount of 50% of your next flight, as well as complementary First Class upgrade.

All you need to do is fill in the form by clicking the link below, and we will send out the voucher codes to you.

<http://complaints.budgetairlineuk.com/voucher/50percent.html>

We hope to see you again soon

King regards

Dave Cameroon
Senior Complaints Handler
Budget Airline UK

Social Media



- ▶ Never disclose private information when social networking
- ▶ Be wary about who you accept invitations from
- ▶ Consider what you are saying online
- ▶ Look for the verification tick

How secure is your Social Media?

- We strongly advise that you opt for “Friends only”.
- Be a good friend and change your settings to ‘hide’ your friends list to protect their security too. Also helps prevent account cloning issues – do the same for contact details!
- Be mindful that “friends” settings can affect your own security
- It is advised you turn app location settings off when you post to social media as it indicates your current location AND where you are NOT!
- Remember regularly checking in to places, regardless of your settings ‘checking in’ is publically viewable
- Change your settings so that you control what others post about you!



Take a few minutes to review your digital footprint.....

Quite simply, Google yourself!

Limit the amount of information made **PUBLICLY** available

Check www.ukphonebook.com and www.192.com

PHONE NUMBERS

ADDRESSES/POSTCODES

FIND A PERSON

COMPANY SEARCH

DIRECTOR SEARCH

TPS/CTPS

TELEAPPENDING

ZONESEARCH

MAPS

CREDIT REPORTS

AREA CODES

LAND REGISTRY

Saved results

No saved results.

Person Search - Find a Person

Find a person by searching the edited UK electoral register, the phone book, and consumer data.

Find this person:

aimee payne

Search

☒ Exact matches only

Refine search further:

Location:

City, town, village or postcode

Street:

Street or road

Premises:

House name or number

Gender(s):

Any



Age Range:

Min age

Min.

Max age

Max.

DOB:

DD

MM

YYYY

Specify second resident:

Full name of second resident

Search

How to delete this information ?

- ▶ Firstly remove yourself from the Public Electoral Roll - You are automatically enrolled upon voting, meaning anyone can request your information, this can make you a target so contact your local council.
- ▶ By going through public databases like the Electoral Roll, websites such as 192.com are able to collate your address, home phone number & more details all in one place. For a small fee, anyone can then discover a large amount of information about you that you may have considered relatively private.
- ▶ So, if you'd rather people didn't know how much you paid for your current property or other personal details, read on to find out what 192.com knows about you & how to delete your information from the internet.

Passwords

- ▶ Think of your password as your front door
- ▶ Think passphrase! Choose three random unrelated words

VioletMouseCuppa

Vi0letMou\$eCupp@

- Use a different password for each website
- Use a password manager

<https://www.youtube.com/watch?v=yzGzB-yYKcc>

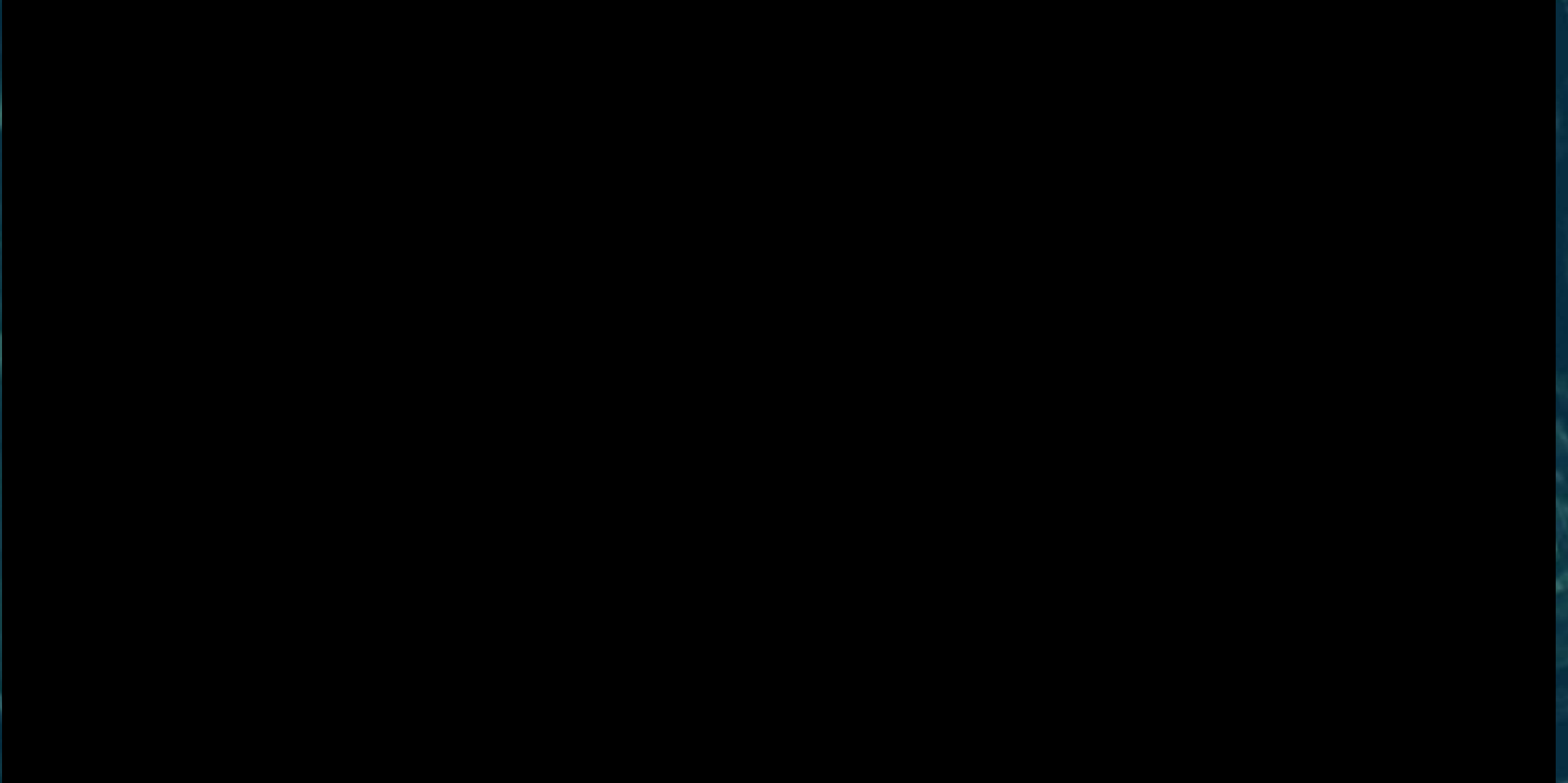
Passwords

<https://www.youtube.com/watch?v=opRMrEfAlil>

Do you use Public WIFI ?



Using public Wifi



Top Tips

- ▶ Don't use public WIFI for sensitive transactions
- ▶ Use 3G 4G - this is always encrypted
- ▶ Use a Virtual Private Network (VPN)
- ▶ Turn off WIFI when your not using it

Phishing Email



Dear Customer,

Nationwide's Internet Banking, is here by announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service, against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below.

<http://www.nationwide.co.uk/update.asp?ID=3b89db2a6001ec93328d21e59a011b0a25a>

Regards

Rafiq Miah

Customer Advisor

Nationwide Direct

Nationwide Building Society

<http://www.drinkrezepte.de/shakes/index.html>

From: Amazon <management@mazoncanada.ca> on behalf of not an Amazon email address
(note the missing A in Amazon)
To: @sheridanc.on.ca
Cc:
Subject: Suspension

amazon.com®

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html>

Sincerely,

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

The Amazon Associates Team

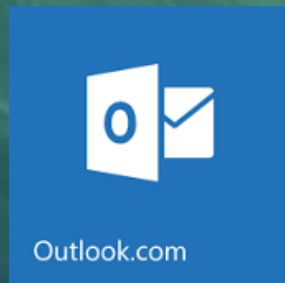


Email addresses can be spoofed to appear from the company, hover over links to check.

Email Top Tips

- ▶ Ensure your spam filter is on
- ▶ Do not open an email you suspect could be spam and send straight to your spam or junk folder
- ▶ Don't open attachments or click links from unknown sources
- ▶ If it's too good to be true- it probably is!
- ▶ Consider having two separate email accounts (public & private)

Two/ Multi Factor Authentication



- Add a second layer of security to your accounts
- Receive a text/ phonecall if a new device is used to access your account
- Temporary password issued
- Gives you the opportunity to confirm if the user is you

'--have i been pwned?

Check if you have an account that has been compromised in a data breach

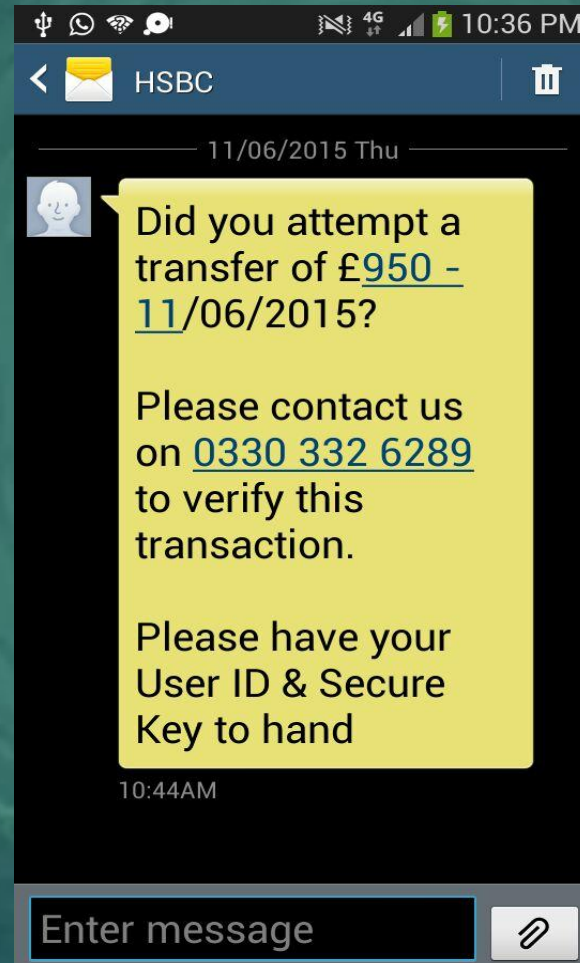
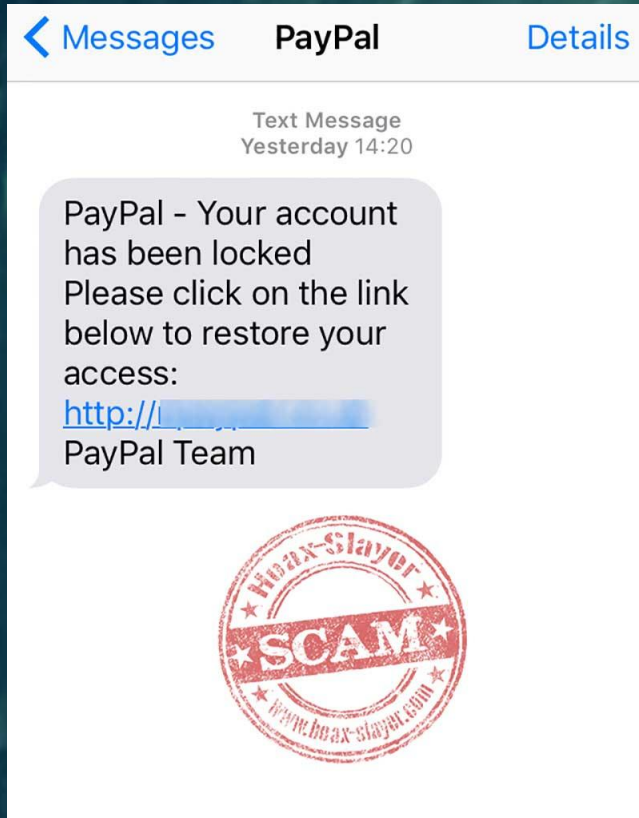
www.haveibeenpwned.com

A website that allows you to check if your personal data has been compromised by data breaches.

"Notify me" service allows visitors to subscribe to notifications about future breaches. Once signed up, you will receive an email message any time their personal information is found in a new data breach.

This service often alerts users to breaches long before it reaches the news, meaning that you can take action immediately instead of your accounts being at risk for months without you knowing.

And it's not just emails.....



Ransomware



- Don't pay ransom, there's no guarantee you will get your files back.
- Contact Action Fraud or the Police
- Back-up your files regularly so that if you are hit with ransomware your special documents are safe.

Ransomware is a form of malware that gives criminals the ability to lock a computer from a remote location - then displays a pop-up window informing the owner that it will not be unlocked until a sum of money is paid.

Sextortion

<https://www.bbc.co.uk/news/av/stories-46323625/what-happened-when-sex-tortion-scammers-targeted-a-bbc-trending-reporter>

Computer Security

- ▶ Install Anti-Virus on all devices
- ▶ Update your software as soon as your computer prompts you
- ▶ Back up your data to an external device and remove that device from your computer
- ▶ Check Op Systems are supported and running the latest version (Windows 7 end of life is January 2020)



Gifting, part exchanging, selling or disposing of devices?

- ▶ Ensure any cloud services are disconnected from the device!
- ▶ Make sure you have backed up your data and contacts!
- ▶ Perform a **FACTORY RESET** of the device
- ▶ **REMOVE** and removable media ie SIM card/memory card
- ▶ If you are disposing of the computers, laptops or tablets, destroy hard drives

Computer Software Service Fraud

| How to protect yourself |



Never reveal your personal or financial details as a result of a cold call.

Never install any software or visit a website as a result of a cold call.

Need professional tech support? Ask your friends or family for recommendations and look online for reviews first. Don't contact companies promoting tech support services via browser pop-ups.

Top Tips

- ▶ **NEVER** allow a cold caller remote access to your device
- ▶ **NEVER** reveal your personal or financial details
- ▶ **NEVER** install any software or visit a website as a result of a cold call
- ▶ A legitimate company wouldn't cold call you, if your unsure hang up and call them back from a different phone and the number you have for them.
- ▶ Consider investing in a call blocking system (Truecall, Call Guardian or speak to your service provider)

Romance Fraud #Fauxmance

Action Fraud reveal 50 million was
lost to romance fraud in 2018



Top Tips

- ▶ **D**on't rush into an online relationship – get to know the person, not the profile and ask plenty of questions.
- ▶ **A**nalyse their profile and check the person is genuine by putting their name, profile pictures or any repeatedly used phrases and the term 'dating scam' into your search engine.
- ▶ **T**alk to your friends and family about your dating choices. Be wary of anyone who tells you not to tell others about them.
- ▶ **E**vade scammers by never sending money to, or sharing your bank details with, someone you've met online, no matter what reason they give or how long you've been speaking to them.
- ▶ **S**tay on the dating site messenger service until you're confident the person is who they say they are. If you do decide to meet in person, make sure the first meeting is in a public place and let someone else know where you're going to be.

Courier Fraud



Top Tips

- ▶ Never divulge passwords or PIN codes to people over the phone – you cannot be sure who you are speaking to
- ▶ Police, HMRC or Banks will NEVER send a courier/unmarked unit to collect bank cards/PINs for investigation!
- ▶ There is no such thing as a “Safe Account”. Banks nor Police will ever ask for funds to be transferred to one
- ▶ Police will never ask you to be involved in ‘undercover’ operations

Online shopping

- Look for the padlock – this also provides an additional layer of encryption to the security of the page.
- When you have finished with the – log off properly.
- Using credit cards online actually provides you with more assurances that your bank cards do if something goes wrong. That isn't to say that banks will not help in hour of need.
- Keeping receipts/proof of purchase will help towards any issues.

Take 5

- *Never disclose security details, such as your PIN or full password – it's never right to reveal these details*
- *Don't assume an email request or caller is genuine – people aren't always who they say they are*
- *Don't be rushed – a bank or genuine organisation won't mind waiting to give you time to stop and think*
- *Listen to your instincts – if something feels wrong then it is usually right to pause and question it*
- *Stay in control – have the confidence to refuse unusual requests for information*



TO STOP FRAUD™

Don't let a scammer enjoy your retirement



Follow our four steps on
how to protect your pension

Be ScamSmart with your pension.



Pension Scams

- **Step 1 – Reject unexpected offers – *If you get a cold call about your pension, hang up! Report to Information commissioner's office (ICO)***
- **Step 2 – Check who you're dealing with? *Check the Financial Services Register, Need help checking call 0800 111 6768 – Consumer Helpline***
- **Step 3 – Don't be rushed or pressured**
- **Step 4 – Get impartial information or advice - *The Pensions Advisory Service, provides free independent advice***

Action Fraud customer channels



Social Media

Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.



0300 123 2040

Report fraud and cyber crime.
Help, support and advice.



24/7 Live cyber

Specialist line for business, charities or organisations
suffering live cyber attacks

Report 24/7 & Web Chat

www.actionfraud.police.uk

Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

National Fraud and Cyber Crime
Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance

Further information and advice

General advice on Cyber Security and Passwords:
Cyber Aware www.cyberaware.gov.uk

Online safety on all areas for everyone:
GetSafeOnline www.getsafeonline.org

CEOP online safety for under 18s, parents and schools:
ThinkUknow www.thinkuknow.co.uk

Advice on spam emails, spam phonecalls and scams
Take 5 to Stop Fraud <https://takefive-topfraud.org.uk/>



Follow us @kentpolicecyber

Support and advice for victims

[Welcome](#)[What We Do](#)[Who We Are](#)[Get Involved](#)[Contact Us](#)[Donate now](#)

Our helpline



Our specially-trained

- Offer information
- Link callers to
- Offer regular f
- Protect and su

You can call us at anytime and from anywhere in the UK

There is no questions too big, no problem too small and no need to be alone.

VS VICTIM SUPPORT

phone line
e year



**Become a Friends against scams
Scamchampion ?**

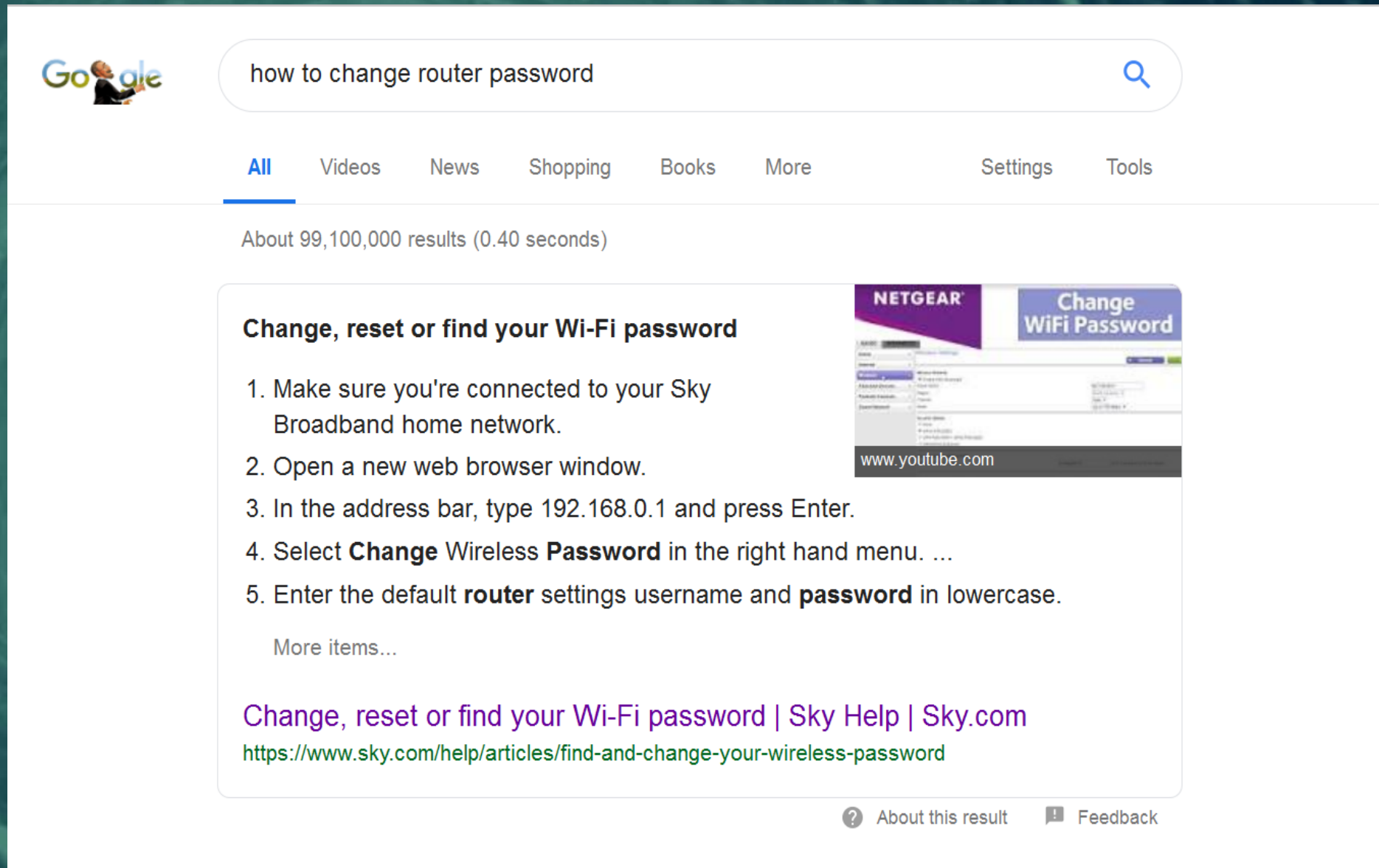


Checklist:

- ▶ Check Op Systems are supported and running the latest version
- ▶ Check Firewalls, Antivirus, Antimalware and Antispyware installed and running
- ▶ Check your passwords are secure enough and not used across platforms
- ▶ Check your digital footprint
- ▶ Check UK Phonebook & 192.com for entries in your name – request removal
- ▶ Check your social media settings
- ▶ Check your email address with www.haveibeenpwned.com and set up Two/multi Factor Authentication (2FA)
- ▶ Ensure your home router has a password set, if the original default, change it
- ▶ Don't use public WiFi for sensitive transactions such as banking/social media/email unless you've set up a VPN, or revert to 3G/4G on your device
- ▶ ***Share this information with family, friends, and the public!***

How to change your router password ?

► Example....



The screenshot shows a Google search interface. The search bar contains the text "how to change router password". Below the search bar, the "All" tab is selected. The search results show "About 99,100,000 results (0.40 seconds)". The first result is titled "Change, reset or find your Wi-Fi password" and includes a list of five steps. To the right of the steps is a thumbnail image of a Netgear router's web interface with the text "Change WiFi Password". Below the steps is a link to "Change, reset or find your Wi-Fi password | Sky Help | Sky.com" with the URL "https://www.sky.com/help/articles/find-and-change-your-wireless-password". At the bottom right, there are links for "About this result" and "Feedback".

Google

how to change router password

All Videos News Shopping Books More Settings Tools

About 99,100,000 results (0.40 seconds)

Change, reset or find your Wi-Fi password

1. Make sure you're connected to your Sky Broadband home network.
2. Open a new web browser window.
3. In the address bar, type 192.168.0.1 and press Enter.
4. Select **Change** Wireless **Password** in the right hand menu. ...
5. Enter the default **router** settings username and **password** in lowercase.

More items...

[Change, reset or find your Wi-Fi password | Sky Help | Sky.com](https://www.sky.com/help/articles/find-and-change-your-wireless-password)
<https://www.sky.com/help/articles/find-and-change-your-wireless-password>

NETGEAR Change WiFi Password

www.youtube.com

? About this result Feedback

Questions ?

Aimee Payne
Cyber Protect & Prevent Officer
Serious Economic Crime Unit
Kent & Essex Serious Crime Directorate
aimee.payne@kent.pnn.police.uk
Twitter - @kentpolicecyber

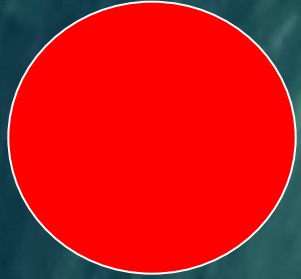
Cyber PREVENT;

#CyberChoices

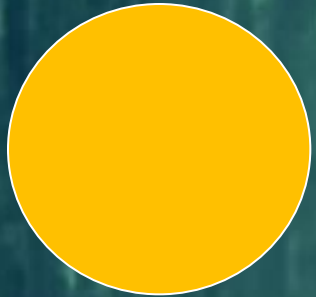
*Preventing individuals from becoming
involved in cyber dependent crime*

<https://www.youtube.com/watch?v=PJ0KddbbxrE>

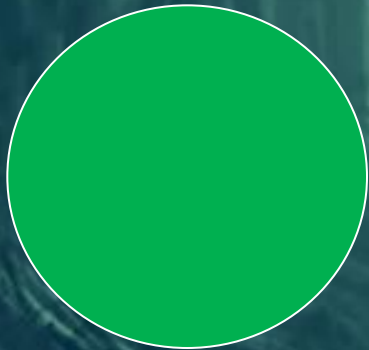
Cyber Prevent Aims



To deter individuals from getting involved in cyber dependent crime.



To prevent re-offending



To promote legal and ethical use of skills, including opportunities in cybersecurity

Pathways

Understanding the pathways for cybercriminals vs those in the cybersecurity professions



Legislation;

The Computer Misuse Act 1990

- ▶ **Section 1 > Unauthorised access to computer material** - *Example - Without them knowing, you watched your friend put their password into their phone. You then used it to gain access to their phone & download their photos.*
- ▶ **Section 2 > Unauthorised access with intent to commit or facilitate commission of further offences** – *Example – Without their permission, you accessed your friend's smartphone, obtaining their bank details, so you could transfer money from their account and download their photos.*
- ▶ **Section 3 > Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer** – *Example – You used a booter tool to knock a friend offline from an online game.*

Legislation;

The Computer Misuse Act 1990

- ▶ **Section 3ZA > Unauthorised acts causing, or creating risk of, serious damage** – *Example – You hacked into the computer system of a Government Agency and were reckless as to the consequences. National security was undermined.*
- ▶ **Section 3A > Making, supplying or obtaining articles for use in another CMA offence** – *Example – You download a product to deploy malware to a friends computer, so you could control it. You didn't even get a chance to use it.*

Consequences

- ▶ A visit and warning from the Police – Cease & Desist
- ▶ Being Arrested
- ▶ Having your computer(s) seized and internet access restricted
- ▶ Paying a penalty or fine
- ▶ A significant prison sentence
- ▶ A permanent criminal record could affect education and career prospects, as well as overseas travel

Consequences

- ▶ **Maximum sentence that can be handed down for a CMA offence? LIFE**
- ▶ Section 1 up to 6 months and / or a fine
- ▶ Section 2 up to 5 years and / or a fine
- ▶ Section 3 up to 2 years and / or a fine
- ▶ Section 3A up to 2 years and / or a fine
- ▶ Section 3Za up to 14 years and /or a fine...

<https://www.youtube.com/watch?v=9Z3W3J9MC-M>

Positive Diversion Programmes

***cyber
discovery***

Could you have a hidden
talent for cyber security?

Cyber Discovery, HM Government's Cyber Schools Programme, is an extracurricular learning programme for students in years 10-13 across England. Its goal is to ensure that many more people enter the cyber security profession in the coming years.

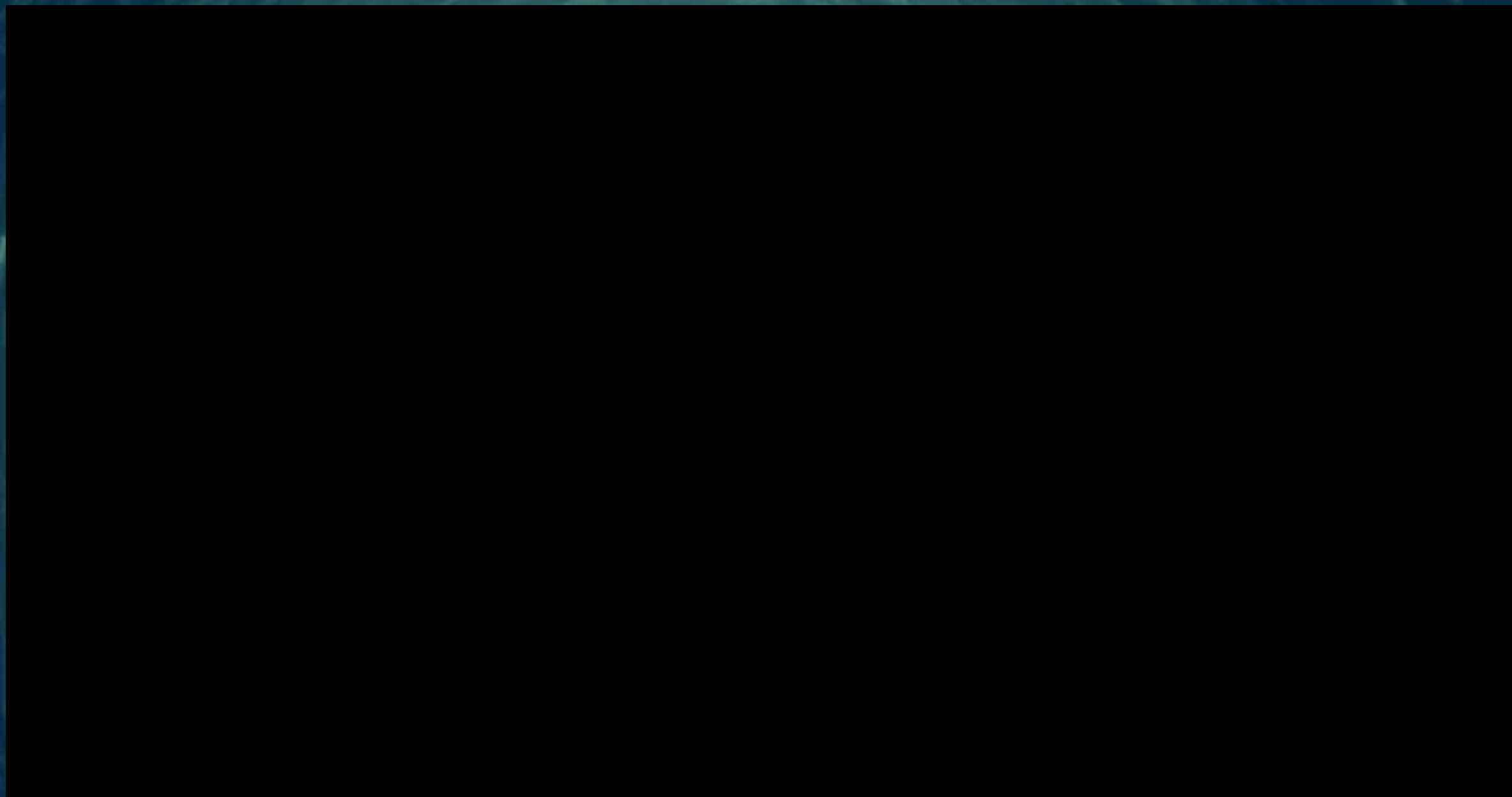
[Sign up now](#)

[Already have an account? Sign in >](#)

Positive Diversion Programmes



Cyber
Security
Challenge UK





Bug Bounties

Apple pays teenager for discovery of Group FaceTime bug with bug bounty, scholarship



<https://www.bbc.co.uk/news/av/technology-47407609/how-one-teenager-is-making-millions-by-hacking-legally>

Code Clubs

- ▶ **Kent County Council run Digital Den for children aged 8 – 11 at the following locations;**
- ▶ Ashford Library
- ▶ Gravesend Library
- ▶ Newington Library (Thanet)
- ▶ Sheerness Library
- ▶ Swanley Library
- ▶ **Additionally they run Coderdojo's for children aged 7-17 at the following locations;**
- ▶ Canterbury Library
- ▶ Gravesend Library
- ▶ Sevenoaks Library

For additional Information;



<http://www.nationalcrimeagency.gov.uk>

Questions ?

Aimee Payne
Cyber Protect & Prevent Officer
Serious Economic Crime Unit
Kent & Essex Serious Crime Directorate
aimee.payne@kent.pnn.police.uk
Twitter - @kentpolicecyber