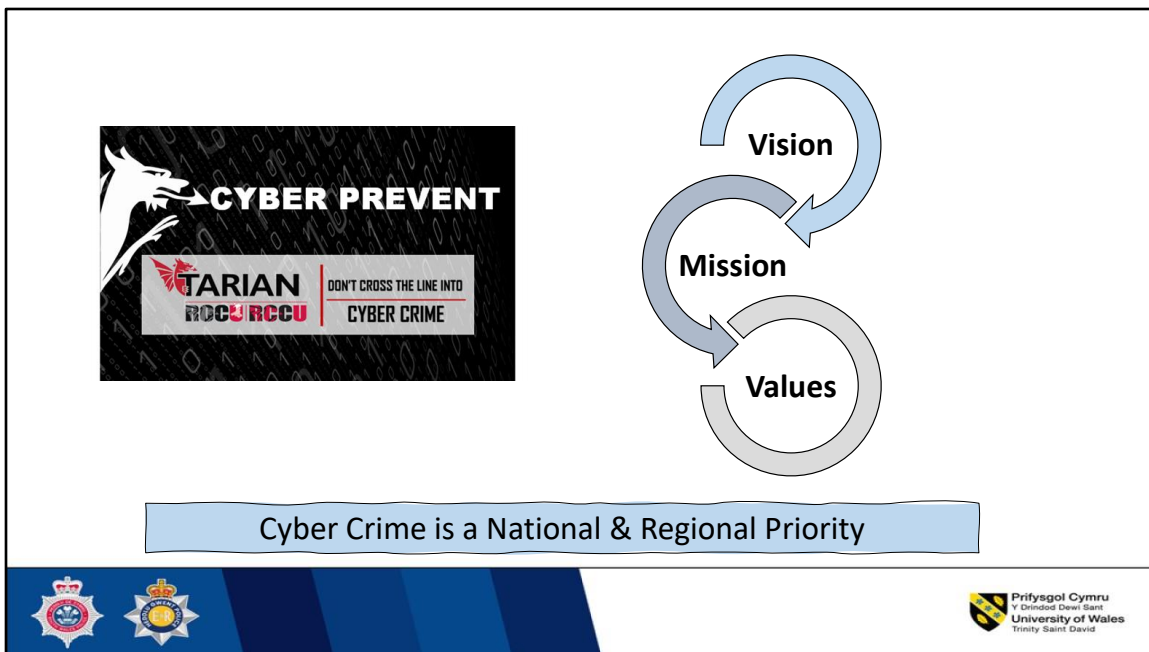




On successful completion of this module, learners will be able to:

1. Explain the differences between common terms used within the digital world.
2. Identify different devices that could be used in criminality and what types of evidence devices may hold.
3. Identify the different types of crimes that can be committed through use of the internet.
4. Identify offences that constitute a digital crime.
5. Identify ways in which an initial responder can secure and preserve evidence in a Cybercrime investigation.



TARIAN - the Regional Organised Crime Unit, part funded by the Home Office, Welsh Government and the three Southern Wales Police Forces is a multi-disciplinary team of Police officers and Police staff seconded from the three forces of Dyfed-Powys, Gwent and South Wales. With departments ranging from fraud and cyber-crime investigators to asset recovery experts and intelligence specialists, the teams are dedicated to disrupting and dismantling Organised Crime Groups across the whole of Southern Wales.

Our Vision

Our vision is to protect the communities of the Southern Wales Region from the threats and risks of Serious and Organised Crime.

Our Mission

Our mission is to identify, disrupt and dismantle organised crime groups causing most harm to the Southern Wales Region.

Our Values

We are Professional in tackling Serious and Organised Crime

We are Committed to collaboration and working with partners and other law enforcement agencies.

Tarian Teams include:

Asset Confiscation Enforcement (ACE) Team

Child Sex Exploitation

Regional Task Force

Regional Asset Recovery Team

Regional Intelligence Unit

Protected Persons Unit

Regional Prison Intelligence Unit

Regional Fraud Team

Regional Cyber Crime Unit

E-Forensics

Regional Undercover Unit

Government Agency Intelligence Network

Regional Technical Support Unit

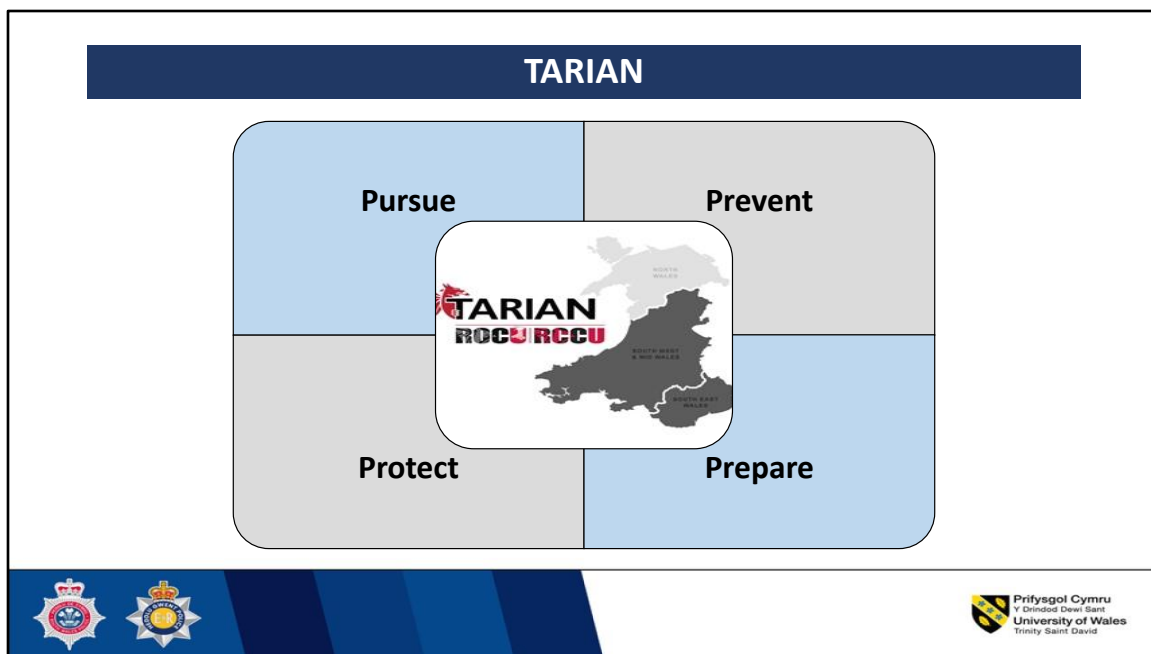
Confidential Unit

Operational Security Officer

Modern Slavery

Communications Data Account Manager

Disruption Team



The **Regional Cyber Crime Unit** within Tarian has a remit that covers the main principles of the CONTEST Strategy:

Pursue - Prosecuting and disrupting those engaged in Cybercrime

The RCCU tackles those responsible for the most serious incidents of: • Computer and network intrusion • Distribution of malware • Denial of service attacks • Phishing

Prevent - Prevent people from becoming involved in or providing support for Cybercrime

Using a variety of tactics to identify and divert possible Cyber offenders, e.g. conducting cease and desist visits to those identified from International Intelligence as purchasers of known Malware variants.

The Prevent capability has recently expanded to improve the capacity for pro-active engagements.

Protect - Strengthen the protection of individuals, communities and organisations against Cybercrime

The Unit are working collaboratively with Welsh Government with the aim of developing a 'secure digital nation'.

Current information available suggests that 80% of Cybercrime is preventable and it

is our intention through partnership engagement and education to develop Wales as a safe place to live, visit and do business.

Our Regional Cyber Protect Officer reached out to over 700 small, medium enterprise businesses in 2016 raising awareness of Cybercrime and advising how to protect themselves.

The Protect capability has expanded to improve the capacity for pro-active engagements

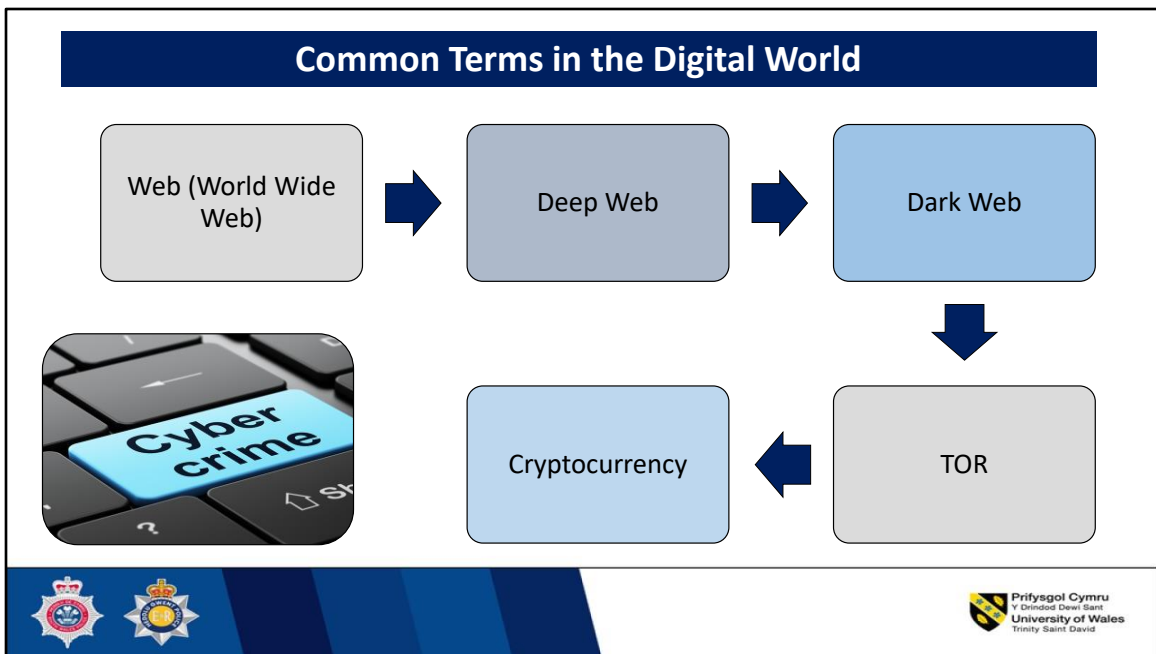
Prepare - Prepare our staff to understand and effectively deal with Cybercrime
Major contributor to the All Wales Cyber Operational Framework, seeking to develop and pool the expertise across Law Enforcement in Wales.
Developing and coordinating bespoke training for delivery at local and Regional level.

The Unit, working closely with the National Cyber Crime Unit (NCCU), National Cyber Security Centre (NCSC), Europol (EC3), other Regions, Forces, International Partners such as the FBI and USSS provide a national investigative response to the most serious incidents of cyber-crime.

Other For further advice and guidance please follow visit the below websites:

<https://www.getsafeonline.org/>

<https://www.cyberaware.gov.uk>



Activity 1 – Trainer to split the class into 5 groups and allocate each group one of the following heading – Web, deep web, dark web, TOR (Onion Router) and cryptocurrency.

Students to present their findings to the class.

Common terms you may hear in the digital world...

1. **Web – or World Wide Web** is the web we all use and is the part of the Internet that is indexed and can be searched.

Google, Bing, Duck Duck Go, Available to all and indexed to allow quick access to all users

Deep Web

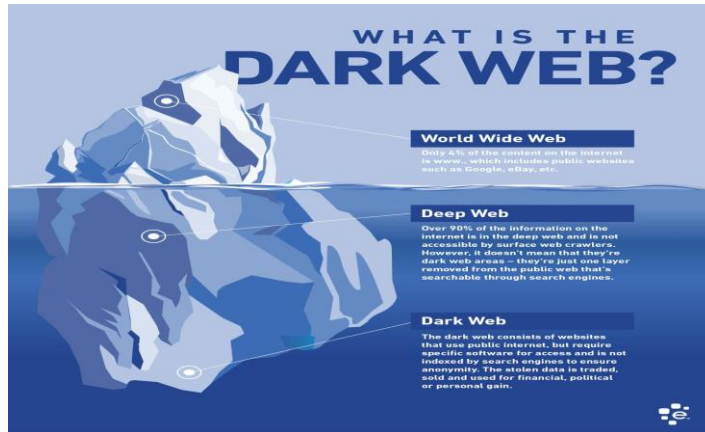


Common terms you may hear in the digital world...

2. The **Deep Web** is simply the content of databases and other web services that for one reason or another cannot be indexed by conventional search engines. We might have found Titanic, but there is a lot to discover in the bottomless oceans. Similar is the case of the search engine crawlers, they haven't identified various parts of the World Wide Web, and we call it the Deep Web
- The Public Web – Only 4% of web content is available via search engines such as google
- The Deep Web – Approx. 96% of the digital universe is on the Deep Web

<https://www.youtube.com/watch?v= UOK7aRmUtw>

Dark Web



The **Dark Web** is the encrypted network that exists between **Tor** servers and their clients.

The dark web, sometimes referred to as Darknet, is accessed by Tor (The Onion Router) which uses masked IP addresses to maintain anonymity for users and site owners.

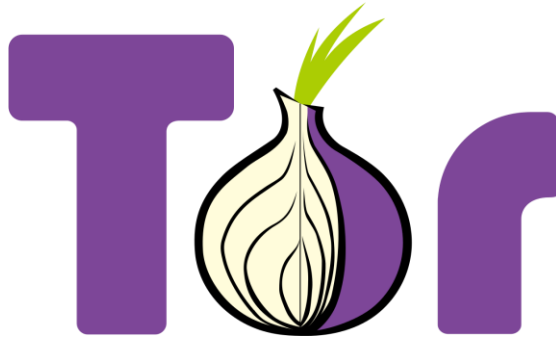
This way, people who use the **dark web** for illegal purposes can't be traced

The key thing to keep in mind is the **Dark Web** is a small portion of the **Deep Web**.

Silk Road was an online black market and the first modern darknet market, best known as a platform for selling illegal drugs. As part of the dark web, it was operated as a Tor hidden service, such that online users were able to browse it anonymously and securely without potential traffic monitoring



TOR



Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

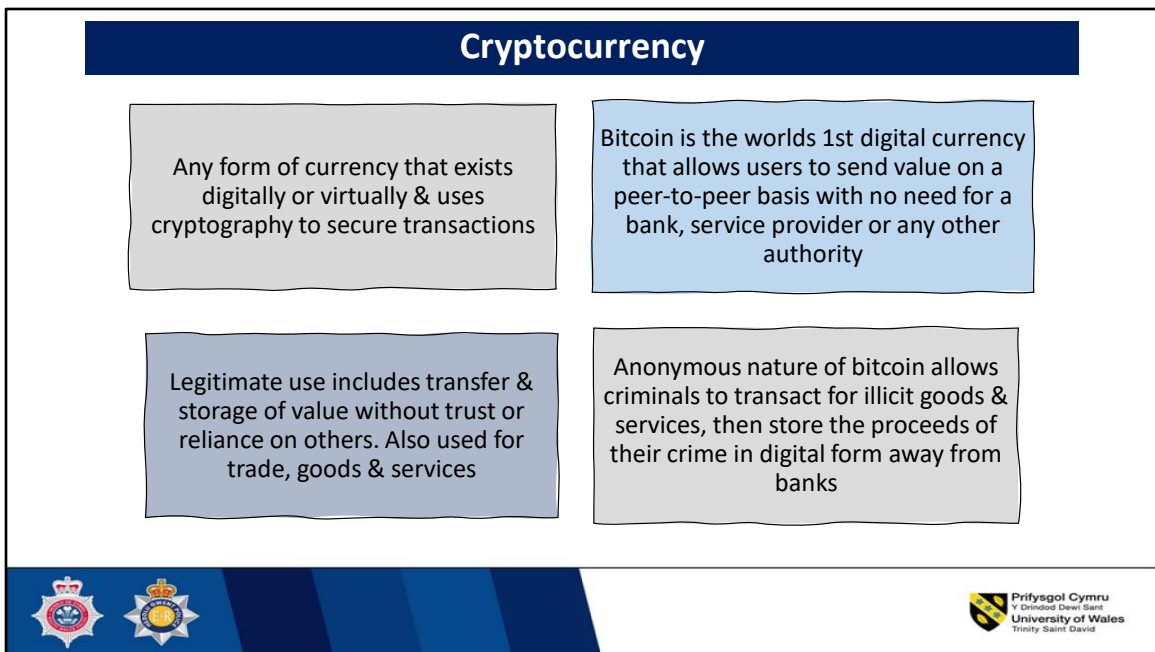
Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Why people use TOR?

- They protect their privacy from unscrupulous marketers and identity thieves.
- They protect their communications from irresponsible corporations.
- They protect their children online.
- They research sensitive topics.
- They skirt surveillance.
- They circumvent censorship.

Who uses TOR?

- Journalists
- Law enforcement
- Activists & Whistleblowers
- Business executives
- Bloggers
- Military
- IT Professionals



Cryptocurrency, sometimes called crypto-currency or crypto, is **any form of currency that exists digitally or virtually and uses cryptography to secure transactions**. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units.

What exactly is bitcoin and how do criminals take advantage of the technology?

- 1.Bitcoin is the world's first digital currency that allows users to send value on a peer-to-peer basis, with no need for a bank, service provider or any other authority to be involved. Transactions are verified and shared by members of the global bitcoin network.
- 2.Legitimate uses include the transfer and storage of value without trust or reliance on others, such as banks. Bitcoin is also used for trade, with payment services becoming increasingly common for services and goods – even those as mundane as clothing and beer. Value is sustained by the finite number of bitcoins 'mined' and by the need for a user's private key(s) to access them. Users simply need a device with a data connection, rendering access and use for up to two billion people who do not have access to banks.
- 3.Criminals take advantage of the seemingly anonymous nature of bitcoin. They can

transact for illicit goods and services, then store the proceeds of their crime in digital form away from bank accounts. They can then launder the proceeds by converting them to other cryptocurrencies or cash.

4. Law enforcement dedicate specialist officer resources into developing guidance and sharing best practice. Investigation guidance is provided by the NPCC and shared on the police Knowledge Hub. Collaborative working with industry and academia is key to providing an effective response.

5.If you want to buy bitcoin, there are plenty of resources online. You can get 'hands on' with the technology available by installing a wallet, creating an account with an exchange, and then purchasing and transferring a small amount.

Internet Usage

List the ways that we access the internet & what it is used for....



QTS – What do you use the internet for? Boardblast

Ask the class for ways that they access the internet and what it is used for:
Banking, shopping, Porn, Info, Facebook, Homework, Teams, Cloud Storage etc



QTS – How has social media changed over the years?

Pope's inauguration 2005 and 2013

QTS - 2018 – what devices would be new today?

- Wearables (eg, Fitbit, Apple watches etc)
- GPS, Satnav, Drones
- Vehicle data (telematics, infotainment etc)
- Internet of things (connected home)
- Games consoles (e-readers, other mobile devices)
- Routers, Wi-Fi, VPN and communications data
- Data storage including Cloud, removable drives, memory sticks and volatile data

Facilitate discussion on how social media / online presence has changed dramatically. Discuss ways in which social media can be used to assist investigation such as CCTV, digital devices, echo, google home acting as 'digital witnesses'.

The SMART Phone



QTS- How has the use of SMART phones changed over the years?

Convergence

Discussion here surrounding how SMART phones have changed how we should now look at this area of investigation.

A phone is no longer just a phone.

Upgrades etc...

Apps



QTS – What Apps do you use on your smart phone?

What do you use the Apps for?

What evidence can the Apps hold?

How is the information backed up?

Calendars, address books, health apps, gaming apps, CCTV linked to home, IOT Apps (NEST), Music apps (Soundcloud) Photos, Kindle, Mapping, Browsers, Find my friend, Evernote, Weather, Password Apps, Email, Phone list, Contacts, Sleep monitor, Banking, Shopping, Loyalty, Clubs, Hidden Apps

Board Blast



EL CHAPO "Fugitive drug lord", one of Southern America's most wanted was photographed by his son whilst out having a Pizza, shortly after taking the photo he shared it on TWITTER.

Unfortunately for El Chapo his son left his GPS location turned on whilst taking the photo, shortly after this photograph South Americas most wanted was not wanted any more as he was in custody!!!! 17 mins from posting until arrest.....

SWP & Gwent use of Twitter/FB etc – are the forces using it to their potential?

Mayhill Riots – Swansea 2021



Mayhill Riots May 20th May 2021 – Swansea

Trainer to click on arrow button which will take you to the BBC news website and from there can play the footage at the beginning of the article on the Mayhill Riots

Details below how the footage was used as evidence in helping to convict the perpetrators

Violence erupted in the Mayhill area in May 2021 during a vigil for a local teenager who had died.

Cars were burnt out and windows smashed in Mayhill on 20 May 2021 after a balloon release for local teenager Ethan Powell, 19, who collapsed and died the day before.

The area was described as a "warzone" after cars were torched, homes vandalised and residents and police attacked during two hours of disorder.

Messages were exchanged on social media between suspects about obtaining a number cars for the event in anticipation of them being used in an anti-social manner.

One vehicle was set alight and social media footage shows the car rolling down the hill,

CCTV and mobile phone footage included a video of a Ford Ka being set on fire.

Another video also showed a Vauxhall Astra doing wheel spins with a person on the bonnet trying to kick through the windscreen. Another video showed the car being pushed down the hill amidst cheers and screams.

A small number of officers in riot gear are also shown attempting to stop the riot as they are attacked and one officer can be heard desperately calling for back up.

Kieran Hurley, 24, was handed the longest sentence of 6 years and 9 months after his version of events was rejected at a [Newton Hearing](#), Judge Thomas said: "You filmed what was going on, you celebrated and exulted in what was happening."



Details inappropriate use of social media.

“LEAGUE OF SHADOWS”

This was a self named group of police officers who used social media to discuss police activity they were involved in – PSU officers in Cardiff commenting things like “can’t wait to go beating up the Jacks at the weekend”

Allow students to read and facilitate discussion on appropriate use of Personal Social Media – Link to **Code of Ethics**

The Social Media Revolution



Prior to showing the slide

QTS – what social media platforms can you name?

We are going to look at a couple of different Social Media Platforms and their effect on policing

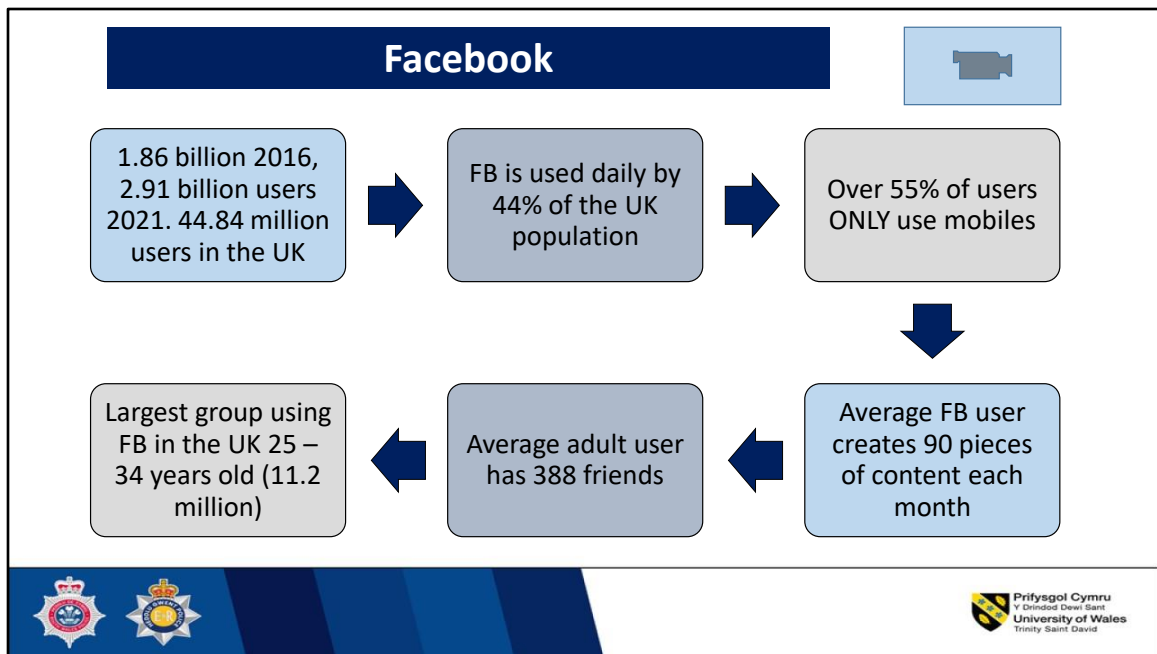
<https://www.youtube.com/watch?v=jottDMuLesU> (Click on YouTube icon)

Discussion points – video is from 2015.

QTS - How much has changed already?

QTS – what do you think officers need to be mindful of?





QTS – what social media platforms can you name?

‘Can I be your friend video?’ is imbedded in video Logo click to view –

<https://www.youtube.com/watch?v=aDycZH0CA4I>

Crime Prevention - Use of Social Media during investigations

Trainer to inform students of crime prevention advice, Social media is popular but people forgot about basic crime prevention advice. Don't divulge too much information via social media

Screenshots by victims for evidence gathering. Incidents can be on Social Media before Niche!

Discuss “normalization” and crime prevention – dangers of “over sharing” – giving out too much personal data

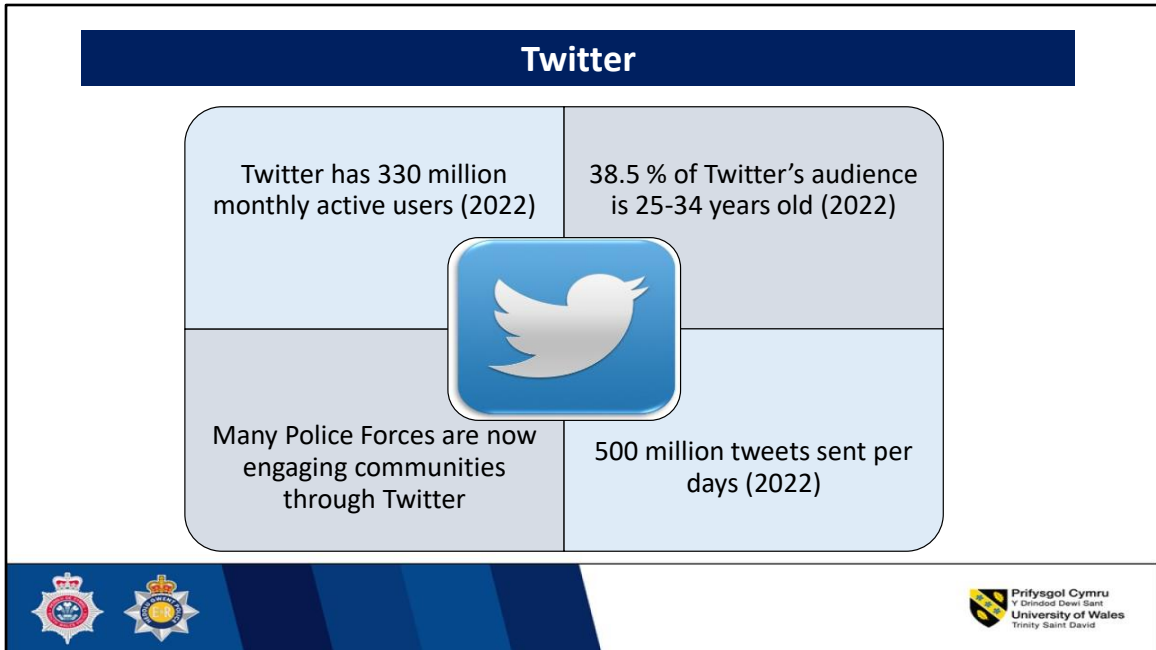
Discuss use in investigations – screenshots by victims used as evidence

Since 2012, the 18 to 24 market has declined in prominence, when it comprised 24 percent of all users. In contrast, older users are now much more prominent on the site, with over 65s only 4 percent of users in 2012, suggesting an ageing userbase.

Women are the most frequent users of Facebook in the UK with 52 percent of users, a trend that has been stable since 2012, likely reflecting the underlying demographics of the country. However, female users are slightly more common than male users, 27 percent being aged 25 to 34, compared to 25 percent for men. In contrast, older men are more common on the site than older women.

According to Ofcom's annual review of UK internet consumption,

around nine in ten internet users visit Facebook each month, spending an average of 23 minutes per day on the site. 74% percent of Facebook users check the site at least once a day. With more than a third (35 percent) of total time spent on the internet in the UK being on websites owned by either Google or Facebook. Despite this, trust amongst users regarding the protection of user data was low, at only 31 percent.

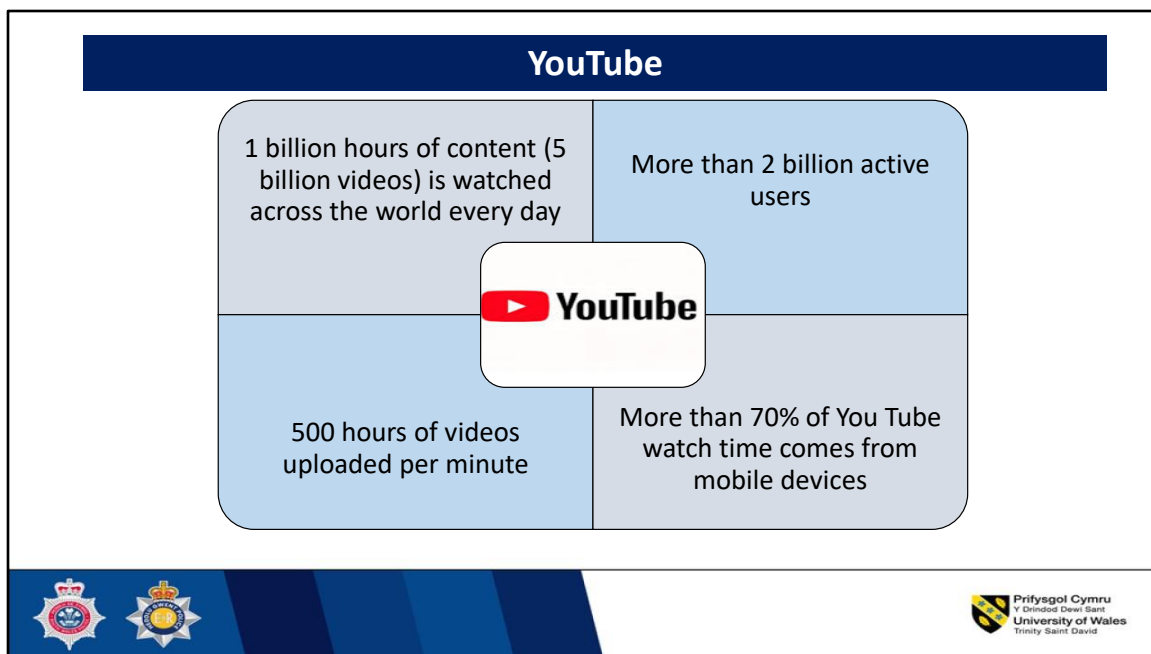


Prompt discussion around the use of Twitter by Police Forces

Pro's & Con's

What experience have officers had using it?

Are there any success stories as a result, or any nightmares?



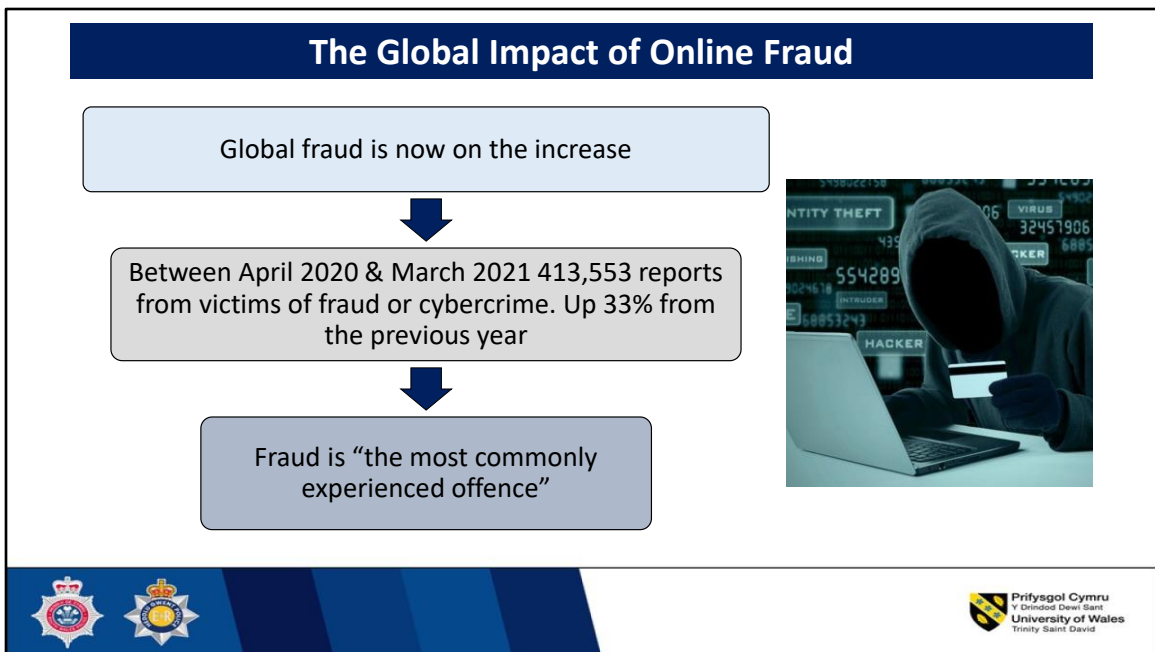
QTS – How much has changed already since 2015? (when the ‘Can I be your friend’ video was recorded)

QTS – What do you think officers need to be mindful of?

YouTube – Facts and figures – sheer volume – tie into investigating crime.

Discuss evidence (dashcam uploads etc)

Discuss officer awareness – mobile phones recording us in public – offences? Can we prevent it?



Facilitate discussion on reasons behind

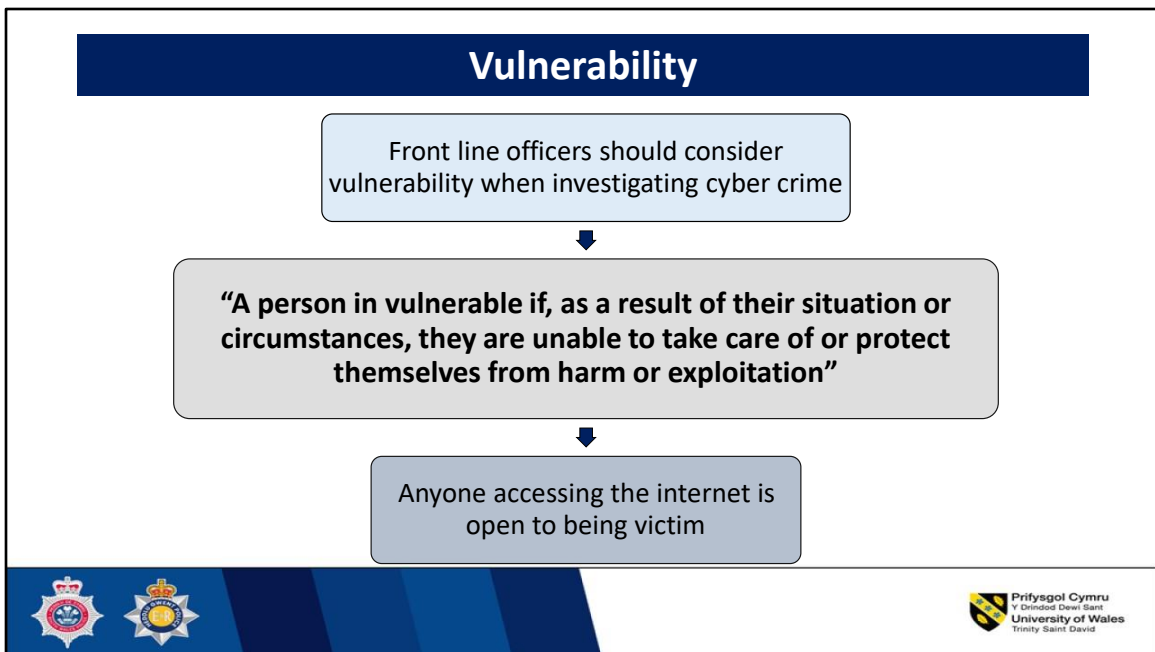
- increase (increased awareness, ease of reporting (Action Fraud – standardised national reporting)
- better recording (included in crime survey for first time in 35 years) as well as an increase in opportunity

Link to vulnerability – average age of victims is 63. Office of National Statistics (ONS) – Fraud and Cybercrime included in official stats for first time in 2017. (Crime survey started 35 years ago)

Estimated annual 3, 863.00 million cases of fraud offences against adults in England and Wales (Office of National statistics June 2019) and 1.8 million computer misuse offences for the 12 months ending June 2021.

Vulnerable victims of online fraud – average age between 45 and 54

Under reporting? Tinder/Grindr victims, other reasons for embarrassment



Anyone accessing the internet is open to being victim.

Show first paragraph and discuss what vulnerabilities may be relevant

QTS – When is a person vulnerable?

QTS – What does this mean for the police?

QTS – How can we help safeguard vulnerable victims?

QTS – What issues may we encounter with social media evidence?

"A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves from harm or exploitation"

Reveal 2nd Paragraph and reinforce

Trainer to show slide. Brief discussion on who "US" is – means victims and witnesses as well as police and partners (CPS, partner agencies etc)

Cybernews.com - Most vulnerable to cybercrime tend to be adults over 75 and younger adults. Particular vulnerability of young and old adults is largely due to the surge of

new customers going online during 2020. It's easy to assume that young adults are tech-savvy and therefore relatively immune from attacks, but they often have a false sense of their capabilities and therefore tend to be more relaxed, especially in terms of their willingness to share personal information. The older demographic, by contrast, are much less familiar with the latest technologies, and it's their lack of familiarity which raises their own susceptibility to the various scams and phishing attacks that criminals will target them with.

Saferinternet.org.uk - We are all vulnerable at certain times of our lives, depending on our circumstances and life events. When thinking of those more at risk than others, this could include a wide range of people e.g. those with physical disabilities or illnesses, care leavers, people with mental health difficulties, those with addictions, homeless people, abuse survivors, those in poverty, ex-offenders, ex-service personnel, minority groups, etc.

There may be a greater exposure to particular online risks for certain groups, e.g. a third of LGBT people experience [online hate crime](#); and for a number of reasons (including lack of staff awareness and lack of education), young people with learning disabilities are more susceptible than others to [online grooming and sexual exploitation](#).

Consider their vulnerability and clues they may provide to you - the person's wants and needs, abilities, experiences and influences. They may have particular vulnerabilities that are amplified online. Talk to them about what they enjoy most about the internet, ask them how, where and when they go online, as well as what they do and who they are talking to.

It's useful to consider who their peers are online. Do other people in their physical or online environment provide support or pose a risk to them (e.g. over-sharing, abuse or neglect)? Would they know how to recognise and respond to an issue? The same applies to you as a professional, it's important that you know how to respond to an online safety incident.

Support the person to keep themselves safe online. Technical settings (blocking, filtering, passwords etc.) may be appropriate. Discuss the kinds of online activities which would be illegal, inappropriate, or break an app's terms & conditions. Are they informed about their online rights? Where would they go for help if they needed it?

Victims & Suspects are Social Media Savvy

So what does that
mean for us?

We need to identify, secure &
retrieve evidence/intelligence
of social media use at the
earliest opportunity



QTS – What issues may we encounter with Social Media evidence?

WE – DOESN'T MEAN US IT MEANS THE WITNESSES & VICTIMS, Partner agencies etc... AS WELL.

Discuss issues with Social Media evidence – easily changed, deleted, overwritten – not always easy to search

Internet Facilitated Crimes



Hate Crime



Sexting/Revenge porn



Abuse, bullying & harassment



Online fraud



Child grooming



Radicalisation



Financial crime



Modern slavery & human trafficking



QTS- what types of crime are committed on the internet? Boardblast

Types of internet facilitated crimes:

- Hate Crime
- Sexting/Revenge porn
- Abuse, bullying & harassment
- Online Fraud
- Child grooming
- Radicalisation
- Financial Crime
- Modern slavery and human trafficking



CRIME has moved into the ONLINE world – so we have to!



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Office For National Statistics Year ending September 2021

Patterns of crime in the year ending September 2021 have been significantly affected by the coronavirus (COVID-19) pandemic and government restrictions on social contact. There was significant variation in the level of restrictions in place across this time period and, at times, further variation across regions. This creates a challenge in isolating the level of impact that restrictions may have had on patterns of crime.

The number of incidents decreased for many types of crime during periods of national lockdowns. However, police recorded crime data show indications that over the last six months, certain offence types are returning to or exceeding the levels seen before the pandemic.

Fraud and computer misuse offences do not follow the lockdown-related pattern of reduced victimisation, and increases in these offences more than offset the reductions seen for other types of crime.

Estimates from the TCSEW (The Crime Survey for England & Wales) for

the year ending September 2021 compared with the pre-coronavirus year ending September 2019² show:

- a 14% increase in total crime, driven by a 47% increase in fraud and computer misuse
- crime excluding fraud and computer misuse decreased by 14%, largely driven by an 18% decrease in theft offences

The TCSEW shows little change in total number of incidents of violence but a 27% decrease in the number of victims of violent crime. This is largely driven by falls in violence where the offender was a stranger³, where the number of victims has dropped by 50%, in part reflecting the closure of the night-time economy for several months of the year.

CRIME has moved into the ONLINE world – so we have to!

Evidence Gathering

As Investigators

We need to
consider the use
of digital
media/online
world



But we also need
to know what we
can and cannot
do



And what we do
with the
information we
gather



Device	Types of Potential Evidence
Digital/Video Camera	• Pictures • Videos • Files stored locally or on media card
Cell Phone	• Text Messages • Call Logs • Applications used • Social Media accounts • Everything from All Categories
Computer/Laptop	• Everything from All Categories • Social Media accounts • Internet Search History • Documents • Email (Non-web-based)
Mobile device	• Everything from All Categories • Applications used • Social Media accounts
Game consoles	• Pictures • Videos • Documents

QTS - What digital devices could be used by criminal?

QTS – What potential evidence could be taken from these devices? (Digital witnesses)

QTS – What technology do police use to assist them with their investigations?

These items may be identified during investigations and seized as evidence

Police use technology to support their day to day policing duties

Examples:

- Body worn cameras
- Smart phones
- Laptops
- Tablets
- ANPR
- Facial Recognition
- Mobile Fingerprints
- Cell site
- Vehicle telematics
- Tracking stolen devices
- Internet telephony - refers to all types of telephony services

(including phone calls, fax, voicemail, video calls and other forms of communication) where calls and data are sent digitally over the Internet using the Internet Protocol (IP), rather than being transmitted over traditional analogue landlines.

The Digital World is Constantly Changing so



We follow the NPCC Good Practice Guide for Computer-Based Electronic Evidence &/or local procedures



Due to the fact the Digital Landscape is ever changing, it is very difficult to allocate specific rules/practices to the use of social media during investigations.

This is recognised by NPCC who have developed these guidelines that are to be adhered to. – 4 PRINCIPLES

These are not law but good practice guidance

Principle 1

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court



No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court

Crucial for forensic examination of equipment and must only be undertaken by suitably qualified persons.

THIS IS THE RESPONSE OFFICER ROLE – stop anything changing

Principle 2

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so & be able to give evidence explaining the relevance & implications of their actions



In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

DIGITAL/CYBER INVESTIGATORS IN DIVISION
HI-TEC CRIME UNIT

Principle 3

An audit or other record of all processes applied to computer-based electronic evidence should be created & preserved

An independent third party should be able to examine those processes & achieve the same result



An audit or other record of all processes applied to computer-based electronic evidence should be created and preserved

An independent third party should be able to examine those processes and achieve the same result.

AS WITH ANY COLATION SECURING OR PRESERVATION OF EVIDENCE, WE HAVE TO PROVE OUR CONTINUITY AND OUR TRANSPARENCY WITH HOW WE OBTAINED IT.

IT IS NO DIFFERENT WITH OUR LINES OF ENQUIRY THAT INCLUDE TECHNICAL DATA.

THE ONUS IS ON US AS INVESTIGATORS AND WITHIN YOUR ROLE AS OIC TO PROVE

WHAT YOU HAVE NOW IS THE SAME AS WHEN YOU RECOVERED IT.

An audit or other record of all processes applied to computer-based electronic evidence should be created and preserved

An independent third party should be able to examine those processes and achieve

the same result

Principle 4 ...

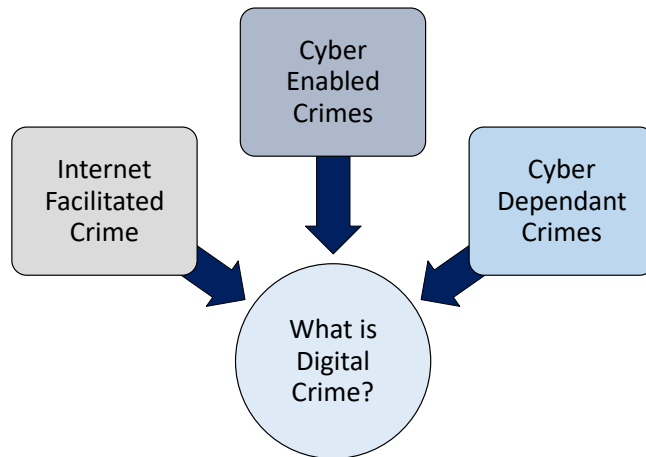
The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law & these principles are adhered to



The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to

OIC ROLE – ie you!

NPCC Principles of Investigating Cyber/Digital Crime



Activity 2 - GROUP WORK – 5 mins

3 Groups – each consider each type of crime and definition and types of crime.

A reminder of the earlier session.....

Internet facilitated Crime – where the internet and smart phones are used in the planning or committing of traditional criminal activity. This can range from online abuse from a neighbour dispute to communications between terrorists planning attacks.

Cyber enabled – such as fraud purchasing illegal drugs/firearms and child sexual exploitation. This can be conducted on or off line however on line can take place at unprecedented speed.

Cyber dependant – crimes which can only be committed using computers, computer networks or other forms of ICT eg, the creation and spreading of malware, hacking, denial of service attacks.



What would you do?

Whilst on patrol you come into contact with an individual whom you suspect to be recently involved in supplying a controlled drug. Under sufficient grounds, you search the individual under S23 Misuse of Drugs Act 1971 & find a substantial quantity of drugs & 3 mobile phones. You seize the drugs & the mobile phones under S23 Misuse of Drugs Act 1971

How would you safely recover the phones?



Activity 3 - Split the Class into 3 groups

Facilitate and group discussion around 'SMART PHONES CAN BE REMOTELY WIPE'D'

Group 1 would seize a phone which is locked (Smartphone – switched on – Charger available).

****Best practice is for the phone to be placed in Aeroplane mode (demonstrate this). If unable, place phone in Faraday bag or place in foil. Get to examiner asap due to battery.**

Group 2 would seize a phone which is on and unlocked (Smartphone – 15% battery).

****Best practice is for the phone to be placed in Aeroplane mode (demonstrate this). If unable, place phone in Faraday bag or place in foil. Get to examiner asap due to battery.**

Group 3 would seize an old fashioned phone – no internet access so minimal threat of loss by remote wipe. If in doubt place in Faraday bag.

Faraday Bag is designed to block wireless signals and prevent the phone making a connection – prevents external interference – will not prevent internally run changes (logic bombs) If a person was supposed to simultaneously press a set of keys daily to keep a destructive program from running on the cell phone, this would be one example of a logic bomb

Note: Section 23 Misuse of Drugs Act 1971

If a [constable](#) has [reasonable grounds to suspect](#) that any person is in possession of a [controlled drug](#) in contravention of this Act or of any regulations or orders made thereunder, the constable may -

- (a) search that person, and [detain](#) him for the purpose of searching him;
- (b) search any [vehicle](#) or vessel in which the constable suspects that the drug may be found, and for the purpose require the person in control of the vehicle or vessel to stop it;
- (c) **seize** and detain, for the purposes of proceedings under this Act, **anything found in the course of the search, which appears to the constable to be evidence of an offence under this Act .**

Police powers to seize phones and obtain passwords

Under PACE, officers can search, seize and retain data from a mobile phone belonging to anyone who has been arrested on suspicion of committing an offence, provided that they have a reasonable belief that it contains evidence of an offence or has been obtained in consequence of the commission of an offence.

Similar seizure powers exist in regards to the execution of search warrants production orders. Data seized can only be kept for the purpose of a criminal investigation and for use as evidence at trial. The police also have additional powers to seize mobile phones under other statutes, such as the Misuse of Drugs Act 1971 and Terrorism Act 2000.

In the case of a suspect's refusal to supply police with the necessary passwords once a mobile phone has been seized, Parliament has provided a partial remedy in the form of a written notice served under section 49 of the [Regulation of Investigatory Powers Act 2000 \(RIPA\)](#) This formal demand addressed to the suspect requires him/her to hand over passwords or encryption keys, or to provide unencrypted copies of material (e.g. biometric data such as thumb prints or iris scanners). If the suspect persists in their refusal this renders them guilty of an offence under section 53 of RIPA, for which they could be sentenced to up to two years imprisonment, and up to five years if the case is one of national security.

**** Trainer to distribute/ email students the Digital Processing Notices, the DPNa, DPNb and DPNc. Trainer to make students aware that these forms DPNa and DPNb and c are the forms that need to be completed if they are seizing a mobile**

phone from a witness (DPNa) or a suspect (DPNc). DPNb provides written guidance in relation to this. These are generic to both forces.**

Digital Devices Exercise



Laptop Eraser



Games Console



Tablet



USB Stick



Wireless Router



Broken Smartphone



Activity 4 – students to remain in the same groups and to rank the items on the PPT slide in order of priority of seizure and why

QTS – what will you be doing prior to seizing any items?

Expected responses – putting on gloves, masks, exhibit bags etc

In your groups rank the following items in order of priority when seizing and why?

Be prepared that you will need to justify your answers and explain what actions you would take in relation to each item.

ANSWERS

Trainer Notes

Seized items Priority list – ensure that latex gloves & masks are worn at all times (Think traditional forensics for attribution purposes)

1) Laptop erasing – immediate action required to preserve evidence which maybe

being erased. Photograph/video what is happening on the screen and photograph in situ. Immediately remove the battery from the laptop as if you just pull the power out of the back it will still run on battery power. Remove the power lead and seize also before packaging and exhibiting correctly (no need for Faraday bag as not able to communicate wirelessly with the internet if power removed)

- 2) Tablet – Immediately place in Airplane mode and turn power off. Place in Faraday bag or wrap in tin foil
- 3) Games consoles – if connected to the internet and powered on remove power leads from rear before packaging and exhibiting correctly
- 4) Broken smartphone – it would appear that it has no power and therefore cannot communicate with wi-fi/telephone services. Consider Faraday bag but seize and package/exhibit correctly
- 5) Wireless router – **DO NOT SWITCH OFF TO SEIZE**. You will lose all data stored in the memory. Also if disconnected very likely to reconnect with a new IP address. Remind of Principle 1 – Not to change anything. High Tech crime can attend and download the router if required
- 6) USB sticks – no power or connection to the internet so seize and packaging and exhibiting correctly

Trainer to highlight the investigative opportunities these devices can potentially provide in the case of a missing persons and Golden Hour principles.

By reviewing Internet searches, recently viewed maps, voice mail, saved favourite places on a navigation app, emails, text messages, phone call logs, and other data, clues can be uncovered as to where the person was headed and who they may be traveling with.

How is Cyber Crime Committed?



Activity 5: Students to use facilities available to research in their groups. Record their findings on a flip chart to debrief.

- **GROUP 1** – COMPUTER MISUSE ACT 1,2,3,3A
- **GROUP 2** – MALICIOUS COMMUNICATIONS
- **GROUP 3** – GENERAL DATA PROTECTION REGULATIONS 2018

The following information has been taken from the NPCC 2012 Good Practice Guide for Digital Evidence

Computer Misuse Act 1990 (UK Wide)

(<http://www.legislation.gov.uk/ukpga/1990/18/introduction>)

COMPUTER MISUSE ACT:

S1 Unauthorised Access To Computer Material

- It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer. It will be necessary to prove the access secured is unauthorised and the suspect knows this is the case.

This is commonly referred to as 'hacking'.

- The Police and Justice Bill 2006 amended the maximum penalty for Section 1 offences. The offence is now triable either way, i.e. in the Magistrates Court or the Crown Court. The maximum custodial sentence has been increased from six months to two years.

S2 Unauthorised Access with Intent to Commit Other Offence

- An offence is committed as per S1 but the S2 offence is committed with the intention of committing an offence or facilitating the commission of an offence. The offence to be committed must carry a sentence fixed by law or carry a sentence of imprisonment of 5 years or more. Even if it is not possible to prove the intent to commit the further offence, the S1 offence is still committed. Max penalty: 5 years imprisonment.

S3 Unauthorised Acts with Intent to Impair Operation

- An offence is committed if any person does an unauthorised act with the intention of impairing the operation of any computer. This 'impairment' may be such that access to data is prevented or hindered or that the operation or reliability of any program is affected. This offence carries a maximum penalty of ten years imprisonment. This offence is used instead of the Criminal Damage Act 1971, since it is not possible to criminally damage something that is not tangible. The Police and Justice Bill 2006 amended the original Section 3 Computer Misuse Act offence, unauthorised modification, and increased the maximum penalty to ten years imprisonment.

S3A Making, Supplying or Obtaining Article for Use in S1 or S3 offences

- The Police and Justice Bill 2006 created a new S3A offence of making, supplying (including offers to supply) or obtaining articles for use in S1 or S3 computer misuse offences. The maximum penalty for this offence is two years imprisonment.

S10 Saving For Certain Law Enforcement Powers

- This section explains that S1 of the Act has effect without prejudice to the operation in England, Wales or Scotland of any enactment relating to powers of inspection, search and seizure.

MALICIOUS COMMUNICATIONS ACT:

Section 1 Mal Comms

1(1) Any person who sends to another person -

(a) a letter, electronic communication or article of any description which conveys -

(i) a message which is indecent or grossly offensive;

(ii) a threat; or

(iii) information which is false and known or believed to be false by the sender; or

(b) any article or electronic communication which is, in whole or in part, of an indecent or grossly offensive nature,

is guilty of an offence if his purpose, or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

1(2) A person is not guilty of an offence by virtue of subsection 1(a)(ii) above if he shows -

(a) that the threat was used to reinforce a demand made by him on reasonable grounds; and

(b) that he believed and had reasonable grounds for believing that the use of the threat was a proper means of reinforcing the demand.

1(2A) In this section **electronic communication** includes -

(a) any oral or other communication by means of an [electronic communications network](#); and

(b) any communication (however sent) that is in electronic form.

1(3) In this section references to **sending** include references to delivering or transmitting and to causing to be sent delivered or transmitted and **sender** shall be construed accordingly.

All Either Way offences

Summary 12 months and/or fine

Indictment 2 years and / or fine

GDPR:

GDPR

General Data Protection Regulation

EU legislation brought into UK legislation under Data Protection Act 2018

Replaces and updates the old Data Protection Act (1998)

Applies to controllers and processors

Applies to any personal data – data that relates to an identified or identifiable individual

8 Principles

Fairly and lawfully processed.

Identify valid grounds

Don't process in any way which is unduly detrimental, unexpected or misleading

Be clear open and honest about how data will be used

Processed for limited purposes.

Must be clear what purposes are

Purpose must be recorded

Cannot use for a new purpose unless compatible with original purpose, consent of subject or clear basis in law

Adequate, relevant and not excessive.

Accurate and up to date

Not kept for longer than is necessary.

Processed in line with the data subject's rights.

Secure.

Not transferred to other countries without adequate protection.

Exemptions for Law Enforcement and National Security – but still need to comply with Part 3 of DPA 2018

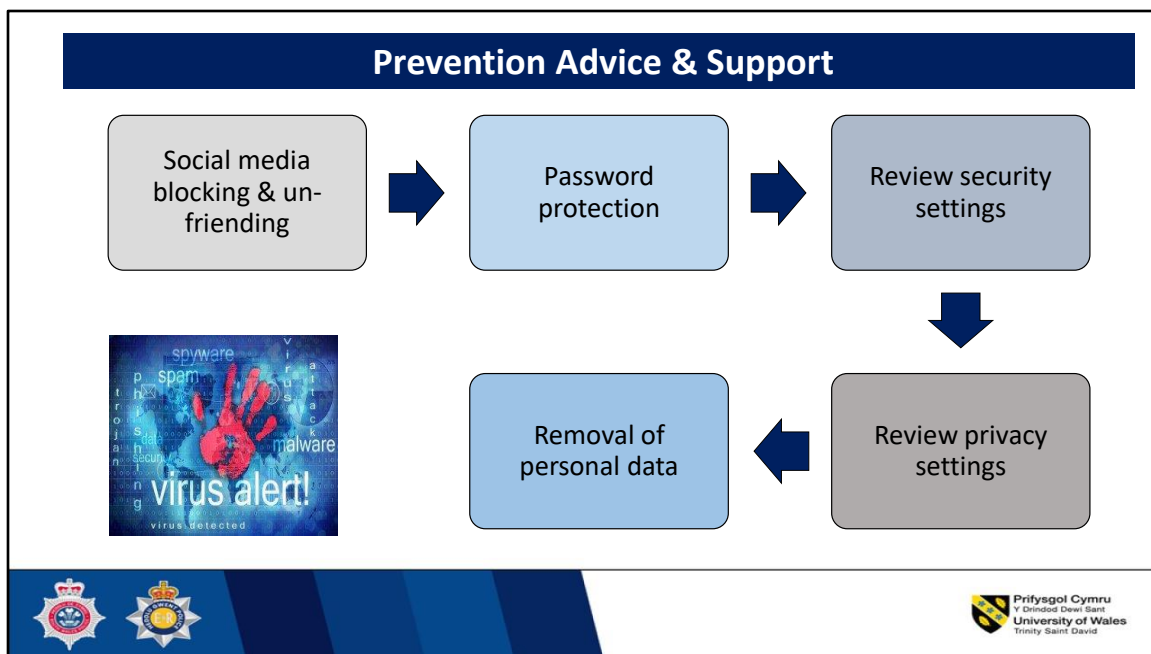
Other Key Legislation to note

PACE 1984	CPIA 1996	RIPA 2000	Criminal Justice & Police Act 2001
Wireless Telegraphy Act 2006	NPCC good practice guide for Digital Evidence 2012	IPA 2016	DPA 2018
	Computer Misuse Act 2018	Police, Crime, Sentencing & Courts Act 2022	



1. Police and Criminal Evidence Act 1984 - makes provisions in relation to police powers, police duties, persons in police detention, evidence, police discipline and complaints against the police.
2. Criminal Procedure and Investigations Act 1996 - it sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation and which may be relevant to the investigation, and related matters.
3. Regulation of Investigatory Powers Act 2000 - governs the use of covert surveillance by public bodies. This includes bugs, video surveillance and interceptions of private communications (eg phone calls and emails), and even undercover agents ('covert human intelligence sources').
4. Criminal Justice and Police Act 2001 - the primary purpose of the is to put policies in place which are aimed at combating crime and disorder within our local community. It deals with issues regarding elements of Anti-Social Behaviour In The Neighbourhood and for the imposition of 'on the spot' fines for other offences as well as being concerned with other issues.
5. Wireless Telegraphy Act 2006 - An Act to consolidate enactments about wireless telegraphy.
6. NPCC Good Practice Guide for Digital Evidence 2012 – (already covered in session)

7. Investigatory Powers Act 2016 - It provides a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies.
8. Data Protection Act 2018 - The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation
9. Computer Misuse Act 2018 – main legislation that criminalises unauthorised access to computer systems & data, & the damaging or destroying of these
10. Police, Crime, Sentencing & Courts Act 2022 – Chapter 3 Extraction of information from electronic devices. S37 – sets out when an authorised person may extract information stored on an electronic device for the purpose of preventing, investigating etc crime, to help locate missing persons or to protect children or at-risk adults from harm. Also, within this section the Secretary of State must prepare a code of practice on the exercise of powers to extract information from electronic devices.



Police officers play an important role in providing prevention advice for internet facilitated crime..

The support agencies that can provide crime prevention advice for digital devices are:

- Get safe online - UK's leading internet safety website providing unbiased, factual & easy to understand information on online safety. Their website provides practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. Every conceivable topic is included on the site – including safe online shopping, gaming and dating ... so you really can stay safe with everything you do online.
- Action Fraud
 - DMIs (Digital Media Investigator)
 - HTCU (High Tec Crime Unit)
 - POLKA (Police Online Knowledge Area)
 - NCA (National Cyber Crime Unit) - Support the most critical

organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

More specifically, the NCSC:

- understands cyber security, and distils this knowledge into practical guidance that we make available to all
- responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK
- uses industry and academic expertise to nurture the UK's cyber security capability
- reduces risks to the UK by securing public and private sector networks

- CEOP (Child Exploitation and Online protection) - is a command of the **UK's National Crime Agency (NCA)**, and is tasked to work both nationally and internationally to bring online child sex offenders, including those involved in the production, distribution and viewing of child abuse material, to the UK courts.

Digital Media Investigators

Provide tactical technical advice & assistance to officers throughout all phases of the investigation of digital/cyber-crimes within the BCU/Division or throughout the South Wales area.



Provides advice & guidance to investigating officers on the completion of relevant applications to obtain digital data from service providers



Attend at search warrants, crime scenes or on police premises to undertake a triage process to assist officers in the seizure, removal & storage of digital equipment



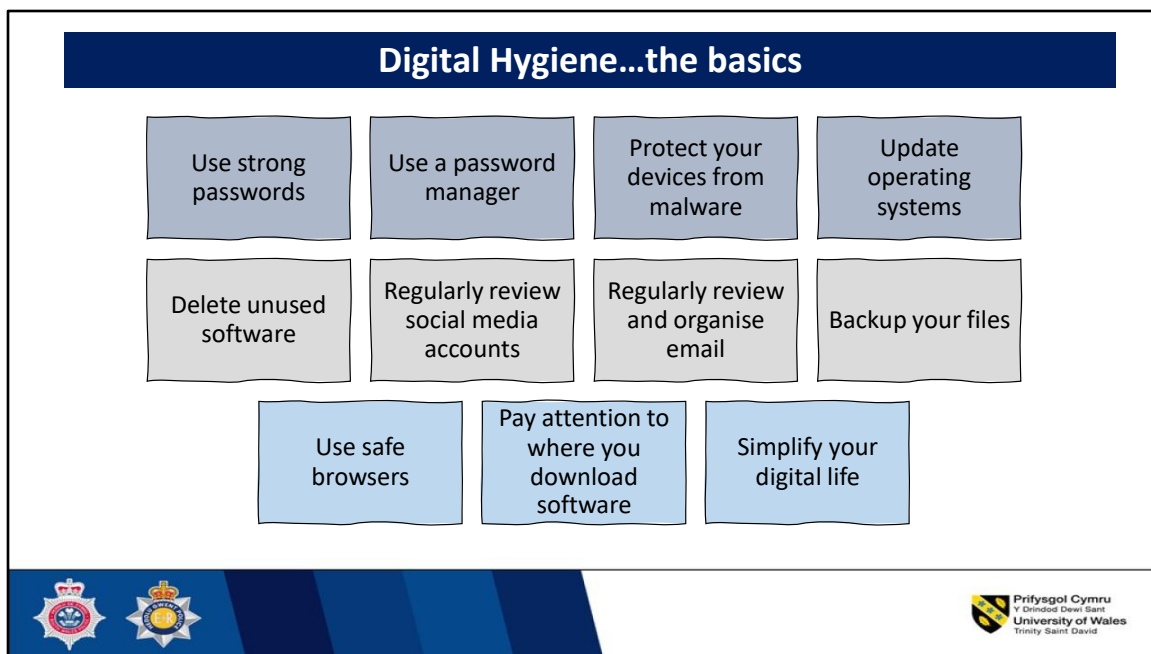
Digital Media Investigators

Will undertake the subsequent examination & retrieval of digital evidence &/or intelligence from computers, computer related media & other digital devices recovered during investigations



Will process the data obtained into a suitable form for investigators to examine for evidential content, & provide prosecution support through preparation of reports & related evidence





QTS – what is digital hygiene?

Digital Hygiene is a phrase that refers to the practice of maintaining your tech devices, protecting your digital information, & safeguarding your electronic assets. In a nutshell, two components revolve around Digital Hygiene, which is simply, organisation & security.

Practicing good digital hygiene can protect your computer from dangers in the same way that practicing good personal hygiene can help protect you from illness.

Poor digital hygiene makes it easier for people to attack you with phishing scams, malware attacks, & other online crimes. It puts your privacy, & potentially the privacy of those you care

about, at risk.

Practicing good digital hygiene involves regularly updating & cleaning electronic devices, using passwords that follow security protocols, organising the files stored on the device, optimising settings, & more. It's a way of keeping the digital devices used by your organisation from becoming more of a liability than an asset.

1. Use strong passwords - As computers get faster, cracking simple passwords gets easier. Ideally, you'll use two-factor authentication everywhere it's allowed, but that doesn't negate the need for a strong password. Hackers use dictionaries to try popular words, as well as combinations and misspellings of those words. A good password won't contain common words. A longer password is harder to crack; over 12 characters is

generally recommended. Using special characters & numbers in the password also increases the complexity required to crack it.

2. Use a password manager - one of the main reasons people use easy to crack passwords is because they are also easy to remember. Nobody wants to be confronted with a login page only to find they can't remember their password.

Password managers make it easy to store passwords in a secure way so they don't have to be remembered every time you want to log in to a site.

3. Protect your devices from malware - Malware comes in many forms. Some of it will silently log the keystrokes on your device & send them back to be collected. With this type of malware, malicious individuals can get passwords, credit card information, & more. Ransomware will

shut down your computer or block access to your files unless you pay a fee to the person who hijacked your system. Anti-virus & anti-malware software can scan for known threats & keep your devices safe from them. Be sure to regularly update these apps so they stay current with the threats that arise.

4. Update operating systems -**Keeping operating systems updated** is important for getting rid of bugs & getting access to improved features & functionality. But beyond that, it's important because each update patches

security threats that have been discovered. These threats, which are now well-known, make your computer a sitting duck for those who wish to do it harm.

5. Delete unused software - Unused software covers both the maintenance & security aspects of good digital hygiene. First of all, it unnecessarily clutters your storage space and your file folders. It might also have services that run in the background, slowing down your devices & using up memory. Over time, many unnecessary apps can cause a marked degradation in performance. Unused software is also

likely not to be updated regularly. This means that if it is used by someone, it may become a security threat.

6. Regularly review social media accounts -

There are several reasons to regularly look over your social media accounts. Some content might not have aged well, & would best be deleted. While this mostly applies to individuals, it's something any organisation should be aware of as well. Occasionally, someone will accidentally post something on social media that contains personally-identifying information. Outdated information on social media bio & about pages can interrupt the regular flow of your operations. A regular review of the content helps prevent these & other mishaps from occurring.

7. Regularly review & organise emails -

Email is still a vital form of communication.

If a security breach happens, the company will likely notify you by email. Expiration of services failed payments, & other important information is also communicated through the media.

Regularly reviewing your inbox will ensure you don't miss anything important. It's also quite common to need to refer back to an email. Organising your email into logical buckets makes it easier to keep it organised. Emails that contain important information, those that you haven't responded to, ones you want to follow up on if there's no replay, can all be much better kept track of if they are organised in a logical way.

8. Backup your files - There are multiple threats to your data. Ransomware can take

control over your files, natural disasters can destroy equipment, hard drives can fail. Whatever the case, losing access to your files is an annoyance at best and a catastrophe at worst.

Keeping multiple backups of your files is an important safeguard against such a disaster. Ideally, at least one of your backups will be at a separate location, such as a cloud backup service (using

archiving online tools)

9. Use safe browsers - Most popular modern browsers have functionality built into them that will alert you if you are going to a dangerous site. You may have even seen such a warning already. These often pop up when a security certificate has expired and the safety of the site cannot be guaranteed. These types of

threats usually come with a warning you can bypass. Other sites are known to be malicious & will be more aggressively blocked by a good browser. Using a browser that offers this protection for you & not bypassing those protections will help keep you safe online.

10. Pay attention to where you download software - Malware very often comes

packaged as legitimate software. Good anti-virus & anti-malware software will scan your downloads to ensure they are safe, but these methods are not fool-proof. They only scan for threats that are known about & only after the software has been updated to include those threats. By only downloading software from reputable companies & reputable sites, you offer

one less avenue of attack for malicious code.

11. Simplify your digital life -

These best practices are something that nobody else can do for you. In fact, they're something that employees & volunteers should be doing, for both their personal computers & for any device owned by your organisation. Other aspects of your digital presence, however, can be

more effectively managed
by a third party.

Digital Hygiene



Risks of using
personal devices for
work?



QTS – what are the risks of using your personal devices for work as oppose to a works device?

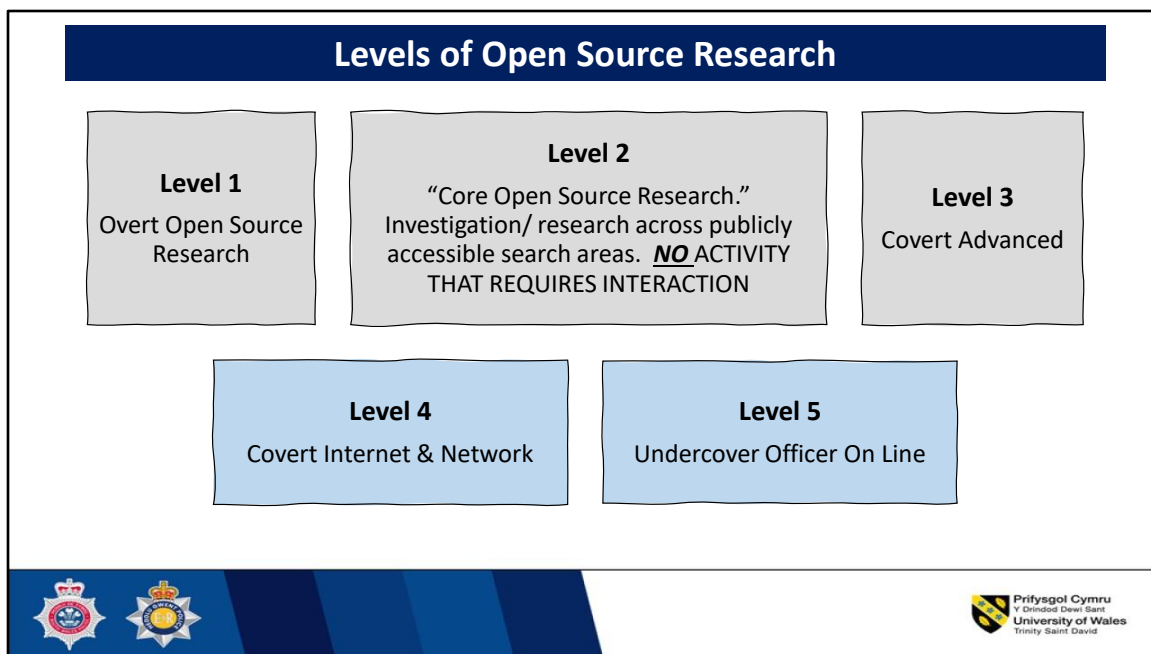
Discuss covering the below points

- Impacts of using personal devices for police business (e.g. automatic connection to networks (no VPN), taking photographs etc.)
 - Seizure of the personal device for evidence and subsequent disclosure at court (e.g. crime scene photographs)
 - Risk of disclosure of personal data in court (if the device is seized)
 - Risk of leaking information about live police operations
 - Tracking and scanning devices
- Data loss – physical loss or theft of a device (& thereby loss or compromise of sensitive data)
- Public exposure – Susceptibility to man-in-the-middle attacks and eavesdropping at public wifi hotspots often used by remote workers. Connecting to personal area networks, e.g. using Bluetooth, poses similar security risks.

Discuss security of passwords

Facilitate discussion around responsibility for keeping personal and force data secure. Discuss strong password choice (i.e. using mix of upper and lowercase, numbers, characters) but using tricks to make them memorable – 1st letter from each word of a sentence – Prefaced by First and Last letter of website and * - finish with number of letters in website

e.g. For Facebook (8 letters) - I drive to work at unit 3 becomes
“Fk*IdTwAuT8”



Open-source is data collected from publicly available sources to be used in an intelligence context.

In the intelligence community the term "open" refers to **overt** publicly available sources (as opposed to covert).

Level 1 – Conduct research across publicly accessible search areas of the internet such as map viewing, street views, and Google etc. As the research is overt, there is no need for a RIPA or police authority.

This research must **NOT** be made through your own Facebook account!

Level 2- A level of authority may be needed to conduct this research, such as directed surveillance under RIPA. This will be on a case by case basis
Staff conducting this research will be DMIs/Cyber trained officers who have received the appropriate training.

Level 3-5 Officers specially trained and must be able to evidentially capture and store the material. It must be evaluated and submitted via the force intelligence management system

Screen Capture and Screenshots



Trainer to facilitate discussion on screenshotting from a range of devices. Use students experience of their own devices. Remind them of usefulness of google

CONSIDER – from smartphones and on computer

iPhone – top and home button

Androids - varies (Swipe for Samsung)

If in doubt, ask the user – consider google / youtube

DEMONSTRATE – windows screen capture.

With desired item/website in view press SCREEN PRINT, on keyboard. Open Word and right click and PASTE. Hold CTRL, ALT and press PRNT SCRN you will only capture the active window

Or to capture specific part of a screen. Press PRT SCRN on the desired page, then open PAINT, within our PNN system and PASTE into the blank screen. Click on select square and then rectangle and cut out the desired area of the screen. SAVE to the desired location.

Use Snipping Tool in Windows 10 – Start Button > Type “snip” in search bar > Select “Snipping Tool” – follow on screen instructions

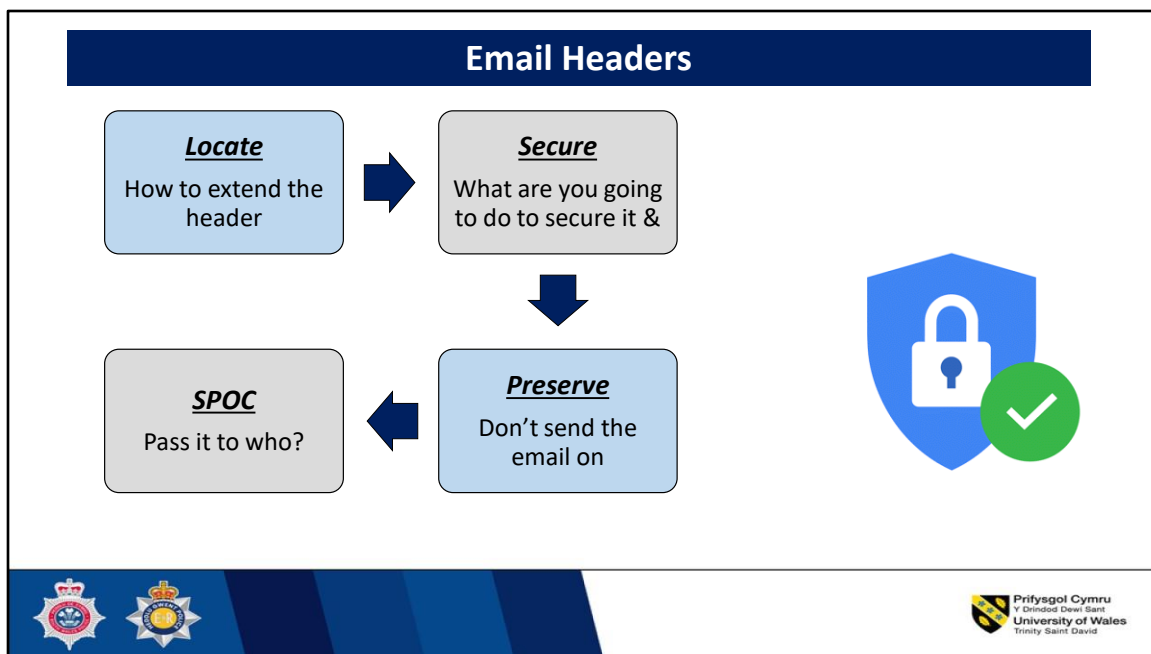
Facilitate discussion on exhibiting (references & statement)

EXHIBITING –

CMJ1 – full screen print

CMJ2 – Full page minus threat (cut out)

CMJ3 – Threat (paste this alone)



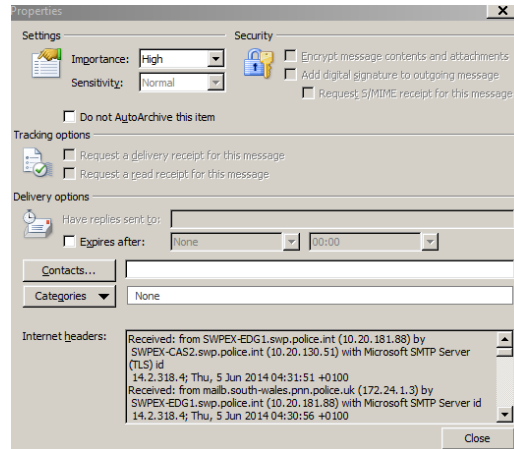
THERE ARE SIMPLE ACTIONS THAT THE FIRST RESPONDER CAN COMPLETE TO SECURE AND PRESERVE EVIDENCE.

THE DATA BEHIND AN E MAIL WILL SHOW YOU ITS JOURNEY FROM ITS SENDER TO RECEIVER AS WELL AS POTENTIAL OTHER VALUABLE EVIDENTIAL OPPORTUNITIES .

THIS IS WHAT WE SEEK TO BE ABLE TO ACHIEVE FROM THIS SESSION.

- 1) LOCATE – we will show you how to extend an e mail to view the hidden data.
- 2) SECURE - how to secure the information you find,
- 3) PRESERVE – how to preserve the information.
- 4) SPOC – who will be able to assist with the information you have gained.

Locating Email Headers



Show on own email how to locate –

- Open email, double click to open full screen
- File
- Properties
- Copy and past the 'internet headers' into a word document

Explain that the digital information may appear to be gibberish to us but lots of data available about the email to the trained eye – Shows Audit Trail of the email from address to address.





External Trainer to follow – Tarian Prevent Cybercrime team

Trainer to handout: Digital Policing Other Considerations