Computer Misuse Act 1990

Police and Justice Act 2006

Regulation of Investigatory Powers Act 2000

Investigatory Powers Act 2016

INTERPOL

National Cyber Security Centre

a part of GCHQ

Consider your Professional Practice !

1. Do you know the relevant legislation in this area?
2. What is currently in the news?
3. If you had to assess a website for vulnerability would you know what to do?
4. If your role was to guide the development of a secure system from scratch, how would you brief the development team?
5. Should you worry about ‘Meltdown’ or ‘Spectre’ ?

19 Security tips to protect your website from hackers (Jan 2017)

- https://psyphire.com/web-hosting/website-security-tips/
  - Passwords
  - Application vulnerabilities
  - https
  - File Permissions
  - File uploads
  - backups
  - SQL injection
  - XSS
  - Error messages
  - Secure email transmissions
  - Server side validation/form validation
  - Sensible user privileges
  - Default CMS settings
  - DDOS protection
  - Web application firewall
  - Email throttling
  - Virus/malware protection
  - Server configuration files
  - Website security testing tools
  - https://transparencyreport.google.com/safe-browsing/search

Why was Computer Misuse Act introduced?

- Robert Schifreen and Stephen Gold, using conventional home computers and modems in late 1984 and early 1985, gained unauthorised access to British Telecom's Prestel interactive viewdata service.
  - The pair were charged under section 1 of the Forgery and Counterfeiting Act 1981
  - Convicted and fined
  - Appealed successfully
  - Prosecution went to House of Lords but appeal failed

Computer Misuse Act 1990

- The Computer Misuse Act is designed to protect computer users against wilful attacks and theft of information.

- Offences under the act include hacking, unauthorised access to computer systems and purposefully spreading malicious and damaging software (malware), such as viruses.

- Unauthorised access to modify computers include altering software and data, changing passwords and settings to prevent others accessing the system, interfering with the normal operation of the system to its detriment.

Computer Misuse Act 1990

- The act makes it an offence to access or even attempt to access a computer system without the appropriate authorisation. Therefore, even if a hacker tries to get into a system but is unsuccessful they can be prosecuted using this law. The act also outlaws "hacking" software, such as packet sniffers, that can be used to break into or discover ways to get into systems.

- Although intention to do wilful damage cannot be easily proved, the act makes it an offence for a hacker to access and use a system using another person's user name, including e-mail, chat and other services.

- The act also covers unauthorised access to different parts of a computer system, therefore, a person may be allowed to access one part of a system but not others, and the accessing of the other parts will be an offence.

- The penalties of breaking the CMA range from fines to imprisonment.

What is it?

- A device for storing, processing and retrieving information.

- The Crown Prosecution Service guidance points to a House of Lords case where Lord Hoffman defined a computer as “a device for storing, processing and retrieving information”.
- https://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/

CMA - Section 1 Offence

1. Unauthorised access to computer material.
   - A person is guilty if:
     - they cause a computer to perform any function with intent to secure access to any program or data held in a computer;
     - the access they intend to secure is unauthorized; and
     - they know at the time when they cause the computer to perform the function that this is the case.

CMA - Section 1 Offence

- The intent a person has to commit an offence under this section need not be directed at
  - any particular program or data;
  - a program or data of any particular kind; or
  - a program or data held in any particular computer.

- A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5, on the standard scale or both.

CMA - Section 2 Offence

2. Unauthorised access with intent to commit or facilitate commission of further offences

- A person is guilty of an offence under this section if
  - he commits an offence under section 1 with intent to commit an offence to which this section applies; or
  - to facilitate the commission of such an offence (whether by himself or by any other person) and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

CMA - Section 2 Offence

- It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

- A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

- A person guilty of an offence under this section shall be liable on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or both; and on conviction on indictment, to imprisonment for a term not exceeding five years, or to a fine, or both.

CMA - Section 3 Offence

3. Unauthorised modification of computer material.
   - A person is guilty of an offence if
     - he does any act which causes the unauthorized modification of the contents of any computer; and
     - at the time when he does the act he has the requisite intent and the requisite knowledge.

- For the purposes of the above, the requisite intent is an intent to cause a modification of the contents of any computer and by so doing:
  - to impair the operation of any computer;
  - to prevent or hinder access to any program or data held in any computer; or
  - to impair the operation of any such program or the reliability of any such data.

CMA - Section 3 Offence

- The intent need not be directed at
  - any particular computer;
  - any particular program or data or a program or data of any particular kind; or
  - any particular modification or a modification of any particular kind.

- For the purpose of the above, the requisite knowledge is knowledge that any modification he intends to cause is unauthorized.

- It is immaterial for the purposes of this section whether an unauthorized modification or any intended effect of it of a kind mentioned above is, or is intended to be, permanent or merely temporary.

Legal or illegal ?

- Time-locking is the practice of disabling functionality or whole programs in order to ensure that software, potentially delivered on condition of further payment, will "expire" and thus no longer function.

US hospital pays $55,000 to hackers after ransomware attack

Hancock Health paid up despite having backups available.

By Charlie Osborne for Zero Day | January 17, 2018 -- 09:53 GMT (09:53 GMT) | Topic: Security

- https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/
- https://us.norton.com/internetsecurity-malware-ransomware.html
- https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

- http://www.bbc.co.uk/news/technology-38123403
- http://www.bbc.co.uk/news/technology-38731011
- http://www.bbc.co.uk/news/uk-england-london-38868152
- http://www.bbc.co.uk/news/technology-36772461
- http://www.bbc.co.uk/news/technology-36575687

Police and Justice Act 2006

- The amendments to the Computer Misuse Act 1990 by Part 5 of the Police and Justice Act 2006 are
  - Section 35. Unauthorised access to computer material
  - Section 36. Unauthorised acts with intent to impair operation of computer, etc.
  - Section 37. Making, supplying or obtaining articles for use in computer misuse offences
  - https://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/

Communications Act 2003

- If a Wi-Fi network is hacked, there will be an offence under the Computer Misuse Act. But using an open wireless network without permission can also be an offence, under the Communications Act 2003.

- Section 125 of the Communications Act describes an offence of dishonestly obtaining communications services. It states: "A person who (a) dishonestly obtains an electronic communications service, and (b) does so with intent to avoid payment of a charge applicable to the provision of that service, is guilty of an offence."

Fraud Act 2006

- Under the Fraud Act 2006 there is a general offence of fraud which can be committed by false representation, by failing to disclose information or by abuse of position.

- Phishing attacks could be prosecuted as fraud. These attacks usually involve sending thousands of emails that purport to come from a bank or another trusted brand in the hope that passwords or account details can be lured from recipients.

- The Fraud Act also provides that it is an offence for a person to be in possession of articles for use in fraud (including software).

The Regulation of Investigatory Powers Act 2000 (RIPA)

- “The Regulation of Investigatory Powers Act 2000 (RIPA) is the main statute bearing on hacking. Section 1 of the Act creates the offence of unlawful interception of a communication.
- In summary, the offence under section 1 is committed by a person who, intentionally and without lawful authority, intercepts any communication "in the course of its transmission" by means of a public (or private) telecommunications system.
- An offender may be sentenced on indictment to a term of imprisonment of up to two years.”

- “Under section 1 of the Computer Misuse Act 1990, it is an offence for a person knowingly to cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer, or to enable any such access to be secured.
- A modern mobile telephone can fairly be described as a computer, as can the servers on which voicemail messages are stored. It appears, however, that the Computer Misuse Act has not yet been used as the basis for a prosecution in relation to hacking.”

Are you being monitored?

https://www.bbc.co.uk/news/uk-34444233 (Oct 2015)

Smartphone users can do "very little" to stop security services getting "total control" over their devices, US whistleblower Edward Snowden has said.

https://news.sky.com/story/how-the-edward-snowden-leaks-revealed-unlawful-spying-11395290

- "All of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight, including from the secretary of state, the Interception and Intelligence Services Commissioners and the Parliamentary Intelligence and Security Committee," a spokeswoman from GCHQ said.

- "All our operational processes rigorously support this position.“

News › UK › UK Politics

GCHQ hacking phones and computers is legal, says top UK court

The ruling includes remotely activating microphones and cameras on electronic devices without the owner's knowledge

Peter Yeung | @ptr_yeung | Saturday 13 February 2016 | 3 comments

- https://www.independent.co.uk/news/uk/politics/gchq-hacking-phones-and-computers-is-legal-says-top-uk-court-a6871716.html

- “The Investigatory Powers Tribunal ruled on Friday that computer network exploitation (CNE) – which can include remotely activating microphones and cameras on electronic devices such as iPhones without the owner’s knowledge – is legal.”
- Campaigners Privacy International’s legal challenge claimed GCHQ's hacking operations are too intrusive and break European law.

- The Home Office has now published a code of practice for hacking, or "equipment interference" as it is also known, and aims to put it on a firmer legal footing in its Investigatory Powers Bill, which became law in 2016.
- According to the judgment, the legal structure under which warrants are issued for GCHQ to carry out equipment interference in the UK is compatible with the European convention on human rights.

- Philip Hammond –
  - "The ability to exploit computer networks plays a crucial part in our ability to protect the British public."
  - "A proper balance is being struck between the need to keep Britain safe and the protection of individuals' privacy."

- Scarlet Kim, a legal officer at Privacy International
  - “During the course of the proceedings, the government sought to create law ‘on the hoof’, changing anti-hacking laws [the 1990 Computer Misuse Act] through an addition to the 2015 Serious Crime Act and producing a code of practice for hacking.
  - Hacking is one of the most intrusive surveillance capabilities available to intelligence agencies.”

How the Dyn DDoS attack unfolded

A massive botnet patched together and deployed around the world swamped regional DNS data centers

By Tim Greene | Follow
Senior Editor, Network World | OCT 21, 2016 4:52 PM PT

http://www.networkworld.com/article/3134057/security/how-the-dyn-ddos-attack-unfolded.html

IS ANYONE SPYING ON YOU THROUGH YOUR WEBCAM?

28 January 2017

News Article

https://www.europol.europa.eu/newsroom/news/anyone-spying-you-through-your-webcam

Global police smash huge online crime network (Update)

December 1, 2016

The "Avalanche" network would be contacted by other criminal groups to send emails to containing malware to steal bank details and password

https://phys.org/news/2016-12-europol-unprecedented-cybercrime-op.html

Attack code for 'unpatchable' USB flaw released (Oct 2014)

- Details of the BadUSB flaw were released at the Black Hat computer security conference in August by Karsten Nohl and Jakob Lell.
- Their work revealed how to exploit flaws in the software that helps devices connect to computers via USB. The biggest problem they discovered lurks in the onboard software, known as firmware, found on these devices.
- Among other things, the firmware tells a computer what kind of a device is being plugged into a USB socket but the two cybersecurity researchers found a way to subvert this and install attack code. At Black Hat, the BBC saw demonstrations using a smartphone and a USB stick that could steal data when plugged into target machines.
- https://www.bbc.co.uk/news/technology-29475566

What is the Dark Web?

- The Dark Web is a term that refers specifically to a collection of websites that are publicly visible, but hide the IP addresses of the servers that run them. Thus they can be visited by any web user, but it is very difficult to work out who is behind the sites. And you cannot find these sites using search engines.
- Almost all sites on the so-called Dark Web hide their identity using the Tor encryption tool. You may know Tor for its end-user-hiding properties. You can use Tor to hide your identity, and spoof your location. When a website is run through Tor it has much the same effect.

- Indeed, it multiplies the effect. To visit a site on the Dark Web that is using Tor encryption, the web user needs to be using Tor. Just as the end user's IP is bounced through several layers of encryption to appear to be at another IP address on the Tor network, so is that of the website. So there are several layers of magnitude more secrecy than the already secret act of using Tor to visit a website on the open internet - for both parties
- Not all Dark Web sites use Tor. Some use similar services such as I2P - indeed the all new Silk Road Reloaded uses this service. But the principle remains the same. The visitor has to use the same encryption tool as the site and - crucially - know where to find the site, in order to type in the URL and visit.
- http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-3593569/

Deep v Dark

- The 'Deep Web' refers to web pages that are invisible to search engines.
- “the 'Deep Web' includes the 'Dark Web', but also includes all user databases, webmail pages, registration-required web forums, and pages behind paywalls.”

Blog post

Active Cyber Defence - tackling cyber attacks on the UK

Created: 01 Nov 2016
Updated: 01 Nov 2016
Author: Ian Levy
Part of: Cyber strategy, Government strategy, The NCSC

National Cyber Security Centre

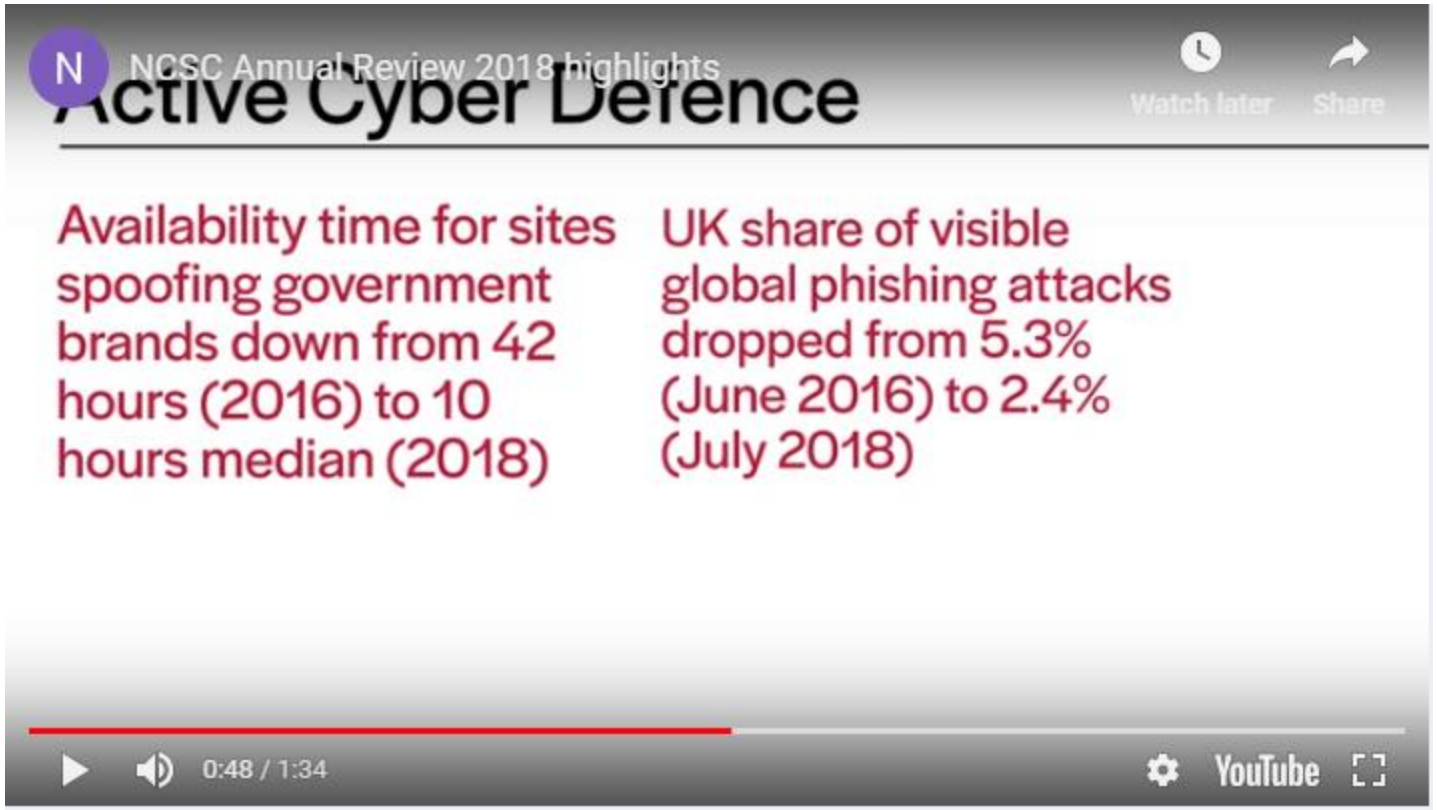
a part of GCHQ

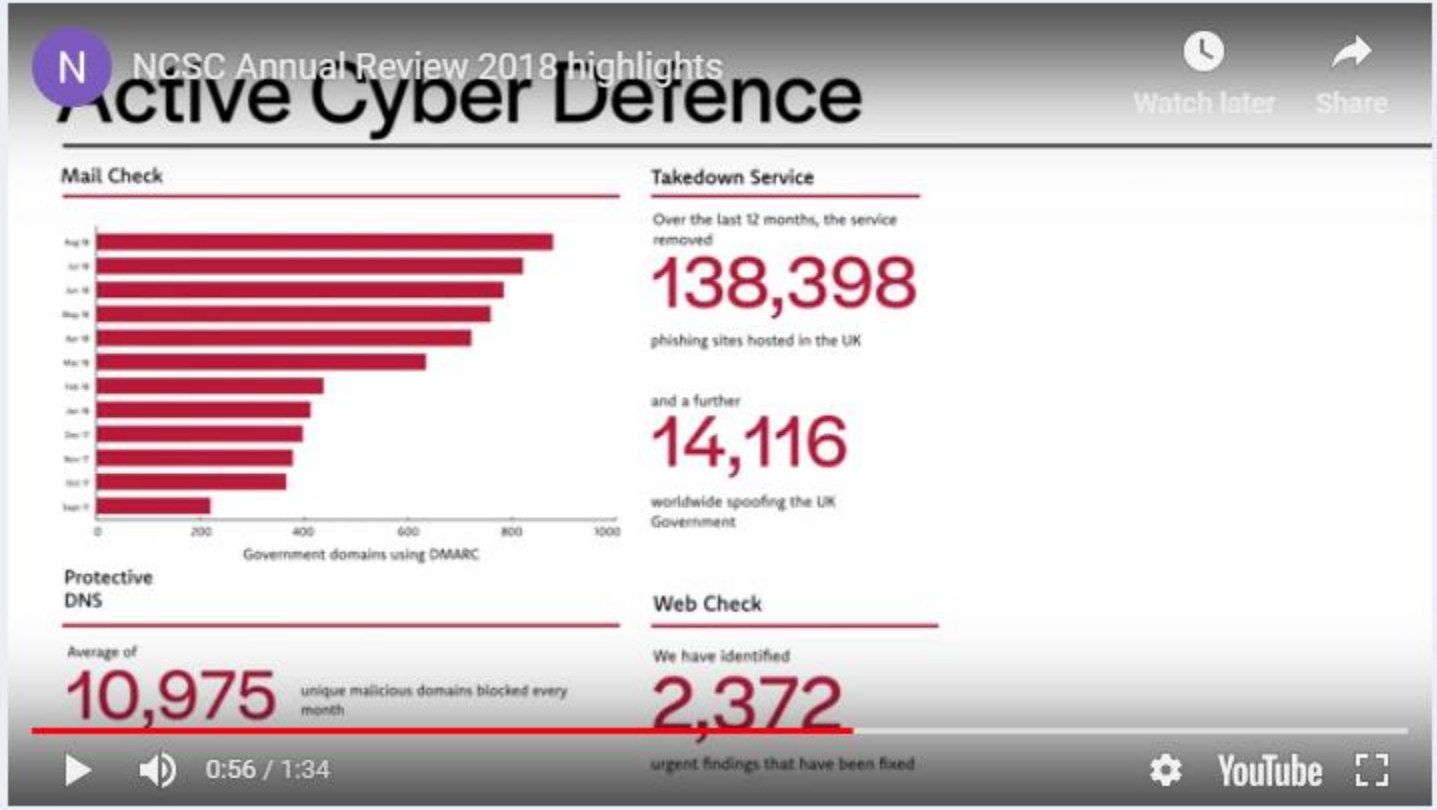
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

National Cyber Security Centre
a part of GCHQ

- The UK Government is fully committed to defending against cyber threats and address the cyber skills gap to develop and grow talent. The NCSC was created as part of the five year National Cyber Security Strategy (NCSS) announced in 2016, supported by £1.9billion of transformational investment.
- The NCSC provides a single, central body for cyber security at a national level and is the UK's technical authority on cyber. It manages national cyber security incidents, carries out real-time threat analysis and provides tailored sectoral advice.
- GCHQ is the parent body for the NCSC, meaning that it can draw on the organisation's world-class skills and sensitive capabilities.

- https://www.ncsc.gov.uk/blog-post/securing-office-365-better-configuration
- https://www.ncsc.gov.uk/information/about-ncsc
- Career path for some of you in cyber security??


N
NCSC Annual Review 2018 highlights
Watch later
Share
Active Cyber Defence
Availability time for sites spoofing government brands down from 42 hours (2016) to 10 hours median (2018)
UK share of visible global phishing attacks dropped from 5.3% (June 2016) to 2.4% (July 2018)
0:48 / 1:34
YouTube


NCSC Annual Review 2018 highlights
Active Cyber Defence
Watch later
Share
Mail Check
0
200
400
600
800
1000
Government domains using DMARC
Takedown Service
Over the last 12 months, the service removed
138,398
phishing sites hosted in the UK
and a further
14,116
worldwide spoofing the UK Government
Protective DNS
Average of
10,975
unique malicious domains blocked every month
Web Check
We have identified
2,372
urgent findings that have been fixed
0:56 / 1:34
YouTube