Written by R. J. Nixon

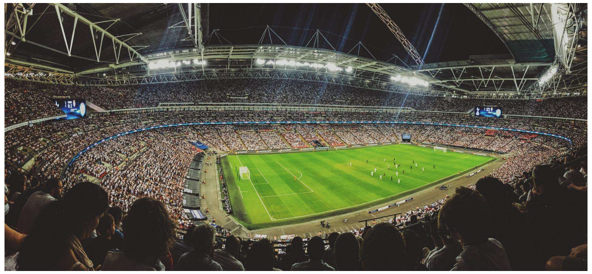
Knowledge Organiser - Cyber Security

Key Terms & Definitions

1	Data	Individual facts or statistics
2	Information	Processed data with added context so that it is meaningful
3	Cyber Security	Protecting computer systems from cyber criminals
4	Cyber Criminal	A person who uses digital technology to commit crime
5	Profiling	Gathering information about a person in order to make predictions about them
6	User behaviour	How a person interacts with a computer system
7	Privacy policy	A document produced by an organisation which explains how they store and process user data.
8	Data protection act (2018)	UK law which controls how your personal information is stored and processed by organisations
9	Data subject	The person who some personal data stored by an organisation is about.
10	Data portability	The right that a person has to move their personal data from one computer system to another in a safe and secure way
11	Malware	Any software which is designed to do harm to a computer system
12	Social engineering	Tricking other people so that they give up confidential information
13	Phishing	Sending a message to a person which is designed to trick them into giving up confidential information
14	Blagging	Making up a story designed to encourage another person to give up confidential information
15	Shouldering	Stealing confidential information by watching someone enter it into a keypad or other device
16	Name generator attack	Using a quiz (which creates a name, for example, your superhero name) to obtain personal information that can be used to gain access to a person's personal information
17	Scam	A dishonest scheme carried out to gain access to some confidential information
18	Hacking	Gaining unauthorised access to or control of a computer system

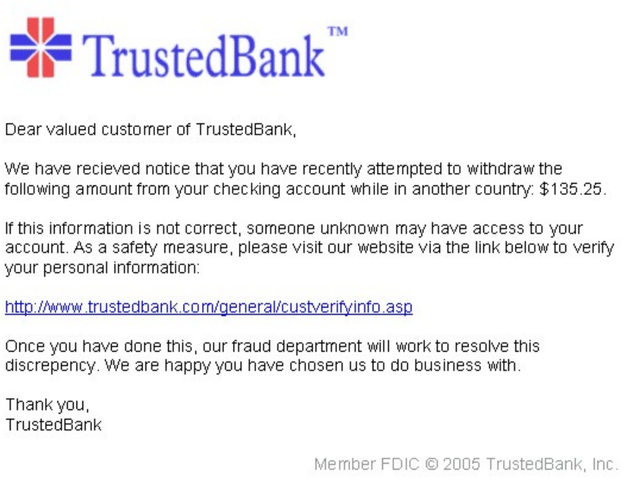
19	Ethical hacking	Gaining access to a computer system with the permission of its owner to help them identify vulnerabilities in their computer systems.
20	Penetration testing	A form of ethical hacking, penetration testing involves an organisation hiring an ethical hacker to test the security of their computer systems and report any vulnerabilities back to them
21	Brute force attack	Trying to gain access to a computer system by trial and error such as by guessing all possible passwords until the correct one is guessed.
22	Script kiddie	A person who uses tools downloaded from the internet to allow them to hack into computer systems with little technical knowledge
23	Denial of service attack (DoS)	Sending a lot of information to a computer system in an attempt to overload the system so that it becomes unavailable to its intended users
24	Distributed denial of service attack (DDoS)	Using multiple computers to perform a DoS attack
25	Computer misuse act (1990)	UK law which introduced a range of offences relating to computer misuse including accessing computer material without permission, using and creating malware and accessing computer material with intent to commit further crime
26	Ransomware	Malware designed to stop a person or organisation accessing their data. The attacker who created the ransomware will demand the person or organisation pays a large amount of money to regain access to their data
27	Virus	Malware in the form of a program which attaches itself to another file and can create copies of itself when the file is opened / run
28	Trojan	Malware that is hidden inside another file. Often done with the purpose of tricking a user into downloading it by disguising the malware as something they want, for example, a free game
29	Worm	Malware that is able to create copies of itself without the use of another file
30	Adware	Unwanted software which is designed to display adverts on a user’s computer screen
31	Spyware	Software used to secretly monitor the behaviour of a user
32	Bot	Software which is programed to do certain tasks by itself
33	Botnet	A network of computers which a hacker has infected with malware allowing them to remotely control the computers
34	Anti-malware	Software which is designed to identify malware and remove it from a computer system

35	Firewall	A piece of hardware or software which filters traffic going in and out of an organisation’s network based on rules set by the network administrator
36	Biometrics	Physical characteristics that can be used to identify individuals
37	Two factor authentication	An extra layer of security used to make sure an individual is who they say they are
38	CAPTCHA	A test used to determine whether a human or a computer is interacting with a piece of software
39	Backup	A copy of some data created so that the data can be restored if the original is lost
40	ISP	Internet service provider. An organisation that provides services for accessing, using and participating in the Internet.
41	Auto-updates	Changes to software that are made without the user needing to do anything
42	User authentication	Any method used to work out if a user is who they say they are
43	User permissions	Grouping users by role (for example administrators, teachers, students) and allowing those groups of users access to different parts of a computer system

Data	**Information**	**UK Law**	
Data is just facts and figures: Man City 1 Liverpool 2 Chelsea 3 	**Information** is created when that data is given context: These are football teams that play in the premier league and their positions in the league table. 	**Data Protection Act (2018)** 	**Organisations must use data:** ● Fairly, openly and in accordance with the law ● For a specific and stated reason ● Only in a way that is necessary and sufficient for the purpose for which it was collected ● Which is accurate and up to date ● Only for as long as it is needed They must also protect data from loss, damage and unauthorised access. **You have the right to:** ● Find out how your data is being used ● Access data that an organisation has about you ● Update your data ● Have your data deleted ● Stop an organisation processing your data ● Transfer your data to a different organisation
The value of user data 	User data is valuable to businesses because, once collected, they can use it for **profiling**. **Profiling** can help a business make decisions about how to become more profitable. For example, if a supermarket knows how many ice creams it is likely to sell on a particular day, they can order just the right number to avoid wasting money ordering too many.	**The Computer Misuse Act (1990)**	**Makes it illegal to:** ● Gain unauthorised access to computer material ● Gain unauthorised access to computer material with intent to commit or facilitate other offences ● Impair the operation of a computer without the authorisation to do so

Social Engineering Methods

Phishing



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

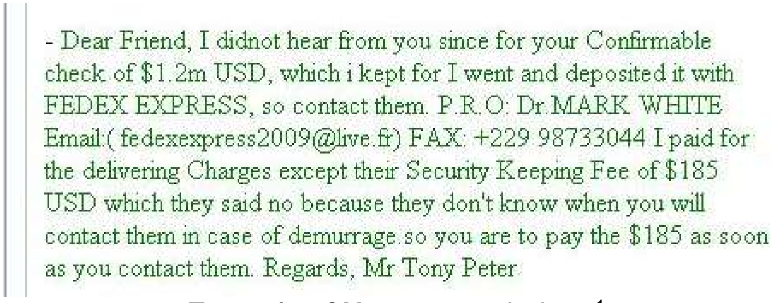
Key indicators of a phishing message:

- The message was not expected
- The message contains spelling errors
- The message is generic, not addressed using your name and does not contain any personal information you'd expect the sender to know
- The message contains suspicious links

Blagging

Psychological techniques used to make a user more likely to act:

- **Urgency** - “you must send the information in the next 24 hours”
- **Fear** - “all your data will be lost if you don't click this link”
- **Request for help** - “please send the details of your IT manager so we can create your free account”
- **Worry** - “your friends Alice and Bob are in trouble. Please send the money quickly so I can help them”



- Dear Friend, I didnot hear from you since for your Confirmable check of $1.2m USD, which i kept for I went and deposited it with FEDEX EXPRESS, so contact them. P.R.O: Dr.MARK WHITE Email:(fedexexpress2009@live.fr) FAX: +229 98733044 I paid for the delivering Charges except their Security Keeping Fee of $185 USD which they said no because they don't know when you will contact them in case of demurrage.so you are to pay the $185 as soon as you contact them. Regards, Mr Tony Peter

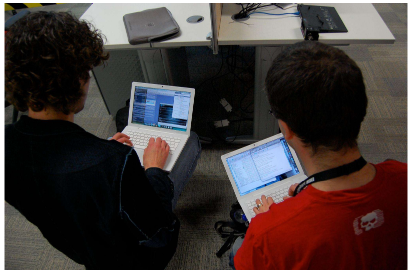
Example of **Urgency** technique[1]

Shouldering

An obvious example of shouldering is looking over someone's shoulder at the bank as they enter their PIN number.

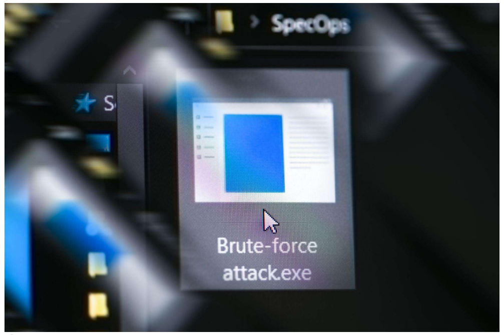
However, this is not the only way shouldering can happen. Cameras can be used to observe people entering sensitive information remotely. An attacker could look at someone entering their password via a reflection in a window. These are also examples of shouldering.

[1] “Pitifully Bad Spear Phishing Attempt” by Purple Slog is licensed under CC BY 2.0

Types of hackers		**Denial of service attacks**	
Unethical hackers 	Gain **unauthorised** access to or control of a computer system. **Reasons someone might do unethical hacking:** ● To steal data ● To disrupt services ● For financial gain ● For political reasons ● For fun	**Denial of service (DoS)**	Usually done to stop other computer users being able to access a service being provided by a server. Can cause damage to a company's reputation (unavailability of service) and income (loss of sales/business). Can cause harm to individuals too. For example, if a bank was a victim of a DoS attack people may not be able to access their money.
Ethical hackers  [2]	Gain access to a computer system with the **permission of its owner** to help them identify vulnerabilities in their computer systems. Companies pay **penetration testers** to hack into their computer systems and tell them how to improve the security of their computer systems. These **penetration testers** are ethical hackers.	**Distributed denial of service (DDoS)**	Harder to prevent than a normal DoS attack because requests are coming from multiple sources. Since requests come from different sources it is difficult to identify who is behind the attack.
Script kiddies	Gain access to computer systems without much technical knowledge using tools they download from the internet. They're usually doing this for **unethical** reasons so can be considered a type of unethical hacker.	**Case study: 2007 Estonia DoS attack** 	In 2007, the country of Estonia suffered a major DoS attack. It led to people in the country not being able to access their money online or through cash machines, government employees not being able to use their email accounts and news organisations not being able to report the news.

[2] "Hacking in progress at BarCampLondon 3" by Cristiano Betta is licensed under CC BY 2.0

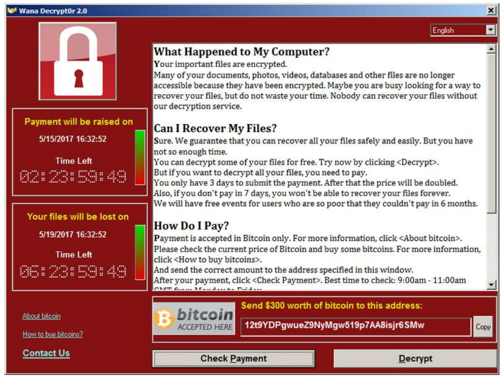
		[3]	

Brute force attacks  [4]	IT administrators can take a range of measures to prevent hackers using brute force attacks on their systems. **Methods of prevention:** - Limit number of login attempts. - Time delay between access attempts. - The use of a **CAPTCHA**. - Using 2FA.	**Viruses** 	**Common ways to catch a computer virus:** - Downloading it from an email attachment - Clicking on a webpage pop-up window without reading it - Downloading files from illegal websites
Malware [5]	Malicious software (malware) can be used for a range of reasons: - To disable hardware - To steal data - To send email spam - To steal money - For forced advertising Malware can also come in a variety of forms: - Viruses - Trojans	**Ransomware**	**Ransomware** is a specific kind of virus. Ransom payment is usually demanded in a cryptocurrency such as bitcoin. This makes it harder to identify who is responsible for the attack. **Case study: WannaCry** In 2017, the WannaCry ransomware spread globally through computers running Microsoft Windows. Many organisations were impacted from

[3] "Flag-map of Estonia" by Stasyan117 is licensed under CC BY-SA 4.0

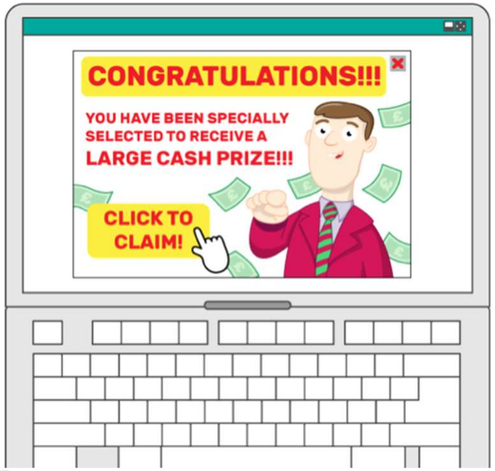
[4] "Mouse cursor about to double-click and run "Brute-force attack" executable" by Ivan Radic is licensed under CC BY 2.0

[5] Malware by Nick Youngson CC BY-SA 3.0

	● Worms ● Adware ● Spyware ● Ransomware	 **What Happened to My Computer?** Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service. **Can I Recover My Files?** Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months. **How Do I Pay?** Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am Payment will be raised on 5/15/2017 16:32:52 Time Left 02:23:59:49 Your files will be lost on 5/19/2017 16:32:52 Time Left 06:23:59:49 Send $300 worth of bitcoin to this address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Wana Decrypt0r 2.0 English bitcoin ACCEPTED HERE Copy About bitcoin How to buy bitcoins? Contact Us Check Payment Decrypt 6	hospitals to schools, banks and charities. Read more about it here.

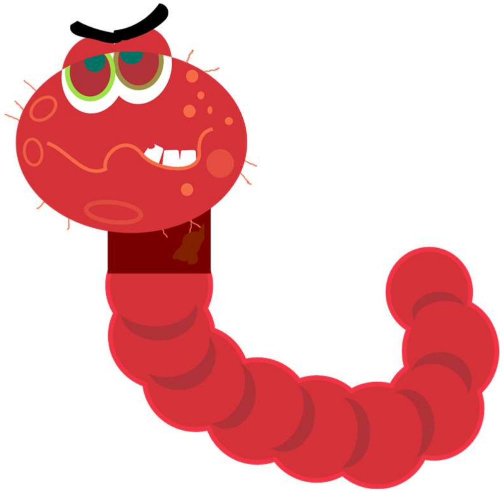
[6] 감염사진 by 황승환 is licensed under CC BY-SA 4.0

<table>
<tr>
<td><b>Trojans</b>
 </td>
<td>Trojan’s can be effective because they’re often downloaded by mistake by a user who falls for the disguised file. It may be disguised as something they want such as a free game, film or music file.

<b>Case study: ZeroAccess</b> is a Trojan that affects computers that run Microsoft Windows. Its purpose is to turn victims' computers into bitcoin miners or click fraud machines for the attacker. You can read more about it here.</td>
<td><b>Adware</b>


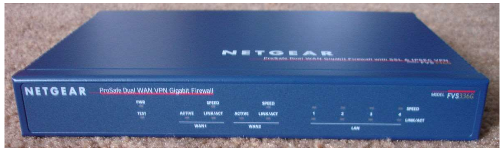
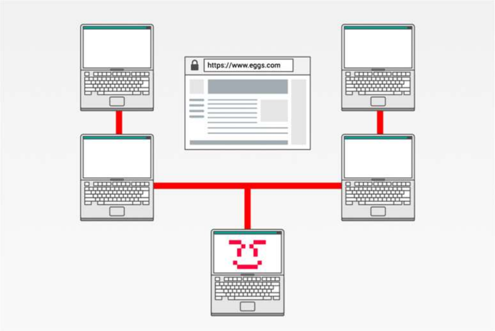
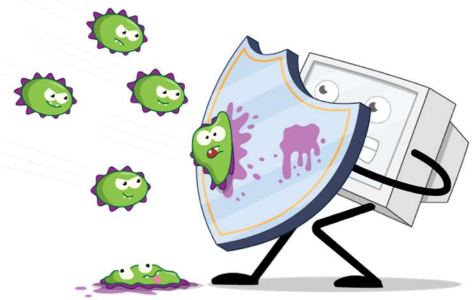
[7]</td>
<td><b>Adware</b> can be used to make money for its developers by automatically showing the user of an infected computer adverts.

Some more dangerous <b>Adware</b> can be used as a way for an attacker to spread other malware onto a user’s machine.</td>
</tr>
<tr>
<td><b>Spyware</b>
 </td>
<td>Some <b>Spyware</b> can be used for spam purposes, sending you harmless but annoying adverts.

However, some more dangerous <b>Spyware</b> can also contain keyloggers that can be used by an attacker to steal personal information such as passwords.</td>
<td><b>Worms</b>
</td>
<td><b>Worms</b> can be especially effective because they are a type of malware which is capable of self-replication without the user needing to do anything.

<b>Case Study: Father Christmas Worm</b>
In 1998 a relatively harmless worm was unleashed on a large scientific computing network whose users included universities and NASA. It sent a “Merry Christmas” message to every user on every machine it infected. Learn more about the Father Christmas Worm here.</td>
</tr>
</table>

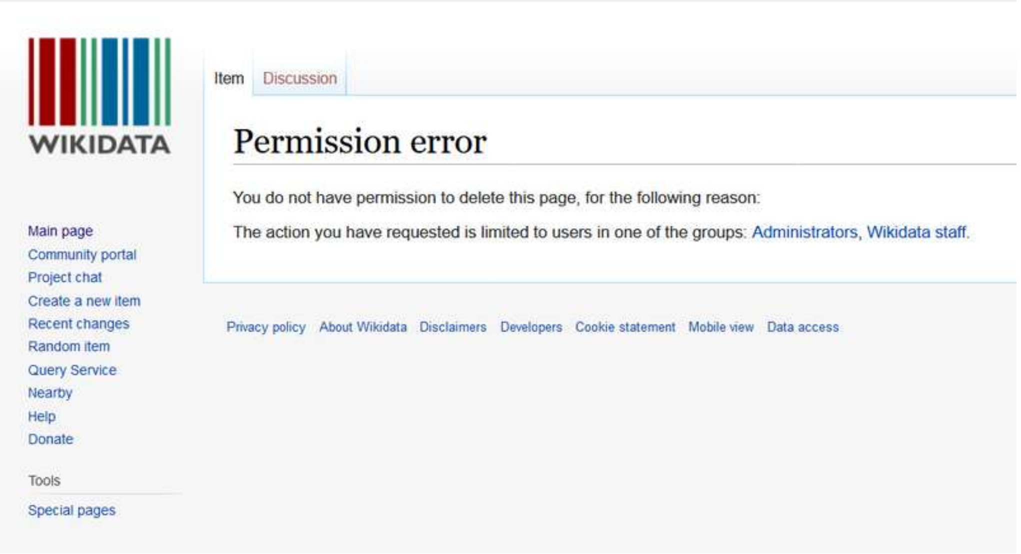
[7] Image by NCCE is licensed under the Open Government Licence v3.0.

Bots		Protection Methods	
Good Bots 	**Bots** aren’t always bad. In fact bots are essential for the modern internet to function. For example, Google uses bots to find new and updated websites for search results. **Bots** are also used by online businesses to help customers using their websites (chatbots) and they can be used to monitor prices of items to get the best deal.	**Firewall**  A physical (hardware) firewall[8]	**Firewalls** can be physical or virtual (software). **Firewalls** can be used to stop malware from entering a network. They can also be used to enforce network policies. For example, a school could use a firewall to stop students playing games in their lessons.
Bad Bots  9	However bots can be used by cyber criminals for criminal purposes. For example, **botnets** can be used to perform a **DDoS** attack.	**Anti-malware software**  10	**Anti-malware software** works by checking files on your computer against a list of malware **definitions**. Malware **definitions** are sequences of code that are known to be malicious. It's important to keep your anti-malware software up to date so that it has the most recent list of **definitions**. If a file on your computer contains code that matches a malware definition it will be **quarantined** (separated from the rest of the files on your computer so it can’t do any harm).

[8] Netgear ProSafe Dual WAN VPN Gigabit Firewall FVS336G front by Zuzu is licenced under CC BY-SA 3.0

[9] Image by NCCE is licensed under the Open Government Licence v3.0.

[10] Image by NCCE is licensed under the Open Government Licence v3.0.

Protection Methods		
Auto-updates 	**Automatic updates** are useful because lots of user's will not bother to or know how to install software updates themselves. Auto-updates mean that these people still have the latest security fixes. **Example:** A chromebook will automatically update its operating system without needing to do anything. This means that you always have the version of the operating system with the most up to date security fixes.	**User permissions** User permissions are helpful for restricting the parts of a computer system that a group of users can access. This improves security because it reduces the number of people with access to part of a computer system to only those who need it. For example, in a school, a student should not be able to access and take a register. Therefore this permission is restricted to only those who need to perform this task, the teachers.
User authentication 	Passwords are one of the most common methods of **user authentication**. Password rules, such as a minimum length, are usually enforced to try to make users choose strong passwords. There are other methods of user authentication too. For example, fingerprint and iris scanners, known as biometric methods, are also reasonably common now. User authentication can be made more secure using **2FA** (2 factor authentication). This is where the user has to pass some other challenge as well as entering their password, such as entering a code from a text message.	 WIKIDATA Item Discussion Main page Community portal Project chat Create a new item Recent changes Random item Query Service Nearby Help Donate Tools Special pages Privacy policy About Wikidata Disclaimers Developers Cookie statement Mobile view Data access Permission error You do not have permission to delete this page, for the following reason: The action you have requested is limited to users in one of the groups: Administrators, Wikidata staff. [11]

[11] Permission error by ErraticProfessional is licensed under CC BY-SA 4.0