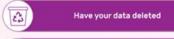
DATA PROTECTION ACT 2018

ALL ORGANISATIONS USING AND STORING DATA MUST **ABIDE BY THE FOLLOWING PRINCIPLES**











SOCIAL ENGINEERING

Social engineering is a set of methods used by cybercriminals to deceive indi- viduals into handing over information that they can use for fraudulent purposes.

How might a hacker use the data you submitted?

- Name of first pet
- Favorite colour
- Mother's maiden name
- Favorite band or artist
- Date of birth
- Name / Email address



Shouldering (also known as shoulder surfing) is an attack designed to steal a vic- tim's password or other sensitive data. It involves the attacker watching the vic- tim while they provide sensitive information, for example, over their shoulder. This type of attack might be familiar; it is often used to find out someone's PIN at a cash machine.

PHISHING ATTACK

A phishing attack is an attack in which the victim receives an email disguised to look as if it has come from a reputable source, in order to trick them into giving up valuable data. The email usually provides a link to another website where the information can be inputted.

Phishing: Key indicators of a phishing email

- Unexpected email with a request for information
- Message content contains spelling errors
- Suspicious hyperlinks in email
 - Text that is hyperlinked to a web address that contains spell- ing errors and/or lots of random numbers and letters
 - Text that is hyperlinked to a domain name that you don't recognise and/or isn't connected to the email sender
- Generic emails that don't address you by name or contain any personal information that you would expect the sender to know

BLAGGING

Blagging (also known as **pretexting**) is an attack in which the perpetrator invents a sce- nario in order to convince the victim to give them data or money.

Hacking in the context of cyber security is: Gaining unauthorised access to or control of a computer system

Why might people want to hack?

system.

Distributed denial of service attack (DDoS)

This uses the same concept as a DoS attack, but this time it is multiple computers making the attacks at the same time.

Denial of service attack (DoS) This is a cyberattack in which the criminal makes a

network resource unavailable to its intended users. This is done by **flooding** the

targeted machine or website with lots of requests in an attempt to overload the

It is a lot harder to:

BLAGGING

- Stop the attack by simply blocking a single source
- Identify who is responsible, as lots of machines are making requests, many of them because they are infected by malware

Brute force attack This is a form of attack that makes multiple attempts to discover something (such as a password).

MALWARE

Typical actions of malware include deleting or modifying files.

Spyware—secretly monitors user actions, e.g. key presses, and sends information to the hacker. Some spyware can even use your webcam without your knowledge.

Viruses—spreads through normal programs and might slow down your device or change your ap-plications and documents.

Worms– spread from device to device and copy themselves hundreds of times. A worm might copy itself onto your email account and then send a copy to all of your email contacts!

Trojan horse—pretends it will be a useful and safe program, when actually it will try to attack your device.

Adware—displays adverts while it is running; some can serve as spyware, gathering information

BOTS

Internet bots

Bots are automated programs that perform tasks repeatedly.

Bots are a crucial part of the internet's infrastructure and perform useful tasks such as:

- Finding new websites for search engines to index
- Providing customer service online (chatbots)
- Monitoring the prices of items to find the best deal (shopbots)

PROTECTION

Firewalls A firewall checks incoming and outgoing network traffic. It scans the data to make sure it doesn't contain anything malicious and that it follows the rules set by the network.

Anti-malware Anti-malware is software that scans any file that is able to execute code. The anti- malware will have a list of definitions of sequences of code that they are aware are malicious. If the code in your files matches the definitions, the files are quarantined.

Auto-updates Auto-updates refers to software that automatically checks for available updates for the software you have on your computer. Once it finds an update, the software can be set either to alert the user or to install it automatically. This software is often included with an operating system. User

permissions Users on a network can be put into groups, with each group having

The Computer Misuse Act (1990)

The Computer Misuse Act (1990) and its amendments were created so that unauthorized access to computers and crimes committed using a computer could be prosecuted. The act is based on three principles and makes the fol-lowing actions illegal:

PRINCIPLES

LEGAL ACTIONS

Unauthorised access to digital/computer material. This means a person asking a computer to perform any function with the fine. intent of accessing anything on the computer for which they do not have per- mission, and for which they know they do not have permission.

Punishable by up to two years in prison and a £5,000

Used for a specific and stated reason

sufficient for the purpose for which it was collected

Accurate and up-to-date

Only kept for as long as it is needed

Protected against loss, damage, and unauthorised access

AS A DATA SUBJECT YOU

HAVE THE RIGHT TO FIND

THE GOVERNMENT AND

OTHER ORGANISATIONS

STORE ABOUT YOU.

OUT WHAT INFOR- MATION

Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to commit another crime or to enable someone

Punishable by up to five years in prison and an unlimited fine determined by the damage caused and the severity of the crime.

else to commit a crime.

Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer. This means a person intentionally im-pairing the

Punishable by a prison sentence of up to ten years and an unlim- ited fine, but if the act puts life operation of any computer or program, or at risk or endangers