Computing GCSE – 1.6a

J276/01 – System Security

KEY VOCABULARY - VULNERABILITIES	
Hacking	Attempting to bypass a system's security features to gain unauthorised access to a computer
Malware	Malware is malicious software, loaded onto a computer with the intention to cause damage or to steal information. Viruses are a type of malware
Phishing	Phishing is a common way to try to steal information like passwords. Emails are sent, requesting the user logs into a website, but the site is a fake, and the users details are logged
Social engineering	People are the weakest point of any system. If a hacker can convince a user to give over their data, this is the easiest way into a secure system
Brute force attack	Using and algorithm to try every possible combination of characters to 'guess' the users password.
Data interception	Data interception, or *Man in the Middle attacks* are hacks that use 'packet sniffer' software to look at every piece of data being transmitted in the local area to find ones that meet the hacker's criteria. Often done by creating 'fake' wireless networks to record users details
SQL injection	Using SQL statements to trick a database management system (DBMS) into providing large amounts of data to the hacker
Denial of Service Attack	Hackers flood a network with huge amounts of fake data and requests in an attempt to overload the system so that it crashes

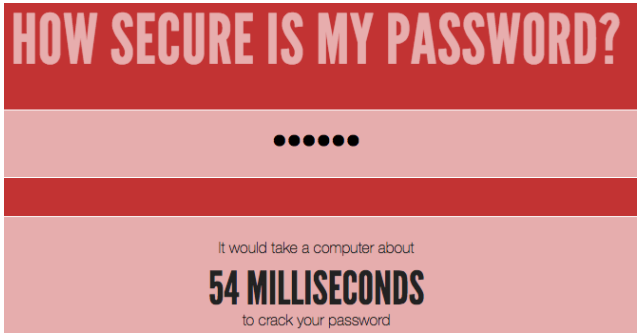
KEY VOCABULARY - PROTECTIONS	
Penetration Testing	Employing a *white hat hacker* to try to break into a system to test how good the security is. Any problems in the security can then be fixed before they become vulnerable to real attack
Network forensics	Network procedures that capture, record and analyse all network events to discover the source of security attacks
Network Policies	Rules which govern how a network may be used – see over page
Anti-malware software	Software which analyses files, network traffic and incoming data to look for known malware such as viruses or worms. An infected file is quarantined, and either cleaned or securely deleted to prevent further infection. Needs updating very regularly to ensure that the newest malware is being checked for
Firewall	A firewall protects a system by checking all incoming and outgoing network traffic is legitimate
User level access	Limiting the access of a user by their requirements to carry out their job. An admin will have more rights than a student, for example. Often even admins do not give themselves full rights to prevent accidents, and will instead have a *super-user* account that will be used only for special high level jobs.
encryption	Encoding all data with a secure private, asymmetric key system, so that if data is stolen, it cannot be read or used.

TYPES OF MALWARE	
Virus	A program designed to infect a computer, then copy itself. Requires human 'help' to spread; usually through infected software being installed or spread through unsecure removable media such as usb-drives
Worm	A self-replicating program, which can run itself allowing it to spread very quickly
Trojan Horse	A program which disguises itself as legitimate software, and appears to perform one task, but is actually performing another
Ransomware	Ransomware secretly encodes a users data and files, then offers to un-encode the files if a large amount of money is paid to the hacker
Rootkit	A rootkit allows a hacker to gain full, and often repeated, control of a computer, including the host operating system, which helps the hacker avoid detection

Computing GCSE – 1.6b

J276/01 – System Security – Network Policy

COMMON AREAS OF NETWORK POLICY	
Acceptable Use	Governs the general use of the computer system and equipment by employees. Usually limited to that which is required to carry out only the tasks that a user is employed to undertake
Passwords	Rules to ensure that passwords are strong enough to prevent guessing or brute force attack - often requiring the use of upper and lower case letters, numbers and special characters. Also usually a minimum length is required. Passwords usually have to be changed on a regular basis
Email	Governs what may and may not be sent by email
Web Access	The configuration of web browsers may limit the types and categories of website that can be accessed
Mobile Use	What devices are and are not allowed to be used
Remote Access	Govern what can be accessed from outside the system, and what can only be accessed onsite
Wireless	Govern how wireless access points (WAPs) are secured, who has access, and under what circumstances
Software	Governs who can install software, and which users are able to use that software. May have different levels of access once inside the software
Server	Rules about what services are provided by the institution and who may access data stored centrally and for what purposes
Back Up	Back up policy determines how frequently back ups are undertaken, and what type of back up (full, incremental, differential). It will also state where the back up media must be stored and for how long. Often a full weekly back up is required to be stored in a fire proof box in an offsite location
Incident Response Plan	Details what to do if something goes wrong, or if an attack is discovered.



HOW SECURE IS MY PASSWORD?

••••••

It would take a computer about

54 MILLISECONDS

to crack your password

Even modest desktop computers can undertake billions of cycles a second these days. Therefore, without any security features, such as limited password attempts, or asking for only selected characters from a password, a home PC could *brute force crack* commonly used passwords in very, very short periods of time!

PEOPLE ARE ALWAYS THE WEAKEST PART OF A COMPUTER SYSTEM!