Key information:

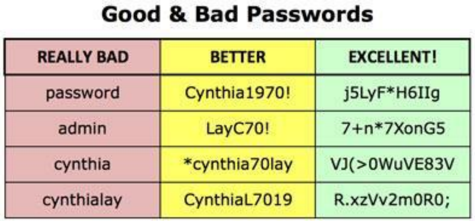
Card: 9.1

Security threats

- Hacking- unauthorised person accessing network resources to steal information or cause damage to systems
- Virus
- Interception- listening into a communication and viewing the data and/or tampering with it
- Physical theft
- Data theft from discarded components

Prevention methods

Access levels- giving permission to access/do certain things
Passwords- Good V's weak password combinations
Encryption- techniques to scramble a message so sender/receiver can understand messages



Good & Bad Passwords

REALLY BAD	BETTER	EXCELLENT!
password	Cynthia1970!	j5LyF*H6IIg
admin	LayC70!	7+n*7XonG5
cynthia	*cynthia70lay	VJ(>0WuVE83V
cynthialay	CynthiaL7019	R.xzVv2m0R0;

Data management

Backups of data- on site, off site, cloud
Archiving of data- process of storing data which is no longer in current or frequent use. It is held for security, legal or historical reasons.

Key information:

Card: 9.2

Compression

Reduces file sizes

1. Lossy compression results in reduction of data quality following compression.
2. Lossless compression results in no loss of data quality following compression.

$$Compression\ ratio = \frac{Original\ file\ size}{Compressed\ file\ size}$$

Internet cookies

A small piece of code that is given to a web browser from a server

It identifies a user and prepares customized web pages OR login information

They hold personal information which can be sold or used to track users

Key information:

Card: 9.3

Network security

Anti virus

Designed to detect and block attacks from malware by scanning all files

Firewall

Software that checks all network traffic entering or leaving specific ports and blocks programs accessing the internet

2 factor authentication

A method of confirming a users identify by using a combination of 2 factors

1- something they know

2- Something they have

3-Something they are

Other protection

Updating software that may be out of date

Using physical

Security tools like biometrics

Key information:

Card: 9.3

Cyber security threats

Short for malicious software, malware is a broad-spectrum term used to describe software used to disrupt computer operation.

Malware

Is similar to a virus but is a standalone program that replicates itself in order to spread to other computers. It does not need a vector.

Worm

A virus is a computer program that is able to copy itself onto other programs often with the intention of maliciously damaging data. A virus is transmitted by 'piggybacking' on another program known as a 'vector'.

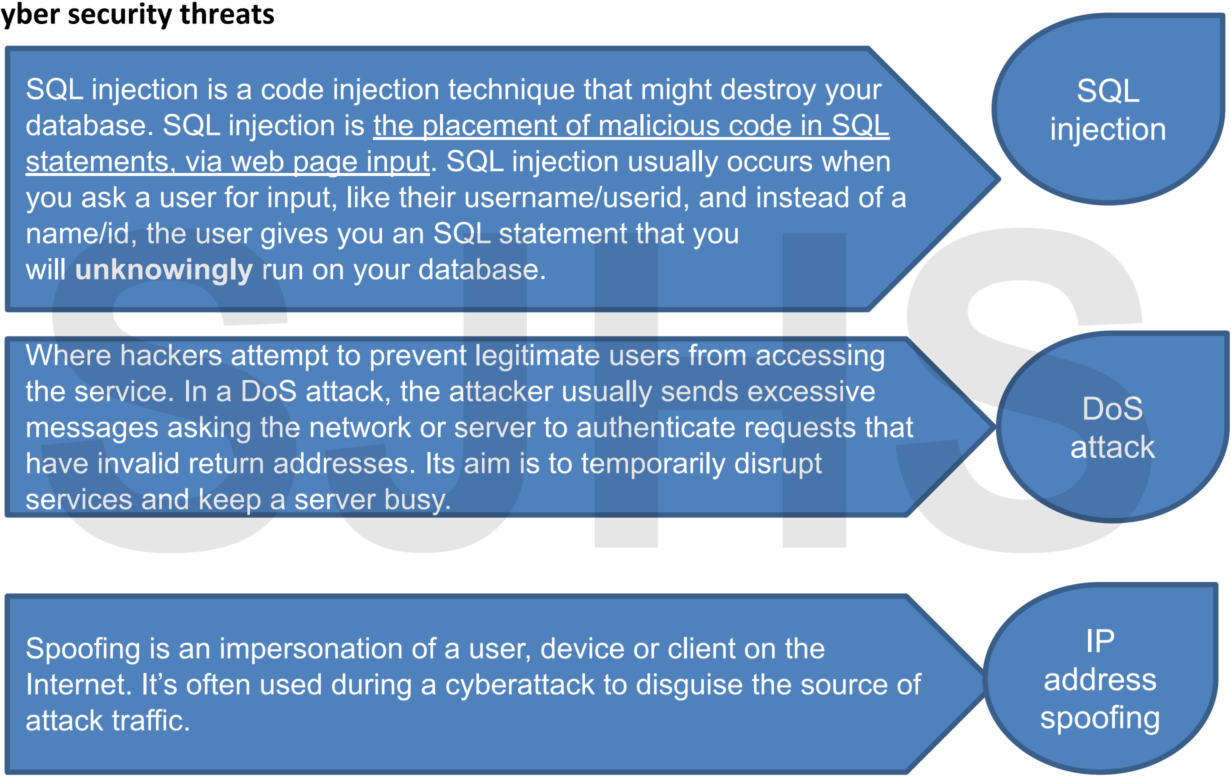
Virus

Are covert programs that capture keyboard (or other input device) input and transmit this data to a third party or hold the data for collection.

Keylogger

Key information:

Cyber security threats



SQL injection is a code injection technique that might destroy your database. SQL injection is the placement of malicious code in SQL statements, via web page input. SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

SQL injection

Where hackers attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. Its aim is to temporarily disrupt services and keep a server busy.

DoS attack

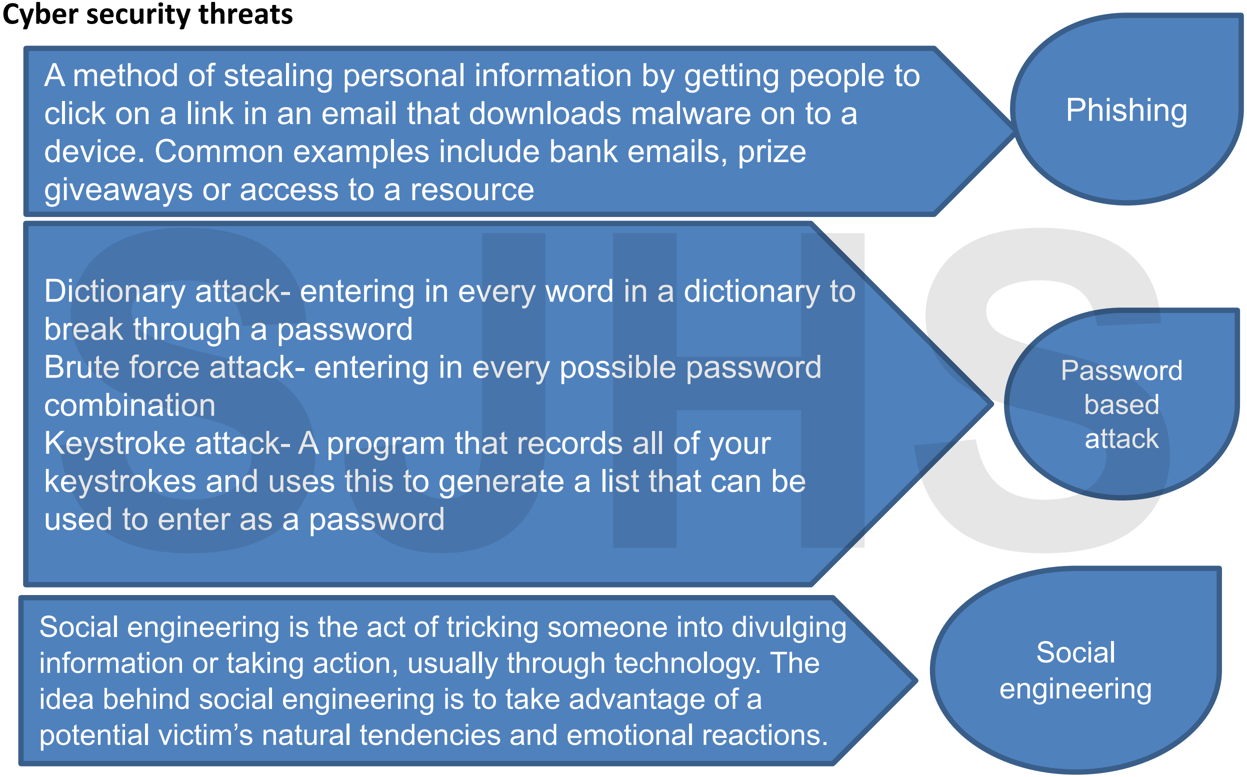
Spoofing is an impersonation of a user, device or client on the Internet. It's often used during a cyberattack to disguise the source of attack traffic.

IP address spoofing

https://www.w3schools.com/sql/sql_injection.asp

Key information:

Cyber security threats



A method of stealing personal information by getting people to click on a link in an email that downloads malware on to a device. Common examples include bank emails, prize giveaways or access to a resource

Phishing

Dictionary attack- entering in every word in a dictionary to break through a password

Brute force attack- entering in every possible password combination

Keystroke attack- A program that records all of your keystrokes and uses this to generate a list that can be used to enter as a password

Password based attack

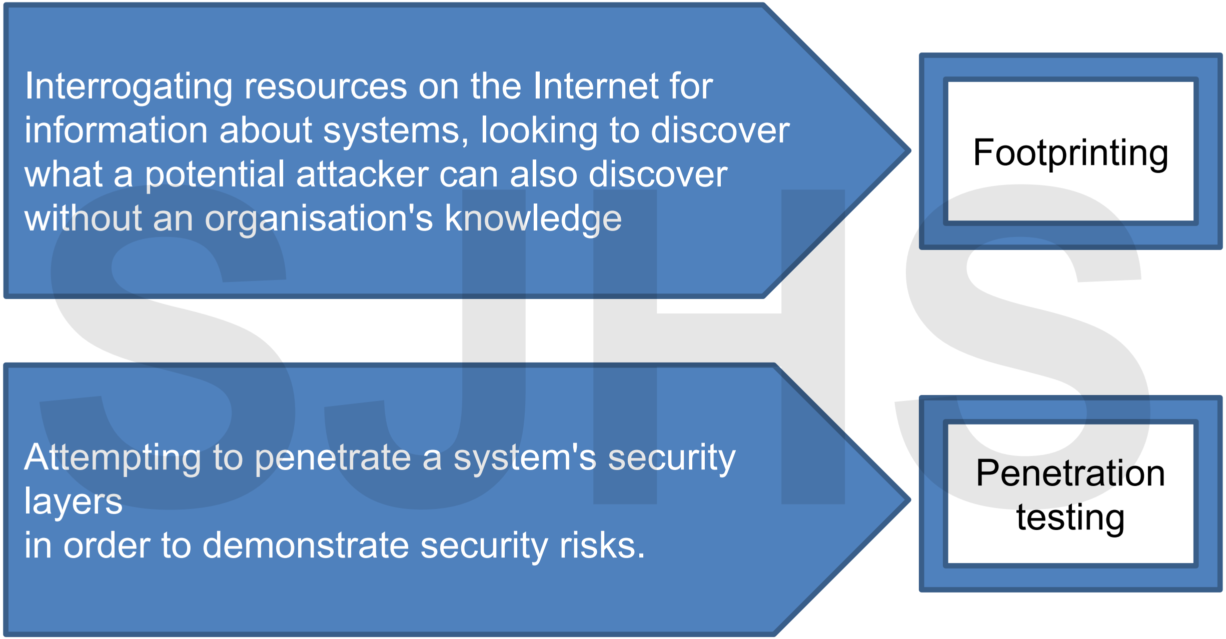
Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim’s natural tendencies and emotional reactions.

Social engineering

Key information:

Card: 9.4

Ways to identify vulnerabilities



Interrogating resources on the Internet for information about systems, looking to discover what a potential attacker can also discover without an organisation's knowledge

Footprinting

Attempting to penetrate a system's security layers
in order to demonstrate security risks.

Penetration testing

Key information:

Card: 9.5

Internet cookies

A cookie is the term given to describe a small piece of code that is given to a Web browser by a Web server.

The main purpose of a cookie is to identify users and prepare customized Web pages or to save site login information.

Cookies can be seen as a security issue as they hold personal information and this can be used or sold and tracking cookies can hold information on the websites visited by users.

Key information:

Protecting software during design, creation and testing

Ways to protect software when it is being designed, created or tested include:

Buffer overflows
Too many permissions
Scripting restrictions
Accepting parameter without validation