technoteach

technocamps

Llywodraeth Cymru
Welsh Government

Prifysgol Abertawe
Swansea University

Cardiff University
Prifysgol Caerdydd

Prifysgol Bangor University

Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd

University of South Wales
Prifysgol De Cymru

Medr
Y Comisiwn Addysg Drydyddol ac Ymchwil
Commission for Tertiary Education and Research

institute of CODING in wales
technocamps

Prifysgol Aberystwyth University

Prifysgol Wrecsam
Wrexham University

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

technoteach
technocamps

Cybersecurity

Why do we need cybersecurity?

Cybersecurity

The methods and measures taken to safeguard:

- Computer Systems
- Networks
- Data

Ensures data is secure and free from loss and corruption

This is very important for individuals, but essential for businesses to meet their legal requirements (and maintain a good reputation)

What is the best way to keep your data safe?

Cyberattacks

Cyberattacks

Cyberattacks come in many forms:

- **Malware** – malicious software
- **Social Engineering** – manipulating people
- **Brute Force Attacks** – hacking through trial and error
- **Denial of Service Attacks** – rendering a system unusable
- **Data Interception** – capturing data during transmission
- **SQL Injection** – injecting SQL commands to alter SQL statements and compromise the security of SQL databases

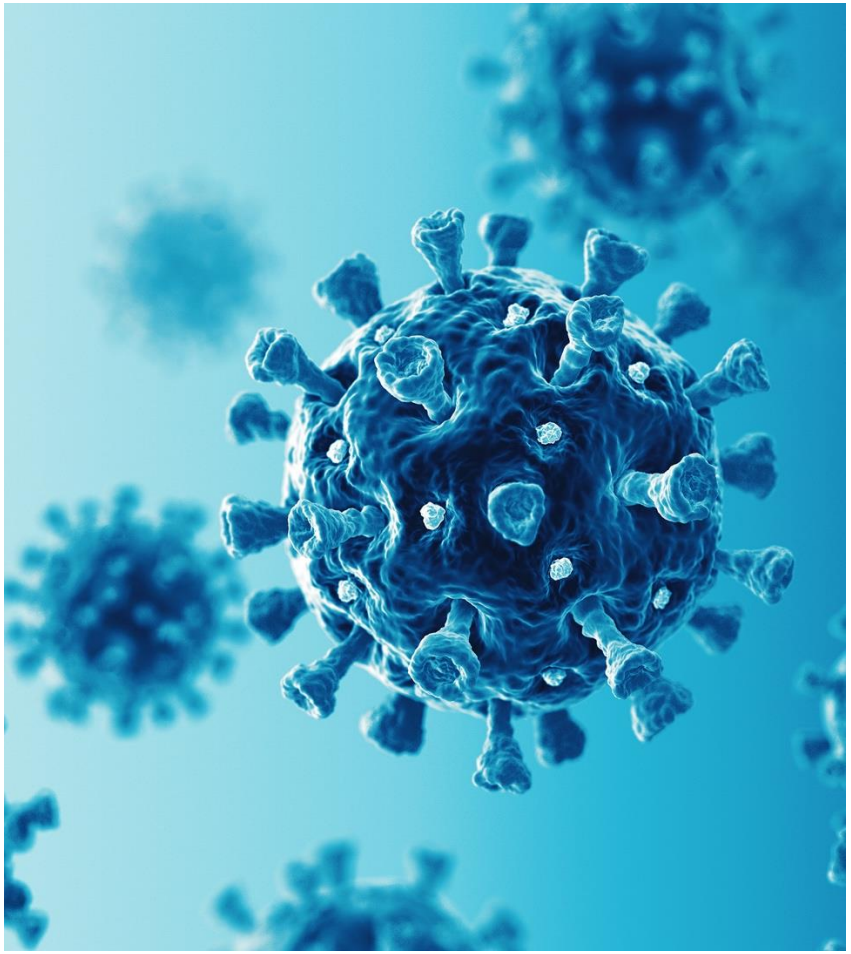
Let's take a closer look

Malware - Viruses

A computer program that copies itself onto other programs to damage data

Needs to "piggyback" on another program to get into the system

We call this host program a **vector**



Malware - Worms

A standalone program that replicates itself to spread to other computers

Similar to a virus, but do not require a vector

Searches for system vulnerabilities and then multiplies itself to attack

May corrupt or delete data, or enable backdoor access

Malware - Trojan Horse

Software that presents itself as harmless but contains harmful code

Tricks users into activating it and allowing unauthorised access

May steal data, or provide a backdoor for system access

May be able to go undetected

Malware - Ransomware

Holds a user's data hostage

Restricts access to data, programs or systems unless a ransom is paid

May encrypt, lock or otherwise block data

Malware - Spyware

Monitors a user's activities, collecting information without the user's consent

Can be installed by opening email attachments or installing infected software

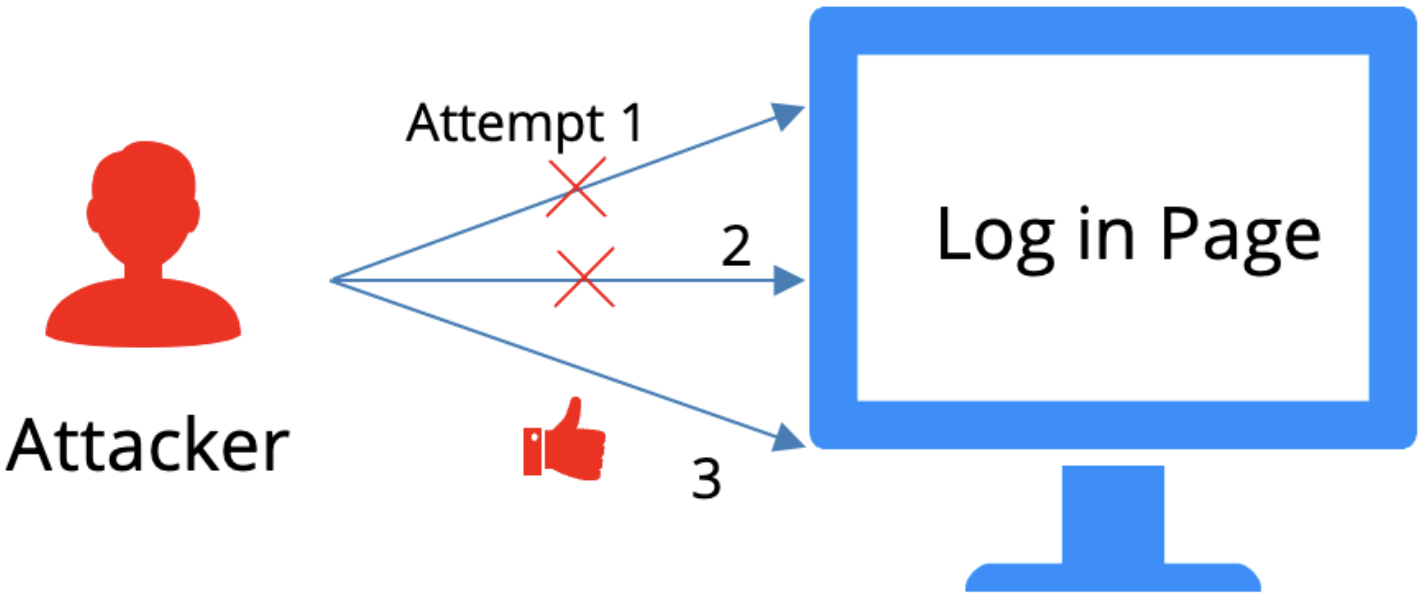
May track browsing habits, messages, keystrokes, etc

Keyloggers capture passwords, pins and account numbers

Social Engineering

Attack	Description
Phishing	Attempts to gather information through text, email or phone call by pretending to be a legitimate company
Pretexting	Setting up the context of a fictional scenario to make someone more likely to believe a phishing attempt
Baiting	Luring someone into giving their information, or installing malware by offering an incentive
Quid Pro Quo	Tricking someone into giving their information by making them feel like they are being helpful
Impersonation	Pretending to be someone trustworthy to trick someone into giving their private information

Brute Force Attacks

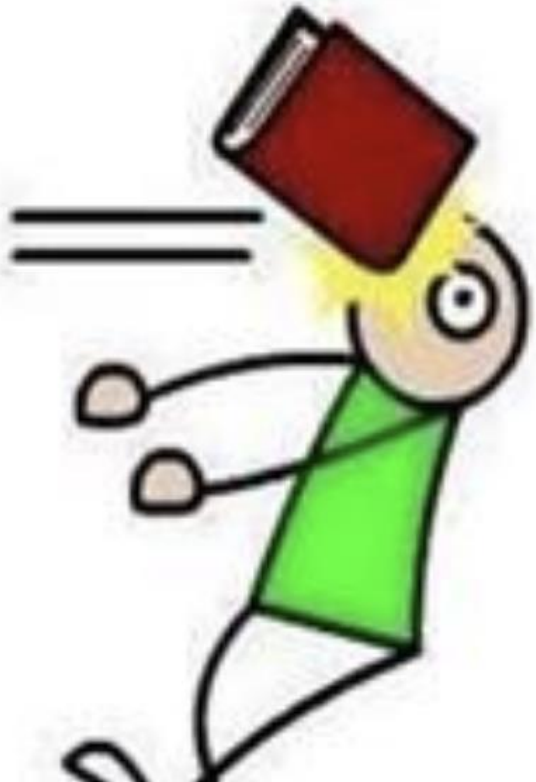


Brute Force Attacks

Attack	Description
Dictionary Attack	Working out passwords and/or encryption keys by using dictionaries of common words
Hybrid Brute Force	A mixture of traditional brute forcing and dictionary attacks
Reverse Brute Force	Commonly used passwords are used against username and login details to gain access
Credential Stuffing	Using stolen username and password details to access accounts with the same credentials

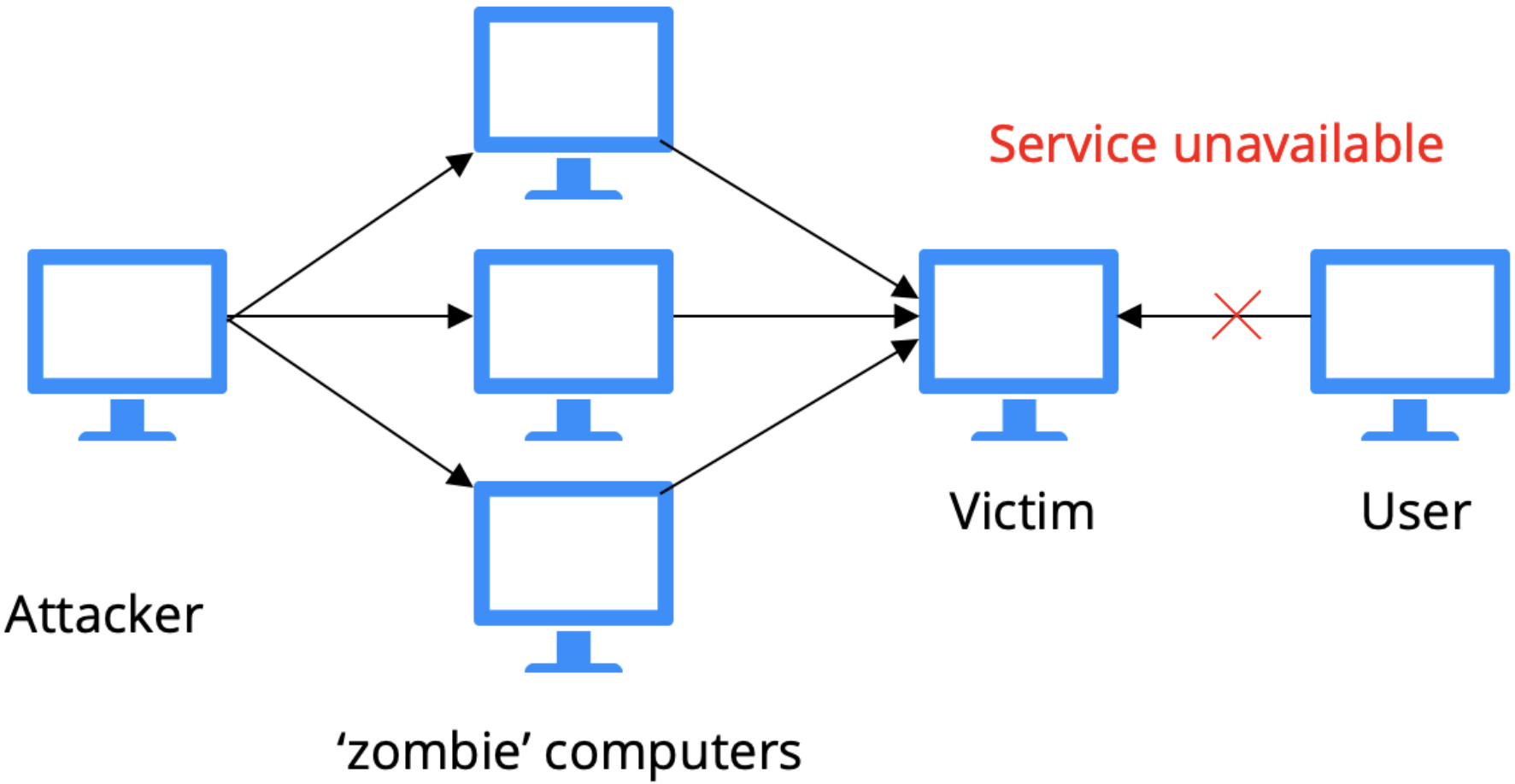
Brute Force Attacks

Attack	Description
Dictionary Attack	Working out passwords and/or encryption keys by using dictionaries of common words



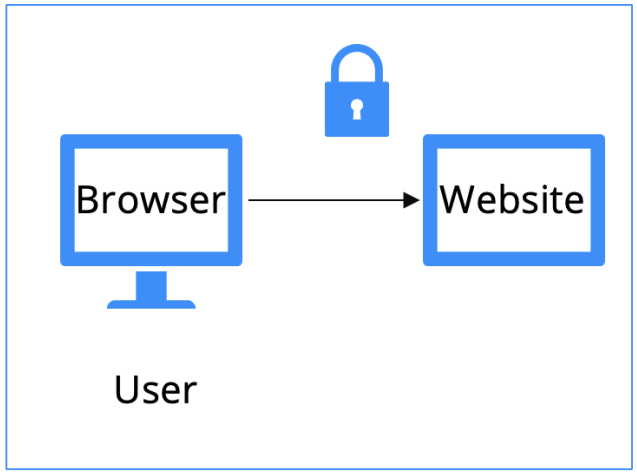
Denial of Service Attacks

Attack	Description
Distributed Denial-of-Service	Sends frequent, simultaneous requests from multiple systems to the same server
Volume-Based Attacks	Sends a large volume of data to exhaust the bandwidth and render the system unusable
Protocol Attacks	Finds vulnerabilities in communication protocols. Aims to overwhelm specific system resources such as firewalls to break the server
Application-Layer Attacks	Attacks the application layer of communication, stopping the webserver from communicating with users

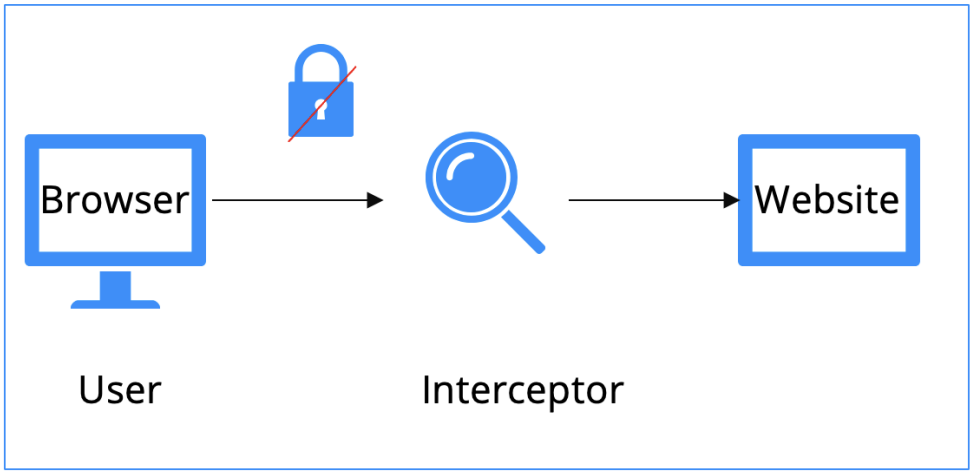

Service unavailable
Victim
User
Attacker
'zombie' computers

DDoS Attack

Data Interception & Theft



Regular connection



Data interception

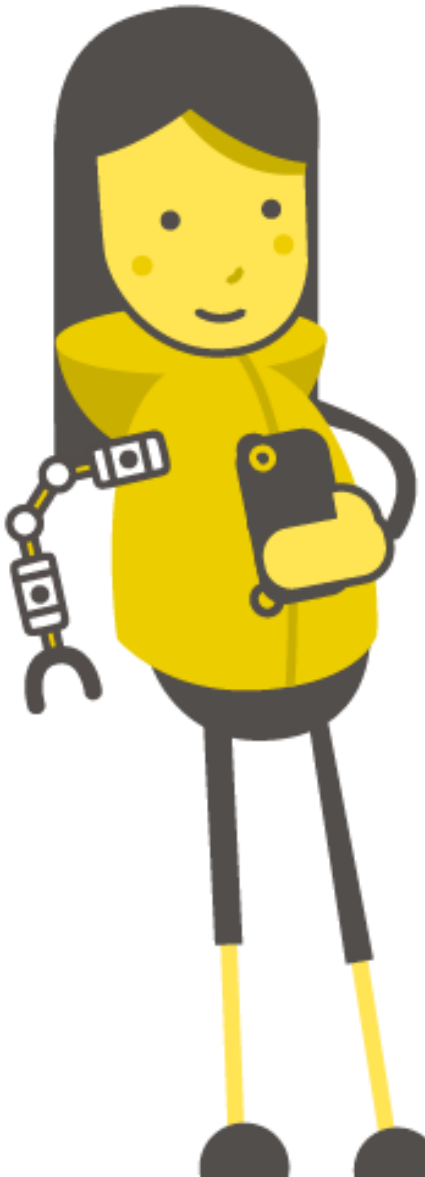
Data Interception & Theft

Attack	Description
Man-in-The-Middle (MiTM) Attacks	Finds weaknesses in communications between a server and a user, intercepts data being sent
Packet Sniffing	Intercepting and analysing weakly encrypted communication packets sent within a network – sniffing may be active or passive
Keylogging	Monitors keystrokes to track sensitive data
Session Hijacking	Sniffs for sessions between a user and server, then gains access to the session ID or cookies. The attacker uses these to act as the user
IP Spoofing	The attacker changes their IP to appear as a legitimate host, visitors who connect to the URL of a legitimate website can then be shown a fraudulent web page designed to steal data

SQL Injection

Attack	Description
Error-based	Produces errors that reveal information about the database, such as table or column names
Union-based	Uses "UNION" SQL operator to combine and retrieve results of multiple database tables – requires the attacker to know the column names, numbers and datatypes
Blind Boolean-based	Extracts information on the database, making Boolean queries with true/false responses
Blind Time-based	Causes website slow down, or delays responses. By observing the delays an attacker can intuit information a server would never directly show

Laws & Regulations



Why must developers have a good knowledge of cybersecurity?

Laws & Regulations

There is a moral duty to keep the users of our software safe, but there is also a legal one.

We must understand the following laws and regulations:

- UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA 2018)
- Computer Misuse Act 1990
- Telecommunications (Security) Act 2021
- Investigatory Powers Act 2016 (IPA)
- Digital Economy Act 2017

General Data Protection Regulation

Initially enacted by the European Union, UK GDPR is an identical replacement implemented post leaving the EU

Regulates data controllers – any organisation that collects information about living people

Applies to data controllers based in the UK, and any data controller that collects data on people living in the UK

Sets out 7 principles relating to the lawful processing of personal data – personal data being any data that could be used to identify the subject

GDPR Principles

1. Data should be processed lawfully, fairly and transparently – data should not be processed unless there is a legal basis
2. The purpose of data gathering should be defined at the start, and processed data should only be used for that purpose
3. Data controllers should gather only the minimum required data to meet the stated purpose
4. Subjects have the right to correct inaccurate data, and controllers should have processes in place to ensure accuracy
5. Data can only be kept for a duration defined within the original requirements
6. Data should only be accessed and managed by those that need to. There should be a way to recover lost or altered data
7. Controllers are responsible for their data interactions

GDPR Principles

1. Data should be processed lawfully, fairly and transparently – data should not be processed unless there is a legal basis
2. The purpose of data gathering should be defined at the start, and processed data should only be used for that purpose
3. Data controllers should gather only the minimum required data to meet the stated purpose
4. Subjects have the right to correct inaccurate data, and controllers should have processes in place to ensure accuracy
5. Data can only be kept for a duration defined within the original requirements
6. **Data should only be accessed and managed by those that need to. There should be a way to recover lost or altered data**
7. Controllers should be accountable for their data interactions

Data Protection Act 2018

DPA 2018 protects personal data stored in computer systems. Organisations often collect personal data from users

It is the right of the individual to protect his/her data from unauthorised distribution

The data controller of an organisation is responsible for protecting the personal data of all users

Data Protection Act 2018

Under the provisions of the DPA 2018:

- Data must be obtained fairly and lawfully
- Data should only be used for the purpose specified to the data protection agency and should not be disclosed to other parties without the necessary permission
- Data should be relevant and not excessive
- Data should be accurate and up to date
- Data should be only kept for as long as necessary

Computer Misuse Act 1990

Under the provisions of the Computer Misuse Act 1990, it is illegal to make any unauthorised access to computer material:

- With the intent to commit further offences, such as blackmailing
- With the intent to modify computer material, such as distributing viruses.

Telecommunications (Security) Act 2021

Expands the Communications Act 2003

The Communications Act is far-reaching covering a lot of communication media – radio, telephones, television, newspapers etc

The Communications Act made it a crime to access an internet connection without permission, and to send or repeat offensive language on social media

The Telecommunications (Security) Act 2021 is more narrowly focused – requiring telecommunication network providers to identify, prepare and reduce the risk of security compromises

Investigatory Powers Act 2016

AKA the Snooper's Charter

Expands electronic surveillance powers of British intelligence & police:

- Requires CSP's to retain British internet user's "internet connection records" for one year
- Allows police, intelligence officers and any government department to view those records without a warrant
- Permits police and intelligence to hack devices and retrieve data

Investigatory Powers Act 2016

- Permits intelligence and law enforcement carry out targeted or bulk interception and bulk collection of communications
- Places a legal obligation on CSPs to assist with targeted interception of data, communications and hacking
- Provides local government some investigatory powers but not to internet records
- Creates a criminal offence for CSPs or their employees to reveal that data has been requested
- Creates a criminal offence for unlawfully accessing internet data

- Communications of MPs are exempt from interception… unless authorised by the Prime Minister

Digital Economy Act 2017

Focuses on policy issues relating to electronic communications infrastructure and services:

- Allows data sharing between government departments to enable Digital Government
- Requires commercial pornography websites to implement age-verification
- Requires ISPs to block all websites with adult content by default until customers opt out
- Users may request a minimum broadband speed of 10 mbps
- Requires ISPs to provide compensation to customers if service requirement are not met
- Raises the maximum penalty for internet copyright infringement to 10 years in prison

technoteach
technocamps

Protecting Against Threats

Design Stage

Ensuring security is a core focus from the beginning of the design process allows security feature to be integrated into the system itself, instead of tacked on later

- Firewalls
- User Permissions
- Multifactor Authentication MFA

Creation Stage

How do we keep the source code safe and free from tampering during development?

- Anti-malware
- Firewalls
- Encryption
- Endpoint Protections

Testing Stage

The tests we can undertake to ensure the finished software is secure

- Penetration Testing

Simulating real world cyber attacks to detect vulnerabilities. Used to identify security weaknesses, evaluate defence effectiveness and make suggestions for improvements

- Network Forensics

Analysing network traffic and logs to investigate suspicious activities, security breaches or anomalies. Includes: monitoring and capturing network data, tracing the source of the attack and ensure compliance with security protocols, such as encryption and secure communications

Use Stage

- Monitoring Systems
- Secure Supply Chains
- Security Audits
- Anti-Malware
- User Permissions
- Firewalls
- Passwords
- Backups
- Multifactor Authentication
- Incident Response Plan
- Software Updates
- Encryption