DDoS:

A Distributed Denial of Service (DDoS) Attack is where the attacker generates a large quantity of packages and requests to the server which as a result ends up overwhelming the system. In specifically DDoS uses multiple sources rather than just a singular one in a DoS attack. As a result of the overwhelming requests of the server it will most often slow down or come to a complete halt.

One recommendation is to use firewalls to determine what traffic can reach your server and therefore limit the number of users which the DDoS relies on. Another solution is to prevent the exploit is to use a Web Application Firewall (WAF) which deals with the prevention of SQL injections, or any other exploits that compromise the system that allow for a DDoS attack. Another final recommendation is to scale your resource so that it can handle large volumes of data at any given time as the DDoS attack relies on this to work.

https://aws.amazon.com/shield/ddos-attack-protection/

Water Holing:

This is an attack where the attacker has either guessed or observed a website than an employee of an organisation or sector uses and then has infected the employee with Malware. From there a user will download the virus without realising (known as a drive-by-attack) from the other website where the attacker will then gain remote access to the system of the organisation. From there they can easily access data and compromise the system further. This is often done on popular websites due to the high chance that the employee uses to gain access to the system though if monitored enough can be done on any website the employee uses.

The largest defence against this kind of attack is to deal with vulnerabilities and apply patches as soon as possible as it prevents the system from being compromised. Another solution recommended is to ensure someone is monitoring the network traffic for malicious traffic and to block it if it occurs. Another recommendation is to prevent the use of certain websites during office hours for the employee as it will reduce the likelihood of this attack occurring. Finally, a VPN is also suggested to hide the browsing history of the users to prevent the observation from the attacker which makes it far more difficult to do the first step.

<https://en.wikipedia.org/wiki/Watering_hole_attack>

<https://www.techadvisory.org/2019/07/tips-and-tricks-to-prevent-watering-hole-attacks/>

Phishing:

Phishing involves the attacker directly targeting a user into clicking a malicious link or downloading a file which contains malware. This can be done through emails, text messages, social media, or really anything that involves any sort of messaging. From there data is stolen about the user and often passwords, credit card information, and other pivotal information are taken. The whole point of Phishing involves the attacker masquerading as a genuine company, charity, or person to try and make the user believe them and trust them.

A method to prevent this attack from happening to the users is to ensure that as an organisation you prevent your email addressed from being “spoofed” which involves an attacker using the likeliness of your email in a new one that they own. Spoofing in itself has recommendations such as using the Domain Keys Identified Mail (DKIM) which allows you to sign emails using encryption to prove its from your domain. Another recommendation is to inform uses identify and report phishing emails which banks often do through stating that “we will never ask for your personal information” which assists in raising awareness to prevent users from clicking a spoofed email address.

<https://www.ncsc.gov.uk/guidance/phishing>

<https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>

Spear Phishing:

Spear Phishing is primarily based of Phishing but with more steps and detail. Rather than targeting a mass number of users through an email it targets specific users through a more personalised email with information relating to the user that increases its legitimacy. For example, an attacker might get the information of an employer and then sends an email to an employee acting like the employer. From there they might get the employee to download a malicious file or click link. At that point, the employee is then compromised and can be exploited further. Whale phishing is to do with targeting a specific user; often a particularly important one like a board member, CEO, etc.

One recommendation is to ensure that employees only know what they need to know and no other extra information as it will assist in preventing the attacker pretending to be someone they’re not since they don’t have information to go off. The other recommendations fall in the same category of regular Phishing, so ensuring that your employees are aware of what information you will request to prevent the attacker from masquerading successfully.

<https://www.ncsc.gov.uk/blog-post/phishing-spear-phishing-and-whaling-does-it-change-price-phish>

<https://www.imperva.com/learn/application-security/phishing-attack-scam/>

Ransomware:

Ransomware itself is where an infected computer system is unable to have access to any of its data, or any real use unless a ransom is paid to release it. The data from this can be locked, stolen, or just generally accessed by the attacker. Often crypto currency is requested as it does not have a paper trail leading back to the attacker. Something to keep note of is that if you do give in and pay there is no guarantee they’ll honour the agreement as they are a criminal group; furthermore, you are also funding a criminal group. Threats of releasing the data may also be stated to try and blackmail the user into paying the fee. The difference between this and malware is that this is a specific type of malware.

One of the easiest approaches to this is to make constant back-ups of the devices as it will mean if the system is compromised you can hard reset it and then use the back-up data without any issues. These back-ups can be either online cloud ones or physical data drives, but having multiple makes you less likely to lose the data for any unforeseen reason. Also make sure that these back-up devices area not permanently attached as if the system is compromised then it might also try and compromise the back-up too. You can also prevent the malware from distributing the ransomware by ensuring that you can only download accepted files, blocking malicious websites, or by using an enterprise level anti-virus software to ensure no malware is downloaded.

<https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

Malware:

Malware is software which during runtime of the software will cause a variety of harm to the device due to it being compromised. The harm caused can include it being unusable and locked (known as Ransomware), taking remote control of the device to access personal data/systems and using the hardware to mine crypto currency like BitCoin, or Ethereum. Malware is a general term for more specific types of Malware which include things like Ransomware, viruses, worms, spyware and trojans. Viruses often aim to corrupt files and lock people out of their machines. Worms start from one machine and move across the network to other machines to spread the virus. Spyware is used as a background process to monitor and steal data from the user including such sensitive information like passwords. Finally, there are trojans which disguise themselves as legitimate software for the user to download and run which then results in the device being compromised.

One of the solutions to preventing malware is to ensure there are back-up copies of the device stored both on the cloud and on a physical disk to allow for the highest chance of the data to be recovered. Another method is to install an anti-virus software which will detect such threats through a variety of algorithms and data. A firewall can also help to block access to computers from private networks which will help preventing a worm attack. Ensuring Software is regularly updated will also help as it ensured that it does not have any vulnerabilities to exploit. A final recommendation for the users is to not download any malicious files/software, click any suspicious links, and so on.

<https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

<https://www.metacompliance.com/blog/what-is-malware-and-how-to-prevent-against-it/>

Scanning:

Scanning involves the process of identifying all devices connected to a specific network and includes all types of devices like firewalls, switches, etc. It then keeps note of all these devices and collects further data about it like the operating system, software installed, etc. It then checks these devices for known vulnerabilities and if one is spotted will use it to compromise the system. An attempt to log into a variety of systems using default credentials is also made for an easy compromise. With all this information the attacker can go even further to manually identify vulnerabilities in a software to exploit on each device. The higher the number of devices on a network means a higher chance of a system being able to be exploited. This scan can be done internally which is inside the network, or externally through an open port in the network firewall. These scanners can be used to fix vulnerabilities as well to exploit them. Penetration testing on the other hand involves exploiting weaknesses in the network itself which can result in the unauthorized access of data.

Due to scanning being a system which identifies vulnerabilities the best way to deal with it being used maliciously is to use it yourself to find the vulnerabilities. From there you can patch the issues you have found yourself to prevent anyone doing the same, but with malicious intent.

https://www.esecurityplanet.com/network-security/vulnerability-scanning.html

SQL Injection:

The main basis for an SQL Injection is the idea of using malicious SQL Code to access back-end information that was not originally intended to be displayed to the user. The information can vary, but typically it would be anything you would store in an SQL database such as passwords, addressed, stored bank details, etc. One type of this method is the Blind SQLi where the attacker will send data request to the servers and request a response to try and figure out the structure. With this type of attack the attacker can determine if a result is true or false depending on the time it took to receive a response of some sort. The most common type of SQLi is ‘In-band’ which refers to the idea of causing actions that results in a return error for the database which can potentially provide more information about the structure.

One solution to mitigate this issues is to use a method called “sanitisation” which refers to the idea of writing code which identifies illegal inputs from the users as it’ll prevent them from identifying the structure of the system. Another solution is to use a Web Application Firewall which uses a variety of data to determine malicious SQL queries. The data used often contains common practices and SQL Injection commands to try and counter them. Another solution is to use the correct privileges when it comes to SQL Databases as giving a user any sort of administrative power can result in a quick compromise of the database. A final recommendation – as with most of the cyber security attacks – is to update and patch software often as it’ll fix potential vulnerabilities that might have cropped up recently.

<https://www.imperva.com/learn/application-security/sql-injection-sqli/>

<https://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm>

Botnet

A botnet is where several devices which are internet connected which are running one or many bots on the device. They are often used to invoke a Distributed Denial of Service (DDoS) attack. They can also be used to send spam messages in a Phishing attempt to steal data from a variety of users. All these bots on a variety of devices can be accessed by an owner using a “command and control” software rather than having to individually access one. The devices used can either be owned by the attacker, or instead by another unsuspecting user if it has already been compromised. These computers are known as a “Zombie Computer” and are used unknowingly by the user to carry out the botnet tasks.

One solution to the problem is to deny access to the C&C network as if the attacker cannot access the bots then they can no longer do anymore harm, or compromise anything; however, this is not as effective when dealing with a C&C network on a P2P network, so other methods must be utilised. There are also pieces of software that can be used to detect Botnets which analyse network traffic through patterns and malicious behaviour. Another method being utilised is to use a honeypot software which convinces malware that a system is vulnerable which can then be used to research further with the malware stored.

<https://en.wikipedia.org/wiki/Botnet>

Subvert Supply Chain

A supply chain attack is a type of attack that attempts to compromise an organisation by attacking more vulnerable elements to a network. For example, they can compromise a supplier of a manufacturer which allows the attacker to then compromise the manufacturer (this moves them up the supply chain). This often occurs in an industry of some sort as it involves installing a rootkit, or some spying components for hardware. Often this rootkit disguises itself as legitimate software and is installed through a vulnerability of some sort where it keeps it control of the system without being known. With this access they can do a variety of damages, or observations through malware and subsidiaries like spyware to collect data.

One of the recommendations made to business is to restrict the access of network from anyone above or below the chain as this makes it far harder for an attacker to get in since if they compromise one system on the chain then they must try again for your part of the chain. A method to dealing with a rootkit is to use security software which typically are included in an anti-virus to determine if there is one and then to remove it if so. A more powerful solution is to hard reset the OS and even hardware once compromised. A method to defend against it is to update often to ensure vulnerabilities across the board are patched and less likely to be compromised.

https://en.wikipedia.org/wiki/Supply\_chain\_attack