**Types of Attacks on Information Systems**

1. Denial of Service (DoS) Attack:

This type of attack floods the network with traffic, making it impossible for legitimate users to access the network.

There are several ways to mitigate DoS attacks. One way is to use a content delivery network (CDN) that can distribute traffic across multiple servers, making it harder for attackers to overwhelm a single server. Another way is to use firewalls and intrusion detection systems (IDS) that can detect and block malicious traffic. Additionally, implementing rate limiting and throttling techniques can help prevent excessive traffic from overwhelming a server. Notably, turning off the servers and hosts during such an attack can reduce the risks of data theft and destruction.  
  
2. Man-in-the-Middle (MitM) Attack:

In this type of attack, an attacker intercepts communication between two parties and can eavesdrop or modify the communication.

One of the most effective ways to prevent MitM attacks is to use encryption protocols such as SSL/TLS, which encrypts the data being transmitted between two parties. Another way to mitigate MitM attacks is to use digital certificates and public key infrastructure (PKI). Digital certificates are used to verify the identity of a website or server, ensuring that the user is communicating with the intended party.  
  
3. Phishing Attack:

This type of attack involves tricking users into providing sensitive information such as passwords or credit card numbers by posing as a trustworthy entity.

Phishing attacks can be mitigated through a combination of technical and non-technical measures. Some technical measures include implementing email filters to block suspicious emails and using multi-factor authentication to prevent unauthorized access. Non-technical measures include educating employees on how to identify and report phishing attempts, creating strong password policies, and conducting regular security awareness training.  
  
4. Malware Attack:

Malware is malicious software that can infect a network and cause damage or steal sensitive information.

Another effective way to mitigate malware attacks is to use antivirus and anti-malware software. These programs can detect and remove malicious software before it can do any damage. Additionally, it's important to be cautious when downloading files or clicking on links from unknown sources, as these can often be a source of malware.  
  
5. Password Attack:

This type of attack involves attempting to guess or crack passwords to gain unauthorized access to a network.

There are several ways to mitigate password attacks. One of the most effective methods is to use strong and complex passwords that are difficult for hackers to guess. It is also important to avoid using the same password for multiple accounts, as this can make it easier for attackers to gain access to multiple systems. Additionally, implementing two-factor authentication and regularly changing password can add an extra layer of security, making it more difficult for hackers to gain unauthorized access.  
  
6. SQL Injection Attack:

In this type of attack, an attacker injects malicious code into a database query in order to gain unauthorized access to data.

SQL injection attacks can be mitigated by using parameterized queries or prepared statements. This involves separating the SQL code from the user input and using placeholders for the input values. This way, even if an attacker tries to inject malicious code into the input, it will be treated as a value and not executed as SQL code. Additionally, it is important to sanitize user input by validating and filtering it before using it in SQL queries.

7. Key Logger Attack:

A key logger is a type of software or hardware device that records every keystroke made on a computer or mobile device. It can be used for legitimate purposes, such as monitoring employee activity or parental control, but it can also be used maliciously to steal sensitive information like passwords, credit card numbers, and other personal data.

It is recommended to use anti-virus software and firewalls to protect your computer from malicious software that may contain key loggers. Also, using strong passwords and two-factor authentication can also help prevent key logger attacks by making it more difficult for attackers to gain access to your accounts.