**Cybersecurity Attacks Documentation**

1. **Phishing Attacks**
   1. **How It Works:**

Phishing attacks involve social engineering by impersonating legitimate entities like banks, email providers, or ecommerce platforms that make victims hand over sensitive information such as a username, password, or even financial information. In most cases, phishing attacks come in the form of emails or text messages with a fake legitimate website.

* 1. **Effects**
* Financial Loss: Victims end up losing money due to transactions carried out under fraudulent circumstances.
* Identity Theft: The thief can steal your Social Security number or credit card information.
* Reputation Damage: In case of a company, the customers will lose trust and damage the brand name.
  1. **Preventive Measures:**
* Educate Users: Educate them to recognize phishing emails and suspicious links.
* Use Multifactor Authentication (MFA): Require additional verification to access sensitive accounts.
* Antiphishing Tools: Employ filters and security software that scan emails for phishing attacks.
* Verify Sources: Confirm whether an email and a website are genuine before opening a link.

1. **DDoS (Distributed Denial of Service) Attack**
   1. **How It Works:**

DDoS attack overwhelms a targeted system, like a website or server, with excessive traffic, thus causing the website to be very slow or totally unavailable. This traffic is coming from a large number of compromised devices, known as a botnet, which can be hard to block.

* 1. **Effects**
* Service Disruption: In such an event, affected services or websites might become unavailable and result in downtime.
* Financial Loss: Businesses could lose revenue from downtime of their website or service.
* Brand Damage: The reputation of a company can be affected by multiple DDoS attacks.
  1. **Countermeasures:**
* AntiDDoS Services: Use cloudbased DDoS protection services that absorb traffic spikes.
* Bandwidth: Increase server capacity to accommodate larger volumes of traffic.
* Rate Limiting: Set limits on the number of requests a server can accept from a single IP address.
* Firewalls and Load Balancers: Firewalls and load balancers help distribute traffic and mitigate attacks.

1. **SQL Injection**
   1. **How It Works:**

SQL Injection is a type of code injection attack where malicious SQL queries are inserted into input fields, such as search bars, login forms, of a website or application. The injected SQL code is then executed by the database, potentially allowing attackers to view, modify, or delete data.

* 1. **Impacts:**
* Data Breach: Attackers may access sensitive data, including usernames, passwords, and personal information.
* Data Loss or Corruption: The attacker may delete or corrupt data in the database.
* System Compromise: In some cases, the entire system can be compromised by the attacker.
  1. **Preventive Measures**
* Use Parameterized Queries: Always use prepared statements to prevent SQL injection.
* Validate Input: Sanitize and validate user inputs to avoid malicious data entry.
* Limit Database Permissions: Ensure that database accounts have the least privilege and only access necessary data.
* Patch Software Regularly: Ensure that your DBMS and web applications have security patches.

1. **Malware (Malicious Software)**
   1. **How It Works:**

Malware is any kind of software designed to harm or exploit devices or networks. This includes viruses, worms, trojans, ransomware, and spyware. Malware often spreads through infected downloads, email attachments, or malicious websites.

* 1. **Impacts:**
* Data Theft: Malware can steal sensitive data. This includes passwords, financial information, and personal details.
* Device Damage: Malware may corrupt or delete files, leading to system crashes.
* Financial Loss: Specifically ransomware asks for payments from the victims so that the victim will regain access to their data.
  1. **Preventive Measures:**
* Install Antivirus Software: Install trusted antivirus software to detect and remove malware.
* Update Software Regularly: Keep the operating systems, software, and applications updated to patch known vulnerabilities.
* Avoid Suspicious Links: Don't click on unknown links or open attachments from untrusted sources.
* Back Up Data: Regularly back up critical data to prevent loss due to malware attacks.

1. **ManintheMiddle (MitM) Attack**
   1. **How It Works:**

In the MitM attack, the communication of two parties is intercepted in many cases. One party doesn't even notice, and thus data eavesdropping, tampering with data, and stealing such things as logon credentials and credit card numbers may occur.

* 1. **Impacts:**
* Data will be either stolen or manipulated.
* Attackers can be fraudulent by taking all the data related to their finance.
* There is also loss of trust because both parties distrust the application due to such type of issue.
  1. **Preventive Measures:**
* Encryption: Use endtoend encryption, such as TLS/SSL, to encrypt communications.
* Verify Websites: Check if websites use HTTPS and verify the validity of SSL certificates.
* Avoid Public WiFi: Refrain from sending sensitive information over unsecured public networks.
* VPNs: A Virtual Private Network (VPN) can encrypt internet traffic and prevent eavesdropping.

1. **CrossSite Scripting (XSS)**
   1. **How It Works:**

In XSS attacks, the attacker injects malicious scripts into trusted websites or applications that are then executed in a user's browser. These scripts can steal session cookies, redirect users to malicious websites, or display fake content.

* 1. **Impacts:**
* Session Hijacking: Attackers can steal user session cookies to impersonate victims.
* Data Theft: Malicious scripts can steal sensitive user data entered on the website.
* Reputation Damage: In case users' personal information is stolen, it may damage the reputation of the organization.
  1. **Preventive Measures:**
* Sanitize User Input: Sanitize all user inputs to prevent malicious scripts.
* Use Content Security Policy (CSP): Use CSP to limit the types of content that can be executed in the browser.
* Escape Output: Encode outputs to prevent browser execution of injected code.
* Use HttpOnly and Secure Cookies: Make sure that cookies are flagged as HttpOnly and Secure so that they cannot be accessed through clientside scripts.

1. **Ransomware Attack**
   1. **How It Works:**

Ransomware is a type of malware that encrypts files or systems and demands payment (usually in cryptocurrency) for the decryption key. It often spreads through email attachments, malicious downloads, or exploiting system vulnerabilities.

* 1. **Impacts:**
* Loss of data: Critical files and data are lost.
* Financial loss: Paying the ransom is a loss, and there is no promise that the attacker will return the access.
* Reputation loss: An organization infected by ransomware may lose customer trust as well as come into legal hurdles.
  1. **Precautions**
* Backup important data: Such data must be saved regularly for loss prevention.
* Update Systems: Apply patches and updates to close vulnerabilities.
* Email Filtering: Use email filtering tools to block suspicious attachments.
* Train Employees: Educate users on recognizing suspicious emails and avoiding malwareladen downloads.
* **Conclusion :**

The results of a cyberattack could range from loss in finance to reputational damage. But knowing what it is and putting measures in place to prevent such attacks reduces the risk substantially. By employing best security practices such as frequent updates of software, input validation, encryption, and educating the users, the different types of cyber threats can be defended against.