# How to Respond to 10 Common Cyber Attacks

| Attack | Incident | Response |
|---|---|---|
| **Malware** | Malware typically infects an Endpoints by tricking users into clicking and/or installing a program that they shouldn't from the Internet and unknown sources. | • Isolate the infected system(s) and remove it (them) from the network to prevent the spread of malware.<br>• Scan the system(s) for malware and remove it.<br>• Restore data from backups, if necessary.<br>• Patch any vulnerabilities that may have been exploited. |
| **Ransomware** | A type of malware that encrypts files and requests for a ransom(money) from the victim to decrypt the files. | • Isolate the infected systems and remove them from the network to prevent the spread of the ransomware.<br>• Backup any important data to prevent the loss of data.<br>• Do not pay the ransom, as there is no guarantee that the attacker will provide the decryption key.<br>• Clean up the infected systems and restore them to their original state. |
| **Social Engineering** | Social engineering is the art of hacking the humans to obtain their confidential information.<br>The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick you into giving them your passwords or bank information or access your computer to secretly install malicious software that will give them access to your privacy. | • Educate users on how to identify social engineering attacks and how to avoid falling for them.<br>• Verify the source of any requests for sensitive information.<br>• Review logs to determine if any sensitive information was disclosed.<br>• Implement a plan to detect and respond to similar incidents in the future. |

| | | |
|---|---|---|
| **Phishing** | It occurs when an attacker masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.<br>The recipient is then tricked into clicking a malicious link or opening an attachment, which can lead to the installation of malware. | • Notify users to delete suspicious emails or links.<br>• Verify the source of the email or the link before clicking on it.<br>• Review logs to determine if any sensitive information was disclosed.<br>• Educate users on how to identify phishing emails and how to avoid falling for them. |
| **SQL Injection** | It occurs when the application accepts a malicious user input and then uses it as a part of SQL statement to query a backend database. | • Check the application logs to determine the extent of the attack.<br>• Block the IP address of the attacker.<br>• Clean up any malicious code that was injected into the system.<br>• Update the application to fix any vulnerabilities that may have been exploited. |
| **Cross-Site Scripting (XSS)** | Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript files to users.<br>When the malicious code executes inside the victim's browser, the attacker becomes able to fully compromise the user interaction with the application.<br>Once the malicious code is injected into the page, it can be used to steal user data, such as login credentials or personal information, redirect users to phishing sites, or even take over the user's account. | • Identify the source of the attack and remove any malicious scripts.<br>• Ensure that any affected data is cleaned up and sanitized.<br>• Update the application to fix any vulnerabilities that may have been exploited.<br>• Notify users who may have been impacted by the attack. |

| | | |
|---|---|---|
| **Man-in-the-Middle (MitM)** | A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. | • Notify users who may have been impacted by the attack.<br>• Verify the integrity of any sensitive information that may have been intercepted.<br>• Review logs to determine the extent of the attack.<br>• Take steps to prevent future MitM attacks, such as implementing SSL/TLS encryption or using a virtual private network (VPN). |
| **Drive-by Download** | A drive-by attack, also known as a drive-by download attack, refers to a cyberattack in which a malicious script causes a program to download and install itself on a user device, without explicit permission from the user. | • Remove any malicious code or payloads that may have been installed on the system.<br>• Review logs to determine the extent of the attack and any potential damage.<br>• Update the affected systems with the latest security patches and software updates. |
| **Denial of Service (DoS)**<br>**And**<br>**Distributed Denial of Service (DDoS)** | DoS and DDoS are both aim to disrupt the availability of a targeted system or network. The key difference between the two is in the scale and the method of the attack.<br>In the DoS attack, a single attack source is used to sends many requests to a server or network to overwhelm it.<br>DDoS is a more advanced attack where multiple compromised devices, often called a botnet, are used to flood a target with a massive number of requests simultaneously.<br>DDoS also overwhelms the target to make it inaccessible, but the attack source is much larger and distributed across multiple devices, making it much more difficult to defend against. | • Identify the source of the attack and block the IP address of the attacker.<br>• Implement rate limiting and traffic filtering to prevent the attack from continuing.<br>• Notify the hosting provider or Internet Service Provider (ISP) to act against the attacker.<br>• Review logs to determine the extent of the attack and any potential damage. |