# **Top 10 Most Common Types of Cyber Attacks**

The past couple of years has seen a massive surge in internet usage. We certainly cannot argue with the benefits of the internet, however, at the same time, there are several disadvantages that the world of the internet brings to our doorsteps. Among other issues that may arise from internet usage, business owners need to be wary of cyber-attacks the most.

A well-rooted cyber-attack can entirely crumble the infrastructure of any business and can have a devastating impact on business operations. For users to securely store data and use safe practices online, it is important to know about the most common types of cyber-attacks.

Here are the top 10 most common types of cyber-attacks that we face today.

## Malware Attacks

One of the most common types of attacks that businesses have to deal with is malware attacks. These attacks are caused when cybercriminals or hackers develop software that is harmful or dangerous to businesses. The software is then installed in the victim's system and is used to hack into databases, cause privacy breaches, and take over the company's finances.

Malware attacks can be of different types and varying intensities. Some of the most common types of malware attacks are virus attacks, ransomware attacks, spyware attacks, and Trojan horses. There are several ways through which you can protect your system from malware attacks. Some of the most effective ones are quite simple – regularly updating software is a smart way to combat viruses of this nature and keep your system clean.

## Eavesdropping Attack

An eavesdropping attack is exactly what it sounds like. Hackers eavesdrop on the system's traffic to get hold of sensitive information such as passwords. There are two kinds of eavesdropping that are used by hackers. Passive eavesdropping is the kind in which the hacker will detect useful data by acquiring data from the system's network.

Whereas, active eavesdropping is when the hacker disguises himself as a relevant person to gain hold of information. One of the best ways to prevent an eavesdropping attack is data encryption.

## Phishing Attacks

Another common attack that business owners have to face is a phishing attack. The concept of phishing attacks is similar to "fishing". Bait is put out in the form of a link in an email. Once the user opens the email, their computer is instantly taken over by the foreign attackers. Spear phishing is an advanced kind of phishing in which the attacker thoroughly studies his target and creates emails that either seems from a trusted source or are extremely relevant.

Therefore, the user ends up clicking on them which leads to the victim's system getting hacked. An effective way to stop a phishing attack is to teach your employees to be careful when they open the email. They should hover over emails to scan the URL before they click on it or open the email in a protected environment.

## SQL Injections

This type of attack is carried out on only those systems that use SQL databases. Typically speaking, an SQL database is coding with statements that are implemented to an HTML form via a webpage. In case of a successful SQL injection, the system is compromised as the commands are inserted inside the code and they can now modify the code to run different operations which may not be in the interest of the business.

The hacker gains complete control of the system as they can dictate it to do exactly what they wish. The results can be devastating! Strong codes and strengthening the permissions model of your database can protect your system from an SQL attack.

## Brute-force Attacks

In a Brute-force attack, hackers break into the system of the user by force. They enter different password combinations and gain access to the system. They do this by using the victim's hobbies, date of birth, job, or any other phrase or word that the user might have used in their passwords.

In order to prevent illegal [digital access](http://cardzgroup.com/)businesses can protect their systems through a lockout policy to protect accounts. An account lockout policy locks the account after a few incorrect attempts and it can only be accessed by the owner.

## Denial of Service (DoS) and Distributed Denial of Service Attacks (DDoS)

The purpose behind these two attacks is to flood the system with traffic to a point that it becomes unable to function. It doesn't end there – while the victim is still searching for a way to deal with the traffic, the attacker takes over other systems to gain access to the company’s financial accounts or confidential data.

Even if the attacker does not end up causing another attack, the reputational damage caused by an interruption in services is an embarrassment on its own. Integrating your system with a powerful DDoS monitoring tool can help keep this kind of attack at bay.

## Artificial Intelligence Attacks

The rising popularity of Artificial Intelligence (AI) in the world of digital marketing has also led to its use in illegal practices such as hacking. Yes, you heard that right! There is a type of cyber-attacks that is based on AI technology. The most alarming aspect of these kinds of attacks is that they are well-designed to exploit system vulnerabilities. The sophisticated machinery guarantees system access which makes them even more dangerous.

## Man-in-the-middle (MitM) Attack

These types of attacks take place when an attacker strategically places himself between the client and the server. The three types of MitM attacks that are most common are Session Hijacking, IP Spoofing, and Replay.

All these attacks have one thing in common, they intercept the connection between the client and server and hijack the connection by substituting the client's IP, making the user believe that he is communicating with a trusted source. Detecting MitM attacks can be extremely difficult. Therefore, it is best to take precautionary measures rather than having to deal with it later.

## Cryptojacking

It is common to carry out financial transactions in the form of cryptocurrencies. However, transactions through cryptocurrencies bring us to another type of cyber-attack known as cryptojacking in which cyber criminals access the user's system and mine cryptocurrencies.

## Cross-Site Scripting Attacks

Cross-site scripting attacks or XXS attacks work in a similar way as SQL attacks but they don't exactly extract data from the database. Instead, they infect those who visit the domain. These types of attacks can result in a privacy breach of your customer's information and cause damage to your business's reputation and customer loyalty.

## Key Takeaways

The internet is a wonderful place but it can be quite dangerous too. If you are extensively using the internet you need to familiarize yourself with how you can fall victim to different types of cyber-attacks. Only then you can protect yourself and your business from any external threats.