**10 Most Common Cyber Threats**

The usage of internet has become a widespread phenomenon in recent times. Though the benefits of internet are countless, it has also brought along many problems with itself. Among many other issues that arise with internet usage, the most common problem is constant cyber threats that individuals and businesses face.

A well-designed cyber-attack can crumble the entire infrastructure of a business. It can badly impact the business’s reputation and operations. These threats affect businesses and individuals alike and can ruin your entire computer systems. This is why it is very important for anyone who uses internet to have knowledge of common cyber threats and how to avoid them.

Here are ten most common cyber threats that are prevalent today.

1. **Malware**

Malware stands for “malicious software”. It is one of the most common attacks affecting users. A malware attack takes place when cyber attackers create a harmful software to infect its target systems. When the user visits a certain website, opens a malware infected file or clicks a link, the malware gets installed into their system. It can then be used for hacking into a database, causing a privacy breach or for gathering critical information of a business.

Malware can be of different types, of which the most common are viruses, ransomware, spyware, worms and Trojan horses. The key to protecting yourself against malware is to never download suspicious files and regularly install an anti-malware program into your system.

1. **Phishing Attacks**

Phishing attacks are the second most common type of cyber-attacks. Also known as a phishing scam, it works on the principle of putting bait for the user and infecting their system. A scammer sends a link, usually via email, and tricks the user into clicking the link. Once the user clicks on a phishing link, their system gets compromised. Spear phishing is a specific phishing scam where the user studies their victim before targeting them and sends them personalized messages which seem to be from relevant and trusted sources. It is for this reason that spear phishing attacks are usually very successful.

The best way to stay away from phishing attacks is to educate your employees about different phishing techniques and how to recognize them. They should know the best practices of staying vigilant before opening an email. Always hover over the link to check the URL before trying to open it.

1. **Eavesdropping Attack**

Eavesdropping attacks are exactly what they sound like. In an eavesdropping attack, the attacker spies on the system’s traffic to get access to sensitive information like passwords and credit card numbers. There are two types of eavesdropping attacks. In Passive eavesdropping, the hacker gets useful information by acquiring data from a system’s network. In active eavesdropping, a hacker disguises themself as a relevant person and extracts important information. Data encryption is one of the most important ways to protect yourself from an eavesdropping attack.

1. **SQL Injections**

SQL injections are carried out on systems that use SQL database. An SQL database is typically coding of statements implemented to HTML form through a webpage. An SQL injection works by inserting commands inside the code and modifying it to run various operations that may not necessarily be in the best interest of the business.

By getting complete control, the hacker can dictate the system to operate according to them. Hence, a successful SQL injection can result in devastating results for a business. To protect your system from SQL injection attacks, use strong codes and strengthen your database’s permission model.

1. **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**

These attacks aim to flood the network with irregular traffic to the extent that it stops providing any service. It does not end here, rather, when the victim is looking for a way to come out of the issue, the cyber attacker takes control of other systems to get access to confidential data or financial accounts of the company.

Even if gaining information access is not the attacker’s motive, a DoS attack can give a severe blow to an organization’s reputation and cause severe financial losses during the time its service goes down. To prevent this threat, it’s imperative to deploy an effective DDoS monitoring tool.

1. **Brute-Force Attack**

As the name suggests, in a brute-force attack, the cyber criminals access a user’s system by force. They do this by using different password combinations to gain a system’s access. Password combinations are derived by using victim’s date of birth, hobbies, job, workplace or any other words that they can possibly use as their password.

To prevent a brute-force attack, a lockout policy must be implemented by organizations. This means that after a number of unsuccessful user attempts, the system locks the account temporarily and only reopens after a certain time when accessed by the real owner.

1. **Artificial Intelligence Attack**

The increased usage of artificial intelligence technology in digital marketing also has a downside to it. This type of cyber attack uses sophisticated machinery to gain access into a system and exploit vulnerabilities in the system.

1. **Man-in-the-Middle (MitM) Attacks**

A Man-in-the-Middle attack takes place when an attacker quietly places themselves between a server and client. MitM attacks can take place in many ways, the most common of which are IP Spoofing, Hijacking and Replay. The hacker or the middle man intercepts the connection between two parties and communicates with them from both ends, making them believe that they are communicating with each other. While pretending to be a trusted source, hackers can extract confidential information from the other party or communicate misinformation.

1. **Cross-Site Scripting**

A cross-site scripting or XXS attack works similar to SQL injections but instead of extracting data from the database, they infect the person visiting the domain. The purpose of these attacks is to extract customer’s information such as bank or [credit card](http://www.cardzgroup.com/BankCards.html) details and cause damage to customer loyalty and business reputation in the long run.

1. **Cryptojacking**

Cryptocurrency is now an acceptable way of carrying out financial transactions for many. Cryptojacking, also known as malicious cryptomining, is an emerging threat in which a hacker uses a victim’s mobile device or computer’s resources to “mine” cryptocurrency without their knowledge or consent. Instead of using dedicated servers for mining they use other system’s resources to mine currency, resulting in slowing down of the victim’s device.

It’s not easy to find out if your device is under a cryptojacking attack or not. The best way to prevent it from happening is to block JavaScript in your browser when you don’t require its functionality. Likewise, you can use programs like Miner Block or No Coin to block any mining activity in common browsers.

**Conclusion**

In an online threat landscape that is progressively changing every day, it’s a full-time job to stay safe from latest menaces. It’s always a good choice for businesses to invest in a complete cybersecurity solution that can save them from potential attacks, protect against bigger financial losses and ensure that your computer resources are yours alone.