The 12 most common cyber attacks

Cyber attacks happen all day every day in many different and sophisticated ways. In this handy guide, we highlight the 12 most commonly used cyber attacks and hope it'll encourage you to think about the basics of cyber security and how you're protecting your data and computer systems.

Denial Of Service (DOS) attack

A hacker overwhelms a computer or a network with traffic to such an extent that it can't operate and continue. This can mean a flooded inbox or server making it inaccessible to the intended user and therefore causing a system disruption.

Man-in-the-Middle (MitM) attack

A hacker inserts themselves between two places such as a wifi network and a victim's machine. This can mean info is stolen or malicious software is installed to carry out a malware attack.

Phishing attack

A user is tricked into thinking an email is from a reputable source, when it's actually fraudulent communication. It can steal sensitive personal information such as credit card numbers and login details on the victim's machine.

Drive-by download attack

A hacker slips malicious code into apps, operating systems or web browsers that haven't been updated and therefore contain vulnerabilities. Don't keep apps that you hardly use or update as those ones are the risky ones.

Wifi Eavesdropping attack

When a user is connected to a public wifi network, hackers can intercept communication and steal usernames, passwords and other unencrypted confidential information sent. You can avoid this by using a VPN.

Formjacking attack

A hacker loads malicious code onto an e-commerce site and steals customers' credit card details from the checkout pages. Small to mid-sized retailers are the biggest targets though Ticketmaster and British Airways were also compromised this way.

Malware attack

A user activates malicious software (virus, spyware, ransomware) that has installed via a link or an email attachment click. It can block access to the network, steal information by transmitting it from the hard-drive and disrupt a victim's machine.

Password attack

A hacker tries to guess a password by repeatedly trying different passwords to gain entry. This doesn't work when a lockout policy protects the account and it locks after three incorrect password entries.

Zero day attack

A hacker hears about a network, app or system insecurity and exploits it before a patch or update has been issued. This is an opportunistic attack and can only be avoided if users have advanced cyber security in place.

SQL injection attack

A hacker embeds malicious code (structured query language) into a poorly designed application and is then able to gain access to resources or alter data.

Brute force attack

A hacker uses trial-and-error to guess a username or password, trying repeatedly with various combinations until eventually gaining access. This is an old attack method that's surprisingly effective and still popular with hackers.

Cross-site scripting (XSS) attack

A hacker injects malicious code into a trusted app or website. The code triggers when a victim visits the app or page. Most common in forums, message boards and web pages that allow comments. Can also be used to deface a website.

Why not try our Cyber Security product?

Free 30 day trial