cardonet
making IT happen

Cyber Security Jargon Buster

Cyber security is possible, but it's difficult to know what protection you need (or from what) without some understanding of the emerging terminology.

This "jargon buster" defines the words and phrases of the evolving cyber threat and will help you to make decisions for your business.

Anti-virus – software that scans a computer for signs of security risks.

Cybergedden - a state of emergency resulting from a large-scale sabotage of all computer networks.

DOS - a denial-of-service attack typically floods servers, systems or networks with traffic in order to overwhelm and incapacitate the victim's resources/website.

DNS - Domain Name System - the Internet's system for converting alphabetic names into numeric IP addresses.

Encryption - The transformation of data to hide its information content.

Firewall - Tool designed to prevent unauthorised access to a computer or network.

GDPR - The General Data Protection Regulation is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union. GDPR is enforceable from May 2018.

Hacker - Someone who violates computer security for malicious reasons, kudos or personal gain.

Hacking- an unauthorised intrusion into a computer or a network. The perpetrators (hackers) may alter the system or its security features for malicious reasons, kudos or personal gain.

Malvertising - The use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

Malware - software which is specifically designed to disrupt, damage or gain authorised access to a computer system.

Patch - a file designed to address a vulnerability within a computer network or software.

Phishing - the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information

Ransomware - a type of malicious software designed to block access to a computer system until a ransom, usually a sum of money - is provided.

Screen scraper - A virus or physical device that logs information sent to a visual display to capture private or personal information.

Spear-phishing - an email-spoofing attack that targets a specific organisation or individual, to elicit sensitive information. It's targeted rather than random.

Spyware - Malware that passes information about a computer user's activities to an external party.

Two-factor authentication - Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.

Virus – Malicious software that is loaded onto a computer and then run without the user's knowledge or permission.

Whaling - a type of phishing that targets high-profile individuals such as CEOs, politicians and celebrities.

Worm - Malware that replicates itself so it can spread and infiltrate other computers within a network.

Zero-day attack – an attack consisting of malware that is entirely new or as yet undiscovered by cybersecurity experts.