Security Jargon Buster

In a technical world, you need to know your botnets from your clouds. Below is a simple glossary for the need to know words.

Antivirus
Software designed to detect, stop and remove viruses and malicious software.

Advanced Multi Factor Authorisation (MFA)
Uses multiple forms of identification to access software and can deliver push notifications to your phone for fast and secure access.

Botnet
A network of infected devices used to commit coordinated cyber-attacks.

Breach
When data, computer systems or networks are accessed or affected without authorisation.

Bring your own device (BYOD)
Employees use their own personal devices for work purposes.

Certificate
A form of digital identity for a computer, user or organisation to allow the authentication and secure exchange of information.

Cloud
A shared pool and storage resource usually accessed over the Internet.

Credentials
User's information used to verify identity; typically a password, token or certificate.

Cyber attack
Malicious attempts to damage, disrupt or gain unauthorised access to systems, networks or devices via cyber means.

Cyber security
The protection of devices, services and networks from theft or damage.

Dictionary attack
An attack in which known dictionary words, phrases or common passwords are used as guesses.

Download attack
The unintentional installation of malicious software or virus onto a device without the user's knowledge.

Encryption
A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device or Endpoint
Collective term for smartphones, laptops and tablets that connect to an organisation's network.

Firewall
Hardware or software to protect a network from unauthorised access.

Hacker
Someone with computer skills who uses them to break into computers, systems and networks.

Malvertising
Using online advertising as a delivery method for malware.

Malware
Malicious software - a term that includes viruses, trojans, worms or content that could have an adverse impact on organisations.

Network
Two or more computers linked in order to share resources.

Patching
Keeps software up to date across all managed devices to avoid potential vulnerabilities.

Phishing
Untargeted, mass emails asking for sensitive information or linking to a fake website.

Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Remote Monitoring
Monitors desktops, laptops, servers and mobile devices across operating platforms remotely.

Router
A network device which sends data packets from one network to another.

Smishing
Phishing via SMS/text messages.

Spear-phishing
A targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Standardisation
Makes sure all users are working in the same way.

Self-service Password Management
Lets users reset and manage their passwords.

Two-factor authentication (2FA)
The use of two different components to login eg. a password and fingerprint.

Trusted Platform Module (TPM)
A specialised chip on an endpoint that stores RSA encryption keys specific to the host system for hardware authentication.