TERRIFYING TERMINOLOGY

Use the link in the chat to access this list of terms

Advanced End-Point Protection - Protects systems from file, fileless, script-based and zero-day threats by using machine-learning or behavioral analysis. Traditional, reactive endpoint security tools such as firewalls and anti-virus software generally depend upon known threat information to detect attacks.

Anti-virus - Also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Anti-virus software was originally developed to detect and remove computer viruses, hence the name. Anti-virus software is not comprehensive enough to protect business systems against today's threats.

Cloud - A technology that allows us to access our files or services through the internet from anywhere in the world. It is a collection of computers with large storage capabilities that remotely serve requests.

Cyber-Insurance – An insurance policy that provides coverage against the potentially devastating impact of cyber crime.

Cybersecurity - Cybersecurity or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Data Backup - In information technology, a backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. Backing up the business' data is the only real protection against data loss.

Data Breach - The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to see the information.

Disaster Recovery - Involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Encryption - The process of encoding data so that it can only be accessed with a key.

Follow Me Printing- A type of print queue that isn't tied to a single device. Print jobs can be sent to the print queue and then printed from any device that is connected to the print queue.

Hacker - An unauthorized user who attempts to or gains access to an information system.

Image Overwrite - A security option on MFP's that electronically "shreds" information stored on the hard drive of the device.

Malware - An umbrella term that describes all forms of malicious software designed to cause harm, disclose information, or violate the stability of a system. Common forms include viruses, worms, trojans, spyware and ransomware.

MSP (Managed Service Provider) - A third-party company that specializes in handling IT operations for organizations. Are responsible for the entirety or portions of the business' IT systems including managing the customer infrastructure and end-user systems, security and around-the-clock monitoring, issue resolution and reporting, and more.

Multifactor Authentication- an authentication method that requires a user to provide two or more forms of verification to access a resource.

Ransomware - A form of malware that encrypts files to deliberately prevent you from accessing those files on your computer – holding your data hostage. It is followed by a demand that a ransom be paid, typically in the form of Bitcoin (an untraceable digital current) in order to have the data decrypted or recovered.

Virus - A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.