Cybersecurity best practices

Encryption

The process of changing data so that it is unreadable or unusable without a key. Data can be encrypted in two ways, symmetric and asymmetric. Symmetric encryption uses the same key for both encrypting and decrypting data. Asymmetric encryption uses a public key that can be shared with anyone while keeping the private key private.

Two-factor authentication

A security measure that requires two different factors to verify your identity. It can be in the form of a code sent via text message or an app that generates codes.

Antivirus software

Protects a computer from any type of malicious software. It prevents malware from infecting the computer and running without the user's knowledge.

VPN (virtual private network)

A virtual private network creates a secure and encrypted connection to another computer or server through the internet in a way that protects your privacy and data from cybercriminals, corporations, and other third parties.

Backup data

A copy of your data that can be used to restore your original data if it gets lost, stolen, or corrupted.

Application whitelisting

The process of restricting software installation on a device or network by allowing only certain software packages from trusted sources. If there are vulnerabilities in these applications, they will not be able to be exploited by potential hackers.

Employee training

Helps employees better understand how to protect themselves and their information, while also preparing them for the inevitable cyberattack. Training courses are designed to teach employees how to identify suspicious emails, recognise signs of phishing scams, avoid malware and other cyber threats, and report any errors or suspicious activity that they may cause.