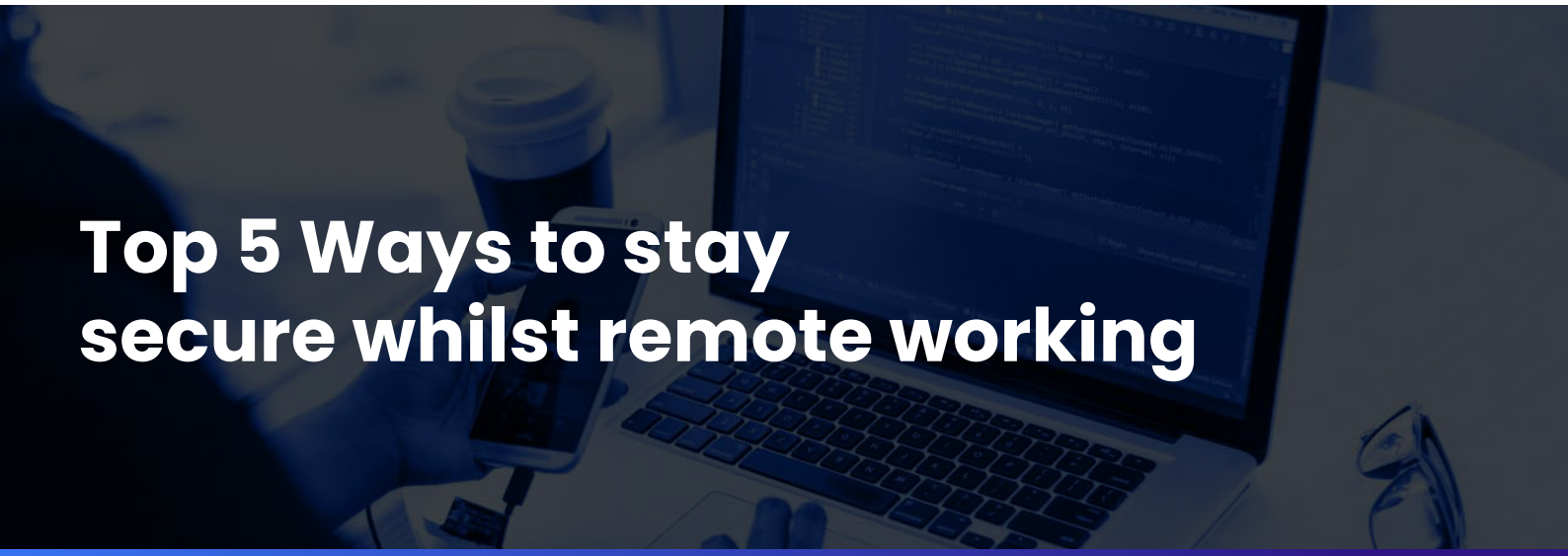
nybble

Call: 0330 0020886

Email: sales@nybble.co.uk



Top 5 Ways to stay secure whilst remote working

Nybble is your trusted partner for IT Services and Support

The current coronavirus outbreak has resulted in many more employees working from home, however this isn't a new phenomenon. Many organisations offer a flexible working policy, where staff can spend some of their working week from the comfort of their own homes. However, this luxury has its downsides, mainly in the form of online security threats.

Here are our Top 5 ways to stay secure whilst remote working...

Multifactor Authentification

Having a strong password often isn't enough, for example, if your credentials are leaked in a data breach. Multifactor authentication involves an additional step to add an extra layer of protection to your accounts. The extra step could be an email or text message confirmation, or even a biometric method such as facial recognition or a fingerprint scan.

VPN Encryption

Many people are familiar with using a Virtual Private Network (VPN) to bypass geographic restrictions on streaming sites and other location-specific content. VPN encryption is the process of securing the data within the VPN client-VPNserver tunnel to make sure it can't be exploited by anyone. Basically, when you run a VPN client and connect to a VPN server, your connection requests are encrypted before they are sent to the server.

Mobile Device Management

The average office worker will probably have more than one work device, i.e. a laptop and a smart phone, especially during a lockdown! These devices are deployed across multiple mobile service providers and across multiple mobile operating systems, so can be little difficult to manage. A mobile device management (MDM) solution can be used to monitor, manage and secure employees' mobile devices.

Anti Virus Software

Although having a firewall is important, it's inevitable that online threats can get through. A good antivirus software can act as the next line of defence by detecting and blocking known malware. Even if malware does manage to find its way onto your device, an antivirus may be able to detect and, in some cases, remove it.

Backup Your Data

Data can be lost in a number of ways including; human error, physical damage to hardware, or a cyberattack. While hardware backups are still an option, one of the most convenient and cost-effective ways to store your datais in the cloud. Cloud backup services come with a wealth of options enabling you to customise your backup schedule and storage options.