Microtrading
Your trusted IT partner

part of the Air IT group

A guide to cyber security when working remotely

Tips to keep your business and employees safe when you work from home

Cyber Security When Working Remotely

Despite the perceived benefits for employees, working from home is leading to an increase in cyber threats:

- Systems and networks are being used in ways for which they weren't designed
- Staff are detached from standard workplace protocols
- Fraudsters are taking advantage of Covid-19 through phishing scams and credential theft

The good news is there are steps you can take to protect your business and employees.

Microtrading
Your trusted IT partner
part of the Air IT group


Top
5
Cyber Security
Tips for Remote
Working

User Awareness

*46% of businesses experienced a cyber attack in the 12 months prior to a recent government survey

Using the same weak passwords across multiple accounts, clicking on suspicious links and falling for phishing emails are just some of the ways employees could inadvertently subject your business to cyberattacks.

Throughout the pandemic, over half of UK businesses have found impersonation attempts harder to detect and have been subject to more attempts of employee account hijacking.

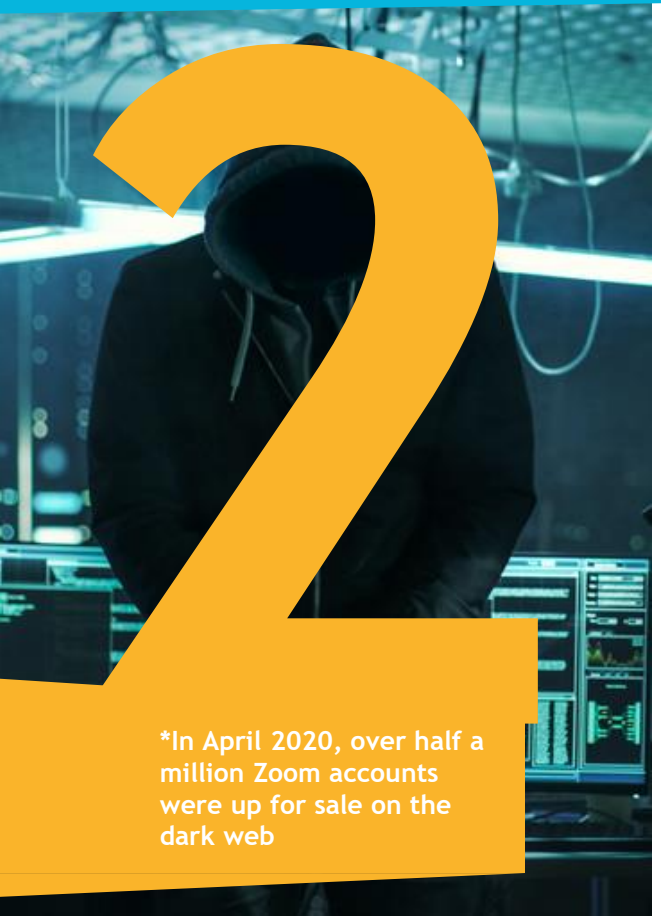
Investing in your employees by providing cyber security training will ensure that they are up to date on best practice and know how to spot suspicious activity.

**UK Government's Cyber Security Breaches Survey 2020*

Microtrading
Your trusted IT partner

part of the Air IT group

Dark Web Monitoring



*In April 2020, over half a million Zoom accounts were up for sale on the dark web

Credentials and other sensitive information stolen through phishing emails and third party data breaches are often trafficked and sold on the Dark Web, without you or your employees ever knowing about it.

This stolen information is usually used for financial benefit, whether it's buying goods with stolen credit card numbers or holding internet accounts for ransom.

Dark web scans provide real-time alerts of compromised credentials and actionable intelligence so we can help you remediate threats, keeping your organisation and staff better protected.

**https://www.independent.co.uk/life-style/gadgets-and-tech/news/zoom-app-accounts-sale-buy-dark-web-a9463661.html*

Microtrading
Your trusted IT partner
part of the Air IT group

Cloud Network Security

3

*The amount of businesses experiencing phishing attacks has increased from 72% to 86%

Working from home presents challenges in that employees are often required to use personal devices and networks, which weren't designed for professional use.

This, coupled with the fact that employees may let their guard down to phishing or malware scams whilst at home, means that they are more vulnerable to cyberattacks.

Investing in Cloud Network Security means that your users and their devices are protected, regardless of their location or the network they are using.

UK Government's Cyber Security Breaches Survey 2020

Microtrading
Your trusted IT partner
part of the Air IT group

Two-factor authentication

4

*99.9% of account compromise attacks can be blocked by 2-way or multi-factor authentication

Many people use the same password across several personal and work accounts, which makes it easier for hackers to gain access to important information regarding your business.

Setting up two-factor authentication means that employees will be notified and sent a unique code whenever login is attempted, adding an extra layer of security.

*https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Microtrading Your trusted IT partner | part of the Air IT group

Test, test, test!

5

*In a recent government survey, only 35% of businesses had carried out a cyber risk assessment

If you never test the systems and processes you have put in place, you may not find out that they are sub-par until it's too late. It's important to regularly audit your systems to ensure consistent protection from cyber threats.

As a trusted IT provider, Microtrading can carry out regular IT audits, penetration testing and phishing simulations to gauge the security of your systems and the alertness of your employees when it comes to falling for fraudsters.

**UK Government's Cyber Security Breaches Survey 2020*

Microtrading
Your trusted IT partner

part of the Air IT group

Don’t be the next victim

The team at Microtrading are committed to helping clients better protect their business and operate securely when working remotely during the pandemic and beyond.

With the increasing rise of cyber attacks threatening businesses every week, now is the time to **request your FREE risk assessment.**

To find out more about our remote working cyber security packages, please don’t hesitate to get in touch – we will be more than happy to help.

Microtrading
Your trusted IT partner

part of the Air IT group

Request your FREE risk assessment today

0121 784 0077 sales@microtrading.co.uk microtrading.co.uk