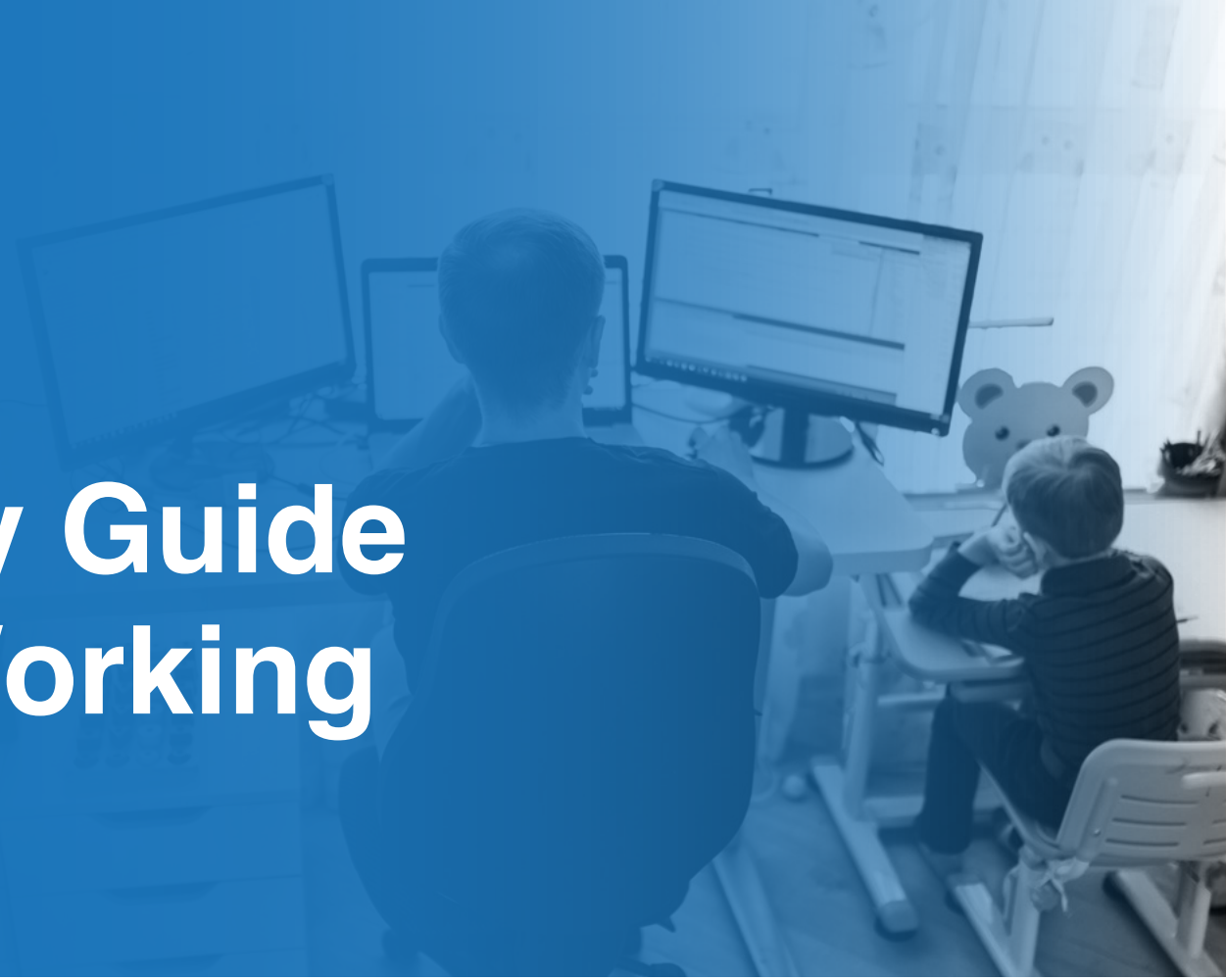
The Ultimate Cybersecurity Guide for Remote Working



Mainframe
Consulting Business & IT Solutions

nicholas@mainframeconsulting.co.uk

Working remotely has become a necessity for employees globally in 2020

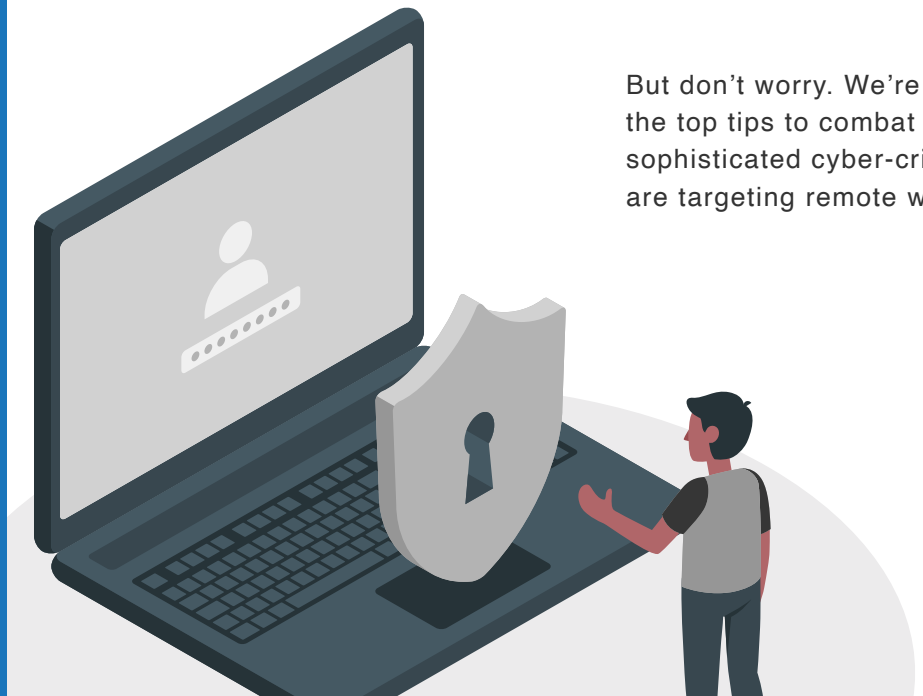
Working from home creates many benefits such as:

- Flexibility
- Maintained levels of productivity
- Employee retention

Some employees may never decide to stop regularly working from home. It's vital therefore to **equip your employees** with everything they need in order to work safely, wherever in the world they're based.

Alongside the rise of remote workers, we've seen an increase in cyber-attacks on businesses of all sizes due to security vulnerabilities being exposed.

- Insecure networks are being used to access company data
- Not everyone is able to remotely monitor and manage staff and their devices
- Hackers are attacking individuals directly through phishing attacks and COVID-19 specific scams



But don't worry. We're sharing the top tips to combat the new sophisticated cyber-crimes that are targeting remote workers.

Top 5 Cybersecurity Tips for Remote Working

88%

88% of remote workers are expected to continue working from home to some extent, even after the pandemic.

Acronis

1. Security Awareness Training

Did you know that the leading cause of a data breach is human error?

All it takes is one simple mistake from a member of your team. Simply clicking a link on a deceptive email is enough to grant cybercriminals access to your business network.

Your team is the first line of defence against cyber threats.

Investing in your employees by providing comprehensive Security Awareness Training will ensure that everyone across the board can spot a cyber-attack. When everyone knows what to look out for, suspicious activity will be highlighted quickly and can be dealt with efficiently.

31%

31% of companies report daily cyber attacks, and 50% report being targeted at least once a week.

Acronis

2. Safety in the Cloud

Have you ever been fooled by a phishing email?

People are generally on their guard less when working from home and are not as likely to spot cyber threats.

Most employees working remotely will access company data via their own personal device, or on a network that is less secure than what you might have in your physical office space. While it's incredibly useful to access data through the cloud remotely, it does lend itself to potential network security vulnerabilities.

Ensuring that your cloud security is airtight will mean that your company data, your users and their devices are safe no matter where they are.

89%

89% of MSPs report ransomware infecting endpoint systems.

datto

3. Real Dark Web Threats

Did you know that the Dark Web is estimated to be roughly 500 times larger than the common internet?

When a cybercriminal successfully steals confidential information such as credit card details or finance information, they will almost always go and sell it on the dark web. Many organisations could be forgiven for thinking that the dark web is some mysterious place that poses no real threat unless you go looking for it.

This is not the case. Stolen information from SMEs and large corporates alike can be sold on the dark web for a profit. Sadly, everyone is a potential target for cybercriminals.

Dark Web scans will highlight any of your company data that has already been compromised. This scan will provide you with the insight you need to remediate threats and mitigate risks.

60%

60% of the data for sale on the Dark Web is harmful to enterprises.

Kaseya

4. Access Management & Two-factor Athentication

Do you have the same password for everything? Most people do...

Your users will be logging in from their own devices on a regular basis when working remotely. Without rolling out strict access management processes, it can be near impossible to stay on top of access security issues.

Implementing two-factor or multi-factor authentication makes it much harder for hackers to succeed. Every time a user logs in, no matter where they are, they will receive a unique access code. This adds a necessary layer of security and control rather than relying on employees to use super secure passwords and devices.

99.9%

Using multi-factor authentication blocks 99.9% of automated attacks.

Microsoft

5. Assess, Report, Repeat.

You might have cybersecurity policies in place – but are they up to date?

Cyberthreats are constantly evolving, and so should your cybersecurity measures. It's essential to assess your current plans, test them and check that they are good enough to ensure comprehensive protection for your business.

Work with a Managed Service Provider (MSP) who will implement thorough audits, tests and updates to your cybersecurity systems.

The threat is real, it's best to be prepared.

28%

In 2019 only 28% of SMBs were 'very concerned' about ransomware despite 1 in 5 SMEs being victims.

datto

Don’t let cybercriminals turn your business into a victim

Equip your business with a robust cybersecurity procedure and ensure that you have help and advice from the experts.

Start protecting your business today.
Speak to a member of our team:

nicholas@mainframeconsulting.co.uk