The security problem **of John’s “other” laptop**

How to keep your business data ultra safe during the Work From Home revolution

net technical solutions

Love it or hate it, Working From Home is huge and here to stay.

As a nation, we've really embraced the changes forced upon us by the pandemic. Many businesses have become more flexible with a mixture of office-based workers, hybrid workers and fully remote workers.

We had no idea that we could change so much, so quickly, did we? Work just doesn't look the same as it did in 2019.

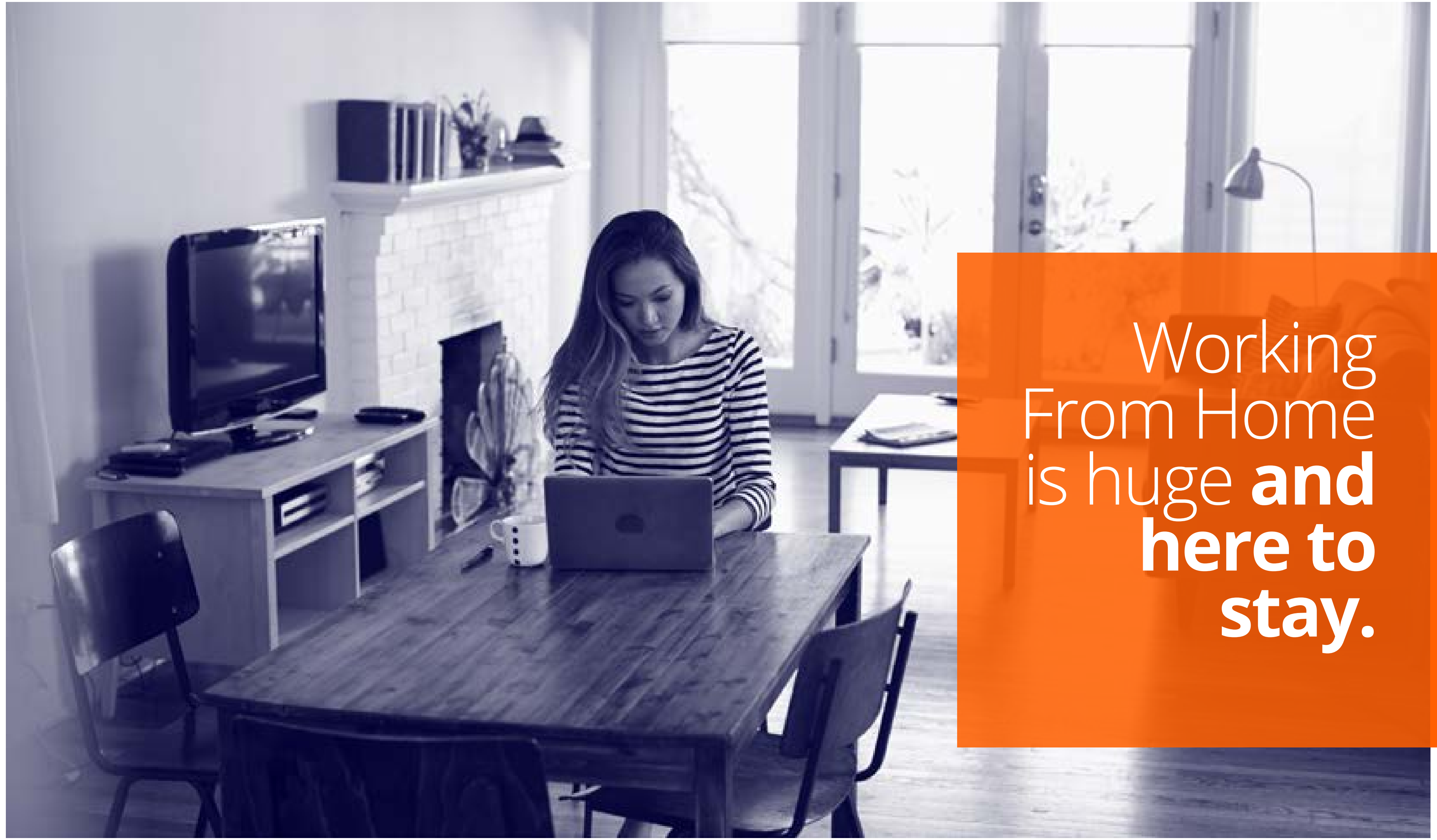
Because of that, cybersecurity in 2022 doesn't look the same either. When you have people working away from your office you need to take additional security measures to keep your data safe.

Even before we'd heard of the word "Coronavirus", many of us were working from home intermittently. Checking emails at the weekend. Finishing up a project in the evening. Getting a head start on your week.

Now Working From Home has to be taken more seriously. If any of your staff works anywhere away from the office, there's a chance that they're taking unnecessary risks with your data.

Many businesses seem to have this covered. They've invested in new company devices, increased remote security and have trained their people on best practice.

But there's something important that some businesses haven't considered.



Working From Home is huge **and here to stay.**

Unmanaged devices

We mean devices used to access business data that the company doesn't know about.

Your company laptop and mobile are likely to be safe because they've been set up properly with managed security.

But what about other devices your team use for work? John's "other" laptop; the one he grabs sometimes in the evenings just to do his email.

In fact the risk is bigger than this. There's a risk from virtually all other devices on your employees' home networks.

Their games consoles, other laptops, tablets and phones. Most people have an entire household of gadgets connected to the network.

And almost all of them are at risk of being accessed by cyber criminals.

The bad guys will find a way

If there's one thing we know about cyber criminals it's that they're very persistent. If they want to get in, they will keep going until they find a way. Sometimes, your team will make it too easy for them.

All a hacker needs to do is access one device on someone's home network. Let's say it's a games console. Once they access the console it's a waiting game. The hacker will be patient and watch the traffic on the network. It's possible they'll be able to learn enough from that to eventually spot a security hole with a work device.

Often, by the time someone's noticed something's wrong, it's too late. The hacker may have gained access to the VPN – the Virtual Private Network that allows you to securely connect to your company's data.

That means they can potentially gain access to your business's valuable data and might make a copy and sell it on the dark web.

Or they might install malware, malicious software that can create damage and corrupt data.

Or in the very worst case scenario, they launch a ransomware attack, where your data is encrypted and useless to you, unless you pay a huge ransom fee.

This is the most frightening thing that can happen to your organisation's data and you do not want to risk this.

What's the **solution?**

The answer isn't straightforward. Unless your business wants to take on the security responsibility of all of your staff's home networks, and all of their devices too.

It's just not realistic.

However, there are things you can do to lower your risk of an intruder getting into your business network via an unsecured home network. It all comes down to a layered approach to security.

There are five things we recommend.

Help your team secure their home routers

The router is the box that spreads the internet around the house. You might know it as the Wi-Fi box.

You can give every member of your team advice and direct support to keeping their router secure.

Such as changing default admin passwords to randomly generated long passwords.

Making sure the router's operating system, known as firmware, is always up-to-date.

And disabling remote access, so no one can change anything in the router unless they are physically in the property.

You could create a policy to make it clear your team must follow standard security guidance for their home network if they want to Work From Home.

01

Make sure your systems are monitored

Your IT support partner should be monitoring your network and systems, and if you are a client of ours then rest assured we are doing just that.

Our RMM (remote monitoring and management) tool is deployed on your network and will be constantly monitoring your systems 24/7, looking for anything unusual that may cause an issue and preventing problems from escalating.

Unfortunately, cyber criminals don't work to our schedules. They certainly don't work a 9-5 day job. It's more likely that they'll make changes when they believe no one is watching, so we have setup alerts to trigger an early warning should the worst happen. We also have tools and triggers deployed within the Microsoft 365 environment which will act as an early warning system should anyone try to gain access maliciously.

02

Reassess your VPN

Virtual Private Networks have been invaluable over the last couple of years. But while they've allowed remote access to your business network, the large-scale use of VPNs has created a higher risk of a data breach.

If a hacker breached a device using a VPN to gain access to your network, it means they could have full access to everything… without needing to pass further security measures.

That's frightening!

An alternative option is to lose the VPN and take a zero-trust approach.

This means that the credentials of every device and person trying to access the network is challenged and must be confirmed.

This way, if a hacker does gain access, they can only cause damage to the specific system they have accessed.

03

Carry out a security audit

The best way to ensure your business is protected from this kind of attack is to get a security audit.

Take a look at the security you already have in place and identify what's missing to keep your business as safe as possible without it getting in the way of everyday work.

If you are a client of ours, we probably already have a fully detailed account of your security systems. If so, we can tell you what weak areas, if any, we have identified and let you know your options for improving them.

If we haven't done so, we can assess your organisation and the way your staff work, and make suggestions on the security measures that will work best for you.

04

Trust a true partner to worry about this for you

As one of our customers, your company's technology strategy is very important to us and we take it very seriously. We will work in partnership with you to make sure your data remains as safe as possible.

If you have any concerns, or would like to know more about our approach to IT Security and what we could do for your business, please get in touch.

CALL: 01252 235 235 **| EMAIL** sales@ntsols.com
WEBSITE: www.ntsols.com

net technical solutions