The security problem of John's "other" laptop

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

breathetechnology
infrastructure | support | security | cloud

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 organisations 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.

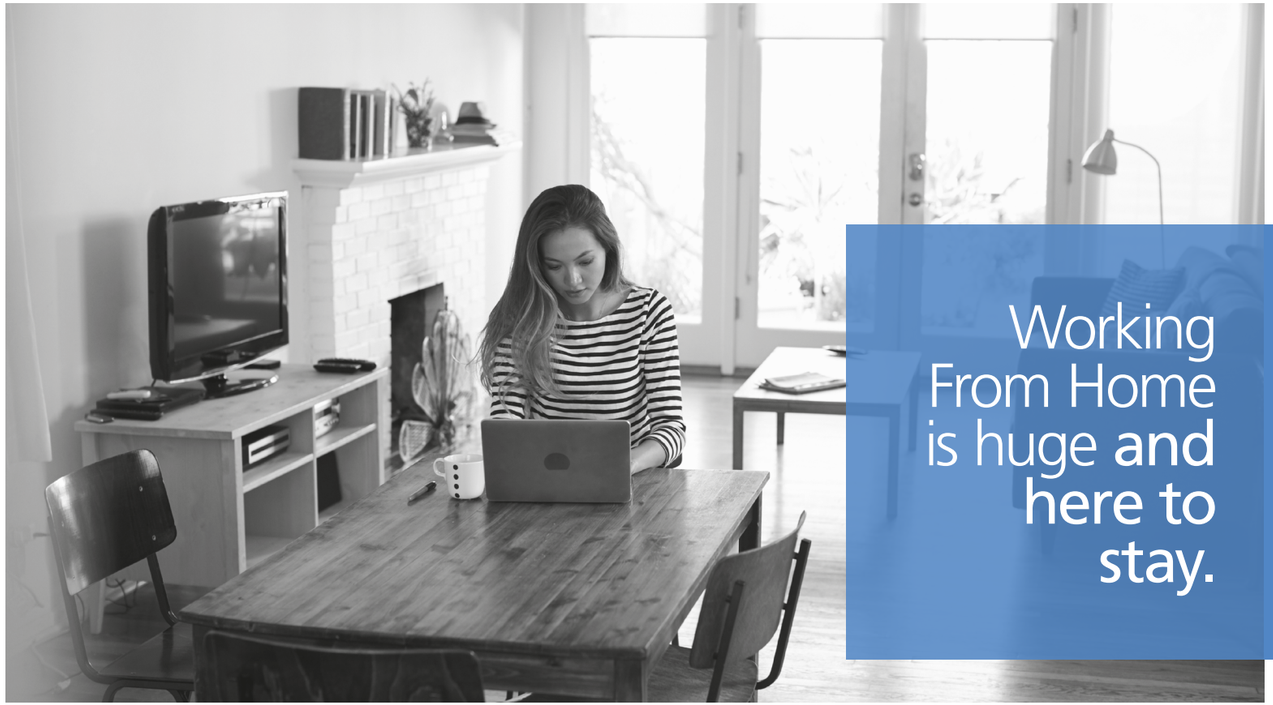
Because of that, cyber security in 2022 doesn't look the same either. When you have people working away from your office you need to take additional security measures to keep your data safe.

Even before we'd heard the word "Coronavirus", many of us were working from home now and then. 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 they're taking unnecessary risks with your data.

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

However there's something important some organisations haven't considered.



Unmanaged devices

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

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

However 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 team's home networks.

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

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 in, they will keep going till they find a way, and 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 the school's or business's data.

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

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

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

This is the scariest thing that can happen to your school's or business's data. You do not want to risk this.

What's the solution?

The answer isn't straightforward. Unless your organisation 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 school or business network via an unsecured home network. It all comes down to a layered approach to security.

There are six things we recommend.

#1

Help your team secure their home setup

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

Things like changing default admin passwords to randomly generated long passwords.

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

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.

#2

Make sure your systems are monitored

Your IT support partner should be monitoring your systems. That doesn't mean having a quick check that everything is working as it should be, and waiting for you to flag up any issues.

They should be constantly monitoring your network 24/7, looking for anything unusual that may cause an issue. Preventing problems from escalating.

Unfortunately, cyber criminals don't work to our schedules. They certainly don't work a 9-5 job. It's more likely that they'll make changes when they believe no-one is watching.

They may launch an attack at 3am on a Sunday, to give them as much time as possible to do what they need to do. Your IT team needs to be ready.

#3

Reassess your VPN

Virtual Private Networks have been invaluable over the last couple of years, but while they've allowed remote access to your organisations 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 get onto your network, it means they could have full access to everything… without needing to pass further security measures.

That's scary.

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

This means 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.

#4

Carry out a security audit

The best way to ensure your organisation 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 getting in the way of everyday work.

If you're working with an IT support provider, they should already have a fully detailed account of your security systems. It's worth asking them what weak areas they have identified and your options for improving them.

An expert will be able to assess your organisation and the way your people work, and make suggestions on the security measures that will work best for you.

Specific security improvements we make and some really good advice

- Change the default username on all devices. Most of the default usernames and passwords are freely available on the internet. By changing the default username, there is no starting point for the attacker to brute force or dictionary attack the username.
- You must have **Office 365 Multi Factor** or a another vendor solution to protect your Office 365 access. If you don't … it's a matter of time before your account is hacked.
- If you have storage devices such as a NAS or SAN, ensure that you restrict access to the appliance and check with the manufacturer on how to lock it down. There will be advice available. Most can now have 2 Factor authentication enabled too.
- Do not use the same Admin username and password for firewalls, VPN Appliances and your Servers. Ensure that these are complicated phrases.
- Application passwords for databases, finance systems, CRM or MIS Systems etc should all be different and not be accessible via the network admin password.
- Ensure that you have an off-site copy of your backup, in case the local copy is damaged during a successful attack.
- For remote access, use an industry recognised VPN or Remote Access Server with 2 Factor Authentication. 2 Factor is really important because it removes the ability to crack the password easily. It's also cost effective and easy to use.
- Not only should you backup your servers and on-prem data … but give thought to backing up your Office 365 and SharePoint Data and scanning it with a cloud malware scanner.

#5

The following services to backup and protect your Cloud systems are available at a low cost per user. *To give you an idea:*

– **StorageCraft Cloud Backup for Office 365** - £2 per user per month

– **SonicWall Cloud App Security for scanning data in SharePoint** £2.50 per user per month

– **SonicWall End Point Security (replacing old fashioned anti-virus)** £2.50 per user per month

– **ProofPoint Cloud Email Anti-Spam and Anti Malware** £2.50 per user per month

– **Cisco Duo 2 Factor Authentication** £3.00 per user per month

#6

Trust a true partner to worry about this for you

Are you 100% happy with your current IT Support Provider?

Your technology strategy is too important to be trusted to a company you don't have a true partnership with.

We're now taking on new clients again. Get in touch and let's have a short no obligation conversation about your organisation.

www.breathetechnology.com
(live chat available)

01223209920

lucy@breathetechnology.com

breathetechnology
infrastructure | support | security | cloud