



**PiSYS**.net

A COMCEN COMPANY

We make **IT** easy

# The security problem "other" laptop



**Keep your business's data safe working from home**

# WORKING FROM HOME IS LIKE MARMITE

## You either love it or hate it!

The pandemic has shown working from home can work, and in some cases improve results. Majority of businesses have adapted and become more flexible with hybrid working.

Look back on 2019 and look at how much has changed with working environments.

With hybrid working, comes higher risks to cyber security. It's vital and essential to keep your data protected from outsiders.

A lot of employees working from home would check the odd email here and there in their free time, to try get a head start on the week. Some even working more.

Now that working from home is an option for most, their location is critical to data protection. Are they using unprotected free wifi?

Along with the advancement in working environments and cyber threats, there has also been an advancement in technology and its demand to help support the motions.





**Is working  
from home  
here to stay?**

## Unmanaged devices



Devices can be 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? Joe'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.

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 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 business's data.

And that means they can potentially gain access to your 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 business's data. You do not want to risk this.



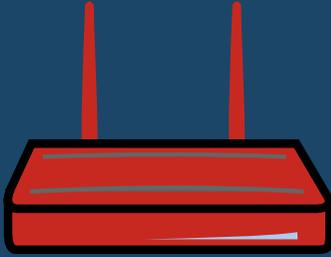
**The answer isn't  
easy or straightforward.  
Unless your business wants to take  
on the responsibility of all your staff's  
home security and device**

**What's the  
solution?**

A layered approach to security can help you towards the journey  
of protecting your data.

**5 things Pisis 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 keeping their router secure.

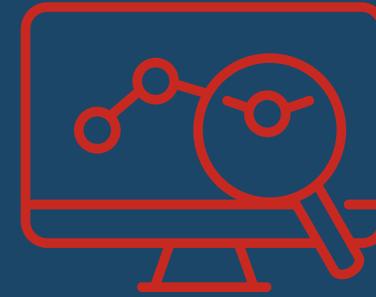
Things like changing default admin passwords to randomly generated long passwords.

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

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 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.

It means they should be constantly monitoring your network 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 job. It's more likely that they'll make changes when they believe no-one is watching.

And 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.

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 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

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 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 business and the way your people 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

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 taking on new clients**  
**Get in touch and let's have a short no obligation conversation about your business.**

05

**CALL: 01792 464748 | EMAIL [support@pisys.net](mailto:support@pisys.net)**  
**WEBSITE: [www.pisys.net/](http://www.pisys.net/)**

**PiSYS** .net

A COMCEN COMPANY

We make **IT** easy