Virgin media BUSINESS

SAFETY IN SIMPLICITY

How to make cybersecurity work for your least tech-savvy employee

Contents

Your new everyday: protected

Yesterday's security solutions were built at a time when everyone was more contained: contained to one workplace, contained to one network, contained to one device.

Now, quite frankly, we're all over the place. And with hybrid working – a mix of remote and office-based work – looking likely to stick around, enabling staff to work anywhere securely is essential.

But with people now working in so many different places on so many different devices and networks, defending against attacks is not as simple as it once was. You increasingly have to think outside the safety of your corporate network.

And when 48% of employees are less likely to follow safe data practices while working from home and home networks are 3.5 times more likely than a corporate network to have at least one malware family, there are more opportunities for human error to occur.

How do you overcome that?

By embedding cybersecurity into your network and everything that runs on it, making it easy and intuitive for every employee, whatever they happen to be doing.

Easier said than done.

Get it right, however, and the rewards are huge.

You can empower your people to do their job wherever they are, however works best for them and your customers, without losing sleep over sensitive data.

This will increase your competitiveness as a business, your attractiveness as an employer and your ability to serve customers or the public in the way they're now accustomed to.

And effective cybersecurity is at the heart of it.

Not only can the right approach protect your organisation from a harmful data breach, it can also be a key enabler in helping you adapt to new ways of working, giving you more time and resource to spend on the digital transformation projects that matter.

Our research with the Centre for Economics and Business Research (Cebr) highlighted three key areas of digital investment that could add tens of billions to the UK's annual GDP by 2025:

1. Flexible working

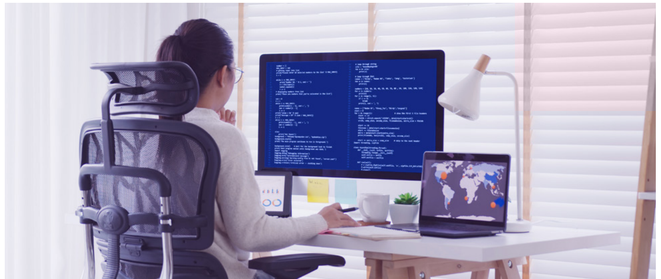
2. Digital delivery of services

3. Richer data for analytics and AI

All three rely on effective cybersecurity. In fact they're a lost cause without it.

We've created this simple, plain-English guide to help you navigate all this change, whatever stage you're currently at and whatever your future plans might be.

Read on to find out more.



Chapter 1 – The impact of human error

Virgin media BUSINESS

Please don’t click that

The impact of human error and how to reduce it

What is the leading cause of cybersecurity problems?

Human error.

Basic, avoidable human error – clicking on a phishing link, for example – caused 90% of all data breaches in 2019, according to CybSafe after it analysed data from the UK Information Commissioner’s Office (ICO).

Perhaps that’s a little unfair on end users. After all, the *real* leading cause of a cybercrime is a criminal’s decision to commit it in the first place.

But the fact is they *are* committing it. More so than ever.

An INTERPOL report last year contained dire warnings about the rise in cybercrime since the start of the pandemic, with the organisation’s Secretary General Jürgen Stock concluding: “Cybercriminals are developing and boosting their attacks at an alarming pace.”

Human error is precisely the thing that cybercriminals are usually trying to exploit: that one rogue click, that lapse of concentration, that moment of misjudgement – just enough to let them in.

And despite an explosion in online content educating people on what not to do, the problem appears to be getting worse.

According to CybSafe’s analysis, the percentage of data breaches caused by human error in 2017 was just 67%.

That’s a 23% increase in just two years.

So what’s going on here? Are cybercriminals getting smarter? Are end users getting less savvy? Is it all just a side effect of new ways of working?

Let’s start with cybercrime itself.

According to INTERPOL's analysis, the following types of attack (among others) have been increasing and evolving since the start of the pandemic:

- **Phishing:** An attempt to obtain sensitive information by impersonating a trusted entity, usually encouraging people to click on a link and provide some personal details
- **Ransomware:** Malicious software that infects your computer and displays messages demanding a fee be paid in order for your system to work again
- **Data-harvesting malware:** Criminals use software to infiltrate systems, compromise networks, steal data, divert money and build botnets, which can be used to carry out further attacks like distributed denial-of-service (DDoS)

All of these attacks rely to some degree on employees unwittingly (or worse: intentionally) letting the criminal in.

You can see why reducing human error is so important, then. But in the context of workplace cybersecurity, what does "human error" really mean?

Cybersecurity training provider usecure highlights two distinct types of human error:

1. Skill-based errors

2. Decision-based errors

Usecure defines skill-based errors as "slips and lapses". The end user knows the right thing to do but for some reason doesn't do it, maybe because they're tired, distracted or simply not paying attention.

Decision-based errors, on the other hand, are when an end user actively does the wrong thing, perhaps through a lack of knowledge or training.

Clearly there is a fine line between the two. But while decision-based errors can be overcome through more and better training and knowledge-sharing, can you ever prevent skill-based errors completely?

No matter what level we're operating at, we all have moments of misjudgement. It's human nature. And when it comes to cybersecurity, a moment is often all it takes.

Instead of hoping to eliminate human error altogether, then, it makes more sense to put measures in place to reduce the impact if and when it does happen.

In the next chapter we'll explore how to do that.

Chapter 2 – Why security and connectivity should work as one

Virgin media BUSINESS

The integration equation

Why security and connectivity should work as one (and how to make sure they do)

63% of public sector organisations told us they will be continuing flexible working practices in future, while 55% of private sector firms said the same.

And this is before you account for the inevitable long-term pressure employers will face from a talent attraction and retention perspective.

A recent Buffer survey asked respondents if they'd like to work remotely at least some of the time for the rest of their career.

97.6% said yes.

And when you look at the top reasons respondents gave – flexible schedule, ability to work from anywhere, no commute, more family time – it's easy to see why many won't be rushing to get back to the office five days a week.

In short: remote work is here to stay. And when offices do open up again, we're going to see the hybrid approach we mentioned earlier become the permanent norm.

What does that mean for cybersecurity?

It really plays into the previous chapter. At its core, cybersecurity is all about people. The people behind the attacks and the people they're trying to exploit.

In the old world, where the majority of people worked in an office most of the time (let's remember that this was only last year), traditional perimeter security methods served us well.

Most people, devices, apps and data would be inside your network, with a few operating outside it.

Now that's shifted in the other direction.

Applications are now dispersed all over the internet in a variety of different clouds. It's no longer possible to take a centralised approach.

So what can you do instead?

Move your security closer to those applications, tackling each application, user and device on an individual basis.

Virgin media BUSINESS

Welcome to the world of zero trust

The idea of not trusting people by default might seem a little harsh. But it's an absolute must for effective cybersecurity in a hybrid working world.

So how do approaches like zero trust and SASE (Secure Access Service Edge) actually work in practice?

The former pretty much does what it says on the tin. In essence: nobody is trusted until your security platform can determine otherwise.

Whether someone is logging in from a café, their kitchen or your head office, they're treated exactly the same way. So your devices, data and apps have the same level of protection wherever they happen to be.

SASE, a term coined by Gartner, works hand in hand with a zero trust approach. It's a cloud-based security model that essentially allows you to control and configure all your security services from a single software platform.

Let's unpack this a little bit in the context of hybrid working and human error.

In the traditional way of doing things, once somebody got access into your network they were free to cause all the damage they wanted.

The answer to that was to make absolutely sure that nothing and no-one could penetrate that network.

But in a modern, hybrid working world where people, data, apps and devices are spread all over the country and across the internet in various different clouds, that simply doesn't work. Most people aren't even working inside that network.

By taking a zero-trust approach, you move from trying to secure your whole network at once to looking at individual users.

You can then make instant judgements based on their specific situation, and either allow or not allow them access to certain data or applications.

By segmenting your users right down the individual level, you achieve two things:

1. You make it easier to catch vulnerabilities by looking at security risk on a case-by-case basis rather than taking a blanket approach

2. You remove security barriers to individual employees who should have access to things, freeing them to be more productive and improving the overall employee experience

But there is another important outcome from zero trust that links to the risk of human error we covered in the previous chapter.

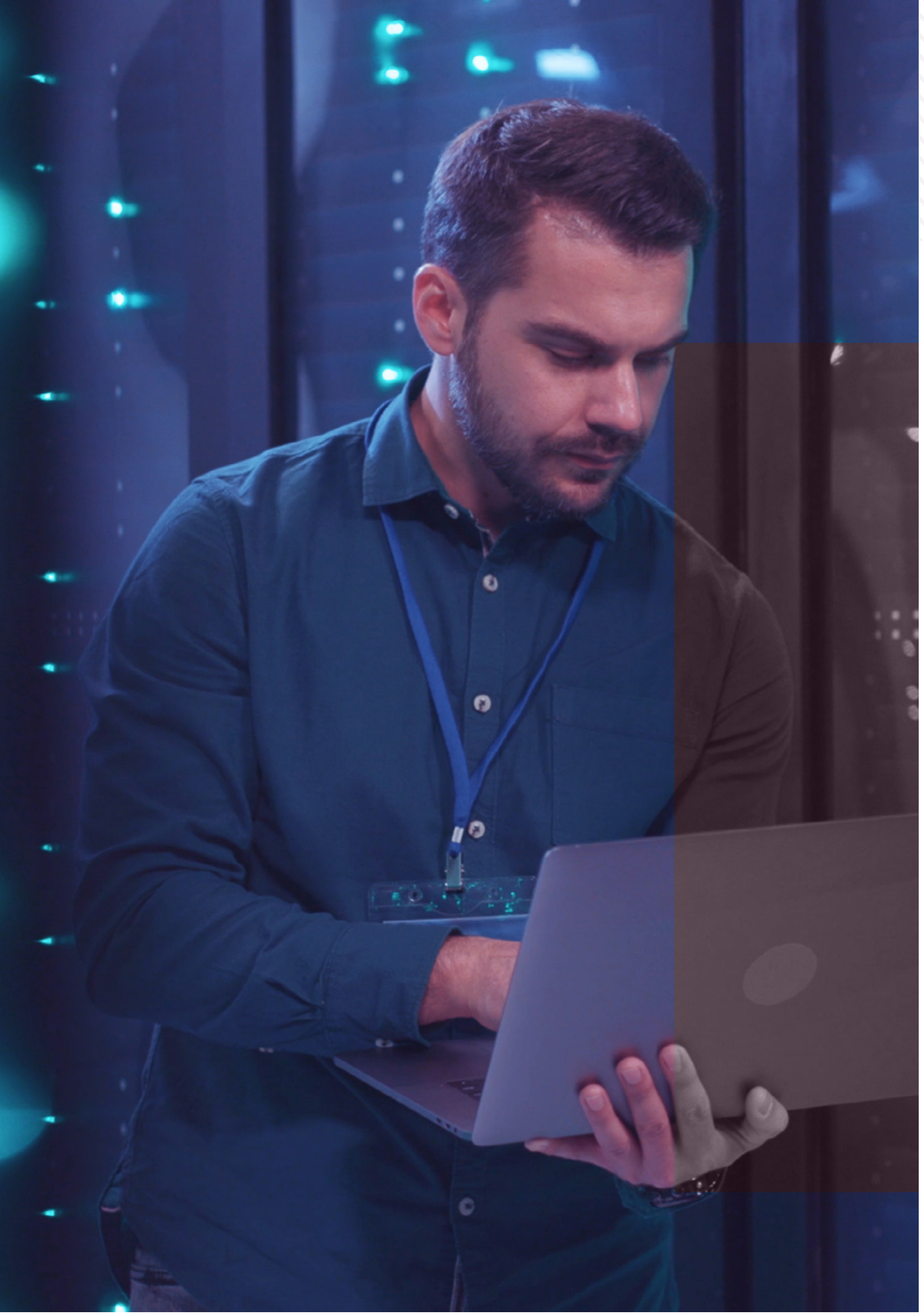
When you take a zero-trust approach, you are only allowing someone access to that one specific application in that particular moment.

So even if somebody does inadvertently let a cybercriminal in, that attacker will only have access to that one application.

It's still not an ideal situation, but it's far more contained and controlled than the traditional scenario where the attacker would have had access to your entire network and everything that runs on it.

You might not be able to eradicate human error altogether, but by taking a zero trust approach, you can certainly make it less of a problem.

So where does connectivity play into all of this?



Treat security and connectivity as one

Security and connectivity are like wings: if they don't come as a pair, you might as well have neither.

And one of the biggest mistakes a modern organisation can make is treating them as two separate entities.

Gartner's SASE model is the perfect illustration of this.

Software-defined networking in a wide area network (SD-WAN) is part of that model. Where SD-WAN allows you to securely connect geographically dispersed branch offices to your corporate network securely, SASE takes things one step further and integrates all your cloud security needs with SD-WAN.

This gives you a single, centralised view of your entire network. So you can quickly identify users, devices and endpoints, apply their networking access and security policies and then securely connect them to the aps and data they need – all from one platform.

This kind of zero trust, single-platform, integrated approach to security and connectivity is the only way to protect your data in a hybrid working world without slowing people's productivity down.

But don't take our word for it.

By 2024, Gartner predicts that 40% of enterprises will have explicit strategies to adopt SASE.

To put that into context, at the end of 2018 that figure was 1%.

The above shows how quickly things have changed. And how quickly forward-thinking organisations are moving to adapt.

And again, it all comes down to people. Not just helping them avoid mistakes that could lead to a cybersecurity breach, but making sure cybersecurity enables and empowers them rather than slows their progress down.

The word “security” comes from the Latin word “securitas”, which translates as “free from care”.

Free from care is exactly what you want your employees to be when it comes to cybersecurity.

That might sound counterintuitive, but if you can get to a point where they don’t have to live in fear of causing a cyberbreach, and there aren’t any clunky cybersecurity barriers holding them back, they will be free to be as productive, collaborative and innovative as possible – wherever they happen to be.

And the only way to truly achieve this is by treating connectivity and cybersecurity as one: a zero-trust approach to security enabled by a modern, cloud-based network – all controlled through one central platform.

Chapter 3 – Legacy problems

Virgin media BUSINESS

Legacy problems

How to enable secure hybrid working when your IT is growing in age, not budget

Much of what we've talked about in this guide so far revolves around a modern, cloud-based approach to networking.

But what if your organisation is running on ageing legacy infrastructure?

According to a survey by Cloud Industry Forum, 90% of organisations have experienced difficulties migrating to a cloud solution, with 43% citing complexity as a migration issue – the most-cited issue by far.

In the public sector especially, this issue became all too clear as the pandemic began to take hold in 2020.

67% of government IT leaders in Europe said legacy infrastructure was holding back digital progress as they tried to adapt in the wake of Covid-19, according to a Pure Storage survey last year, with 87% saying operational costs were increasing as a result.

That latter point is critical here. Lack of budget is often cited as a barrier to digital investment, particularly in the public sector. And often decision-makers are stuck between a rock and a hard place.

They know investing in the right technology could save them money in the long run. And this is especially true of cybersecurity, where not investing in the right approach brings with it the potential (enormous) added cost of a data breach.

Equally, however, they don't have money to burn on a large-scale transformation project.

But when 66% of respondents in that same survey feel investment in infrastructure security is not keeping up with security threats, clearly something has to give.

And that something doesn't have to be the quality of the experience you give to employees, customers or citizens. Because while 57% of leaders said they would sacrifice technology performance in favour of enhanced security, that isn't always necessary.

There are ways you can have your cake and eat it, even if your infrastructure is as old as your budget is small.

It’s never “all or nothing”

The phrase “digital transformation” can sometimes be misleading.

Aside from being overused to the point of becoming meaningless, it doesn’t accurately portray what the phrase actually means.

The word “transformation” feels enormous. It immediately makes the task sound scary, disruptive, too big to achieve.

But that’s not what digital transformation is about.

It’s about making changes wherever you can, however small, in a way that has a real impact on the way your people work and serve your customers. And all those changes add up to a better-performing organisation.

This is true of cybersecurity too.

You don’t need to overhaul everything at once – every system, process and piece of technology.

It’s possible (in fact, advisable) to modernise your cybersecurity in incremental stages while unlocking some of the immediate benefits like the ability to enable secure hybrid working.

One London council we worked with, facing the kind of infrastructure and budget challenges we highlighted earlier in this chapter, decided to take more of a half-and-half approach.

The council adopted a cloud-based approach where it was possible and affordable to do so. And where it wasn’t, the team deployed a more traditional firewall to keep those elements protected.

At some point, budget and resource allowing, the council may decide to move more of its infrastructure to the cloud, and its cybersecurity approach will adjust accordingly.

For now, however, the council can enjoy the benefits of digital transformation in a way that works for its current situation – all while keeping critical data safe.

This shift away from traditional thinking is allowing even public-sector organisations to completely modernise the way they do things when it comes to connectivity and cybersecurity.

If you can move something into the cloud, make it happen. If you can’t, use a combination of traditional and cloud-based approaches until you can.

Virgin media BUSINESS

Find your cybersecurity roadmap

Achieving the above is no walk in the park, of course.

The path to digital transformation doesn't always have to be fast, but the journey can be complicated – especially when you're trying to balance today's technology needs with yesterday's infrastructure.

To navigate those complexities successfully, you need a roadmap: a solid picture of where you are today, a clear vision of where you want to be and a realistic plan to get from the former to the latter based on your current infrastructure and budget.

This is where cybersecurity becomes less about technology and process and more about strategy. An outcome enabler rather than something you only do out of necessity.

And while some organisations may have skills and resource to manage that roadmap in-house, many will choose to outsource much of the heavy lifting to a technology partner.

If you are going to do that, make sure you look for a partner that doesn't have a vested interest in one particular solution or approach.

That partner will always say the answer to your cybersecurity challenge is the thing they happen to be selling.

If you work with a partner that has no vested interest one way or another, however, they'll look at your situation objectively and help you plan a roadmap of digital change that actually reflects what you need today and in future.

Eight cyber-hygiene must-haves for hybrid working

Eight cyber-hygiene must-haves for hybrid working

Cybersecurity is a complex beast, but it pays to remember the basics. If you and your employees follow these eight simple steps, you'll have a much better chance at reducing the biggest cause of a data breach: human error.

1. No more "Password1"

The most common password in 2020 was "123456". In the nicest possible way, don't rely on employees to come up with a decent one on their own. Make sure your password policy reflects the latest guidance. Advise people not to use their company password for personal use (e.g. for their social media accounts) and make sure your password policy applies to all devices accessing your network, including mobile.

2. Multi-factor authentication

While it creates an extra step for employees, multi-factor authentication is sometimes a vital extra layer of protection (when people are accessing Microsoft Teams remotely outside the corporate network, for example). If staff have mobile device for work, it's best to use those for authentication. It's unlikely a cybercriminal will have access to an employee's password and physical device.

3. Anti-malware software

You can't always stop people clicking on dodgy links. But by installing anti-malware software on all devices and network servers, you can help reduce the damage when they do. Not only can anti-malware software detect incoming malware and prevent it from being installed on an employee's device, it can also prevent malware spreading to other devices on the network.

4. Updates, updates, updates

This is might seem like an obvious one. But with roughly one in three cybersecurity breaches caused by unpatched vulnerabilities, it's clear that many organisations aren't getting this basic step right. Make it a requirement that every employee has automatic security updates activated as standard. Again, this takes the human-error element out of the equation and closes an easily avoidable open door for hackers.

5. Safe browsers and HTTPS

A safe browser is a web browser with extra security measures that help prevent unauthorised third-party activity while you're surfing the web. Mozilla Firefox or Google Chrome are two of the best-known examples. And make sure all your web pages or apps use an HTTPS (secured) connection rather than HTTP (unsecured), especially if that page or app contains sensitive data.

6. Data common sense

There are a number of steps individual employees can take to protect sensitive company data. Don't download any work-related data onto personal devices. Don't leave physical documents containing sensitive data in an accessible place overnight (e.g. your desk). Try not to print documents containing sensitive data while working remotely. And shred any documents containing sensitive data as soon as they're no longer needed.

7. Solid data backup

Back to that point about human error. You can't always avoid it, but you can take steps to reduce its impact. Make sure you are systematically backing up your data. And make sure you're regularly testing your backup systems too. Would you be able to quickly recover critical information that was lost in an attack? If not, you're risking potentially severe disruption to your day-to-day operations.

8. Regular training

Of course, technology, culture and process are only part of the equation. Regular training that really engages people is crucial to reducing the impact of human error and keeping your data protected. Make sure people know what a phishing email looks like. Reiterate the basic measures they need to be taking every day. And put clear steps in place for them to take if they spot something strange or click on something they shouldn't have.

Next steps

Next steps
Ready to protect your new everyday?

If you need help navigating any or all of the topics we've explored in this guide, you've come to the right place.

We understand networks better than anyone, which means we understand how to keep your network safe without slowing anyone down.

Our experts look at security in the context of your overall connectivity needs, working closely with you to build something bespoke that helps you achieve the wider outcomes you want for your organisation.

Here's what you get with us:

Continuity

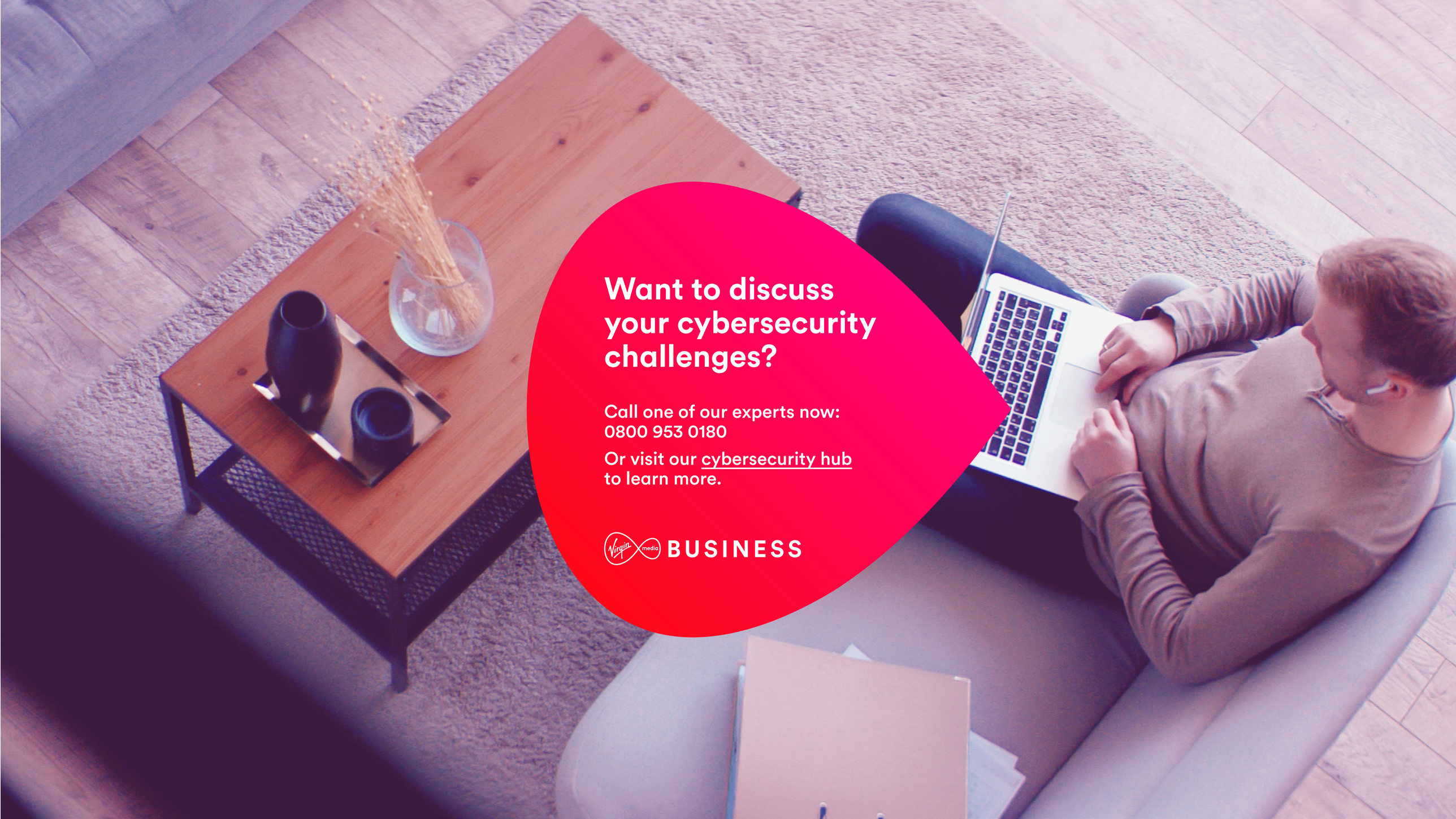
- A network that is secure by design with built-in early-warning systems, coupled with end-to-end customer service to make sure you're always proactively protected – all through one point of contact

Expertise

- Fully certified, CISSP-accredited security experts who live and breathe penetration testing, exposure analysis and everything in between, so you get a safe pair of hands as standard

Flexibility

- The simplicity and control that comes with buying connectivity and security as one, with managed and unmanaged options, so you can empower secure hybrid working your way


Want to discuss your cybersecurity challenges?
Call one of our experts now:
0800 953 0180
Or visit our cybersecurity hub to learn more.
Virgin media BUSINESS