Bring Your Own Device

7 crucial steps to keep your company

Bring Your Own Device

7 crucial steps to keep your company data safe on your staff's devices

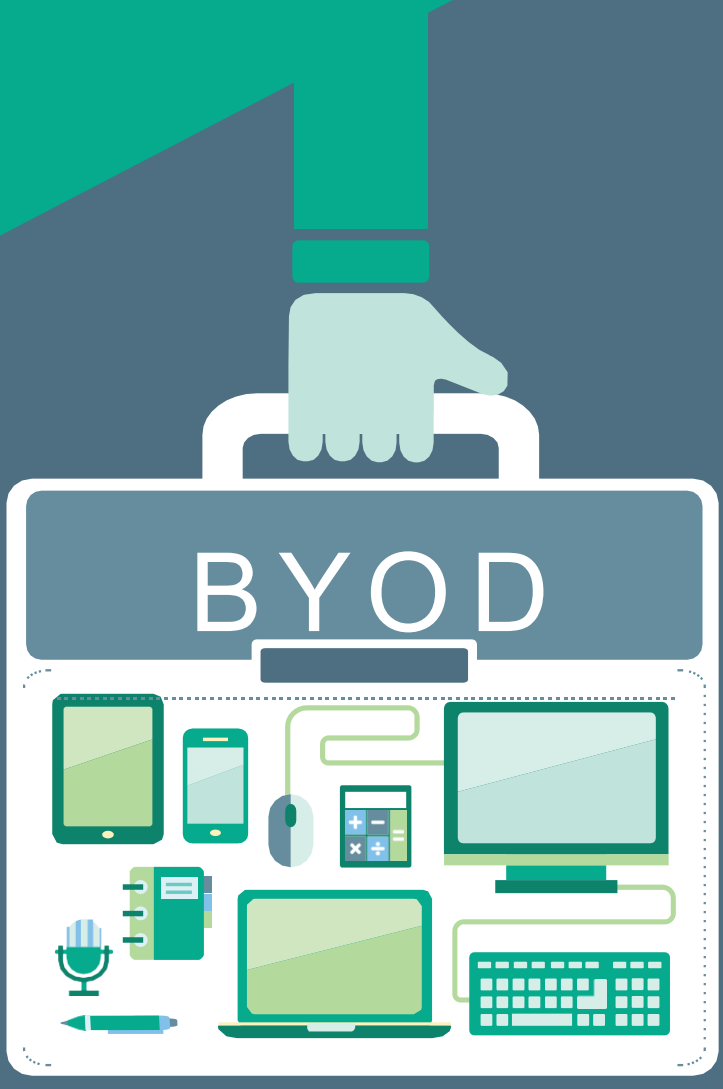
Working from home has quickly become the new "normal", thanks to the current situation.

And it's uncovered a whole new set of challenges for many businesses.

Some of the biggest sit within the concept of BYOD (that's Bring Your Own Device). The thinking is that so long as your people have their own laptop, computer, or tablet and are connected to the internet they should be fine. Right?

Actually, there's a lot you still need to consider. Just because we're all working from home doesn't mean we can forget about the security measures we're so fastidious about in the office. In fact, if your people are using their own devices, you should be even more cautious.

Sadly, cyber criminals are taking advantage of this global panic to do what they do best. We've seen an upsurge in attempts to steal data and breach systems, many based around the Coronavirus.



So in this guide, we've created a checklist for you to work through to ensure that your people can work on their own devices, without compromising your business's data security.

1 - Passwords

We do talk a lot about passwords, but hopefully you understand why. They're so important. Even if your people are working from home and they're less likely to lose their device, there still may be other people in their home with access to it. Strong passwords for applications and even to access the device are a must.

If you haven't already, you should consider implementing multi-factor authentication for your applications (where you get a log in code from a separate device). This gives you an added layer of protection.

2 - Who else has access to the device?

Out of the millions of people in this world, we like to think we can trust our families the most. We're not suggesting otherwise. But in cases where a member of staff has say, a shared laptop, can they be sure that their children won't click a dodgy link and inadvertently hackers give access to your company's data? We'd bet not.

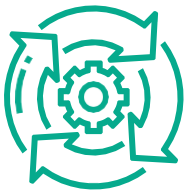
Consider who has access to your employees' devices and judge whether it would be wiser to provide them with a company device instead. If you do issue company devices, you need to give strict instruction that it can only be used for work purposes; not gaming, shopping, or anything else.

Your IT service provider can also ensure that work devices don't allow unauthorised downloads.

3 - Do they have the latest antivirus protection installed?

This is really important. If their device doesn't have antivirus protection, yes, there is potential for it to become compromised, but the device may already have malware installed. Once that device has access to your confidential data, it could go straight into the hands of the wrong people.

We'd suggest that you allow your IT professionals to remotely check all devices. to make sure they are clean, up-to-date, and secure.



4. Are they using the most current operating system?

Could Karen in accounts still be working on the now-dead Windows 7 at home? If she is and she uses that device for work, you could be in trouble. Since Windows 7 is now defunct, it's unsupported. Should something go wrong, you've nowhere to turn to retrieve data or resolve an issue.

Make sure that whatever operating system your team uses at home is the most current version. And all the updates have been installed.

It's worth your while to make a list of your employees, what device they will be using, and the operating system they're running, so that should they need support your IT support provider is informed and prepared.

5. More updates

Yes, updates to applications are a pain. They often take ages and they always want to run when we're in a rush to use our device and get working. But they're vital and so it's important that we take the time to run updates as soon as they're available.

The same goes for installing patches available for your operating system.

Do your employees have the relevant patches installed on their devices? If not, again you're opening yourself up to cyber criminals, malware and data loss.

6. Which VPN?

If you already have people working remotely, you may already have a VPN set up (a VPN is a Virtual Private Network, and it's the safest way for your team to access company data).

If you don't, you'll want one to allow your team to access the company network from home. Either way, it's important to assess which VPN is most suitable for your new requirements.

With everyone in your business working remotely, is your current VPN up to the task?

Speak to your IT service provider about which VPN is best for you. Don't just choose the first result of a Google search.

7. Update your handbook

Ok, it's not actually a technical learning point, but it's a great time to look at your company's policy on home working.

Update your handbook so everyone knows what is expected, what's acceptable and what certainly isn't while they're working from home. There's nothing like a time of crisis to discover who can really be trusted. But if you have policy and procedure to fall back on, your team will have no excuse to slack off.

You should also make it clear that any potential data breaches should follow the same IT plan as they would in the office. Make sure your people know who to report an issue to and what steps they should follow if they're concerned.

There's no doubt that this is a testing time for business. We made sure the majority of our clients were ready for remote working, long before they needed it.

If your IT provider wasn't so proactive or can't service you properly now, then let's talk. We'd love to see what we can do to help you in the current situation. And then when it's appropriate, have a bigger conversation about your business.