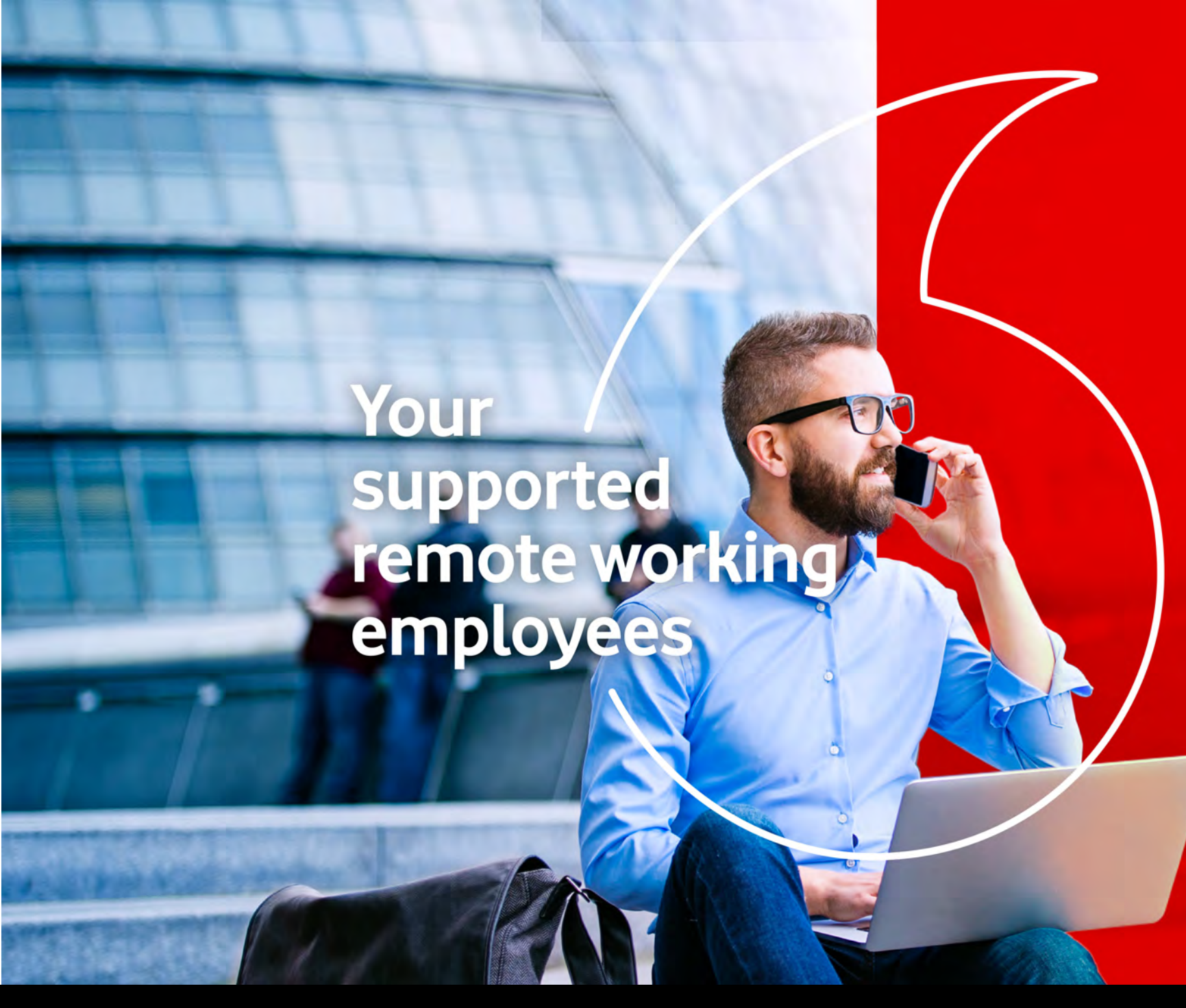


Our first 13 steps checklist to keeping your business cyber-secure

The future is exciting.
Ready?

vodafone business

Cyber security is more important than ever

And now, with many people working from home and handling sensitive data remotely, keeping your business safe is essential to stay operational and profitable.

We've put together a simple, first steps checklist to getting your business cyber-secure.

How many can you tick off?

no.1

Implement a new password routine

Whether setting up new user accounts for remote working or updating existing account logins, all passwords need to be changed regularly.

- Get your employees to change their passwords every 3 months.
- If your business has less than 40 employees, consider changing shared passwords every time someone leaves.

no.2

Set up multi-factor authentication

Multi-factor authentication is when a user's identity is confirmed using multiple credentials covering something you 'know', 'have' and 'are'. For example, a user name, a code sent to a mobile and a fingerprint. It helps keep accounts secure, as only the user has all this information.

- If you've got Office 365, then it's easy to set up.[2]

no.3

Turn your firewall on

Firewalls are often off by default.

- If you have a Windows system, here's **a guide to turning Windows Defender** on.[3]
- If you have a Mac, here's **a guide to turning your firewall on.**[4]

no.4

Secure your mobile devices

Mobiles can be a business' weakest link. And with more employees now working from home, it's harder to keep tabs on how your employees use devices that have sensitive work data on them.

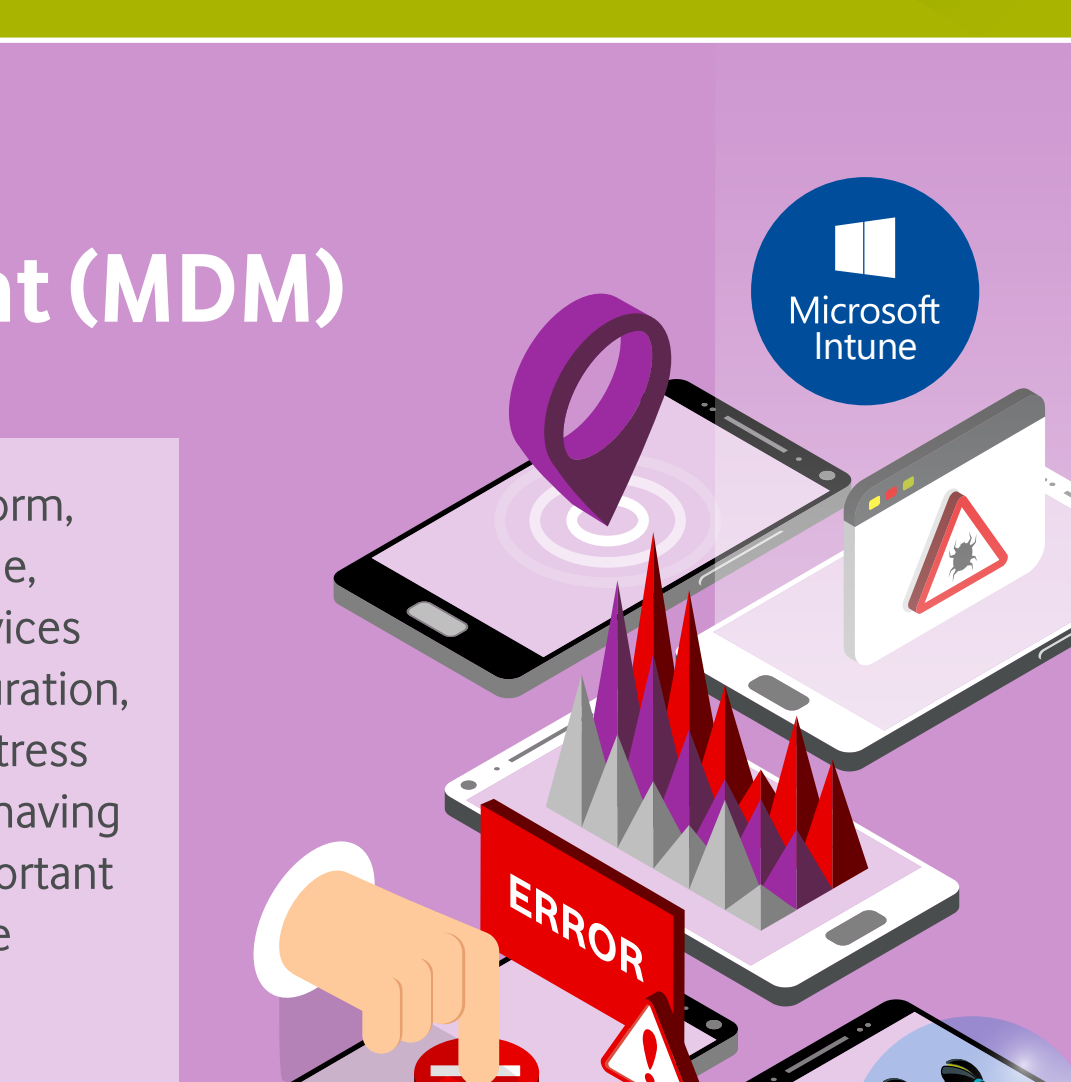
- Lookout secures your mobile devices from phishing, harmful content and threats on your network.

no.5

Advise employees on how to encrypt data on their devices

Make sure employees set their devices to encrypt data while not in use. This will protect the device's data if it is lost or stolen.

- Most modern devices have encryption built in, but it may still need to be turned on and configured by going to the device settings.



no.6

Get Mobile Device Management (MDM)

This lets you monitor and secure all work devices, even if they're owned by your employees. MDM means you can shut down apps and devices if they're breached.

- Through an MDM platform, such as Microsoft Intune, you can also set up devices with a standard configuration, this will help take the stress away from employees having to remotely adjust important settings (such as device encryption and regular software updates).

no.7

Take a cyber security training course

Taking a training course is a great way to keep your knowledge up-to-date and build an internal culture of cyber security. Most online courses are inexpensive too.

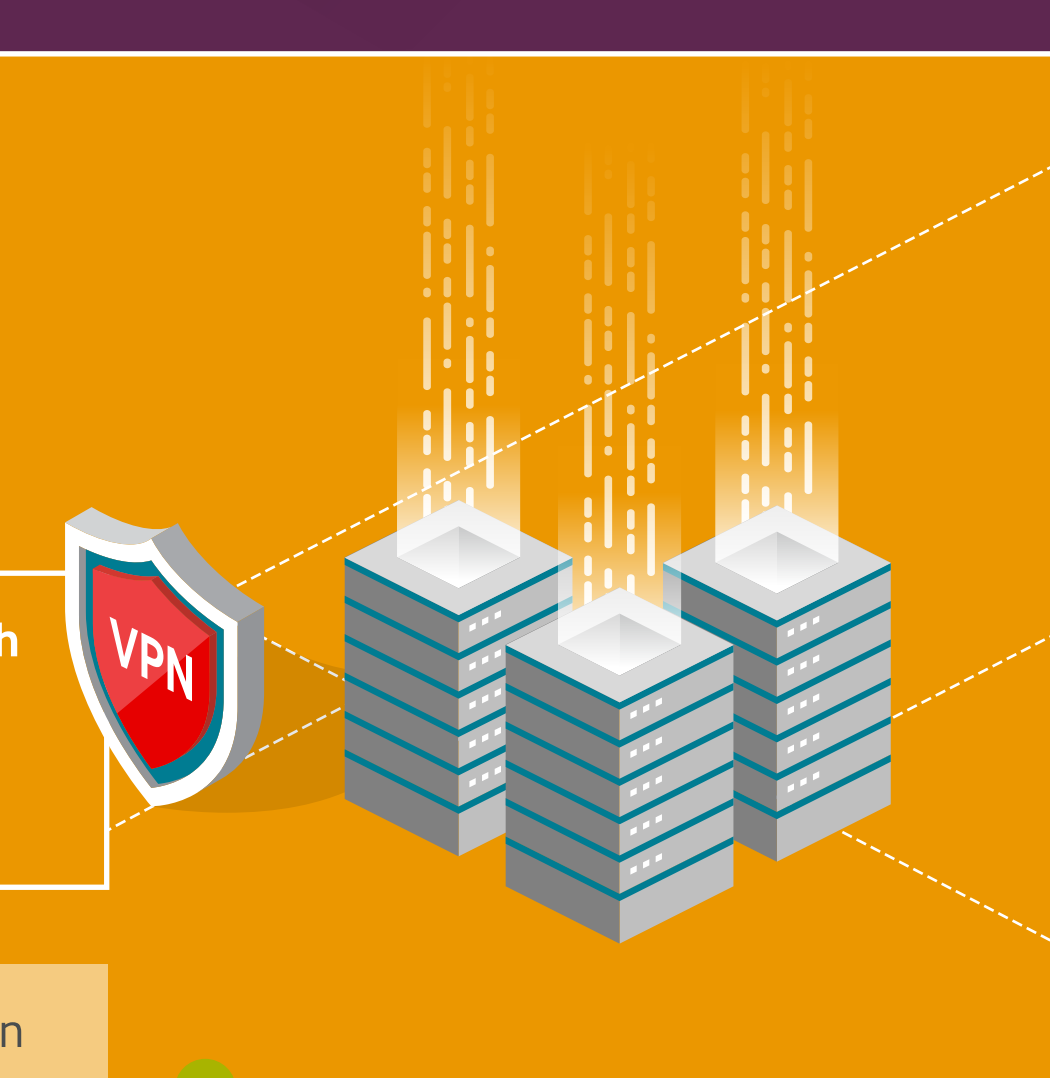
- **Stay Safe Online** offers plenty of useful, free resources on getting cyber-aware. Offer this to your staff too to make them feel empowered and in-the-know.[5]

no.8

Control and limit removable media

Removable media such as USBs or hard drives can contain sensitive information, are easily misplaced and can introduce malware into IT systems.

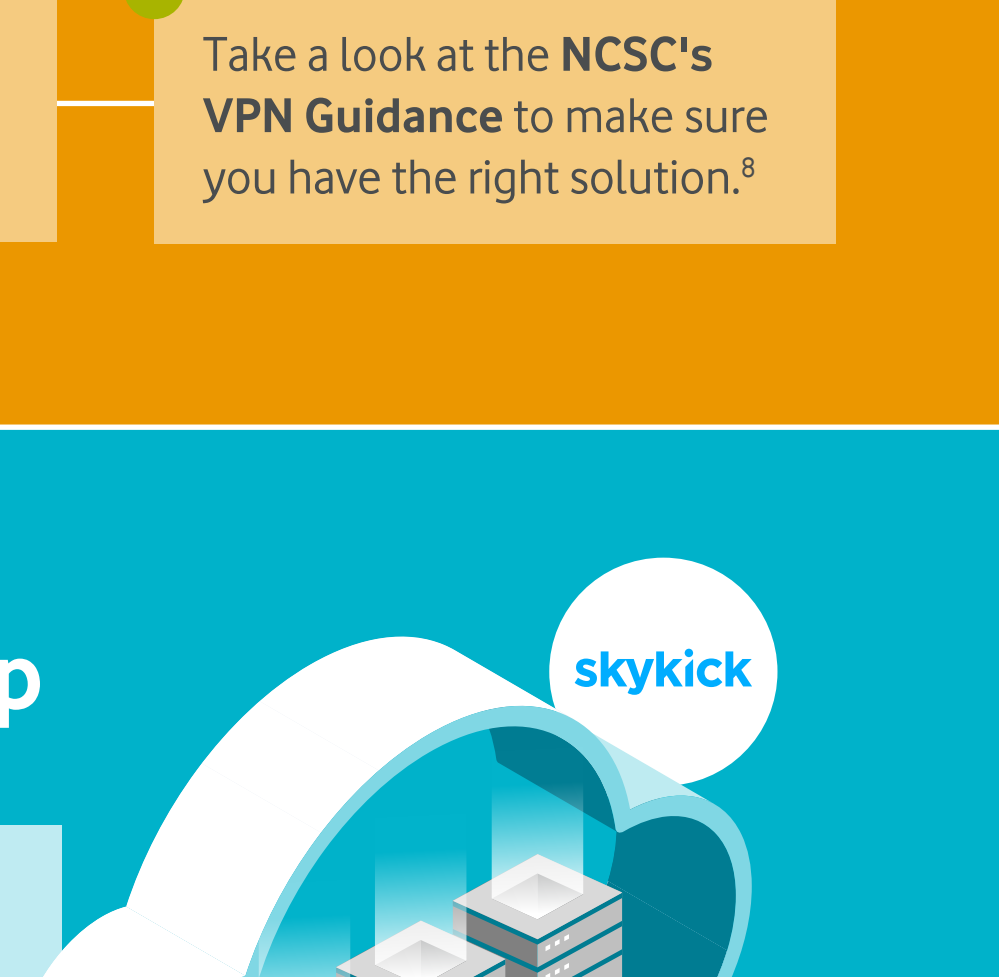
- To reduce risk, only allow products supplied by the business to be used or ask staff to transfer files using alternative means (e.g. a storage platform like Dropbox[6] or collaboration tools like Slack[7]).



no.9

Manage use of Virtual Private Networks (VPNs)

Allow remote users to securely access your IT resources, such as email and file services. VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit.



- If you have a VPN, make sure it is fully 'patched'. If your organisation normally has a limited number of remote users watch out for the need for additional licenses, capacity or bandwidth, if you have not used it much before, are expanding or have more people working from home.
- Take a look at the **NCSC's VPN Guidance** to make sure you have the right solution.[8]

no.10

Make sure everything is backed up

If a cyber attack happens, you need to know your work is safe. You need to put some precautions in place.

- Skykick offers unlimited cloud storage, and can back up files automatically up to six times a day.

no.11

Evaluate your partners

Keeping your business secure isn't just about your own security. You need to be thinking about checking in with your partners and regular suppliers and asking what their cyber security policy is to ensure it meets your standards.

- For example: if you use an ecommerce platform, check that it's PCI-DSS (payment card industry data security standards) Level 1 compliant.

no.12

Move to the cloud

Out-of-date software is a perfect target for hackers. Moving your apps to the cloud means you've always got the latest, most secure app. And it makes it easier for employees to collaborate in our new WFH world.

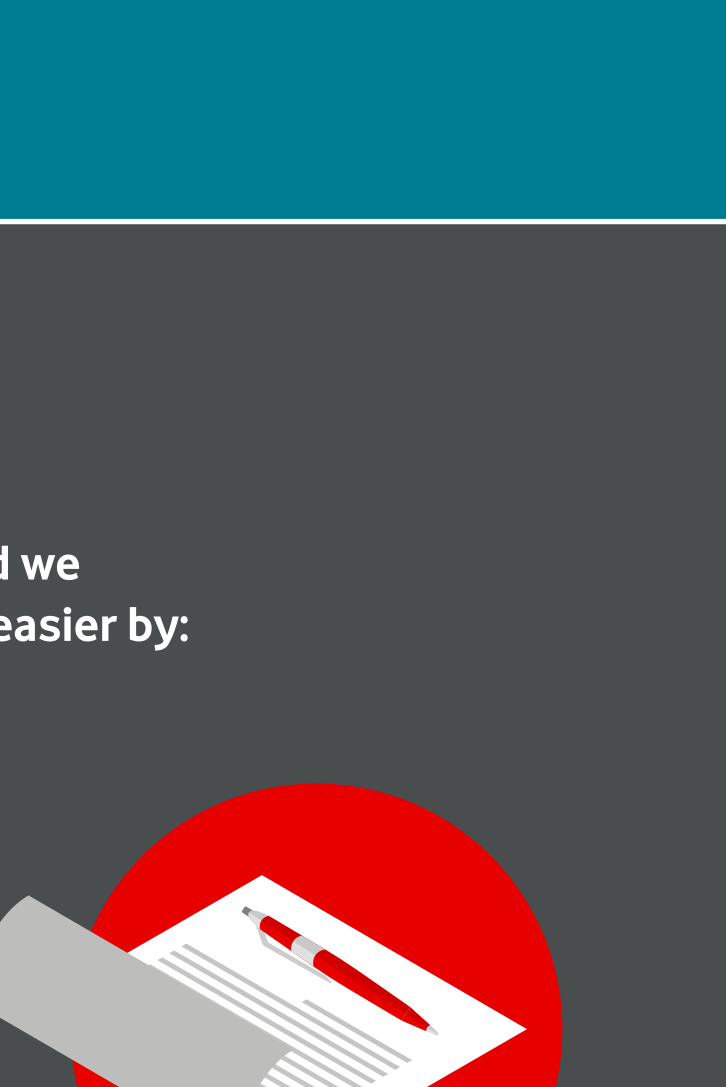
- Check out Vodafone Business Marketplace for **cloud-based apps**.

no.13

Create a clear policy on reporting security issues

If any issues do arise, make sure staff know how to report any problems, including loss of data, theft or any security issue. Write a set of easy, blame-free instructions and contact details, then make them easily available in your company handbook or equivalent.

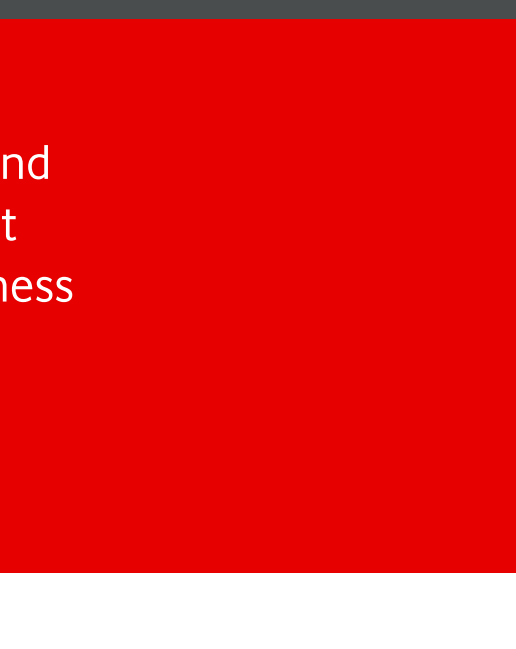
- Make it clear that problems should be reported as soon as possible to minimise risk.
- This is especially important when staff are not in the office and don't have direct access to support.



Be smart. Be sure. Be cyber-secure.

Cyber security is a fundamental consideration of any modern business and we believe getting started should be simple. Vodafone makes getting secure easier by:

Letting you buy multiple security apps in one place, making them simpler and less time-consuming to manage



Offering our apps at a competitive price

Providing flexible monthly contracts so you can try apps on a temporary basis, to see what works for you

Visit **Vodafone Business Marketplace** to find the security and Mobile Device Management apps you need to start protecting your business and employees today.

The future is exciting.
Ready?

vodafone business

1. FSB, https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html, 2019.
2. Microsoft, https://docs.microsoft.com/en-gb/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide, 2020.
3. Microsoft, https://support.microsoft.com/en-gb/help/4028544/windows-10-turn-microsoft-defender-firewall-on-or-off, 2020.
4. How to Geek, https://www.howtogeek.com/205108/your-mac%E2%80%99s-firewall-is-off-by-default-do-you-need-to-enable-it/, 2017.
5. Stay Safe Online, https://staysafeonline.org/cybersecure-business/, 2020.
6. Dropbox, https://www.dropbox.com/en_GB/?_hp=c, 2020.
7. Slack, https://slack.com/intl/en-gb/, 2020.
8. NCSC, https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks, 2020.