O2 business

Seven tips to improve data security

Telefonica

Discover more

Contents

A different world

With more people using smartphones, tablets and mobile apps for work, employers are switching to cloud-based technology and adopting collaboration tools to support the transition. Workers are now more free than ever to get on with the job just as they would in the office, wherever they want to do it.

See how we helped make Addleshaw Goddard's workplace more mobile, so their lawyers can work wherever and whenever they need.

Discover more

Mobile working can improve a workforce, with

80%

of remote workers reporting an increased morale[1]

As you make changes to help your people work when, where and how they want, you'll start seeing benefits – like greater productivity, raised morale and cost savings. But you might also uncover new challenges, such as working out how to keep your data secure.

Working remotely will inevitably at some point require a need to access company data on multiple devices, work in public places and connect to different wifi networks. That puts data at risk.

While keeping your data safe is a priority, it should be done with your people in mind. They want to work when and where they please, without the hassle of restrictive security measures. Striking this balance between user freedom and data protection is possible, and these seven practical tips for data security, will help you on your way.

[1] https://www.forbes.com/sites/andrealoubier/2017/07/20/benefits-of-telecommuting-for-the-future-of-work/#6abb911916c6

Tip 1

Password protect everything

Protect your devices

All your digital devices should be password-protected. A tricky password or biometric login makes it much harder to break in. If your password is simple, it's easy to open your device and access your personal information – putting you at risk of identity theft.

Protect your online accounts

It's tempting to use the same password for all your online accounts. But if you are hacked, it means all your accounts are vulnerable. The solution is to use a password manager. That way, you have the security of using passwords, without needing to remember them all.

The same goes for security questions – the questions you're asked in case you forget your password. These can be really easy for hackers to find out, so create false answers and store them in your password manager. For an additional security measure, turn on two-factor authentication for any site that supports it.

Tip 2

Keep your computer virus-free

If your device becomes infected by a virus or malware, hackers can use it to dig through your data and steal your identity or lock up your files and demand a ransom to return them. Running an antivirus program protects your devices. It’s also good practice to keep your software up to date with the latest security patches - you can make this task easier by configuring updates to download automatically.

Tip 3
Secure your browser

Turn off cookies

Advertisers use cookies to see where you've been and use this information to tailor the ads they show you. Hackers have similar habits and will use cookies to follow you around the web. Find out how to block cookies on **Chrome**, **Edge**, **Internet Explorer**, **Firefox** and **Safari**.

Disable JavaScript

Another way advertisers and hackers track you is through JavaScript. You can disable JavaScript to keep them at bay, but it might stop some web pages from working. In this situation, you need to balance security risk with the disruption it will cause to workflow. If disabling JavaScript will protect your business more than it will affect productivity, then removing it could be the right choice.

Be wary of public wifi

When you're out and about browsing, be wary of public wifi. Connections can be intercepted by someone else on the network, allowing them to access data on your device. When you're working remotely, it's safest to skip public wifi and find a secure network.

Tip 4

Be switched on to scams

Scammers are getting better at mimicking businesses – and that makes them much harder to spot. So beware of websites, phone calls and emails that try to extract your personal information. Scams often pressure you to act. If you feel stressed, take a step back and ask to hand over your details later – a legitimate company should be willing to wait.

Tip 5

Only use software you trust

Make sure the software you install on your device comes from a trustworthy source.

After all, if you don’t know where your software comes from, you can’t know what it’s really doing to your device. Even software that looks legitimate can be a scam, so always choose your software and apps from a trusted developer.

And when it comes to apps, consider what they’re asking to access. Apps can ask for permissions to use various things on your phone, like your camera, microphone and files. These are often needed for the app to function but make you more vulnerable to hacking. If an app is making too many access requests, look for alternatives.

Learn how Surrey & Sussex police saved an estimated £7 million annually, cut two hours of admin per shift per officer and made the roads safer in the process.

Discover more

Tip 6

Train your users

Establish a culture of security awareness within the organisation. Train your users to identify phishing attacks, set strong passwords and protect their devices. People are more likely to act if they feel empowered to prevent cyberattacks themselves.

Tip 7

Stop auto-forwarding emails

Once hackers gain access to a mailbox, they can steal mail from it via auto-forwarding. This can happen even without the user even knowing, so it’s best to configure a mail flow rule.

Why O_2 for your business

Choosing a service provider is a big decision for any business. Get it right, and you can accelerate growth. Get it wrong and you can create as many challenges as you can solve. So we're here to help you get it right, with the right network, service, and flexibility for your business.

Award-winning coverage[1]

We were voted Best Network for Coverage in the Uswitch Mobile Awards for 3 years running, from 2018 – 2020[1]

Unrivalled service

Dedicated business service teams and expert Digital Advisors provide the advice and support your business needs

Greater flexibility

We help your business thrive with solutions you can tailor to your needs

[1] Best Network for Coverage: Uswitch 2018, 2019 and 2020 Awards. uswitch.com/mobiles/broadband-and-mobile-awards/

Meet our dedicated Digital Advisors

Your business is close to your heart. So our Digital Advisors get close to the heart of your business. They’re dedicated experts, helping you make the most of tech, so your people are free to work more flexibly and productively. Whatever your business needs, we can help.

Get in touch with a Digital Advisor today and discover how you can improve your security.

Published in February 2020. All information is correct at time of going to print.

Telefónica UK Limited. Registered in England no. 1743099. Registered Office: 260 Bath Road, Slough, SL1 4DX

O2 business