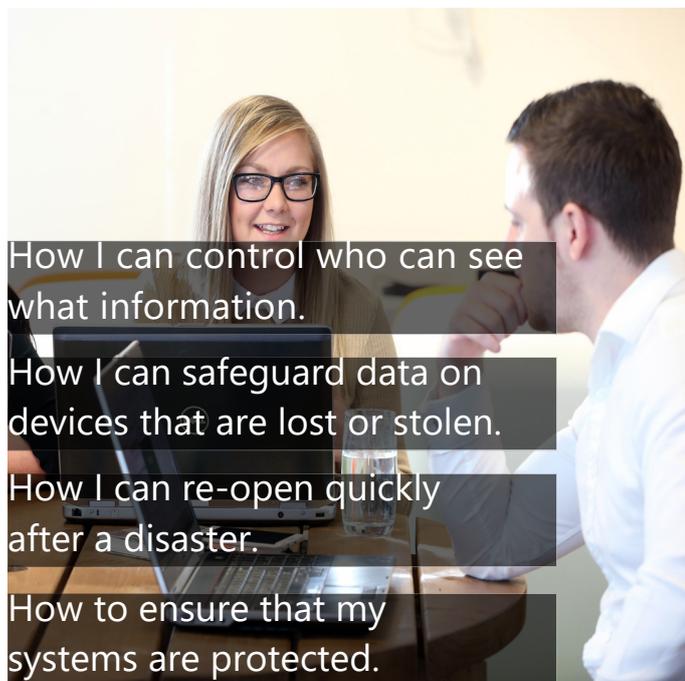# Safeguard Your Business

Why is it important to safeguard your business?

The internet brings such a huge scope of business benefits and opportunities; from the email orders you receive to your e-billing system, the internet is intrinsic to your business. However, did you know that 60% of SMEs in 2014 experienced a cyber breach with the average cost of the worst breaches ranging from £65,000 - £115,000 (HM GOV). It can happen to anyone, even you. Lost or stolen mobile devices can result in lost company files and data. Malicious hackers or malware can disrupt business and steal critical data and systems can go down unexpectedly. But you can help keep your data protected, control access to information, and restore your systems with technologies built with your security in mind.

What do you want to learn today?

How I can control who can see what information.

How I can safeguard data on devices that are lost or stolen.

How I can re-open quickly after a disaster.

How to ensure that my systems are protected.

Safeguarding your business

Employees want the freedom to access the applications and data they need on whatever device they choose – whether at the office, at home, or on the road. At the same time, you need to make sure data is protected and available only to the people who should have access.

Microsoft provides built-in security features at every level of your technology platform, from mobile devices to PCs to servers. Because it's all Microsoft, you have peace of mind that it works together—and that the right people can access files and information.

Microsoft builds resiliency and recovery capabilities into its products and technologies, from server software to the cloud, to PCs and devices. So you can be confident your business can get back up and running, even if disaster strikes.

8 Top Security Tips

1 Download software updates
Download software and app updates as soon as they appear. They contain vital security upgrades that keep your devices and business information safe.

2 Manage user privileges
Be careful who you dedicate user privilege rights to. Restrict staff and third parties access to your IT equipment, systems and information. Keep items physically secure to prevent unauthorised access.

3 Malware protection
Install anti-virus software on all devices to help prevent infection. Your computers, tablets and smartphones can become easily infected by viruses or malware.

4 Use strong passwords
Create a strong password using a lower and upper case letters, numbers and special characters. A combination of these will make your passwords hard to break.

5 Delete suspicious emails
Be careful to delete suspicious looking emails. They may contain fraudulent requests for sensitive information or links to viruses.

6 Manage removable media
Restrict the use of removable media such as USB drives, CDs and DVDs. To protect this data, look to move to the cloud where you will be able to access your data from any device, location and choose who to share your documents with.

7 Train your staff
Make your staff aware of cyber security, threats and how to deal with them. The Government offers free online training courses for you and your staff which take around 60 minutes to complete.

8 Count on the reliability of the cloud
Get right back to work when you rely on the financially backed 99.9% uptime service guarantee for Microsoft online services like Office 365 and Microsoft Azure.

"It's hard to fully quantify all the benefits Office365 has brought to Boyes Rees. It works well for us and we can rest with the knowledge that our data is safe – and that's all that's important!"
– Russell Baker, Boyes Rees Architects

How Net Support UK can help
We're there to help you every step of the way. Contact us today to get started in safeguarding your business with services and technologies from Microsoft.

netsupportuk

Contact information
Net Support UK Ltd
Charnwood House, Collivaud Place,
Ocean Way, CF24 5HF
Call us: 029 200 22 300
Email: enquiries@nsuk.com