Cyber Security Tips for Small Businesses

28%

Data breaches that involve small-medium sized businesses

165,000

cyber attacks attempted every day on SMEs

£8,460

Average cost of cyber security breaches in 2021

83%

Cyber attacks identified in 2021 were phishing attacks

Employee Awareness

With human error still the number one cause of cyber breach, training employees to use devices safely and know how to spot threats is vital. Formal policies are a good way to ensure your staff understand rules and best practices within your organisation, and can be integrated into your onboarding process, but many SMEs do not even have cyber security policies.

Only **13%** of small businesses train their staff on cyber security, with **17%** testing employees' responses to data breaches

Cyber security 'Live Fire' exercises are a good way to test the speed and effectiveness of an organisation's response to a cyber attack and encourage employees to learn what roles and responsibilities they must take on.

31%
of SMEs have cyber security policies

Check out these resources:
NCSC - Top Tips for Staff
KnowBe4

Access Control

Restricting access privileges will reduce risk of cyber breach for your business as hackers will have fewer entry points to access important data. The general rule is:

"Only allow a user access to that which they need to perform their specific job role or function."

32%

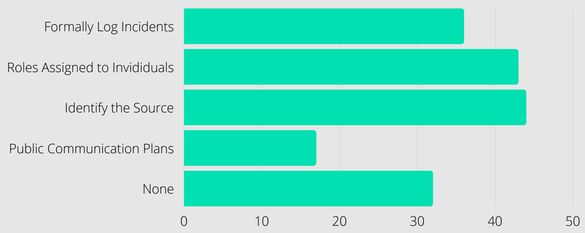
Businesses that monitor user activity

The number of admin users should be limited, with regular audits to review access controls carried out. For Office 365 users, Microsoft recommends that businesses have between 2-4 admins.

Incident Response

Most businesses (66%) do report having some kind of response process in place, but these are not usually very comprehensive. SMEs have to be prepared for a cyber attack and how they will respond to both the short and longer-term effects.

66%



36%
still take no action to prevent future attacks after being targeted

Cyber attacks can impact your business in several ways and its important to be prepared for all of them

Damage to Reputation
How will you regain trust of suppliers, partners & customers?

Monetary Loss
This could arise from theft, loss of sales, and regulatory fines.

Legal and Compliance
If you failed to comply with data laws, you could face legal consequences.

77%

of SMEs say that their cyber security is a priority

Small businesses are starting to acknowledge the cyber threat, but many after it's too late. Take action and protect your business *before* an attack by implementing these key steps and improving your overall security maturity.

CYBER TEC SECURITY

Vulnerability analyses and framework assessments can help SMEs uncover gaps in their security and better protect against malware.

15%
SMEs run vulnerability audits

Data Protection

43% of businesses have a policy to apply software updates within 14 days. Operating on end-of-life systems instantly increases your cyber risk and should be avoided.

Sectors that are most likely to hold customer personal data include finance, insurance, health, social care and real estate.

88%

Businesses that backup data in some way

It is important to backup data regularly, and keep backups in a restricted location, either on an external drive or the Cloud

Fewer businesses have rules around data storage and transfer in 2021. These policies are vital for protecting data. Consider who you share your data with and ensure they too have measures in place.

Malware Protection

SMEs need to have basic controls in place that cover malware protection. Meeting cyber security standards like Cyber Essentials is a good way to ensure this.

Other best practices for protecting against malware include switching on your firewalls and ensuring you have anti-virus software installed and activated.

Password Security

- Change all default passwords
- Use non guessable passwords that include a mixture of character sets
- Where given the option, always use multi-factor authentication
- Utilise account lockouts if passwords are entered incorrectly too many times
- Ensure passwords are at minimum 8-12 characters long
- Keep a written password policy to guide employees on rules and best practice

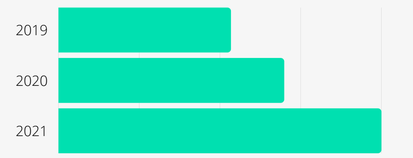
21%

of us use different passwords for every platform

2.5m

use the password 123456, according to Nordpass

Password managers are a useful way to keep track of passwords across multiple platforms



No. Google searches for Password Manager