CyberSmart

Cybersecurity training for small businesses:

a step-by-step guide

cybersmart.co.uk

Contents

Cybersecurity training for small businesses:

A step-by-step guide

When it comes to cybersecurity, small businesses are often perceived as easier targets. This is because they lack the resources to protect themselves.

The solution to this, however, is simpler than you might think.

Forget about expensive security systems and complex technical solutions. You already have the most powerful cybersecurity tool in your business – your team.

Let's explore how to create and implement cybersecurity training for small businesses in five practical steps.

Step 1. Assess your cybersecurity needs

Step 2. Choose your focus area

Step 3. Create a training schedule

Step 4. Select your delivery method

Step 5. Implement cybersecurity tools and resources

Step 1. Assess your cybersecurity needs

Before you launch a training programme, find out what you need to protect and identify your biggest threats.

Analyse past incidents

Two-thirds of businesses that fall victim to a cyberattack are likely to experience another one within a year. So, it's essential to review any previous security events to identify patterns and vulnerabilities.

Identify valuable data

Customer information, financial records, intellectual property, and operational data all need different levels of protection.

Evaluate existing knowledge

Test your team's current security awareness to establish a baseline. This will help you identify knowledge gaps and measure improvements.

You can do this with:

- Surveys about security practices
- Phishing simulations
- Password policy reviews
- Compliance check

Consider industry-specific threats

Different sectors face unique challenges. Finance, for instance, is the most advanced sector in terms of cybersecurity due to extensive regulatory requirements in Europe and the US.

Step 2. Choose your focus areas

Based on your assessment, prioritise training areas that help your team protect your biggest digital assets.

Here are some areas you may choose to focus on:

Password security

Cybercriminals don't need sophisticated hacking tools when weak passwords give them an open door into your systems. A look at the 10 most common passwords in the UK shows most people opt for weak passwords.

Most common passwords in the UK

- password
- qwerty123
- qwerty1
- 123456
- liverpool
- 123456789
- password1
- qwerty
- liverpool1
- arsenal

Train your team to create strong, unique passwords for each account. However, strong passwords alone aren't enough in today's threat landscape, which is why we encourage multi-factor authentication (MFA).

Multi-factor authentication

MFA adds a crucial second layer of protection that prevents unauthorised access even if passwords are compromised. Many organisations face regular brute force attacks, but those using MFA remain secure because attackers can't provide the authentication app code, SMS message, or email verification required alongside the password.

Ensure your team enables MFA on all business accounts and understands that this simple step dramatically reduces the risk of account compromise.

Phishing and social engineering

Nearly half (46%) of organisations affected by cyber-attacks in the last year say an employee was the first point of entry via social engineering.

Statistics like this underline the importance of teaching your team how to spot suspicious messages and telltale signs, such as:

- Urgency
- Generic greetings
- Suspicious sender addresses

Consider implementing a phishing simulator as part of your training platform to test and educate employees on the latest phishing tactics. These tools send realistic but harmless phishing emails to staff, tracking who clicks and providing immediate educational feedback.

Mobile device security

With 60% of organisations now expecting staff to use mobile devices for work, mobile security can't be overlooked. Surprisingly, 59% of SMEs don't provide mobile cybersecurity training to employees, despite being the fastest-growing point of entry for cyber-attacks.

To mitigate the risks associated with mobile devices, implement mobile device training that covers:

- Device updates
- App security
- Public Wi-Fi risks
- Device protection
- Data backup
- Remote wiping

Data handling

Data is the lifeblood of your business, and proper handling is essential for security and compliance. Data theft is the most common goal of malware, especially for attacks that target small to medium-sized enterprises. However, the mishandling of data is still a greater threat and is the number one contributor to data breaches.

Data classification

Teach your team to recognise different categories of data sensitivity and handling requirements.

For example:

Level	Description	Examples	Handling requirements
Public	Can be freely shared	Marketing materials, website content, press releases	No restrictions, freely distributable
Internal	For company use only	Employee directories, procedures, internal communications	Keep within the company, no external sharing without approval
Confidential	Sensitive information	Financial data, customer info, business strategies	Password protection, limited access, two-factor authentication and encryption recommended
Restricted	Highly sensitive	Payment data, credentials, trade secrets, legal documents	Strict access controls, strong encryption, and audit trails

Legal requirements

Ensure employees understand the basics of relevant data protection laws like GDPR and their personal responsibilities.

3. Create a training schedule

Cybersecurity training for small businesses isn't a one-and-done deal. Threats change all the time, so training needs to be an ongoing task.

Consider these approaches:

Initial onboarding

Provide comprehensive security training for all new hires during their first week. This establishes security as a priority from day one and ensures everyone starts with the same foundational knowledge. Cover your security policies, tools, and threats relevant to their role.

Regular refreshers

Schedule quarterly or monthly short training sessions (15-30 minutes) focused on specific topics.

Did you know?

"Ghost" or "phantom" tax preparers is a growing (and frightening) cybercrime where fraudsters pose as tax professionals, collect your personal information, file false returns, and vanish with your refund.

Just-in-time training

Deliver specific guidance:

- At financial year-end when phishing attempts increase
- Before major holidays when scams spike
- When new threats emerge that target your industry
- After security incidents, to prevent recurrence

Micro-learning moments

Send weekly security tips via email or company messaging platforms. These quick reminders (1-2 minutes to read) keep security top-of-mind without disrupting workflow.

Comprehensive annual reviews

Cover all topics to reinforce knowledge and update on new threats. This is also a good time to review and update your security policies.

Targeted training

Provide additional specialised training for high-risk roles (like finance staff) or for employees who have demonstrated vulnerability in simulated phishing tests.

Step 4. Select your delivery method

Match your training approach to your team's preferences and organisational context. Different delivery methods work better for different topics and audiences, so consider using a mix.

In-person workshops

Interactive sessions work particularly well for complex topics. They provide immediate feedback and create a shared experience. Informal lunch-and-learn sessions are a good way to keep engagement high.

Online courses

Self-paced learning that fits around work schedules is excellent for distributed teams. Look for courses designed specifically for small business environments, as these will be more relevant than enterprise-focused content.

Simulated phishing exercises

Send fake phishing emails to test knowledge and identify who needs additional support. These practical exercises reveal how well your team reacts in real-world situations. Make sure to follow up with constructive feedback rather than punishment when employees fall for these tests.

Microlearning

These bite-sized pieces of content (2-5 minutes each) are perfect for reinforcing key messages without overwhelming busy colleagues. They can include quick videos, infographics, or scenario-based questions.

Team discussions

Hold regular security talks in team meetings to maintain awareness. These normalise security conversations and allow colleagues to share their experiences and questions. They're also a great opportunity to acknowledge and praise security-conscious behaviours you've observed.

Storytelling

Share real examples (anonymised if necessary) of security incidents that affected similar businesses. Stories are more memorable than abstract concepts and help employees understand the real-world implications of security practices.

Step 5. Implement cybersecurity tools and resources

Support your training with tools that make cybersecurity easier.

Password managers

Tools like LastPass, 1Password, or Bitwarden securely store unique, complex passwords for each site, meaning employees only need to remember one master password. This improves security while making life easier for your team.

Security awareness platforms

Consider platforms specifically designed for cybersecurity training for small business environments. These provide ready-made content, track completion rates, and often include simulated phishing tools.

Clear policies

Document security expectations in straightforward language. Avoid technical jargon and focus on what employees need to do.

Technical protections

Implement tools that help enforce security best practices, such as:

- Email filtering to catch obvious phishing attempts
- Automatic software updates to patch vulnerabilities quickly
- Endpoint protection to detect and block malware
- Access controls to ensure employees can only access what they need

Incident response plan

Lack of incident response preparedness is among the top three challenges to cyber resilience for small businesses. Creating a simple guide for what to do when something goes wrong should be a top priority.

Your plan should include:

- Who to contact (with multiple contact methods)
- What information to gather about the incident
- Immediate actions to take (like disconnecting affected systems)
- Brand protection guidelines

Strengthen your defences with cybersecurity certifications

Different cybersecurity certifications exist for every business size and need. Whether you're ready for the comprehensive ISO 27001 or starting with Cyber Essentials, there's an option that fits your small business.

Other than providing the obvious security benefits, cybersecurity certifications also:

- Demonstrate your commitment to protecting client data
- Instil confidence in customers and partners
- Make you eligible for government contracts that require suppliers to hold certifications
- Help lower insurance costs
- Satisfy government and industry regulations, such as GDPR

Overcome the big cyber threats

98.5%
Reduction in cyber risk for organisations holding Cyber Essentials certification

92%
fewer insurance claims made by organisations with Cyber Essentials

91%
of businesses report improved confidence in their ability to reduce cybersecurity risks

facing your small business

Your business may be small, but the cyber threats it faces aren't. Effective cybersecurity training for small businesses isn't just about transferring knowledge, it's about transforming behaviour.

Read the guide

cybersmart.co.uk

CyberSmart