Website Security Basics for UK SMEs

Executive Summary

- Securing your website promotes confidence in customers and continuity in your business.
- Most small to medium-sized enterprise (SME) websites are compromised due to either being out of date, or caused by weak passwords.
- SSL (HTTPS), back-ups and regular updates are the key fundamental blocks of security.
- The quality of your hosting provider has a major impact on your site's overall security.
- The General Data Protection Regulation (GDPR) will apply if you are gathering personal data through your website.
- Even small changes can have a significant effect on reducing your risk.
- Continual monitoring is important, rather than a once-off fix.
- You do not need to be a technical person to improve the security of your website.

Who This Guide Is For

- UK SMEs (1-50 employees)
- Owner-managed businesses
- Marketing managers that are responsible for websites
- Any non-technical decision maker

What You Will Achieve

- An understanding of what the most significant website security risks are;
- Get a general impression of what a "good enough" standard would be;
- Providing you with practical steps to make the necessary changes;
- Knowing when it is appropriate to bring in professional assistance.

Section 1: Why Website Security Matters (UK Context)

Why you should care about security

- Reputation and Trust
- Investigative Agencies
- Protecting Your Customers Information
- (Your GDPR obligations)
- The impact downtime has on small companies
- Cyber Insurance Expectation
- UK Examples (no false information)

- Example: 10 person Consultancy Website Compromised From Using Outdated Plugin

Section 2: Common Website Threats Facing UK SMEs

There are many risks that websites have to deal with every day due to people making simple mistakes. Below is a simple definition of what each of these means:

1. **Malware:** Malicious software that gets into your site (often through outdated code), steals data, sends unsolicited e-mails or re-directs visitors to another site etc., UK SMEs have incurred 40% of all reported breaches (according to ICO data).
2. **Phishing:** Fraudulent e-mail messages that trick staff members into giving away their login credentials to the phisher, after the phisher has had their credentials/identity confirmation emailed back to them, they would have access to modify the information and take customer's private details e.g. common within property or retail website activities.
3. **Ransomware:** Encrypts a website or related files and asks for payment. Reported to be 50% on the increase as indicated by NCSC by 2025; generally occurs via unsecure plugins etc.
4. **Brute Force Attacks:** Automated guessing of passwords for administrative access (i.e. to CMS; for example: WordPress).
5. **Outdated Plug-ins/Theme:** Plug-ins and themes that have not received updates create vulnerabilities. As an example (as of 2025), 60% of reported breaches for SMEs were from out-dated plug-ins/themes by ICO.

Generally these threats all start as small problems, but as they grow larger, they have a greater impact on Customer personal data and/or on your compliance with GDPR.

Section 3: Key Security Measures

Essential measures explained simply: I will describe each measure as follows: Definition, Implementation minimum (Free/DIY), Better (Low-Cost), Best (Managed), Common Errors (Mistakes), and Quick Wins (Best method of implementing).

1) Regular Software Updates

Definition: Updates that you apply to your CMS, Plugin, or Hosting environment to ensure that you have the latest security patches to resolve an identified vulnerability.

Implementation:

Minimum: Log into your website once a week and check for any updates in the WordPress Dashboard for your Site.

Better: Enable the automatic updates for minor patches; install a Plugin such as UpdraftPlus to remind you to check for updates.

Best: Use a Managed Hosting Provider (i.e., Site-Ground) that automatically applies all updates.

Common Errors: Ignoring Minor Updates. Minor updates often resolve security vulnerabilities that could impact your website.

Quick Wins: Set a calendar reminder to log in once weekly to check for updates; test all updates first in the staging environment if you're able

2) Firewall Protection

Definition: A barrier that blocks malicious traffic from being routed to your Website (like a doorman at a bar).

Implementation:

Minimum: Use Cloud-flare (Free) as your Basic Firewall.

Better: Install the Word-fence (Free) Plugin to create rules specific to your website.

Best: Use a Paid Web Application Firewall (WAF) from Sucuri (£200 per year).

Common Errors: Not configuring rules correctly; leaving rules in default mode may not provide adequate protection against threats common to UK businesses.

Quick Wins: Use the free version of Cloud-flare today; Block any known bad IP Addresses.

3) Secured Plugins & Themes

What it is: Choosing and managing add-on's without introducing risk.

How to implement:

Minimum: Use only reputable sources (WordPress.org); remove ones that are not in use.

Better: Scan with free tools like WPScan; limit to only necessary plugins.

Best: Audit with a professional tool like Patchstack (£100 per year) annually.

Common mistakes: Installing pirated themes as they can contain malware.

Quick wins: Remove 2-3 unused PlugIns immediately, read reviews prior to installing them.

4) User Input Validation

What it is: Checking forms/contact pages against malicious coding (i.e. SQL injection).

How to implement:

Minimum: Use built in CMS functions; add CAPTCHA to your forms.

Better: Install Anti-Spam Plugin such as Akismet (free for basic).

Best: Custom code review if using developers.

Common mistakes: Leaving default forms open (as bots can take advantage of them).

Quick wins: Add reCAPTCHA to your contact form (provided free by Google).

5) Malware Scanning

What it is: Regularly checking for hidden threats.

How to implement:

Minimum: Use free online scanner (i.e. Virus Total).

Better: Run free scans with Word-fence or Sucuri weekly.

Best: Use a paid service to automate daily scans (£50 per month).

Common mistakes: Scanning only after problems occur (prevention is important).

Quick wins: Run a free scan this week and create alerts!

Section 4: Hosting & CMS Considerations

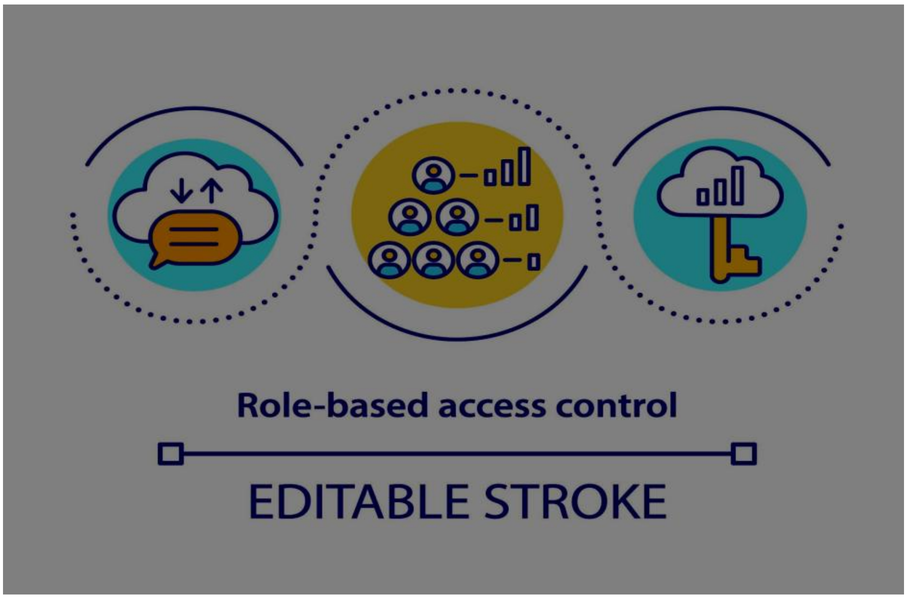
- WordPress Vs. Other Content Management Systems
- Custom Built Websites
- Managed Hosting Vs. Unmanaged Hosting
- Domain Registrars Security
- Domain Name System (DNS) Security

Example:

- E-commerce Business in the Market with 30 Users that Used an Unsecured Version of Woo-commerce Plugin has been Compromised

Section 5: Passwords & Access Control

- Review all Administrators have Access to Your Site
- Role Based Access to Users
- Remove User Access from All Shared Administrator Accounts
- Create a Leaver Process for All Website Administrator Account Access
- Multi-factor Authentication (MFA) Implementation Checklist



Section 6: SSL/TLS & HTTPS (Deeper Practical Guide)

- Certificate Verification
- Redirect from HTTP to HTTPS
- Details on Mixed Content
- Using Browser Developer Tools for Verification

Section 7: Backup Strategy & Disaster Recovery (Expanded)

- Daily Backups versus Weekly Backups
- Off-site Backups

- Immutable Backups (Concise Overview)
- Ordering of Recovery Time (RTO) & Recurring Purchase Orders (RPO) from the Websites Perspective.
- Testing Backups on a Quarterly Basis.

Section 8: 30-Day Implementation Plan

Days 1–7	Days 8–15	Days 16–30
Immediate Risk Reduction	**Strengthen Defences**	**Formalise & Document**
• Enable HTTPS • Change admin passwords • Delete inactive accounts • Enable Data Backups • Update CMS and all plugins	• Enable Multi-Factor Authentication • Review Hosting Service • Configure Firewall (if available) • Review Forms on Site	• Create a website security checklist for reference. • Schedule regular maintenance checks on a monthly basis. • Conduct a review of Privacy Notice and disclose the use of cookies by your website(s). • Test the effectiveness of your backup by attempting to restore it.

Implementation Checklist (tick as done):

- ➢ MFA enabled
- ➢ SSL enabled
- ➢ Updates current
- ➢ Backups established
- ➢ Scan conducted
- ➢ Privacy policy revised
- ➢ Monitoring tool deployed
- ➢ Staff educated

FAQ

- ➢ **What is the cost for basic website security?** Most free resources provide sufficient coverage. A reasonable price range for other solutions is £20-£50 per month.
- ➢ **Is it possible to secure your own website?** Yes. Free internet resources (ex WordPress guides) can help you do it. You may need to hire someone if your site is complicated.

- **What do I do if my website is hacked?** Upon discovery, take steps to contain the threat (change passwords), scan your website, restore from backup, and report to ICO (if personal data was compromised).
- **Does GDPR apply to my simple website?** Yes, if your website collects any personal data (ex contact forms).
- **Is WordPress secure enough for a SME?** Yes, assuming you are applying all necessary updates and/or plugins. If you will not maintain an updated WordPress site, do not use it.
- **How frequently do I need to run a backup?** Dynamic websites require a backup at least every day. Static websites should have a backup at minimum once per week.
- **What is the best way to scan my site for viruses?** Sucuri or Word-fence provide free versions of their scanning software.
- **Do I need a firewall?** Yes, I recommend that you start with the free version of Cloud-flare.
- **How do I use plugins safely on my site?** Only install a plugin from a trusted source, and make sure you are regularly updating it.
- **What should I do for e-commerce website security?** Make sure you are PCI compliant for payment processing, and that you are using secure payment gateways such as Stripe.
- **What types of tools do I need to run a test on my website?** You can use free tools such as Mozilla Observatory to run tests on your website.

About This Guide

This manual “Basic Website Security for UK SMEs (2026)” was produced by **Computer Support Centre**, a UK US-based information technology and cyberspace organisation that assists smaller businesses in producing safe websites and ensuring that their programs operate successfully at low cost.

The purpose of this book is to instruct non-technical SMEs on how to secure their website based on practical advice requested by many SMEs within NCSC/ICO guidance and issues that are customary between the years 2025, 2026.

The types of services we offer are:

- Simple website security checks;
- WordPress upgrades and plug-in audit;
- SSL certification, backup and monitoring;
- GDPR draughts and cookie fixes.

Contact us by texting or using one of the below-listed methods to request a FREE 15 minute website security scan or obtain quick website assistance.

Computer Support Centre

visit https://computersupportcentre.com.

Conclusion

If you focus just on the basic principles of website security, such as using strong passwords with multi-factor authentication (MFA), performing regular updates, implementing free SSLs, making good backups and performing monthly audits, you will significantly reduce the risks associated with exposing customers to unauthorised access to their data, non-compliance with GDPR guidelines and business failure due to operational issues all at a very low cost to your business.

Start small by selecting one of the many quick wins from your 30-day action plan and building on that success. Good luck; you can do this!