What Hackers See When They Look At Your Website

A guide for UK business owners who think "it won't happen to me"

PulseShield | 2026

1. The 30-Second Recon

Before a hacker ever tries to break into your website, they spend about 30 seconds gathering intelligence. They don't need special skills. They don't need expensive tools. Everything they need is free, legal, and available to anyone with a web browser.

In the time it takes to make a cup of tea, someone can determine what software your website runs on, what email provider you use, whether your security headers are configured, and which of your systems are exposed to the internet.

This is called reconnaissance. And it happens to your website **every single day**.

> **Automated scanners probe millions of websites 24/7. Your site has almost certainly been scanned already this week — you just weren't told about it.**

2. The Numbers Don't Lie

Here are the facts about UK small businesses and cyber crime:

43%
of UK cyber attacks target small businesses

£8,460
average cost of a single breach

60%
of SMBs close within 6 months of a serious breach

4 in 10
UK businesses have no security plan at all

Sources: UK Government Cyber Security Breaches Survey 2025, Hiscox Cyber Readiness Report

3. Open Ports: The Doors You Forgot to Lock

Every server has ports — numbered doorways that allow different types of connections. Ports 80 and 443 serve your website. But what about port 22 (SSH)? Port 3306 (MySQL)? Port 8080 (admin panels)?

Hackers scan all 65,535 ports on your domain in seconds. Every open port is a potential entry point. If it's running outdated software with a known vulnerability, they're in before you finish reading this sentence.

WHAT THEY SEE

A list of every open door into your server.

Most businesses have 2–3 ports open that they don't need, don't use, and don't realise are there.

4. Security Headers: The Warning Signs

When your website responds to a visitor, it sends invisible instructions that tell browsers how to handle your content. Security headers are like signs on a building: "CCTV in operation", "Alarm system active", "Staff only beyond this point".

When these headers are missing, it tells attackers that your website was set up without security in mind. It's the digital equivalent of a building with no locks, no cameras, and a side door wedged open.

- **Strict-Transport-Security** — forces HTTPS connections
- **Content-Security-Policy** — prevents malicious code injection
- **X-Frame-Options** — stops clickjacking attacks
- **X-Content-Type-Options** — prevents MIME-type attacks
- **Permissions-Policy** — controls browser feature access

> **Over 60% of UK business websites are missing at least 3 critical security headers. That's like leaving 3 doors unlocked — and the burglars know exactly which ones.**

5. Cookie Compliance: The ICO's Low-Hanging Fruit

The Information Commissioner's Office (ICO) enforces cookie consent rules under GDPR and PECR. Non-compliance isn't just a legal risk — it's the easiest thing for attackers to spot, and the easiest thing for regulators to fine you for.

Hackers check if your cookie banner actually blocks trackers before consent. They check if analytics cookies fire without permission. They check if third-party tracking scripts load in the background regardless of what the user clicked.

WHAT THEY SEE

Whether your website respects visitor privacy — or just pretends to.

> **ICO fines** for cookie consent failures can reach £17.5 million or 4% of annual turnover. In 2024, multiple UK businesses received enforcement notices for exactly these issues.

6. Email Security: Your Weakest Link

Most businesses focus on their website and forget that email is the #1 attack vector. Hackers check your DNS records for SPF, DKIM, and DMARC — the three protocols that prevent someone from sending emails that look like they came from you.

Without these records, a hacker can send an email to your customers from **invoices@yourdomain.co.uk** and it will look completely legitimate. Your customers click the link, enter their bank details, and the damage is done.

WHAT THEY SEE

Whether they can impersonate your domain in a phishing attack.

7. DNS Records: Your Business Card for Attackers

Your DNS records are public. Anyone can look them up. They reveal your email provider, hosting company, domain registrar, and sometimes your internal network architecture. It's like taping a map of your office to the front door.

Hackers use this to build a complete picture of your digital infrastructure before they ever attempt an attack.

WHAT THEY SEE

A complete map of your online infrastructure.

8. Exposed Files & Admin Panels

Many websites accidentally expose sensitive files and admin panels to the public internet:

- WordPress login pages at **/wp-admin**
- Database management tools like **phpMyAdmin**
- Configuration files (.env, config.php, web.config)
- Backup archives (.sql, .zip, .tar.gz)
- Server status pages revealing internal details
- Development and staging environments
- API documentation with endpoint details

Attackers run automated scripts checking hundreds of these paths on thousands of websites simultaneously. If yours returns a "200 OK", it goes straight on their list.

9. The Attack Timeline

Here's how long each phase takes when someone targets your business:

30 seconds	**Reconnaissance**	Scan your ports, headers, DNS records, exposed files
2 minutes	**Vulnerability matching**	Match findings against known exploit databases
5 minutes	**Weaponisation**	Prepare a targeted attack specific to your setup
1 minute	**Delivery**	Send a phishing email using your own domain
Under 10 min	**Total time to compromise**	From first look to full access

> **The average time to detect a breach is 197 days. If someone got in today, you probably wouldn't know until November.**

10. What You Should Do Next

You don't need to become a cybersecurity expert. But you **do** need to know where you stand. A professional security assessment takes minutes and gives you a clear picture of what hackers would see if they looked at your website today.

Think of it like a health check for your business. You wouldn't ignore a lump because you "probably don't have cancer". Don't ignore your website security because you "probably won't get hacked".

Find out what hackers see on your website.

Get a professional PulseShield security assessment.
We show you exactly what an attacker would find — before they find it.

Statistics sourced from UK Government Cyber Security Breaches Survey 2025 and Hiscox Cyber Readiness Report.

PulseShield

Professional website security for UK businesses