WEB HOSTING CYMRU / CUSTOMER RESOURCE

Website Security & Maintenance Health Check

A practical workbook to help you understand, review and protect your business website.

Website / business details	Complete below
Business name	_____
Website address	_____
Date completed	_____
Person completing this review	_____
Next review date	_____

How to use this workbook

Work through each question and tick Yes, No, Unsure or Not Applicable. If you are unsure, ask the person who manages your website or hosting. Record follow-up actions at the end. You do not need to be technically experienced to complete this exercise.

Important: This is a self-assessment, not a malware scan, professional security audit or guarantee that a website is secure. Never record passwords, recovery codes or private customer data here.

What to do first

Identify who manages your domain, hosting, website software and backups. They may be different people or organisations.

01 / Software and maintenance

Updates reduce exposure to known vulnerabilities, but changes should also be checked for compatibility and website functionality.

Security check	Yes	No	Unsure	N/A
Website platform or CMS is supported and up to date	[ ]	[ ]	[ ]	[ ]
Plugins, themes and extensions are kept current	[ ]	[ ]	[ ]	[ ]
Unused software is removed rather than merely forgotten	[ ]	[ ]	[ ]	[ ]
Updates are checked for compatibility and site functionality	[ ]	[ ]	[ ]	[ ]
Someone is responsible for regular maintenance	[ ]	[ ]	[ ]	[ ]
There is a record of significant website changes	[ ]	[ ]	[ ]	[ ]
Custom code and integrations are maintained	[ ]	[ ]	[ ]	[ ]

Notes / actions: _____
_____

02 / Accounts and access

Protect every route into your online business, including your website, domain registrar, hosting control panel and email.

Security check	Yes	No	Unsure	N/A
Each administrator has an individual account	[ ]	[ ]	[ ]	[ ]
Strong, unique passwords are used	[ ]	[ ]	[ ]	[ ]
Multi-factor authentication is enabled where supported	[ ]	[ ]	[ ]	[ ]
Former staff and contractors no longer have access	[ ]	[ ]	[ ]	[ ]
Administrator privileges are limited to those who need them	[ ]	[ ]	[ ]	[ ]
Hosting, domain and email accounts are also protected	[ ]	[ ]	[ ]	[ ]
Recovery contacts and account ownership are up to date	[ ]	[ ]	[ ]	[ ]

Notes / actions: _____
_____

03 / Hosting backups and recovery

Web Hosting Cymru provides hosting backups, but a backup records a website at a point in time. If malware was present, the backup may contain it too. A restore alone may not remove an infection.

Security check	Yes	No	Unsure	N/A
I know what my hosting backups cover	[ ]	[ ]	[ ]	[ ]
I know how frequently backups are created	[ ]	[ ]	[ ]	[ ]
I know how long backup copies are retained	[ ]	[ ]	[ ]	[ ]
I have an independent copy stored outside my hosting account	[ ]	[ ]	[ ]	[ ]
I keep appropriate historical recovery points	[ ]	[ ]	[ ]	[ ]
A restore has been tested in a safe environment	[ ]	[ ]	[ ]	[ ]
I know who will investigate and restore a compromised site	[ ]	[ ]	[ ]	[ ]

Notes / actions: _____
_____

Key distinction: backed up does not always mean clean

For example, if malware entered a site weeks before it was detected, several recent backups might contain the same infection. Recovery may require investigating the cause, identifying a clean recovery point or cleaning the website before returning it to service.

Do not restore a suspected infected copy directly over a live site without assessing the risk.

Practical exercise / Create your own off-site copy

For WordPress websites, All-in-One WP Migration can export a copy of your site that you download and store independently. Its standard export workflow should not be confused with a fully automated off-site backup service. Features and limits can vary by version and extensions.

WordPress plugin: All-in-One WP Migration — WordPress.org

Step	Action
1	Confirm you have permission to export the website and that you have sufficient secure storage.
2	In WordPress, install or open All-in-One WP Migration from the Plugins area.
3	Use its Export function to create a site export. Check the export completes successfully.
4	Download the export file and store it securely outside the hosting account.
5	Record the date, storage location and person responsible. Protect access to the file: it may contain customer information.
6	Arrange a periodic restoration test in a separate, safe environment. An export file alone does not prove recovery will work.

Independent backup record

Record	Your details
Last export date	_____
Off-site storage location (not a password)	_____
Responsible person	_____
Last tested restore	_____
Next scheduled export / test	_____

Note: Store exports securely, ideally encrypted with restricted access. Retain copies according to your business and data-protection requirements. For busy websites, manual exports may not be frequent enough; consider a suitable automated off-site backup service.

04 / Monitoring and website protection

Security measures help detect problems and reduce exposure, but no single plugin, firewall or scan can guarantee protection.

Security check	Yes	No	Unsure	N/A
HTTPS works correctly across the website	[ ]	[ ]	[ ]	[ ]
Security alerts or unusual logins are reviewed	[ ]	[ ]	[ ]	[ ]
Malware or integrity checks are carried out appropriately	[ ]	[ ]	[ ]	[ ]
Website availability or uptime is monitored	[ ]	[ ]	[ ]	[ ]
A firewall or other relevant protection is configured	[ ]	[ ]	[ ]	[ ]
There is a process for responding to security warnings	[ ]	[ ]	[ ]	[ ]
Website forms and important user journeys are checked	[ ]	[ ]	[ ]	[ ]

Notes / actions: _____
_____

05 / Domains, email and business continuity

Your website depends on more than the WordPress dashboard. Domain and email access are essential to keeping your business operating.

Security check	Yes	No	Unsure	N/A
Domain renewal and ownership details are correct	[ ]	[ ]	[ ]	[ ]
Registrar access is secured with MFA where supported	[ ]	[ ]	[ ]	[ ]
DNS changes are restricted to authorised people	[ ]	[ ]	[ ]	[ ]
Business email accounts are protected	[ ]	[ ]	[ ]	[ ]
SPF, DKIM and DMARC have been reviewed where applicable	[ ]	[ ]	[ ]	[ ]
Staff know how to recognise suspicious messages	[ ]	[ ]	[ ]	[ ]
A named contact can respond if the website goes offline	[ ]	[ ]	[ ]	[ ]

Notes / actions: _____
_____

06 / Data and customer-facing functions

If your website accepts enquiries, accounts, orders or payments, review the systems and information your customers rely on.

Security check	Yes	No	Unsure	N/A
Forms are working and submissions reach the right people	[ ]	[ ]	[ ]	[ ]
Customer data is collected only where needed	[ ]	[ ]	[ ]	[ ]
Access to personal data is appropriately restricted	[ ]	[ ]	[ ]	[ ]
Payment services and integrations are maintained	[ ]	[ ]	[ ]	[ ]
Privacy and data retention arrangements are reviewed	[ ]	[ ]	[ ]	[ ]
There is a process for handling a suspected data breach	[ ]	[ ]	[ ]	[ ]

Notes / actions: _____
_____

Your three most important actions

Priority	What needs attention?	Who will act?	By when?
1	_____	_____	_____
2	_____	_____	_____
3	_____	_____	_____

Review summary

Questions marked No: _____ Questions marked Unsure: _____ Next review date: _____

Do not treat the number of Yes answers as a security score. One serious weakness can matter more than many completed checks.

Need help understanding your findings?

Web Hosting Cymru provides hosting backups as part of its hosting services. Website updates, application security, incident investigation and recovery support may require separate arrangements depending on your service. We can help you understand what is covered and what needs attention.

webhostingcymru.co.uk | Website Security Guide