

Cyber Score Card



demo.com

Your business website and email lack critical protections, risking data loss and fraud.

Key Takeaway

7

Dark Web Breaches



SCORING CRITERIA

Why it matters:

It's more cost-effective to prevent breaches by regularly scanning your external risk surface than to pay the steep price of recovering from an attack. Find and fix weaknesses before criminals can turn them into costly problems.



Email Impersonation Security
Missing valid DMARC spoofing protection to prevent email impersonations.



Website HTTP Security Settings
Missing 11 important settings to secure the site's visitor activity



Dark Web Breaches
7 accounts for sale on the Dark Web out of 20 total email addresses.



Website SSL Encryption
Website traffic is encrypted until 2025-04-22 by an SSL certificate.



Secure Email Gateway
Microsoft Exchange Online Protection gateway detected



Web Application Firewall
The site is not protected from malicious visitors.



ACTION PLAN

This is your 3 Step Cyber Action Plan to reduce security risks:

Install Web Application Firewall

Set up a firewall to block malicious web traffic and protect your site.

Implement Missing Security Headers

Add necessary headers to prevent common web threats and secure data exchange.

Strengthen Email Authentication

Configure SPF, DKIM, and DMARC to protect against email spoofing and phishing.

Cyber Score Card



DARK WEB REPORT SUMMARY

Why it matters:

Discovering your employees' work emails and passwords on the dark web spells serious trouble. It's a gold mine for cybercriminals. Armed with your team's emails and passwords from the Dark Web, they can raid your assets in seconds, not days. This isn't just risky; it's a direct threat to your business's survival.

7

Email accounts for sale on the Dark Web

20

Total Accounts Scanned

Top Accounts	Name	Position	Breaches
test1@demo.com			5
test3@demo.com			2
test_150hour@demo.com			0
test_609@demo.com			0
test_effective@demo.com			0
test12_1@demo.com			0
test234@demo.com			0
test.abc@demo.com			0
www.test@demo.com			0
86-510-510-83712953...			0

How to fix it:

By implementing Multi-Factor Authentication and ongoing Dark Web monitoring, even if passwords are exposed, your business remains sealed. Turn your vulnerabilities into strengths, safeguarding your future and setting you apart from the competition.



3 STEP ATTACK



AUTOMATICALLY
PROFILE
EMPLOYEES

FIND PASSWORDS
ON THE DARK
WEB



BREAK INTO YOUR
BANK ACCOUNTS

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.