HumanRisk Shield
HUMAN RISK MANAGEMENT

SAMPLE REPORT: A FICTIONAL COMPANY

northwind-dental.example

What an attacker sees from outside, and what to fix first. Checked 1 October 2026 from passive and public sources only.

D

EXPOSURE GRADE

61 / 100

Weak – several exposures need attention.

WHAT THIS MEANS

2 infostealer-infected credential set(s) tie to this domain – attackers may be able to log in as your people right now.

humanriskshield.com

01 / ACTION PLAN

What to fix first

8 things to fix, most urgent first. Each says who should handle it, so this page can go straight to your IT provider.

Fix this week

CRITICAL 2 LEAKED AND STOLEN PASSWORDS

Stolen passwords from infected devices

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: 2 staff accounts (r.patel@, frontdesk@) appear in infostealer logs from September 2026, with saved passwords and session cookies.

Why it matters: Password-stealing malware on a device used by your people has captured working passwords and sign-in sessions. Attackers can sign in as them today, even past some two-step checks. This is not an old breach.

WHAT TO DO

1. Treat the affected people's devices as infected: scan or reimage them before anything else.
2. Then reset their passwords from a clean device and sign them out of every session (Microsoft 365, Google, VPN).
3. Make sure two-step sign-in is on for them, and check their mailbox for forwarding rules they did not create.

Who: Your IT provider

HIGH EMAIL SPOOFING PROTECTION

DMARC monitor-only

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: DMARC is p=none: it reports but blocks nothing, so spoofed mail still lands.

Why it matters: Your domain asks receivers to do nothing about spoofed mail, so fake invoices and phishing in your name land in inboxes instead of being blocked.

WHAT TO DO

1. Check the DMARC reports that every genuine sender passes.
2. Change the policy from p=none to p=quarantine, then to p=reject.

Who: Whoever manages your domain's DNS (often your IT provider or where you bought the domain)

HIGH INTERNET-FACING HOSTS

Subdomain open to takeover

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: booking.northwind-dental.example points at an Azure web app that no longer exists (northwind-booking.azurewebsites.example).

Why it matters: A name on your domain still points at a cloud service you no longer use. Anyone can claim it and run a fake site on your own domain.

WHAT TO DO

1. Delete the DNS record that points at the service you no longer use, or reclaim that service.

Who: Whoever manages your domain's DNS (often your IT provider or where you bought the domain)

HIGH 7 LEAKED AND STOLEN PASSWORDS

Staff addresses in data breaches

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: 7 of 14 staff addresses appear in 9 known breaches; 4 of those breaches included passwords.

Why it matters: Staff addresses appear in known data breaches. Passwords from breaches are tried against your email, VPN and other logins until one works.

WHAT TO DO

1. Ask each listed person to change their work password and any personal password they reused it on.
2. Turn on two-step sign-in for every account that offers it.
3. Your IT provider can force a reset for anyone who does not.

Who: Each affected person, with your IT provider

HIGH 2 LOOK-ALIKE DOMAINS

Look-alike domains that can send mail

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: northwind-dental.example (capital i for l) and northwinddental.example have mail servers set up; registered 12 and 40 days ago.

Why it matters: Domains that look like yours are set up to send email, ready to impersonate your people to customers and suppliers.

WHAT TO DO

1. Warn staff, customers and suppliers about the look-alike names.
2. Report the domains for abuse (Professional includes takedown requests), and consider registering the closest variants yourself.

Who: You, the business owner

Fix this month

MEDIUM EMAIL SPOOFING PROTECTION

No DKIM signing found

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: No DKIM selector found for the common providers (selector1, selector2, google).

Why it matters: Without DKIM signing, your genuine mail is easier to forge convincingly and more likely to be marked as spam.

WHAT TO DO

1. Turn on DKIM signing in your email service (Microsoft 365 or Google Workspace admin) and publish the records it gives you.

Who: Whoever manages your domain's DNS (often your IT provider or where you bought the domain)

MEDIUM WEBSITE AND CERTIFICATE SECURITY

No HSTS header

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: https://northwind-dental.example does not send Strict-Transport-Security.

Why it matters: Visitors can be silently moved to an unencrypted version of your site on untrusted Wi-Fi.

WHAT TO DO

1. Add the Strict-Transport-Security header to your site (start with max-age=31536000).

Who: Your web developer or website host

Plan for it

LOW WEBSITE AND CERTIFICATE SECURITY

No Content-Security-Policy

Affected: northwind-dental.example Checked: 1 October 2026

What we saw: https://northwind-dental.example does not send a Content-Security-Policy header.

Why it matters: Your site does not restrict what scripts it loads, making injected content and card-skimming code easier to slip in.

WHAT TO DO

1. Add a Content-Security-Policy header that lists where your site loads scripts from.

Who: Your web developer or website host

02 / FINDINGS

The evidence, area by area

Each finding translated into its real-world consequence, grouped by area.

Credential & Infostealer Exposure

GRADE **F**

- CRITICAL 2
  Active infostealer malware may be holding live, working passwords and session cookies for your people right now – attackers can log in as them today, bypassing the password entirely. This is not an old breach dump.
- HIGH 7
  Employee credentials tied to this domain appear in known breach corpuses and are likely reused against your email, VPN, and SaaS logins.

Email Impersonation Risk

GRADE **C**

- HIGH
  Your domain does not reject spoofed mail, so impersonation emails land in inboxes instead of being blocked.
- MEDIUM
  Without DKIM signing, outbound mail is easier to forge convincingly.
- LOW
  SPF is enforced – basic sender spoofing is blocked.

Look-alike Domains

GRADE **D**

- HIGH 2
  Look-alike domains are already configured to send email – primed to impersonate your people and partners in targeted fraud.

Web Security Hygiene

GRADE **B**

- MEDIUM
  No HSTS – visitors can be silently downgraded to insecure connections.
- LOW
  No Content-Security-Policy – the site is more exposed to injected content and clickjacking.
- LOW
  Web traffic is encrypted with a valid certificate.

External Surface

GRADE **C**

- HIGH
  A name on your domain still points at a cloud service you no longer use. Anyone can claim it and run a fake site on your own domain.
- LOW
  6 hosts found in certificate transparency logs, 4 answering.

03 / WHAT WE CHECKED

What was checked, and what was not

Checked 1 October 2026. A check that could not run is listed as such: it is never the same as nothing found.

Leaked and stolen passwords	Checked: 2 findings to act on.
Email spoofing protection	Checked: 2 findings to act on.
Look-alike domains	Checked: 1 finding to act on.
Website and certificate security	Checked: 2 findings to act on.
Internet-facing hosts	Checked: 1 finding to act on.

Breach data: Have I Been Pwned (haveibeenpwned.com) and Hudson Rock. We never see or store passwords.

04 / THE OTHER HALF OF THE RISK

This is your surface. Your people stand on it.

An exposure grade shows the door is open. HRS closes the loop: each finding here maps to the people it endangers, then targeted training and simulation harden exactly those people – the half of the problem a scanner alone cannot fix.

RECOMMENDED NEXT STEP

Book a 20-minute exposure review: humanriskshield.com