TAILORED CYBER

INSIGHT. CONTEXT. ADVANTAGE.

tailored-cyber.com

YOUR PUBLIC EXPOSURE

What a criminal can already see about your business

What's working, what to fix first, and a one-page brief for your IT provider

Overall picture: solid foundations, one priority gap

PREPARED FOR

EXAMPLE PHYSIO

PREPARED BY

Tailored Cyber

Sample report – for demonstration only

example.com

Passive, outside-only review. No systems were accessed.

FICTIONAL SAMPLE · The business, people, domains and findings in this report are invented.

Your scorecard

We looked at Example Physio the way a criminal would: using only what anyone can see from the internet, without touching your systems. Example Physio has a lot worth protecting – patient health information, two busy clinics, online bookings and regular payments from patients and health funds. Most of what we saw is in reasonable shape. One setting stands out, and it is quick to fix.

Area	Status	What we saw
Website and online bookings	Good	Your website and booking page run on a managed hosting platform, which looks after server security and patching for you.
Email platform	Good	Your business email runs on Microsoft 365, a mainstream platform with strong built-in protection when it is set up well.
Approved email senders list	Good	You publish a list of the services allowed to send email as Example Physio (an SPF record), so receiving mail systems have a starting point for spotting fakes.
Remote-access services	Good	Public internet records showed no remote desktop or similar remote-access services linked to your addresses.
Protection against fake emails	Fix now	Your email anti-impersonation setting (DMARC) is set to "monitor only", so receiving mail systems are not asked to block emails that pretend to be you.
Look-alike website addresses	Check	Three addresses that look like yours exist. Check whether you own them.
Staff visible online	Check	Six staff are publicly listed with job titles, including your Practice Owner and Practice Manager. That's normal, but it makes fake requests in their names more believable.
Account security, backups, staff training	Can't see	These can't be checked from outside. An Active Scan fills in much of this – see page 7.

How we did this

We used only publicly available information – the same view any member of the public, or a criminal, has. We did not log in to, test or access any system. Public records can be out of date, so each item is something to confirm, not proof of a problem or a breach.

Good evidence supports this as working Fix now an agreed priority, not a claim of compromise Check ask the owner or provider to confirm Can't see needs an inside view

Why this matters for Example Physio

149

of 667 data breaches reported to Australia's privacy regulator in January–June 2026 came from health service providers – more than any other sector.

OAIC, Notifiable Data Breaches statistics, Jan–Jun 2026[1]

$166.8m

lost by Australians to payment-redirection scams in 2025, where criminals pose as a trusted business and change where money is paid. The second-largest scam type by losses.

National Anti-Scam Centre, Targeting Scams 2025[2]

$55,400

average reported cost of cybercrime per report for an Australian small business in 2025–26.

ASD Annual Cyber Threat Report 2025–26[3]

Australian context, not a forecast for this business. Figures cover different periods and reporting groups. Sources are listed on page 9.

What a criminal could do with what's public

The fake overdue invoice

Patients get an email that appears to come from the clinic, saying their account is overdue and asking them to pay into a "new" bank account. With the current email setting, nothing tells their mail system to block it.

Linked to Priority 1

The urgent payroll change

The bookkeeper gets a message "from the Practice Owner" asking to update their bank details before this week's pay run. The name and title are easy to find online.

Linked to Priority 2

The look-alike booking page

A criminal registers a similar web address, copies your booking page and collects card details from people searching for an appointment.

Linked to Priority 3

Illustrative scenarios based on common scam patterns.

Why patient information raises the stakes. Because Example Physio provides health services, the Privacy Act and the Notifiable Data Breaches scheme apply whatever its turnover. A scam that exposes patient information could need to be reported to the regulator and to the patients affected.

Your three priorities

Each priority is something you already pay for, or a simple rule in the office. No new software is needed.

1 Stop criminals sending email as you

Fix now

What we saw
Your DMARC setting (the rule that tells other mail systems what to do with fake emails using your name) is set to "monitor only" (p=none). Your approved senders list also ends in a soft "~all" rather than a strict rule.

Why it matters for you
Patients, health funds and suppliers trust emails from the clinic, including ones about payments. Right now, a well-made fake has a better chance of reaching their inbox.

What to do
Ask your IT or email provider to (a) confirm every service that sends email as you – Microsoft 365, your booking system, your newsletter tool and any others, (b) turn on DMARC reports and review them for 2–4 weeks, then (c) move step by step to "quarantine" and then "reject".

WHO	EFFORT	DONE WHEN
IT or email/DNS provider	About 1–3 hours of provider time over a few weeks	DMARC is at quarantine or reject, and genuine emails still arrive

2 Make fake requests easy to spot

Check

What we saw
Six staff are publicly listed with job titles, including the Practice Owner and Practice Manager.

Why it matters for you
With two clinics and part-time staff, people often deal with colleagues by message rather than face to face, which is exactly what fake "urgent request" scams rely on.

What to do
Agree one simple rule for all staff. Any request to change bank details, make an urgent payment or send patient or staff records must be confirmed by phoning a known number, never by replying to the message. Make sure accounts for people handling money and HR use multi-factor authentication (a second login step).

WHO	EFFORT	DONE WHEN
Practice Manager	A 15-minute team briefing, no cost	Staff can explain the call-back rule, and finance accounts use MFA

Your three priorities (continued)

3 Check the look-alike addresses

Check

What we saw examp1e.example, example-physio.example and examplephysio.example.

Why it matters for you Most new patients find you by searching online. A look-alike address could be used for fake booking pages or emails.

What to do Check whether you already own these. If not, look up who does and whether they host a website or email. Consider registering the closest match to your business name.

WHO	EFFORT	DONE WHEN
Whoever manages your domain names	Under an hour, plus small fees if you register any	Each address is recorded as "ours", "unrelated" or "being followed up"

What's working well

Good

Your website runs on a managed platform

Your hosting provider handles server security and patching, which removes a whole class of risk that self-hosted sites carry.

Good

Your email is on Microsoft 365

A mainstream platform with strong built-in protections. The next step is making sure they are fully switched on (Priority 1 and multi-factor authentication).

Good

No exposed remote access

Public records showed no remote desktop or similar services – a common way criminals get in.

Worth keeping an eye on

Check **Business apps.** Your public records show Microsoft 365, an online booking system and an email newsletter service. Confirm each is still used, who owns the account, and that former staff no longer have access.

Check **Suppliers and partners.** Your booking provider, bookkeeper and IT support connect to your systems or send email for you. Keep a simple list of who has access to what.

Your next 30 days

You can do this week

- [ ] **Brief staff on the call-back rule** (Priority 2)
  Done when: staff can explain it.
- [ ] **Check who owns the look-alike addresses** (Priority 3)
  Done when: each one is recorded.

Hand to your IT provider (page 8)

- [ ] **Move email protection to blocking** (Priority 1)
  Done when: DMARC is at quarantine or reject and genuine mail still arrives.
- [ ] **Confirm multi-factor authentication on finance accounts** (Priority 2)
  Done when: coverage is confirmed for priority users.
- [ ] **Confirm business apps, suppliers and who has access** (page 5)
  Done when: each service has a named owner.

What we couldn't see from outside

This report is the view from the street. It shows what public records say about the business, but it can't confirm which systems actually respond, whether their software is up to date, or whether fake emails are really blocked. Several items are marked Check or Can't see for that reason.

Next step: an Active Scan

With your written permission, we safely test the internet-facing systems that belong to you to confirm what is really exposed – and turn the "Check" items in this report into clear answers. See page 7 for what it covers and examples of what it can find.

daniel.hompas@tailored-cyber.com

Complete the picture: an Active Scan

This report used only public records. An Active Scan goes one step further: with your written permission, we safely check the internet-facing systems that belong to you, the same way a criminal would probe them, but with no attempt to break in or access data. It turns "what records suggest" into "what is actually there".

What it adds to this report

Question	Today (public records)	With an Active Scan
What can be reached from the internet?	Addresses and services named in public records	Confirms which of your systems respond, and which "doors" (ports and services) are open, such as remote desktop, VPN or file-sharing logins.
Is the software up to date?	Can't see	Identifies software versions on systems you manage and checks them against published vulnerabilities.
Are fake emails really stopped?	DMARC set to "monitor only"	Sends controlled test emails to confirm what your mail system blocks, flags or delivers, before and after Priority 1.
Are your web pages set up securely?	Main site is on a managed platform	Checks the sites and booking pages you manage for encryption settings, security headers and exposed admin or test pages.
Are old or forgotten systems still online?	Names seen in certificate and DNS records	Checks whether each one is live, still owned and still needed, including old records a criminal could take over.
Are staff logins protected?	Can't see	Checks that Microsoft 365 and other login pages enforce multi-factor authentication and block older login methods that can bypass it.

Examples of what an Active Scan could return

Fix now

Remote desktop open to the internet

A clinic or office computer accepts remote logins from anywhere – a common way criminals get in before launching ransomware.

Fix now

Known flaw in a login portal

A VPN or booking system runs a version with a published vulnerability that the vendor has already fixed.

Check

A forgotten test website

An old development or campaign site is still online with a login page, and nobody is maintaining it.

Check

Weak encryption or expiring certificate

A page you manage allows outdated encryption, or its certificate expires soon, which triggers browser warnings for patients.

Good

Only expected services visible

Everything reachable is meant to be there, is up to date and requires multi-factor authentication.

Good

Fake test email blocked

After Priority 1, a spoofed test email is rejected, which confirms the fix is working.

Illustrative examples of typical results for small businesses.

How it works

1. **Agree the scope** Your systems only. Platforms run by others are included only where their testing rules allow.
2. **Written permission** You sign an authorisation and we agree a testing window.
3. **Safe, low-impact scan** Rate-limited checks with no attempt to break in, change anything or access patient data.
4. **Updated report** An updated scorecard, a walkthrough of results and a refreshed IT provider brief.

Book your Active Scan

Start with a 20-minute call to agree the scope. Email **daniel.hompas@tailored-cyber.com**

Brief for your IT provider

The business has asked us to share these observations from a passive, outside-only review. Please confirm they are current before changing anything.

#	Observation and evidence	Recommended target state	Done when

1	**Email authentication**
	`example.com SPF: v=spf1 include:spf.protection.outlook.com include:_spf.mailer.example.net include:_spf.bookings.example.org ~all`
	`DMARC: v=DMARC1; p=none`
		Inventory all legitimate senders and confirm SPF/DKIM alignment for each. Enable DMARC aggregate reporting (rua). Move to p=quarantine, then p=reject. Consider -all once all senders are confirmed, and keep SPF within the 10 DNS-lookup limit.	DMARC at quarantine or reject with aligned DKIM for all senders; legitimate delivery confirmed.

2	**Look-alike domains**
	`examp1e.example`
	`example-physio.example`
	`examplephysio.example`
		Confirm ownership. For third-party registrations, check for MX/A records and active content. Decide whether to register, monitor or seek takedown.	Ownership and status recorded for each domain.

3	**Identity protection for high-risk roles** `6 public role records incl. Practice Owner, Practice Manager`	Phishing-resistant or app-based MFA on Microsoft 365 for all users, prioritising finance and management. Review Microsoft 365 user and domain impersonation protection policies.	MFA coverage confirmed; impersonation protection enabled for priority users.

4	**SaaS and supplier inventory**
	`Senders: Microsoft 365, newsletter service, booking system`
	`Web: managed hosting platform (203.0.113.10, third-party shared hosting)`
		Confirm each service is in use, has a named business owner and admin, enforces MFA, and retains no access for former staff. Remove unused senders from SPF.	Service, owner, admin and MFA status listed for each service.

Sample collection reference SAMPLE-0000. All records shown are fictional and use reserved example domains and documentation IP addresses. See page 9 for method and limits.

How we did this

Method

Passive, outside-only collection using open-source intelligence tools: public DNS records, certificate and domain registration data, public web content and public professional profiles. We did not log in to, scan with permission-requiring techniques, or test any system.

Limits

Public records can be out of date or incomplete. Findings are observations to confirm with the responsible owner, not evidence of compromise. An outside view cannot assess account security, backups, device patching or internal processes.

Evidence summary

Observation	Source type	Status
SPF record and DMARC policy (p=none)	Public DNS	Recorded
Similar-name domain candidates (3)	Domain registration / DNS	Recorded
Public work-role records (6)	Public professional profiles	Recorded
Service provider indicators	DNS (SPF includes), web hosting	Recorded
No remote-access services on known addresses	Public internet service records	Recorded

Sources

1. Office of the Australian Information Commissioner, "Large-scale data breaches on the rise, latest OAIC statistics reveal" (Notifiable Data Breaches statistics, January–June 2026). oaic.gov.au/news/media-centre/large-scale-data-breaches-on-the-rise,-latest-oaic-statistics-reveal
2. National Anti-Scam Centre, "Continued action critical to combat fraud as annual scam losses exceed $2 billion" (Targeting Scams 2025). nasc.gov.au/news/continued-action-critical-to-combat-fraud-as-annual-scam-losses-exceed-2-billion
3. Australian Signals Directorate, Annual Cyber Threat Report 2025–26, Year in Review. cyber.gov.au/publication/annual-cyber-threat-report-2025-26/year-in-review

This is a fictional sample. Example Physio, its staff, domains, records and findings are invented for demonstration. Domains use the reserved ".example" and "example.com/.net/.org" names, and IP addresses use documentation ranges.