AFRIWEALTH CYBER INTELLIGENCE

The 5-Point Business Exposure Checklist

Five questions that reveal whether your business is an easy target — no technical knowledge required. Takes about ten minutes.

Most businesses that get hit were not chosen. They were **found** — by software scanning for the easiest way in.

The good news: the doors attackers use most are the same five every time, and you can check all of them yourself. Go through each point below, tick honestly, and note anything you can't answer. An honest **"I don't know"** is the most valuable answer on this page — it's exactly where your risk is hiding.

1 Can a stranger send email pretending to be you?

Why it matters: If your domain isn't locked down, anyone on the internet can send an email that looks like it came from your company — to your clients, your bank, or your own staff. No hacking required. This is the single most common route to fraudulent invoices and lost payments, and it costs nothing to fix.

ASK YOUR IT PERSON OR PROVIDER

"Do we have **SPF, DKIM and DMARC** set up on our domain — and is DMARC set to reject, not just monitor?"

☐ Yes, all three enforced ☐ Partly / not sure ☐ No

2 Is every account protected by more than a password?

Why it matters: Passwords leak constantly — usually from somewhere else entirely, then reused on your systems. Two-step verification (a code or prompt after the password) stops the overwhelming majority of account takeovers. Email is the priority: whoever controls your email can reset everything else.

CHECK TODAY

Is **two-step verification** switched on for every company email account — especially finance, management, and anyone who can move money?

☐ Yes, everyone ☐ Some accounts ☐ No / not sure

3 Are your staff's passwords already for sale?

Why it matters: When an employee's password is stolen — often from a personal device infected with malware — it ends up bundled and sold in criminal markets. Your business can be fully exposed without a single system of yours being touched. Most companies only find out after the money is gone.

ASK YOURSELF

Has anyone ever **checked** whether your company's email addresses appear in known data leaks? (If nobody has looked, assume the answer is unknown — not "no".)

☐ Checked recently ☐ Checked once, long ago ☐ Never checked

4 Would you know if someone got in?

Why it matters: Attackers rarely announce themselves. They sit quietly in an email account for weeks, learning how you write and who pays you — then send one convincing message at the right moment. Antivirus does not catch this. Someone has to be watching for the signs.

ASK YOUR IT PERSON OR PROVIDER

"If someone logged into our email from another country tonight, **what would tell us** — and who would see it?"

☐ We'd be alerted ☐ Maybe, eventually ☐ We wouldn't know

5 Can you verify a payment request without email?

Why it matters: The most expensive attacks in West Africa right now are not clever code — they are a believable email asking finance to update bank details. If your only check is replying to that email, you are asking the attacker for permission. One phone-call rule prevents nearly all of it, and costs nothing.

MAKE IT A WRITTEN RULE

Any change to bank or payment details must be confirmed by **phone call to a known number** — never a number supplied in the email itself.

☐ Rule exists & is followed ☐ Informal habit ☐ No rule

How did you do?

Count how many points you could answer with a confident "yes".

4–5 confident yeses
You're ahead of most businesses your size. Keep it reviewed — exposure changes as staff and systems change.

2–3 confident yeses
You have real gaps, but they're closeable. Start with points 1 and 2 — both are free and stop the most common attacks.

0–1 confident yeses
Your business is currently an easy target. Nothing here requires a big budget — it requires someone to actually do it this week.

Free — no obligation

Want to see what attackers can already see?

We run a free **Exposure Snapshot** — a passive check of what's publicly exposed about your organisation: leaked credentials, email security gaps, and weaknesses visible from the outside. No systems are touched and nothing is attacked. You get a plain-language summary of what we find and what to do about it.

Send your business name and website to:
WhatsApp +233 257 225 050 (message CHECK) · info@afriwealthintel.com

This checklist is general guidance for business owners and managers, not a substitute for a full security assessment or legal/regulatory advice. Every organisation's risk is different — if any point above concerns you, talk to a qualified professional about your specific situation.