SecureByDefault

// THE ESSENTIAL SECURITY CHECKLIST

The 25-Point Security Audit Most Businesses Skip.

A no-jargon, engineer-built checklist covering the exact gaps attackers exploit first. Work through it once and you'll be more secure than the overwhelming majority of businesses operating today.

94%
OF LOGINS ONLINE ARE NOW BOTS

99%
OF AUTOMATED ATTACKS BLOCKED BY MFA

24h
UNTIL A NEW SERVER IS PROBED

Built by **Ron Mercier**
Cloud & Cybersecurity Engineer
MSc Cybersecurity · CySA+ · PenTest+ · AWS

securebydefault.io

Most breaches aren't sophisticated. They happen because a password was reused, an update was skipped, or a backup was never tested. This checklist targets those gaps. Print it, work through each box, and revisit it quarterly. No enterprise budget required.

IF YOU ONLY DO THREE THINGS

Start here. These stop the most attacks for the least effort.

- Turn on multi-factor authentication everywhere it's offered
- Put every password in a password manager — zero reuse
- Set up automatic, tested backups using the 3-2-1 rule

1 Identity & Access

Stolen credentials are the #1 entry point for attackers

- [ ] **Multi-factor authentication is enabled** on email, banking, cloud platforms, and every admin account.
- [ ] **A password manager is in use** and no password is reused across two or more accounts.
- [ ] **Default credentials have been changed** on routers, IoT devices, and any new hardware.
- [ ] **Least-privilege access is applied** — people can only reach the systems their role requires.
- [ ] **Old and unused accounts are disabled**, especially for former employees and contractors.

PRO TIP **Phishing-resistant beats SMS.** If a service supports an authenticator app or hardware key, use that instead of text-message codes — SMS can be intercepted via SIM-swap attacks.

2 Email & Phishing Defense

Email is still the most common attack delivery method

- [ ] **Advanced spam and threat filtering is active** — going beyond your provider's default.
- [ ] **SPF, DKIM, and DMARC records are configured** on your domain to prevent spoofing.
- [ ] **The team knows the red flags** — urgency, unexpected attachments, payment changes, lookalike domains.
- [ ] **Financial requests are verified out-of-band** — a phone call before any wire transfer or banking change.

PRO TIP **AI killed the typo tell.** The spelling errors that used to flag phishing are gone — modern lures are AI-written and clean. Train on behavior and context, not grammar.

3 Devices & Updates

Unpatched software is an open door attackers actively scan for

- [ ] **Automatic updates are enabled** on operating systems, browsers, and third-party apps.
- [ ] **Modern endpoint protection (EDR) is installed** on every device — not just basic antivirus.
- [ ] **End-of-life systems have been retired** — unsupported software no longer receives security patches.
- [ ] **Disk encryption is on** for laptops and mobile devices (BitLocker, FileVault).
- [ ] **Screens lock automatically** after a short idle period on all work devices.

PRO TIP **Patch speed is everything.** Attackers weaponize newly disclosed vulnerabilities within days. The window between "patch released" and "exploit live" keeps shrinking — automate updates.

4 Backups & Recovery

A backup you've never restored is not a backup you can trust

- [ ] **The 3-2-1 rule is followed** — 3 copies, 2 media types, 1 off-site or offline.
- [ ] **Backups run automatically** on a schedule — not dependent on someone remembering.
- [ ] **At least one copy is offline or immutable** so ransomware can't encrypt it too.
- [ ] **A test restore has been performed** in the last 90 days and verified working.

PRO TIP **Ransomware's favorite discovery:** that the only backup was on a connected drive it just encrypted. Offline or immutable storage is what actually saves you.

5 Network & Cloud

Misconfiguration is one of the top causes of data exposure

- [ ] **A business-grade firewall is in place** with a deny-by-default rule set.
- [ ] **Wi-Fi uses WPA2/WPA3** and guest traffic is isolated from internal systems.
- [ ] **Cloud storage is not publicly exposed** — buckets, drives, and shares are locked down.
- [ ] **No credential or config files are web-accessible** (.env, key files, backups in web roots).

PRO TIP **From the field:** a brand-new server with no published URL was probed for exposed `.env` and cloud credential files within 24 hours of going live. Assume you are always being scanned.

6 People & Process

Most incidents involve a human — attackers target people, not just tech

- [ ] **Security awareness is ongoing** — short, regular reminders, not one annual session.
- [ ] **A written incident response plan exists** — who to call, how to isolate, how to recover.
- [ ] **The response plan has been practiced** at least once in the past year.
- [ ] **Dark-web monitoring is active** for company email addresses and leaked credentials.
- [ ] **Vendor and supply-chain access is reviewed** — third parties are a common breach path.

PRO TIP **Plans fail when they're untested.** The middle of a live incident is the worst time to discover your response plan has a gap. Run a 30-minute tabletop drill once a year.

2026 THREATS WORTH KNOWING

What changed this year

- AI-generated phishing is now indistinguishable from real email
- Bot traffic now exceeds human traffic across the internet
- Cyber-insurance claims are denied when MFA and backups weren't in place
- Credential lists sell for pennies — password reuse is a direct liability

The takeaway: security in 2026 isn't about perfection or a big budget. It's about consistency on the fundamentals. Handle the basics well and you remove the gaps that the overwhelming majority of real-world attacks rely on.

// YOU'RE AHEAD OF MOST BUSINESSES ALREADY

Want the stories behind every item on this list?

Every checkbox here exists because of a real failure I've seen, fixed, or written about. **SecureByDefault** breaks down real attacks, real configurations, and the tools actually worth trusting — written by an engineer, for people who want the truth without the hype.

YOUR NEXT 3 MOVES

01 Read the breakdown of how a brand-new server was attacked within 24 hours — with the real logs.

02 Join the weekly newsletter for one practical security lesson every week — no fluff.

03 Check the Tools page for security software vetted with an engineer's eye.

Everything starts here:

securebydefault.io

Cloud security · Cybersecurity tools · Real attack breakdowns