YC Youngster Company

FREE GUIDE · NOVEMBER 2026

10 security checks you can run from your browser

No tools to install, no account to create. Ten URLs and commands that show you what attackers see when they look at your company, and what to do about each one.

- Every subdomain your company ever had a certificate for
- Whether your email domain can be spoofed
- What the internet sees on your server
- Files Google indexed that were never meant to be public
- Whether your WordPress site leaks usernames

CHECK 1 OF 10

Every subdomain your company ever had a certificate for

```
crt.sh/?q=yourcompany.com
```

Every HTTPS certificate issued in the last few years is written to a public log. crt.sh searches that log. The result is a list of every hostname your company ever put a certificate on: the main site, the mail server, and the staging, dev and test hosts that were set up for a project and forgotten. Attackers read this list before they touch your main site, because the forgotten hosts are rarely patched.

Good

Only hostnames you recognise and still use.

Needs attention

Hosts you don't recognise, or old staging/dev/test names that still resolve.

Fix: switch off hosts you no longer use (remove the DNS record and the server), and put the ones you keep behind a login or VPN. Repeat the search twice a year.

Related free tool: our website safety check tests the exposure of each host you still run.

CHECK 2 OF 10

Your website's security grade, in 30 seconds

```
youngstercompany.com/#check → paste your domain
```

Our free check looks at your site from the outside, the way an attacker's scanner does, and grades it from A to F. It tests HTTPS and the certificate, the security headers that stop clickjacking and script injection (HSTS, Content-Security-Policy, X-Frame-Options and others), whether your email domain is protected against spoofing, whether files such as .env, .git or backups are exposed, cookie flags and mixed content. No sign-up, and you get a result page you can share with whoever runs your site.

Good

A or B. Keep it that way: re-run after every site change.

Needs attention

C or lower. The usual causes are two or three missing headers and no DMARC record.

Fix: the result page lists each failing check with the exact fix. Most sites go from D to A in an afternoon: add the headers at the web server or through a plugin, publish SPF, DKIM and DMARC, and remove exposed files.

We run this on our own site every Sunday. Current grade: youngstercompany.com/check/youngstercompany.com/.

CHECK 3 OF 10

Can a stranger send email as your CEO?

```
youngstercompany.com/email-security-checker/ → yourcompany.com
```

Three DNS records decide whether receiving mail servers trust mail "from" your domain: SPF (which servers may send for you), DKIM (a signature on each message) and DMARC (what to do when a message fails the first two). Our checker reads all three and explains them in plain English. Most invoice-fraud and "urgent request from the MD" emails work because the target company has no DMARC record, so a forged sender address is accepted.

Good

SPF ends in -all or ~all, DKIM present, DMARC with p=quarantine or p=reject.

Needs attention

No DMARC record, DMARC with p=none, or SPF with +all.

Fix: publish a DMARC record starting with p=none and a reporting address, read the reports for two weeks, then move to p=quarantine and finally p=reject. It is a DNS change, not a product purchase.

Our own path: p=none on 25 Oct, p=quarantine the same day after checking senders, p=reject after a month of clean reports.

CHECK 4 OF 10

Scan a link before you click it

```
urlscan.io → paste the link
```

urlscan.io opens the link in a sandbox on its own servers and shows you what happened: a screenshot of the page, every domain the page contacted, the redirects it went through, and whether the page matches a known phishing kit. The link never touches your device, so a malicious page cannot do anything to you. Use it for links in unexpected emails, WhatsApp forwards and SMS messages about parcels, bank KYC or prizes.

Good

The screenshot shows the site you expected, on the domain you expected.

Needs attention

A login page on a look-alike domain, a redirect chain through unknown hosts, or a "malicious" verdict.

Fix: don't open the link. Report the message to the sender's real organisation and delete it. If you already entered a password on such a page, change it now and turn on two-factor authentication.

For the text of a suspicious message, our scam message checker looks for the common scam patterns.

CHECK 5 OF 10

Is your password already leaked?

```
haveibeenpwned.com → your email address
```

Have I Been Pwned holds billions of accounts from public data breaches. Type an email address and it lists every breach that included it. If a breach included passwords, the password you used on that site is in criminals' hands, and if you reused it anywhere else, those accounts are open too. Companies can register their domain (free) and get an alert whenever a staff address appears in a new breach.

Good

No breaches, or only old ones whose passwords you have since changed.

Needs attention

A breach that included a password you still use anywhere.

Fix: change the reused passwords first, starting with email and banking. Turn on two-factor authentication everywhere it is offered. Use a password manager so every site gets its own password.

Our security policy generator writes a password and access policy for your team in a few minutes.

CHECK 6 OF 10

What the internet sees on your server

```
shodan.io/host/your.server.ip.address
```

Shodan scans the whole internet continuously and records what answers on every port. Look up your server's public IP and you see what any attacker sees: the open ports, the services behind them and their version numbers. The things that should worry you are a database (3306, 5432, 27017, 6379) or an admin panel reachable from the internet, an old SSH or web server version, and ports you don't recognise at all.

Good

Only 80/443 (web) and, if needed, 22 (SSH) with a current version.

Needs attention

Database, RDP, FTP or admin ports open to everyone, or versions with known vulnerabilities.

Fix: close the ports in the firewall or cloud security group, move admin access behind a VPN, and update the services that are left. Re-check after every change.

Our tested SSH hardening checklist covers the settings for port 22.

CHECK 7 OF 10

Does your company have a way to report a security bug?

```
yourcompany.com/.well-known/security.txt
```

security.txt is a small text file with a contact address and a link to your disclosure policy. When a researcher finds a hole in your website, this is where they look for whom to tell. Without it, the finding either goes nowhere, gets posted publicly, or ends up with someone less friendly. Large companies, banks and government sites publish one; it takes ten minutes and costs nothing.

Good

The file opens, has a Contact line and an Expires date in the future.

Needs attention

404, or a file with an expired date or a contact that no one reads.

Fix: create the file with Contact:, Expires: and Policy: lines, serve it at /.well-known/security.txt, and make sure the mailbox is monitored. Pair it with a short disclosure policy page.

Copy ours: security.txt and the disclosure policy.

CHECK 8 OF 10

Files Google indexed that were never meant to be public

```
site:yourcompany.com ext:sql OR ext:env OR ext:bak OR ext:log
```

Search engines index whatever they can reach. If a database dump, a configuration file or a backup was left in a web folder, Google may have it, and so does anyone who searches. Run the search above on your own domain, then try ext:pdf, ext:xlsx and ext:docx to see which documents are public and whether they should be. Try inurl:admin and inurl:login too, to see which admin pages are discoverable.

Good
Only pages and documents you intend to publish.

Needs attention
Any .sql, .env, .bak or .log result, or internal documents.

Fix: remove the file from the server (not just the link), block the file types at the web server, then use Google Search Console's removal tool to drop the cached copy. Rotate any password or key the file contained.

Our website safety check tests for exposed .env, .git, backups and logs on every run.

CHECK 9 OF 10

The one-line DMARC check

```
dig TXT _dmarc.yourcompany.com +short
```

If you have a terminal (macOS, Linux, or Windows with WSL), this command prints your DMARC record in one second. On Windows without WSL use **`nslookup -type=TXT _dmarc.yourcompany.com`**. The record tells receiving servers what to do with mail that fails SPF and DKIM: nothing (p=none), spam folder (p=quarantine) or reject (p=reject). It also names an address that receives daily reports of who is sending mail as your domain.

Good

v=DMARC1; p=quarantine or p=reject; rua=mailto:... present.

Needs attention

No record, p=none for months, or no rua address (you are blind to abuse).

Fix: add rua= so you receive reports, confirm every legitimate sender (your mail provider, newsletter tool, CRM) passes SPF or DKIM, then step up to p=quarantine and p=reject.

No terminal? The email security checker runs the lookup and explains the record.

CHECK 10 OF 10

Does your WordPress site leak usernames?

```
yoursite.com/wp-json/wp/v2/users  ·  yoursite.com/?author=1
```

On a default WordPress install the first URL returns a list of every author with their username, and the second redirects to the first user's profile page, which also shows the username. A username is half of a login. With it, an attacker only has to guess the password, and automated tools try thousands per hour against wp-login.php and xmlrpc.php.

Good

The users endpoint returns 401 or 404 for visitors, and /?author=1 goes to the home page.

Needs attention

A list of usernames, or a redirect to /author/username/.

Fix: block the users REST endpoint for logged-out visitors, redirect author queries, move the login page to a non-default address, rate-limit logins, and require two-factor authentication for every administrator.

Step by step: our WordPress on shared hosting checklist.

WHAT NEXT

If a check came back red

Most of the fixes above take an afternoon if you run your own site. If you would rather have it done, or you need an answer about a specific vulnerability in the news, these are the three ways we help.

Emergency exposure check ₹2,999 · 48 hours

Read about a vulnerability or breach and need to know whether you are affected? Send us up to five hosts, sites or product versions. Within 48 hours you get a written verdict per asset, what to patch first and how to verify the fix.
youngstercompany.com/product/emergency-exposure-check/

Website security fix fixed price

We take your site from its current grade to A: security headers, TLS, email authentication, exposed files, WordPress hardening, and a re-test with the report. Ask for the current price at contact@youngstercompany.com.

ISO 27001, DPDP and VAPT

Readiness assessments, a free DPDP readiness check and ISO 27001 self-assessment, and web-application penetration testing for Indian businesses.
youngstercompany.com/our-services/

Questions about any check? Reply to the email this came with, or write to contact@youngstercompany.com. We answer within one working day.