CheckItNowTools.com
Internet Intelligence • Website Safety • Cybersecurity

CheckItNowTools.com User Guide

Complete Guide to Using CheckItNowTools.com Internet Intelligence, Website Safety, Domain Analysis, and Cybersecurity Tools

Edition 1.0 • Published June 2026

checkitnowtools.com

support@checkitnowtools.com

Table of Contents

Table of Contents 2

1. Welcome 4

- Who it is for . . . 4
- Problems we help you solve . . . 4
- Our mission . . . 4

2. Getting Started 5

- Homepage overview . . . 5
- Navigation structure . . . 5
- Resource Center, Glossary, Methodology, Transparency . . . 5

3. IP & Network Intelligence Tools 6

- What Is My IP — /ip . . . 6
- IP Lookup — /ip/{address} . . . 6
- Reverse DNS — /dns/reverse . . . 6
- Ping, Traceroute, Port Check . . . 6
- Speed Test . . . 6

4. Domain & Website Intelligence Tools 7

- WHOIS / RDAP — /whois . . . 7
- Domain Reputation — /domain-reputation-checker . . . 7
- Domain Age — /domain-age . . . 7
- Website Safety Checker — /website-safety-checker . . . 7

5. DNS & Connectivity Tools 8

- DNS Lookup — /dns . . . 8
- DNS Records by domain — /dns-records/{domain} . . . 8
- Common use cases . . . 8

6. SSL & Security Tools 9

- SSL Certificate — /ssl . . . 9
- HTTP Headers — /headers . . . 9
- How to interpret . . . 9

7. Website Safety & Reputation Tools 10

URL Safety Checker — /url-safety-checker . . . 10

Phishing Detection — /phishing-detection-tool . . . 10

Blacklist Check — /blacklist . . . 10

Risk indicators to watch . . . 10

8. Resource Center 11

9. Glossary System . . . 11

10. Methodology Center 12

Accuracy considerations . . . 12

11. Transparency Center . . . 12

12. Understanding Results 13

WHOIS records . . . 13

DNS records . . . 13

SSL information . . . 13

Domain & IP reputation . . . 13

Security headers . . . 13

13. Frequently Asked Questions 14

14. Best Practices 17

Website safety . . . 17

Cybersecurity awareness . . . 17

Domain research . . . 17

DNS troubleshooting . . . 17

15. Privacy & Security 18

Privacy protections . . . 18

Data handling . . . 18

Transparency commitments . . . 18

16. Contact & Support . . . 18

1. Welcome

CheckItNowTools.com is a free internet intelligence and cybersecurity diagnostics platform. It helps anyone — from curious users to IT operations teams — answer concrete technical questions about IP addresses, DNS, domains, SSL certificates, email infrastructure, and website safety.

Who it is for

- **Everyday users** wanting to verify a website is safe before clicking.
- **Small business owners** protecting domains, email reputation, and customer trust.
- **Developers and IT teams** diagnosing DNS, SSL, headers, and network issues.
- **Security professionals** investigating phishing, blacklisting, and infrastructure risk.
- **Students and educators** learning how the public internet works.

Problems we help you solve

- Is this website legitimate, or a scam?
- Why are my emails being rejected or marked as spam?
- Why is my domain or IP blacklisted?
- Is my SSL certificate correctly installed and current?
- Is my VPN actually hiding my IP?
- What information about me is exposed by my browser?

Our mission

Make internet diagnostics transparent, educational, and accessible — with clear methodology, no dark patterns, and no required signup for everyday checks.

2. Getting Started

Homepage overview

The homepage gives you three entry points: a universal lookup bar (paste any IP, domain, or URL), a card showing your own public IP and network, and curated tool tiles by category. Start with whichever matches your question.

Navigation structure

- Safety Check — fastest path for non-technical users.
- Browse — see every diagnostic, grouped by category.
- Learn — guides, glossary, and how-to articles.
- User Guide — this document.
- Dashboard — saved lookups and monitoring (optional account).
- Pricing — Pro plan for advanced workflows.

Resource Center, Glossary, Methodology, Transparency

Use Methodology to learn how each tool computes a verdict, Data sources to see the upstreams we query, and Advertising disclosure to understand our commercial practices. These pages form our Transparency Center.

3. IP & Network Intelligence Tools

What Is My IP — /ip

Shows your public IPv4/IPv6 address, ISP, ASN, approximate city/region, and a verdict on whether the network is residential, hosting, or VPN/proxy.

> **Example.** Connect to a VPN, refresh the page, and confirm the location changes and the network classification flips to VPN/proxy.

IP Lookup — /ip/{address}

Enter any IPv4 or IPv6 address. Returns geolocation, ASN, organization, and reverse DNS.

Reverse DNS — /dns/reverse

Resolves an IP to its PTR record. Used by mail servers to verify sender legitimacy. A missing PTR on a mail server commonly causes spam-folder delivery.

Ping, Traceroute, Port Check

Ping reports HTTP round-trip latency from the edge. Traceroute reveals the network path. Port check tests TCP reachability of any port on any host.

Speed Test

Browser-based download and latency test. Useful for spotting throttling or congestion without installing software.

4. Domain & Website Intelligence Tools

WHOIS / RDAP — /whois

Pulls the registrar of record, registration and expiration dates, nameservers, status codes, and abuse contacts. Many registrars redact owner contact details under GDPR — this is normal, not suspicious.

Domain Reputation — /domain-reputation-checker

Combines blacklist listings, SSL posture, and HTTP headers into a Safe / Caution / Risky verdict.

Domain Age — /domain-age

Calculates a domain's age from its WHOIS creation date. Brand-new domains (under 30 days) are a common phishing signal.

Website Safety Checker — /website-safety-checker

One-click verdict for non-technical users. Pulls reputation, SSL, and reachability into a plain-English summary.

> **How to interpret.** Treat 'Caution' as 'investigate before trusting'. A clean verdict on a domain under one week old is the most common false-negative pattern — check the domain age tab.

5. DNS & Connectivity Tools

DNS Lookup — /dns

Queries A, AAAA, MX, TXT (including SPF), NS, SOA, and CAA records over DNS-over-HTTPS. We cross-check Cloudflare 1.1.1.1 and Google 8.8.8.8 when results differ.

DNS Records by domain — /dns-records/{domain}

Shareable per-domain DNS view. Use it to send a colleague a snapshot of a domain's records.

Common use cases

- Email migration QA: confirm MX, SPF, DKIM, and DMARC before flipping production.
- Site migration: verify A/AAAA propagation across resolvers.
- Incident response: confirm a domain's nameservers have not been hijacked.

6. SSL & Security Tools

SSL Certificate — /ssl

Performs a real TLS handshake and reports the leaf certificate's subject, SANs, issuer, validity window, and signature algorithm.

HTTP Headers — /headers

Scores response headers against the OWASP Secure Headers Project recommendations: CSP, HSTS, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.

How to interpret

- An expiration within 14 days warrants immediate renewal.
- A missing SAN for the requested hostname is a real misconfiguration.
- Missing CSP and HSTS on a sensitive endpoint is a legitimate concern; on a static marketing page it is lower priority.

7. Website Safety & Reputation Tools

URL Safety Checker — /url-safety-checker

Resolves the URL, fetches reputation, and inspects redirect chains and HTTPS enforcement.

Phishing Detection — /phishing-detection-tool

Flags lookalike domains, suspicious TLDs, recently registered hosts, and known phishing indicators.

Blacklist Check — /blacklist

Queries a curated panel of DNSBLs in parallel and reports per-list verdicts plus the total count.

Risk indicators to watch

- Brand-new domain (under 30 days).
- Free or anomalous TLD combined with a brand keyword in the subdomain.
- Missing or self-signed SSL certificate.
- Multiple DNSBL listings, or appearance on Safe Browsing.
- Cloaked redirects or mismatched WHOIS contact data.

8. Resource Center

The Learn hub indexes every guide. Highlights include:

- Internet Intelligence Playbook — the master index of all guides and tools.
- Cybersecurity Basics — foundational concepts in plain language.
- Website Security Checks — a repeatable security-check workflow.
- Online Privacy — reduce your visible footprint.
- Network Troubleshooting — work through connectivity issues.

9. Glossary System

Every guide and tool defines technical terms inline on first use (DNS, A record, MX, SPF, DKIM, DMARC, CSP, HSTS, ASN, PTR, RDAP, DNSBL, CA, SAN, OCSP, TLS, Safe Browsing). When a term recurs across pages, it links to the most detailed explanation in the Learn hub.

10. Methodology Center

The Methodology page documents, for each tool: **how it works** (data flow and resolvers), **limitations** (what it cannot tell you), and **how to interpret** a result. No tool is a black box.

Accuracy considerations

- IP geolocation is city-accurate at best.
- DNS results reflect what the queried resolver sees; propagation may differ regionally.
- Reputation is a real-time snapshot and can change minute to minute.
- DNSBL listings can include false positives — investigate, do not assume guilt.

11. Transparency Center

- Methodology — how every verdict is computed.
- Data sources — the upstream feeds and resolvers we query.
- Advertising disclosure — how affiliate links and ads work on the site.
- Privacy policy — what we collect and what we do not.
- Cookie policy — cookies by category, with GPC/DNT support.

12. Understanding Results

WHOIS records

Look for creation date (age), expiration (lapse risk), and registrar status codes (clientHold, pendingDelete signal trouble). Redacted contact data is normal.

DNS records

A/AAAA show where the hostname points. MX shows who handles email. TXT carries SPF and verification tokens. CAA restricts which CAs can issue certificates. NS lists the authoritative nameservers.

SSL information

Check the Common Name and SANs match the host you requested, the validity window has not started or ended too soon, and the issuer is a recognised public CA.

Domain & IP reputation

A verdict is a triage signal, not a final judgment. Pair it with WHOIS, domain age, and your own context.

Security headers

Missing CSP / HSTS / X-Content-Type-Options on login or payment endpoints is a real risk. On a static marketing page it is lower priority.

13. Frequently Asked Questions

Q. Is CheckItNowTools free?

A. Yes. Every core diagnostic is free, with optional Pro features for saved history, monitoring, and exports.

Q. Do I need an account?

A. No account is required for one-off checks. An account unlocks saved lookups and monitoring.

Q. Are my lookups logged?

A. By default we do not log lookup content. See the Privacy policy for full detail.

Q. Why does my IP geolocation look wrong?

A. IP geolocation is city-accurate at best, and ISPs reassign addresses across regions. Treat it as approximate.

Q. What is an ASN?

A. An Autonomous System Number identifies a network operator (e.g. an ISP or cloud provider). It is more stable than an IP for identifying who runs a network.

Q. Why is my domain blacklisted?

A. Common causes: a compromised mailbox sending spam, a shared IP poisoned by a neighbour, or an outdated SPF record. Investigate the listing reason on the upstream list.

Q. How long does delisting take?

A. After fixing the underlying issue, most DNSBLs delist within 24–72 hours.

Q. Is my SSL certificate working?

A. Run /ssl and confirm the SAN matches your host, the chain is complete, and expiration is more than 30 days out.

Q. What is SPF, DKIM, and DMARC?

A. Three email-authentication standards. SPF declares who can send mail for your domain, DKIM signs messages cryptographically, and DMARC tells receivers what to do when checks fail.

Q. What is a DNSBL?

A. A DNS-based blocklist. Mail servers query DNSBLs to decide whether to accept mail from a sending IP.

Q. What does a 'Caution' safety verdict mean?

A. There is at least one risk signal that needs human judgement before trusting the site — for example, very new registration or a missing security header on a login page.

Q. How do I check if a website is a scam?

A. Run the Website Safety Checker, then look at domain age, WHOIS, SSL, and reputation. Brand-new domains imitating a known brand are the most common pattern.

Q. What is reverse DNS?

A. The mapping from an IP address back to a hostname via the PTR record. Mail servers use it to filter spam; many consumer IPs have no PTR set.

Q. Why do my DNS changes not show up?

A. Resolvers cache records up to the TTL you set. Wait for the TTL to elapse and re-query.

Q. What is a VPN leak?

A. When your real IP, DNS resolver, or WebRTC endpoint becomes visible despite the VPN being active. The VPN Leak Test inspects all three.

Q. Is using a VPN illegal?

A. In most jurisdictions, no. Check your local laws and your employer's policy.

Q. What information does my browser expose?

A. User-Agent, language, timezone, screen, fonts, and WebGL signatures — together enough for fingerprinting. The Browser Info tool shows exactly what is visible.

Q. Is HTTPS enough for safety?

A. No. HTTPS encrypts the connection but says nothing about the operator's intent. Phishing sites also use HTTPS.

Q. What is a phishing domain?

A. A domain registered to imitate a real one, usually to steal credentials. Lookalike spelling, recent registration, and suspicious TLDs are the common signals.

Q. How do I report a phishing site?

A. Report to Google Safe Browsing, the brand being imitated, and the host's abuse contact (visible via WHOIS).

Q. Can you guarantee a verdict?

A. No. We aggregate public signals and explain our reasoning, but no diagnostic can replace human judgement and context.

Q. Do you sell my data?

A. No. We never sell or share lookup data.

Q. Does the site work on mobile?

A. Yes. Every tool is responsive and works in mobile browsers.

Q. Do you have an API?

A. Yes — request access via the Developers section.

Q. How can I contact support?

A. Email support@checkitnowtools.com.

14. Best Practices

Website safety

- Always check domain age and WHOIS before trusting a new site with credentials or payment.
- Hover over links before clicking — phishing URLs rarely match the visible text.
- Prefer typing the canonical domain over clicking unsolicited links.

Cybersecurity awareness

- Use a password manager — reuse is the single largest cause of account compromise.
- Enable multi-factor authentication everywhere it is offered.
- Keep browsers and operating systems patched.

Domain research

- Start with WHOIS to establish age and registrar.
- Cross-check with DNS, SSL, and reputation before drawing a conclusion.

DNS troubleshooting

- Verify the resolver — your machine, your router, and a public resolver may all see different records during propagation.
- Lower TTLs before a migration; raise them again once stable.

15. Privacy & Security

Privacy protections

- No lookup content is sold or shared with third parties.
- We respect Global Privacy Control (GPC) and Do Not Track (DNT) signals where applicable.
- Optional accounts; everyday checks require no signup.

Data handling

Authentication and account data are stored in our backend with row-level security. Lookup history saved to a Pro account is visible only to you. See the Privacy policy for the full data inventory.

Transparency commitments

Every diagnostic is documented on the Methodology page. Every upstream data source is named on the Data sources page. Commercial relationships (affiliate links, ads) are disclosed on the Advertising disclosure page.

16. Contact & Support

General support: support@checkitnowtools.com

Contact form: checkitnowtools.com/contact

For incident response, abuse reports, and partnership inquiries, please use the same address — your message will be routed to the appropriate team.