

CHECKLIST

Website & DNS Security Checklist

Your website, domain, Domain Name System (DNS) records and email domain are one attack surface, usually spread across several vendors. Work through this list with your web developer and IT team. Every "no" or "not sure" is worth a conversation.

Domain and registrar

- ☐ The registrar account is in the company's name, with a shared company email address as the contact, not a former employee's or agency's
- ☐ Multi-factor authentication (MFA) is on for every registrar user
- ☐ Only the people who need registrar access have it, and the list was reviewed recently
- ☐ Registrar lock (transfer lock) is on for every domain
- ☐ Auto-renew is on and the payment method is current
- ☐ For your most important domain, you have asked your registrar whether registry lock is available

DNS

- ☐ You know which company hosts your DNS, and MFA is on for that account too
- ☐ Domain Name System Security Extensions (DNSSEC) is enabled where your registrar and DNS host support it
- ☐ Every DNS record has a known purpose and owner
- ☐ Records that point to services you no longer use have been removed
- ☐ Protective DNS filtering is in place for your offices and company devices

Email domain

- ☐ Sender Policy Framework (SPF) record lists every service that sends email for you
- ☐ DomainKeys Identified Mail (DKIM) signing is on for your email platform and other senders
- ☐ Domain-based Message Authentication, Reporting and Conformance (DMARC) record is published and its reports are reviewed
- ☐ DMARC is at, or on a plan to reach, quarantine or reject
- ☐ Domains you own but do not send email from are protected against spoofing too

Website edge

- ☐ A web application firewall (WAF) is in front of the site
- ☐ Distributed denial-of-service (DDoS) protection is in place
- ☐ Transport Layer Security (TLS) certificates are tracked, auto-renew where possible, and outdated protocol versions are off
- ☐ Logins and forms are protected against automated abuse (for example rate limiting or bot management)

Website software and access

- ☐ Content management system, plugins and themes are current, and unused ones are removed
- ☐ Every admin account belongs to a named person, uses MFA and is still needed
- ☐ Hosting control panel access is limited and uses MFA
- ☐ Backups run on a schedule, are stored separately and a restore has been tested

Monitoring

- ☐ Someone is alerted if the site goes down
- ☐ Someone is alerted if key pages, DNS records or certificates change unexpectedly
- ☐ The site is scanned for malware and injected code on a schedule

Apps built with AI (artificial intelligence) tools

- ☐ Every app has a named business owner and technical owner
- ☐ Users sign in with company identity and MFA
- ☐ No passwords, keys or tokens are stored in the code
- ☐ The app runs in a company-owned cloud account, not a personal one

Note: No checklist or service can stop every attack. These steps make common attacks much harder and help you spot problems sooner.

[Book a free consultation](#)

BTI Communications Group | www.btigroup.com | Los Angeles main 562-298-5000
Managed IT: Los Angeles 323-510-8003 | Chicagoland 312-492-2613 | Phoenix 480-272-8728



WORKSHEET

Who owns what

Fill this in with your team, web developer and host. Gaps in the "Who" column are where problems hide.

Item	Who manages it (name and company)	Login has MFA?	Last reviewed
Domain registrar account			
DNS hosting account			
Website hosting account			
Website admin accounts			
Cloudflare or other WAF and DDoS service			
TLS certificates			
Email platform and DNS email records (SPF, DKIM, DMARC)			
Third-party services that send email as you			
Website backups			
Uptime, change and malware monitoring			
Apps built with AI tools			

Two kinds of DNS security

- **Your domain's DNS** protects your customers and anyone who emails you: registrar lock, MFA, DNSSEC, clean records, SPF, DKIM and DMARC.
- **Your staff's DNS lookups** protect your people: protective DNS filtering blocks known malicious domains before a connection is made.

WAF, DDoS protection and CDN (content delivery network)

- **WAF:** inspects each web request and blocks attack patterns.
- **DDoS protection:** absorbs floods of traffic so real visitors get through.
- **CDN:** serves copies of your site from nearby servers for speed; security features must be turned on.

Where BTI fits

BTI manages website and DNS security as part of managed IT: domain and registrar lockdown, protective DNS, DNSSEC, managed Cloudflare web security services, SPF, DKIM and DMARC with Email Security & Training, certificate management, website hardening and monitoring. Your web developer and host stay in place. Apps built with AI tools are a separate engagement led by BTI's vCISO (virtual chief information security officer) service.

Sources: Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA) protective DNS guidance ([cisa.gov](https://www.cisa.gov)); National Institute of Standards and Technology (NIST) SP 800-81r3, Secure DNS Deployment Guide ([csrc.nist.gov](https://www.nist.gov)); OWASP Top 10 ([owasp.org](https://www.owasp.org)); IETF RFC 7489 (DMARC).

[Book a free consultation](#)

BTI Communications Group | www.btigroup.com | Los Angeles main 562-298-5000
Managed IT: Los Angeles 323-510-8003 | Chicagoland 312-492-2613 | Phoenix 480-272-8728