DNS and domains: could someone hijack your domains or your DNS?

This month, put phishing-resistant MFA on every registrar and DNS provider account, registry-lock the few domains that sign-in, email and your website depend on, and publish CAA records on every domain. Then send all user DNS through a validating, filtering resolver you control, and sign zones with DNSSEC only where your provider automates the keys.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.2**	**IT and security teams in organizations of any size that own domains, run public DNS and resolve DNS for their users**

Latest version
sheets.einblick.dev/dns-domains/

If you only do five things

1. **Put phishing-resistant MFA on every registrar and DNS account.**
   In the campaign behind CISA's ED 19-01, attackers used stolen credentials to change DNS records, then got valid certificates to decrypt the redirected traffic[1]. Use security keys or passkeys.
2. **Registry-lock the domains everything depends on.**
   Anyone in your registrar account can ask to lift a registrar lock. A registry lock is set by the registry and can take longer to remove[5]; DENIC's .de lock needs a named contact to confirm each change[6]. Lock the domains behind sign-in, email, your website and name servers. Test an unlock, since the lock also delays urgent fixes.
3. **Make expiry impossible.**
   Use auto-renew on a company card and two trusted managers per domain[4]. Answer your provider's holder verification requests, or .de domains go offline and are later released[7].
4. **Publish CAA everywhere and watch CT logs.**
   Name the CAs you and your SaaS providers use, publish `issue ";"` on domains that need no certificates[19] and monitor CT logs for every domain, parked ones included[21]. Parked domains also need the DMARC record from the endpoints and email sheet.
5. **Send all user DNS through a resolver you control.**
   Validate DNSSEC, block known-bad domains with protective DNS, log queries and block DNS that goes around your resolvers[3].

If your domain or DNS is hijacked

1. **Check the delegation at the registry.**
   Query the TLD's name servers for your NS and DS records. Your DNS provider's console can look normal while the domain points elsewhere.
2. **Call your registrar and DNS provider.**
   Ask both to freeze the domain. If a gTLD domain was transferred away, only the registrars involved can file an ICANN transfer dispute, within 12 months[9], so push yours to act today.
3. **Lock the attacker out and restore.**
   Change the passwords and MFA of every account that can change DNS records, and audit every public record on all authoritative servers, as ED 19-01 required before CISA retired it in 2026[1,2]. Revoke API keys and compare against your last zone export.
4. **Hunt down certificates.**
   Find certificates issued during the hijack in CT logs and report them to the issuing CA[1]. CAA can't stop issuance during a hijack, but CAA bound to your ACME account stops attackers reusing that validation afterwards[21].
5. **Treat redirected traffic as stolen.**
   Reset passwords of users who signed in during the window, rotate secrets sent by email and check the EU security laws sheet for reporting duties.

Registrar and DNS provider accounts

- **One owner, several hands.** Move domains out of personal, agency and hosting accounts into ones your organization owns, and have one internal group register every domain[4].
- **Scope who can change records.** In Azure DNS, grant DNS Zone Contributor per zone and ReadOnly-lock zones that rarely change. A CanNotDelete lock on the SOA record blocks deleting the zone[11].
- **Alert on NS and MX changes** and keep DNS change logs in your SIEM[4]. Export every zone weekly as a known-good copy.
- **Report lookalikes to the registrar.** Monitor new registrations[3]. Registrars of gTLDs must act promptly on actionable evidence of phishing and other DNS abuse[10].

What your resolvers should do

- **Recurse only for your own clients.** No internet-facing server should be both authoritative and recursive[3].
- **Validate DNSSEC** with automatic trust anchor updates, two time sources and QNAME minimization[3].
- **Block DNS that goes around them:** outbound ports 53 and 853 except from your resolvers, and known public DoH servers[3].

DNSSEC and CAA

- **Sign only where your provider automates the keys.** DNSSEC can't stop someone who logs in to your registrar or DNS provider, but it lets CAs detect forged CAA records[19]. Use ECDSA P-256 or Ed25519; RSA/SHA-1 is deprecated[17].
- **Know what breaks.** Since 15 March 2026, CAs must validate DNSSEC and may not treat a validation error as permission to issue[18], so a broken signature also blocks renewals. Moving DNS provider? Pull the DS record and wait out its TTL first, as Route 53's guide does[13].
- **Bind CAA to your ACME account.** Let's Encrypt honors `accounturi` now[20]; list every account you renew with. All CAs must from 15 March 2027, and email validation ends on 15 March 2028[18].

Protective DNS and DNS over HTTPS

- **Small teams can start free.** Cloudflare's Zero Trust Free plan, for teams under 50 users, includes its web gateway and keeps logs 24 hours[22]. Quad9 welcomes business forwarders if it is their only upstream; log queries there yourself[23].
- **Otherwise buy one with logs and an API.** Ask for current deny lists, editable allow lists and block logs your SIEM can pull; Cloudflare exports logs only on contract plans[22]. It doesn't replace your own DNS logs[24].

- **Log queries.** Always log blocked queries, and keep a full log for forensics even if the SIEM gets less[3]. In Germany, agree per-user logs and their retention with the works council[15].
- **Practice turning off validation for one zone.** A faulty DENIC key rollover on 5 May 2026 broke .de names, signed or not, on validating resolvers; some large operators suspended validation for .de[14].
- **Want resolution kept in the EU?** DNS4EU's free resolver is for individuals only; companies use Whalebone Immunity, its commercial version on European infrastructure[25].
- **Control DoH in browsers.** Chrome sends no DoH on managed devices unless the `DnsOverHttpsMode` policy allows it[26]. Lock Firefox's `DNSOverHTTPS` policy to off or to your resolver's `ProviderURL`[27].

What changed in 2026

- **Three ccTLD registries were hijacked.** Attackers compromised the registries of .gh, .sl and .as, changed DNS records and got certificates for Google and other brands. Google advises restrictive CAA with ACME account bindings[21].
- **The root zone has a new key.** KSK-2024 (key tag 38696) has signed it since 11 October 2026. Check each validating resolver's trust anchors instead of assuming automatic updates worked[16].
- **.de verifies holder data.** Under NIS2, DENIC has risk-checked holder data since December 2025, now including a phone number, and existing domains can be asked to verify too[8,7]. Verification runs only through your provider, and DENIC never asks for passwords by email[7].
- **Windows DNS Server speaks DoH.** Since the June 2026 update, Windows Server 2025 accepts DoH from clients, but not toward upstream servers[28]. Clients can encrypt DNS without bypassing your resolver.

What you can skip

- **Buying every typo and new TLD.** Register near-misses of sign-in and payment domains; monitor and report the rest.
- **Signing internal zones.** NIST advises against it unless a rule requires it[3].
- **NSEC3 to hide your zone.** It often still reveals every name; NIST calls NSEC the more prudent choice[3].

Mistakes that cost the most

- **Domains in an account that can close.** Closing an AWS account suspends its Route 53 domains within 5 days[12].
- **Recovery email on the domain itself.** A hijacker then gets your password resets. Use an address on another domain.
- **Deleting the zone, not the delegation.** An attacker with an account at that DNS host may then take over the name[3].

What this looks like at your size

Small team, no security staff

- Move every domain into a registrar account you own, with two admins on security keys.
- Turn on auto-renew and registrar lock everywhere, and publish CAA for the CA you use.
- Point your firewall at business-ready protective DNS, such as Cloudflare's free plan or Quad9.

Growing, with IT or security staff

- Registry-lock the critical domains, export zones weekly and alert on NS and MX changes.
- Run validating resolvers with protective DNS and set browser DoH policies.
- Rehearse the hijack steps yearly with your registrar's real contacts.

Enterprise or regulated

- Consolidate at one corporate registrar with registry lock and named contacts.
- Require two-person approval for registrar and DNS changes.
- If you provide DNS for others, check NIS2 scope in the EU security laws sheet.

Version history

5 Nov 2026, version 1.2 Noted that CISA retired ED 19-01 in January 2026, added that German companies agree per-user DNS logs with the works council, and confirmed the transfer dispute rules still stand after ICANN's June 2026 policy decision.

Sources

1. The FDIC's Actions to Mitigate the Risk of DNS Infrastructure Tampering (on CISA ED 19-01). FDIC OIG, 24 Sep 2019. fdicoig.gov
2. CISA Retires Ten Emergency Directives. CISA, 8 Jan 2026. cisa.gov
3. SP 800-81r3, Secure Domain Name System (DNS) Deployment Guide. NIST, Mar 2026. nvlpubs.nist.gov
4. Managing public domain names. NCSC (UK), 25 Sep 2019. ncsc.gov.uk
5. EPP status codes. ICANN, checked 5 Nov 2026. icann.org
6. .de Registry Lock. DENIC, checked 5 Nov 2026. denic.de
7. Domain holder verification. DENIC, checked 5 Nov 2026. denic.de
8. What is changing about the registration of .de domains. DENIC, 19 Dec 2025. blog.denic.de
9. Registrar Transfer Dispute Resolution Policy. ICANN, updated 21 Feb 2024. icann.org
10. 2013 RAA amendment on DNS abuse, Section 3.18. ICANN, effective 5 Apr 2024. itp.cdn.icann.org
11. Protecting DNS zones and records. Microsoft Learn, updated 12 Aug 2026. learn.microsoft.com
12. Route 53 domains when an AWS account is closed. AWS Docs, checked 5 Nov 2026. docs.aws.amazon.com
13. Making Route 53 the DNS service for a domain in use. AWS Docs, checked 5 Nov 2026. docs.aws.amazon.com
14. Final Report: DNS Outage of 5 May 2026. DENIC, 11 Jun 2026. blog.denic.de
15. BetrVG, § 87. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
16. Root KSK rollover. ICANN, checked 5 Nov 2026. icann.org
17. DNSSEC algorithm guidance for registrars. ICANN, 20 May 2026. itp.cdn.icann.org
18. TLS Baseline Requirements, version 2.3.1. CA/Browser Forum, 4 Oct 2026. cabforum.org
19. RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record. IETF, Nov 2019. rfc-editor.org
20. CAA. Let's Encrypt, updated 4 Oct 2026. letsencrypt.org
21. Chrome's response to recent ccTLD registry hijacks. Google, 6 Oct 2026. blog.google
22. SASE and Zero Trust pricing. Cloudflare, checked 5 Nov 2026. cloudflare.com
23. DNS forwarder best practices. Quad9, checked 5 Nov 2026. docs.quad9.net
24. Protective DNS for the private sector. NCSC (UK), 9 Jun 2021. ncsc.gov.uk
25. Free public DNS resolver for Europe. DNS4EU, checked 5 Nov 2026. joindns4.eu
26. DnsOverHttpsMode policy definition. Chromium, checked 5 Nov 2026. github.com
27. DNSOverHTTPS policy. Firefox admin docs, checked 5 Nov 2026. firefox-admin-docs.mozilla.org
28. KB5094125 (OS Build 26100.32995). Microsoft Support, 9 Jun 2026. support.microsoft.com