CHECKLIST · TECHNOLOGY

The internet's master DNS key changes on 11 October. Most people won't notice, but some office networks should check

Published 11 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/root-dns-key-rollover-11-october-2026/

- [ ] **Find out who runs your DNS.** If it is your internet provider or a public DNS service, the operator is the one that has to hold the new key, and there is nothing to change on your own equipment.
- [ ] **Ask your IT provider whether your office runs its own validating resolver.** ICANN warns that some applications also use a resolver set when they were built or deployed.
- [ ] **Confirm the resolver trusts key tag 38696.** ICANN says to look in bind.keys for ISC BIND, root.key for Unbound and PowerDNS Recursor, and root.keys for Knot Resolver.
- [ ] **Turn on automatic trust anchor updates if the key is missing.** Check the resolver can write to its storage directory, then follow the software vendor's instructions.
- [ ] **Run Cloudflare's KSK-2024 readiness test at dnstest.dev/ksk-2024.** Cloudflare notes that a VPN or the browser's secure DNS setting changes which resolver is tested, and that an inconclusive result doesn't mean the key is missing.
- [ ] **Know the quick fix before you need it.** If lookups fail in the days after the switch, ICANN says the operator can temporarily turn off DNSSEC validation, install KSK-2024, then turn validation back on.

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.