

DOMAIN IMPERSONATION DEFENSE CHEATSHEET



The one-page reference for everything attackers do to your domain — and the checks that catch them. One typosquatted letter cost a company **\$545,000** (Cloud Security Alliance, Oct 2026).

1 THE 7 TYPOSQUAT FAMILIES

HOMOGLYPH paypal.com Lookalike Unicode: Cyrillic a for Latin a, rn for m	BITSQUAT bacebook.com One flipped bit in a letter; catches faulty-memory DNS lookups	COMBOSQUAT secure-yourbrand.com Your name + trusted words: secure, login, support, invoice	HYPHENATION your-brand.com Hyphen added or dropped where yours has none	TLD-SQUAT yourbrand.co Same name, different ending: .co .cm .io .net	SUBDOMAIN-SPOOF yourbrand.evil.com Your brand placed left of an attacker-owned domain	OMITTED DOT wwwyourbrand.com The dot dropped — www. fused into the name
--	--	--	---	--	---	---

2 CERTIFICATES & DNS POSTURE

CT MONITORING FREE Certificate Transparency logs are public records of every TLS certificate issued. A cert for your domain you didn't request = red flag. Why now: October 2026 reports say hackers forged valid TLS certs for Google domains (The Register, Oct 7) — Google now recommends all domain owners monitor CT logs. Free 10-second check: search your domain on crt.sh .	CAA RECORDS 2-MIN FIX A CAA record names which Certificate Authorities may issue for your domain. No CAA record = any CA worldwide can issue one. Setup: add at your DNS host: 0 issue "letsencrypt.org" (add 0 issuewild too if you use wildcard certs).	DMARC / SPF / DKIM GAP CHECK The 1-line check: look up the TXT record at _dmarc.yourdomain.com. No record = anyone can send email as your domain . Fix: publish SPF + DKIM, then DMARC starting at p=none — tighten to p=reject.
---	--	---

3 EARLY WARNINGS MOST OWNERS MISS

BEC EARLY WARNING MX records say where a domain receives email. A <i>lookalike</i> publishing MX records means someone set up mailboxes there — usually the first step before a CEO-fraud / invoice email goes out "as" you. Action: lookalike + MX records = investigate <i>today</i> , before the wire request arrives.	CANARY SUBDOMAINS — THE TRIPWIRE Plant a fake subdomain that should never exist — e.g. billing-verify-9f3.yourdomain.com — and watch CT logs for it. Why it works: nobody legitimate requests a cert for a subdomain only you know. ANY cert issued for it = you are being targeted right now.
---	--

4 TAKEDOWN: THE 3-REPORT PLAYBOOK

STEP 1 Registrar abuse report Look up the fake domain's registrar via WHOIS/RDAP ; report to their abuse contact with screenshots.	STEP 2 Host abuse report Find the host via IP lookup; file with the hosting provider's abuse desk — phishing pages get suspended fast.	STEP 3 Browser blocklists Report the URL to Google Safe Browsing so Chrome/Firefox/Safari warn visitors. safebrowsing.google.com/safebrowsing/report_phish/
--	---	--

Also file with Microsoft SmartScreen and PhishTank — and consider defensively registering your highest-risk variants: a few dollars a year beats a dispute.

5 THE 60-SECOND SELF-CHECK

☐ crt.sh → search your domain. A cert you didn't request? Investigate.	☐ CAA: dig CAA yourdomain.com. Empty? Any CA can issue for you.	☐ DMARC: TXT at _dmarc.yourdomain.com. None? You're spoofable.
☐ Dot test: visit wwwyourdomain.com. Not yours? Watch it.	☐ TLD test: check .co .cm .io .net versions. Registered = risk.	☐ MX test: a lookalike with MX records can email as you.

October 2026 — v1.0 · reviewed quarterly · For guidance only

FROM CHECKLIST TO COVERAGE

This sheet teaches what to check once.
DomainGuard monitors all of it, 24/7.

https://domain-guard-08k7.onrender.com/?utm_source=cheatsheet&utm_medium=pdf&utm_campaign=domain-guard

Monitor your domain free