

Can You Spot the Real Domain in 5 Seconds?

Lookalike domains • the psychology of trust • and why DNSSEC still matters

paypal.com



paypa1.com

same glance • different trust

Three links. Five seconds each.

Choose the domain you would trust enough to click. Don't call out the answer yet.

01

paypal.com

OR

paypa1.com

02

icann.org

OR

icann-org.com

03

apple.com

OR

apple.com

LOOK CLOSELY

All three are traps.

The visual difference can be tiny — while the trust decision is immediate.

paypa1.com

Typosquatting

1 replaces l

icann-org.com

Combosquatting / TLD swap

extra word/hyphen + different TLD

apple.com

Homograph / IDN spoofing

Cyrillic “a”

~3 sec

median URL-inspection time before trust

74%

phishing success with no inspection habit

Attention

the attacker’s target

Four patterns to recognize.

Once you know the patterns, the five-second check becomes more deliberate.

01 TYPOSQUATTING

Misspellings or adjacent keys

paypa1.com

02 COMBOSQUATTING

Brand + extra word or hyphen

paypal-secure-login.com

03 HOMOGRAPH / IDN

Look-alike characters from another script

apple.com

04 TLD SWAP

Same name, unexpected extension

icann.org → icann.top

This is industrial, not incidental.

The global phishing-domain landscape shows a large and expanding problem.

1.54M

unique phishing domains observed in May
2024–Apr 2025

+38%

year-over-year increase reported for that
period

77%

registered specifically to attack, rather
than hacked

The key shift: attackers often create infrastructure for the attack rather than waiting to compromise a legitimate site.

That makes domain registration and DNS policy part of the abuse conversation — not just the email inbox.

A Lebanon lens: the same trust problem, closer to the user.

Instead of treating Lebanon as a separate topic, use it as a concrete scenario for the global problem we just mapped.

1

MESSAGE

A user receives an SMS or WhatsApp link that appears to come from a familiar service.

2

GLANCE

The brand name looks right — but the domain may contain a small substitution, extra word or different TLD.

3

QUESTION

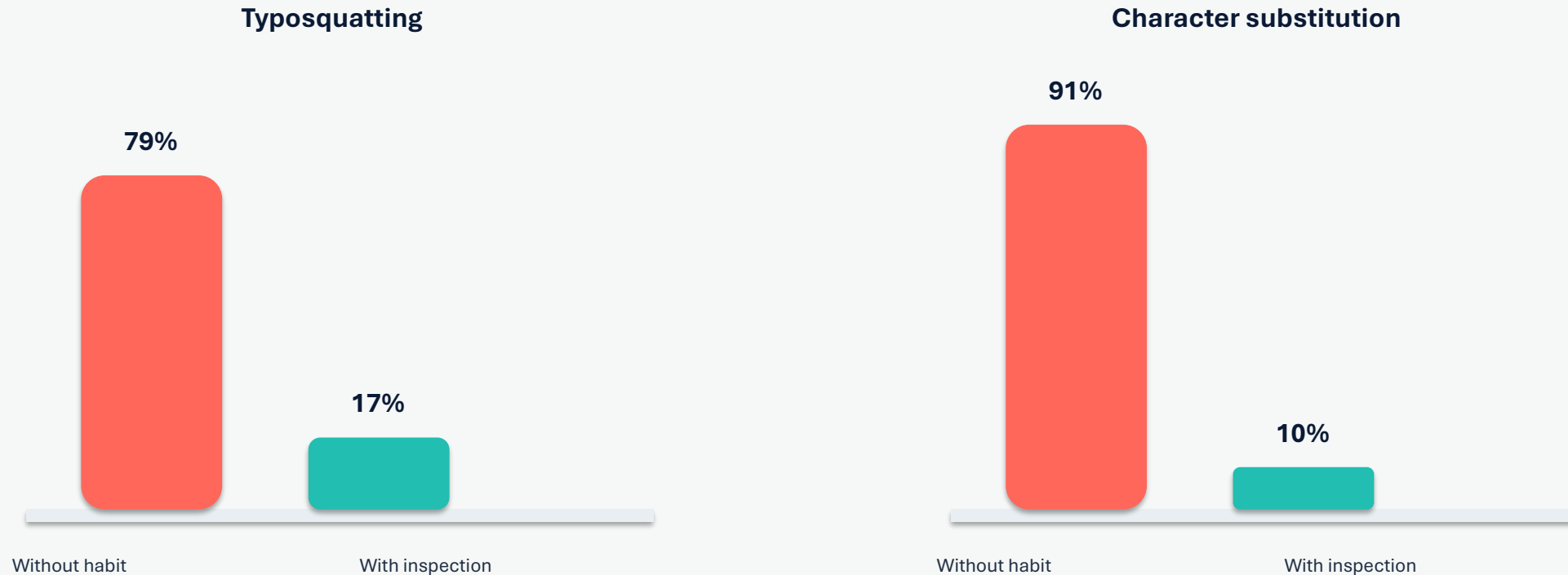
What protects the user: a better five-second habit, stronger platform controls, or both?

LOCAL APPLICATION — NOT A LEBANON-SPECIFIC ATTACK-RATE CLAIM

The global evidence tells us what to look for; the local lens asks how those lessons should be communicated and implemented.

Does slowing down actually work?

The study tested the exact behavior our quiz is asking people to adopt.



A short pause can dramatically reduce successful deception — but it does not solve every DNS problem.

What if the domain is correct — and you still get routed somewhere wrong?

At this point, human literacy reaches its limit.

CACHE POISONING

A resolver stores a forged DNS record for a legitimate domain.

ON-PATH SPOOFING

A forged DNS response is injected before the real answer arrives.

UNSIGNED DNS

Without cryptographic signatures, the resolver cannot verify the answer.

This is a protocol-trust problem, not a human-attention problem.

You can be excellent at spotting lookalikes and still depend on DNS answering honestly.

A second layer of trust — not a replacement for the first.

DNSSEC addresses forged DNS responses; it does not make lookalike domains disappear.

WHAT IT DOES

- ✓ Cryptographically signs DNS records.
- ✓ Lets validating resolvers verify the response.
- ✓ Helps prevent forged answers from being trusted.

WHAT IT DOES NOT DO

- ✗ Does not stop typosquatting or homographs.
- ✗ Does not encrypt DNS traffic.
- ✗ Needs both a signed zone and a validating resolver.

Human layer + DNS layer = complementary protection

The pieces exist — but end-to-end protection is still limited.

Global telemetry shows progress, but a large gap between capability and actual validation.

11.53%

queries handled by resolvers that support DNSSEC validation

8.22%

queries reaching a signed zone

0.62%

queries both reaching signed zones and validated end-to-end

≈ 6 in 100

of potentially protectable queries were actually protected end-to-end in this telemetry view

End-to-end validation was reported up 68% year over year — from 0.37% to 0.62%.

Three ideas to take away.

The presentation started with a five-second glance. It ends with a two-layer model of trust.

01

SLOW THE GLANCE

Build deliberate domain inspection into user habits and interface design.

02

CLOSE THE DNSSEC GAP

Zones need signing; resolver operators and ISPs need validation.

03

TEACH IT EARLY

Domain-trust literacy and DNSSEC awareness belong in onboarding and public education.

The goal is not perfect users. It is a safer system with more than one layer of trust.

SOURCES

Reports and research used in this presentation.

- 1 Interisle Consulting Group — Phishing Landscape 2025 (May 2024–Apr 2025).
- 2 Anti-Phishing Working Group (APWG) — Phishing Activity Trends Report, Q1 2026.
- 3 Cloudflare Radar DNS/DNSSEC telemetry, analyzed by TechnologyChecker.io, August 2026.
- 4 Lain, Nakatsuka, Kostianen, Tsudik & Capkun — “URL Inspection Tasks: Helping Users Detect Phishing Links in Emails,” USENIX Security 2025.
- 5 ICANN OCTO — Domain Abuse Activity Reporting (DAAR) / Domain Metrica archive.
- 6 Zheng, Xudong — “Phishing with Unicode Domains” (2017), used for the IDN homograph example.