1. TYPOSQUATTING / DOMAIN SQUATTING

Attackers register domains that closely resemble legitimate ones, hoping users won’t notice small mistakes.

These domains might swap letters, add numbers, or use characters that look similar, such as:

micorsoft.com, facebo0k.com, or rnicrosoft.com (r+n made to look like m).

WHAT IS TYPOSQUATTING?

Attackers create domains that look similar to legitimate ones, such as:

micorsoft.com

faceboOk.com

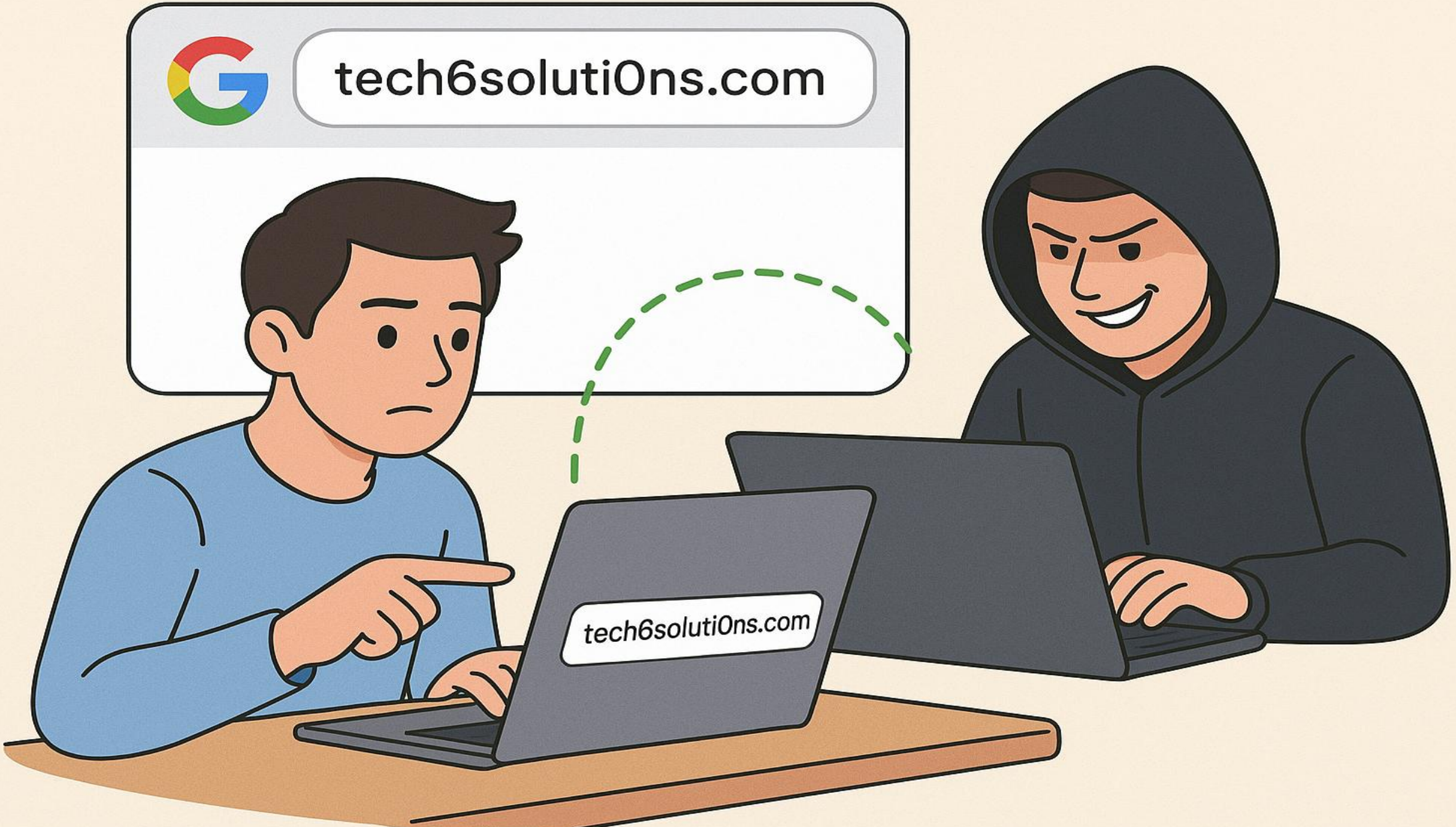
rnicrosoft.com

(r+n looks like m)

Scenario: Arham Opens “Tech6Soluti0ns.com”

He clicks the first result he sees: tech6soluti0ns.com. The attacker replaced the letter “o” with a zero.
The website looks completely identical to the real one, but it silently captures any credentials Arham enters, giving the attacker full access.

Lesson: Always double-check URLs for small spelling changes or unusual characters, especially when logging in or entering sensitive information.


tech6soluti0ns.com
tech6soluti0ns.com

Why Typosquatting Works?

- Employees type URLs manually
- Attackers buy misspelled domains
- Copy exact design of original website
- Users don’t verify spelling

How to Detect Lookalike Domains?

- Check for numbers replacing letters
- Beware hyphens or extra characters
- Look for HTTPS but still inspect URL carefully
- Never trust links from unknown sources

Prevention Tips

- Bookmark official corporate URLs
- Avoid typing URLs under pressure
- Train employees in visual domain inspection