2. HOMOGRAPH / IDN SPOOFING

Homograph spoofing is a technique where attackers use foreign or look-alike characters in domain names to make fake websites look legitimate. These characters appear identical to normal letters, tricking users into trusting the site.

Examples include:

- google.com (uses Cyrillic “o” instead of English “o”)
- paypal.com (capital “I” instead of “l”)
- microsoft.com (one Cyrillic “o” hidden among real ones)
- apple.com (uppercase “I” instead of lowercase “l”)

Scenario: Maryam Clicks a Fake VPN Portal

Maryam receives a message from “IT” with a link to “update her VPN settings”:

https://vpn-tech6solutions.com

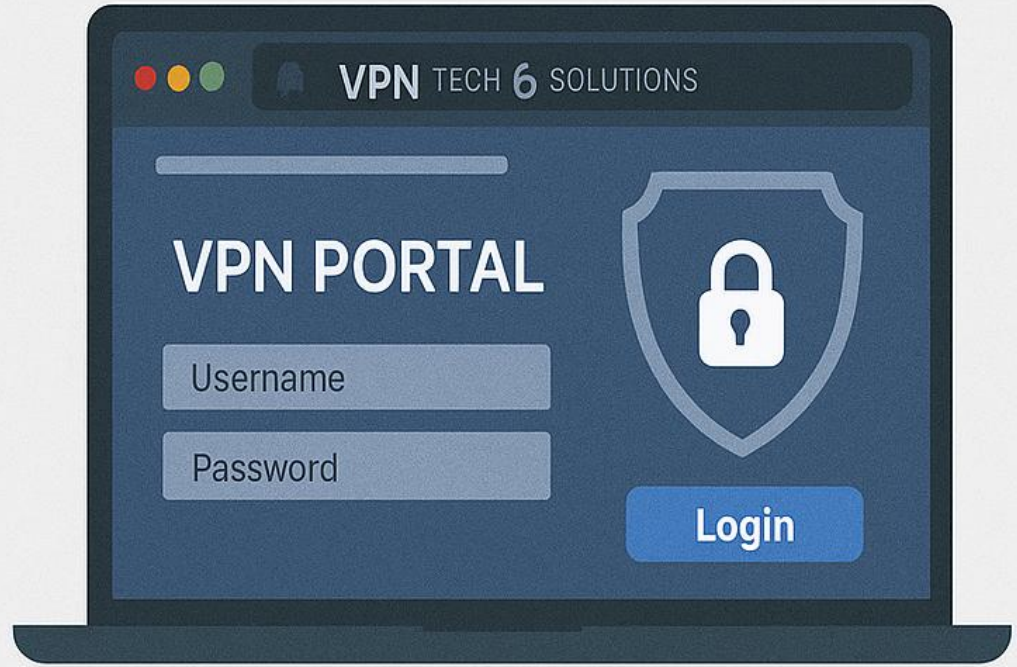
At first glance, everything looks normal — but the “o” in solutions is actually a Cyrillic character that looks almost identical to the real English “o.”

When Maryam opens the site, it loads a perfect clone of the company’s VPN login page. The moment she enters her username and password, the attacker captures her credentials and gains access to the real VPN.

Lesson: Always check URLs carefully before logging in, especially for VPN, email, or cloud portals. Even a single foreign or look-alike character can turn a trusted site into a credential trap.

Maryam receives a link from “IT”:
https://vpn-tech6solutions.com

But the “o” is Cyrillic, not English.



The website is a perfect clone used to steal credentials.

How Attackers Create These Domains?

- Unicode characters
- International domain registration
- Custom fonts
- Fake SSL certificates

How to Spot Homograph Attacks?

- Copy URL into Notepad (strange characters appear)
- Hover over links before clicking
- Pay attention to tiny visual differences

Prevention Tips

- Use password managers—they detect fake domains
- Use browser protection tools
- Double-check any login page sent via email