

Forum:[Hack Forums](#)

Thread: [What is a Homoglyph Attack and how hackers use this in 2025](#)

JoseMar - February 10, 2025, 10:01 am

What is a Homoglyph Attack
and how hackers use this in 2025

A Homoglyph Attack is a form of cyber attack where attackers use characters that look alike from various alphabets or character sets to mislead users. This method is often seen in phishing, domain spoofing, and impersonation attacks.

How It Works: Attackers substitute letters in a real URL, username, or email with characters that appear similar.

This deceives users into clicking harmful links or engaging with fake profiles.

Numerous homoglyph attacks take advantage of Unicode characters, making them difficult to spot at first glance.

Look this: the Latin letter "O" (U+004F) and the Cyrillic letter "?" (U+041E) may look the same, but they are distinct characters encoded differently by computers...

Example of a Homoglyph Attack: Legit site: paypal.

com Fake site: paypal.

com (The capital "I" replaces the lowercase "l") Another fake: ?aypal.

com (The "p" is actually a Cyrillic "?", not a Latin "p")

More Examples:

Is It Still Working in 2025?

Yes! Homoglyph attacks is still a serious threat in 2025.
Phishing sites still use homoglyphs to deceive users.

Social engineering attacks utilize fake usernames to impersonate trusted individuals.

Email spoofing using homoglyphs still gets around some security filters.

How to Protect Yourself:

Verify URLs – Manually enter website addresses instead of clicking on unfamiliar links.

Enable MFA (Multi-Factor Authentication) – Even if your credentials are stolen, attackers can't log in.

Use Security Tools – Some modern browsers and email services identify homoglyph attacks.

Check SSL Certificates – Look for HTTPS and official domain registrations.

Generating a Domain Name with EvilURL for a Homoglyph Attack

I use EvilURL to generate homoglyph domain names and check if they are available for purchase to create a phishing ready website!

Step 1: Using EvilURL v3.0

Once installed, navigate to the EvilURL directory and run the following command in the terminal:

```
Code python3 evilurl.py -g -d instagram.com
```

Copy the red domain name and check its availability for purchase, for example, on NameCheap.

Step 2: Enhancing Phishing Realism

To make the phishing attack more convincing, buy an SSL certificate and install it. This way, the URL will appear as <https://instagram.com>, making it look more legitimate.

Alternative Method: Online Generator

If EvilURL doesn't work, you can use an online tool:

[IronGeek Homoglyph Attack Generator](#)

Enter the target domain name, and the tool will replace characters with similar-looking ones while keeping the domain appearance almost identical.

Step 3: Detecting Phishing Links with EvilURL

If you receive a suspicious message containing a link to sites like Facebook, Instagram, or YouTube, you can verify its legitimacy using EvilURL.

Copy the link and save it in a file (e.g., test.txt) inside the EvilURL directory.

Run the following command in the terminal:

```
Code python3 evilurl.py -f /home/parrot/EvilURL/test.txt
```

EvilURL will analyze the link and highlight any altered characters.

Example: If the letter "s" in "instagram.com" is replaced with a similar looking character, EvilURL will detect the phishing attempt.

Final Tip: Always be careful with links, particularly in emails, messages, or ads. If something seems slightly "off," double-check before clicking!

I started this thread to show a simple example of Homoglyph Attacks using sites like Instagram or PayPal; however, in actual situations, hackers usually stay away from famous domains because they are simpler to identify. Instead, they perform homoglyph attacks on smaller, less noticeable domains to deceive victims.

They will send phishing emails or messages with some fake links that seem real but actually will direct to homoglyph websites. The purpose of this thread is to show you how these attacks works, but remember that cybercriminals (hackers) are more clever and inventive methods in this type of attacks

7 - February 10, 2025, 10:04 am

Great tutorial.

Also the use of subdomains is quite common

I owned the domains com-accountrecovery.app and net-accountrecovery.app too

Literally subdomain anything.com-accountrecovery.app

I didnt use them so no criminal charges brought to me from this, merely for demonstration purposes

JoseMar - February 10, 2025, 10:10 am

(Feb 10, 2025 11:04 AM)7 Wrote: [\[CITE\]](#) Great tutorial.

Also the use of subdomains is quite common

I owned the domains com-accountrecovery.app and net-accountrecovery.app too

Literally subdomain anything.com-accountrecovery.app

I didnt use them so no criminal charges brought to me from this, merely for demonstration purposes
Thanks! I appreciate mate. You're absolutely right about using subdomains is another common tactic in homoglyph attacks.

JoseMar - February 10, 2025, 10:27 am

(Feb 10, 2025 11:20 AM)Lowkey Wrote: [\[CITE\]](#) I've known about this but did not ever know what the name was called.

Neat!

Three years ago, when I first learned about Homoglyph Attack tactics, it completely blew my mind. I initially used it as a demonstration for my friends, explaining how it works and how easily hackers can trick people.

JoseMar - February 10, 2025, 10:53 am

(Feb 10, 2025 11:40 AM)Lowkey Wrote: [\[CITE\]](#) I triple check URL's and more in emails.
I'm glad, this is what we need to do??

m0narch - February 10, 2025, 12:32 pm

good small write up Jose! :P

JoseMar - February 10, 2025, 2:14 pm

(Feb 10, 2025 01:32 PM)m0narch Wrote: [\[CITE\]](#) good small write up Jose! :P
Glad you like it mate, your time now ?