Tool Name:**Homoglyph Puzzle Generator**

By: Ankita Laxman Kolapte

Intern ID: 270

Description:

It is a Python-based security awareness tool that creates phishing-like domain variations using Unicode homoglyphs. It allows cybersecurity teams to simulate IDN homograph attacks, demonstrating how legitimate-looking URLs can be manipulated for social engineering. This helps train users to spot deceptive links before falling victim to phishing campaigns.

Objective /Purpose of the Tool:

The main goal of the Homoglyph Puzzle Generator is to demonstrate and raise awareness about IDN homograph attacks by simulating phishing scenarios. It helps users, security teams, and trainees recognize how visually deceptive URLs can be crafted using Unicode characters, so they can detect and avoid clicking on malicious links in real-world situations.

Key Characteristics / Features:

1. Homoglyph Domain Generation : Replaces Latin characters with visually similar Unicode characters to create deceptive domains.

2. Phishing Simulation : Generates realistic phishing-style alerts and notifications using homoglyph domains.

3. Custom Domain Input: Allows users to enter any domain for targeted simulation.

4. Unicode Exploitation Demonstration – Highlights how IDN (Internationalized Domain Name) attacks work.

5. Security Awareness Training : Educates users to recognize and avoid suspicious links.

6. Lightweight Implementation : Python-based, minimal setup, easy to run on multiple systems.

7. Cross-Platform Compatibility : Runs on Windows, macOS, and Linux environments.

8. Open-Source Friendly : Can be customized or extended for different security use cases.

9. Fast Execution : Quickly generates multiple phishing-like domains within seconds.

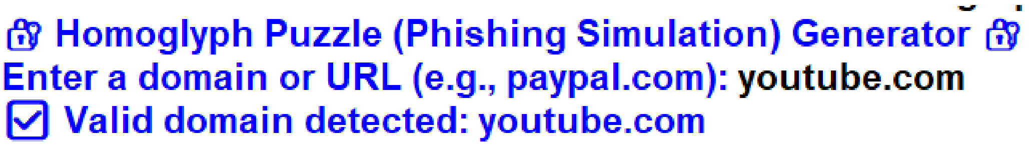
10. Research & Forensics Use : Helps in cybersecurity research, phishing detection testing, and digital forensics.

How Will This Tool Help?

- 1. Demonstrates homoglyph-based phishing attacks.
- 2. Trains users to recognize fake URLs.
- 3. Supports phishing simulation exercises.
- 4. Assists in early detection of suspicious domains.
- 5. Useful for cybersecurity awareness and education.

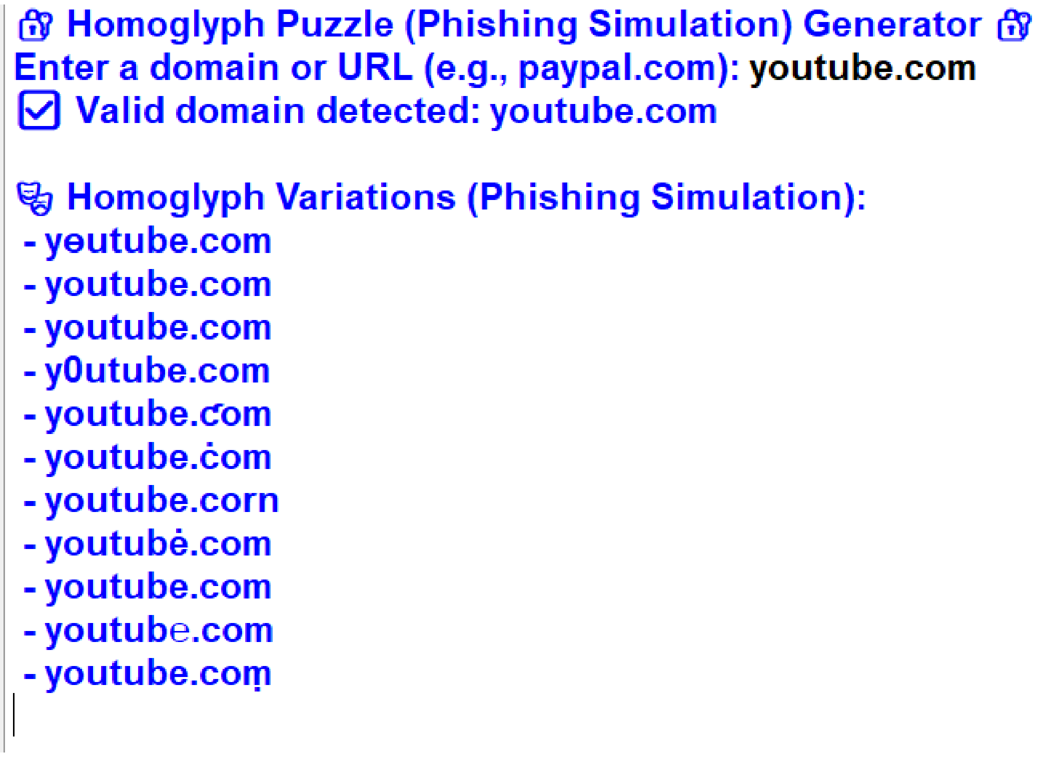
Proof of Concept (PoC)

1. Tool Startup:



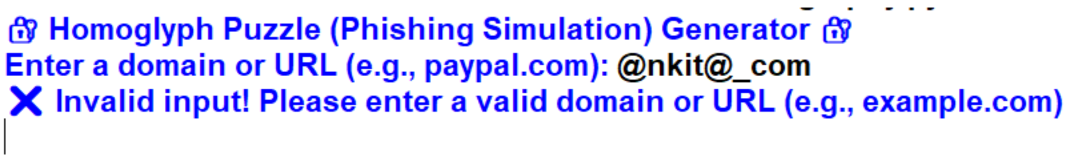
```
🔐 Homoglyph Puzzle (Phishing Simulation) Generator 🔐
Enter a domain or URL (e.g., paypal.com): youtube.com
☑ Valid domain detected: youtube.com
```

2. Valid Domain Input:



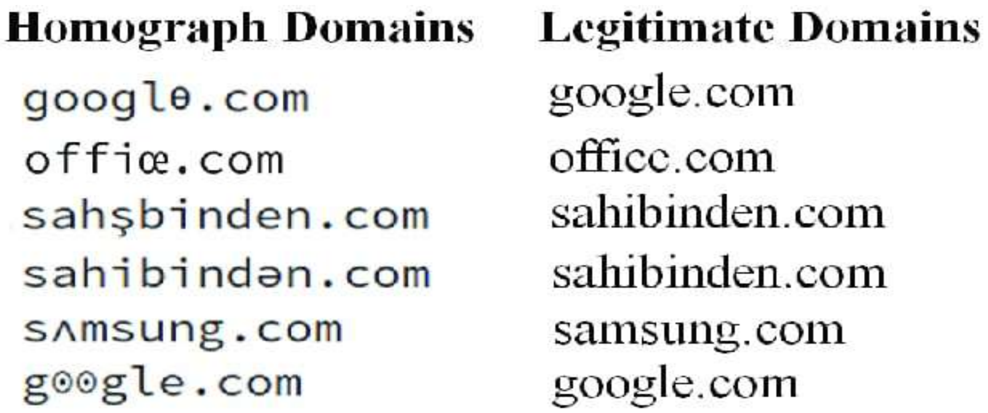
```
🔐 Homoglyph Puzzle (Phishing Simulation) Generator 🔐
Enter a domain or URL (e.g., paypal.com): youtube.com
☑ Valid domain detected: youtube.com

🎭 Homoglyph Variations (Phishing Simulation):
 - yɵutube.com
 - youtube.com
 - youtube.com
 - y0utube.com
 - youtube.ƈom
 - youtube.ċom
 - youtube.corn
 - youtubė.com
 - youtube.com
 - youtubе.com
 - youtube.coṃ
```

3. Invalid Domain Input:



```
🔐 Homoglyph Puzzle (Phishing Simulation) Generator 🔐
Enter a domain or URL (e.g., paypal.com): @nkit@_com
❌ Invalid input! Please enter a valid domain or URL (e.g., example.com)
```

4. Spot the Difference: How Homograph Attacks Imitate Real Domains :



Homograph Domains	Legitimate Domains
googlɵ.com	google.com
offiœ.com	office.com
sahşbinden.com	sahibinden.com
sahibindən.com	sahibinden.com
sʌmsung.com	samsung.com
g⊙⊙gle.com	google.com

Time to Use / Best Case Scenarios:

- ,During cybersecurity training to teach employees how to spot fake URLs.
- While conducting phishing simulations to evaluate awareness levels.
- Before clicking suspicious links in emails, chats, or social media.
- In security awareness campaigns as a demo tool.
- For penetration testing teams to simulate IDN homograph attacks.

When to Use During Investigation:

- When analyzing phishing incidents to identify malicious homoglyph domains.
- While reviewing suspicious email links to confirm if they are look-alike domains.
- During digital forensics to detect domain spoofing techniques.
- In threat hunting to find patterns of homoglyph usage in network logs.
- While correlating threat intelligence data to uncover IDN homograph campaigns.

Best Person to Use This Tool :

- Cybersecurity Analysts – for detecting phishing attempts and domain spoofing.
- Digital Forensics Investigators – for analyzing suspicious domains during incident response.

- SOC (Security Operations Center) Teams – for monitoring and validating suspicious URLs in alerts.
- Threat Intelligence Analysts – for identifying patterns of homoglyph-based attacks.

Required Skills:

- Basic Python Knowledge – to run or modify the script.
- Understanding of Phishing & Social Engineering – to interpret suspicious domain usage.
- Knowledge of IDN Homograph Attacks – to recognize Unicode-based look-alike characters.
- Familiarity with Cyber Threat Investigation – to integrate tool results into larger cases.

Flaws / Suggestions to Improve:

- 1. Add detection mode to scan text and highlight suspicious homoglyph domains.
- 2. Integrate WHOIS lookup to check domain registration details.
- 3. Assign phishing risk scores to generated or detected domains.
- 4. Support bulk domain processing from input files.
- 5. Export investigation results in PDF or CSV format for reports.

Good About the Tool:

- 1. Simple and lightweight, easy to run on any system.
- 2. Effectively demonstrates real phishing attack techniques.
- 3. Increases user awareness of homoglyph domain threats.
- 4. Customizable for different domains and scenarios.
- 5. Useful for both training and security investigations.

In summary:

The Homoglyph Puzzle Generator is a lightweight Python tool that simulates IDN homograph attacks by generating phishing-like domain names using visually similar Unicode characters. It helps cybersecurity professionals, investigators, and educators demonstrate how attackers disguise malicious domains to look like legitimate ones. This tool is valuable for awareness training, phishing simulations, and digital investigations, making it easier to identify and mitigate such threats before real-world exploitation occurs.

Submitted to: Digisuraksha Parhari Foundation