Finding **Impersonating Phishing Domains** with urlscan.io

1. Introduction

This guide explains how to use urlscan.io to detect phishing domains impersonating legitimate brands (e.g., PayPal, Microsoft, or banks). You can search for suspicious domains by analyzing:

- Page titles (e.g., fake login pages)
- Domain names (e.g., paypal-security.com instead of paypal.com)
- Recent scans (last 30 days)

2. Basic Search Queries

A. Find Fake Login Pages by Title

Example: Find pages with "PayPal" in the title but not on PayPal's official domain.

```
page.title:"PayPal" AND NOT page.domain:"paypal.com"
```

✅ Use case: Detects phishing sites pretending to be PayPal.

B. Find Lookalike Domains

Example: Find domains containing "paypal" but not the real paypal.com.

```
domain:*paypal* AND NOT domain:paypal.com
```

✅ Use case: Catches typosquatting domains (e.g., paypal-login.net).

C. Search for Phishing Pages with Login Forms

Example: Find fake PayPal login pages with forms.

```
page.title:"PayPal" AND NOT domain:paypal.com AND task.method:form
```

✅ Use case: Identifies credential-stealing pages.

3. Advanced Search Techniques

A. Filter by Time (Last 30 Days)

```
page.title:"PayPal" AND NOT domain:paypal.com AND date:>=now-30d
```

✅ Use case: Finds recent phishing attempts.

B. Search by Suspicious TLDs (.xyz, .top, etc.)

Phishers often use cheap domains.

```
page.title:"PayPal" AND (domain:*.xyz OR domain:*.top)
```

✅ Use case: Detects phishing sites on high-risk domains.

C. Find Typosquatting Domains (Misspellings)

```
domain:*paypall* OR domain:*payypal* OR domain:*paypal-login*
```

✅ Use case: Catches common misspellings.

4. Best Practices

✔ Check WHOIS data – Look for recently registered domains.https://www.whoxy.com/

✔ Report phishing – Submit malicious URLs to Google Safe Browsing or PhishTank.

✔ Monitor regularly – Run searches weekly to catch new threats.

---

5. Troubleshooting

❌ No results?
→ Try a broader search (e.g., domain:*paypal*).
→ Check if the site was recently scanned.
❌ API not working?
→ Ensure you have a valid API key.
→ Check rate limits (free tier: 100 requests/day).

---

6. Conclusion

By using urlscan.io's search syntax, you can efficiently detect phishing domains impersonating trusted brands. Combine these techniques with WHOIS checks and automated scanning for better security.

🔗 Need help? Visit urlscan.io/docs for official documentation.

📌 Note: Replace "PayPal" with other brands (e.g., "Microsoft", "Bank of America") to adapt searches. Would you like a more detailed guide on automating scans? 🚀