

PHISHING BAIT

UNDERSTANDING AND
DEMONSTRATING REAL-WORLD
PHISHING ATTACKS



Presented By:

ELI DAVID AND AZSANTE HAWKINS

June 9, 2025



INTRODUCTION TO PHISHING

WHAT IS PHISHING?

- A method of tricking users into revealing sensitive data.
- Often done through fake websites, emails, or messages.
- One of the most common and effective cyber threat



COMMON PHISHING TECHNIQUES



Spear Phishing

- A highly targeted form of phishing.
- Attacker customizes emails or messages using specific details about the victim (name, job title, contacts).
- Often appears to come from a trusted source, such as a colleague or supervisor.



Whaling

- A specialized type of spear phishing aimed at high-level executives or key decision-makers.
- Attacks often mimic urgent business requests, like wire transfers or document sign-offs.
- Success can lead to significant financial or identity damage.

COMMON PHISHING TECHNIQUES



Smishing

- Phishing conducted through SMS or messaging apps.
- Messages may include malicious links, fake alerts, or requests for login details.
- Frequently impersonates delivery services, banks, or tech support.



Vishing

- Voice phishing via phone calls.
- Attackers may pose as government agents, bank officials, or tech support.
- Goal is to verbally extract sensitive information like account credentials or social security numbers.

WHY IT MATTERS

WHY IS PHISHING SO DANGEROUS?

- Exploits human trust and behavior
- Often leads to data breaches, financial loss, and identity theft
- Users tend to reuse passwords across multiple accounts





CYBERSECURITY'S ROLE

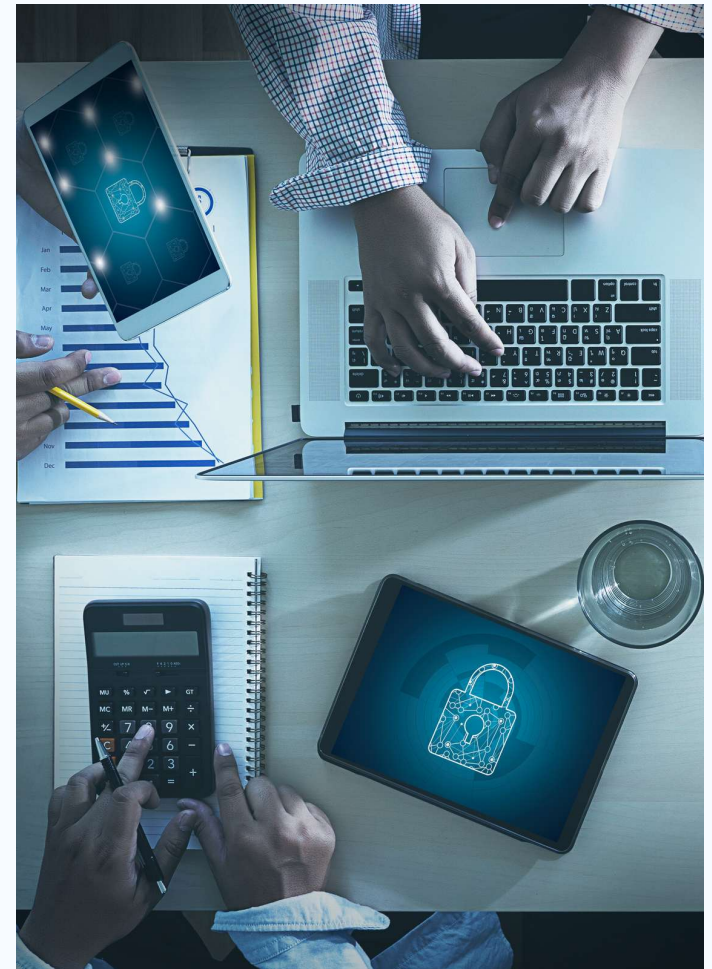
OUR JOB IN CYBERSECURITY



PROJECT OBJECTIVE

PURPOSE OF OUR PROJECT

- ✓ Demonstrate how phishing attacks are executed
- ✓ Raise awareness about common tactics
- ✓ Show how stolen credentials can be misused
- ✓ Promote education and prevention



TOOLS USED

TOOLS FOR THE ATTACK SIMULATION



SOCIAL-ENGINEER TOOLKIT (SET)

For cloning websites



KALI LINUX

The operating system used



DNS SPOOFING

Redirected victims to a fake site

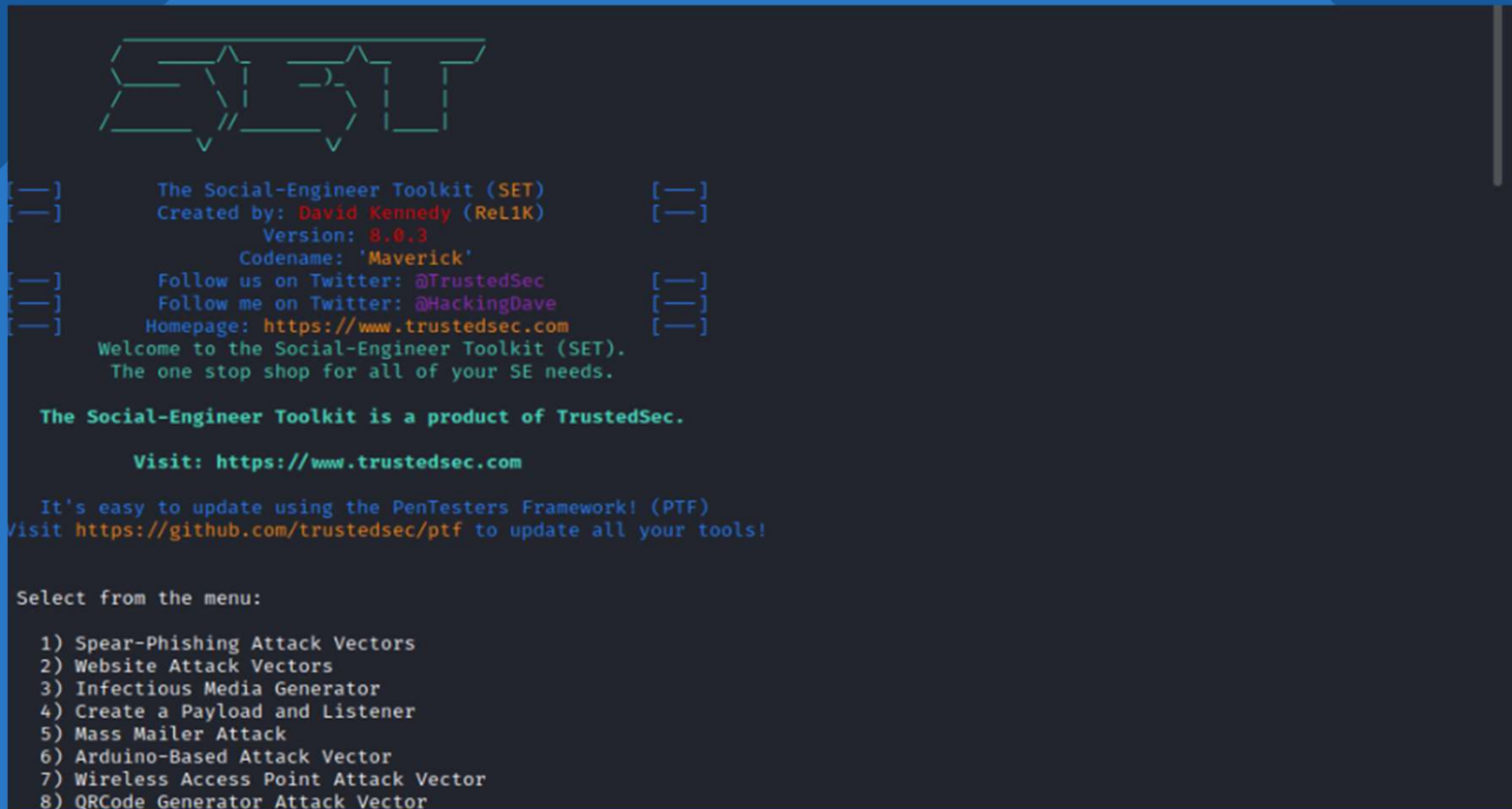
ATTACK SCENARIOS

HOW WE DID IT

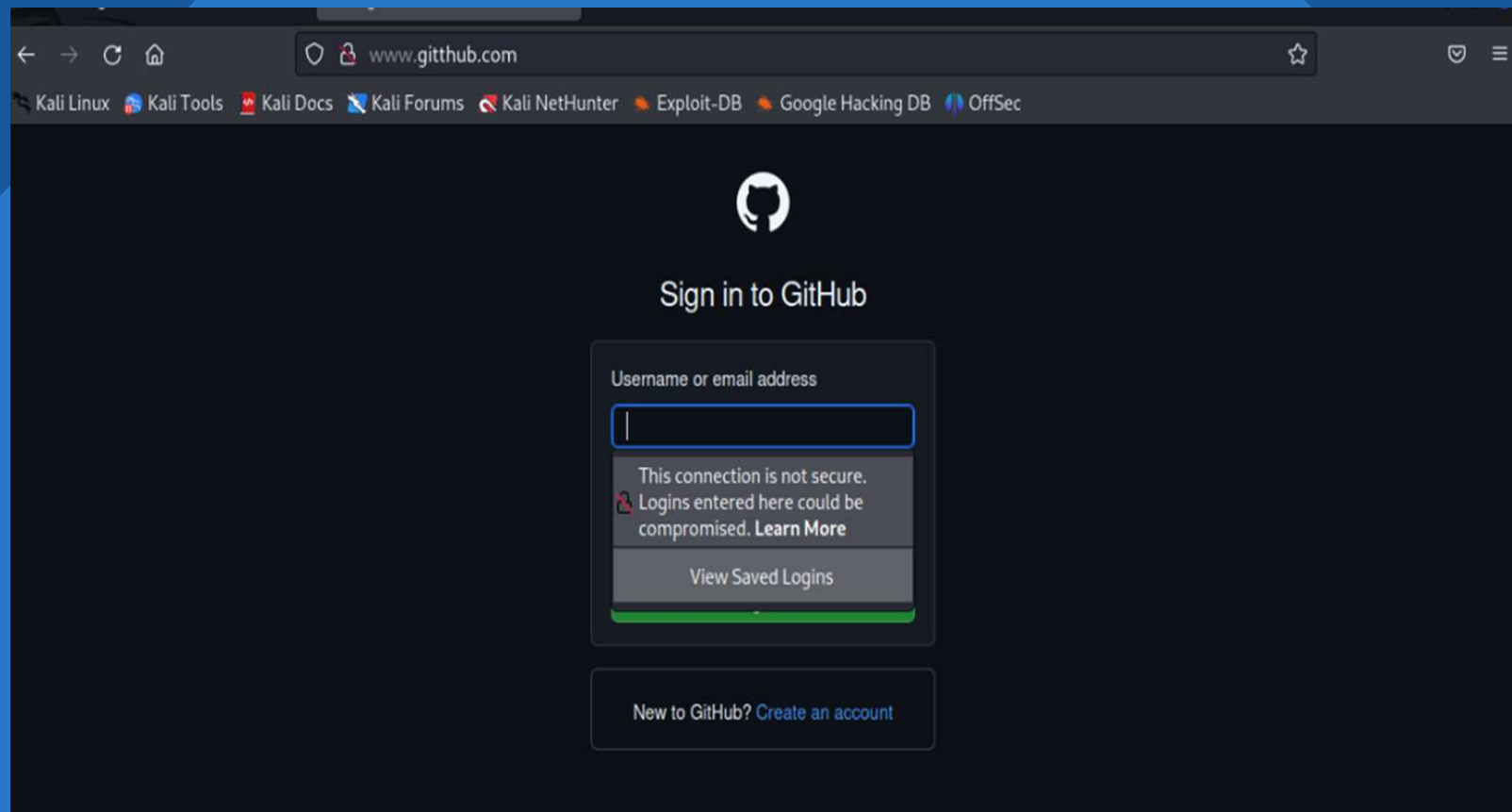
- Cloned LinkedIn login page using SET
- Used DNS spoofing to reroute github.com to our fake site
- Created a phishing email with a malicious link
- Sent email to a fictional executive (John Doe)
- Collected credentials entered on the fake page



SOCIAL ENGINEERING TOOL



CLONED WEBSITE (SET)



DNS SPOOFING

```
GNU nano 7.2                                hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.debian.tpl
# b.) change or remove the value of 'manage_etc_hosts' in
#    /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 ip-172-31-0-143.us-west-2.compute.internal kali
127.0.0.1 localhost
172.31.0.143 www.gitthub.com

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

EMAIL DRAFT

Audit Please Loggin  Inbox x



Azsante Hawkins <azsantehawkins33@yahoo.com>
to me ▾

5:51 PM (4 minutes ago) ★ 😊 ↶ ⋮

Hi [Azsante],

As part of our ongoing internal security audit, we're asking all administrators to verify their access credentials through our secure portal.

Please log in at your earliest convenience to complete the verification process:

[gittub.com](#) (Secure Internal Access Only)

This is a routine measure to ensure compliance with our updated infrastructure access policies. If you encounter any issues accessing the portal or have questions, reach out to [IT/Security contact] immediately.

Thank you for your prompt attention to this matter.

Best regards,

[Darnell Hawkins]

Chief Executive Officer

GitHub

[\[darnellhawkins@gitthub.com\]](#)

COLLECTION OF INFORMATION

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] The Social-Engineer Toolkit Credential Harvester Attack

[*] Credential Harvester is running on port 80

[*] Information will be displayed to you as it arrives below:

172.31.0.143 - - [08/Jun/2025 20:13:40] "GET / HTTP/1.1" 200 -

[*] WE GOT A HIT! Printing the output:

PARAM: commit=Sign+in

PARAM: authenticity_token=PiHPQbbh9Gvi8xbPr03v8KNJT8a2Qw2ffZ5V64cJnVcNt8cW7/c7MmeNSg0hrF7BGN7mYAbEwgaQ9NksU3i8YA==

PARAM: add_account=

POSSIBLE USERNAME FIELD FOUND: login=Azsante

POSSIBLE PASSWORD FIELD FOUND: password=DavidBates19!

PARAM: webauthn-conditional=undefined

PARAM: javascript-support=true

PARAM: webauthn-support=unsupported

PARAM: webauthn-iuvpaa-support=unsupported

POSSIBLE USERNAME FIELD FOUND: return_to=https://github.com/login

PARAM: allow_signup=

PARAM: client_id=

PARAM: integration=

PARAM: required_field_8e7a=

PARAM: timestamp=1749413597566

POSSIBLE PASSWORD FIELD FOUND: timestamp_secret=7ad8354dd20e0c2165998d7368d93197506a9f8e35b3e523142dcecc9de41a65

[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

172.31.0.143 - - [08/Jun/2025 20:13:53] "POST /session HTTP/1.1" 202 -

REAL WORLD IMPACT

THE CONSEQUENCES



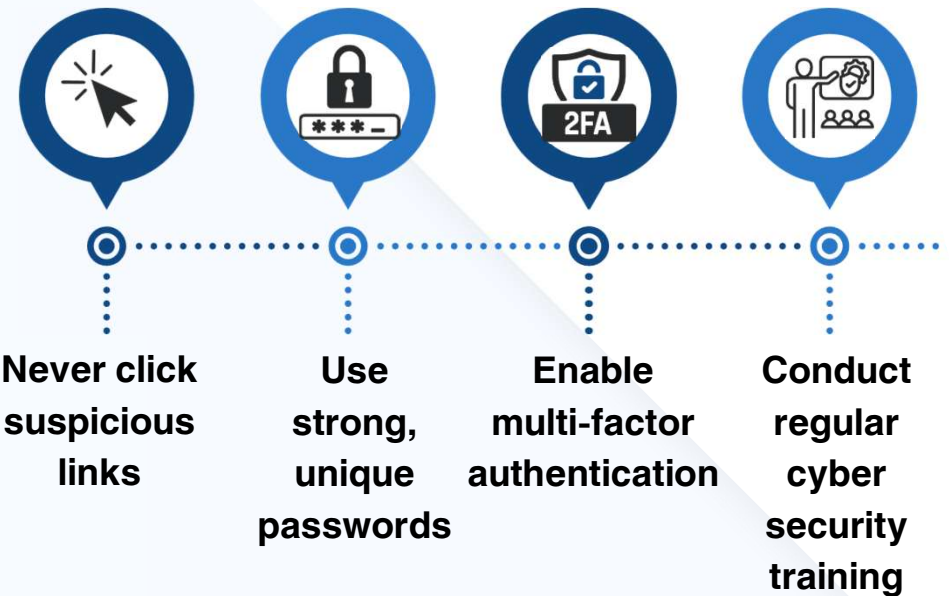
- ✓ Stolen Credentials - Access to multiple systems
- ✓ Targeted Individuals (e.g., executives) = Higher Risk
- ✓ Breaches can be fast and far-reaching





DEFENSE AND PREVENTION

HOW TO PROTECT AGAINST PHISHING



CONCLUSION

WHAT WE LEARNED

Key Takeaways

- Phishing remains a major threat due to human error
- Tools like SET are easily available to attackers
- Awareness and training are the best defense
- Stay vigilant, stay secure

