Phishing Attack Awareness Guide: Understanding the Threat and How to Stay Safe

---

Introduction: The Reality of Phishing Attacks

Phishing is one of the most common and dangerous forms of cyberattacks today. Attackers impersonate legitimate organizations to steal sensitive information such as passwords, credit card numbers, and personal details. With tools like **BlackEye**, these attacks have become increasingly simple to execute, posing a threat to anyone with an online presence.

In this guide, I'll outline how I conducted a phishing attack using BlackEye, specifically targeting an Amazon customer. Additionally, I'll provide insights on how to detect phishing attempts and explain why it's essential to be cautious before clicking on anything suspicious online. Security awareness training is crucial in this digital age to prevent falling victim to such attacks.

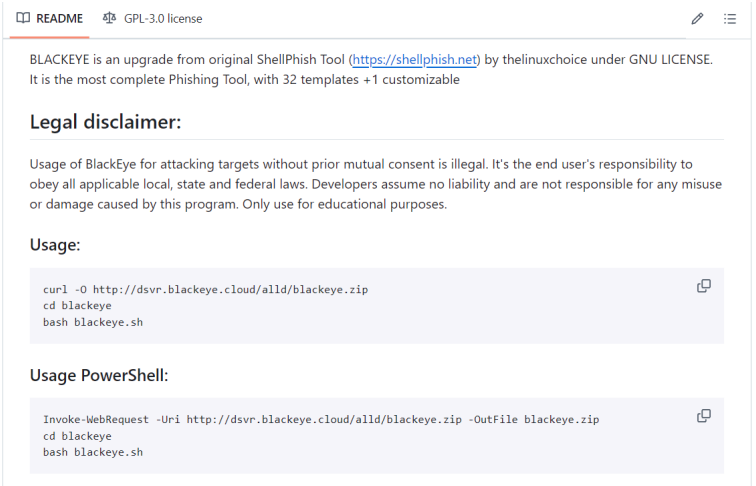
Conducting a Phishing Attack Using BlackEye

Disclaimer: This guide is intended for educational purposes only. Conducting phishing attacks without permission is illegal and unethical.

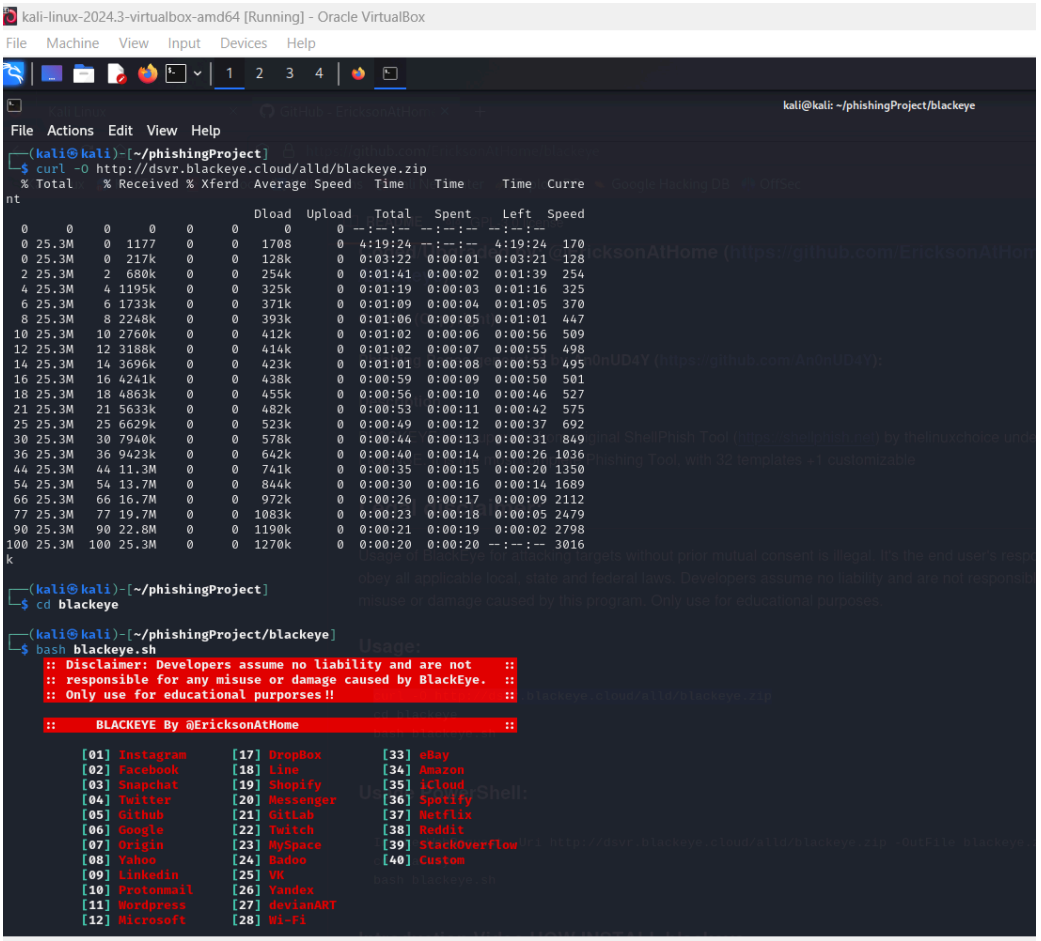
Step-by-Step Guide on Conducting a Phishing Attack Using BlackEye

1. Installing BlackEye on Kali Linux

Link to the repo: https://github.com/EricksonAtHome/blackeye?tab=readme-ov-file



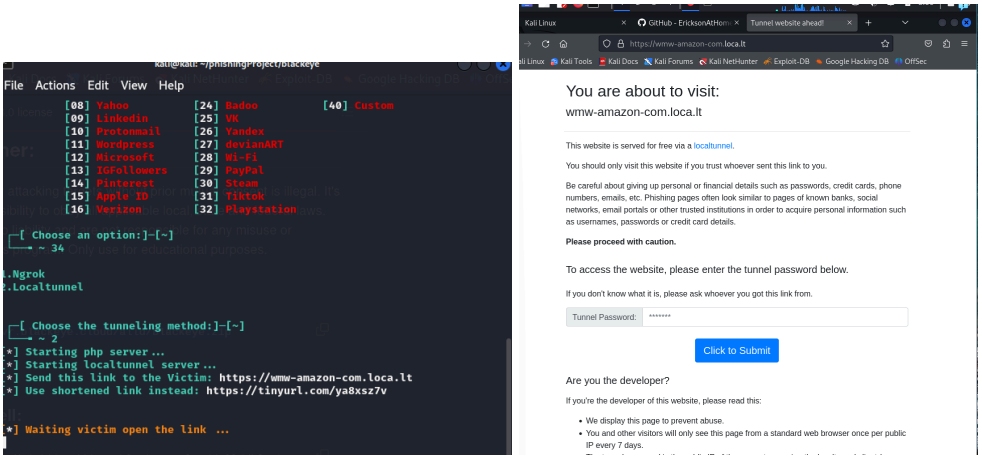
BlackEye is a popular open-source phishing tool that simplifies the process of creating phishing pages by imitating legitimate websites.



Creating a Phishing Page (Amazon Login Imitation)

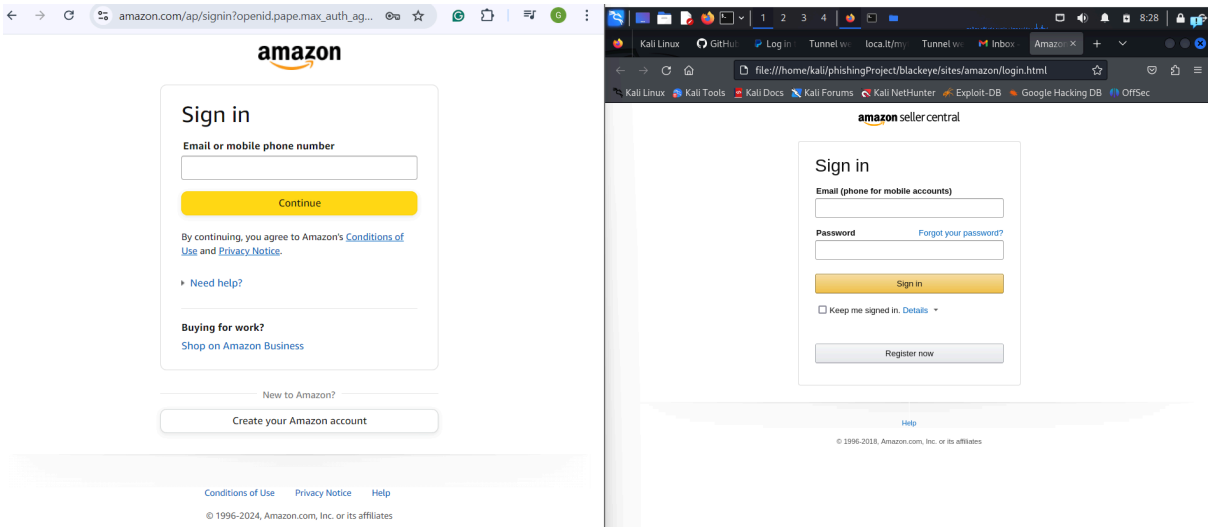
Once I ran BlackEye, a list of websites appeared for phishing page creation. To target Amazon:

1. I chose the option for **Amazon** from the list which was option 34.
2. BlackEye created a clone of Amazon's login page.
3. A phishing URL (similar to a real Amazon login page) was generated. This URL was used to deceive the target into entering their login credentials.

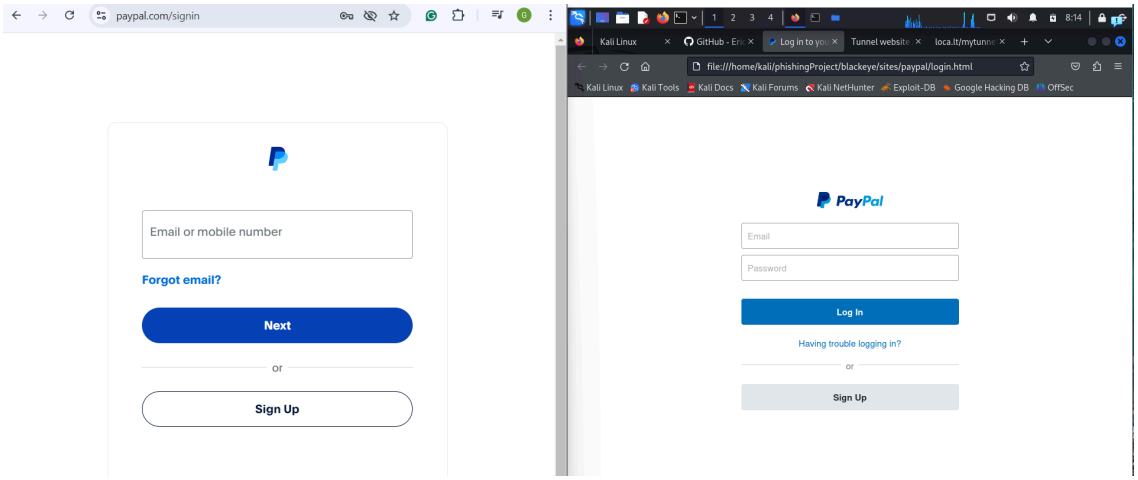


It might take you to this site if you pick **LocalTunnel.**

NB! I am NOT going to say how to go about it after this, for safety purposes.

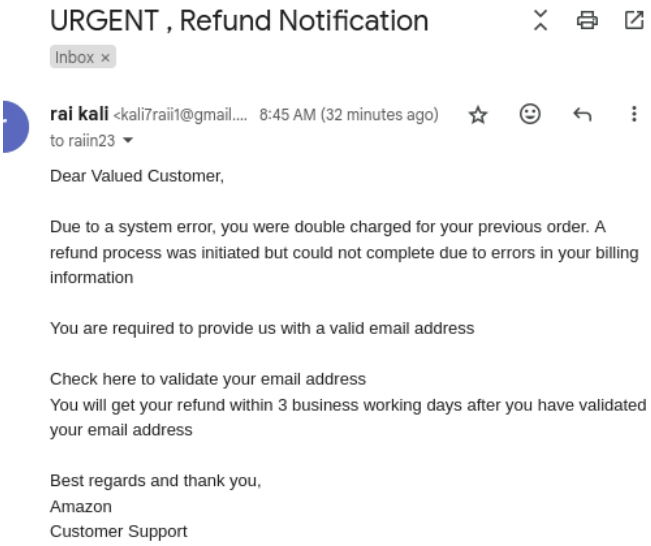


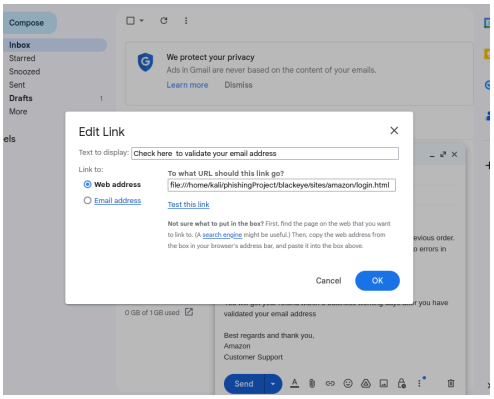
As you can see the sites look the same, for someone who does not pay attention you might fall for this attack. I did it as well with PayPal as I wanted to understand how blackeye is such a dangerous but also eye-opening source. As they look identical



Crafting the Phishing Email (Example)

Here's an example of the phishing email I used to trick the target into clicking on the malicious link and submitting their credentials:





As you can see, the threat actor can hide the malicious link in the written text. Hence always hover over any link and look at the domain name.

Subject: Urgent: Action Required for Your Amazon Refund

Dear Valued Customer,

Due to a system error, you were double charged for your previous order. A refund process was initiated but could not complete due to errors in your billing information.

You are required to provide us with a valid email address to process your refund.

Click here to validate your email address and confirm your billing details.

You will receive your refund within 3 business working days after you have validated your email address.

Best regards and thank you,
Amazon Customer Support

In this email, I imitated Amazon, adding urgency ("urgent action required") to prompt quick action. If the target clicks the link, they would be directed to the fake Amazon login page I created.

How Phishing Works and Why It's Dangerous

Phishing attacks trick users into believing they are interacting with a legitimate website. When users enter their credentials or sensitive information, it is directly sent to the attacker.

Dangers of Phishing Attacks:

- **Identity Theft:** Attackers can use stolen credentials to impersonate the victim and gain access to their personal or financial accounts.
- **Financial Loss:** Attackers can make unauthorized transactions using stolen bank or credit card information.
- **Data Breaches:** Phishing can target company employees, leading to large-scale data breaches.

With easy-to-use phishing tools like BlackEye, even inexperienced attackers can carry out highly effective phishing attacks.

How to Detect Phishing Artifacts and Stay Safe

Knowing how to identify phishing attempts is the first line of defense. Here are some telltale signs of phishing and how you can protect yourself:

1. Verify the Sender's Email Address

- Look for subtle misspellings or unusual characters in email addresses. For example, instead of `support@amazon.com`, it might come from `support@amazan.com`.

2. Hover Over Links Before Clicking

- Always hover your mouse over hyperlinks to see the actual URL. If it looks suspicious or doesn't match the official website, do not click it.

3. Look for HTTPS and SSL Certificates

- Ensure websites have "https://" in the URL, indicating a secure connection. Legitimate sites prioritize security.

4. Watch Out for Urgent Language or Unusual Requests

- Phishing emails often contain urgent messages. Legitimate companies usually don't ask for sensitive information like passwords or credit card numbers via email.

5. Be Wary of Attachments

- Never download attachments from unknown or untrusted sources. They may contain malicious software.

Why You Shouldn't Click Everything You See

Clicking on unverified links or downloading attachments without caution can have serious consequences:

- **Account Compromise:** Clicking on phishing links can lead to your accounts being hijacked.
- **Malware Infections:** Some phishing emails can trigger malware downloads that harm your device.
- **Data Theft:** Attackers can gain access to personal or corporate data for malicious purposes.

It’s essential to practice caution and critical thinking before clicking on unsolicited links or downloading unknown files.

Importance of Security Awareness Training

Given how easily attackers can use tools like BlackEye, it's crucial for individuals and organizations to implement **Security Awareness Training**:

1. **Frequent Training Programs:** Regular sessions on recognizing phishing attempts are essential.
2. **Simulated Phishing Tests:** Organizations can send fake phishing emails to assess employee awareness.
3. **Updated Policies:** Keep security policies current with the latest best practices and responses to phishing.

Conclusion

Phishing is one of the most accessible forms of cyberattacks but also one of the most preventable if you know what to look for. By understanding how phishing attacks work, I can better protect myself and others from falling victim.

Stay vigilant, verify before you click, and always be aware of phishing artifacts.
Through security awareness training and proper precautions, we can avoid becoming victims of phishing attacks.

I got to learn all this from Security Blue Team L1. This is my practical work outside the BTL1 phishing to learn in-depth, about being the attacker and also raise awareness in this Cybersecurity Awareness month. - ***"You got to know what you defending against for you to a great defender" by Gamuchirai Muchafa***