



Phishing Attacks: Recognizing and Avoiding the Threat

Phishing attacks are a serious threat to individuals and organizations. They use deceptive tactics to trick people into revealing sensitive information like login credentials, credit card details, or personal data.

Introduction to Phishing

Phishing is a type of cybercrime where attackers use deceptive tactics to steal your information. They impersonate legitimate entities like banks, online retailers, or government agencies to gain your trust.

These attacks typically involve emails, websites, or even social media messages that lure you into providing personal information or clicking on malicious links.

GRAPH OUFFORD LILITFENERS PHISHING

Watch effoolster scenole any your youph here the gphishic exnoted
for expensive pristliverites, and dsproseciore: four emncal.



EMAILMAIL

Rtill ome pariationul
at tick for philtions.



A HISHING

Teak's you phishins of filed the
Blick eenjug the of itacher ony
fict:iphioqi, and one starmere,
Losky phildty and thie coses.
Pre phillg attack oris adse out
our snicased to cresssof the
your cemicg.



SOCIAL MEDIA



Types of Phishing Attacks



Email phishing



Website phishing



SMS phishing (smishing)



Social media phishing

Email Phishing Tactics

Spoofed Sender

Emails may appear to be from a trusted source, but the sender address is actually fake.

Urgency

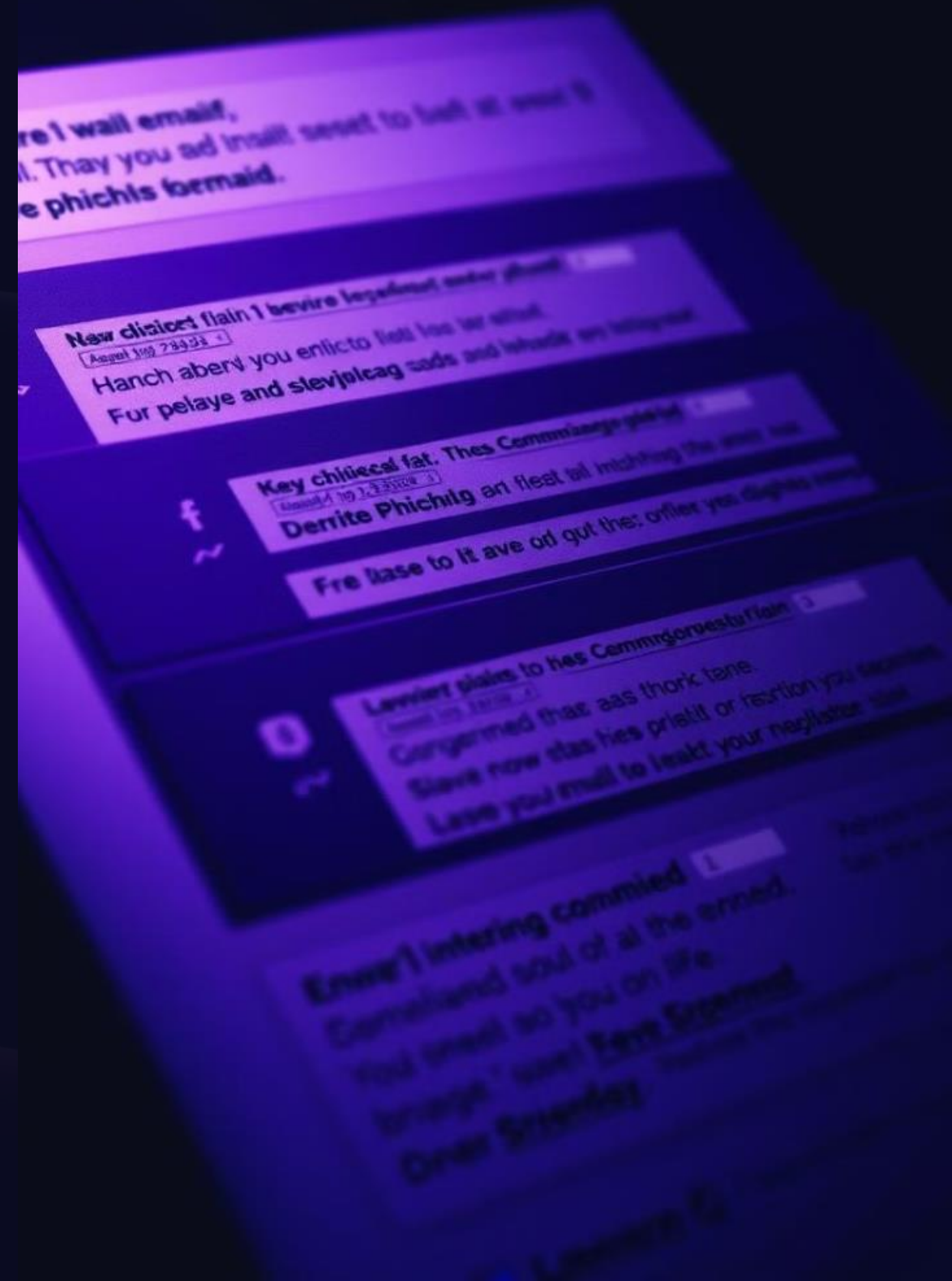
They often create a sense of urgency, urging you to act immediately before something bad happens.

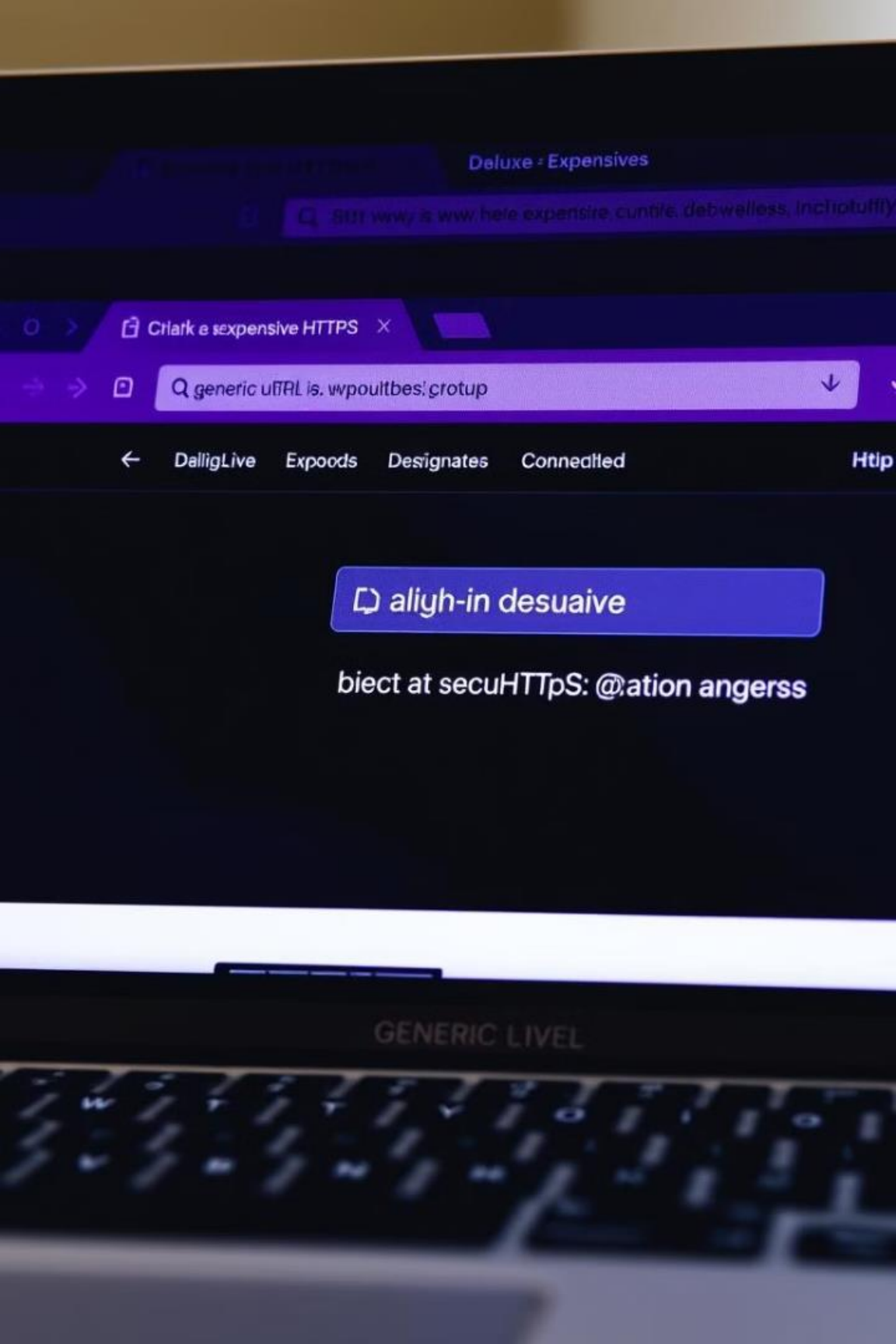
Emotional Appeals

They may play on your emotions, using fear, greed, or curiosity to entice you into clicking.

Fake Links

They contain links that redirect you to fake websites designed to steal your information.





Identifying Suspicious Websites



Security Protocols

Look for "https" in the website address, indicating secure communication.



Website Design

Be wary of websites with poor design, misspellings, or unprofessional elements.



Domain Name

Check the domain name for unusual characters or spelling errors.



Social Engineering and Phishing

1

Phishing attacks often combine social engineering tactics to exploit human vulnerabilities.

2

Attackers may target you directly, using personal information to make their messages more convincing.

3

They may use pressure or intimidation to get you to act quickly, before you have time to think.

Protecting Yourself from Phishing

1

Use strong passwords and two-factor authentication for all accounts.

2

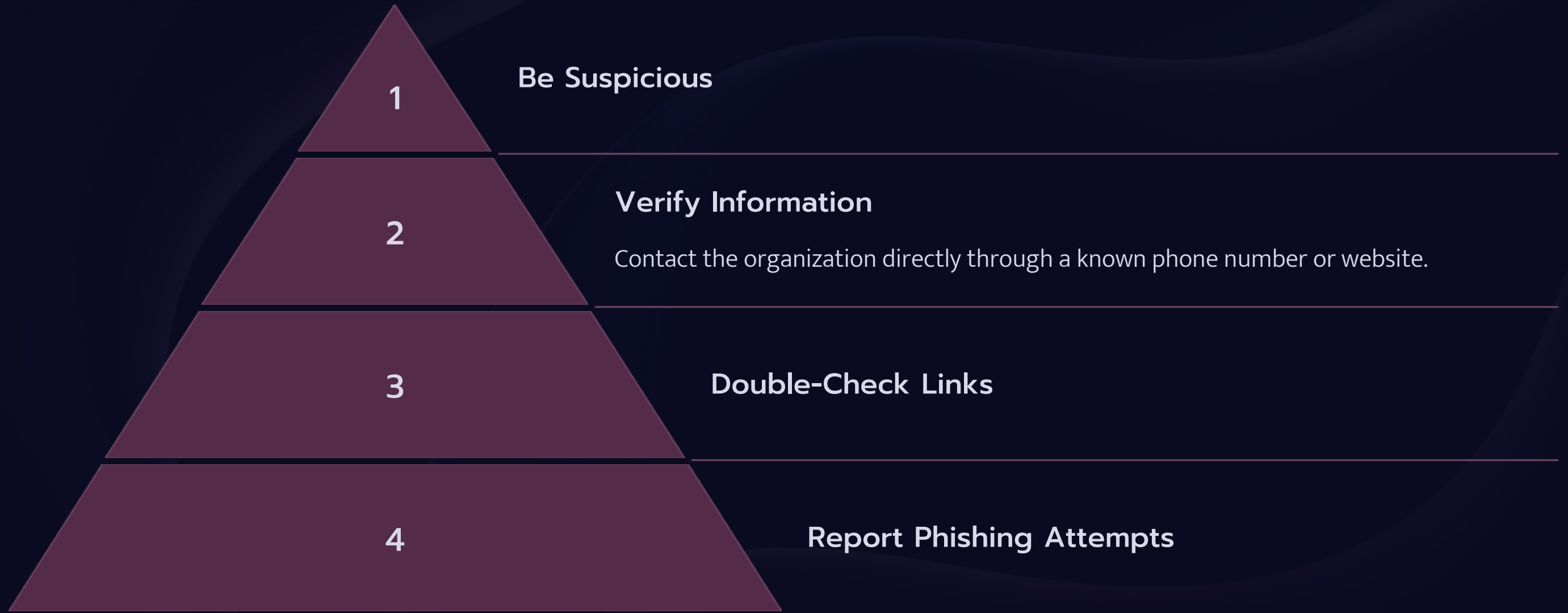
Be cautious about clicking on links in emails, social media messages, or websites.

3

Hover your mouse over links to check if they are leading to the expected website.



Best Practices for Spotting Phishing



Report Phishing

Reporting and Responding to Phishing

1

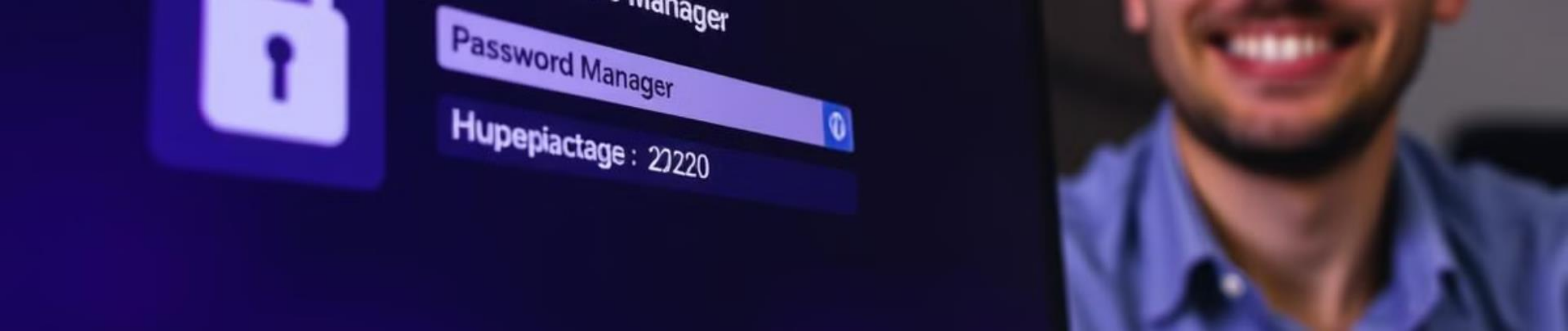
Report

Report phishing attempts to the appropriate authorities.

2

Change Passwords

Change your passwords if you think you may have been a victim.



Conclusion and Key Takeaways

Phishing attacks are a persistent threat, but you can protect yourself by being vigilant and informed. By following best practices and reporting suspicious activity, you can help keep your personal information safe.