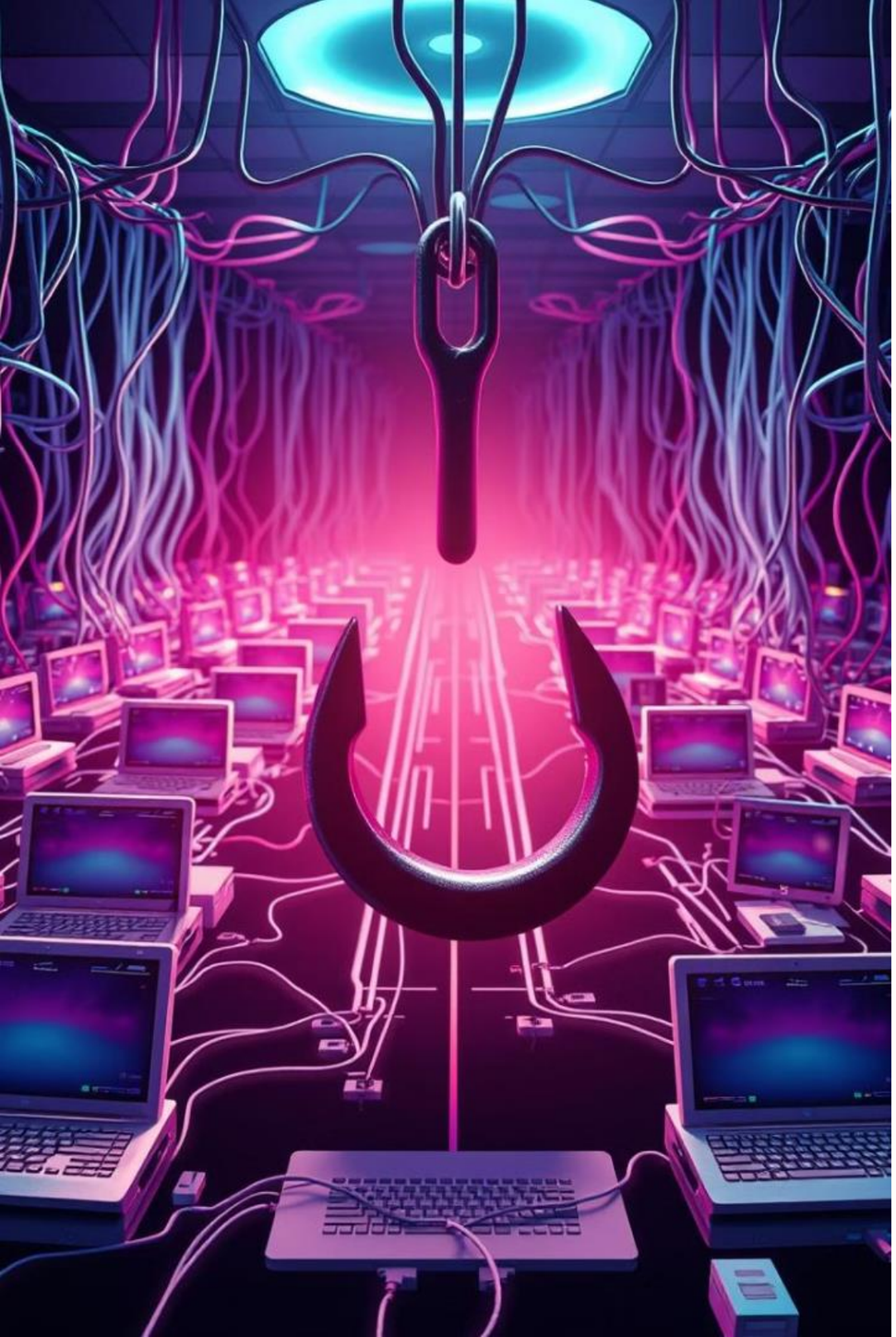


Phishing Attacks: Recognizing Recognizing and Avoiding

This presentation will guide you through the world of phishing attacks and equip you with the knowledge to stay safe.

Types of Phishing Attacks

Email Phishing

This is the most common type of phishing, using emails that appear legitimate to trick users into giving up sensitive information.

Website Phishing

Fake websites are created to mimic real ones, aiming to steal login credentials or financial data.

Social Engineering

Phishers use social manipulation tactics to gain access to sensitive information or systems, often through building trust and exploiting vulnerabilities.

Identifying Phishing Emails

Suspicious Sender

Check the email address and sender name for authenticity.

Urgent Tone

Phishing emails often create a sense of urgency, urging you to act quickly without thinking.

Suspicious Links

Hover over links to reveal their destination before clicking.

Grammar Errors

Phishing emails may contain spelling or grammatical errors, a sign of a fake message.

Spotting Malicious Websites

Missing HTTPS

Look for the "https://" prefix in the URL to ensure a secure connection.

Unprofessional Design

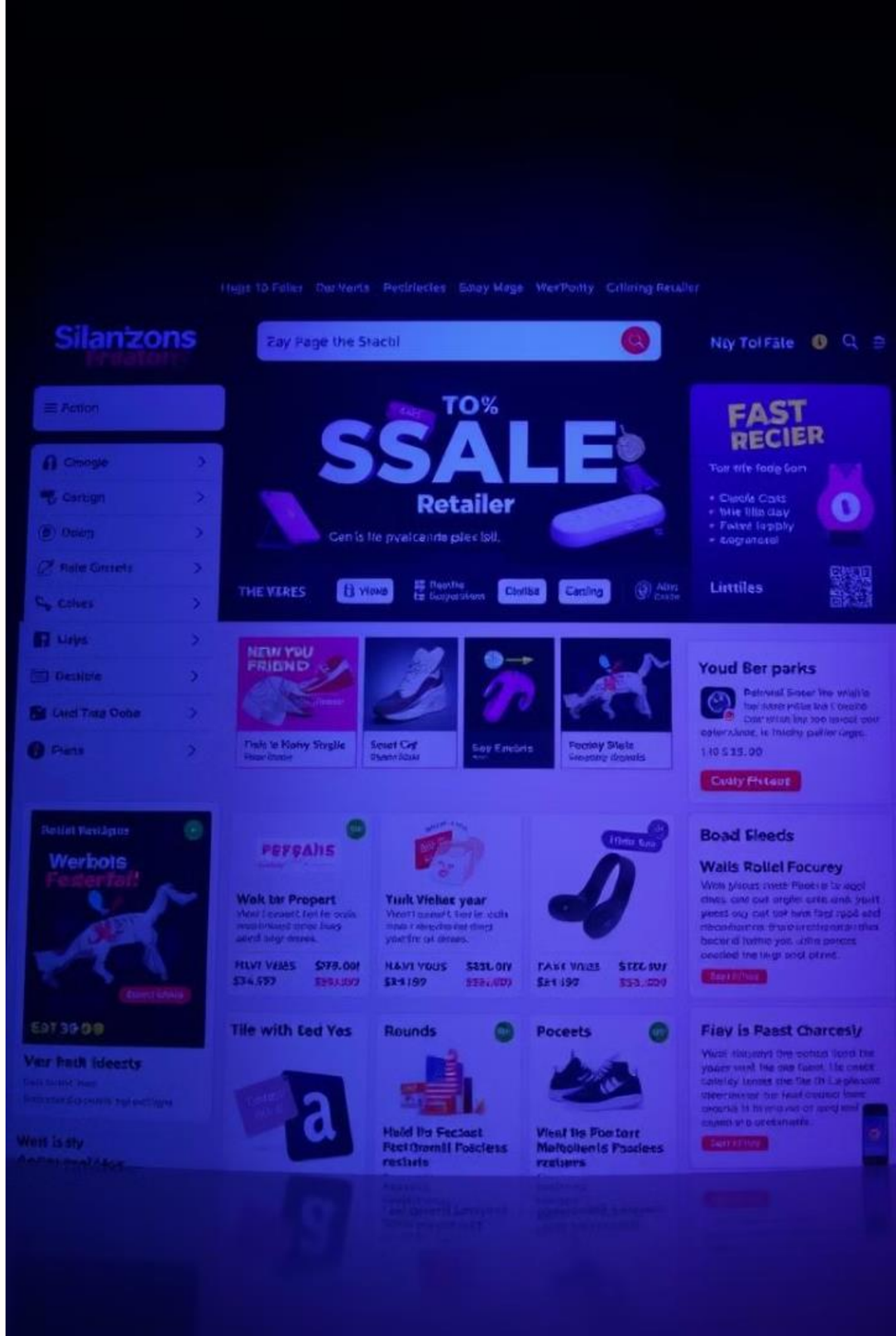
Be wary of websites with poor design, misspellings, or inconsistent branding.

Suspicious Domain

Check the domain name for unusual characters or misspellings.

Expired Certificates

A website with an expired certificate may be compromised.



Protecting Yourself from Social Engineering

1

Be Skeptical

Question requests for sensitive information, especially if they seem unusual.

2

Verify Information

Contact the organization directly to confirm requests and verify their authenticity.

3

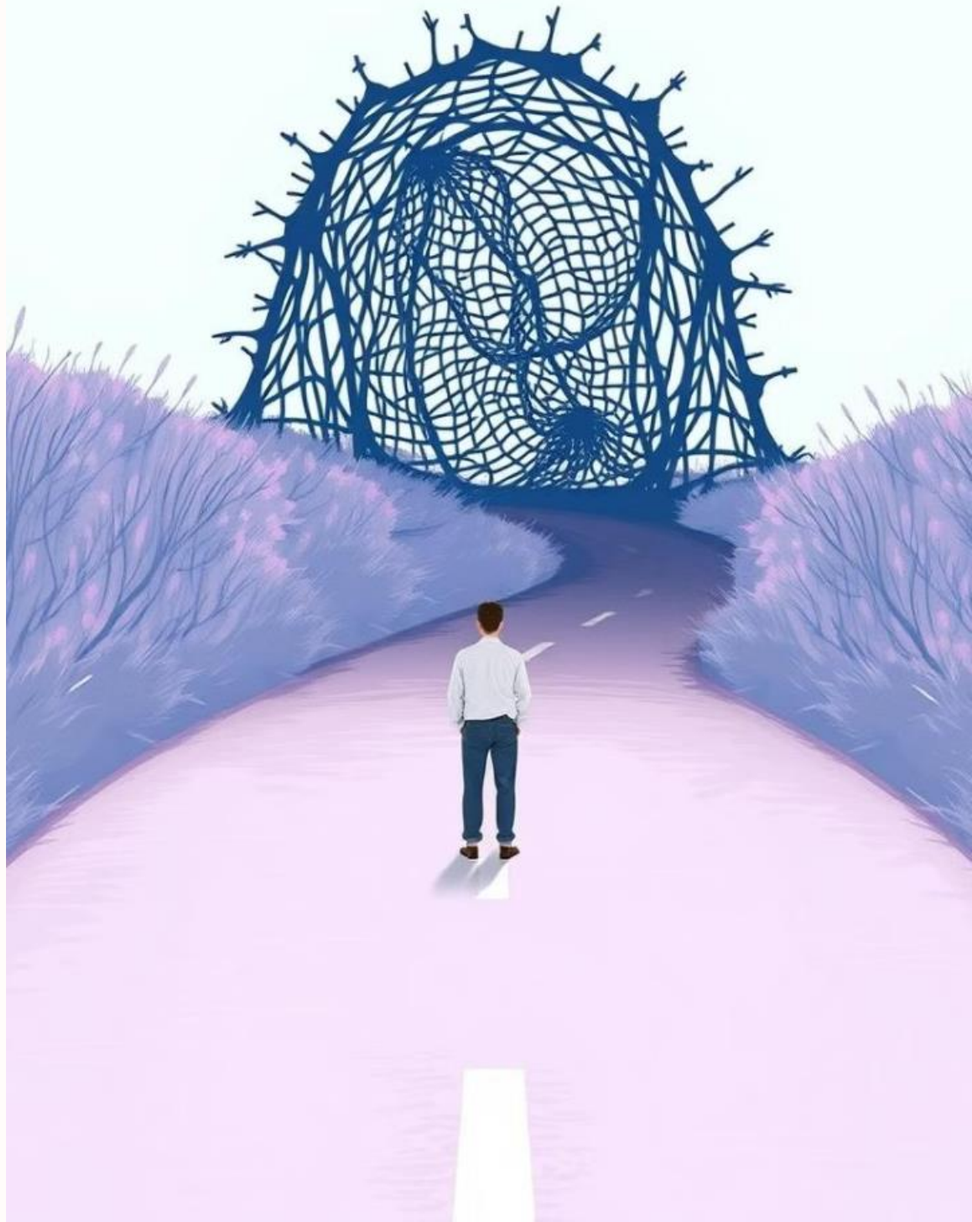
Think Before You Click

Avoid clicking on links or attachments from unknown senders.

4

Report Suspicious Activity

Alert the relevant authorities or organizations if you suspect a phishing attempt.



Best Practices for Email Security

1 **Use Strong Passwords**

Create complex and unique passwords for all your accounts.

2 **Enable Two-Factor Authentication**

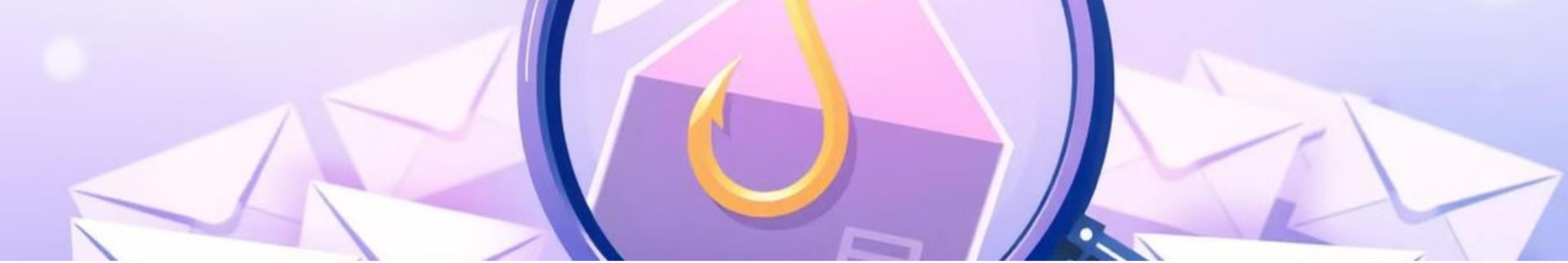
Add an extra layer of security by requiring a second authentication step.

3 **Keep Software Updated**

Regularly update your operating system and software to patch security vulnerabilities.

4 **Be Cautious with Attachments**

Avoid opening attachments from unknown senders or suspicious sources.



Staying Vigilant Against Phishing

Stay Informed

Read articles and resources about the latest phishing tactics.

1

Practice Caution

Always be mindful of potential threats and avoid clicking on links or attachments from unknown sources.

3

2

Report Phishing Attempts

Report suspicious emails, websites, or social media accounts to the relevant authorities.

Conclusion and Key Takeaways

Phishing is a serious threat, but by being informed and practicing caution, you can protect yourself and your data. Remember to stay vigilant and report suspicious activity to prevent phishing attacks.