


Phishing Awareness Training

This training will help you identify and avoid phishing attacks.

 by Shashank Chauhan



What is Phishing?

Definition

Phishing is a cybercrime where attackers attempt to steal sensitive information like passwords and credit card details by disguising themselves as trustworthy entities.

How it Works

Attackers send emails, messages, or links that appear legitimate, but actually lead to fake websites or malicious software.



Common Phishing Tactics

○ Spoofed Emails

Emails that appear to be from a legitimate source but are actually forged.

○ Urgency

Attackers create a sense of urgency to pressure victims into acting quickly and without thinking.

○ Social Engineering

Manipulating people into revealing sensitive information or taking actions that benefit the attacker.

○ Malware

Malicious software designed to steal data, gain access to systems, or disrupt operations.

Identifying Phishing Emails

Sender Address

Look closely at the sender's email address. It might be slightly different from the legitimate source.

Subject Line

Be wary of subject lines that are too urgent, exciting, or generic. They might contain grammatical errors.

Email Content

Pay attention to the email's content. Look for inconsistencies, misspellings, or requests for personal information.



Phishing Website Red Flags

Insecure Connection

Look for a padlock icon in the address bar and ensure the URL begins with "https."

Strange URL

Be cautious of URLs that look unusual or misspelled, especially if they are from a familiar source.

Website Design

Pay attention to the website's design. If it looks unprofessional or different from the legitimate source, it could be a phishing website.

Request for Personal Information

Legitimate websites rarely ask for sensitive information like passwords or credit card details through unsolicited emails or links.

Social Engineering Tricks



Gift Cards

Phishers often use fake promotions or contests that offer gift cards or prizes to lure victims.



Account Verification

Phishers may pretend to be from a legitimate source and request verification of your account details.



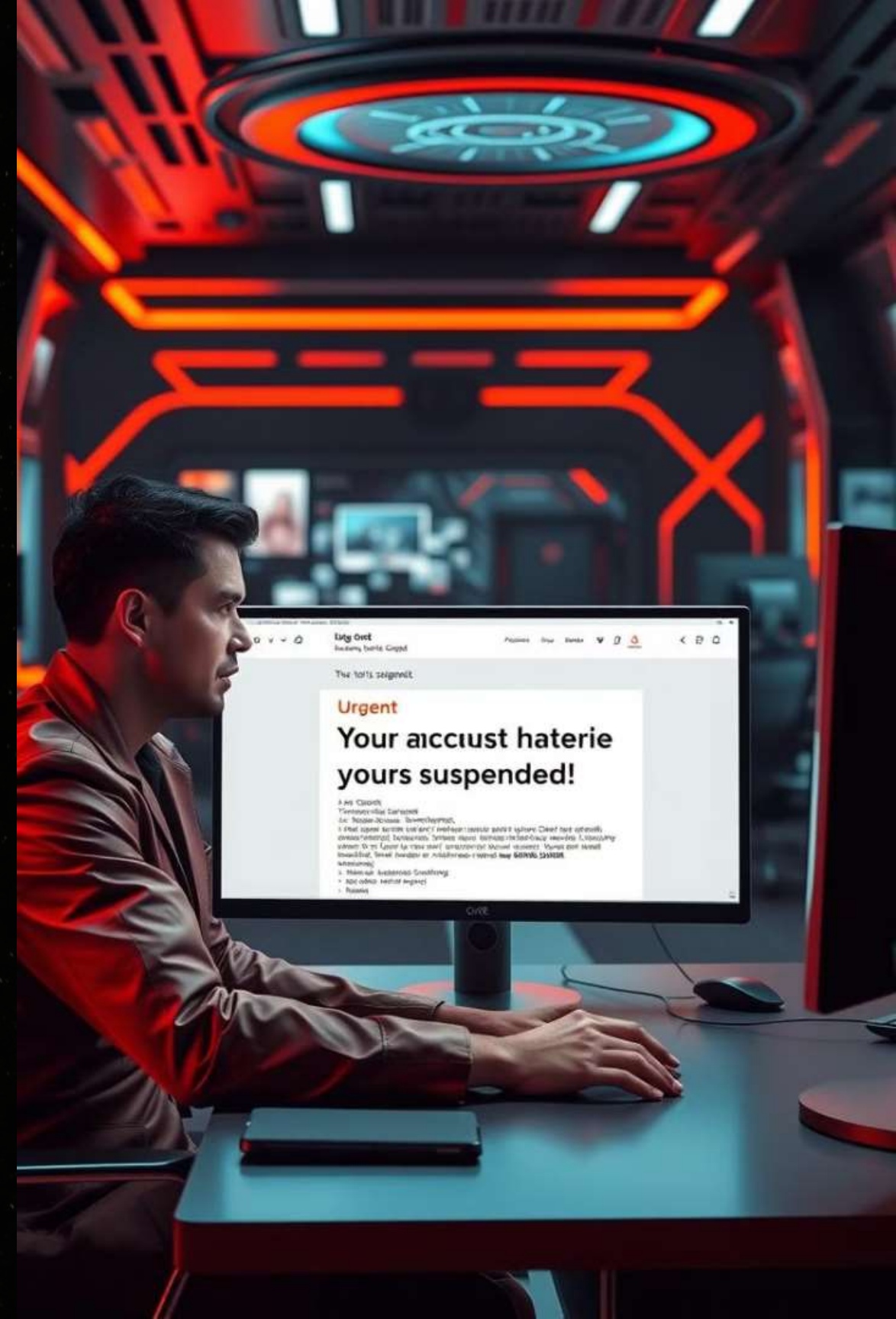
Money Transfers

Attackers may request urgent money transfers or payments for fictitious reasons or to avoid taxes.

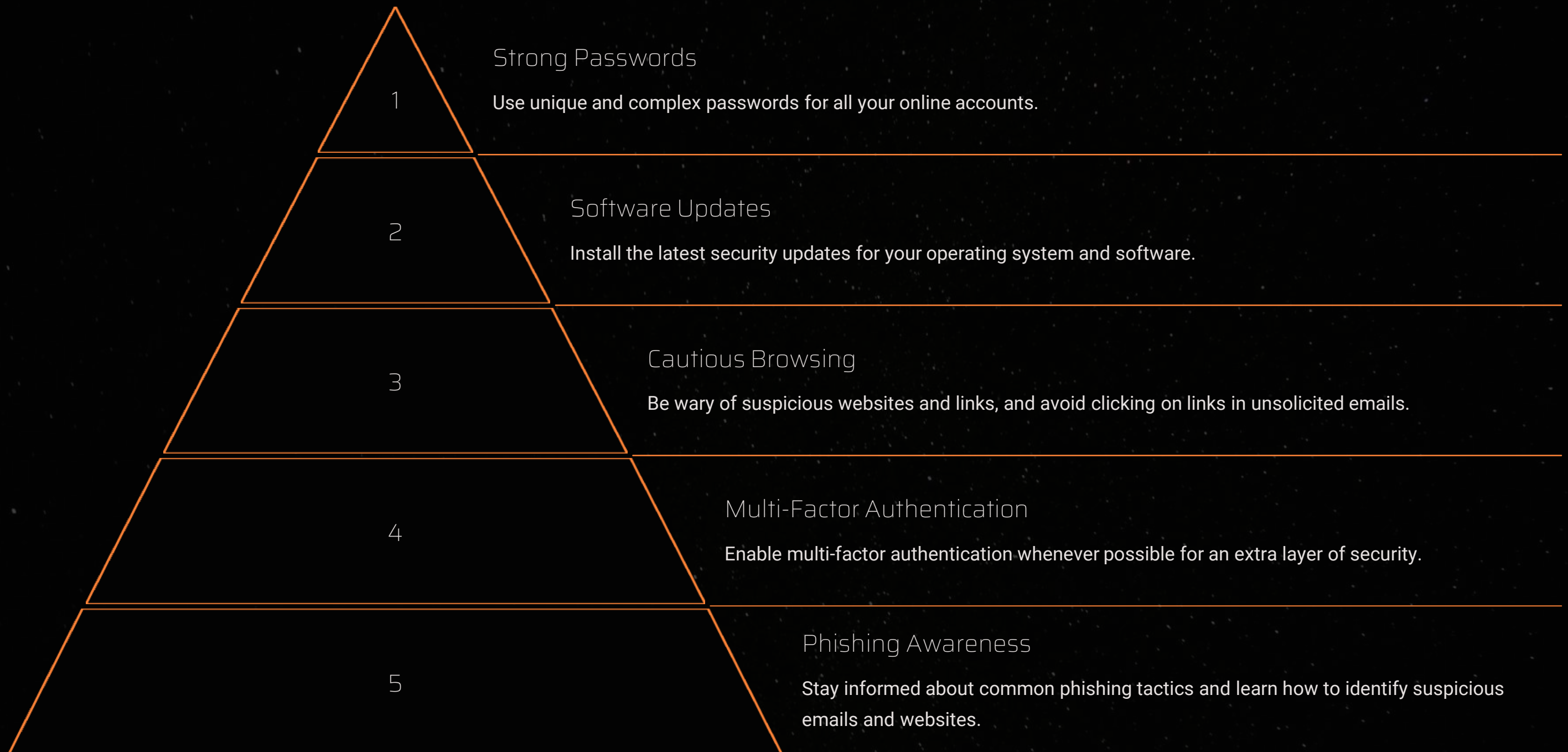


Romance Scams

Attackers may create fake online profiles to build relationships and then request money or personal information.



Protecting Yourself from Phishing



Reporting Suspected Phishing Attempts

1

Forward Suspicious Emails

Forward suspicious emails to your IT department or security team.

2

Contact the Company

Reach out to the company or organization that is allegedly sending the email or message.

3

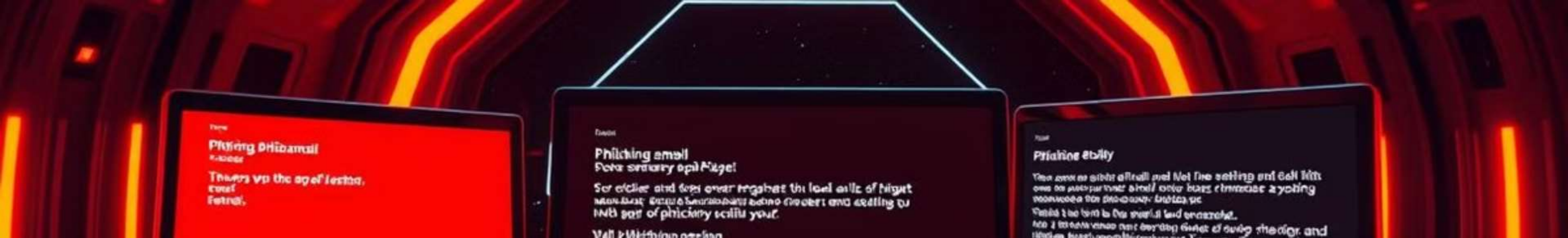
Report the Website

If you encounter a suspicious website, report it to the relevant authorities or website hosting provider.

4

Change Your Passwords

If you believe you might have been phished, change your passwords for all affected accounts.



Real-World Phishing Examples

1

Fake Bank Notifications

Emails pretending to be from a bank, requesting account verification or password updates.

2

Social Media Account Hacks

Messages on social media platforms claiming to be from a friend or family member, asking for sensitive information or money.

3

Delivery Notifications

Fake emails or messages claiming to be from a delivery company, asking for personal information or to track a package.

4

Job Scams

Job offers that require personal information or money before starting work, often through fake websites or emails.

Best Practices for Staying Safe

