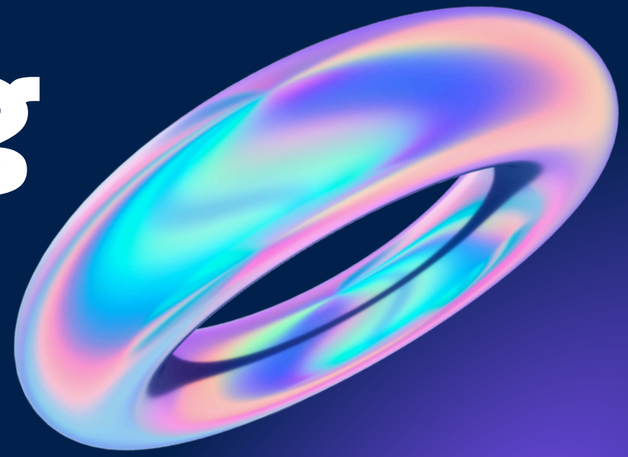
Presentation

Phishing Awareness Training

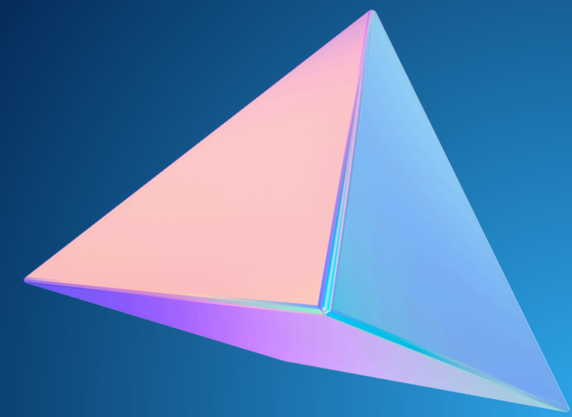


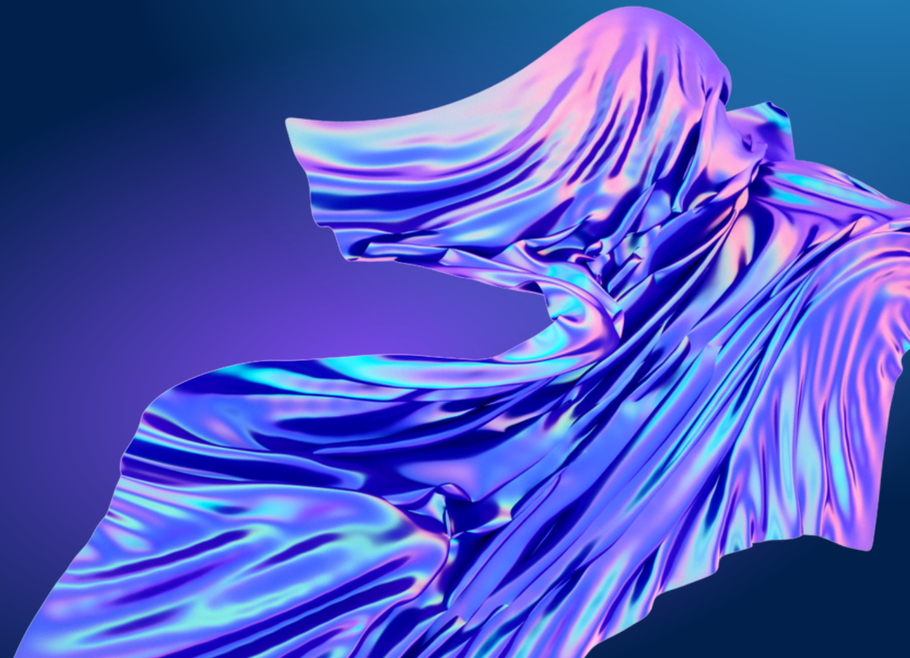
Introduction to Phishing

- Phishing is a cyberattack to steal sensitive information by impersonating legitimate entities.
- Phishing causes financial loss, data breaches, and trust erosion in digital communication.

Types of Phishing Attacks

- Email Phishing
- Spear Phishing
- Whaling
- Vishing (Voice Phishing)
- Smishing (SMS Phishing)
- Clone Phishing





Recognizing Phishing Attacks

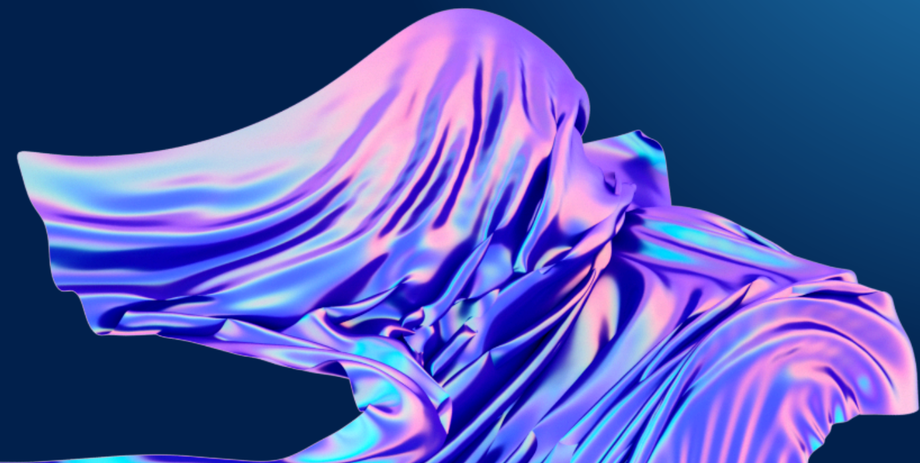
Red Flags in Email Content

Analyzing Email Headers

Spotting URL Spoofing

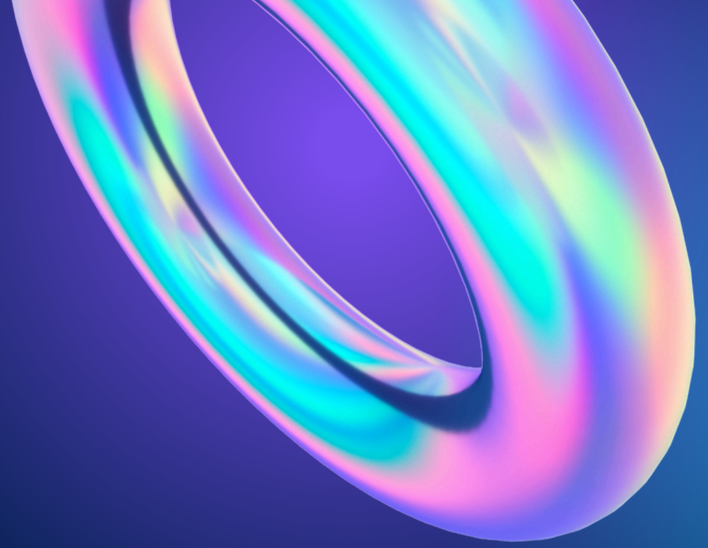
Responding to Phishing Attempts

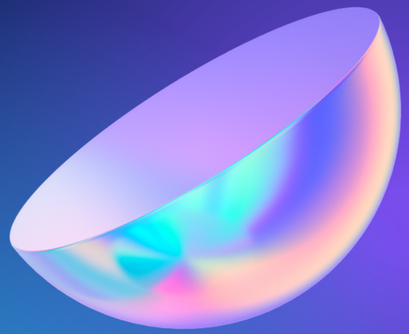
If you receive a phishing email, don’t click links or download attachments—just delete it. Report the attempt to your email provider and relevant authorities. If you’ve been phished, change your passwords, monitor your accounts, and inform your financial institutions or IT department.



Social Engineering Tactics

Social engineering manipulates human psychology to obtain confidential information. Common tactics include pretexting, baiting, and phishing.





Preventative Measures

- Email Security Best Practices
- Safe Internet Browsing Tips
- Use of Multi-Factor Authentication (MFA)
- Importance of Regular Software Updates

Conclusion

To recap, phishing involves deceptive tactics to steal sensitive information and can lead to significant risks like financial loss and data breaches. To stay safe, always verify the source of emails, use strong passwords, and report suspicious activity. Remain vigilant and continually update your knowledge to defend against evolving threats.