Phishing Awareness

Introduction to Phishing

What is Phishing?

Phishing is a type of cyberattack where attackers trick individuals into sharing sensitive information, such as passwords, credit card numbers, or personal data.

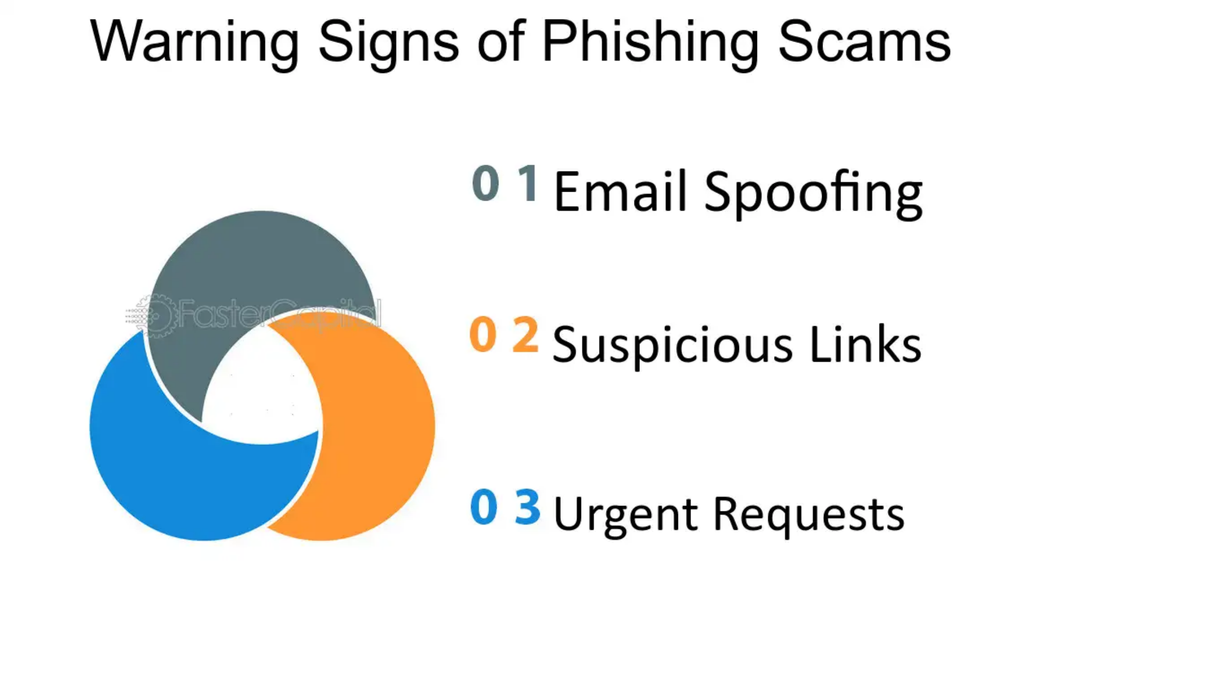
Common mediums: Emails, fake websites, SMS, and social media.

Why Phishing is Dangerous:

Leads to identity theft, financial loss, and unauthorized access to sensitive systems.

One of the most common forms of cyberattacks worldwide.

Common Characteristics of Phishing



Warning Signs of Phishing Scams

0 1 Email Spoofing

0 2 Suspicious Links

0 3 Urgent Requests

- ✓ Urgent or threatening language (e.g., "Your account will be locked!")
- ✓ Spelling and grammatical errors.
- ✓ Unfamiliar sender email addresses or domains.
- ✓ Requests for personal or financial information.
- ✓ Links to unfamiliar or suspicious websites.
- ✓ Unexpected attachments or downloads.

Recognizing Phishing Emails

- **Indicators of a Phishing Email:**
  - ✓Generic greetings like "Dear Customer."
  - ✓Offers that seem too good to be true.
  - ✓Requests for immediate action or sensitive information.
  - ✓Hovering over links reveals suspicious URLs.
- **Example of a Phishing Email:**
  - ✓Visual example with highlighted red flags (e.g., suspicious sender, malicious link).

Avoiding Phishing Websites

How to Identify Safe Websites:

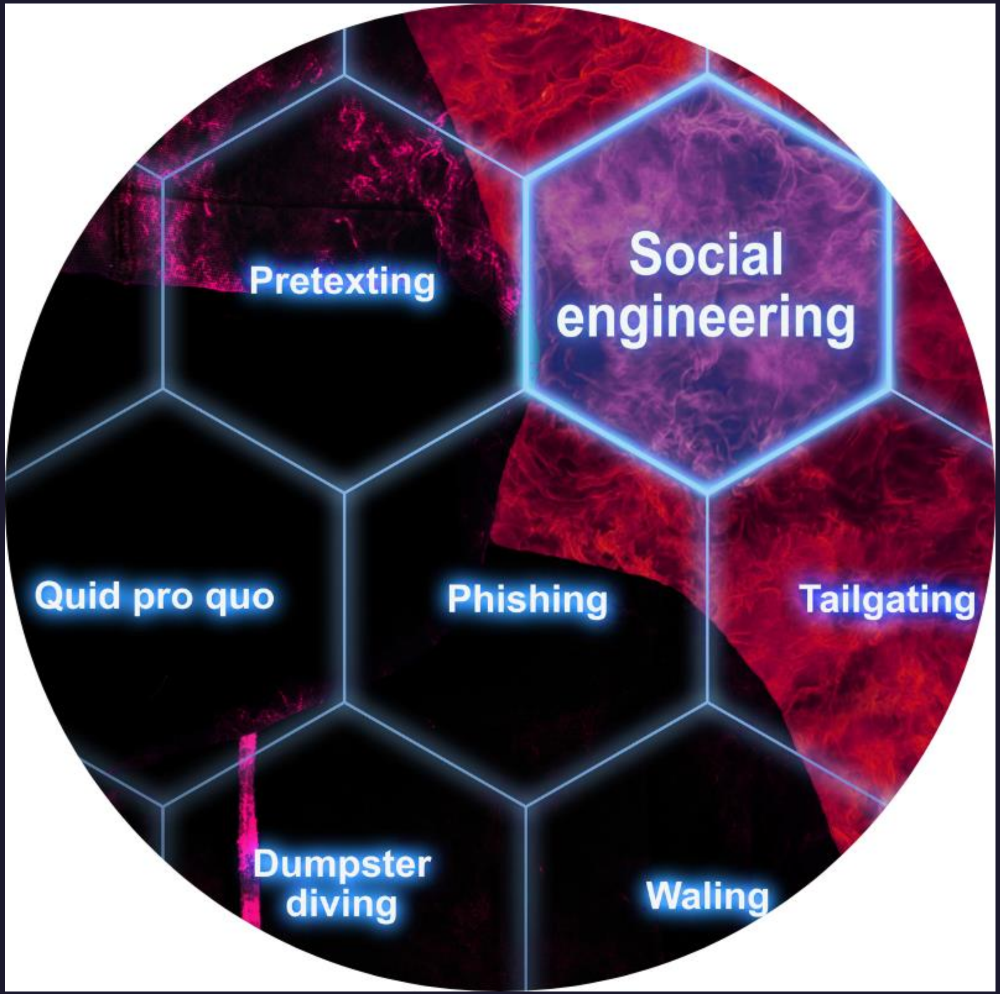
- Look for "https://" and a padlock icon in the URL.
- Verify the URL spelling carefully.
- Avoid clicking on links in unsolicited emails or messages.

What to Do When in Doubt:

- Use bookmarks for frequently visited sites.
- Manually type the URL instead of clicking on links.
- Close the browser if a site looks suspicious.

Social Engineering Tactics

- **What is Social Engineering?**
  - ✓ Manipulating individuals into divulging confidential information through deception.
- **Examples of Social Engineering:**
  - ✓ Impersonation: Pretending to be a trusted authority or colleague.
  - ✓ Baiting: Offering free items or services in exchange for information.
  - ✓ Pretexting: Creating a fabricated scenario to gain trust.
- **How to Stay Safe:**
  - ✓ Verify the identity of individuals before sharing sensitive data.
  - ✓ Be cautious of unsolicited phone calls or messages.



Steps to Take if You Suspect Phishing

Immediate Actions:

Do not click on links or download attachments.

Report the suspicious email or message to your IT or security team.

Delete the email or message from your inbox and trash.

If You’ve Clicked a Phishing Link:

Disconnect from the internet immediately.

Change passwords for affected accounts.

Monitor financial and personal accounts for unauthorized activity.

Report the incident to your organization or local authorities.

Tools and Best Practices

Email Security Tools:

Use spam filters and email authentication protocols (e.g., SPF, DKIM, DMARC).

Best Practices:

Keep software and antivirus programs up to date.

Educate employees and conduct regular phishing awareness training.

Encourage reporting of phishing attempts.

Resources:

Trusted cybersecurity websites and training platforms.

Conclusion

Key Takeaways:

Stay vigilant and cautious of unsolicited messages.

Always verify the source before taking action.

Be aware that fake news can also be used as a tactic to lure you into phishing schemes.

Report phishing attempts promptly.

Remember:

Cybersecurity is a shared responsibility.

THANK YOU!

Think Before You Click – Protect Yourself from Phishing Tricks!