CYBER SECURITY

Phishing Awareness Training

What is Phishing?

a fraudulent practice where attackers impersonate a legitimate entity, like a bank or company, through email, text messages, or phone calls, to trick users into revealing sensitive information like passwords, credit card details, or personal data by clicking malicious links or providing information on fake websites.

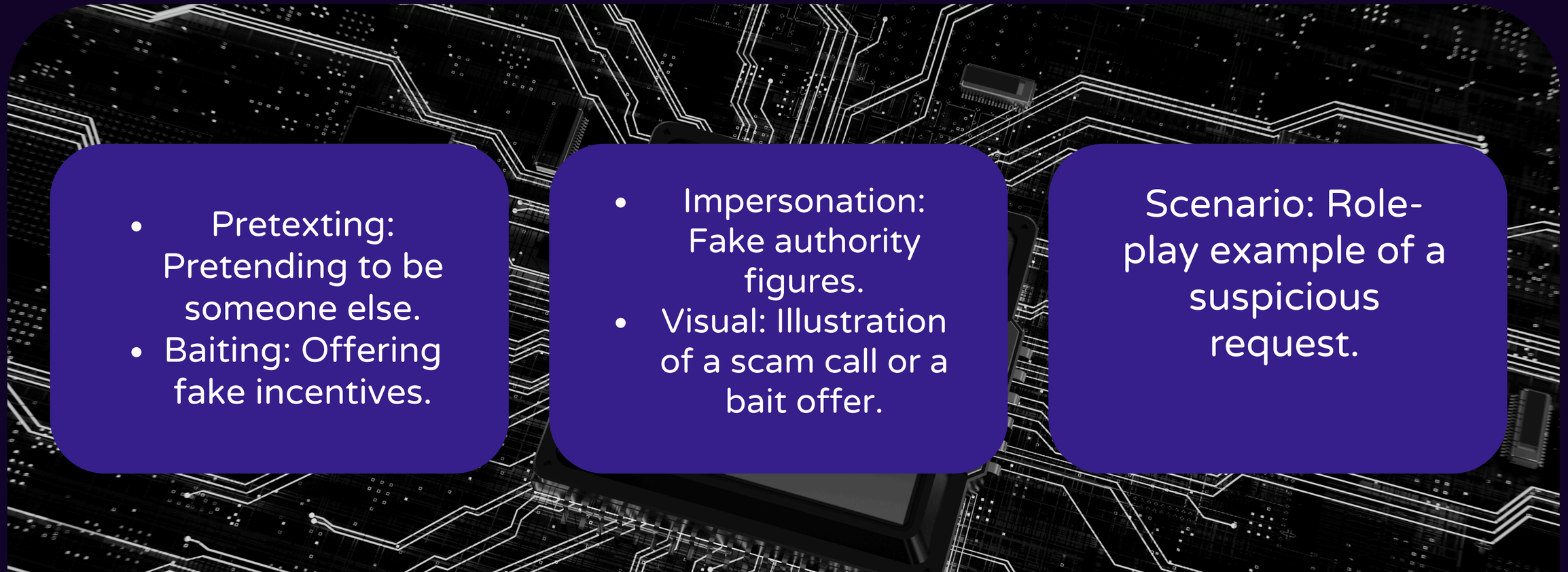
Why is Phishing Dangerous?

1. Financial Loss: Billions lost yearly.
2. Identity Theft: Personal details misused..
3. Data Breaches: Compromised systems.
4. Visual: Infographic showing the impact

Common Phishing Tactics

1. Phishing Emails.
2. Fake Websites.
3. Social Engineering Tactics.
4. Visual: Icons or images representing each tactic.

Social Engineering Tactics



- Pretexting: Pretending to be someone else.
- Baiting: Offering fake incentives.

- Impersonation: Fake authority figures.
- Visual: Illustration of a scam call or a bait offer.

Scenario: Role-play example of a suspicious request.

Basic Security Practices

- Use strong, unique passwords.
- Keep software up to date.
- Enable two-factor authentication (2FA).
- Avoid clicking on suspicious links or attachments.

Protecting Personal Data

1

Encrypt
sensitive data.

2

Regularly
back up data.

3

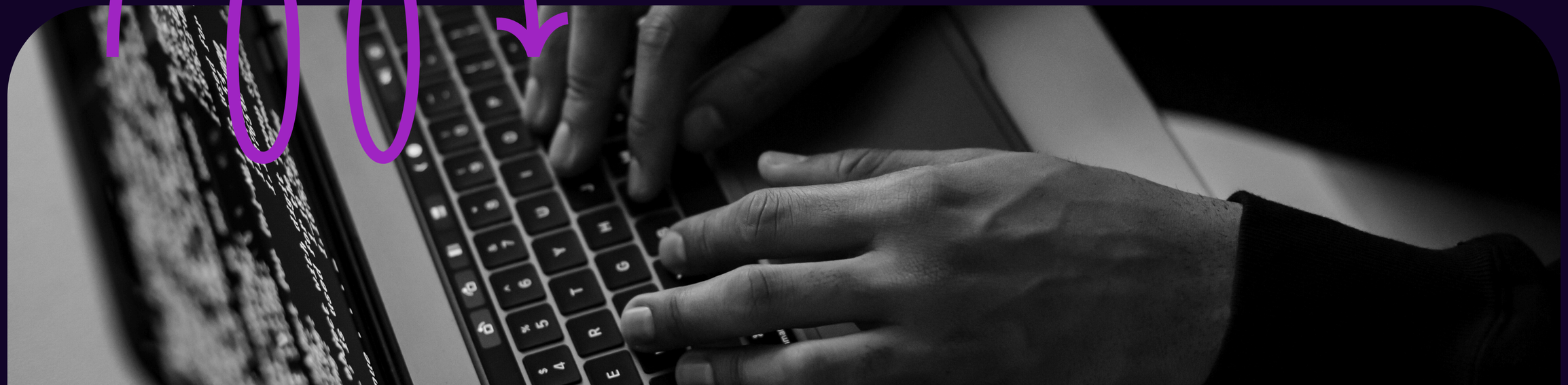
Use VPNs on
public networks.

Real-Life Examples

Between 2013 and 2015, a Lithuanian scammer deceived Google and Facebook into transferring over $100 million by impersonating Quanta Computer, a legitimate supplier. The attacker created fake domains resembling Quanta's and sent fraudulent invoices requesting payments for fabricated services. Trusting the realistic emails, employees transferred funds to bank accounts controlled by the scammer without verifying the requests. The scam succeeded due to social engineering, domain spoofing, and a lack of stringent verification processes. Although the scam was eventually uncovered, it highlighted the need for organizations to implement robust phishing awareness training and thorough procedures for verifying financial transactions.

Phishing Awareness

- Always verify emails, links, and requests for sensitive information.
- Look out for red flags like suspicious sender details and incorrect URLs.
- Use multi-factor authentication (MFA) and keep systems updated.
- Report any suspected phishing attempts to your IT or security team.



THANK YOU!

Together, we can outsmart phishing attacks and protect our organization.