PHISING IN CYBERSECURITY

ABOUT PHISIHNG

Phishing is a prevalent form of cyberattack where attackers masquerade as trustworthy entities to steal sensitive information. These attacks often involve deceptive emails or messages that prompt recipients to click on malicious links or provide personal data. By mimicking legitimate sources like banks or social media platforms, phishers exploit human psychology, such as fear or urgency, to trick their targets. Understanding phishing tactics and recognizing warning signs is crucial in protecting oneself and organizations from these malicious schemes.

HOW PHISHING WORKS

1

Deceptive Communication: Phishers send emails, messages, or social media posts that appear to be from legitimate sources.

2

Fake Websites: Links in these communications often lead to fake websites that mimic real ones.

3

Information Theft: Users are tricked into providing sensitive information, which is then used for fraudulent activities.

TYPES OF PHISHING ATTACKS

01 Email Phishing: The most common form, involving deceptive emails.

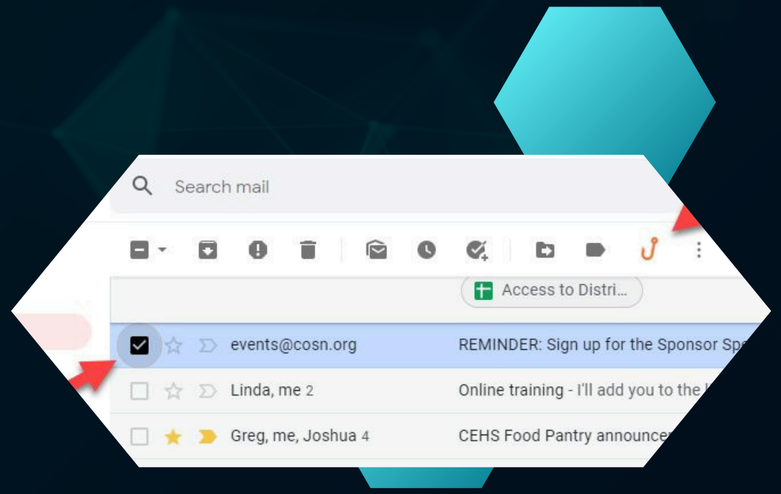
02 Whaling: Targeting high-profile individuals like executives.

03 Smishing and VishingPhishing via SMS/text messages, and Phishing via phone calls.

RECOGNIZING PHISHING ATTEMPTS

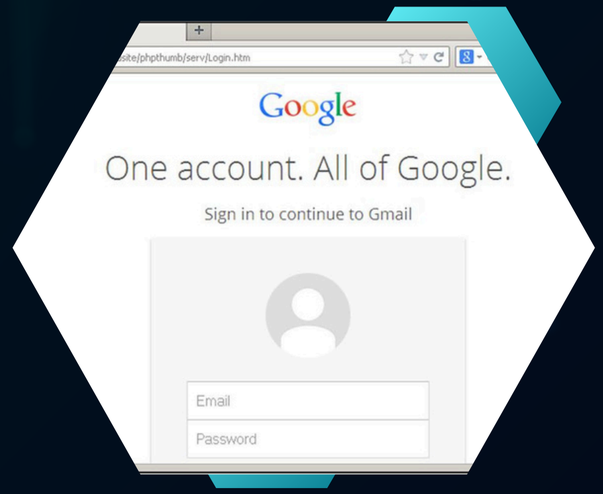
1. Suspicious Sender Addresses: Look for slight misspellings or unusual domains.
2. Generic Greetings: "Dear Customer" instead of your name.
3. Urgent or Alarming Language: Claims that your account will be closed or you need to act immediately.
4. Suspicious Links: Hover over links to check their actual destination.

REAL-WORLD EXAMPLES



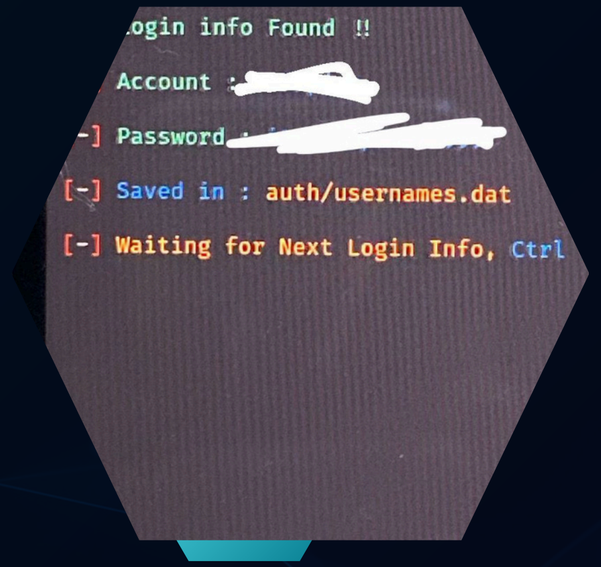
First you receive a Gmail

It might not look suspicious from the outside



You open the link

If you enter the link it's gonna seem like a normal google login page, but if you concentrate well you will notice that its not legit



You entered your credentials

When you enter your credentials they will be sent to the hacker

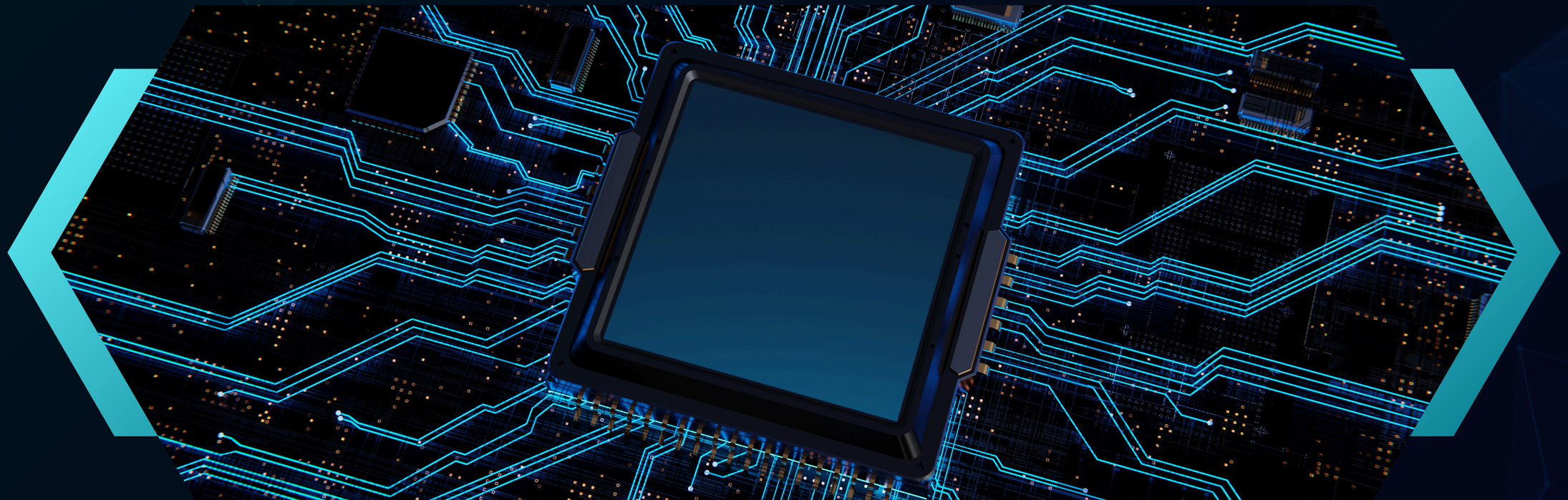
CONSEQUENCES OF PHISHING

Financial Loss: Theft of money and financial information.

Data Breaches: Compromised organizational data.

Identity Theft: Unauthorized use of personal information.

Reputational Damage: Loss of trust and credibility.

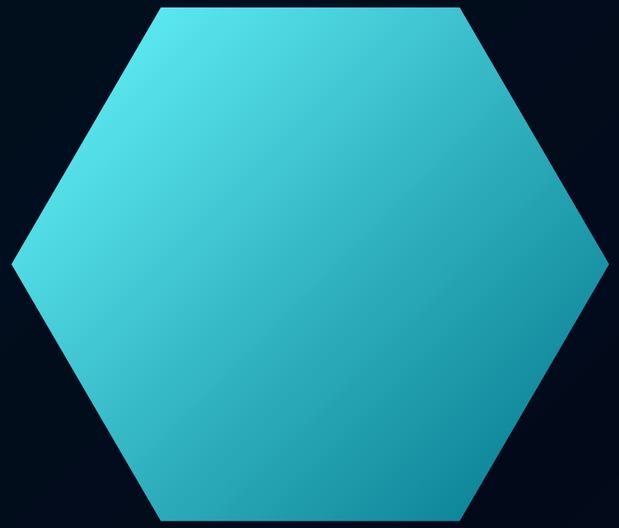


PROTECTING YOURSELF FROM PHISHING

Verify Sources: Always check the legitimacy of emails and messages.

Be Cautious with Links: Avoid clicking on suspicious links.

Use Multi-Factor Authentication (MFA): Adds an extra layer of security.



Keep Software Updated: Ensure all applications and systems are up to date.

Educate Yourself and Others: Stay informed about phishing tactics and share knowledge.

WHAT TO DO IF YOU ARE PHISHED

Do Not Panic

Stay calm and assess the situation.

Report the Attack:

Notify your IT department or the relevant authority.

Change Passwords

Update your credentials immediately.

STAYING VIGILANT AGAINST PHISHING ATTACKS

- Key Points Recap:
  - Phishing aims to steal sensitive information through deception.
  - Recognize signs like suspicious emails and urgent requests.
- Importance of Vigilance:
  - Stay informed about evolving phishing tactics.
  - Participate in regular cybersecurity training.
  - Always verify sources before clicking links or sharing information.
- Empowering Others:
  - Educate family, friends, and colleagues on phishing prevention.
  - Encourage reporting of suspicious messages.
- Security Measures:
  - Use strong, unique passwords and enable multi-factor authentication.
  - Keep software and security programs updated.
- Final Thought:
  - Cybersecurity is a shared responsibility. Stay vigilant and proactive to reduce phishing risks.