Cyber Security

Phishing Awareness: Don't Get Hooked!

-Ishita Jain

What is Phishing?

Understanding the Threat

Phishing is a type of online fraud where attackers impersonate legitimate entities to steal sensitive information. They can be in form of banks, government agencies, or well-known companies, to gain the trust of their targets, tricking individuals into revealing sensitive data, which includes usernames, passwords, credit card details, social security numbers, and other personal information.

Common goals:

- Steal passwords
- Financial data
- Personal information

Deception

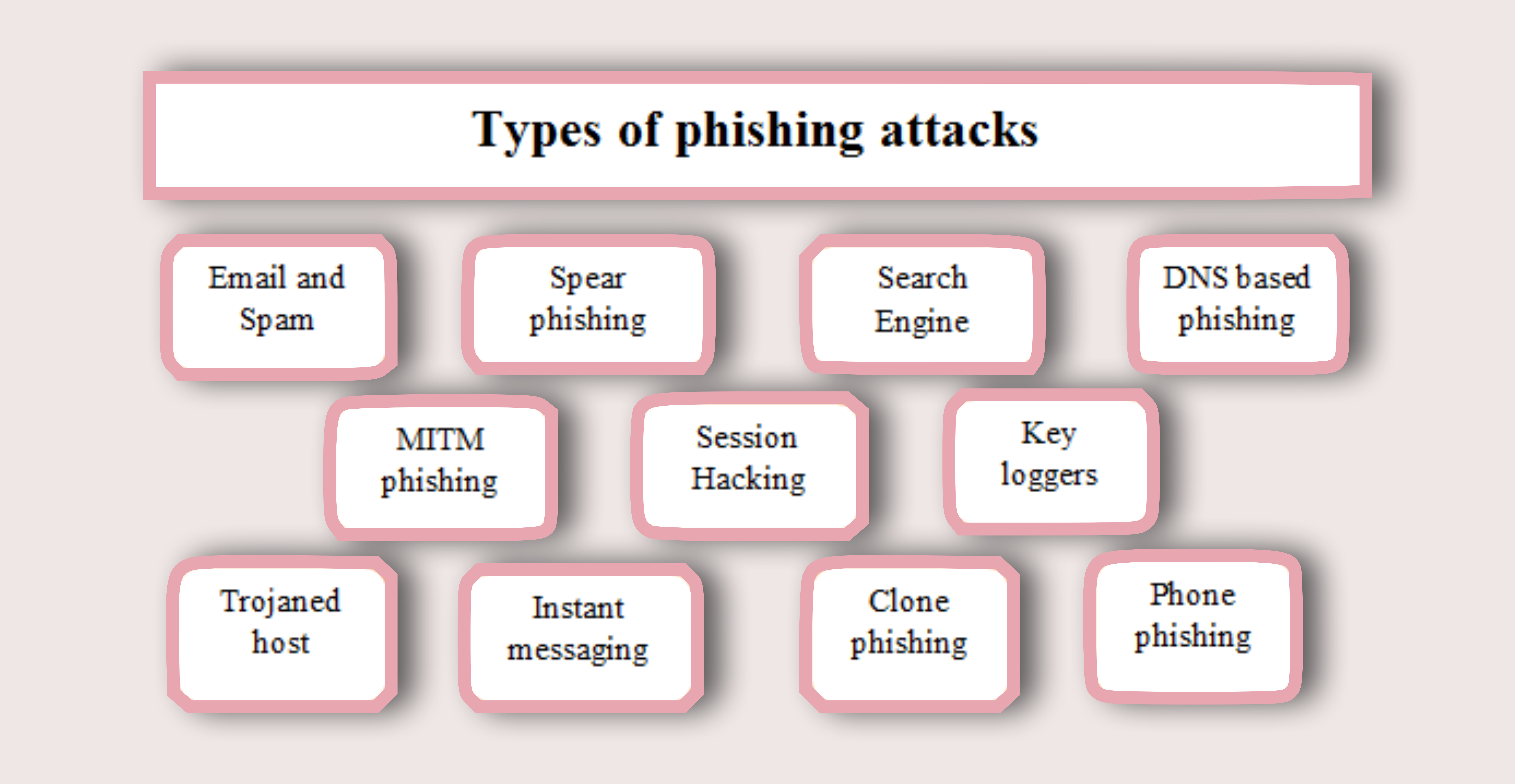
Phishing relies heavily on deception to lure victims into clicking malicious links or opening infected attachments. Attackers craft convincing emails, messages, or websites that appear legitimate, making it difficult for individuals to distinguish them from genuine communications.

Impersonation

Attackers often impersonate trusted entities, such as banks, credit card companies, or government agencies, to create a sense of urgency or authority. This impersonation makes victims more likely to comply with the attacker's requests, such as providing personal information or clicking on suspicious links.

Data Theft

The primary goal of phishing attacks is to steal sensitive information that can be used for financial gain or identity theft. Once attackers obtain this information, they can use it to access bank accounts, make unauthorized purchases, or commit other fraudulent activities.



Types of phishing attacks

- Email and Spam
- Spear phishing
- Search Engine
- DNS based phishing
- MITM phishing
- Session Hacking
- Key loggers
- Trojaned host
- Instant messaging
- Clone phishing
- Phone phishing

Email Phishing

Spotting the Fakes in Your Inbox

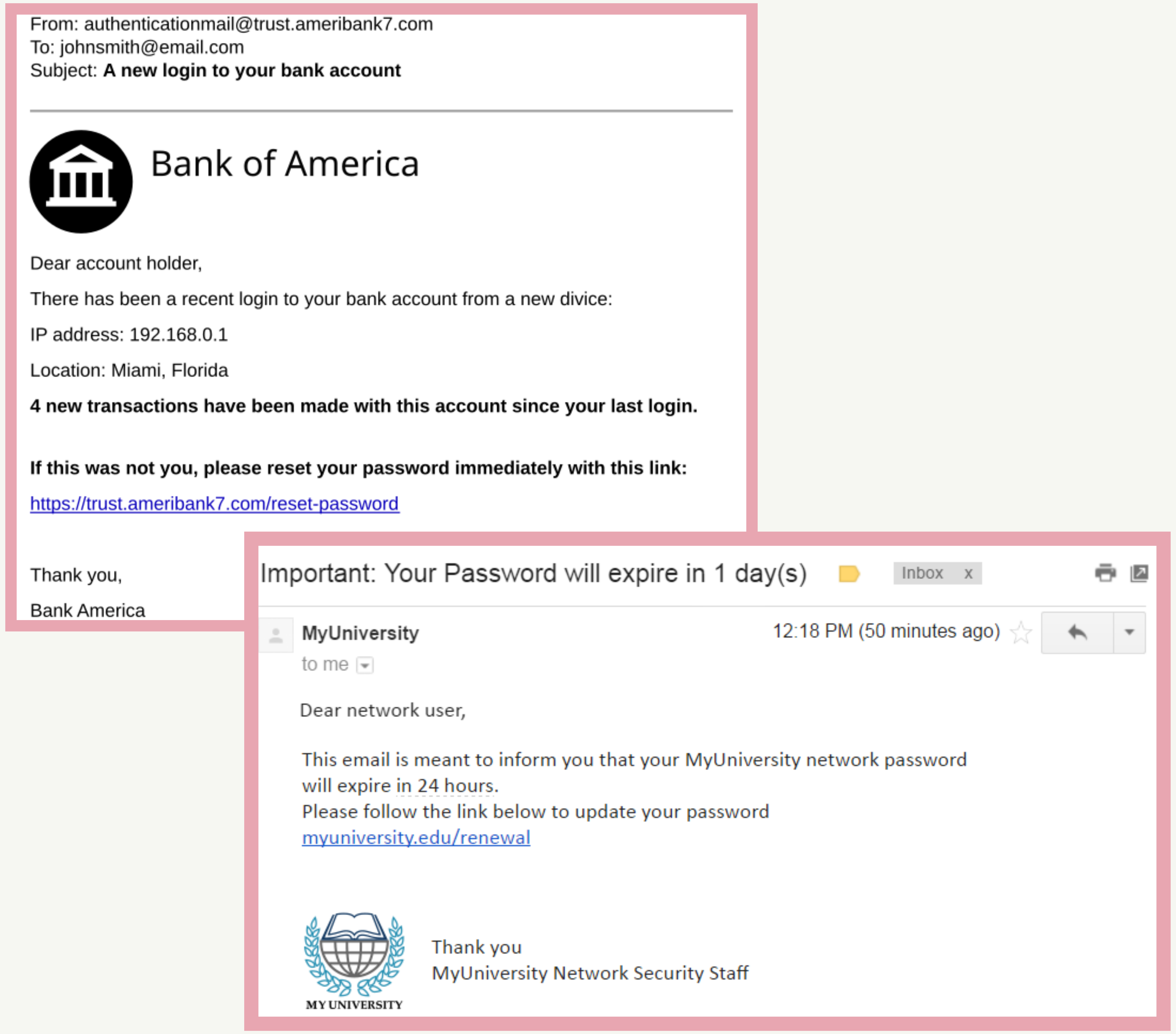
Email phishing is a **fraudulent practice** where cybercriminals send emails disguised as legitimate messages to trick recipients into revealing **sensitive information**, such as login credentials, credit card numbers, or personal data.

Fake Identity – The attacker impersonates a trusted entity (e.g., bank, company, government agency).

Urgency or Fear Tactics – The email often creates panic, such as claiming "Your account has been compromised!"

Malicious Links or Attachments – Clicking the link redirects to a fake website designed to steal credentials or downloads malware.

Data Harvesting – The user unknowingly submits sensitive information to the attacker.



From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

Bank of America

Dear account holder,

There has been a recent login to your bank account from a new divice:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

Thank you,

Bank America

Important: Your Password will expire in 1 day(s)

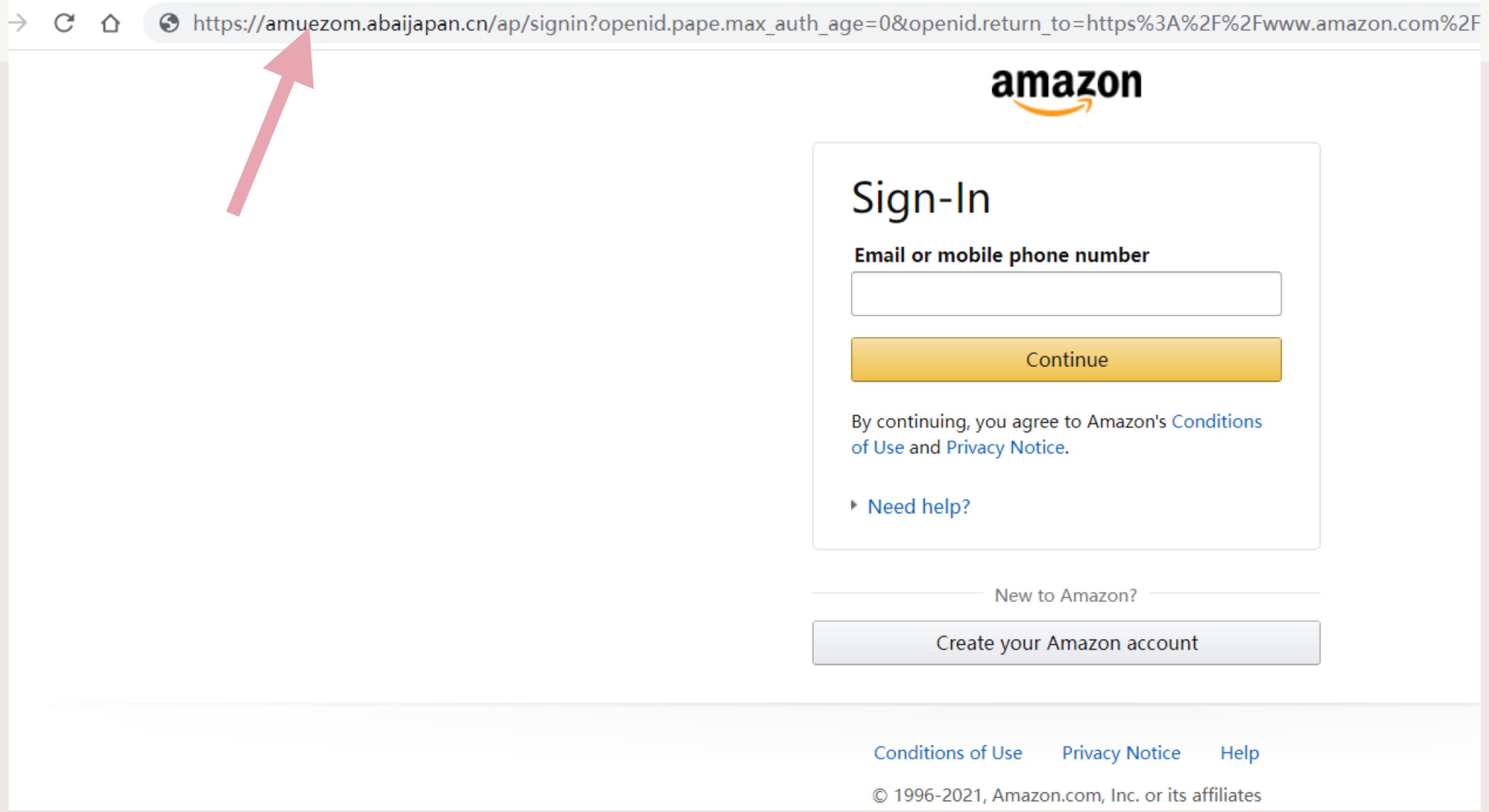
MyUniversity
to me

12:18 PM (50 minutes ago)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff



https://amuezom.abaijapan.cn/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.com%2F

Sign-In

Email or mobile phone number

Continue

By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.

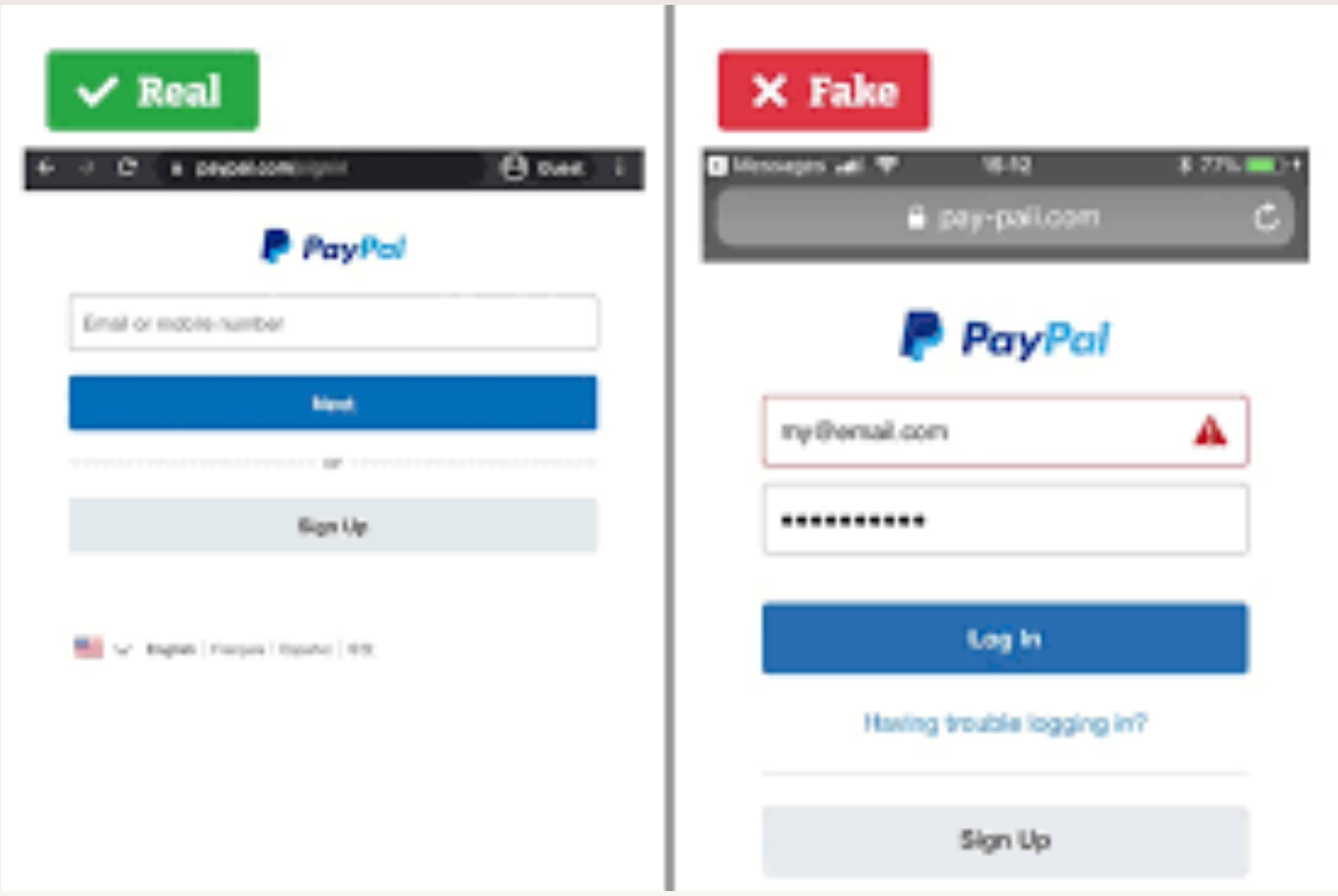
Need help?

New to Amazon?

Create your Amazon account

Conditions of Use Privacy Notice Help

© 1996-2021, Amazon.com, Inc. or its affiliates



Website Phishing

Recognizing Fake Websites

Website phishing is a type of cyberattack where attackers create **fake websites** that mimic legitimate ones to steal sensitive user information, such as login credentials, financial details, or personal data.

Fake Website Creation – The attacker designs a website that looks identical to a well-known platform (e.g., banking sites, social media, e-commerce sites).

Deceptive URL – The web address may have slight misspellings or use **homoglyphs** (e.g., `paypal.com` instead of `paypal.com`).

Phishing Link Distribution – The fake website link is sent via **emails, SMS, ads, or social media** to lure users.

Data Theft – Once users enter their login details or financial information, the attacker captures the data.

Account Takeover – The stolen credentials are used for fraud, unauthorized access, or identity theft.

Social Engineering

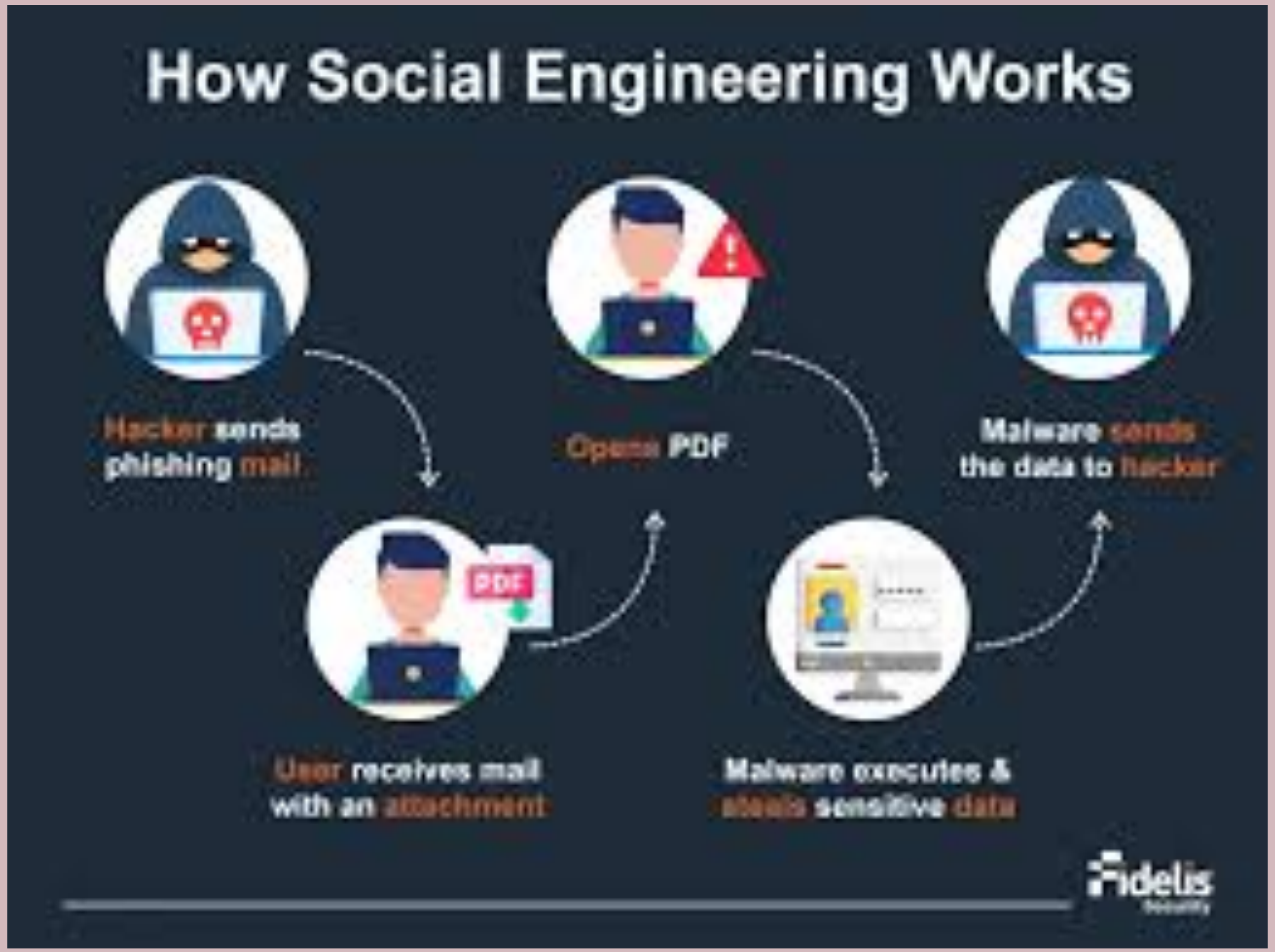
Manipulation Tactics

Social engineering is a **psychological manipulation** technique used by attackers to trick individuals into revealing confidential information, providing access, or taking actions that compromise security. Instead of hacking systems, attackers exploit **human trust and emotions** to achieve their goals.

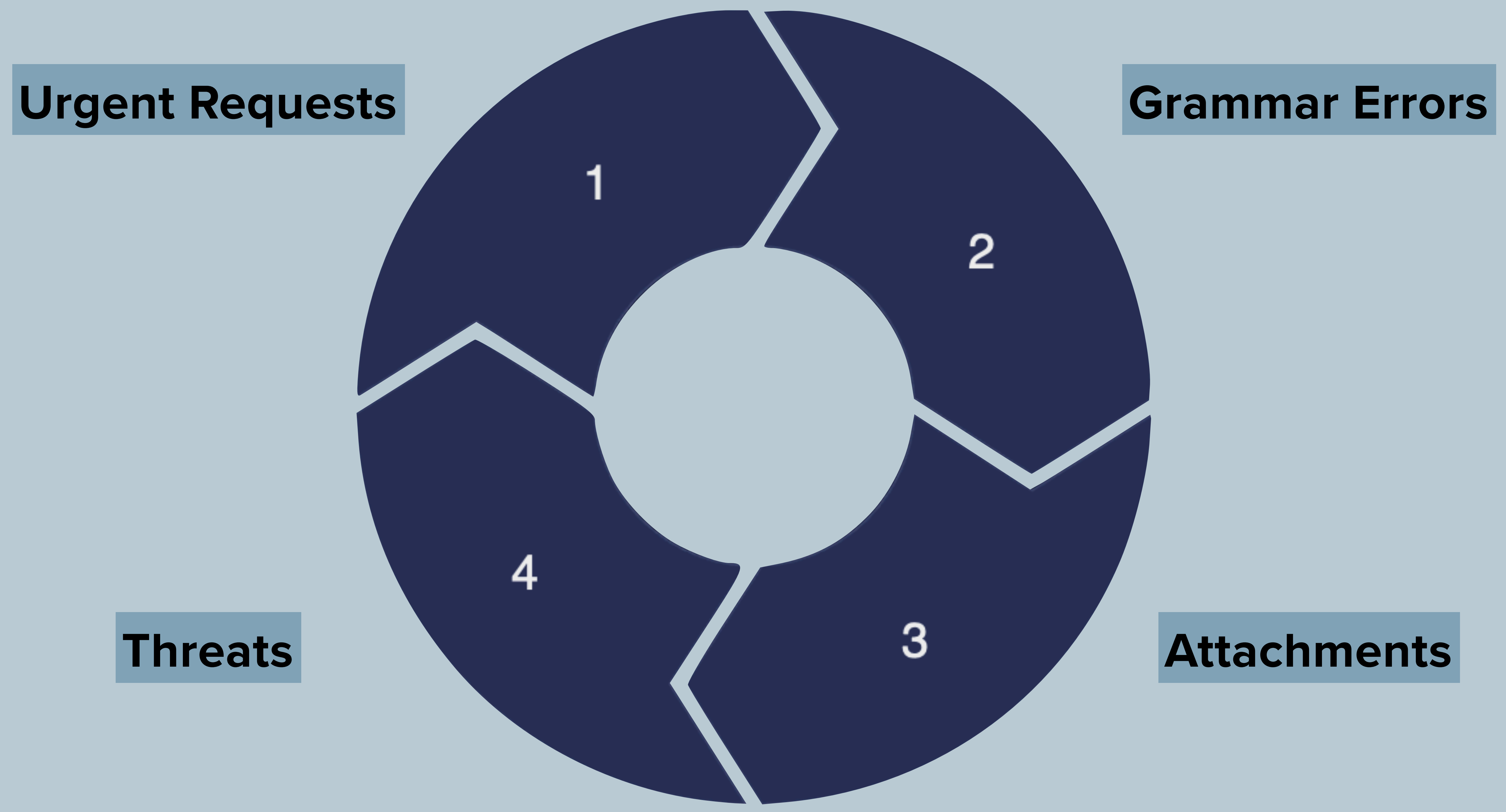
Pretexting – The attacker creates a believable scenario to gain trust.

Manipulation – Using fear, urgency, or authority to pressure the target into acting quickly.

Exploitation – The victim unknowingly provides sensitive information, such as passwords or financial details.


How Social Engineering Works
Hacker sends phishing mail.
User receives mail with an attachment
Opens PDF
Malware executes & steals sensitive data
Malware sends the data to hacker
PDF
Fidelis Security

Red Flags: Common Indicators of Phishing Attempts



Real-World Examples

Case Studies of Phishing Attacks

Google & Facebook (2013-2015) – $100 Million Scam

Attack Method: Business Email Compromise (BEC)

- A Lithuanian hacker impersonated **Quanta Computer**, a legitimate vendor working with **Google and Facebook**.
- He sent fake invoices to the companies, convincing them to wire payments to **fraudulent bank accounts**.
- Since the emails looked authentic, the companies unknowingly paid **over $100 million** before detecting the fraud.

Lesson Learned:

- Always **verify invoices** and payment requests with known contacts.
- Implement **multi-person approval** for large transactions.

Twitter Bitcoin Scam (2020) – High-Profile Account Hijacking

Attack Method: Social Engineering via Vishing (Voice Phishing)

- Hackers **called Twitter employees**, pretending to be from internal IT support.
- They tricked employees into resetting passwords and providing access to internal tools.
- Attackers took control of **verified Twitter accounts** (Elon Musk, Bill Gates, Apple, etc.) and posted **Bitcoin scam tweets**.
- The scam generated **over $100,000** in Bitcoin before being shut down.

Lesson Learned:

- Employees should be trained to **verify IT requests** before providing sensitive access.
- Implement **strict access controls** and monitor internal account activity.

Prevention Tips

Best Practices for Staying Safe

Prevention is the best cure. Here are some preventive measures:

🧠 **Think Before You Click** – Hover over links to check their destination before clicking.

💀 **Verify Senders** – Check email addresses for typos or unusual domains.

🚩 **Look for Red Flags** – Be cautious of urgent language, generic greetings, and unexpected attachments.

🫆 **Use Multi-Factor Authentication (MFA)** – Adds an extra layer of security even if your password is stolen.

📰 **Check Website Authenticity** – Ensure URLs use **HTTPS** and don’t contain misspellings.

↻ **Keep Software Updated** – Install the latest security patches to protect against vulnerabilities.

✉ **Report Suspicious Emails** – Notify IT/security teams if you suspect phishing.

Reporting Phishing

What To Do If You Suspect An Attack

Reporting phishing is essential. If you suspect an attack, report it.

— **Do Not Click** – Avoid clicking on links or downloading attachments.

— **Do Not Respond** – Ignore emails/messages asking for personal information.

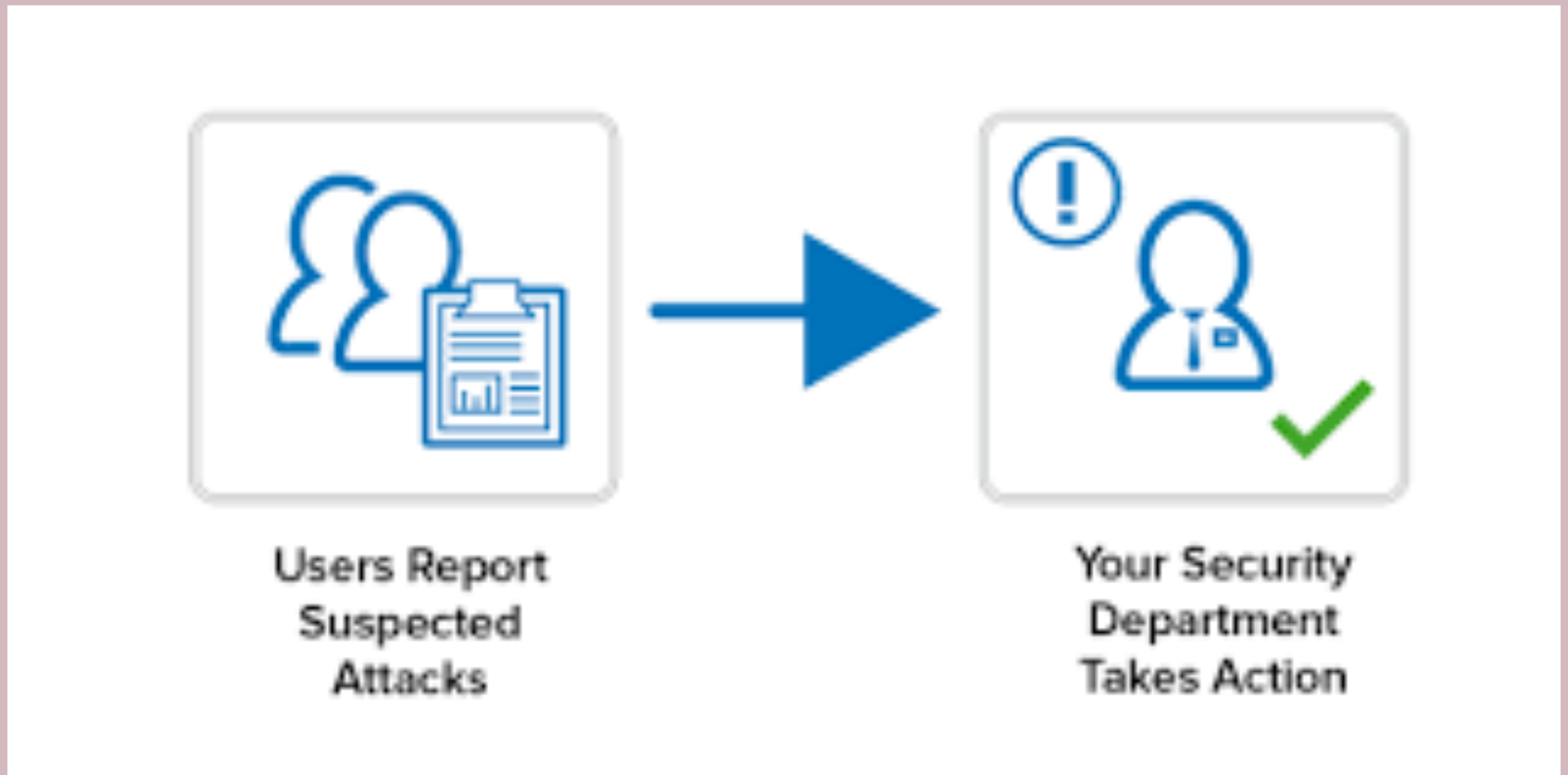
— **Report It** – Forward the email to your **IT/security team** or anti-phishing authorities i.e Anti-Phishing Working Group (**APWG**).

— **Block the Sender** – Mark the email as **spam/phishing** in your email provider.

— **Verify Through Official Channels** – Contact the sender directly using official contact details.

— **Scan Your Device** – Run an **antivirus scan** if you clicked on a suspicious link.

— **Change Your Passwords** – If you suspect a compromise, update your credentials immediately.



Thank You

Staying vigilant is key to protecting yourself.