PHISHING

Think before you click !

What is Phishing?

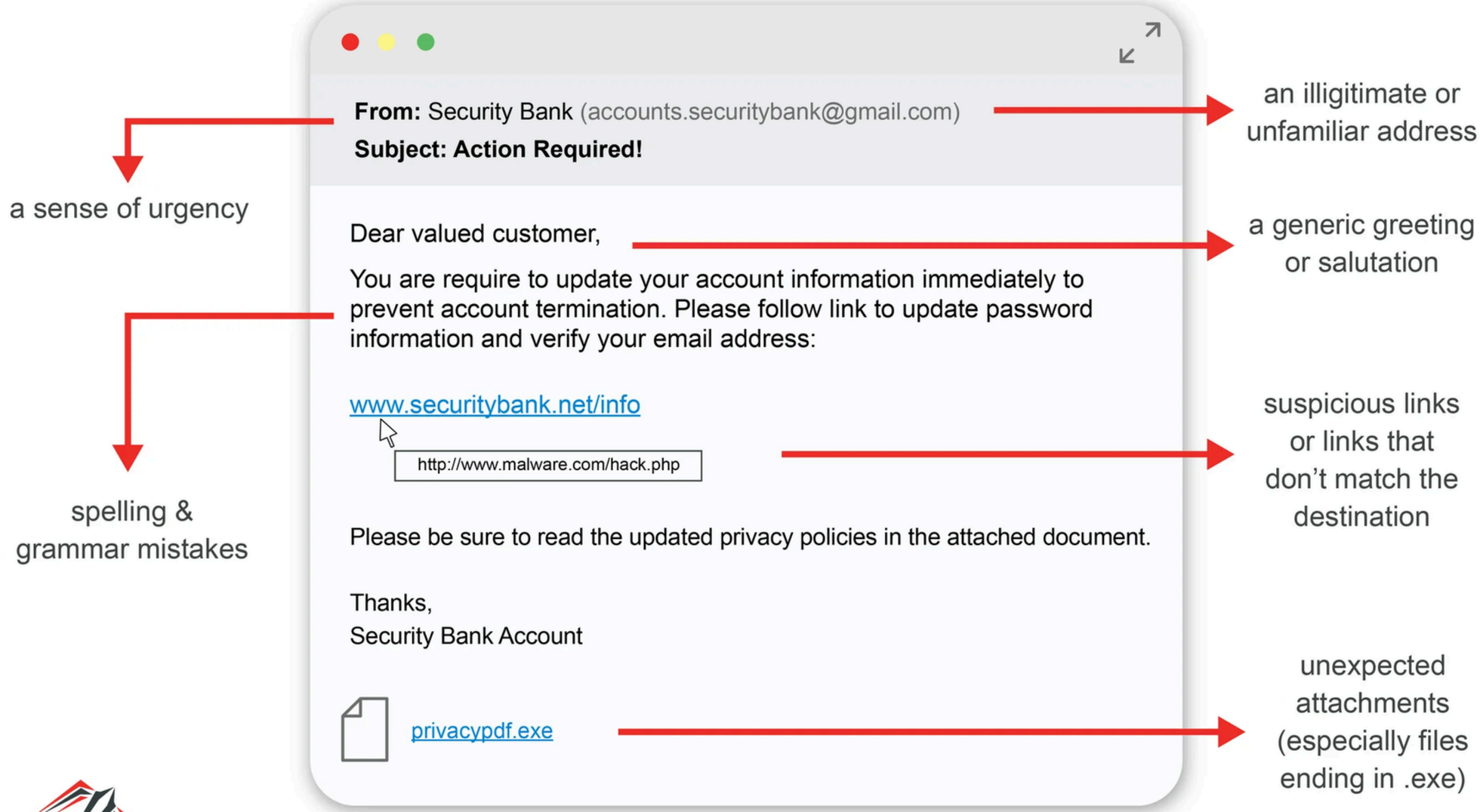
Phishing is a type of cyber attack where attackers trick you into revealing sensitive information like passwords, credit card numbers, or personal details.

Types of Phishing ?

1. Fake emails that trick users into giving sensitive information.
2. Phishing through phone calls or voice messages.
3. Phishing via SMS/text messages to steal data.
4. Personalized attacks on specific individuals.

HOW TO RECOGNIZE ?

Look for suspicious sender addresses (e.g., info@amaz0n.com instead of info@amazon.com).
Generic greetings like “Dear Customer” instead of your name.
Urgency or threats (e.g., “Your account will be closed if you don’t act now!”).
Suspicious links or attachments – hover over links to verify the URL.
Poor grammar or spelling mistakes.


From: Security Bank (accounts.securitybank@gmail.com)
Subject: Action Required!
Dear valued customer,
You are require to update your account information immediately to prevent account termination. Please follow link to update password information and verify your email address:
www.securitybank.net/info
http://www.malware.com/hack.php
Please be sure to read the updated privacy policies in the attached document.
Thanks,
Security Bank Account
privacypdf.exe
a sense of urgency
spelling & grammar mistakes
an illigitimate or unfamiliar address
a generic greeting or salutation
suspicious links or links that don't match the destination
unexpected attachments (especially files ending in .exe)

Phishing Prevention

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

What to Do If You Experience an Attack?

Report the incident to authorities.

Contact IT support or technical assistance.

Change passwords and monitor account activity.