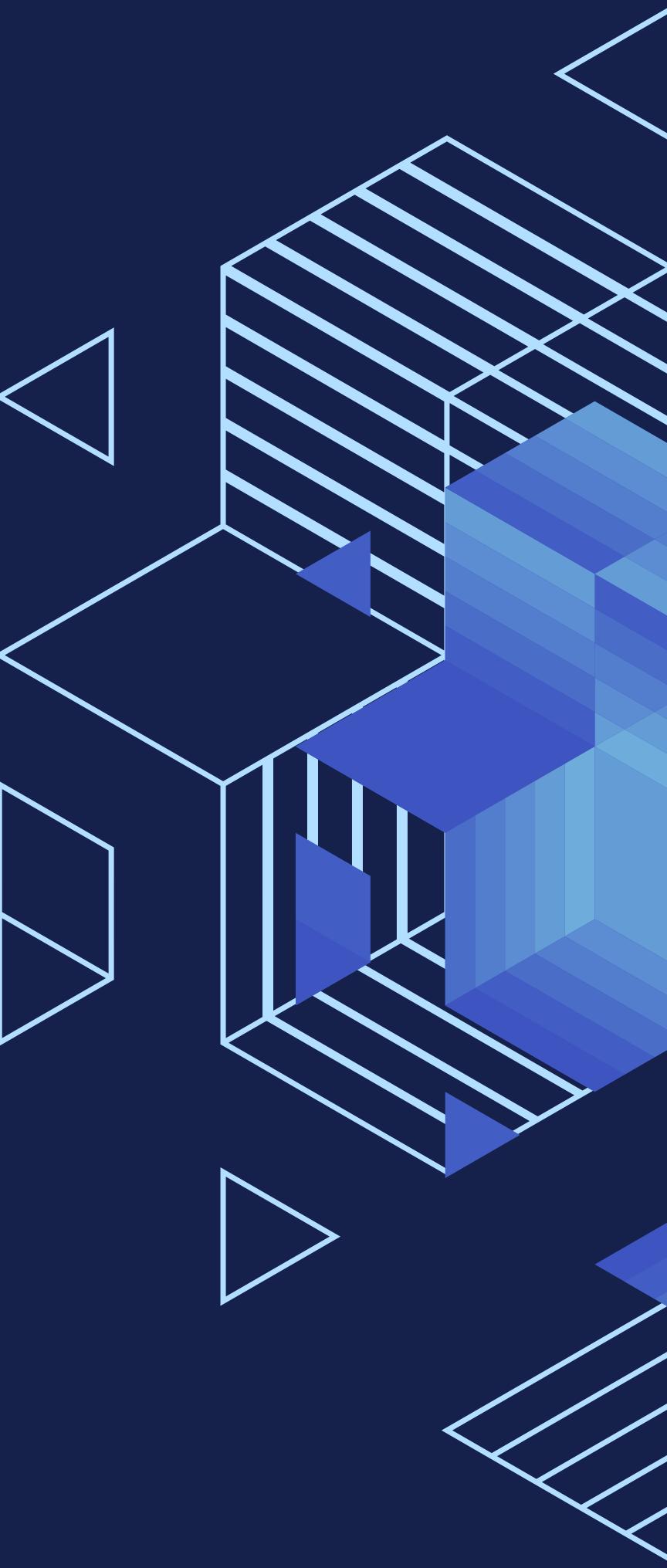


# PHISHING AWARENESS TRAINING



# Table Of Content

- ▶ Understanding Phishing
- ▶ Recognizing Phishing Attacks
- ▶ Avoiding Phishing Traps
- ▶ Responding to Phishing Incidents
- ▶ Tips and Practices





## Why it Matters?

- Phishing attacks are one of the most common cybersecurity threats today.
- It is a widespread problem across every industry because this type of scam is extremely easy to pull off.
- These attacks target individuals and organizations to steal sensitive information like passwords, credit card numbers, and personal data.
- Being aware and educated is the first step in protecting yourself and your organization from these threats.

# What is Phishing?

## Let us Understand Phishing:

Phishing is a social engineering cyberthreat where scammers impersonate a trustworthy source and trick you into revealing sensitive data like passwords, credit card numbers, or personally identifiable information.



- ▶ Phishing attacks often begin with scammers sending a malicious link or attachment via email, possibly triggering a malware download.
- ▶ You may receive a phishing call that comes from a phisher pretending to offer customer service or tech support.

# Types of Phishing Attacks

**Email Phishing**  
Fake emails that appear to be from trusted sources.



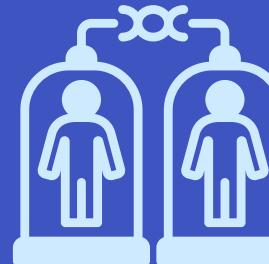
**Spear Phishing**  
Targeted attacks on specific individuals or organizations.



**Clone Phishing**  
An almost identical copy of a legitimate email with malicious links or attachments.



**Smishing**  
Phishing via SMS (text messages) and voice calls.



# How to Spot a Phishing Email?

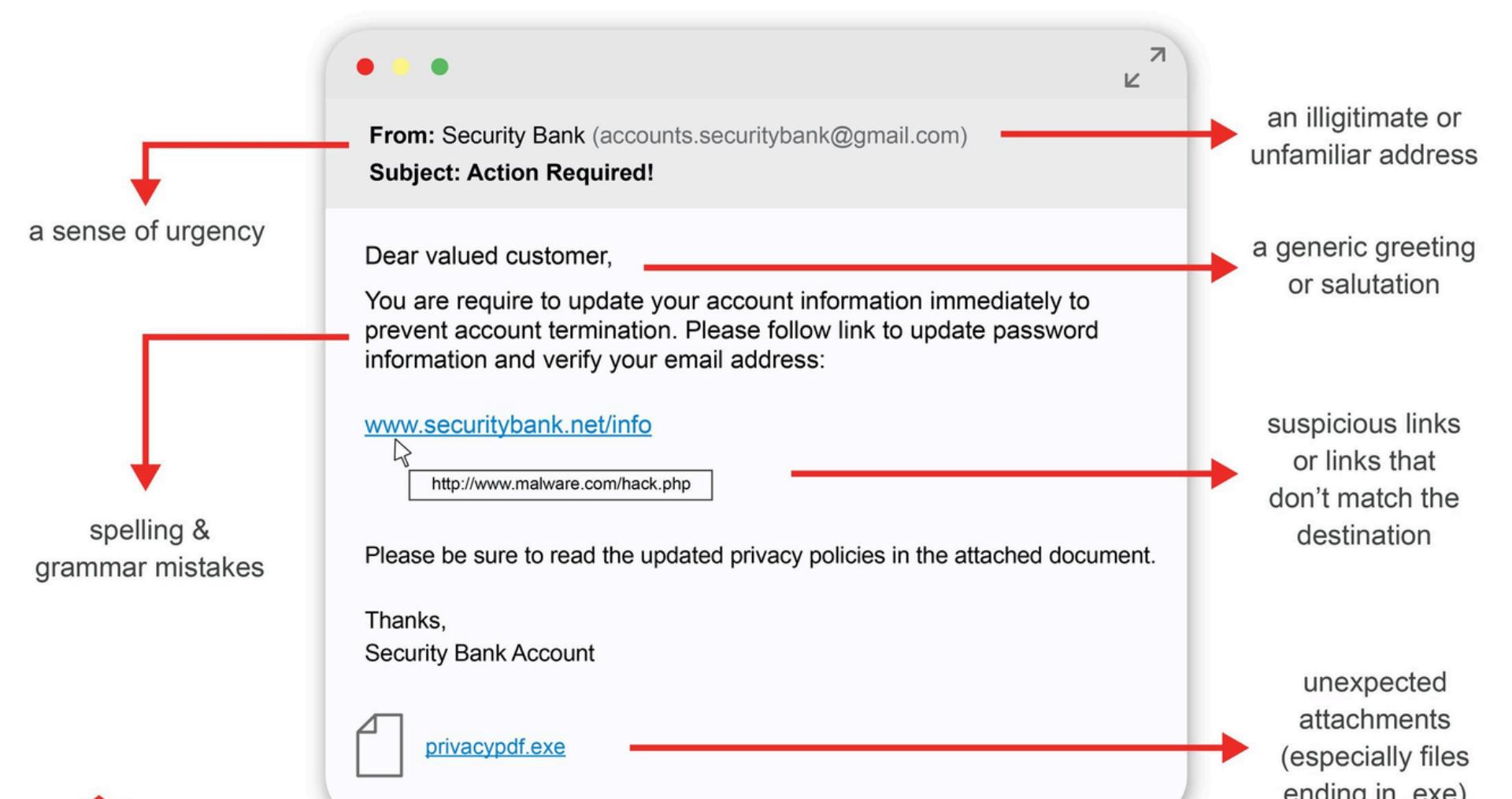
Let's Dive In!



- ▶ **Suspicious Sender:** Check the email address carefully. Phishers often use addresses that are similar but not identical to legitimate ones.
- ▶ **Spelling and Grammar Mistakes:** Poor language is often a sign of a phishing attempt.
- ▶ **Unexpected Attachments or Links:** Never open attachments or click on links from unknown or unexpected sources.
- ▶ **Urgency and Threats:** Phishers often use scare tactics to prompt immediate action.

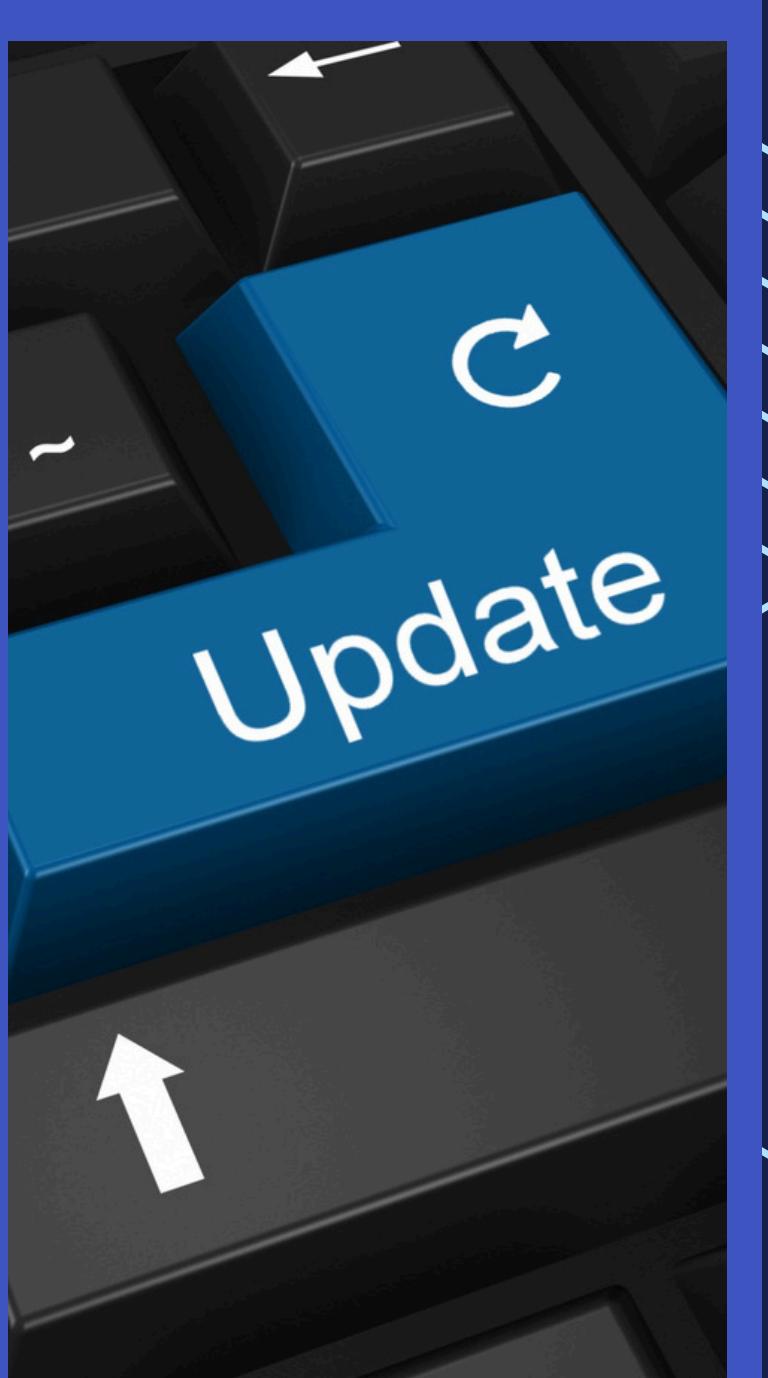
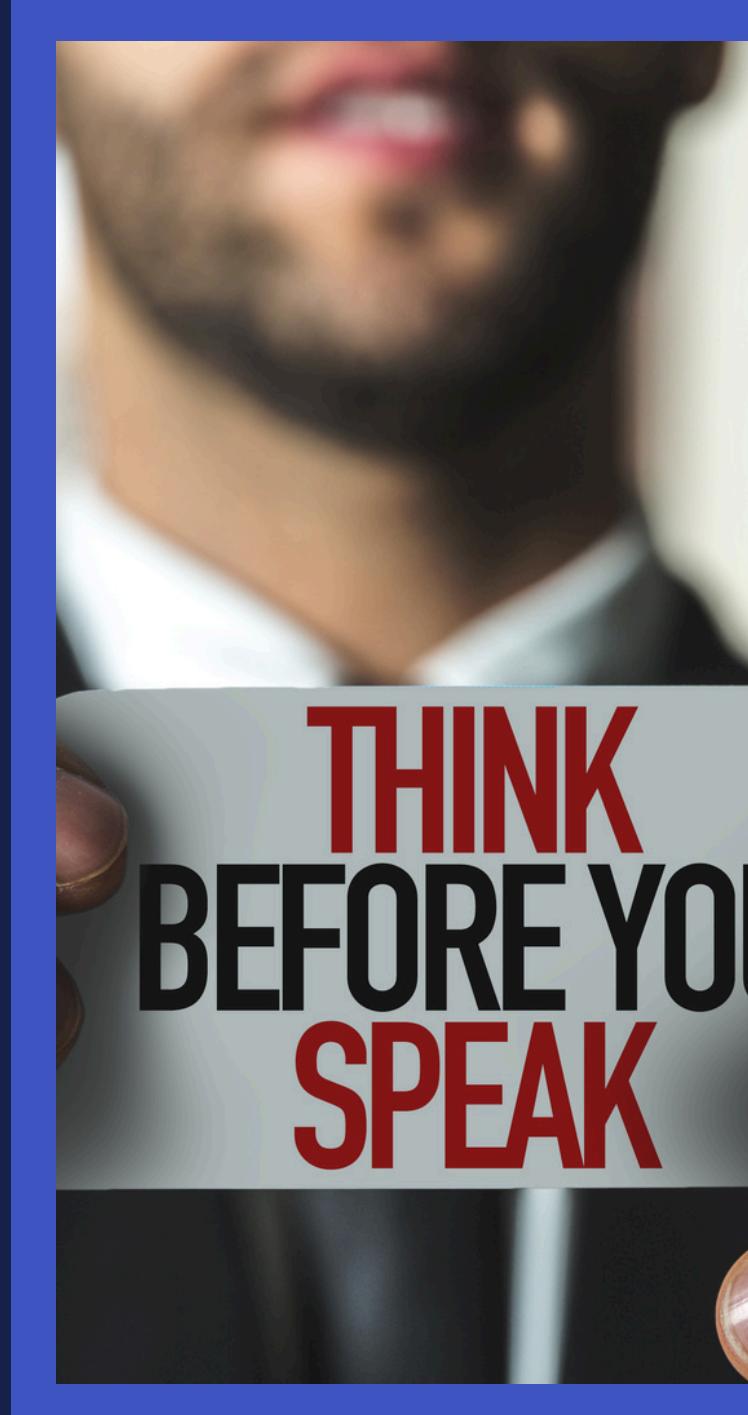
# SAMPLE OF PHISHING EMAIL

## WATCH OUT FOR...



# How To Avoid Phishing Traps?

- **Think Before You Click:** Always hover over links to see the actual URL before clicking.
- **Enable Multi-Factor Authentication (MFA):** Adds an extra layer of security to your accounts.
- **Keep Software Updated:** Regular updates can protect against known vulnerabilities.



# Final Tips and Best Practices

- **Educate Yourself and Others:** Regularly review phishing awareness materials and share knowledge with colleagues.
- **Stay Informed:** Keep up with the latest phishing trends and techniques.
- **Create a Culture of Security:** Encourage a security-conscious environment at work.





# THANK YOU

*Protect Yourself from Online Threats*