Security Awareness Training

mastercard

Cybersecurity Internship on Forage.com

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in digital communication.

Objective: Gain unauthorized access to confidential data or systems.

Departmental Vulnerability Performance

From: hr@banking-secure.com
To: employee@bank.com
Subject: Important: Confirm Your Attendance for Upcoming Training

---

Dear [Employee Name],

As part of our ongoing commitment to professional development, we are excited to confirm your registration for the upcoming [Annual Financial Compliance Training] scheduled for [Date]. This training is mandatory and crucial for maintaining our regulatory standards.

To complete your registration, please verify your details and confirm your attendance by clicking the link below. Your prompt action is required to finalize the process and ensure your spot in the training session.

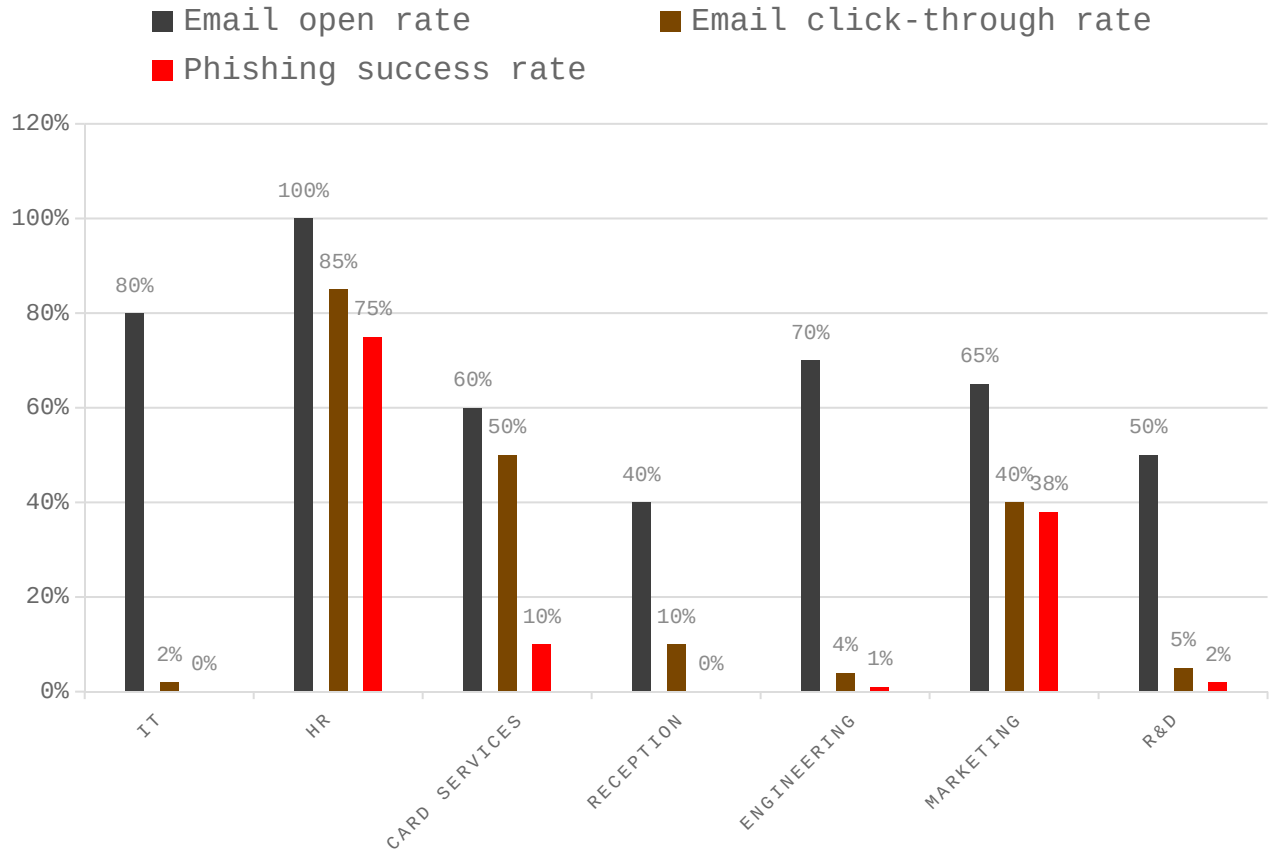
Click here to **Confirm Your Registration**

Additionally, as a reminder, we noticed your recent update about your child's upcoming birthday on our employee portal. If you have any special requests or dietary needs for the event, please let us know through the link above.

Should you have any questions or need assistance, feel free to contact our HR team at hr-support@bank.com.

Thank you for your cooperation and dedication.

Best regards,
Sarah Johnson
HR Manager
Banking Secure



mastercard

Identifying Phishing Attempts

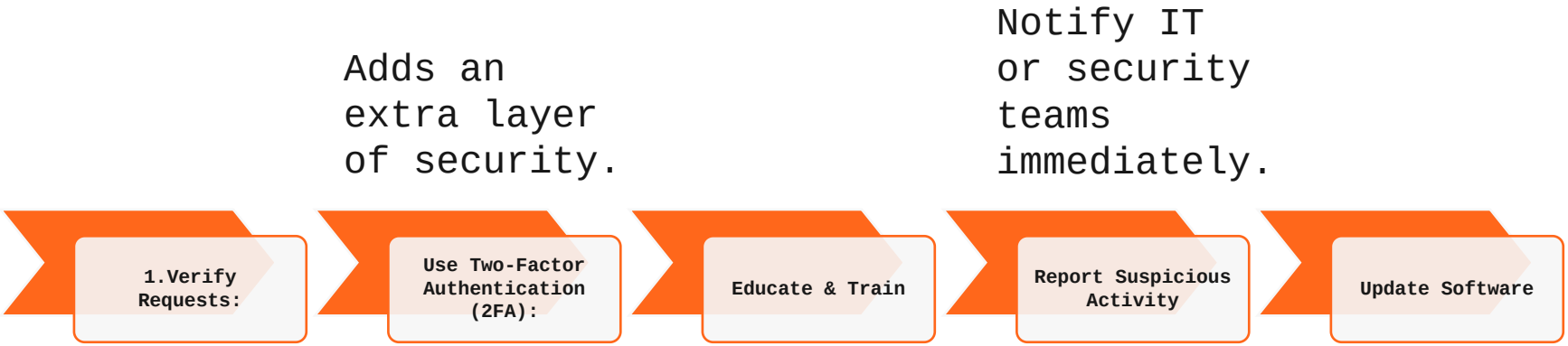
Suspicious Sender: Check for discrepancies in the sender’s email address.

Urgency & Threats: Be cautious of emails that create a sense of urgency or fear.

Generic Greetings: Look for generic greetings like "Dear Valued Employee."

Unverified Links: Hover over links to ensure they lead to a legitimate website.

Preventing Phishing Attacks



mastercard

Summary & Resources

#1 Watch for suspicious senders, urgent requests, generic greetings, and unverified links

#2 Watch for suspicious senders, urgent requests, generic greetings, and unverified links

#3 Verify requests, use two-factor authentication, stay informed, report suspicious activity, and keep software updated.

#4 Analyze phishing incident statistics to identify and address vulnerabilities in different departments.

- **Contact IT Security:** [Contact Information]
- **Phishing Reporting:** [Reporting Procedures]
- **Additional Training:** [Links to further training materials