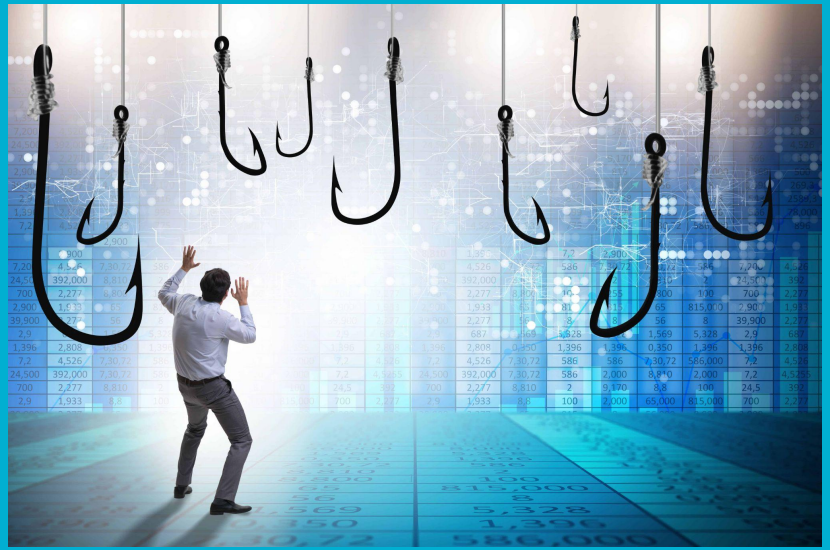
Strengthening Cybersecurity: Phishing Awareness & Prevention

Mastercard Security Team



Familiarize Yourself with Phishing Attacks

High-Risk Teams: HR & Marketing:

- Based on our phishing simulation, these teams were most susceptible.
- This training will help you recognize and avoid phishing threats.
- Stay vigilant to protect our organization's security.

What is Phishing?

- **Phishing is a social engineering attack** used to steal sensitive information by pretending to be a trustworthy source.
- **Cybercriminals often target employees via:**
  - **Emails that look legitimate but contain malicious links.**
  - **Fake websites designed to capture login credentials.**
  - **Urgent messages tricking users into quick action.**
- **Example: An email claiming your account is compromised and urging you to reset your password immediately.**

Learn to Spot Phishing Emails

Key Signs of Phishing Emails:

- **Suspicious Sender:** The sender's email address is slightly altered (e.g., security@mastercard-secure.com instead of security@mastercard.com).
- **Urgency & Threats:** "Immediate action required! Your account will be locked!"
- **Poor Grammar & Spelling:** Phishing emails often have noticeable errors.
- **Mismatched URLs:** Hover over links before clicking! A link that claims to be mastercard.com might actually be mastercard-login.secure-update.com.
- **Unusual Attachments:** Unexpected invoices, receipts, or password-protected files.

How to Stop Getting Phished

- **Think Before You Click:** Hover over links to check authenticity.
- **Verify the Sender:** If in doubt, contact IT or the sender directly.
- **Report Suspicious Emails:** Use the company's phishing report tool or forward to IT Security.
- **Use Multi-Factor Authentication (MFA):** Even if your password is stolen, MFA can prevent access.
- **Stay Updated on Phishing Tactics:** Regular security awareness training will keep you informed.

Think Before You Click