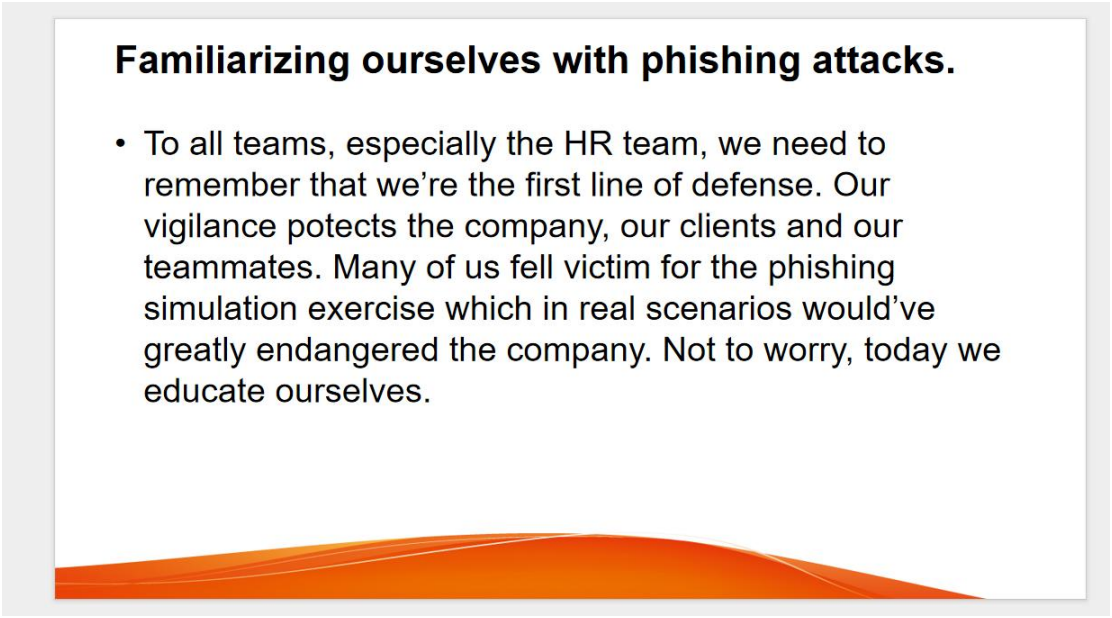
PHISHING AWARENESS CAMPAIGN FOR MASTERCARD



What is PHISHING?

- Phishing is a type of cyber attack where attackers try to trick people into revealing sensitive information—like passwords, credit card numbers, or personal data—by pretending to be a trusted source. It could come in form of:

1. Impersonation e.g Fake email from "IT Support" or "CEO"
2. Fake Emails/Links e.g “Click here to reset your password”
3. Urgent Language e.g “Your account will be locked in 24 hours!”
4. Lookalike Websites e.g www.secure-mastercard.com instead of mastercard.com
5. Data Theft e.g Asking for login, bank info, or OTPs

Spotting a Phishing Email

Red Flags:

- Unexpected request (e.g. "update info now")
- Strange sender or misspelled domain
- Generic greeting: "Dear user"
- Urgent tone or threats
- Weird links: Hover to preview

Don't click — report it!

How to Protect Yourself:

- Use strong, unique passwords
- Enable 2FA (two-factor authentication)
- Lock your screen when away
- Report suspicious emails

What to Do If You Suspect a Threat:

- Don’t engage
- Take a screenshot if needed
- Report to IT/security immediately
- Encourage others to be alert

Reporting helps the whole organization.

THANK YOU!