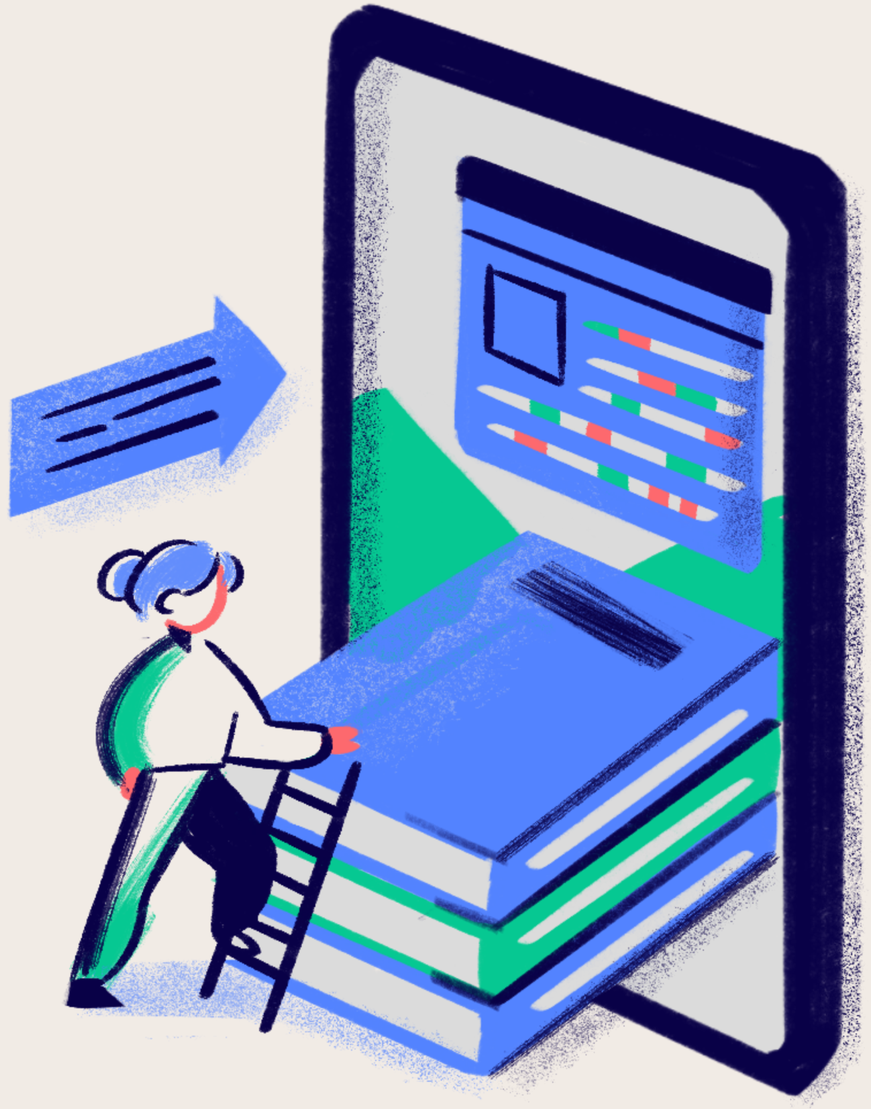
PHISHING ATTACKS

REPORT

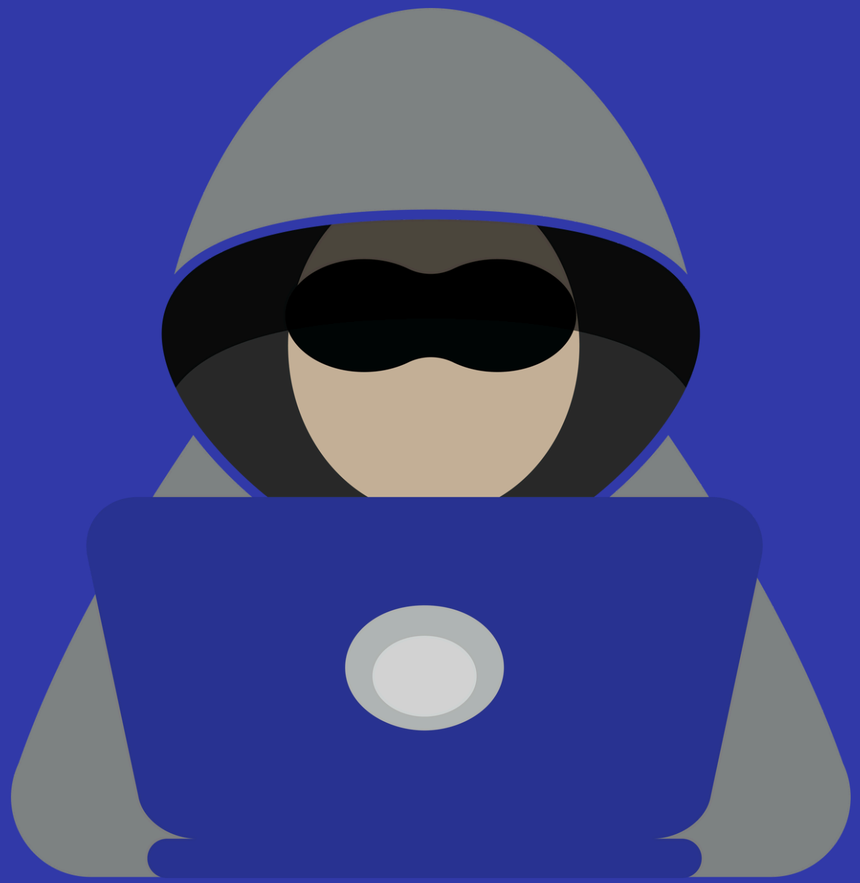


FAMILIARIZE YOURSELF WITH PHISHING ATTACKS

Team	Email open rate	Email click-through rate	Phishing success rate
IT	80%	2%	0%
HR	100%	85%	75%
Card Services	60%	50%	10%
Reception	40%	10%	0%
Engineering	70%	4%	1%
Marketing	65%	40%	38%
R&D	50%	5%	2%
Overall average	**66%**	**28%**	**18%**

RISKS

RISKS



WHAT IS PHISHING?

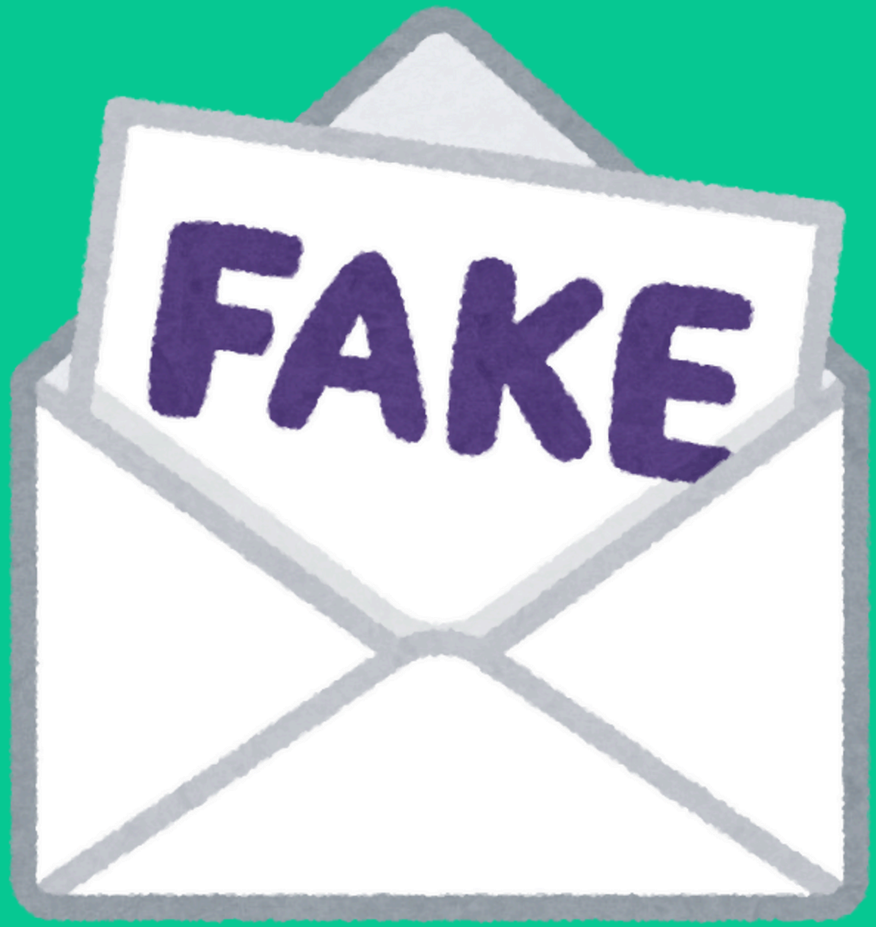
Phishing is a sneaky attempt by attackers to steal your personal information, like passwords, credit card numbers, or even your social security number. They try to trick you by pretending to be someone you trust, like your bank, boss, or a co-worker.

Here's how it typically works:

- You receive an email, text message, or even a social media message.
- The message will look like it's from a real company or person.
- The message will try to create a sense of urgency or trick you into clicking on a link.
- That link will take you to a fake website that looks like the real one.
- Once you enter your information on the fake website, the attacker steals it.

LEARN HOW TO SPOT PHISHING EMAILS

- Urgency: Phishing emails often pressure you to act fast, claiming your account is locked, a payment is overdue, or there's suspicious activity. Legitimate companies will usually give you ample time to respond.
- Generic Greetings: Phishing emails might use generic greetings like "Dear Customer" instead of your name. A real company that interacts with you will likely use your name.
- Poor Grammar & Spelling: While not foolproof, unprofessional writing with typos and grammatical errors can be a sign of a phishing attempt. Legitimate companies typically have good quality control over their email communication.
- Suspicious Links & Attachments: Don't hover over, let alone click, links or open attachments in emails you suspect are phishing attempts. Real companies won't send unexpected attachments unless previously discussed.



HOW DO WE STOP PHISHING?

Awareness and Training:

- Education is key: Simulate phishing attacks with your employees to train them on spotting red flags. Explain how phishing works and the potential consequences.
- Regular reminders: Periodically send reminders about phishing tactics and best practices to keep employees vigilant.

Tech Safeguards:

- Strong Passwords & 2FA: Enforce strong, unique passwords for all accounts and enable two-factor authentication (2FA) wherever possible. This adds an extra layer of security beyond just a password.
- Anti-Phishing Tools: Consider anti-phishing software or browser extensions that can warn users about suspicious links and websites.
- Software Updates: Ensure all devices and software are kept up to date with the latest security patches.

PRESENTED BY PHARAOH BHASA

THANK YOU VERY MUCH!