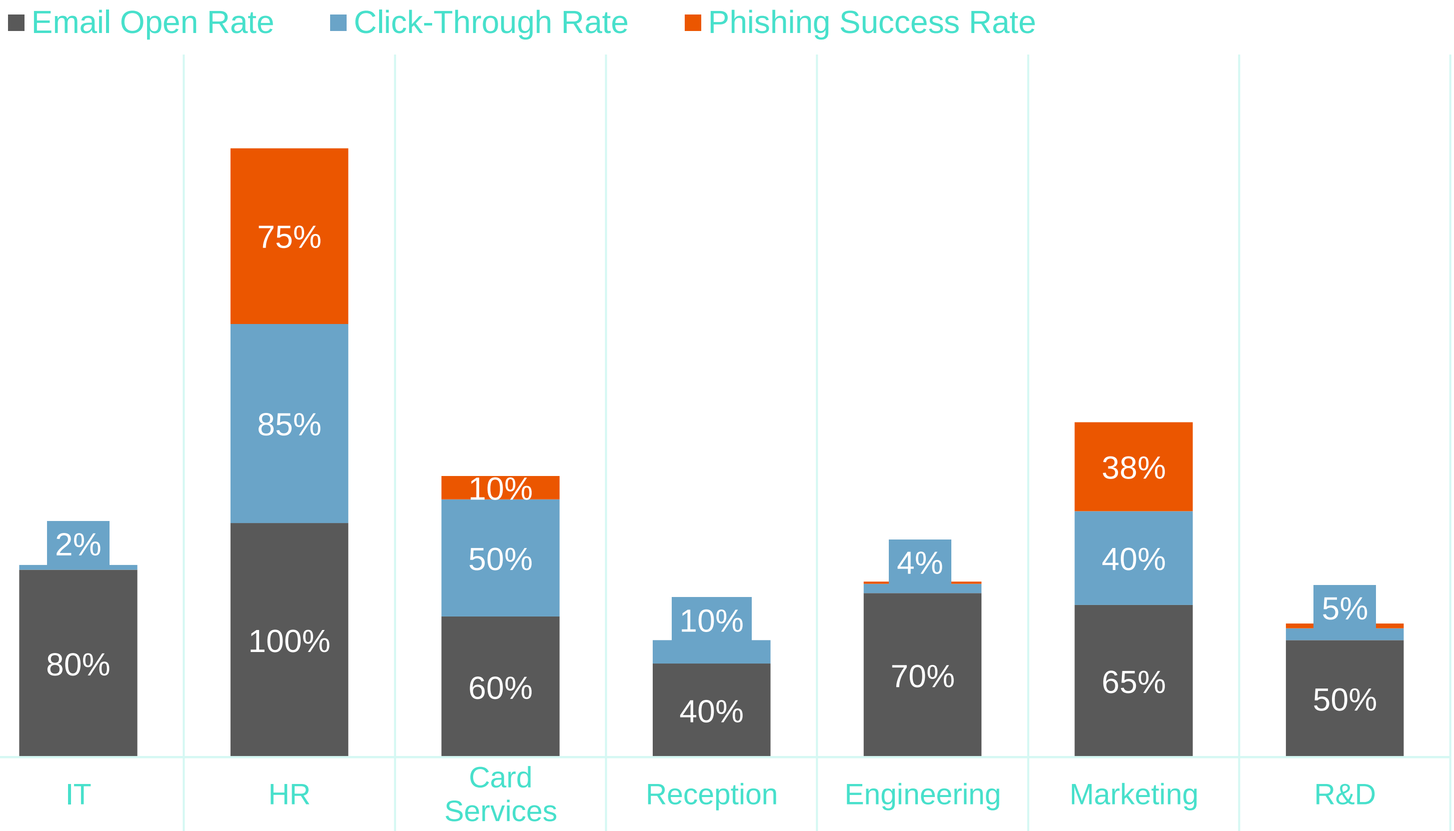
Familiarize yourself with phishing attacks

Based on the phishing simulation, the following departments had the highest click-through and phishing success rates:

-HR Department: 85% and 75%
-Marketing Department: 40% and 38%

DEPARTMENT RATES



	IT	HR	Card Services	Reception	Engineering	Marketing	R&D
🟧 Phishing Success Rate	0%	75%	10%	0%	1%	38%	2%
🟦 Click-Through Rate	2%	85%	50%	10%	4%	40%	5%
⬛ Email Open Rate	80%	100%	60%	40%	70%	65%	50%

What is phishing?

Phishing is a social engineering attack where bad actors pose as legitamate contacts or institutions to trick employees into revealing personally identifiable information, confidential information, or sensitive information such as passwords.

This can be done easily by simply clicking on a malicious link or attachment in the email.

Learn to spot phishing emails

- Look closely at the senders email address, the phising emails will usually originate from an illegitamte domain.
- Watch for urgent or threatening language, bad actors use this tactic often to instill fear and get the victim to take action.
- Hover over links before clicking! Doing this will help reveal the true link which will help you decide if the link is legitimate or not.
- Watch for poor grammar and formatting, amatuer phishing emails will often have this and make it easy to spot.
- Watch for requests of personal info, this is also usually an indicator of a phising email.

How do we stop getting phished?

- Report any suspicious emails, this will prevent others from getting phished sooner.
- DO NOT enter any credentials from an email link.
- Use multi-factor authentication (MFA) to protect passwords in case of a successful phishing attempt.
- Complete phishing awareness training and always be on alert.