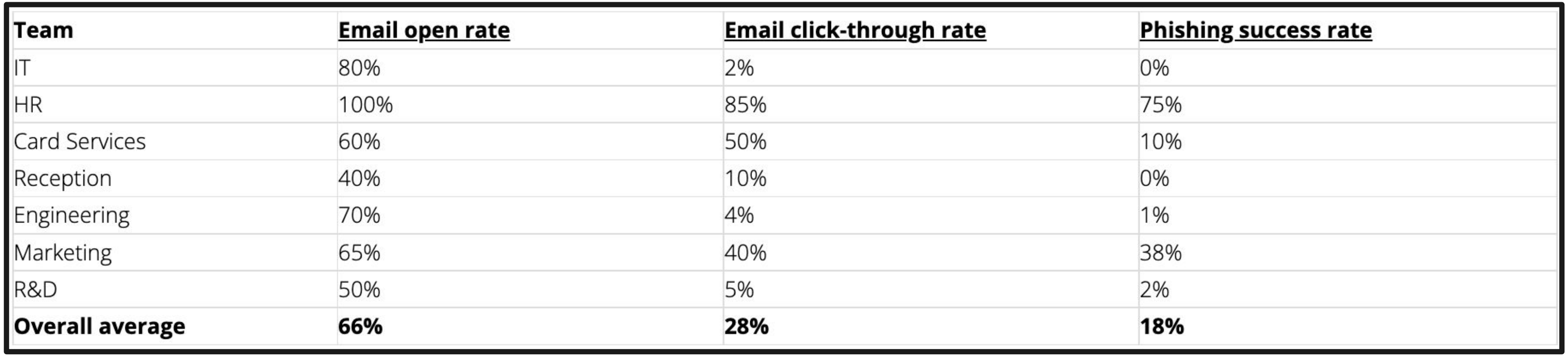
Phishing Emails Awareness

mastercard

Familiarize Yourselves 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%**

Teams Most at Risk

. HR | Phishing Success Rate = 75%

. Marketing | Phishing Success Rate = 38%

What is Phishing?

. Phishing is “*cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.*” (Phishing.org)

. Any time you receive an **Email**, **Text Message**, or **Phonecall** it has the potential to be a phishing attack

Learn How to Spot Phishing Emails

5 Ways to Spot a Phishing Email:

1. **Suspicious Sender Address**: The sender’s email address may look legitimate but includes minor alterations or additional characters (e.g. mc-supports@mastercards.net instead of support@mastercard.com).
2. **Urgent Language or Threats**: Phishing emails often use pressure tactics, like "*Your account will be suspended*" or "*Immediate action required*," to prompt you to act quickly.
3. **Unexpected Attachments or Links**: Be cautious of any email containing attachments or links, especially if you weren’t expecting them.
4. **Unfamiliar URLs**: Hover over links to check the actual destination. If the URL looks suspicious or doesn’t match the official site, it's likely a phishing attempt.
5. **Requests for Personal Information**: Legitimate organizations won’t ask for sensitive data, like passwords or credit card numbers, via email.

Learn How to Spot Phishing Emails

5 Common Phishing Tactics:

1. **Spoofed Email Domains**: Attackers slightly alter domain names to mimic official addresses, hoping the change goes unnoticed (e.g. masterkard.com instead of mastercard.com).
2. **Impersonating Trusted Entities**: Cybercriminals often pretend to be well-known companies, financial institutions, or even coworkers to gain your trust.
3. **Credential Harvesting Websites**: Links in phishing emails direct you to fake login pages designed to steal your username and password.
4. **Attachments Containing Malware**: Phishers send malicious attachments (e.g. PDFs or ZIP files) to infect your device when opened.
5. **Business Email Compromise (BEC)**: Attackers impersonate company executives, asking employees to transfer money or share sensitive information under the guise of an urgent request.

How Do We Prevent Being Phished?

5 Helpful Tips to Detect Phishing Emails

1. **Verify the Sender’s Email Address**: Always check the sender's email carefully, especially if the request seems unusual. Look for subtle misspellings or unfamiliar domain names.
2. **Avoid Clicking on Links or Downloading Attachments**: Hover over any links to see the real URL before clicking. If something looks suspicious, do not open attachments or click links, especially in unsolicited emails.
3. **Be Cautious of Urgent or Threatening Language**: Phishing emails often create a sense of urgency or fear. If an email pressures you to act immediately (e.g., "Your account will be locked!"), take a moment to verify the source.
4. **Report Suspicious Emails**: If you suspect an email is phishing, report it to your IT department or security team. Do not forward the email to others as this could spread potential risks.
5. **Never Share Sensitive Information via Email**: Legitimate organizations will never ask you for passwords, Social Security numbers, or financial details via email. If you're unsure, contact the company directly using official channels.