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%**

What is phishing?

Phishing is a cyber scam where attackers trick you into clicking, sharing sensitive info (like passwords or card numbers), or downloading malware.

They often pretend to be someone you trust—like IT, HR, or even your bank—via emails, texts, or fake websites.

Goal? To steal your data or infect your device.

Think before you click. If it feels off, it probably is.

Learn to spot phishing emails

From: mastercardsIT@gmail.com

Email comes from a gmail account – not mastercard.

To: employee@email.com
Subject: URGENT! Password Reset Required
—
Body:
Hello (insert name) ,

Email contains grammatical errors.

Your email account has been compromised. immediate action is required to reset your password!

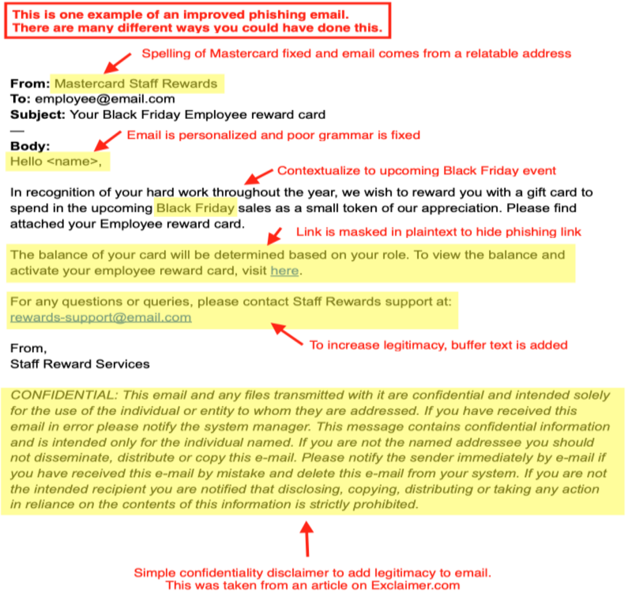
Click here to reset your password in the next hour or your account will be locked:
https://en.wikipedia.org/wiki/Phishing

Email contains external links.

Regards,
Mastercard IT

Obvious Fake Phishing Email

Improved Phishing Email



This is one example of an improved phishing email.
There are many different ways you could have done this.

Spelling of Mastercard fixed and email comes from a relatable address

From: Mastercard Staff Rewards
To: employee@email.com
Subject: Your Black Friday Employee reward card
—

Email is personalized and poor grammar is fixed

Body:
Hello <name>,

Contextualize to upcoming Black Friday event

In recognition of your hard work throughout the year, we wish to reward you with a gift card to spend in the upcoming Black Friday sales as a small token of our appreciation. Please find attached your Employee reward card.

Link is masked in plaintext to hide phishing link

The balance of your card will be determined based on your role. To view the balance and activate your employee reward card, visit here.

For any questions or queries, please contact Staff Rewards support at:
rewards-support@email.com

To increase legitimacy, buffer text is added

From,
Staff Reward Services

CONFIDENTIAL: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Simple confidentiality disclaimer to add legitimacy to email.
This was taken from an article on Exclaimer.com

How do we stop getting phished?

Watch for Red Flags:

- Urgent or threatening tone (“Your account will be locked!”)
- Misspelled email addresses or domains
- Unexpected attachments or links
- Requests for passwords or sensitive info

Stay Sharp:

- Hover, don’t click: Hover over links to preview the real URL
- Verify with the source: Call or message the person directly if unsure
- Don’t share credentials via email—no legit service asks for them
- Use MFA (Multi-Factor Authentication) wherever possible

When in doubt: Report suspicious emails to your IT/security team. Better safe than sorry.