



**Familiarize yourself with phishing attacks**  
**HR & marketing teams**



## What is phishing ?

- Phishing is the act of pretending to be someone, or something, to get information not usually available.
- People can be gullible and curious and click on things they shouldn't - often a link will direct to a fake login page in an attempt to steal credentials.

# Learn to spot phishing emails

securityMETRICS

## 7 Signs of a Phishing Email

Generic greeting or no greeting at all

Request for personal information over email

Buttons with hyperlinks to unfamiliar webpages

Unsolicited attachments

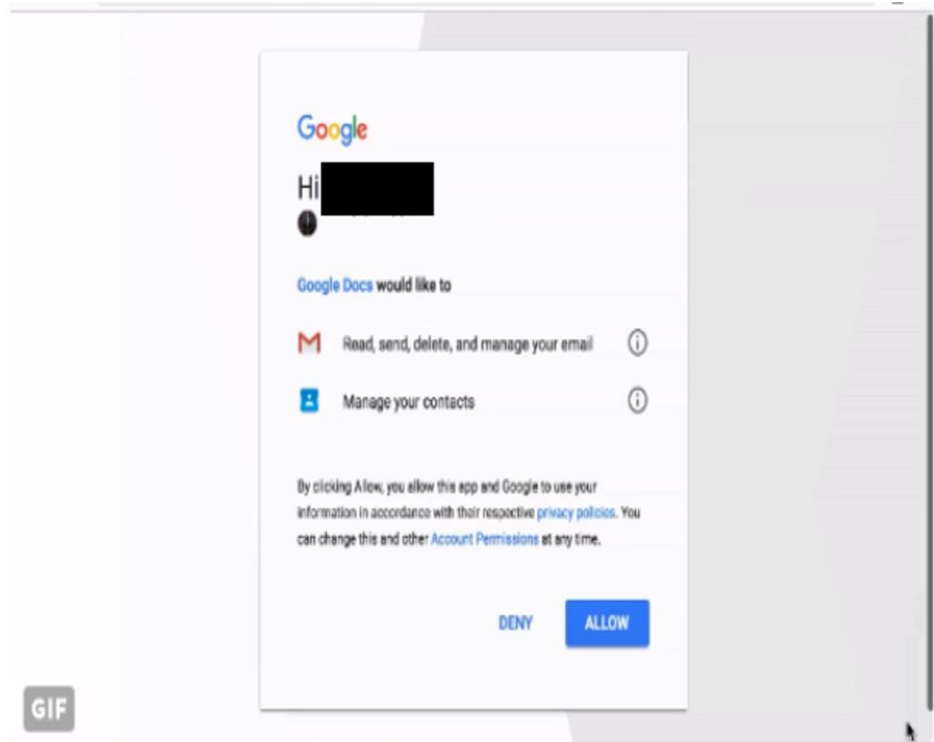
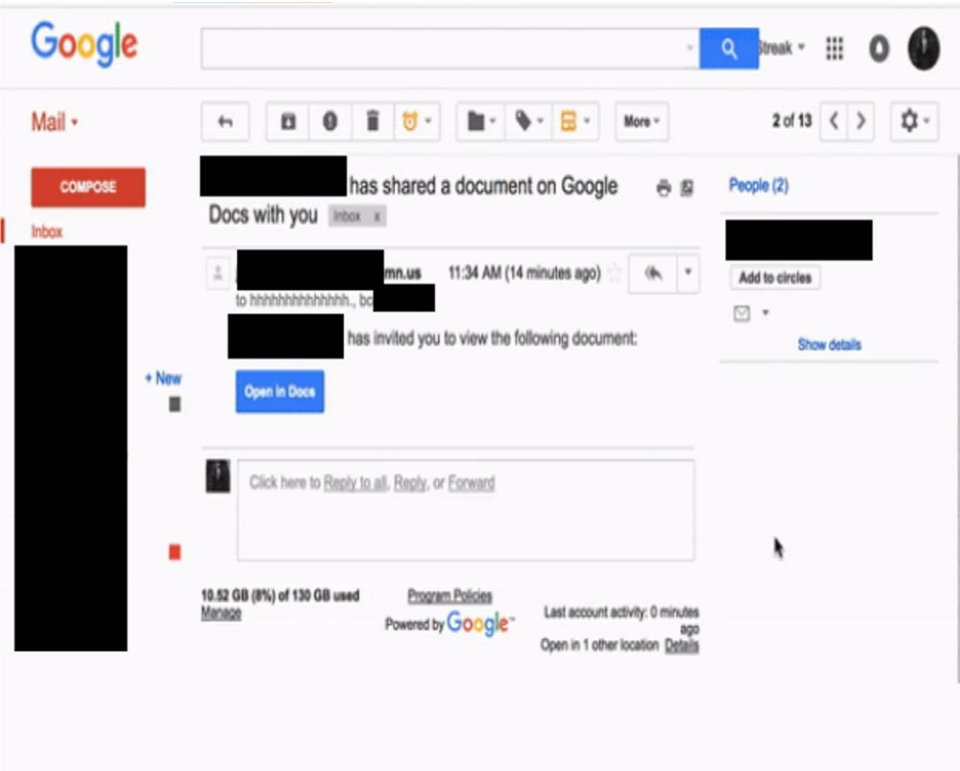


"From" email address is not official

Hover your mouse to reveal misleading URL hyperlinks

Spelling and grammar mistakes

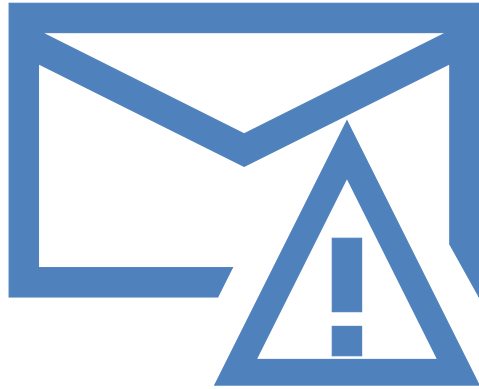
Always be cautious - they can be as sophisticated as this...





## How do we stop getting phished?

- If it's too good to be true it probably is.
- Always be suspicious. Better safe than sorry.
- Double check with other employees on a separate communication channel.
- For example, in the rewards card phishing email, you could confirm by calling Rewards Services about the employee card being sent out before clicking on the email.



## Remember to always:

- Check the URL of the website is correct.
- Always be suspicious of any email requesting personal information.
- Use a password manager to securely store unique passwords for each website.
- Use a secondary/side channel to double check when someone requests you to do something.