Familiarize yourself with phishing attacks

HR & marketing teams

What is phishing?

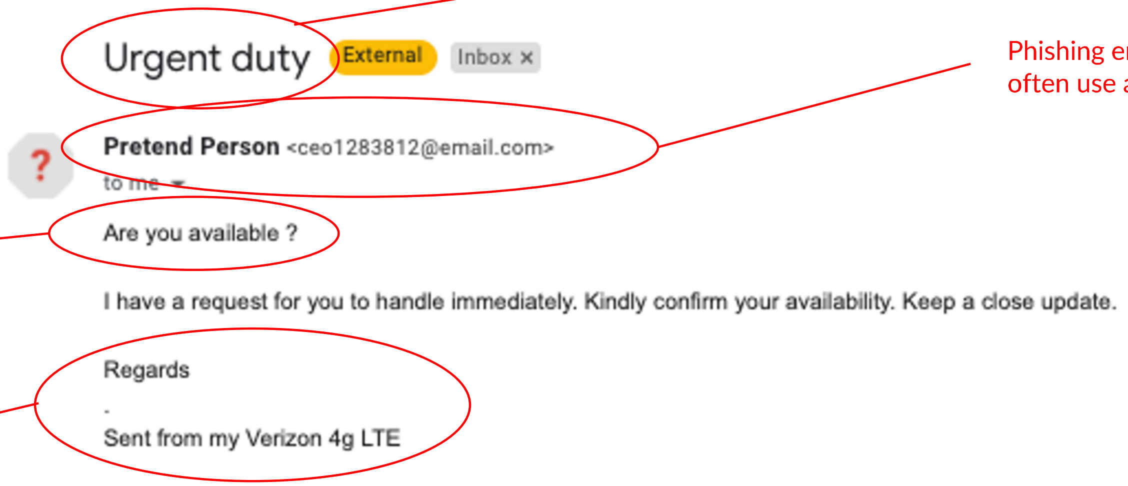
Phishing is the act of pretending to be someone, or something, to get information not usually available.

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

Email is requesting an action with urgency

Phishing emails will pretend to be someone. However, will often use an incorrect email address



Urgent duty

Pretend Person <ceo1283812@email.com>

to me

Are you available ?

I have a request for you to handle immediately. Kindly confirm your availability. Keep a close update.

Regards

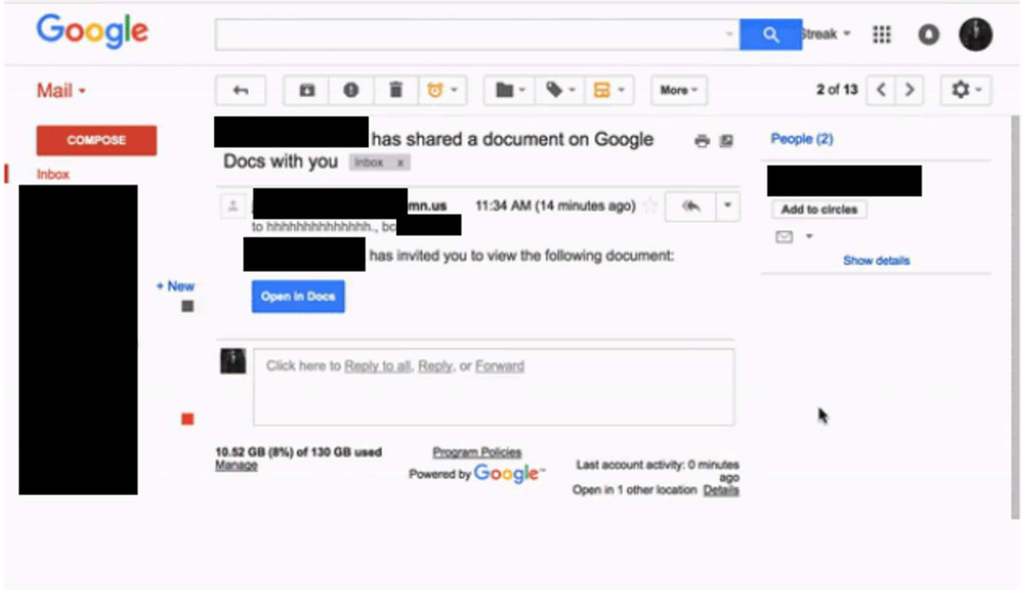
-

Sent from my Verizon 4g LTE

No first name personalization & poor grammar

No sign-off/ signature

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



[redacted] has shared a document on Google Docs with you Inbox x

[redacted] mn.us 11:34 AM (14 minutes ago)

to hhhhhhhhhhhhhh., bc [redacted]

[redacted] has invited you to view the following document:

Click here to Reply to all, Reply, or Forward

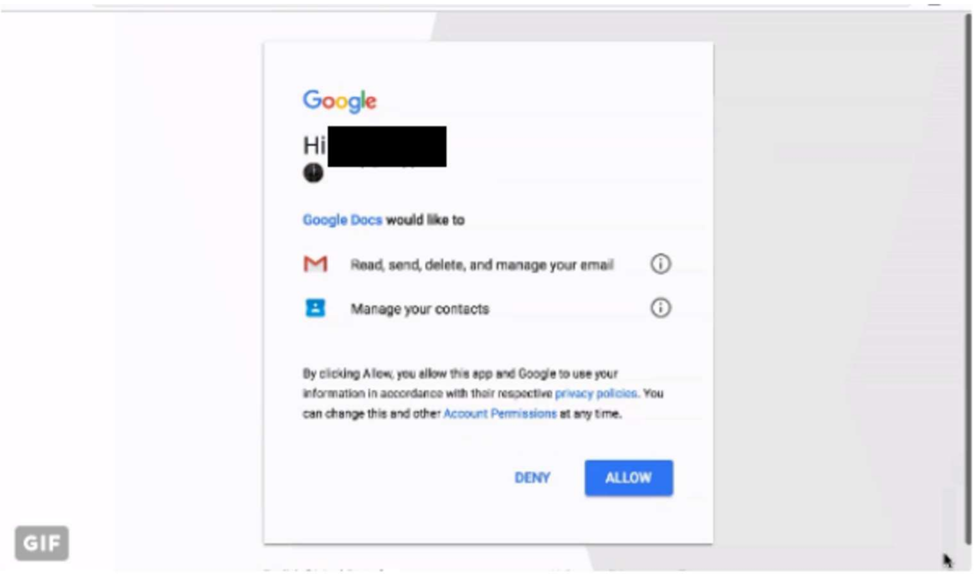
10.52 GB (8%) of 130 GB used
Manage

Program Policies
Powered by Google

Last account activity: 0 minutes ago
Open in 1 other location Details

[redacted]

[redacted]



Hi [redacted]

Google Docs would like to

Read, send, delete, and manage your email

Manage your contacts

By clicking Allow, you allow this app and Google to use your information in accordance with their respective privacy policies. You can change this and other Account Permissions at any time.

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.