



Don't Get Hooked: Phishing Awareness Training

Stay Alert. Stay Safe.



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.

Real-Life Phishing Examples

Learn to spot phishing emails

Urgent duty

External

Inbox x

Email is requesting an action with urgency

Pretend Person <ceo1283812@email.com>

to me

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

Are you available ?

No first name personalization & poor grammar

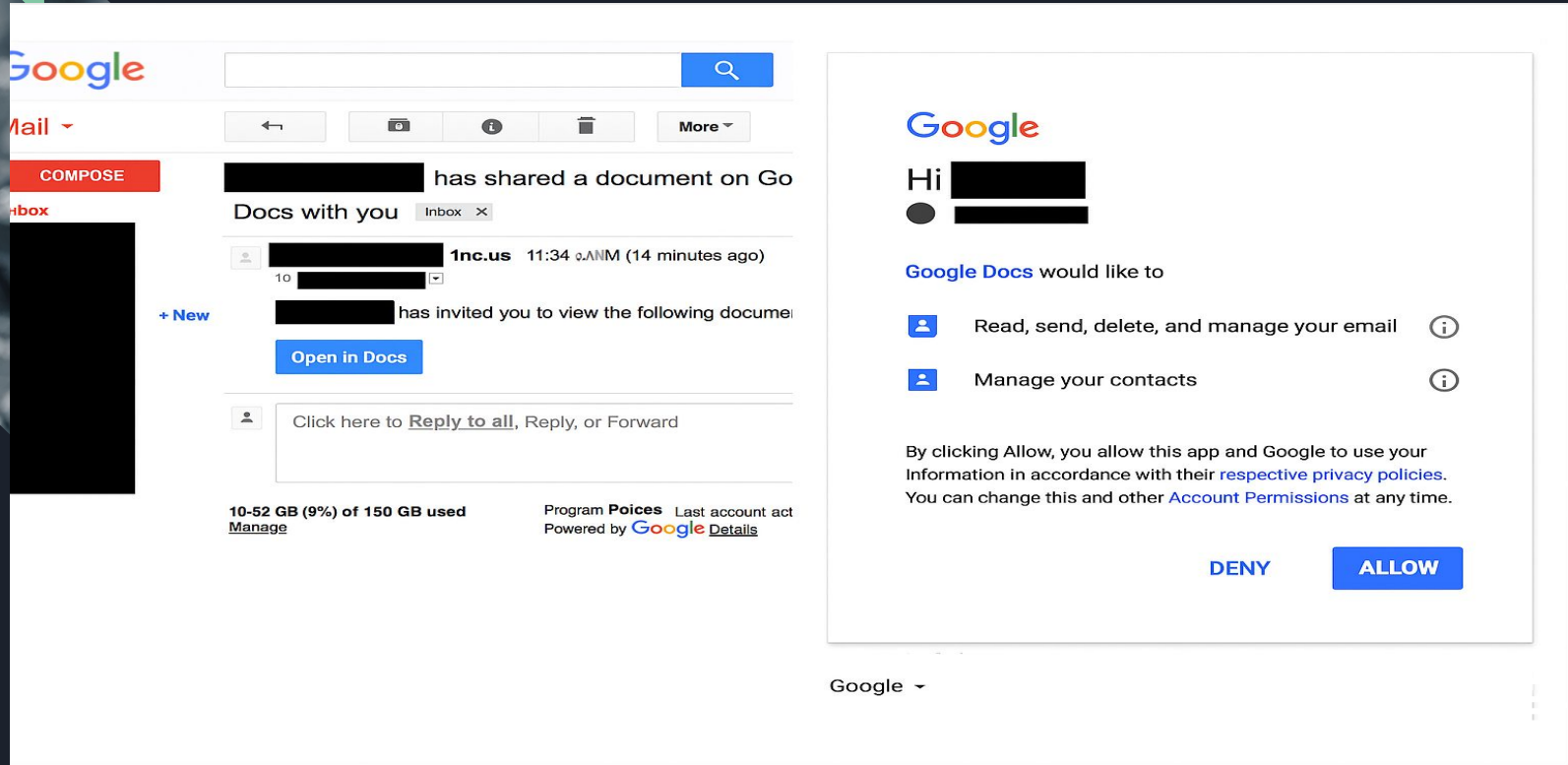
I have a request for you to handle immediately. Kindly confirm your availability. Keep a close update.

Regards

Sent from my Verizon 4g LTE

No sign-off/ signature

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



Fake reward card email

From: AppleID-291869@itunes.apple.com

Date: 3 June 2016 at 08:38:44 BST

Subject: iTunes 50\$ Gift Card Received

FAKE
← **Suspicious**

Dear Apple customer,

CONGRATULATIONS!

Too good to be true

Because you are a loyal customer we have determined that you are eligible to receive a 50\$ iTunes Gift Card reward.

We ask you to take part in our quick and easy survey to receive your 50\$ iTunes Gift card.

[Click here to start the Apple Gift Card Reward Survey](#) ← **Unusual link**

We will use the resulting information to better serve all of our customers.

Copyright © 2016 Apple Inc. All rights reserved.

Fake login pages

Fake Login Page

firebasestorage.googleapis.com/v0/b/ncsu-edu.appspot.com/o/ncsu.edu.
Google Network Scanning...

NC STATE

Shibboleth Login Service



Unity ID Login

NC State Students/Faculty/Staff

Unity ID *

Password *

Show password ☐

LOG IN →

Shibboleth Login Page

https://shib.ncsu.edu/idp/profile/SAML2/Redire
S3cur1ty OSINT splunk personal

NC STATE

Shibboleth Login :



Unity ID Login

NC State Students/Faculty/Staff

Unity ID *

Password *

Show password ☐

LOG IN →

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





Red Flags to Watch

1. Urgent action required
2. Suspicious email address
3. No personalization / poor grammar
4. Missing official signature



How to Stay Safe

- ✓ Verify with coworkers via other channels
- ✓ Check the sender's email carefully
- ✓ Never click on suspicious links
- ✓ Use a password manager and 2FA



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



Phishing Awareness Quiz:

<https://forms.gle/zo4oQticQSgP6UqM7>