Don’t Get Hooked: Phishing Awareness Training

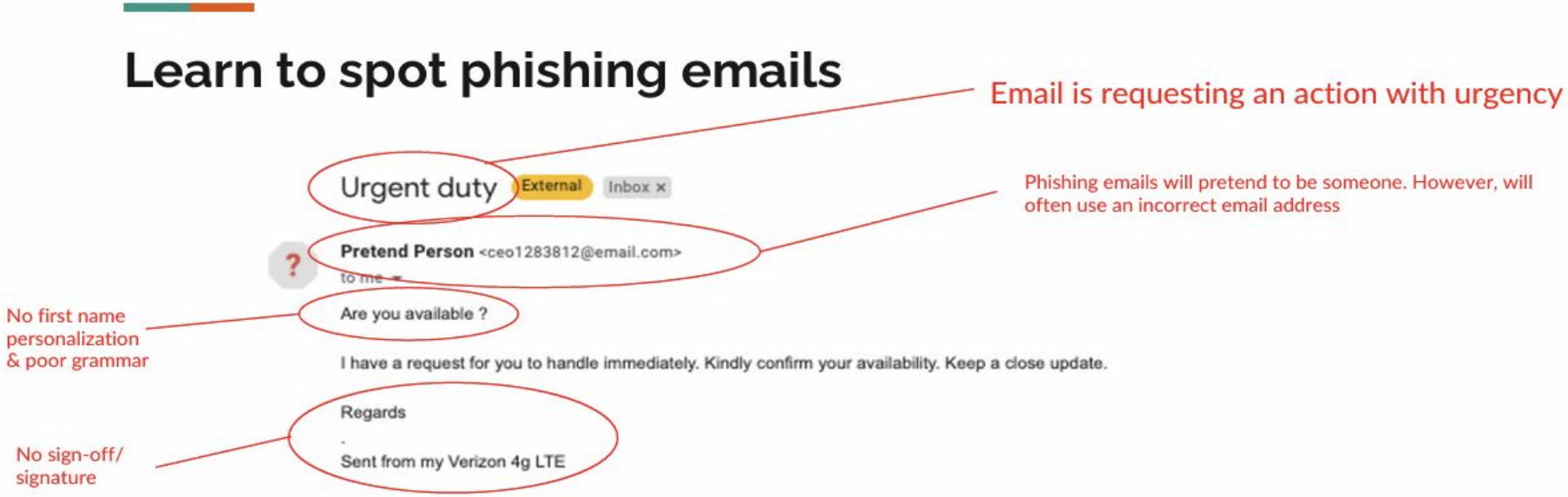
Stay Alert. Stay Safe.

What is phishing?

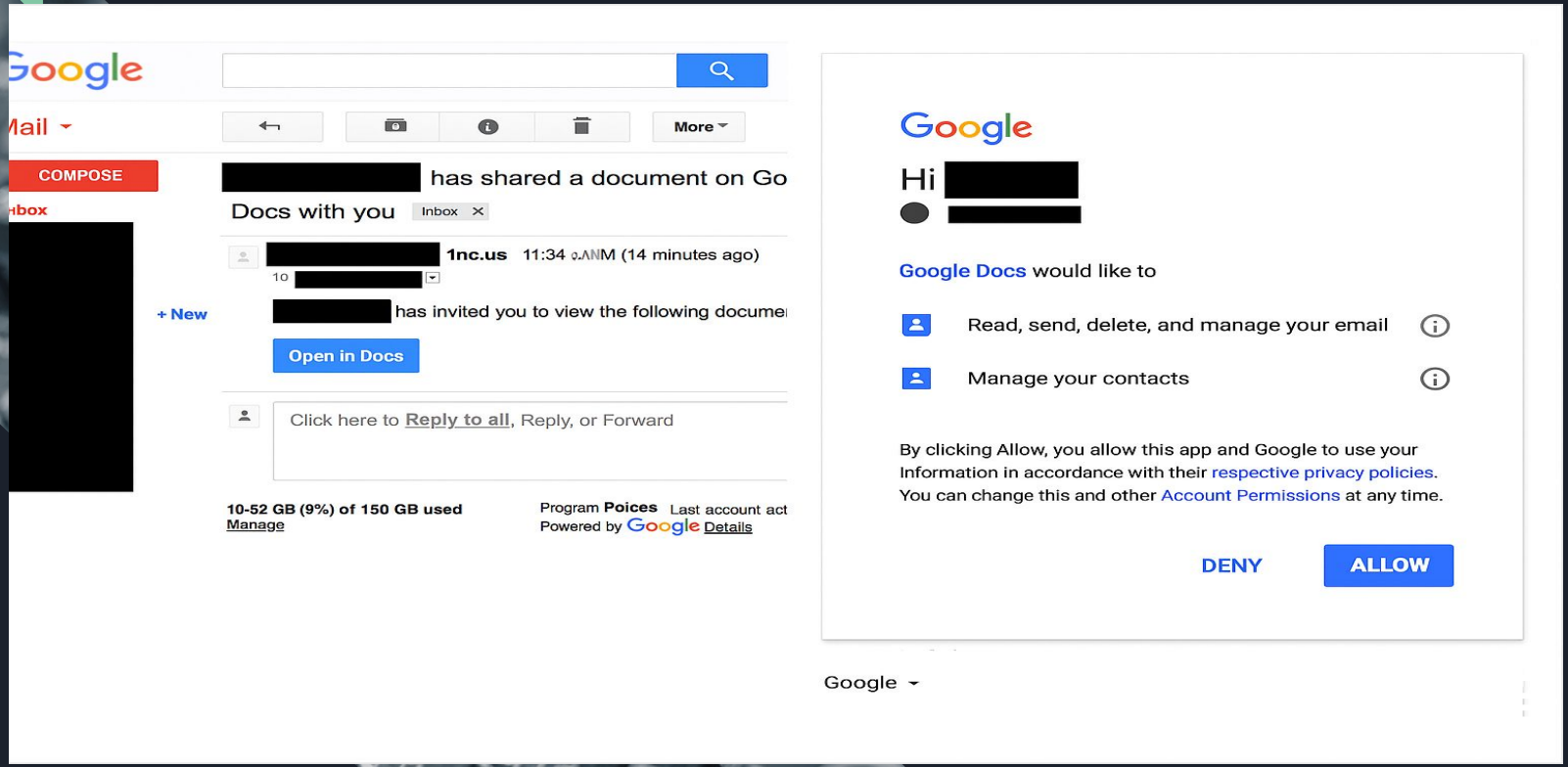
Phishing is the act of pretending to be someone, or something, to get information not usually available.

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.

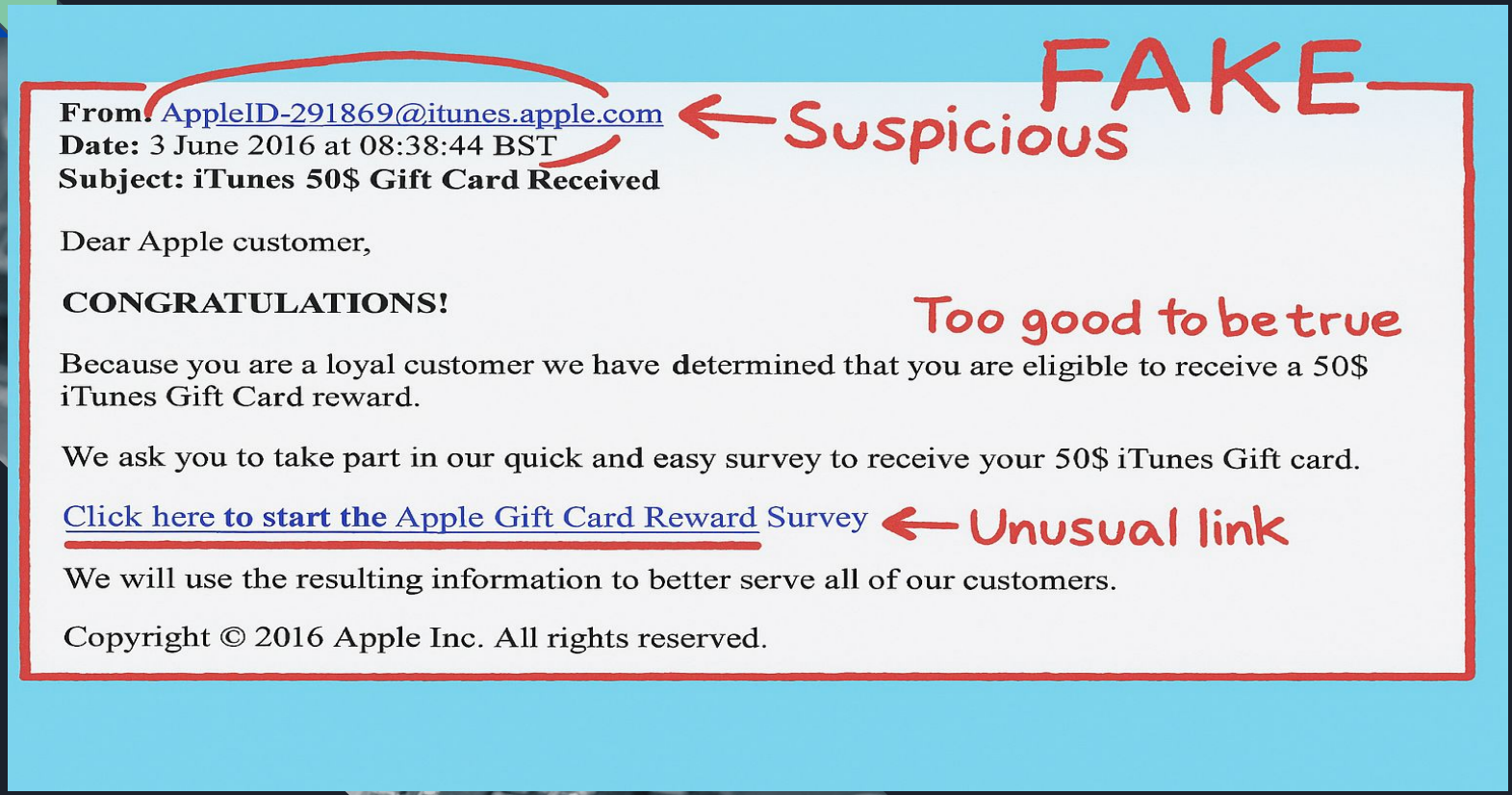
Real-Life Phishing Examples



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



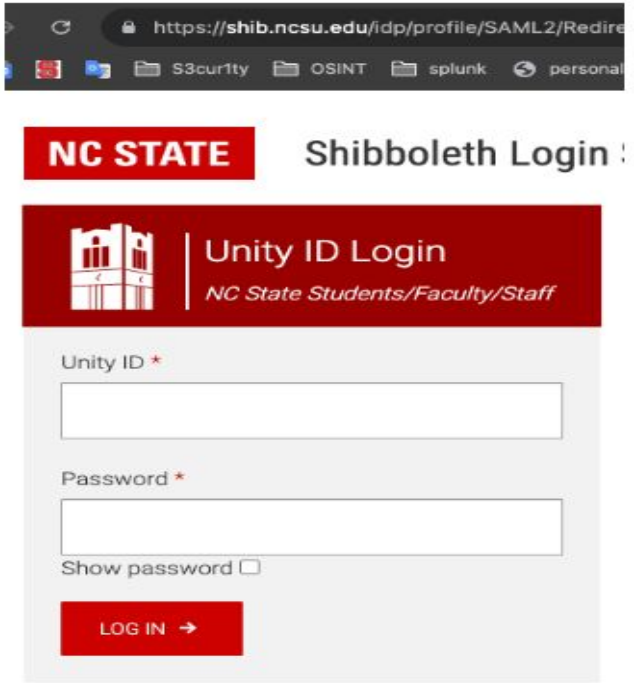
Fake reward card email



Fake login pages

Fake Login Page

Shibboleth Login Page



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