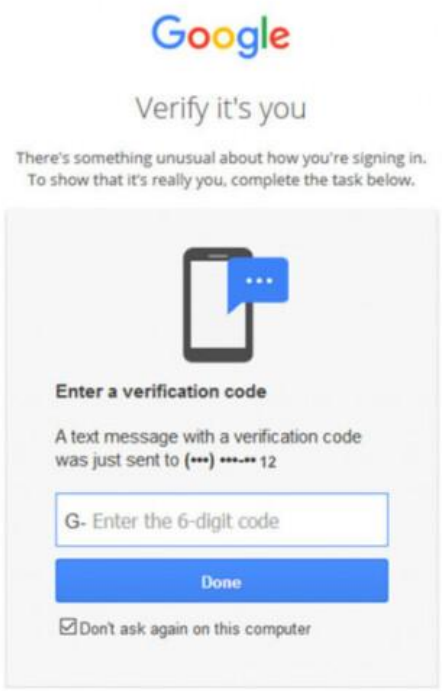
Tip 5: Set up 2 Factor Authentication(2FA)



Two-Factor Authentication (2FA) adds an extra layer of security to your online accounts. After entering your password, a unique verification code is sent to your mobile device, providing an additional step to access your accounts. The protection is worth the hassle!

Contributors:
T452 & Isaac

Resources & Credits:
Images - google's phishing quiz
Quiz QR Code:

Test your knowledge with Google's phishing quiz!

Online Safety Tips

By: T452

Here are some online safety tips to keep safe from scammers!

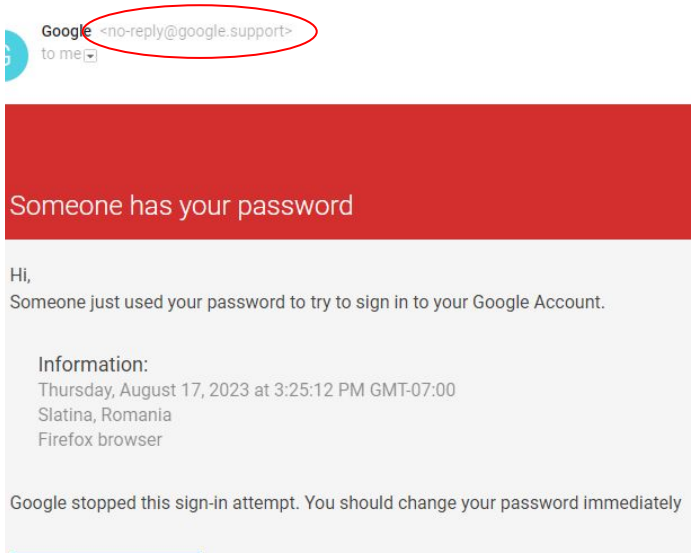
Tip 1:
Use a strong unique password

Weak: bob
Medium: bob123
Strong: #Bob2212!

To create a strong password, follow the following tips:

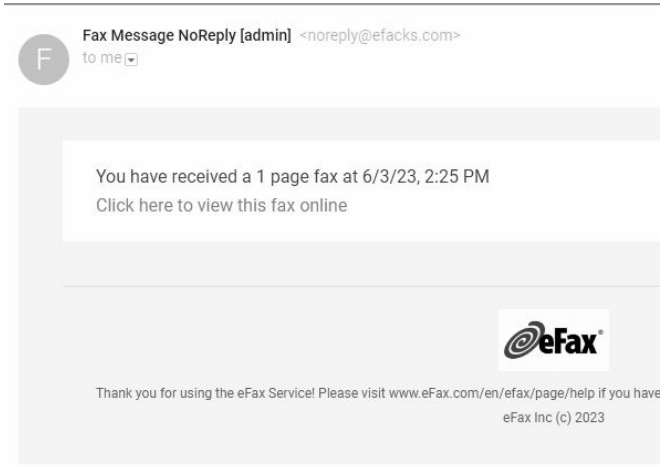
1. At least one capitalized letter
2. At least one special character
3. At least one #
4. More than 8 characters

Tip 2: Be careful of emails that ask for personal information



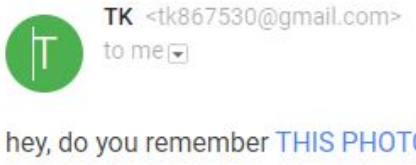
As you can see in the email above, Google is saying that your password is compromised. However, a Google search shows that the email address is not actually google support and is actually a stranger asking for your password.

Tip 3: Verify email addresses if they claim they are from an official organization



In the email above, you can see the email address is noreply@efacks.com when the company is efax. The emails aren't the same! You can verify official email addresses by searching online.

Tip 4: If anyone claims to be someone you know, check with them in person



In this email, someone is pretending to be your friend and is asking you to click on the photo. This photo is actually a virus if you look at the link it leads you to.

Note: Whenever you see something in the email that is blue font, hover your mouse over it to see where the photo leads you to.