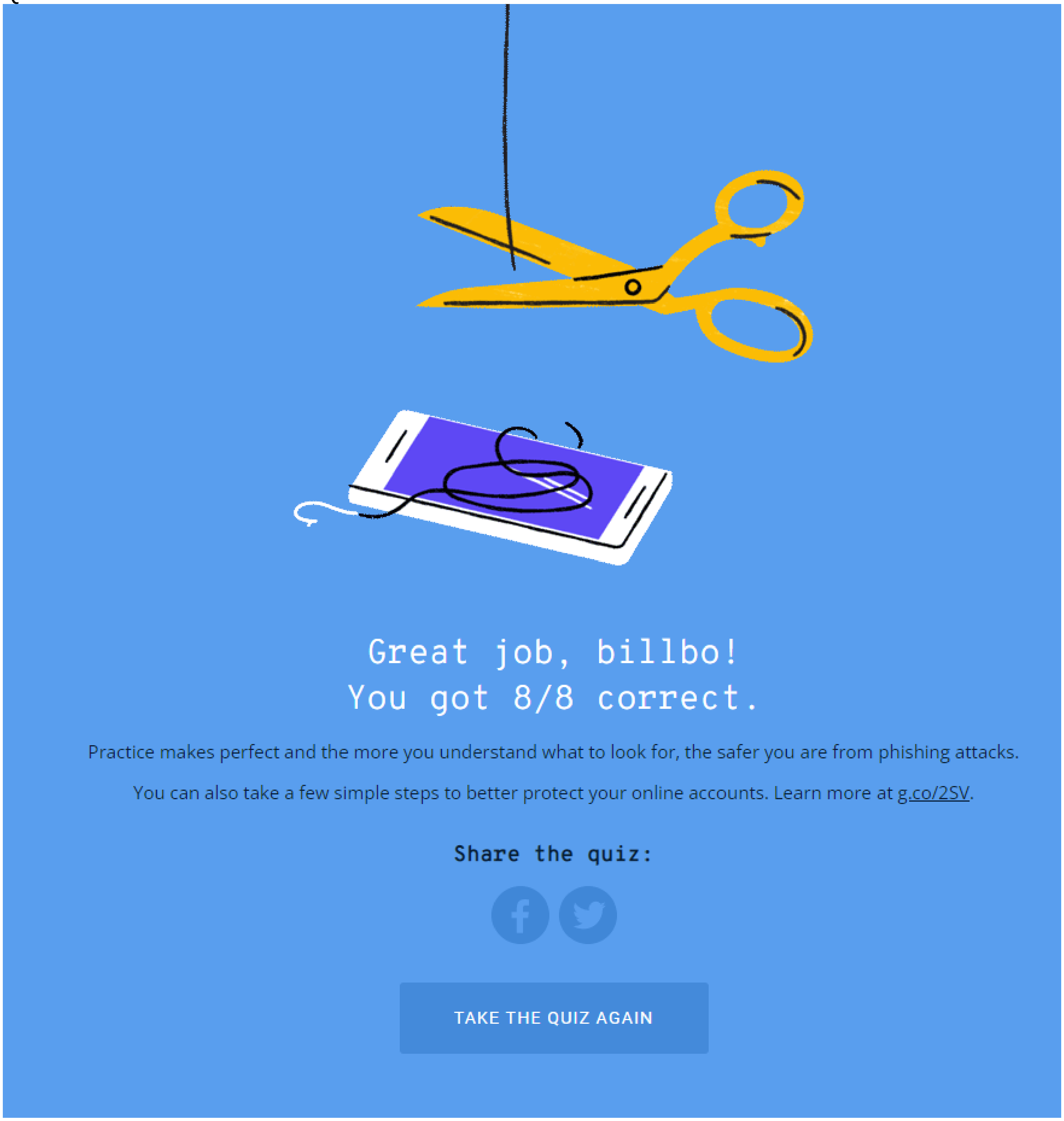
Luke Hauersperger
CIT 41500
Lab 06: Phishing Emails

ABSTRACT:

Throughout this lab I worked to identify multiple spam emails through a variety of games. After this I used the skills and information that I gained from the games, and viewed some of my own emails. I found a few emails that could have lead to viruses, by checking what the links went to, where they came from, and what their response email is. After this I wrote a spam email of my own and sent it out, so I could see phishing emails from the attackers point of view. This will help me in the future, as I will be able to understand what to look for while I am on the defensive side.

T1:
Quiz `



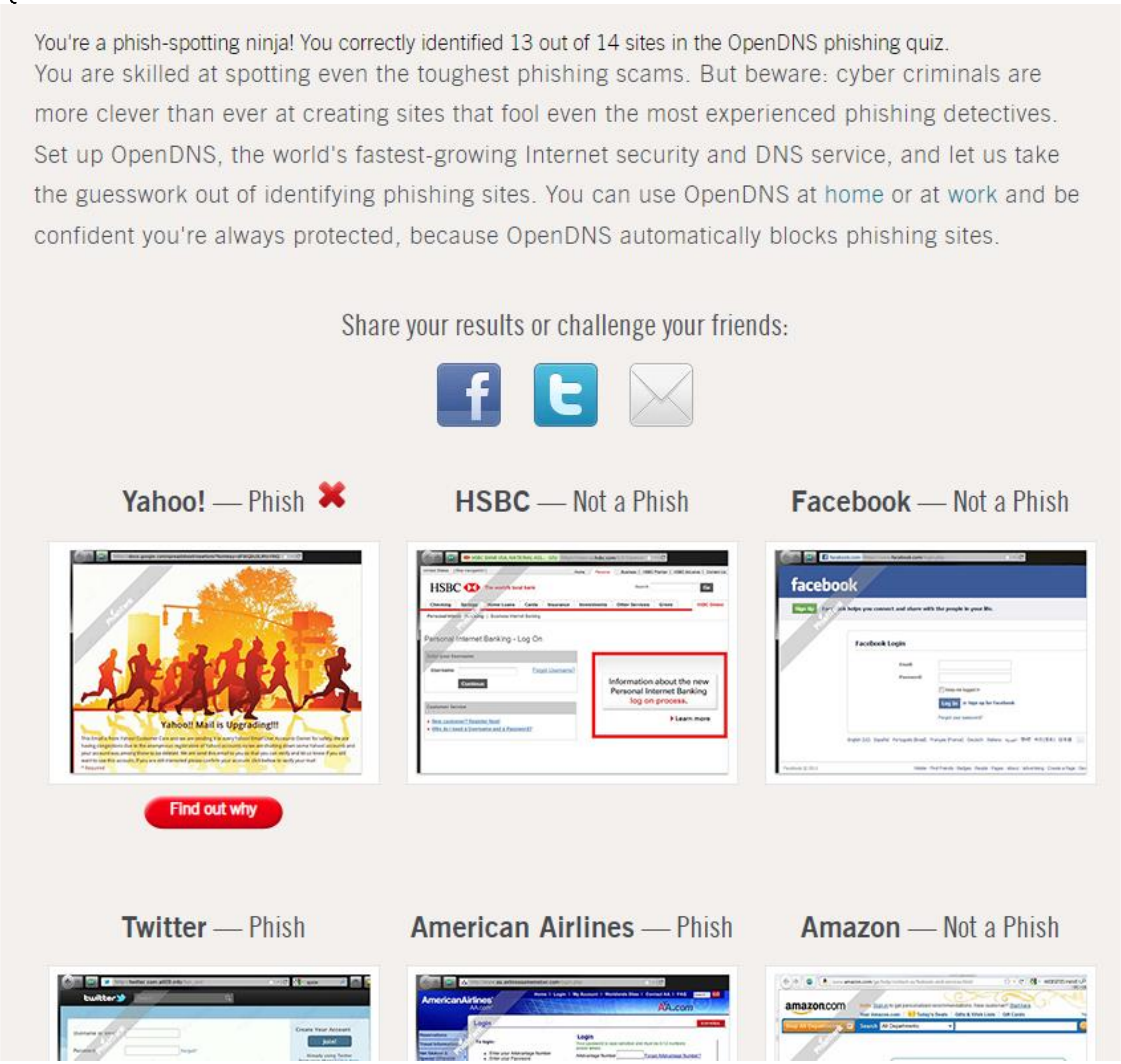
Great job, billbo!
You got 8/8 correct.

Practice makes perfect and the more you understand what to look for, the safer you are from phishing attacks.

You can also take a few simple steps to better protect your online accounts. Learn more at g.co/2SV.

Share the quiz:

Quiz 2



You're a phish-spotting ninja! You correctly identified 13 out of 14 sites in the OpenDNS phishing quiz.

You are skilled at spotting even the toughest phishing scams. But beware: cyber criminals are more clever than ever at creating sites that fool even the most experienced phishing detectives. Set up OpenDNS, the world's fastest-growing Internet security and DNS service, and let us take the guesswork out of identifying phishing sites. You can use OpenDNS at home or at work and be confident you're always protected, because OpenDNS automatically blocks phishing sites.

Share your results or challenge your friends:

Yahoo! — Phish ✗

HSBC — Not a Phish

Facebook — Not a Phish

Yahoo!! Mail is Upgrading!!!
Find out why
HSBC
Personal Internet Banking - Log On
Information about the new Personal Internet Banking log on process.
Learn more
facebook
Facebook Login

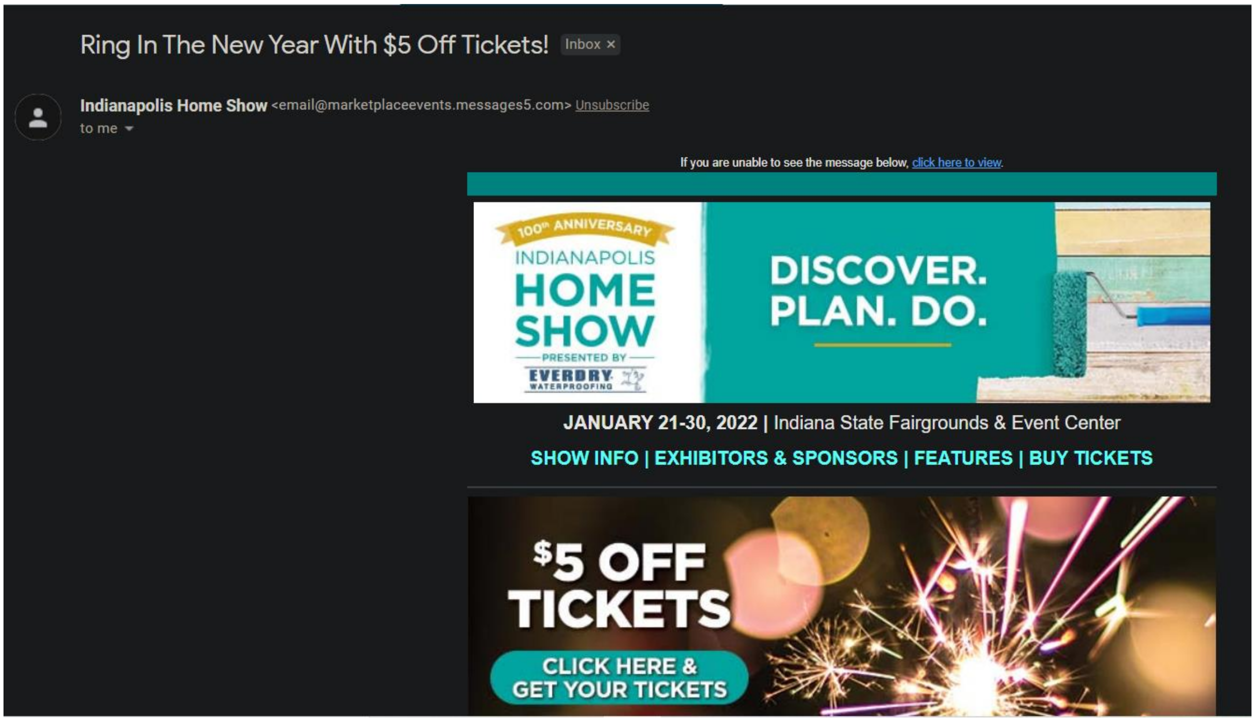
Twitter — Phish

American Airlines — Phish

Amazon — Not a Phish

T2:

First Email



Ring In The New Year With $5 Off Tickets! Inbox ×

Indianapolis Home Show <email@marketplaceevents.messages5.com> Unsubscribe

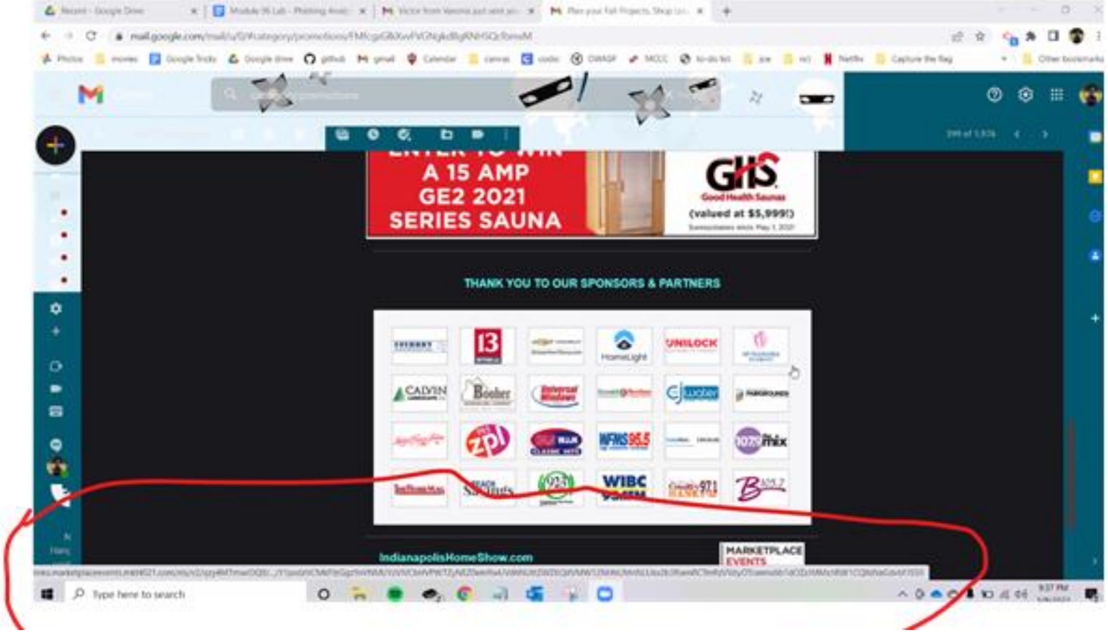
to me

If you are unable to see the message below, click here to view.

JANUARY 21-30, 2022 | Indiana State Fairgrounds & Event Center

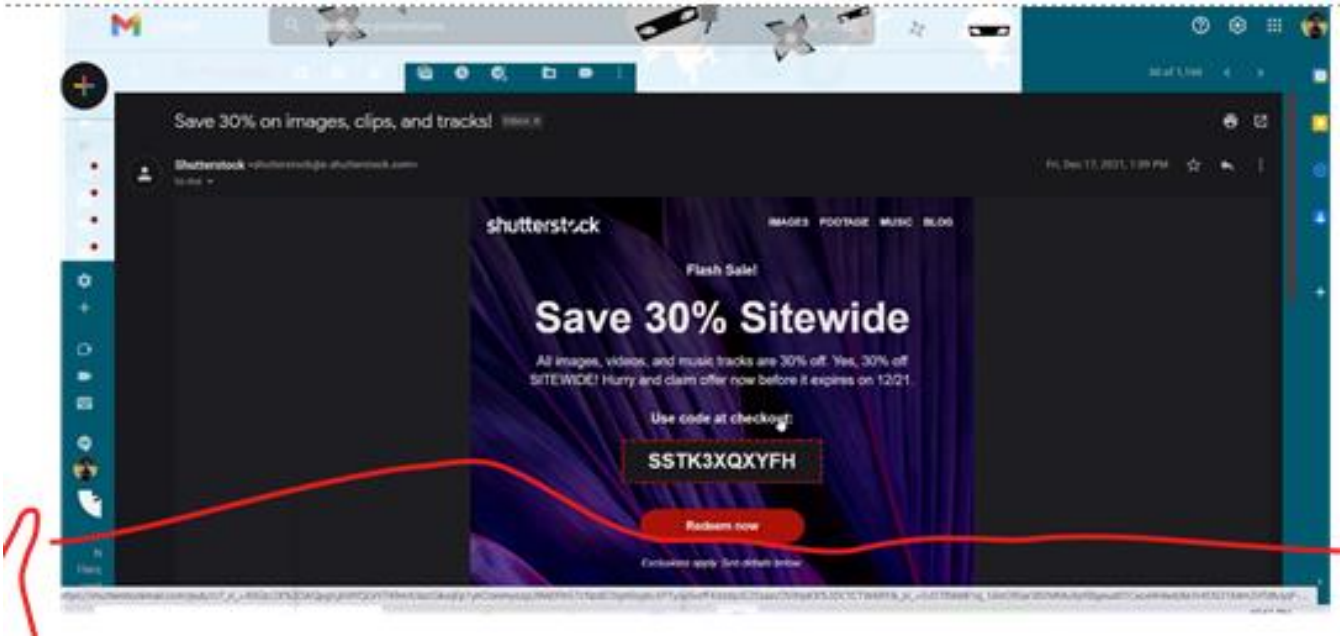
SHOW INFO | EXHIBITORS & SPONSORS | FEATURES | BUY TICKETS

1. This message comes from a different domain than



2. They have a link to their sponsors, but it goes to a really long link.
3. They have a link to their Facebook below that goes to the same site.

Second Email



Save 30% on images, clips, and tracks!

Shutterstock

shutterstock

Flash Sale!

Save 30% Sitewide

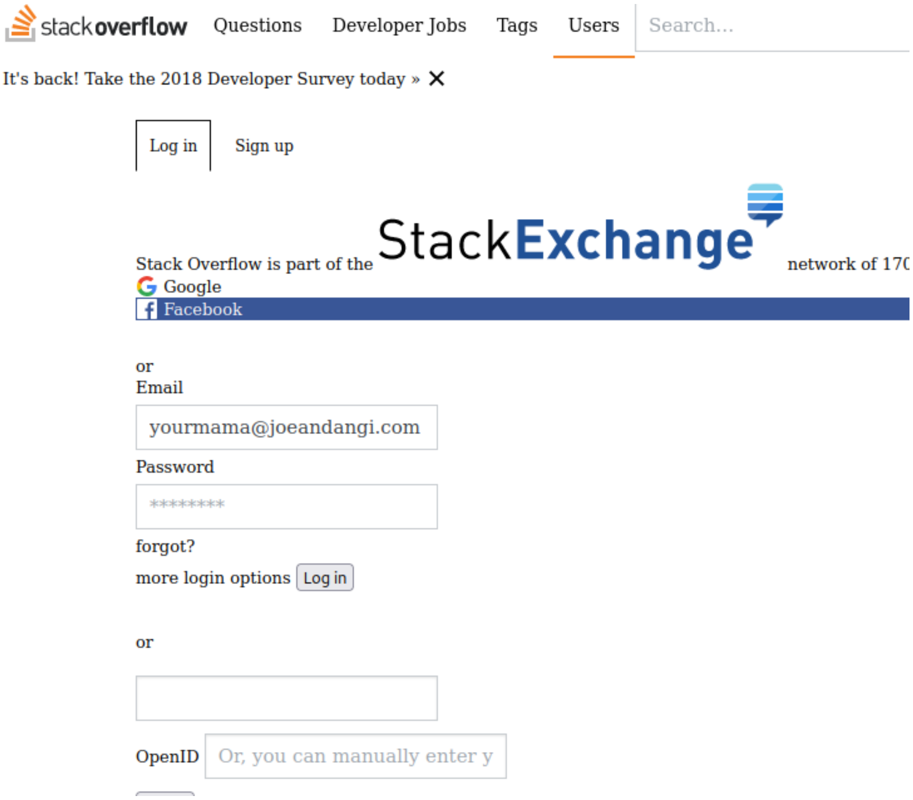
All images, videos, and music tracks are 30% off. Yes, 30% off SITEWIDE! Hurry and claim offer now before it expires on 12/21.

Use code at checkout:

SSTK3XQXYFH

1. The link goes to a website called shuttershockmail.com which does not exist.
2. It wants you to go to an external link.
3. The reply email is different than where it was sent from.

T3:



It's back! Take the 2018 Developer Survey today » ✕

Stack Overflow is part of the StackExchange network of 17(

or

Email

yourmama@joeandangi.com

Password

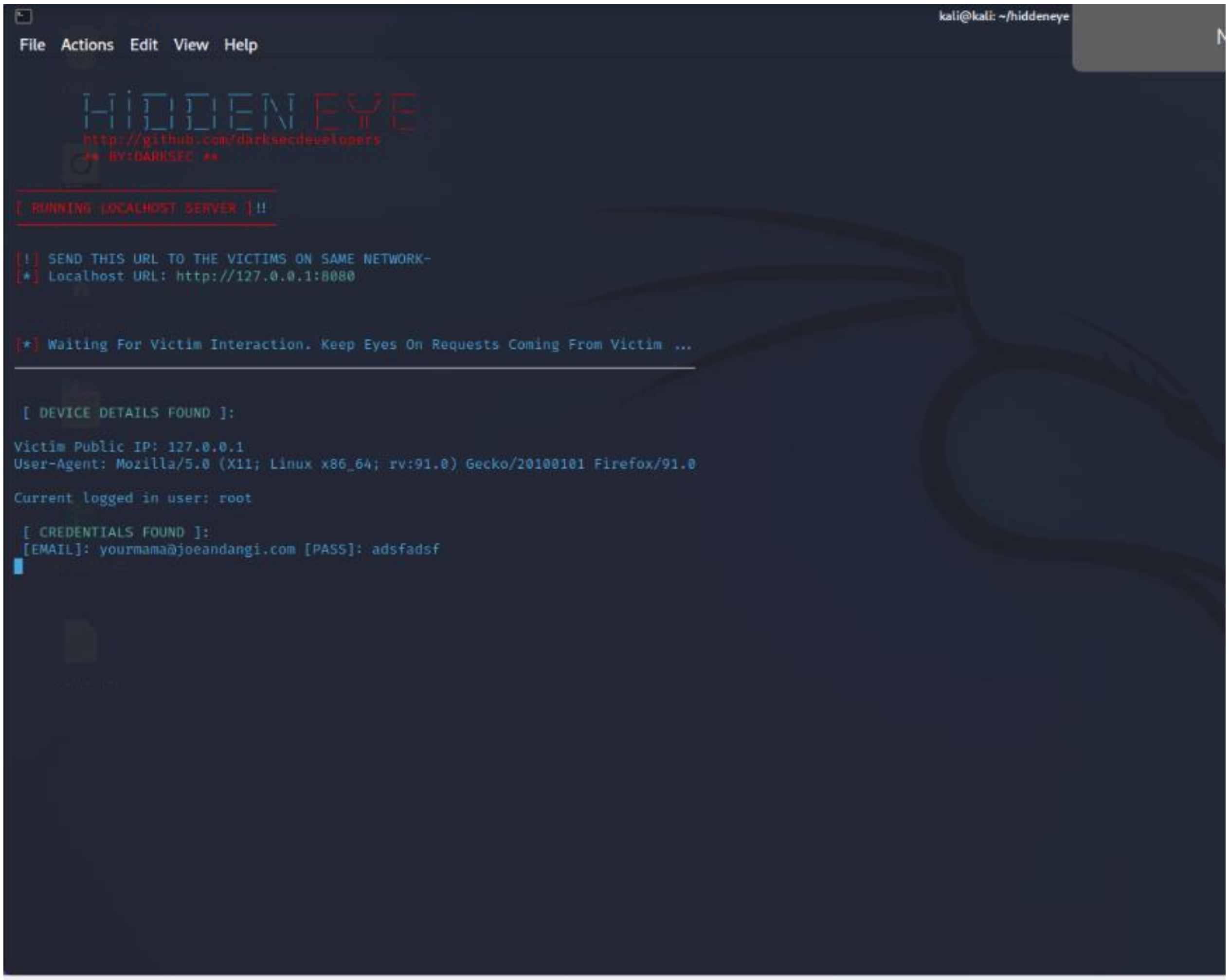
****

forgot?

more login options

or

OpenID Or, you can manually enter y



```
HIDDEN EYE
http://github.com/darksecdevelopers
** BY:DARKSEC **

[ RUNNING LOCALHOST SERVER ]!!

[!] SEND THIS URL TO THE VICTIMS ON SAME NETWORK-
[*] Localhost URL: http://127.0.0.1:8080


[*] Waiting For Victim Interaction. Keep Eyes On Requests Coming From Victim ...


 [ DEVICE DETAILS FOUND ]:

Victim Public IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

Current logged in user: root

 [ CREDENTIALS FOUND ]:
 [EMAIL]: yourmama@joeandangi.com [PASS]: adsfadsf
```

In this section of the lab, I created a phishing email that led to a fake link that was meant to look like Stack Overflow. I used HIDDENEYE on my Kali Linux virtual machine to set up this fake website address. After setting up the link, I went straight to the IP address and typed in my information on the login screen. This information showed up on HIDDENEYE in plain text. It even showed what was submitted as the Email and what was submitted as the password separately. I believe that this link looked somewhat legitimate and if it was set to a website that I used, and if it was updated more recent than 2018, I might have actually fallen for it. I don't click on links through my emails which would've prevented me from falling for this, but if I did it would've been hard to avoid.

TQ : Review/Questions

Research and discuss some mitigations an organization can take to protect people from Business Email Compromise?

- Educate users to avoid links inside of emails. Instruct them to go directly to websites that they need to access instead of using links.
- Have users avoid going to emails that they were not expecting
- Make sure that users never follow links or fill out the information on emails asking for login information
- Set spam filters to avoid phishing attacks
- Set up multi-factor authentication in case threat actors try to log in through an employees account

How can DMARC, DKIM, and SPF help protect against spoofing and phishing?

- SPF decides which domains and servers are allowed to send emails, DKIM adds a digital signature to outgoing messages, and DMARC tells servers what to do if they don't pass SPF and DKIM.

What kind of file extensions do you think might not be good to be sent or received via email? (think email filtering)

- Bash scripts that has a .sh file extension
- Screen saver files with a .scr file extension
- Virtual basic script with a .vbs file extension

Recommendations & Conclusions:

Throughout this lab I viewed phishing emails form multiple different point of views. I checked my email for phishing emails, I played games that taught me how to find phishing emails, and I created a phishing email of my own. I really enjoyed identifying phishing emails and sending some phishing emails, but I didn't like having to search through my own emails, because I have 1,000s of emails and very few are spam/phishing emails.