Lab C

Brandon Trinkle

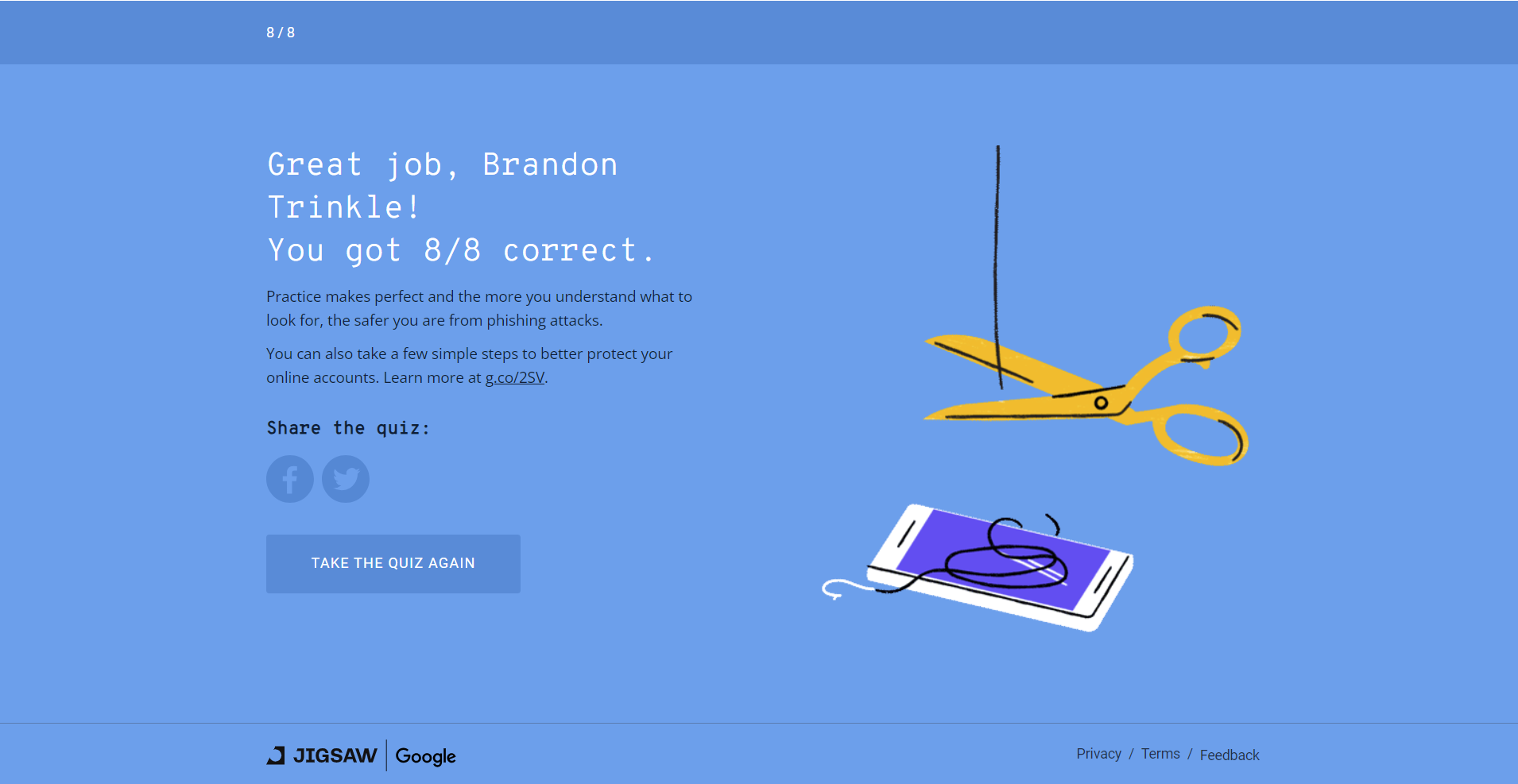
Arizona State University

Course Number: IFT 202

Professor Gary Grindle

Jan 27, 2024

Part 1

Task 1  


Part 2

Question 1. Under the Headers Found section of the results, what is the Header Value for the **Authentication-Results** Header Name?

Answer: spf=fail (sender IP is 148.163.148.157)

Question 2. Under the Headers Found section of the results, what is the Header Value for the **Received-SPF** Header Name?

Answer: Fail (protection.outlook.com: domain of microsoft.com

Question 3. Under the Headers Found section of the results, what is the Header Value for the **To** Header Name?

Answer: Under the headers found, there is no To block. However, reading through the output, this email was sent to eric.bishop@asu.edu.

A white and grey striped background

Description automatically generated with medium confidence

A screenshot of a computer program

Description automatically generated

Question 4. Under the Headers Found section of the results, what is the Header Value for the **From** Header Name?

Answer: Under header there is no from block. However, it was from - "Microsoft Security Center".

A screenshot of a computer program

Description automatically generated

Question 5. Under the Headers Found section of the results, what is the Header Value for the **Reply-To** Header Name?

Answer: There is no Reply-to block in the headers found section, however this is the Reply-to security@microsoft.com.

A screenshot of a computer code

Description automatically generated

Question 6. Under the Headers Found section of the results, what is the Header Value for the **Return-Path** Header Name?

Answer: There is no Return-Path block in the headers found section, however this is the Return-Path - security@microsoft.com



Question 7. Under the Headers Found section of the results, what is the Header Value for the **X-Mailer** Header Name?

Answer: There is no X-Mailer in the Headers found section, however the X-mailer is - Apple Mail

A screenshot of a computer code

Description automatically generated

Question 8. Under the Headers Found section of the results, what is the Header Value for the **Message-Id** Header Name?

Answer: There is no Message-ID in the headers found section, however the Message-id is - <20220929014213.576E060956D@emkei.cz>

A screenshot of a computer code

Description automatically generated

Question 9. Under the Received Header section of the results, look through the raw header and email contents. What URL do the links found in the email message point to?

Answer: There are multiple URL’s found in this email. Most of them are from outlook.com or Microsoft.com. There is also an AWS URL in this message, which hosts Amazon could instance EC2. There was one particular URL that seemed suspicious, pphosted.com. After researching this I found out that it is the domain of a cybersecurity service named ProofPoint essentials.

Question 9. Do you think this is a legitimate email or a phishing email?

Answer: I think this is a legitimate email.

Question 9. Justify your answer to the question above with as much detail and reasons as you are able to. Can you find out where the mail was sent from?

Answer: What is happening here is that this email is going through a series of hops. The first 5 hops are through Microsoft’s security analysis. These all pass, and even the first hop where it starts, mentions its not blacklisted. Where it is failing SPF is when ProofPoint essentials reviews it, before its reviewed by SPF. The handshake between ProofPoint and SPF is where it fails SPF check. Within the output it shows the failing IP address is assigned to ProofPoint. The corrective action would be to add ProofPoint to ASU’s recognized domains.

This is the original sender - pps.filterd 127.0.0.1