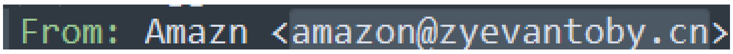
Blue Team Labs Online: Phishing Analysis 2

The following writeup is for Phishing Analysis 2 on Blue Team Labs Online, it's an easy lab that involves analysing a raw phishing email through using tools like a text editor, Mozilla Thunderbird, and more. Similarly to Phishing Analysis 1, this was a super easy challenge that requires little knowledge of email headers.

Scenario: Put your phishing analysis skills to the test by triaging and collecting information about a recent phishing campaign.

What is the sending email address?

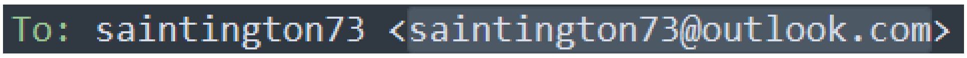
Due to the easy nature of these sorts of questions, I am simply going to provide a screenshot of the answer as they can all be found within the basic email headers:



```
From: Amazn <amazon@zyevantoby.cn>
```

Answer: amazon@zyevantoby.cn

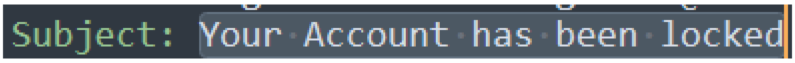
What is the recipient email address?



```
To: saintington73 <saintington73@outlook.com>
```

Answer: saintington73@outlook.com

What is the subject line of the email?



```
Subject: Your Account has been locked
```

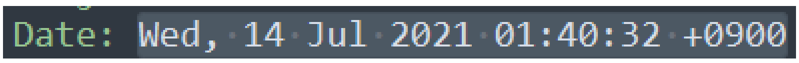
Answer: Your Account has been locked

What company is the attacker trying to imitate?

Based on the from address, it is pretty clear that the attacker is trying to imitate Amazon.

Answer: Amazon

What is the date and time the email was sent? (As copied from a text editor)

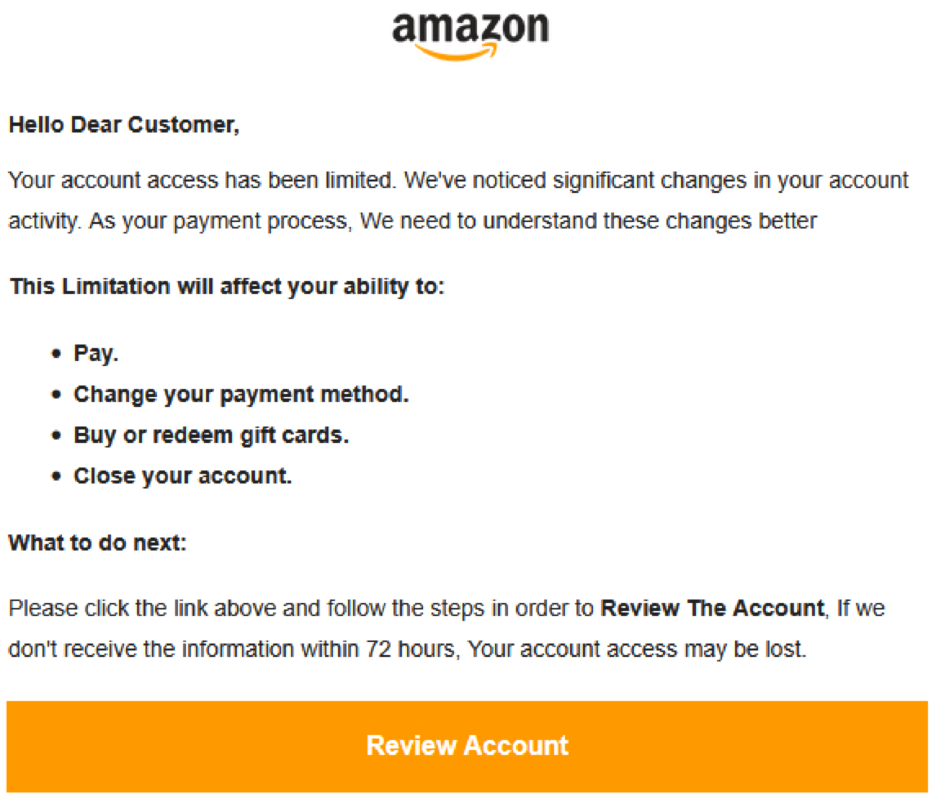


```
Date: Wed, 14 Jul 2021 01:40:32 +0900
```

Answer: Wed, 14 Jul 2021 01:40:32 +0900

What is the URL of the main call-to-action button?

To find this, I simply decoded the base64 encoded email body and used a html viewer to copy the link from the Review Account button:



Hello Dear Customer,

Your account access has been limited. We've noticed significant changes in your account activity. As your payment process, We need to understand these changes better

This Limitation will affect your ability to:

- **Pay.**
- **Change your payment method.**
- **Buy or redeem gift cards.**
- **Close your account.**

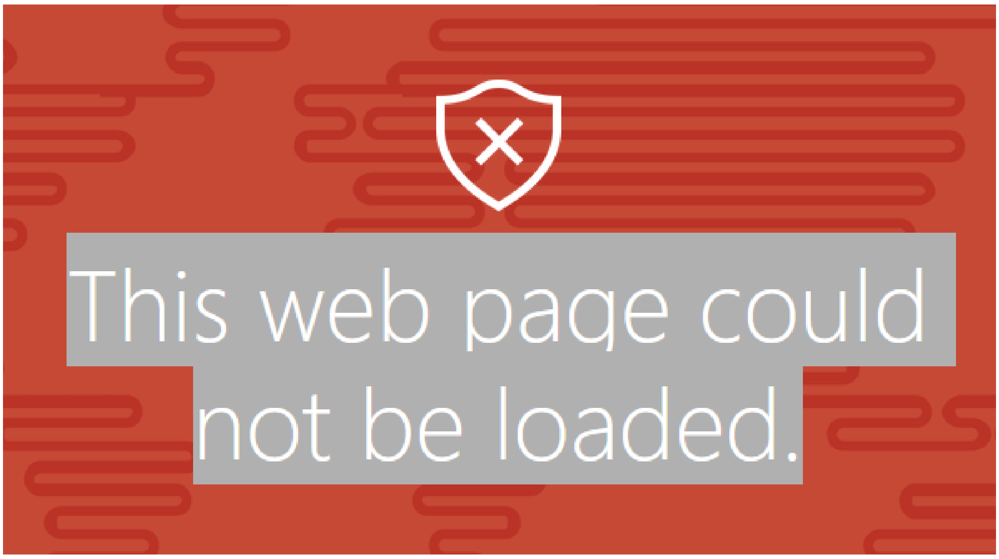
What to do next:

Please click the link above and follow the steps in order to **Review The Account**, If we don't receive the information within 72 hours, Your account access may be lost.

Answer: https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2Famaozn.zzyuchengzhika.cn%2F%3Fmailtoken%3Dsaintington73%40outlook.com&data=04%7C01%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=oPvTW08ASiViZTLfMECsvwDvguT6ODYKPQZNK3203m0%3D&reserved=0

Look at the URL using URL2PNG. What is the first sentence (heading) displayed on this site? (regardless of whether you think the site is malicious or not)

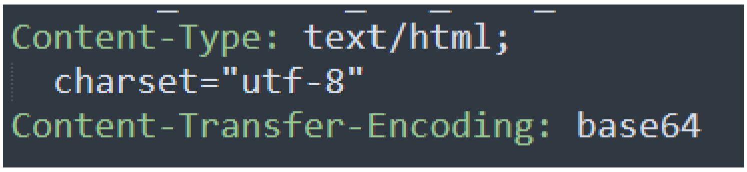
For some unfortunate reason, URL2PNG was unable to load the website, so I simply visited it using a sandboxed environment:


This web page could not be loaded.

Answer: This web page could not be loaded.

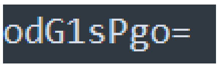
When looking at the main body content in a text editor, what encoding scheme is being used?

As you can see in the header, the encoding scheme used is base64:



```
Content-Type: text/html;
  charset="utf-8"
Content-Transfer-Encoding: base64
```

You can also tell by the padding:

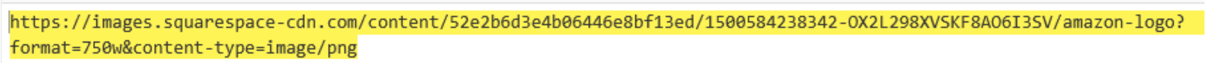


```
odG1sPgo=
```

Answer: base64

What is the URL used to retrieve the company's logo in the email?

To find the URL used to retrieve the company’s logo, I simply decoded the message body with CyberChef, and used the Extract URLs recipe to find any URLs contained within the body:

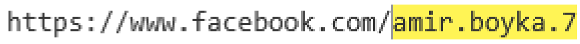


```
https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVSKF8AO6I3SV/amazon-logo?
format=750w&content-type=image/png
```

Answer: https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVSKF8AO6I3SV/amazon-logo?format=750w&content-type=image/png

For some unknown reason one of the URLs contains a Facebook profile URL. What is the username (not necessarily the display name) of this account, based on the URL?

From the CyberChef output of the previous question, you can see a Facebook link to a profile:



```
https://www.facebook.com/amir.boyka.7
```

Answer: amir.boyka.7