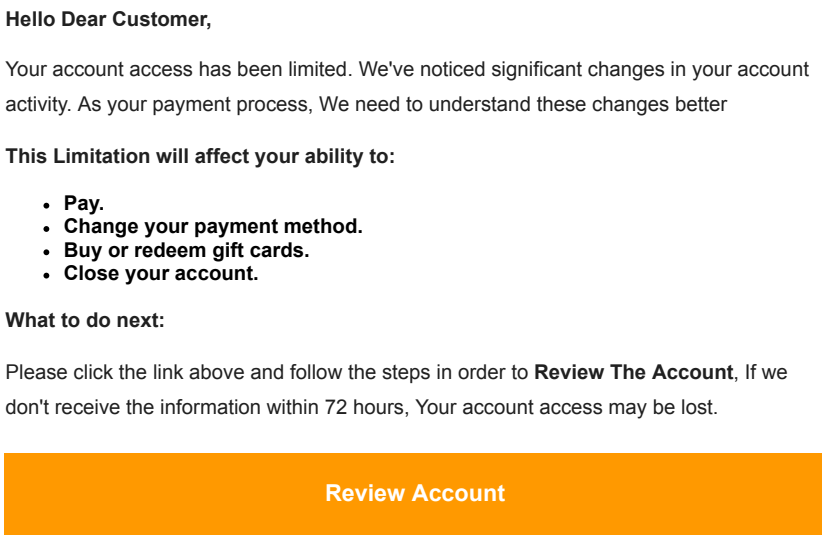
Phishing Email Analysis II Report



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.

Review Account

Yours Sincerely,

Amazon Support Team

Copyright © 1999-2021 Amazon. All rights reserved.

Potential Spam Email

1. Sender and Recipient Information

- **Sender Email Address:** amazon@zyevantoby.cn
- **Sender IP Address:** 45.156.23.138
- **Recipient Email Address:** **saintington73@outlook.com**

2. Email Content

- **Subject Line:** Your Account has been locked
- **Imitated Company:** Amazon
- **Date and Time Sent:** Wed, 14 Jul 2021 01:40:32 +0900

3. Phishing Indicators

- **Sender Email Domain:** The domain `zyevantoby.cn` is suspicious and not associated with Amazon. Legitimate emails from Amazon would come from `@amazon.com`.
- **IP Address:** The IP address `45.156.23.138` is unusual for Amazon's email servers.
- **Main Call-to-Action URL:**

  ```
  https://emea01.safelinks.protection.outlook.com/?
  url=https%3A%2F%2Famaozn.zzyuchengzhika.cn%2F%3Fmailtok
  en%3Dsaintington73%40outlook.com&data=04%7C01%7C%7C7007
  2381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaa
  aaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpb
  GZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1h
  aWwiLCJXVCI6Mn0%3D%7C1000&sdata=oPvTW08ASiViZTLfMECsvwD
  vguT6ODYKPQZNK3203m0%3D&reserved=0
  ```

  The URL redirects to a suspicious domain amaozn.zzyuchengzhika.cn, which is a clear misspelling of Amazon's domain.

- **Website Heading:** When attempting to load the website, the message displayed is: "The webpage could not be loaded." This indicates the site may be down or blocked, but still poses a risk.

4. Email Encoding

- **Encoding Scheme:** The email's main body content is encoded using base64, which is often used to obfuscate malicious content or hide phishing links.

5. Additional Suspicious URLs

- **Company Logo URL:**

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

This image URL is hosted on Squarespace, which is not typically used by Amazon for their logos. Amazon hosts their images on their own servers.

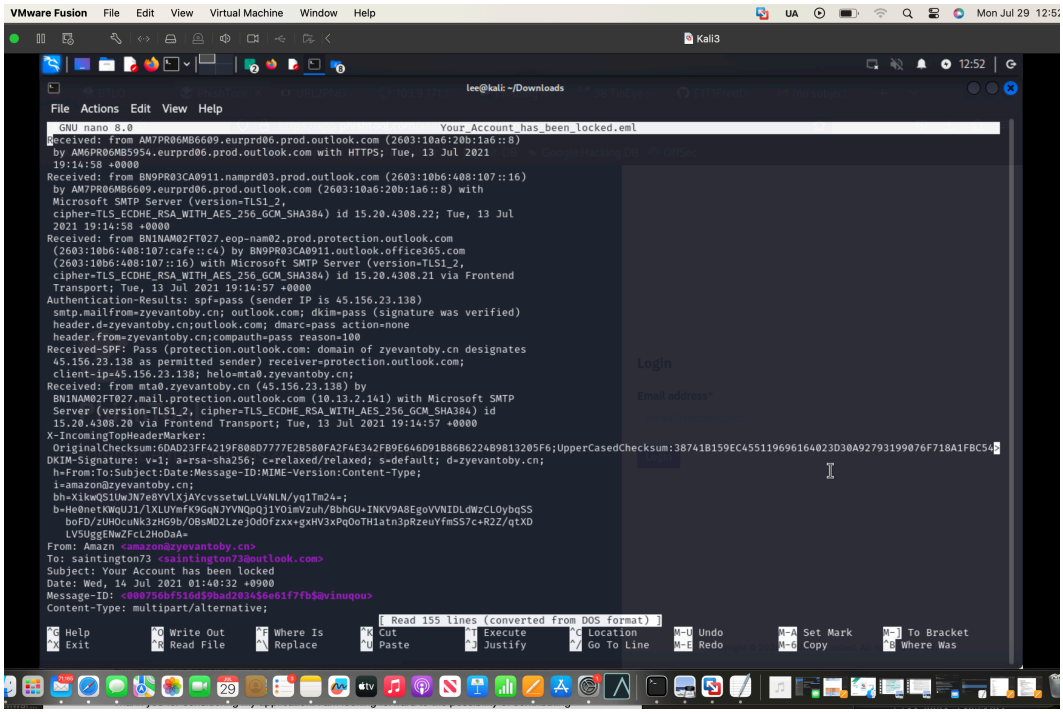
- **Facebook Profile URL:**

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

  This Facebook profile (amir.boyka.7) is irrelevant to Amazon and is likely included to confuse recipients or to add legitimacy.

6. Conclusion

This email exhibits multiple indicators of a phishing attempt, including a suspicious sender address, misspelled domains, obfuscated URLs, and irrelevant social media links. Recipients should not click any links or provide any personal information in response to this email.



Caption