

# Phishing Analysis 2 Walkthrough

## Tools used:

- Notepad
- Mozilla Thunderbird
- base64decode.org
- browserling.com


I downloaded the phishing email file provided by the website, extract it, and then put in "btlo" as the password.

## Phishing Analysis 2

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


Text Editor Thunderbird


Points <b>10</b>	Difficulty <b>Easy</b>	Solves <b>11261</b>	OS <b>Windows/Linux</b>
---------------------	---------------------------	------------------------	----------------------------


**Phishing Email**  
12.6 KB


Password  
btlo

**Download File**

 **First-Blood**

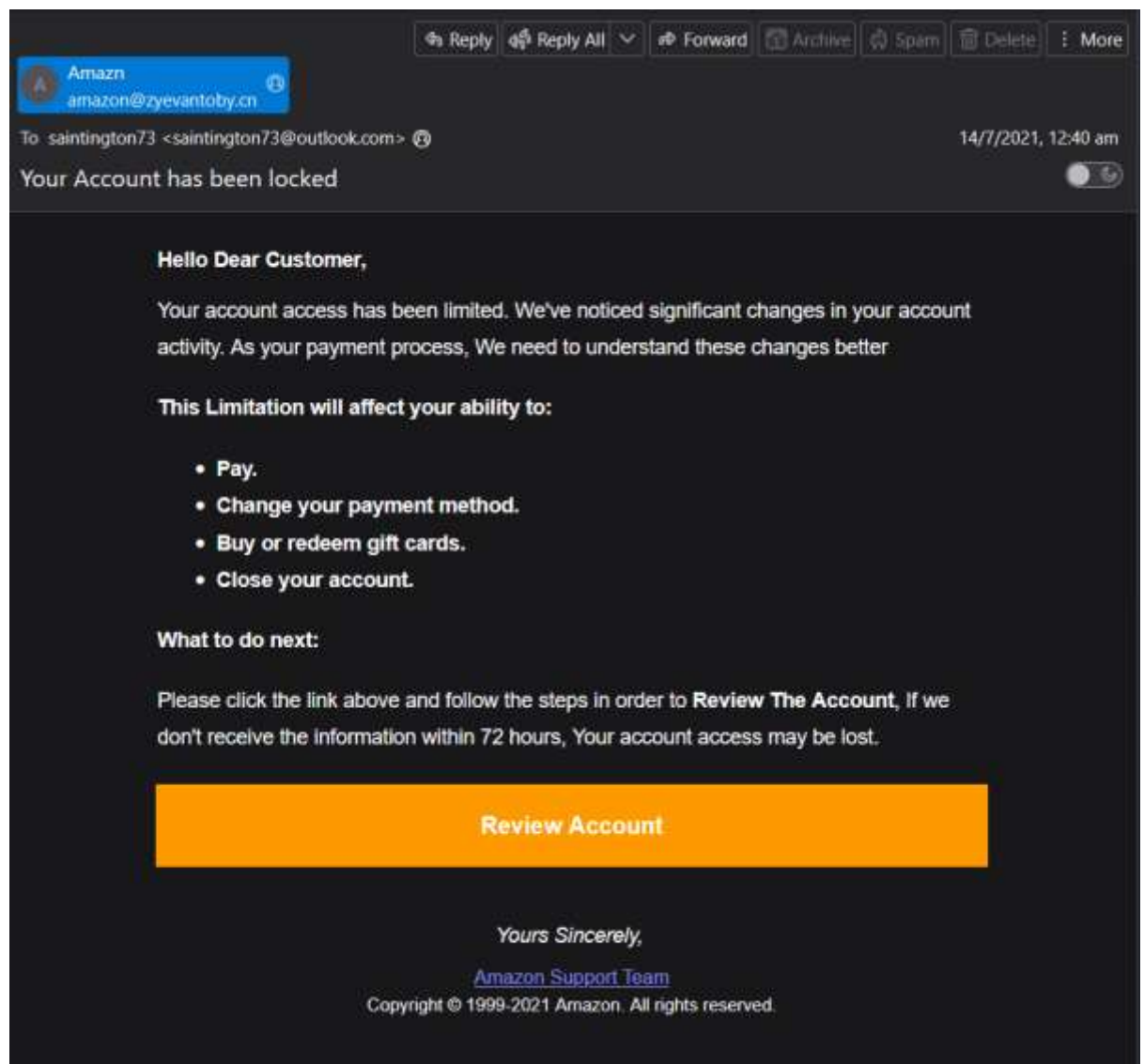
 **Created By**

**SetecAstronomy**  
1623 days ago

**BTLO**  
1623 days ago

# 1. What is the sending email address?

- I double clicked on the phishing email file and it directed me to the Mozilla Thunderbird.



The email of the sender can be clearly seen on the top left of the screen.



Answer: amazon@zyevantoby.cn

## 2. What is the recipient email address?

- Recipient email address can be seen on the To: section.

To saintington73 <saintington73@outlook.com> 

Answer: [saintington73@outlook.com](mailto:saintington73@outlook.com)

**3. What is the subject line of the email?**

- Subject line can be found under the recipient email address.

**Your Account has been locked**

*Answer: Your Account has been locked*

#### 4. What company is the attacker trying to imitate?

- From the sender's address, the company is trying to imitate Amazon.

A Amzn  
amazon@zyevantoby.cn

*Answer: Amazon*

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

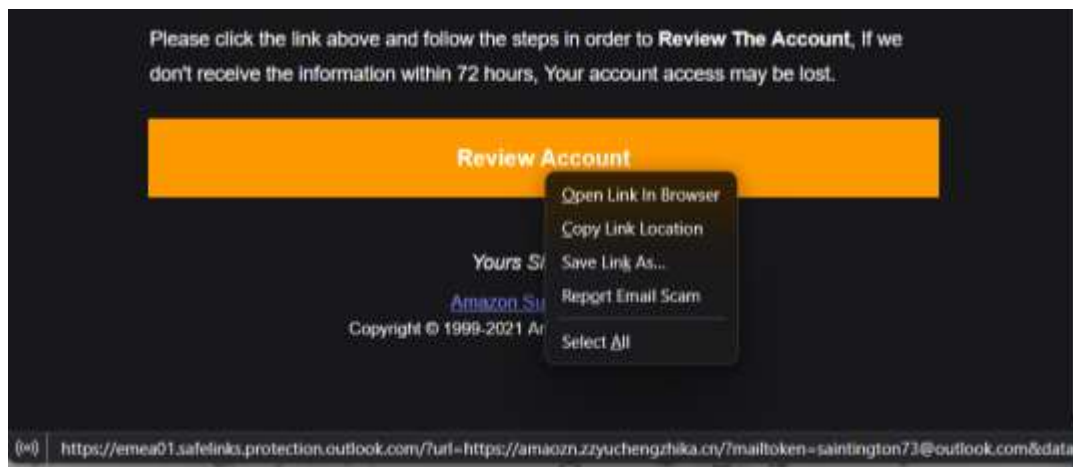
- I open the same file with notepad, and then search for "Date"

[illegible]

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

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

- By right clicking on the “Review Account” button, we can copy the URL to the website.

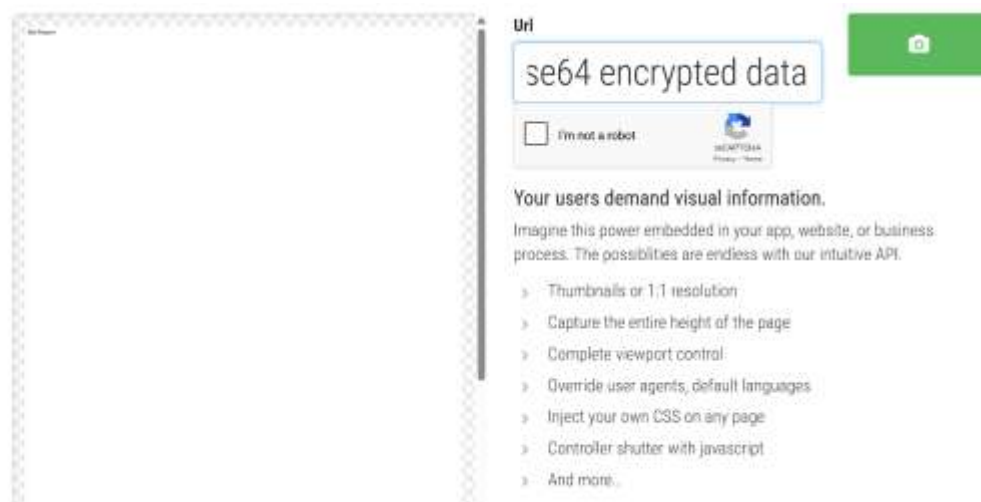


Answer:

<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%7CTWFpbGZsb3d8eyJWljojMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6lk1haWwiLCJXVCi6Mn0%3D%7C1000&sdata=oPvTW08ASiViZTLfMECsvgDvquT6ODYKPQZNK3203m0%3D&reserved=0>

## 7. 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)

I copied the URL and paste it to <https://www.url2png.com/>



However, it shows bad request, which is not the answer that I wanted. So I use [www.browserling.com](http://www.browserling.com) to surf and open the link safely.



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

- I used <https://www.base64decode.org/> to decode the base64 encrypted data

### Decode from Base64 format

Simply enter your data then push the decode button.

PCFET0NUWVBFIEhUtuw+PGh0bWw+PghIYWQ+CjxtZXRhIGh0dHATZXF1axY9IkNv  
bnRlbnQtVhlwZSIgY29udGVudD0idGV4dC9odG1sOyBjaGFyc2V0PXV0ZI04lj48bWV0  
YSBuYW1IPSJHRU5FUkFUT1ilGNvbniRlbnQ9ik1TSFRNTCAxMS4wMC4xMDU3MC4x  
MDAxIjl48L2hiYWQ+Cjxi2R5Pj4bWw+ICAgICAglCAglCAglDxvOm9mZmljZWVyY3Vt  
ZW50c2V0dGlzZM+PG86YWxs b3dwbm c+CiZuYnNwOyZuYnNwOyZuYnNwOyZuYnN  
wOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnN  
wOyZuYnNwOyAmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDs  
mbmJzcDsmbmJzcDsmbmJzcDsbgCjwwbzphbGxvd3BuZz4glCAglCAglCA8L  
286b2ZMaWoiZG9jdW1lbniRZR0aW5ncz4glCAglCAglCA8IS0t2VuZGlmXS0tLS0+I  
CAglCAglAogICAKE1FVEEGaHR0c1lcXVpdjoVC1VS01Db21wYXRypmxllBjb250Z  
W50PSJJRT1IZGdlIl4glCAglAo8TUVUQSUsYwY1IPStJa2wV3C9ydClgY29udGVudD0i  
d2lk dGg9ZGV2aWNILXd pZHRoLCBpbml0aWFSLXNIYWxlPT E iPiAgIAo8VEIU TE U + PC9

**i** For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

```
<TR>
  <TD width="600" align="center" valign="top"
    style="width: 600px;">&nbsp;<IMG width="749" height="67" style="width: 100px;"
    alt="" src="https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13e
d/1500584238342-OX2L298XVSKF8AO6I3SV/amazon-logo?format=750w&content
-type=image%2Fpng"
    border="0" hspace="0">
  <TABLE width="100%" class="templateContainer" border="0" cellspacing="0"
  cellpadding="0">
    <TBODY>
      <TR>
        <TD id="templateBody" valign="top">
```

Answer: <https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVSKF8AO6I3SV/amazon-logo?format=750w&content-type=image%2Fpng>



**10. 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?**

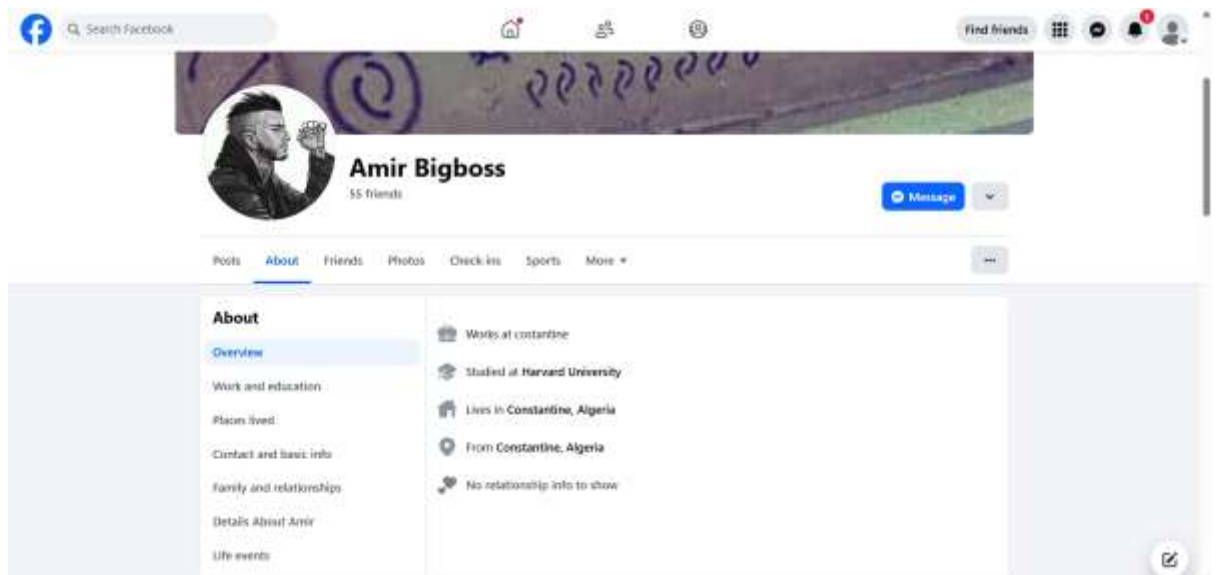
- I pasted the whole decoded base64 into the notepad and then searched for "facebook"

[illegible]

The link is:

www.facebook.com%2Famir.boyka.7&data=04%7C01%7C%7C70072381ba6e49  
d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C6376  
18004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWlloiMC4wLjAwMDAiLCJQlloi  
V2luMzliLCJBTiI6Ik1haWwiLCJXVCi6Mn0%3D%7C1000&sdata=KVi%2BG1%2BFO  
3v3ALNVowA1PrenHiT3aT%2F1vb5y1KxkAkc%3D&reserved=0"  
originalSrc="https://www.facebook.com/amir.boyka.7

Which will show:



*Answer: amir.boyka.7*