

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 10	Difficulty Easy	Solves 11261	OS Windows/Linux
--------------	--------------------	-----------------	---------------------

 [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 screenshot shows an email in Mozilla Thunderbird. The header bar includes standard options like Reply, Forward, Archive, and Delete. The email itself is from 'Amzn' at 'amazon@zyevantoby.cn'. The subject line is 'Your Account has been locked'. The body of the email reads:

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.

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

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

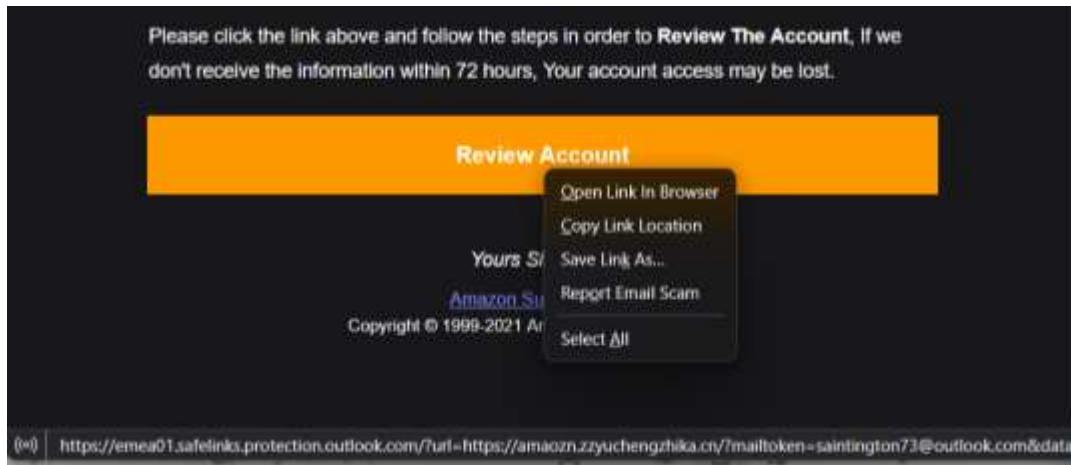
5. What is the date and time the email was sent? (As copied from a text editor)

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

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.

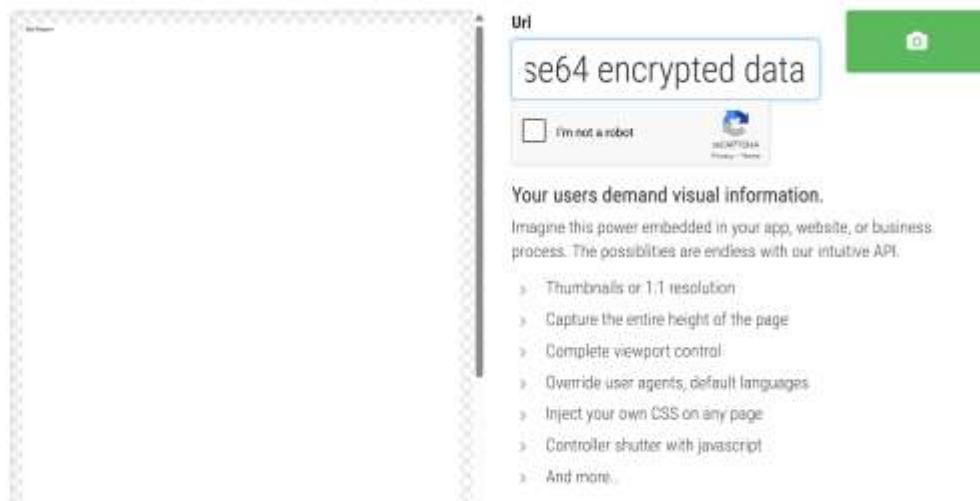


Answer:

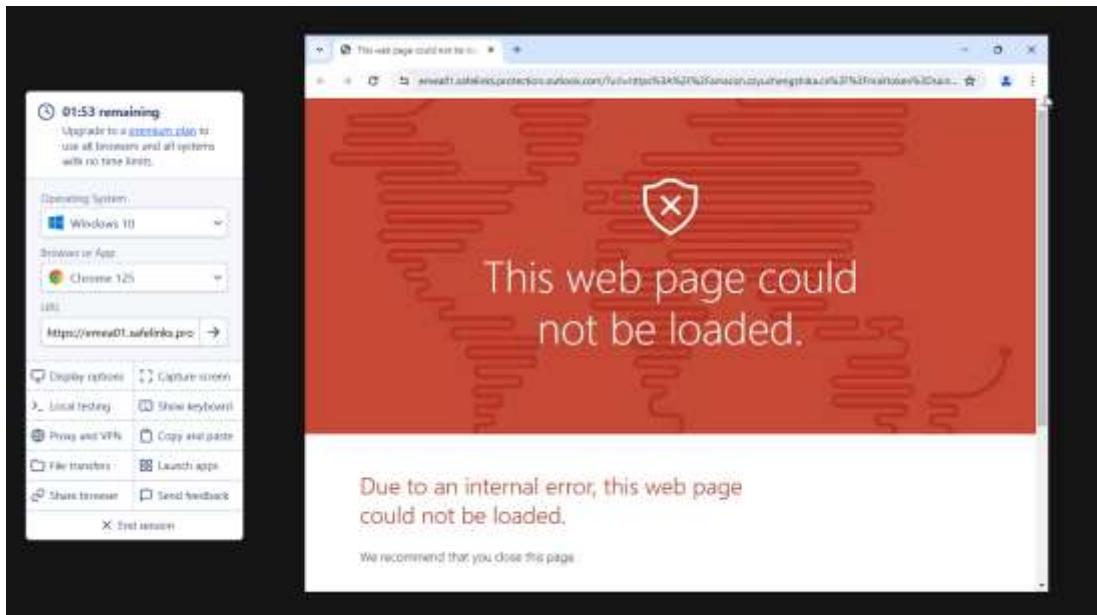
https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2Famaogn.zzyuchengzhihka.cn%2F%3Fmailtoken%3Dsaintington73%40outlook.com&data=04%7C01%7C%7C70072_381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaa%7C1%7C0%7C_637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWljoIiMC4wLjAwMDAiLCJQljoIV2IuMzliLCJBtil6lk1haWwiLCJVCI6Mn0%3D%7C1000&sdata=oPvTW08ASiViZTLfMECsvwDvquT6ODYKPQZNK3203m0%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 to surf and open the link safely.



Answer: This web page could not be loaded.

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

By looking inside the text editor I found:

```
--_NextPart_000_0232_018D8931.1E363E20
Content-Type: text/plain;
    charset="utf-8"
Content-Transfer-Encoding: base64

ICAgICAgICAgICAgICAgICAgICAgIA0KICAgIA0KSGVsbg8gRGVhciBDdXN0b21lcivNC
WW91ciBhz7LPsm91bnQgYWNjZXNzIGHcyBzZWVuIGxpbw10ZWQuIFdlJ3ZlIG5vdGljZWQgd
bmlmaWnhbnQgY2hhbmddcyBpbib5b3VyIGHPss+yb3VudCBhY3Rpdm10eS4gQXMgeW91cibwY
Zm50THByb2N1cmSTEld1Tc51Zwodc8aduslkzy1zdG5vZC8o2CV7zSpia65u72V7Tc11duv1c
```

Answer: base64

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.

```
PCFET0NUWVBFIhUTUw+PGh0bWw+PGhIYWQ+CjxtZXRhIGh0dHAtZXF1aXY9IkNv  
bnRlbNQtVHlwZSlgY29udGVudD0idGV4dC9odG1sOyBjaGFyc2V0PXV0Zi04lj48bWV0  
YSBuYW1IP SJHRU5FUkFUT1ilGNvb nRlbnQ9Ik1TSFRNTCAxMS4wMC4xMDU3MC4x  
MDAxIj48L2hIYWQ+Cjxib2R5Pjx4bWw+ICAgICAgICAgICAgIDxvOm9mZmljZWRvY3Vt  
ZW50c2V0dGluZ3M+PG86YWxsb3dw bmc+CiZuYnNwOyZuYnNwOyZuYnNwOyZuYnN  
wOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZuYnNwOyZu  
YnNwOyAmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDs  
mbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsmbmJzcDsgCjwvbzphbGxvd3BuZz4glCAgICAgICA8L  
286b2ZmaWNIZG9jdW1bnRzZXR0aW5ncz4gICAgICAgICA8IS0tW2VuZGlmXS0tLS0+i  
CAgICAgIAogICAKPE1FVEEgaHR0cC1lcXVpdj0iWC1VQS1Db21wYXRpYmxlliBjb250Z  
W50PSJJRT1ZGdlij4gICAgIAo8TUVUQSBUYW1PSJ2aWV3cG9ydClgY29udGVudD0i  
d2Ik dGg9ZGV2aWNILXdpZHRoLCBpbmloWFsLXNjYWxIPTEiPiAglAo8VEIUTEU+PC9
```

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/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVS KF8AO6I3SV/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-OX2L298XVS KF8AO6I3SV/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"

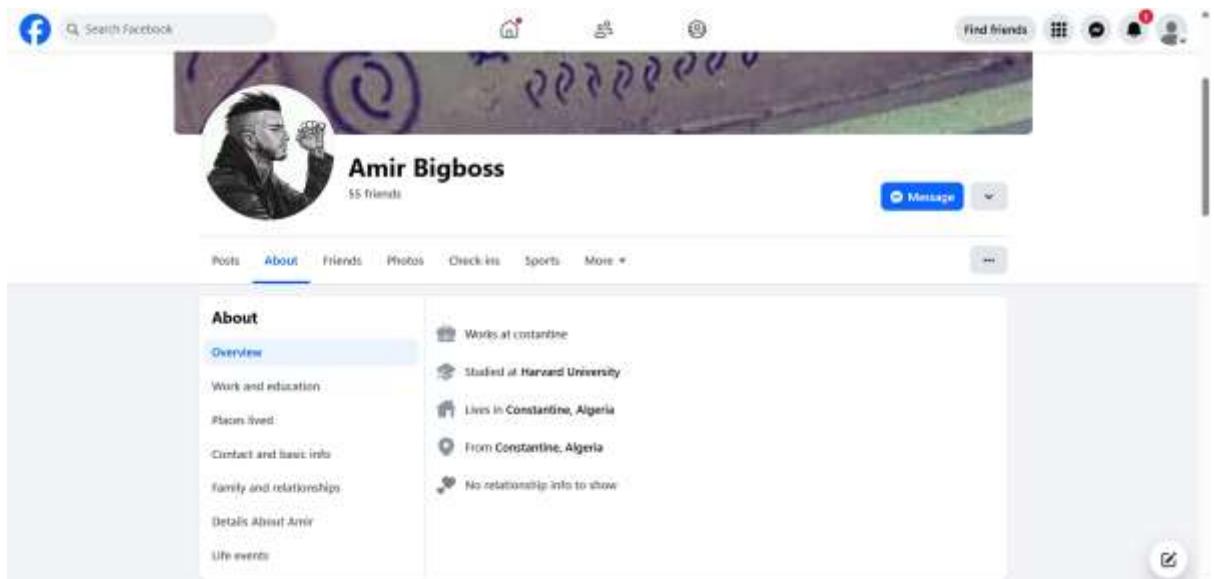


The screenshot shows a browser window with the address bar containing a long, decoded base64 string. The string starts with "www.facebook.com%2Famir.boyka.7&data=04%7C01%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBtil6Ik1haWwiLCJXCI6Mn0%3D%7C1000&sdata=KVi%2BG1%2BF03v3ALNVowA1PrenHiT3aT%2Flvb5y1KxkAkc%3D&reserved=0" and ends with "originalSrc="https://www.facebook.com/amir.boyka.7". Below the address bar, the page content is mostly obscured by a large redacted area.

The link is:

www.facebook.com%2Famir.boyka.7&data=04%7C01%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBtil6Ik1haWwiLCJXCI6Mn0%3D%7C1000&sdata=KVi%2BG1%2BF03v3ALNVowA1PrenHiT3aT%2Flvb5y1KxkAkc%3D&reserved=0"
originalSrc="https://www.facebook.com/amir.boyka.7

Which will show:



Answer: amir.boyka.7