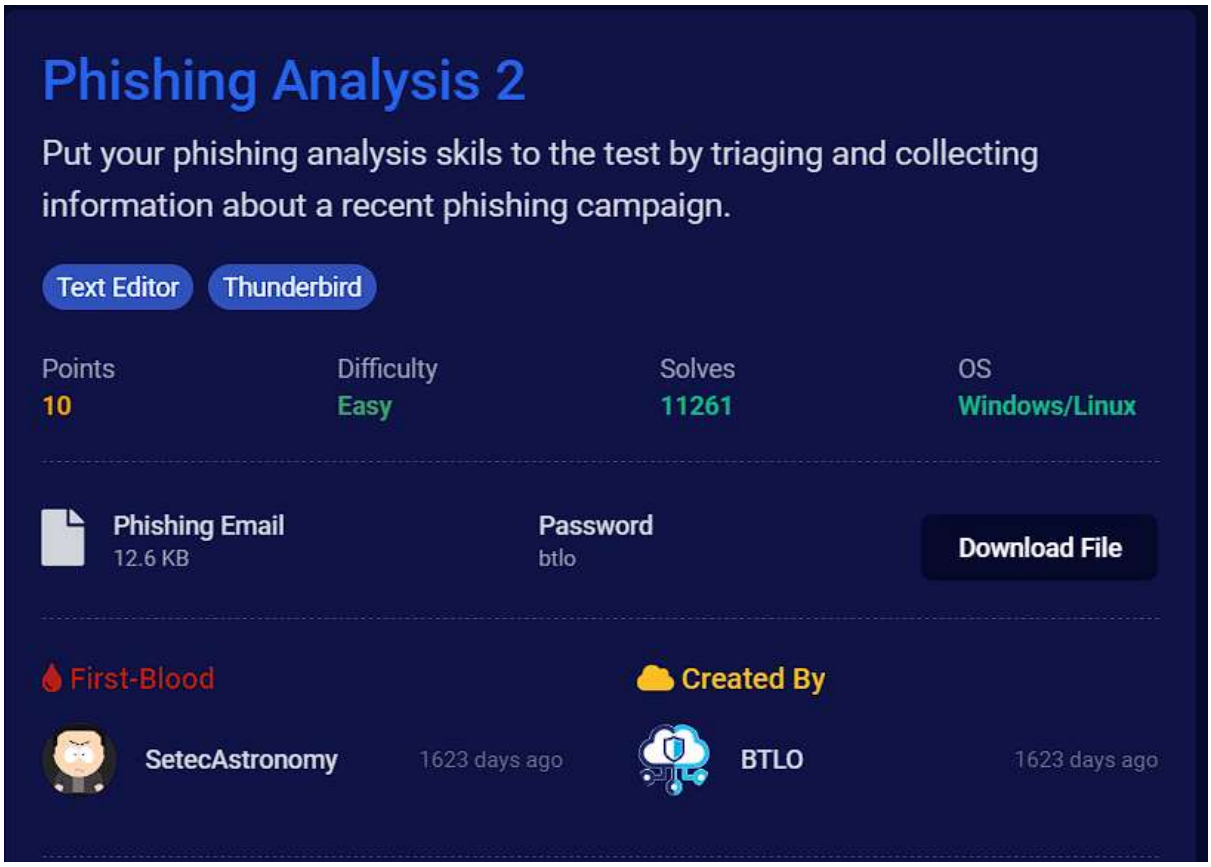
Phishing Analysis 2 Walkthrough

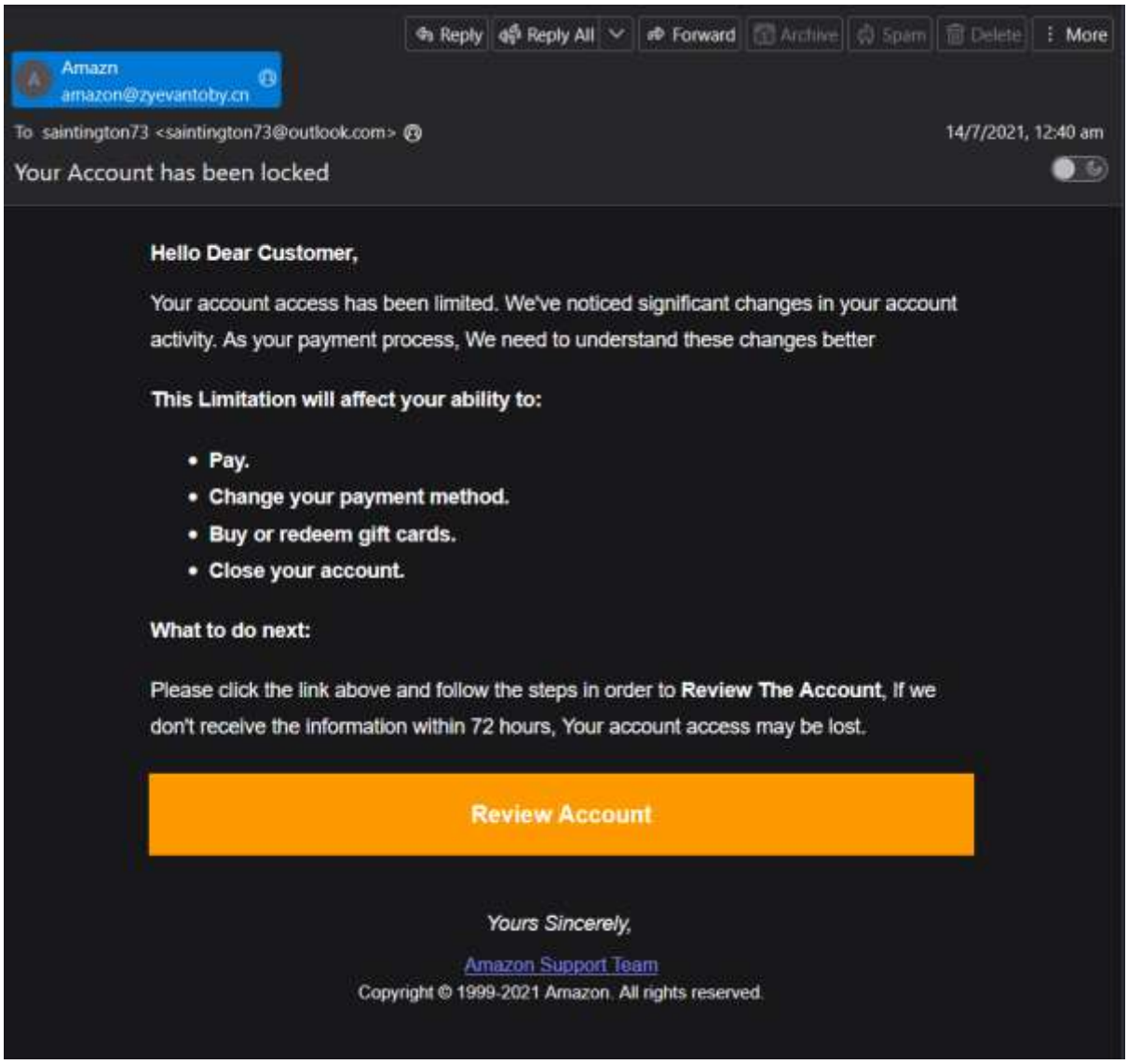
Tools used:

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

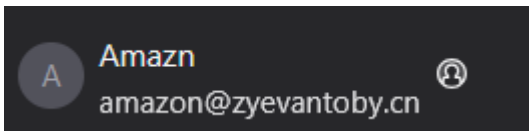
I downloaded the phishing email file provided by the website, extract it, and then put in “btlo” as the password.



1. **What is the sending email address?**
   - I double clicked on the phishing email file and it directed me to the Mozilla Thunderbird.

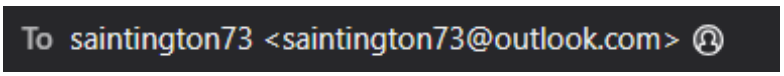


The email of the sender can be clearly seen on the top left of the screen.



Answer: amazon@zyevantoby.cn

2. **What is the recipient email address?**
   - Recipient email address can be seen on the To: section.

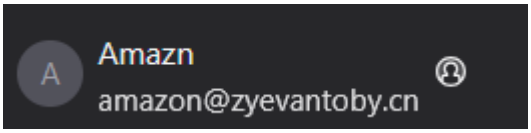


Answer: saintington73@outlook.com

3. **What is the subject line of the email?**
   - Subject line can be found under the recipient email address.

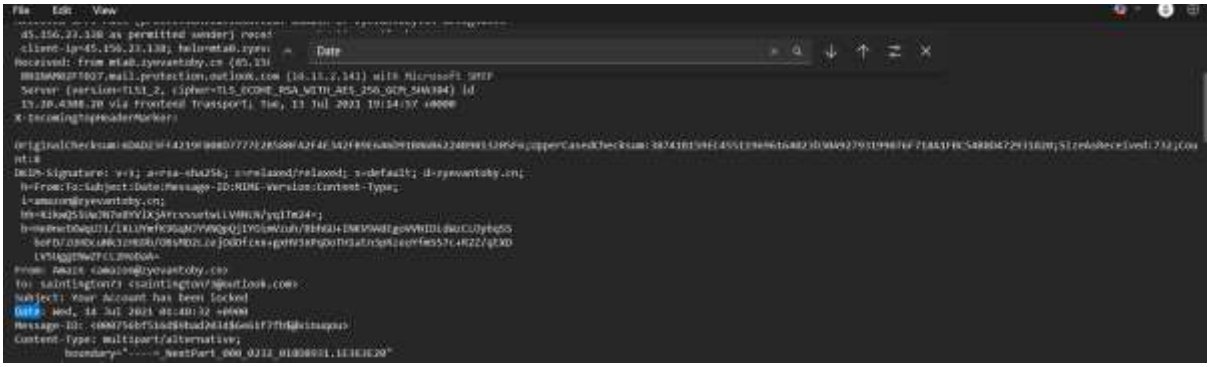
Answer: Your Account has been locked

4. **What company is the attacker trying to imitate?**
   - From the sender's address, the company is trying to imitate Amazon.



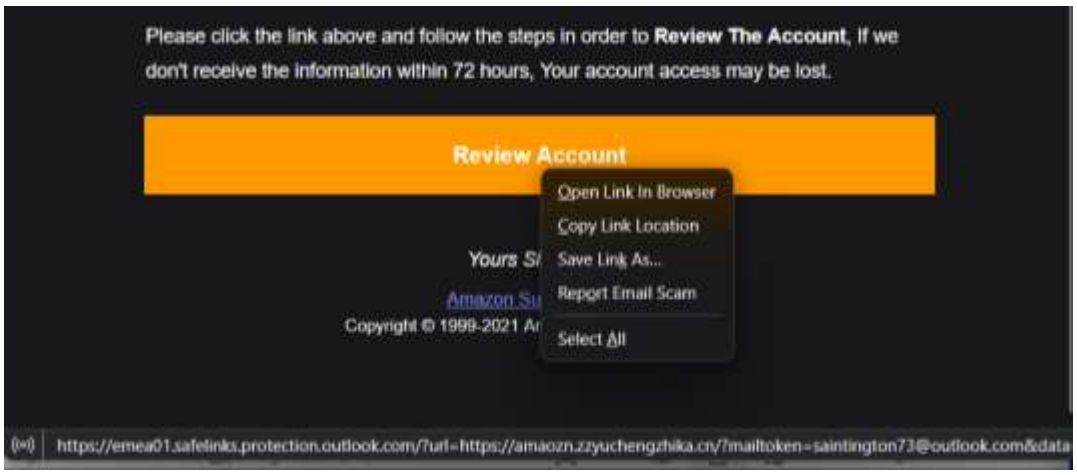
Answer: Amazon

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

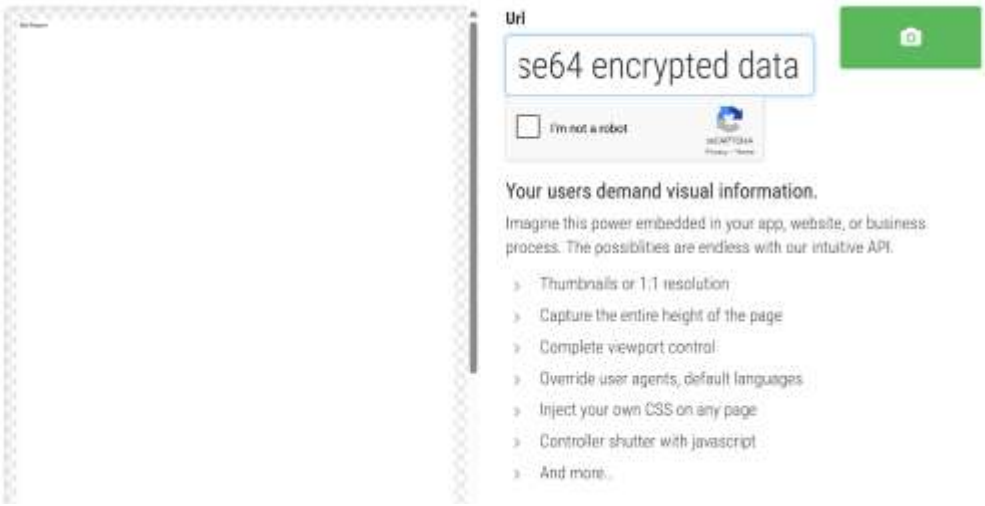
6. **What is the URL of the main call-to-action button?**
   - By right clicking on the “Review Account” button, we can copy the URL to the website.



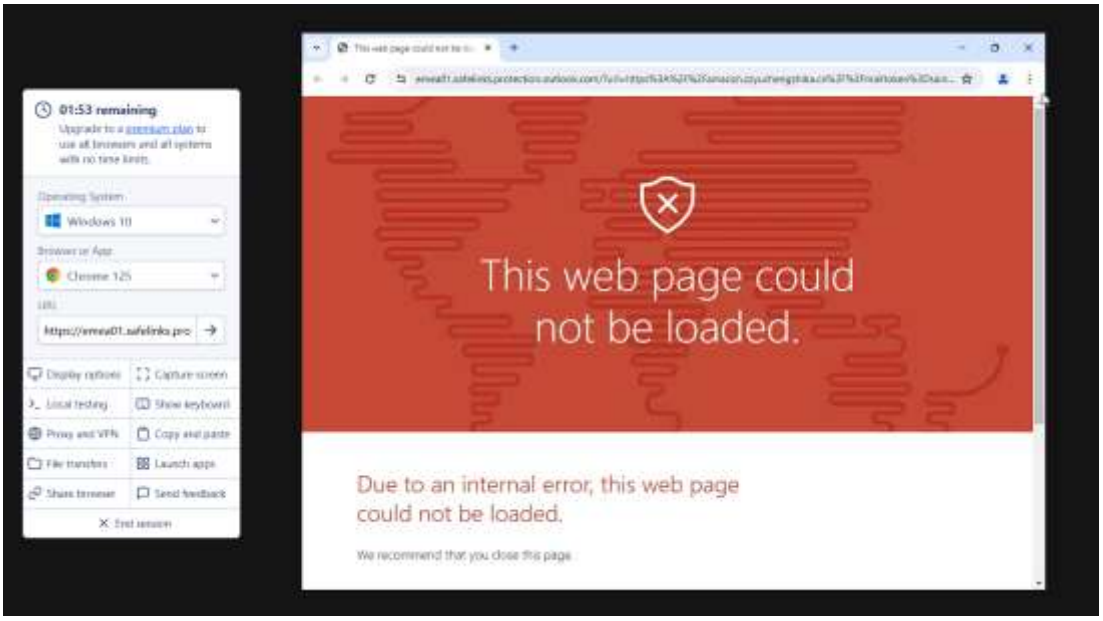
Answer:
https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2Famaozn.zzyuchengzhika.cn%2F%3Fmailtoken%3Dsaintington73%40outlook.com&data=04%7C01%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=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

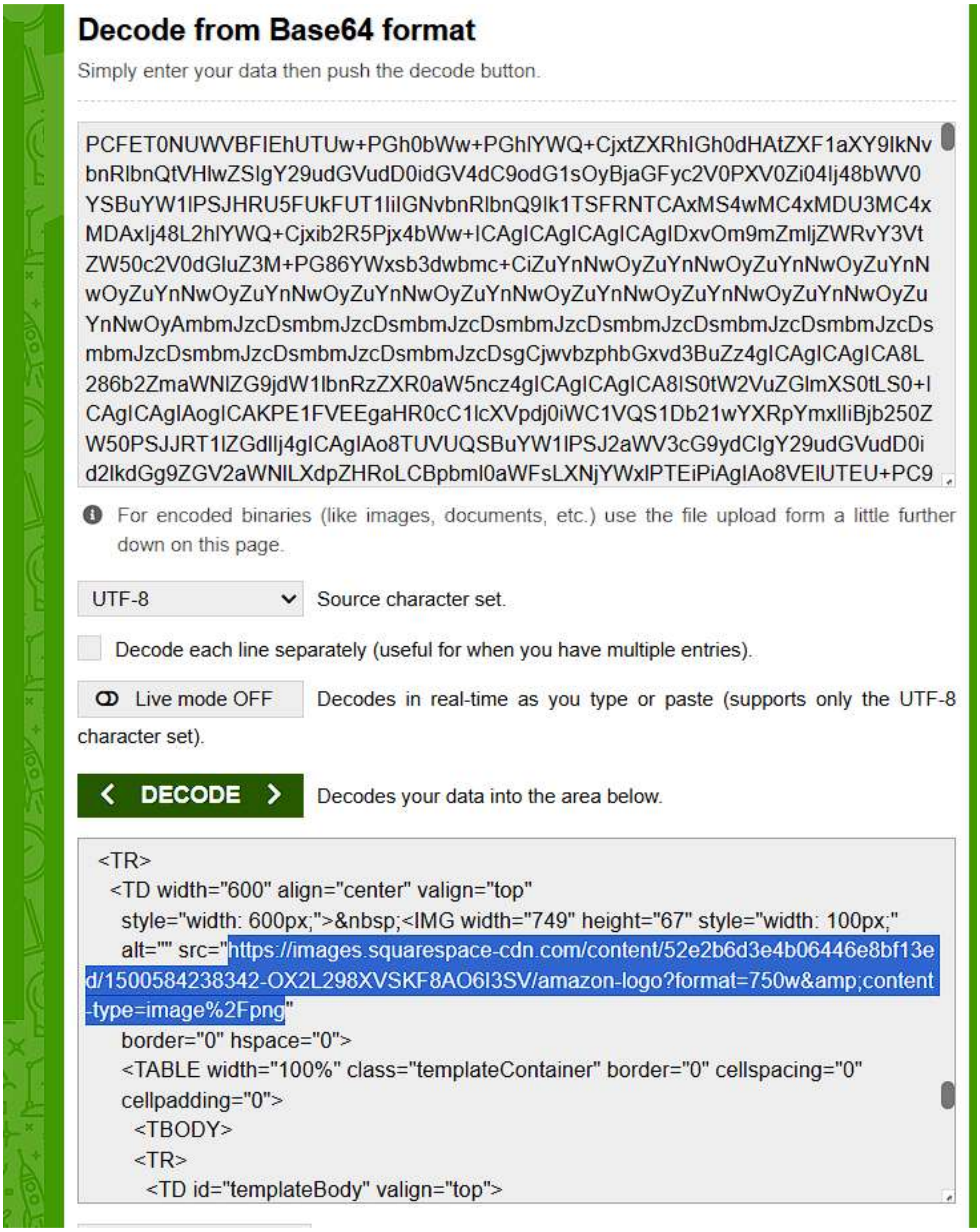
By looking inside the text editor I found:

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

ICAgICAgICAgICAgICAgICAgICAgICAgIA0KICAgIA0KSGVsbG8gRGVhciBDdXN0b21lciwNC
WW91ciBhz7LPsm91bnQgYWNjZXNzIGhhcyBiZWVuIGxpbWl0ZWQuIFdlJ3ZlIG5vdGljZWQgc
bmlmaWNhbnQgY2hhbmdlcyBpbiB5b3VyIGHPss+yb3VudCBhY3Rpdml0eS4gQXMgeW91ciBwY
ZW50IHRyb2Nlc3MsIFdlIG5lZWQgdG8gdW5kZXJzdGFuZCB0aGVzZSBjaGFuZ2VzIGJldHRlc
```

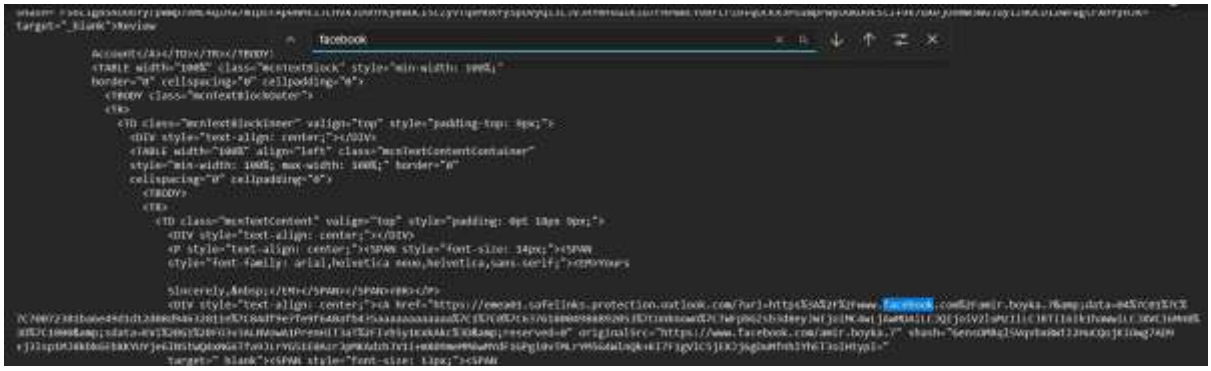
Answer: base64

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



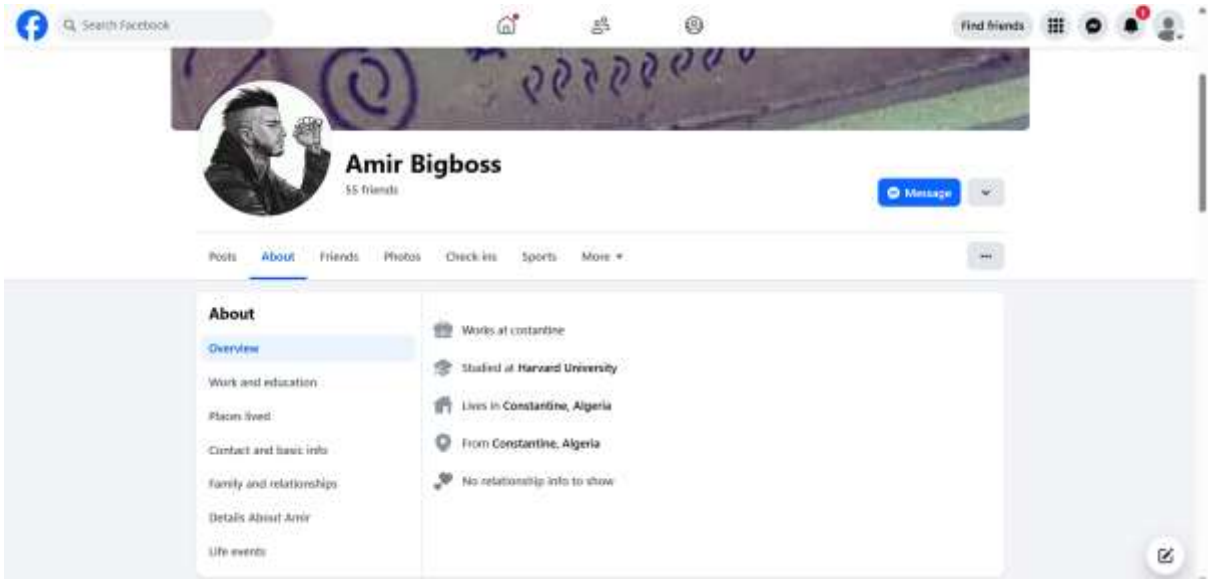
Answer: https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVSKF8AO6I3SV/amazon-logo?format=750w&content-type=image%2Fpng

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”



The link is:
www.facebook.com%2Famir.boyka.7&data=04%7C01%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=KVi%2BG1%2BFO3v3ALNVowA1PrenHiT3aT%2FIvb5y1KxkAkc%3D&reserved=0" originalSrc="https://www.facebook.com/amir.boyka.7

Which will show:



Answer: amir.boyka.7