**Phishing Email**

**Task 2: Analyze a Phishing Email Sample**

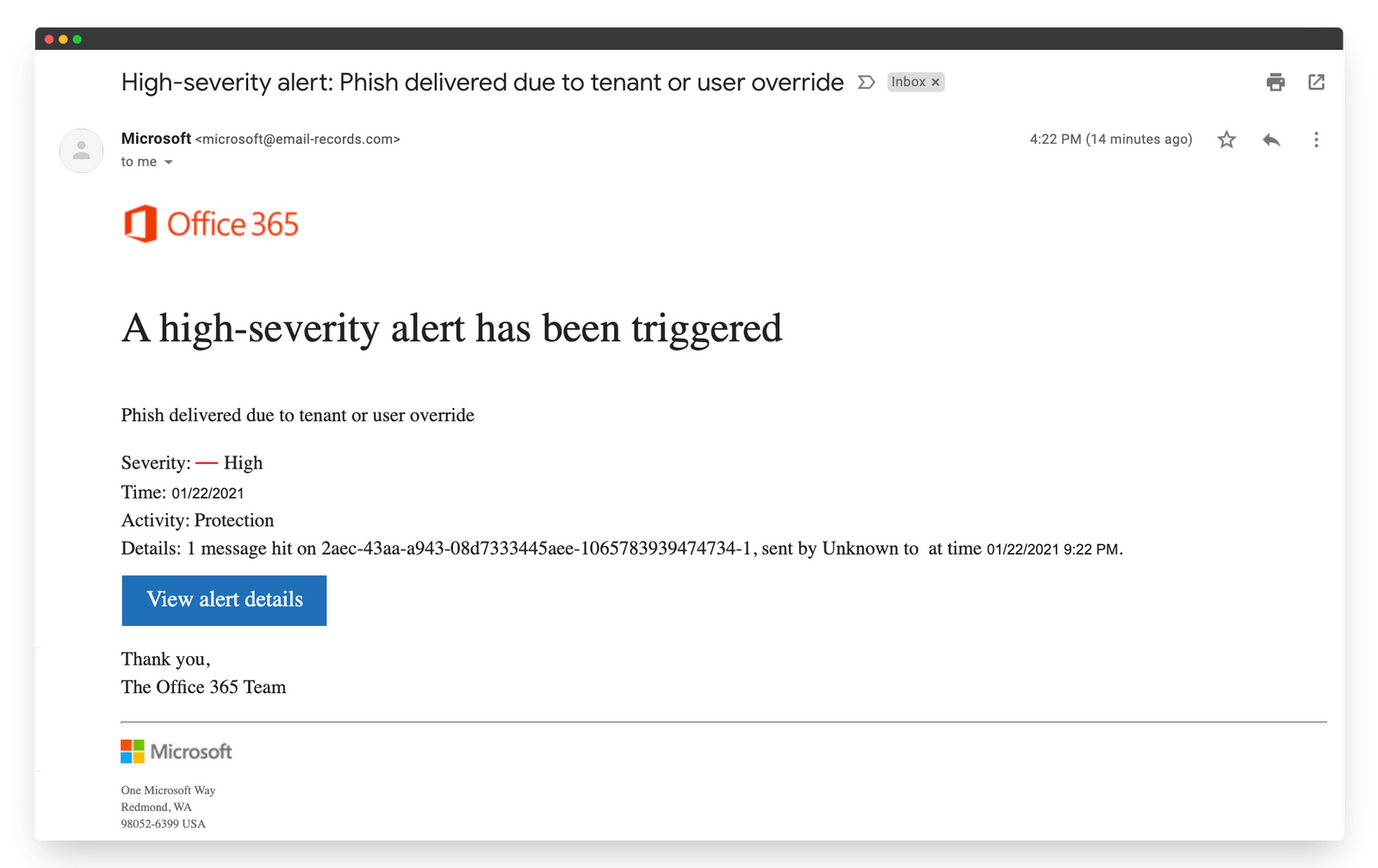
**Objective:** Identify phishing characteristics in a suspecious email sample.

**Tools:** Email client or saved email file (text), free onlibe header analyzer.

**Delivarables:** A report listing phishing indicators found.

**Procedure:**

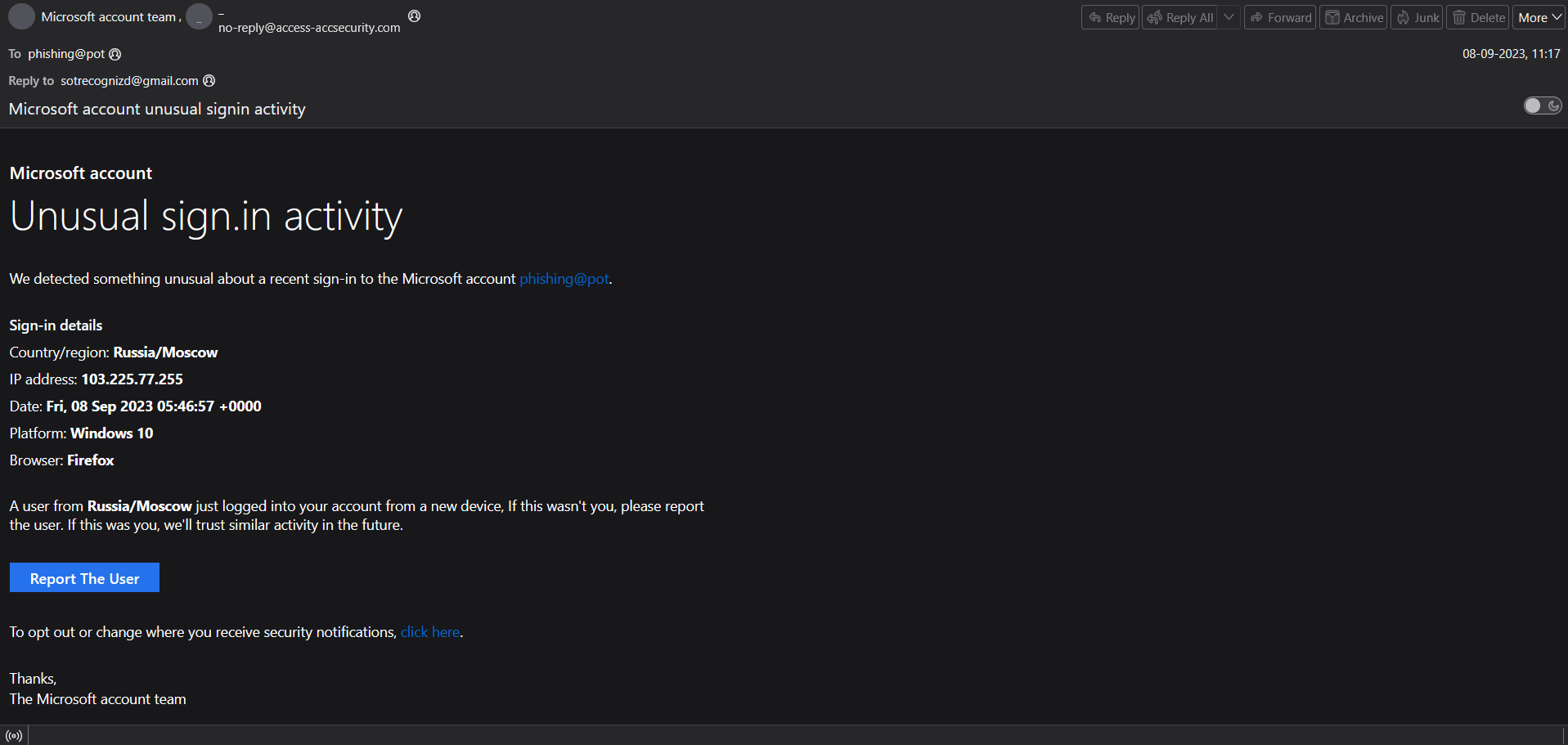
Let us collect a sample phishing mail and examie the red flags in it.



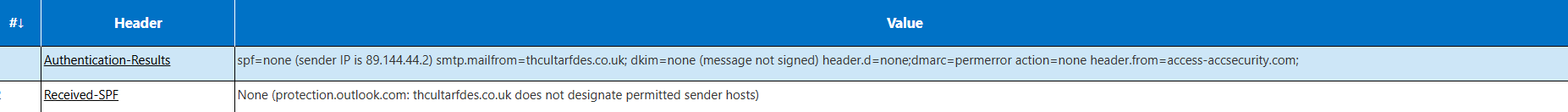
Here we can see the logo of Office 365. But if you look the header [(microsoft@gmail-records.com)](mailto:(microsoft@gmail-records.com)) the domain name is not legitimate, because microsoft mail domain name ends with @microsoft.com

This mail is designed for threatening language in the email body. So most of the users click on the details without looking the mail header. This may lead to exploit the macine or get the sensitive details to reveal.

Let me show you an another example

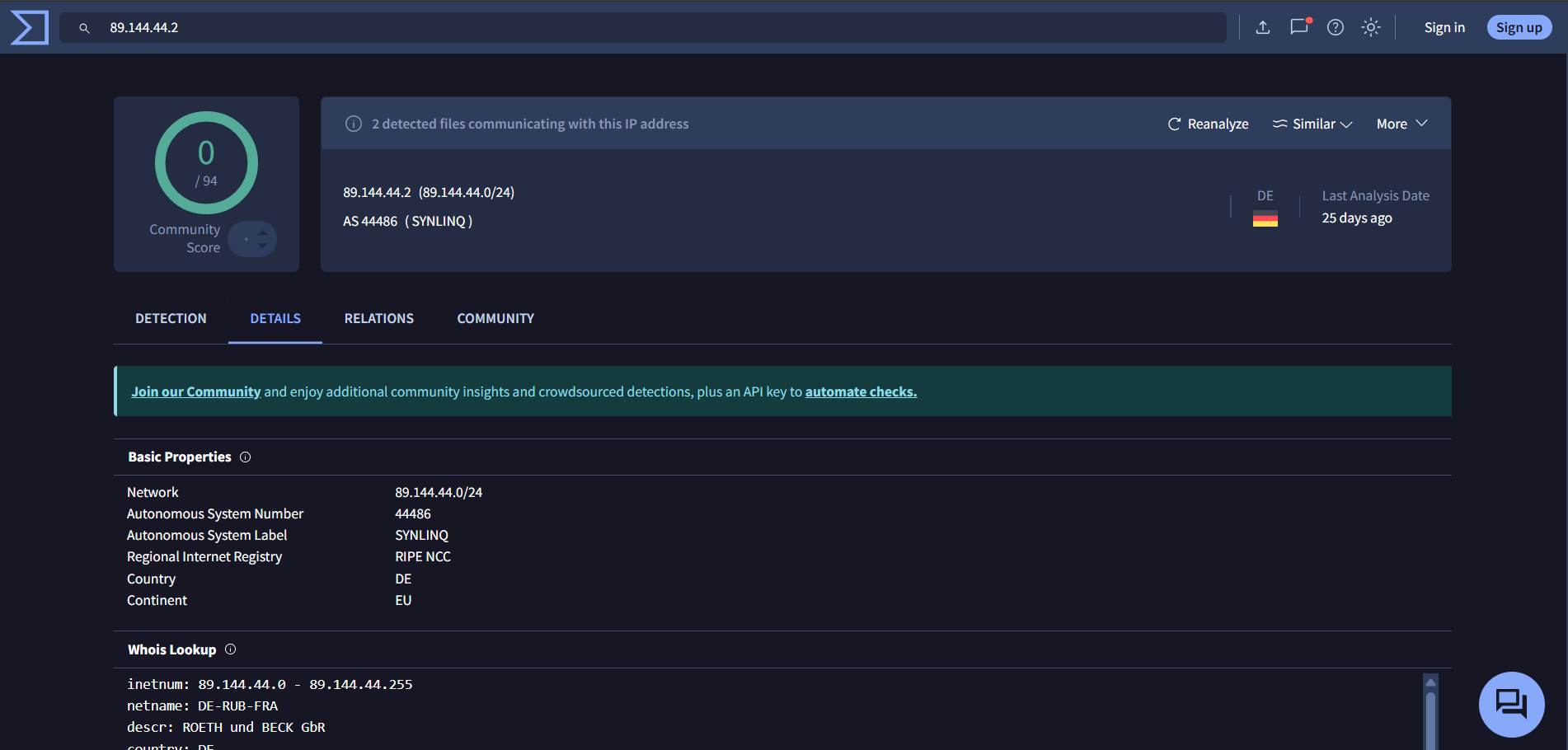


In the above mail you can see that sounds like from microsoft account team, but the sender domain is suspecious [(no-reply@access-accsecurity.com)](mailto:(no-reply@access-accsecurity.com)) which isn’t legitimate. For the deeper examination lets check the hearder of the mail.



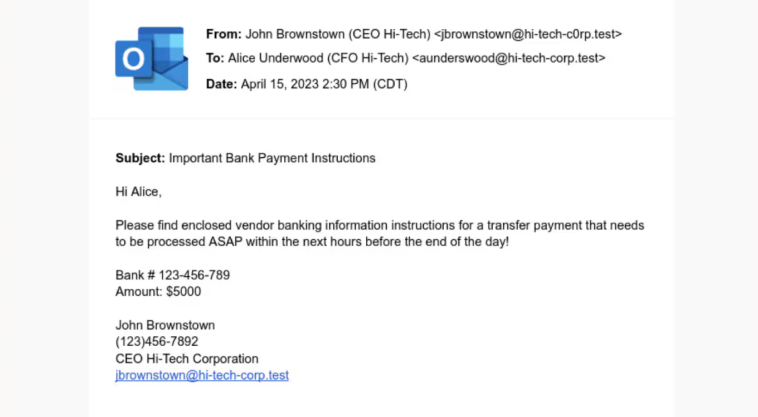
SPF and DMARK failed to AntiSpamReport, this is the crucial technical evidence to consider that this is a phishing mail.

When I tried to look for the sender ip address, the results were



This explains that it’s not a microsoft-owned ip block. This conclude that this ip address may be from a compromised server.

An another example,



In the above mail when we see the from address [(jbrownstown@hi-tech-c0rp.test)](mailto:(jbrownstown@hi-tech-c0rp.test)) there is a typosquatting domain name by replacing alphabet “o” with number “0”. However the domain name is suspecious, but sometime you may face these type of red falgs in your day to day life. For example:

[support@gmail.com](mailto:support@gmal.com) can be replaced with [support@gmal.com](mailto:support@gmal.com) . When you look hurry both are same, but both are different.

**Summarize:**

Phishing attack is form of Social Engineering attack, where attacker exploits human error to gain the sensitive information. Phishing attack can be happened in many ways.The receipter amy get the mail in an urgent way or the threatened way or Offereing way etc.. every possible way to make user to click on the link or open the document or an image.

The flags you can notice that it’s a phishing mail.

* Generic greeting
* Grammatical errors
* Low resolution logs or images
* Suspecious sender email address
* Strange URL’s
* Requesting for Personal details