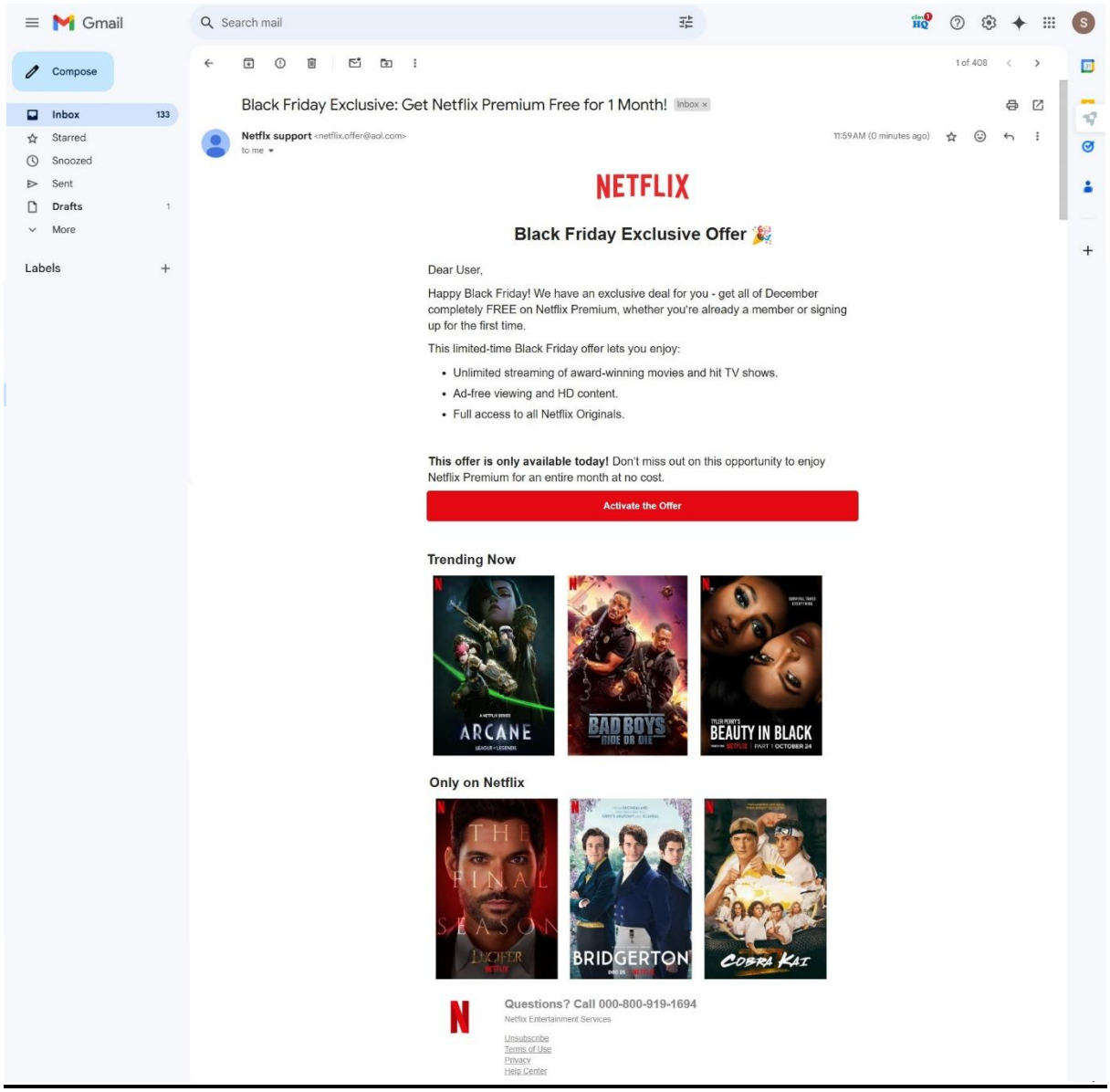
Phishing Email Explanation

Since Black Friday is approaching, I came up with this idea, which can be really effective during this time when people are excited and receiving lots of emails about special offers from different brands. I chose Netflix for the phishing attempt because it's a well-known brand. Everyone loves Netflix, and who doesn't know about it? So, when someone gets an email from Netflix, they'll naturally be curious to see what deals Netflix is offering for Black Friday. I used this curiosity to create a phishing email that looks like a legitimate Netflix promotion.

This email is designed to trick people, especially in the USA, where many are waiting for Black Friday deals. If a real malicious link were added and somehow managed to bypass email security filters from Gmail or Outlook, it could easily deceive people into clicking on it. The email looks very real at first, with only a few subtle red flags that are hard to notice right away. But during Black Friday, when people are already excited and overwhelmed with offers, many might miss these red flags and click on the link without thinking twice. In just one day, an attacker could target and deceive a large number of users.

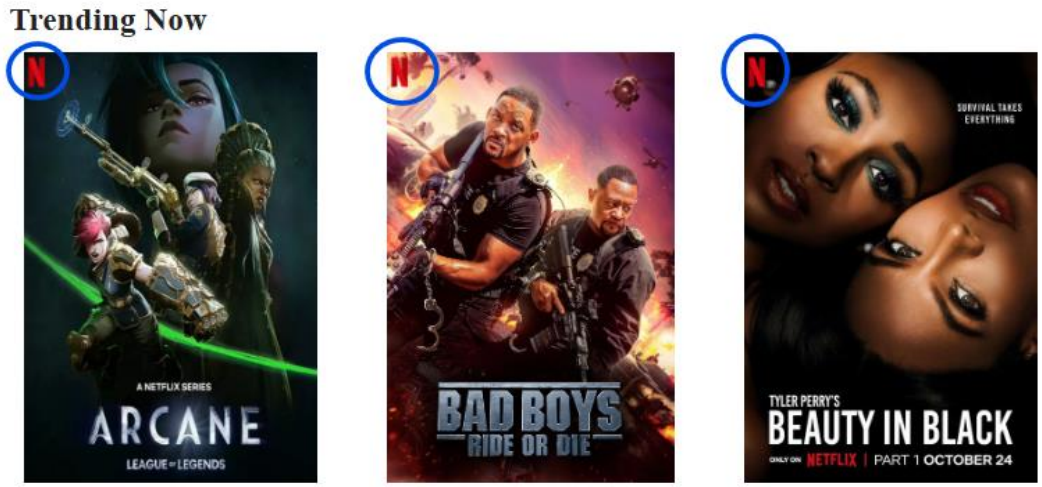
The Mail:



How it traps the users:

1. **Convincing Subject Line and Email ID:** The subject line, "**Black Friday Exclusive: Get Netflix Premium Free for 1 Month!**", catches the reader's eye with an exciting offer. It takes advantage of the hype around Black Friday, making it hard for people to ignore. The email ID- netflix.offer@aol.com- also includes "Netflix," making it look like it's from a real company. Even though the email is actually fake because it's from "aol.com," the subject and email address make people want to open it right away without checking for red flags.

2. **Brand Impersonation:** The email starts with the Netflix logo and familiar images, like banners for trending and Netflix shows such as Arcane, Bridgerton, Cobra Kai, Bad Boys, Beauty in the Black, and Lucifer. Even the posters for these shows have the Netflix logo placed at the top left corner, just like in official Netflix communications (as seen in the image below, which shows the logo on the posters). What makes this email even more deceptive is that the shows listed as trending are actually accurate and reflect what is currently trending on Netflix. This level of detail makes the email feel authentic, tricking even regular Netflix users into believing it's real. By using these familiar visuals and accurate content, the email looks real and trustworthy, increasing the likelihood that recipients will open it and engage with the content.



3. **Perfect Font and Format Match: Mimicking Official Netflix Emails:** The phishing email uses **Helvetica**, **the same font that Netflix employs** in its official communications. Everything from the font size to the line spacing and paragraph gaps has been carefully matched to mimic genuine Netflix emails. This attention to detail makes the email look incredibly convincing, as even the smallest design elements, like text alignment and formatting, closely resemble those in real Netflix messages. Such precise replication can easily fool recipients into believing the email is authentic.

4. **Too Good to Be True: Illusion of a Free Month:** The email says that people can get Netflix Premium for free for a whole month, which is an offer that seems too good to be true, especially on Black Friday. Phishers use these kinds of fake deals to get people to click on malicious links.

5. **The Trap: Using Fake Benefits to Attract Victims:** The email highlights "benefits" like unlimited streaming, ad-free viewing, HD content, and access to Netflix Originals. With each line, excitement builds, making the offer seem more legitimate. This growing excitement eventually pushes the recipient to urgency, encouraging them to click the malicious link without fully thinking it through.

6. **Hurry, Before It's Gone:** The email message creates a sense of urgency by saying it's a "Black Friday Exclusive Offer" and that the offer is only available for a limited time. This tactic is meant to make the recipient act quickly without thinking too much about whether the offer is real.

7. **Misleading Links: Every Click is a Trap:** The email includes a button **"Activate the Offer"** and images of Netflix shows, all linking to a fake website (http://maliciouslink.com/). Even the Netflix logo, trending show banners, privacy, and help center links are all tied to malicious links. This makes the email especially dangerous, as every part of it- from the images to the logos and buttons- contains malicious links, all designed to trick the reader into clicking on them and leading to fake websites.

8. **Realistic Customer Support Details and Links:** The email includes a real Netflix phone number and links such as “Terms of Use,” “Privacy,” and “Help Centre” all formatted exactly like in real Netflix emails. The layout and wording match Netflix's official communications, making the email look very legitimate. However, all these links, including “Privacy” and “Terms of Use,” lead to the same malicious website, making the email look real while hiding its harmful purpose.

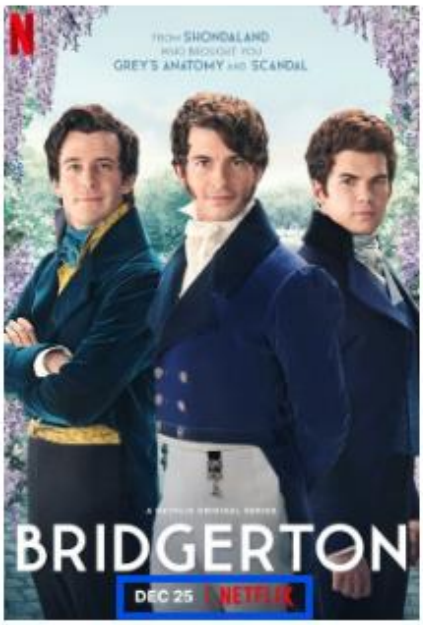
Red Flags (Educational Value):

1. **Fake Email Domain:** The sender’s email address has “Netflix” in it (netflix.offer@aol.com), but the domain is not **netflix.com**, which is only used by Netflix officially. This is a clear sign the email is fake.

2. **Sender Name Tricks:** The sender name says **“netflx support”** instead of "Netflix Support." This small change is easy to miss if someone isn’t paying close attention.

3. **Generic Greeting:** The email starts with **“Dear User”** instead of using the recipient's real name. Real emails from Netflix are personalized, so this is a common clue of a phishing attempt.

4. **Wrong Poster Details:** While the posters include the Netflix logo at the top left corner to look official, some also have “Netflix” written at the bottom along with a release date- something Netflix doesn’t usually include in its content. As you can see in the image below, this detail doesn’t align with Netflix's usual formatting, making it a red flag.



5. **Image Quality: Close, but Not Netflix Standard:** The images in the email have good resolution, making them appear convincing at first glance. However, they lack the high-quality resolution that Netflix typically uses in its official communications. This slight difference in image clarity can be a subtle red flag for those familiar with Netflix's usual standards.

6. **Free Netflix Offer:** A free month of Netflix Premium during Black Friday sounds too good to be true, especially as an offer for everyone. While Netflix may offer discounts or special deals during Black Friday, they’re typically limited to selected users or specific conditions. Broad, unrestricted offers like this are a classic phishing tactic, designed to make people click without questioning the legitimacy.

7. **Urgency Tactics:** The email claims, **“This offer is only available today”** a tactic used to rush people into acting quickly. This sense of urgency discourages recipients from taking the time to verify the email’s authenticity, making it a common phishing strategy.

8. **Emoji Use:** One element in the email is the use of an emoji- 🎉, which may or may not be a typical feature in official Netflix emails. The emoji is likely included to grab attention, make the offer seem more appealing, and increase excitement. While it may seem harmless, the use of such eye-catching elements is often a tactic in phishing emails to divert the recipient's focus and encourage quick actions. Whether or not Netflix uses emojis in their official communications, their presence here could be a sign of an attempt to manipulate the recipient’s emotions, pushing them toward clicking the malicious link.

In conclusion, this phishing email is a very well-crafted scam designed to appear legitimate, using familiar visuals, brand impersonation, and tempting offers to trick users. However, there are clear signs, such as the suspicious sender address, generic greeting, and unrealistic offers, that should raise red flags for anyone receiving such emails. By being cautious and looking out for these signs, users can protect themselves from falling victim to phishing attempts and avoid the dangers of malicious links. **Always double-check the source of emails, especially when they promise deals that seem too good to be true**.