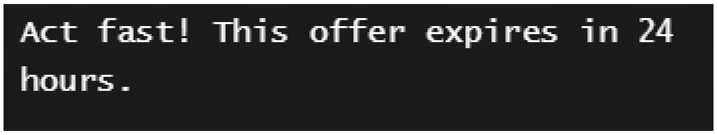
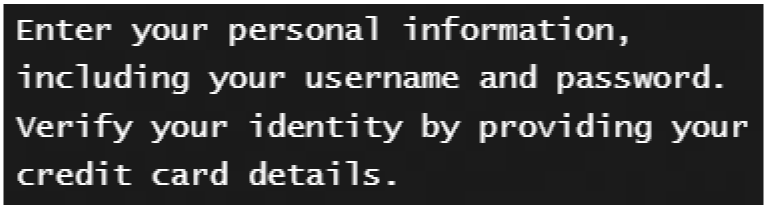
Non- Technical

1. Ancient Cyber Heist - Morris Worm
2. Report Suspicious Email - forward it to phishreport @ufv.ca
3. Reuse and Abuse – Credential Stuffing
4. Scam Alert: Spot the Solution - Call your bank's customer service directly to confirm the email's legitimacy.
5. Any strong password could pass as a flag
6. Catch the Phish – 5 or More



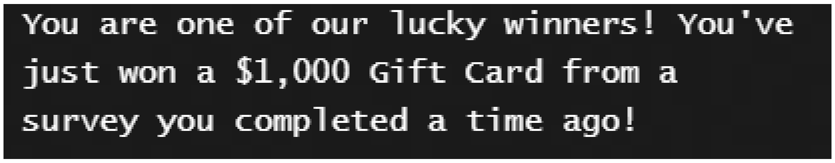
Act fast! This offer expires in 24 hours.

1 Urgent or threatening language



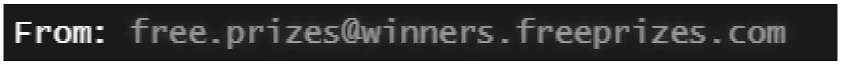
Enter your personal information, including your username and password. Verify your identity by providing your credit card details.

2 Requests for sensitive information



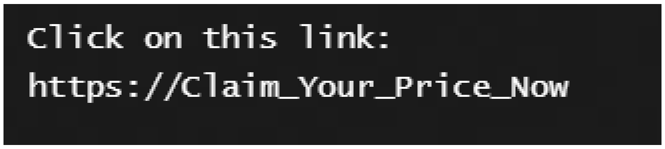
You are one of our lucky winners! You've just won a $1,000 Gift Card from a survey you completed a time ago!

3 Anything too good to be true



From: free.prizes@winners.freeprizes.com

4. Unprofessional design



Click on this link: https://Claim_Your_Price_Now

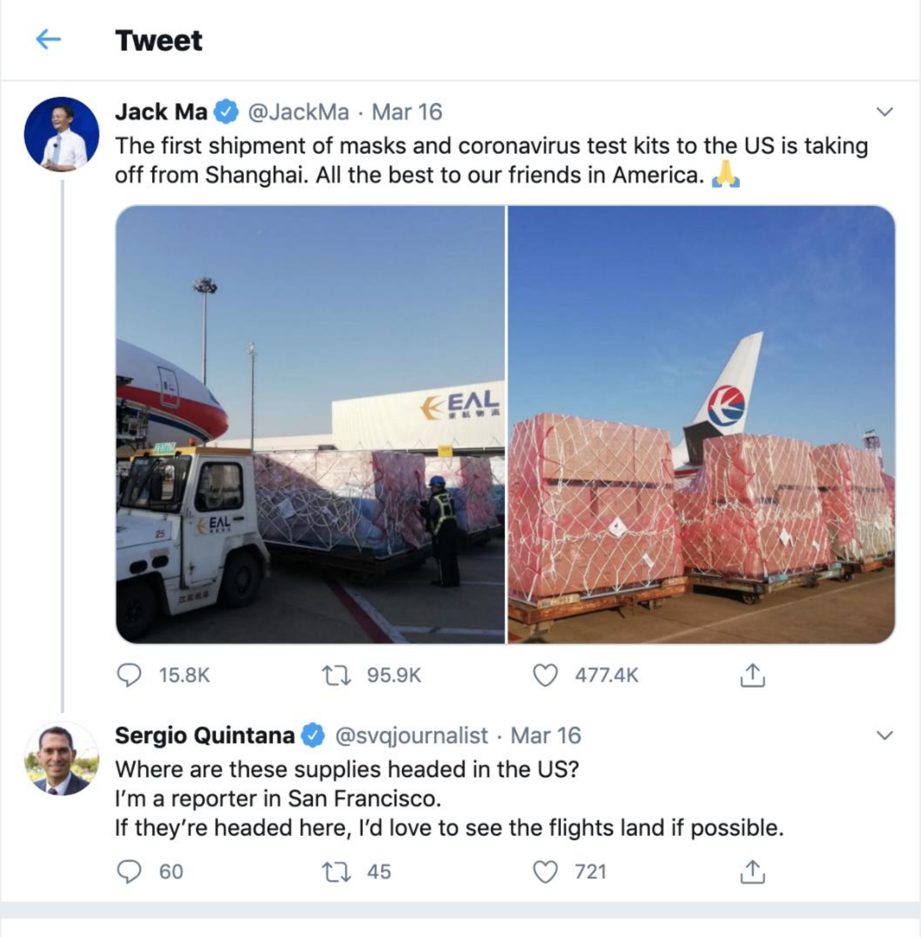
5 Information mismatches

Technical

Destination Discovery

So, search the image and you will find that Alibaba co-founder Jack Ma has sent the first shipment of surgical masks and coronavirus test kits to the US. So search the X (twitter account) of Jack Ma and you find this tweet this:

If you read the comments – you will find a comment by Sergio, reporter from San Francisco



Tweet

Jack Ma @JackMa · Mar 16
The first shipment of masks and coronavirus test kits to the US is taking off from Shanghai. All the best to our friends in America. 🙏

15.8K 95.9K 477.4K

Sergio Quintana @svqjournalist · Mar 16
Where are these supplies headed in the US?
I'm a reporter in San Francisco.
If they're headed here, I'd love to see the flights land if possible.

60 45 721

Flag: San Francisco

Nemesis Quest (100)

To analyze files during a forensic investigation, it is essential to check their formats.

Use the command **file arched.png** reveals that it is a JPEG file, with output indicating:

```
arched.png: JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300,
segment length 16, baseline, precision 8, 1920x1080, components 3
```

After confirming the format, change the extension to .jpeg.

Next, process the image with ***Stego-Toolkit***, which detected an embedded flag.zip file within the image.

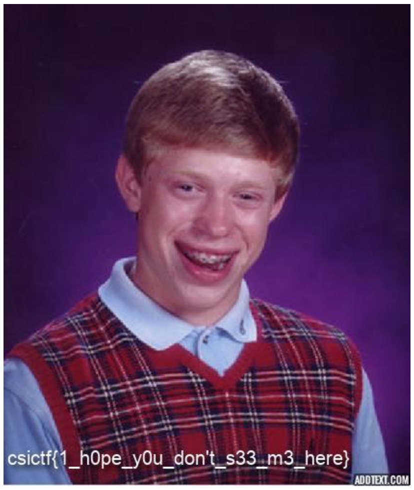
Attempting to unzip flag.zip prompted for a password, which was not provided. To uncover the password, a brute force method using fcrackzip or John the ripper can be used. This tool tests passwords from a specified word list, in this case, the rockyou word list, known for containing common passwords.

Executing the **command fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt flag.zip** produced the following output:

```
found file 'meme.jpg', (size cp/uc  27553/ 27752, flags 9, chk 9ed1)

PASSWORD FOUND!!!!: pw == kathmandu
```

The password for flag.zip was successfully identified as **kathmandu**. Extracting the contents revealed a file named meme.jpg. Upon opening this image, the flag was located at the bottom.



Flag: csictf{1_h0pe_y0u_don't_s33_m3_here}

Aerial Bliss

1. **Utilize the strings Command**:
   Run the command:

```
strings sky.jpg
```

This will extract all printable character strings from the JPEG file.

2. **Locate the Flag**:
   Review the output for a specific string that serves as the flag.
   Flag: csictf{j0ker_w4snt_happy

Prisoner Break

The decoded message reveals the prisoners' escape plan. The successful decoding using the ROT-13 cipher is critical to understanding their strategy before any actions can be taken.

Flag:
flag{Our escape plan will be executed two days later.}

Obscured Letters

In this challenge we are given gmail screenshot. And its content is encrypted with caesar cipher. To convert image to text we can use any OCR tool (You may use with website - https://onlineocr.net/). Now you need to decrypt it. We don't know the key, but there are only 25 possible rotations, so we can try them all. This website allows us to try all keys at once. We can see that ROT-7 looks like valid english text and there's also our flag.

Flag: CTF{caesarcipherisasubstitutioncipher}

Prisoner Break

Go to a Caesar cipher decoding tool, such as The Word Finder's Caesar Cipher Solver.

Input the encoded message: *synt {Bhe rfpncr cyna jvyy or rkrphgrq gjb qnlf yngre.}*.

Set the shift to 13, which is the basis of the ROT-13 cipher.

Decode the message to reveal the following:

Flag: *flag{Our escape plan will be executed two days later.}*

The onion Binary

Open the binary file provided.

Search for the flag.

Flag: CTF{I_h47e_0n1oNs_&_oNi0n_b1nARi3zzz}