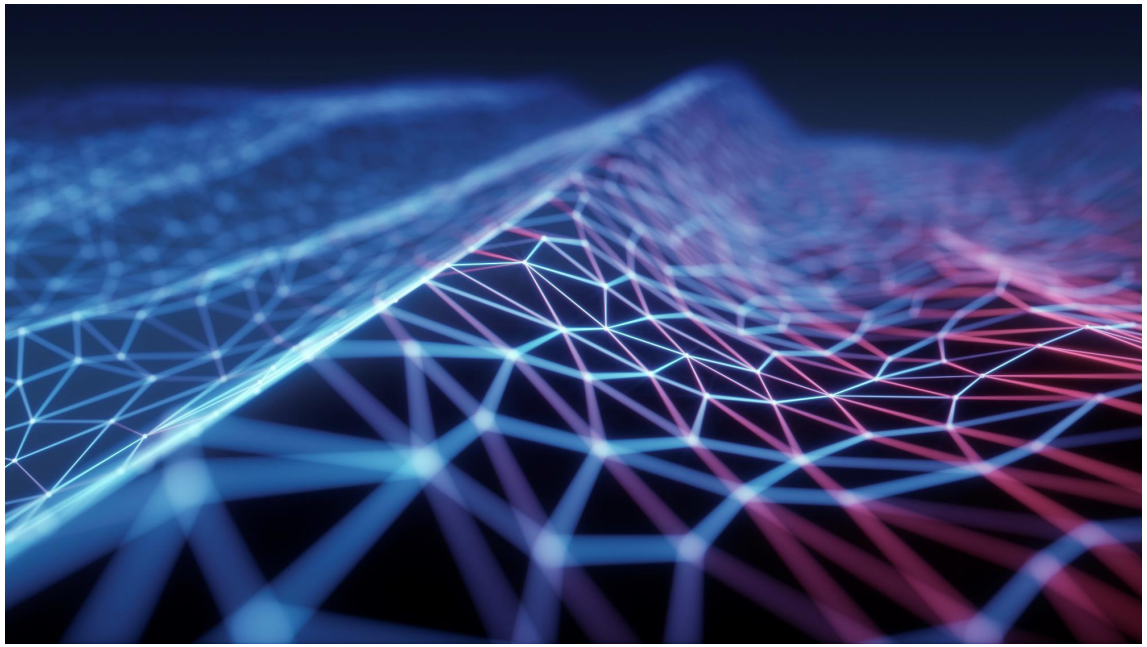


OUT IN TECH

FINAL PRESENTATION

RIPUNJAY SINGH

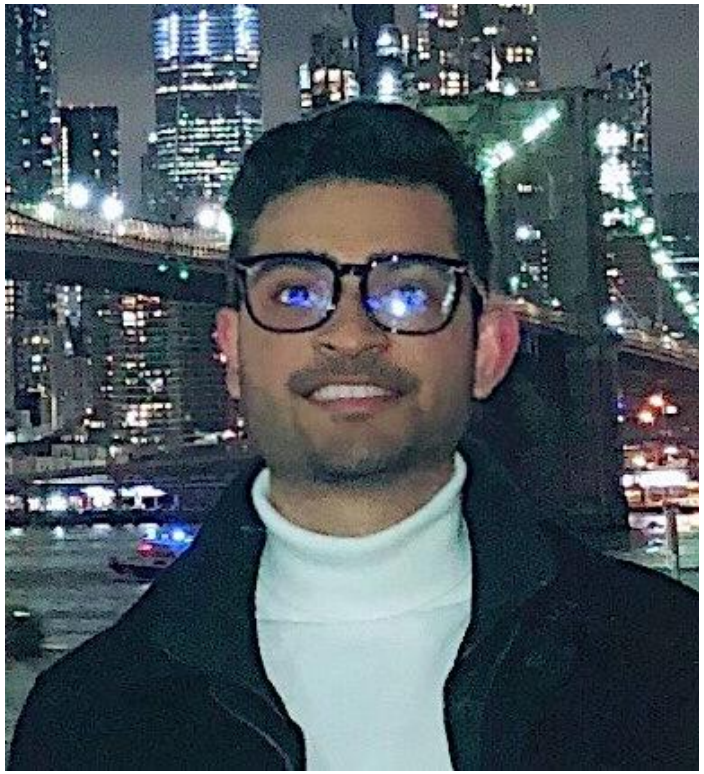
WHAT ARE WE DISCUSSING TODAY?

- INTRODUCTIONS
- EMAIL HEADERS
- EMAIL PHISHING
- EMAIL HEADER ANALYSER
- TECHNICAL SKILLS
- PROFESSIONAL SKILLS
- NEXT STEPS
- QUESTIONS

MENTOR
JOSEPH MCGINTY

- VP, SECURITY ANALYST AT MOELIS AND COMPANY
- PREVIOUS EXPERIENCES AT A LAW FIRM AND THE GOVERNMENT
- HOBBIES
  - CODING
  - REVERSE ENGINEERING
  - GAMING

MENTEE
RIPUNJAY SINGH



- STUDENT, NEW JERSEY CITY UNIVERSITY
- SENIOR, B.S COMPUTER SCIENCE
- HOBBIES
  - READING AND WRITING
  - TRAVELLING
  - CODING

EMAIL HEADERS

What are they?

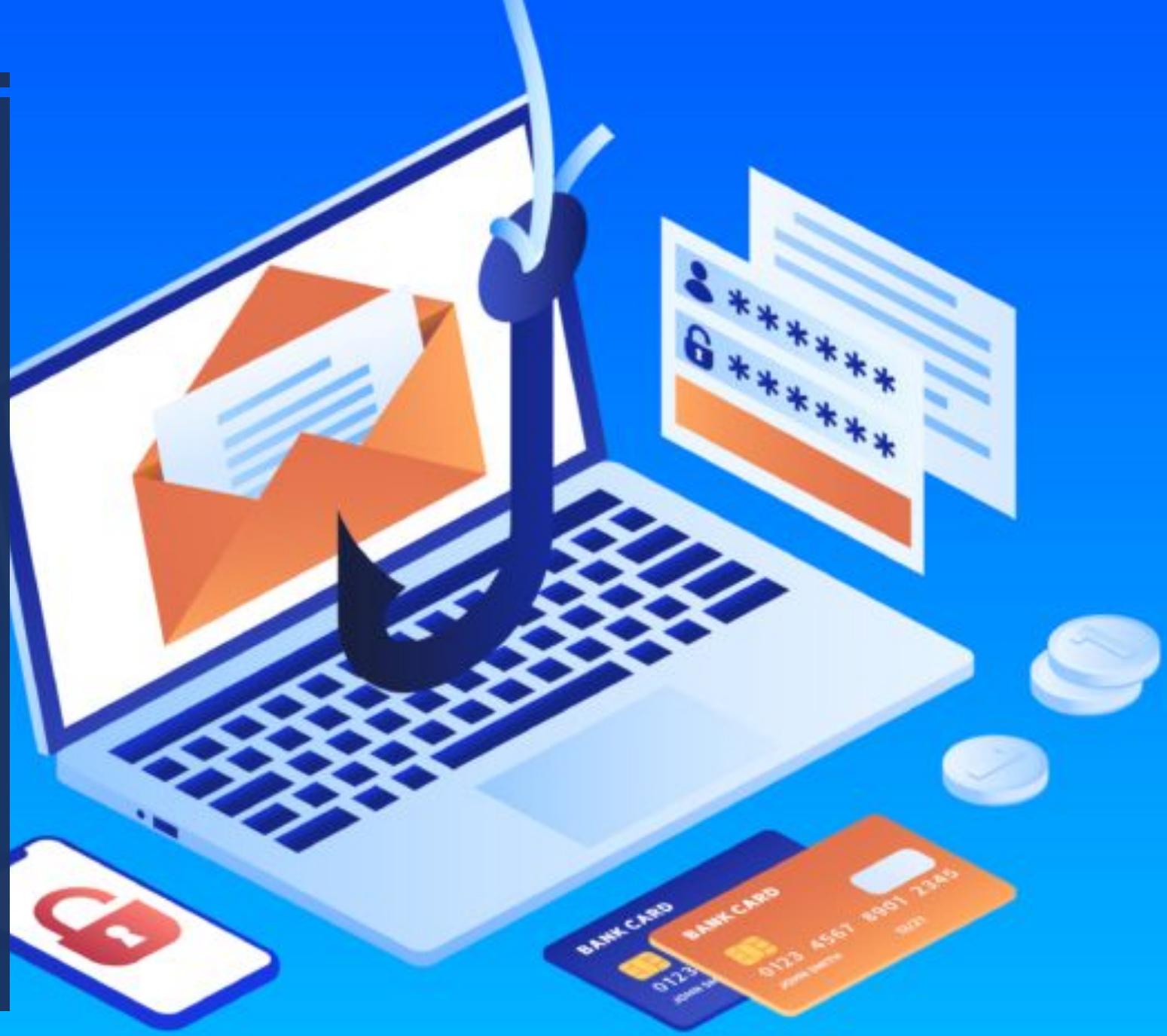
- The **email header** is the routing information for successfully delivering the email, that contains information about the sender, recipient, **email's** route to get to the inbox and various authentication details. The **email header** always precedes the **email** body.

Why are they important?

- The **email header** is important due to the following reasons:
  - Analysis to determine malicious attacks
  - Email tracking
  - Routing of information for successful transmission

EMAIL PHISHING

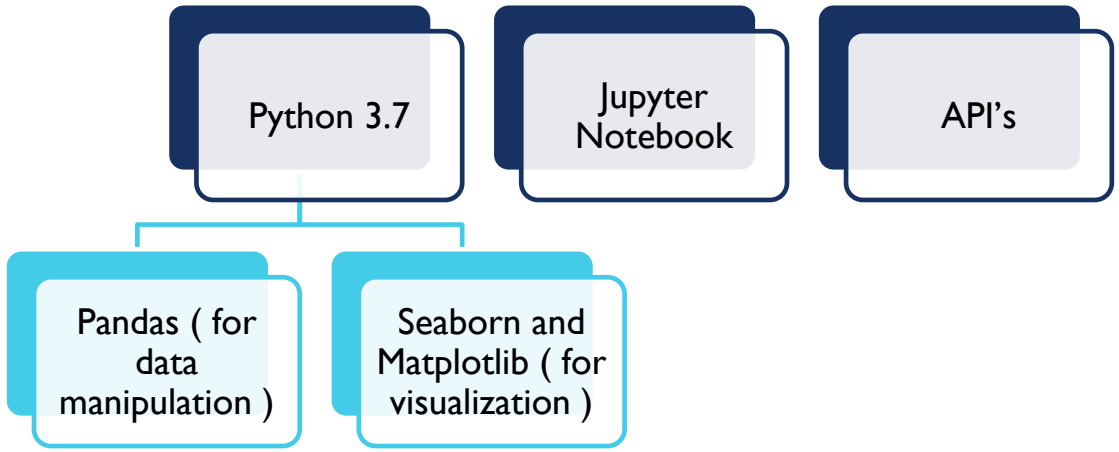
Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.



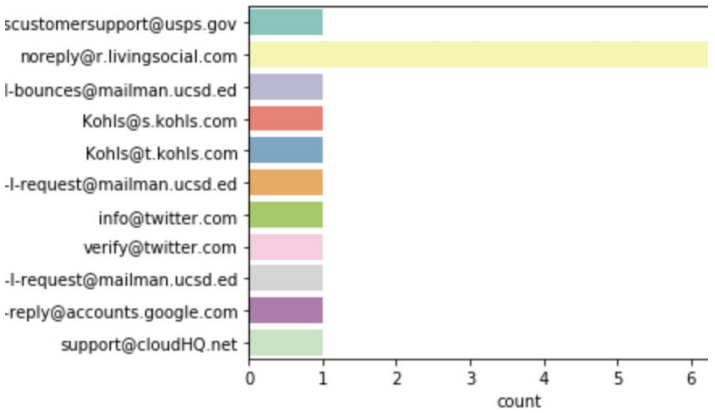
EMAIL_HEADER_ANALYSER

```
Delivered-To: rsingh17@saintpeters.edu
Received: by 2002:a50:2349:0:0:0:0:0 with SMTP id s9csp2731572ecg;
        Tue, 12 May 2020 03:44:52 -0700 (PDT)
X-Google-Smtp-Source: APiQypJnNXUWPkk7mSVEu76GbXN+1gfzlllAUOp1B9dlGEMHi+DZbAGTQGGWbZl+NvH+fpR2hfYG
X-Received: by 2002:a05:6402:793:: with SMTP id d19mr16811303edy.95.1589280292335;
        Tue, 12 May 2020 03:44:52 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1589280292; cv=none;
        d=google.com; s=arc-20160816;
        b=KGX2VcLRm57P4k3pbwuSWN56ixtUUj/6zvYnK+k06kiUxFPvklzzX0oP+4zr++46Ic
         GV2xg3orFxG0v8DMZmWfpd7MYX0QhNULYc69/qV82XfvpiYcrdRsPoJwhqUOV4xV9a6a
         Fp4g/tJcqVa5UZQ7YJFFUurJ9rY5zwxdXkPj7OV44kdLHUXrHUgjl29HQRT9MXxoY5Me
         20poWKLI+TdpgTashk0HBguID8CNJD/SPHFMwHyS62+PS2si4bOHsQYbOLES8dvjbVrH
         ZA5UNenlp+BF1m3N1zvLgpTQ8ThlN842akcg9OVmNaYl/hiBjBPixzM/qRcHlEXe8J1d
         TirA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:mime-version:from:date
         :content-transfer-encoding:dkim-signature;
        bh=YKhyEDxiESDtaw/stJxdjBYTh+4TgR5kUqisnVPfx7M=;
        b=XC9LQm9i3oH0BaaJTne20034X/kr07GDTjqw0dwbLdP/8A3Nzv8fXQ6lzO34lnH+bl
         9Vi4eTg9Y8zYFHmQHSbPEIyOmmCoxhGxZXt5ly9sZ0fXQeqiIF+3xLIHDjbT++AZFyzM
         7N216ulNftMWuMl6lyGqI1UieQapTyWon719bhQAXpdBiphIFbI12Hk7R9IW5dnkTxm/
         dS2C8P7vlYd+EYnsolkXhqd0Vf5rPDOD39Y7RMEsp/gFyTfGAFxIzMEoXXj19UFQPgLQ
         IZ8fSJuaBelmgH6aHSO2Z9g2WsV0ueucySMs6HB3b7xhCzI33VsQbRAB5ka4cx7PO+Q0
         B1IQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@barefootstudent.com header.s=m1 header.b=xGsr8gsY;
       spf=pass (google.com: domain of bounces+8243091-79b9-rsingh17=saintpeters.edu@em3469.barefootstudent.com designates
168.245.49.143 as permitted sender) smtp.mailfrom="bounces+8243091-79b9-rsingh17=saintpeters.edu@em3469.barefootstudent.com"
Return-Path: <bounces+8243091-79b9-rsingh17=saintpeters.edu@em3469.barefootstudent.com>
Received: from o1.emailalerts.barefootstudent.com (o1.emailalerts.barefootstudent.com. [168.245.49.143])
        by mx.google.com with ESMTPS id w18si2976604edv.185.2020.05.12.03.44.51
        for <rsingh17@saintpeters.edu>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Tue, 12 May 2020 03:44:52 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounces+8243091-79b9-rsingh17=saintpeters.edu@em3469.barefootstudent.com designates
168.245.49.143 as permitted sender) client-ip=168.245.49.143;
```

Tools Used



SNAPSHOTS



	SPAM_STATUS_FROM_'matrix.spfbl.net'	SPAM_STATUS_FROM_'zen.spamhaus.org'	FROM	IP_ADDRESS
0	This email server is currently clean.	IP: 50.115.223.158 is NOT listed in zen.spamha...	noreply@r.livingsocial.com	50.115.223.158
1	This email server is currently clean.	IP: 199.91.53.56 is NOT listed in zen.spamhaus...	noreply@r.livingsocial.com	199.91.53.56
2	This email server is currently clean.	IP: 199.91.53.20 is NOT listed in zen.spamhaus...	noreply@r.livingsocial.com	199.91.53.20
3	This email server is currently clean.	IP: 199.91.53.77 is NOT listed in zen.spamhaus...	noreply@r.livingsocial.com	199.91.53.77
4	This email server is currently clean.	IP: 50.115.223.113 is NOT listed in zen.spamha...	noreply@r.livingsocial.com	50.115.223.113

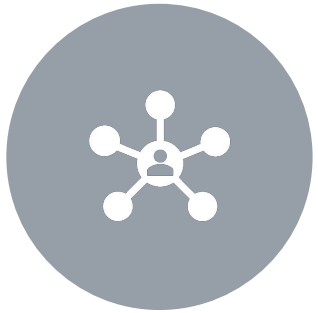

```
['This email server is currently clean.']
IP: 50.115.223.158 is NOT listed in zen.spamhaus.org
{
    "ip": "50.115.223.158",
    "success": true,
    "type": "IPv4",
    "continent": "North America",
    "continent_code": "NA",
    "country": "United States",
    "country_code": "US",
    "country_flag": "https://cdn.ipwhois.io/flags/us.svg",
    "country_capital": "Washington",
    "country_phone": "+1",
    "country_neighbours": "CA,MX,CU",
    "region": "California",
    "city": "San Jose",
    "latitude": "37.3382082",
    "longitude": "-121.8863286",
    "asn": "AS12269",
    "org": "Groupon, Inc.",
    "isp": "Groupon, Inc.",
    "timezone": "America/Los_Angeles",
    "timezone_name": "Pacific Standard Time",
    "timezone_dstOffset": "0",
    "timezone_gmtOffset": "-28800",
    "timezone_gmt": "GMT -8:00",
    "currency": "US Dollar",
    "currency_code": "USD",
    "currency_symbol": "$",
    "currency_rates": "1",
    "currency_plural": "US dollars",
    "completed_requests": 33
}
IP from where it was sent : 50.115.223.158
```

TECHNICAL SKILLS

- CIS BENCHMARKS
- FIREWALLS
- MITRE ATT&CK FRAMEWORK
- RFC
- DNS Blacklists
- OWASP
- WINDOWS EVENTS
- HOST FIREWALL/AV
- DATA SCIENCE
- USING MATPLOTLIB AND SEABORN TO VISUALIZE DATA

LinkedIn Tips to gather more views and be up in recruiter searches

Resume tips to make sure that all the information is clear



Networking techniques that will assist in connecting with recruiters and making sure the interest is displayed

Interview preparation techniques

PROFESSIONAL SKILLS

NEXT STEPS

1

CREATE A GUI

2

ADD MORE DETAILS TO GEOLOCATION DATA

3

AUTOMATE THE PROCESS AND STORE DATA ON A DAILY BASIS

THANK YOU

ANY QUESTION?