Email Security

Jitendra Kumar

Joint Director CDAC Bangalore

What is email security?

- Process of preventing email-based cyber attacks and protecting against unwanted communications. It may comprise the following
  - Protecting inboxes from takeover
  - Protecting domains from spoofing
  - Stopping phishing attacks
  - Preventing fraud
  - Blocking malware delivery
  - Filtering spam
  - Use of encryption to protect the contents of emails from unauthorized access.
- Includes the techniques and technologies used to protect email accounts and communications.
- Email has the organization’s largest attack surface
  - Primary target of phishing attacks
  - Can be used to spread malware

Major concern with email

- Security and privacy were not built at the time it was first invented
  - still not built into email by default
- Open format can be read on any device without decryption once it is intercepted.
- Normally message contents are not secured
  - Can be read/modified either in transit or at destination by the attacker
- E-mail service is like postcard service
  - just pick it up and read it
- Major attack vector for organizations large and small, and for individual people as well.

Major concern with email contd..

- Email is a top threat vector because it is a ubiquitous tool that everyone in an organization uses.
- Does not go straight to the recipient before landing in an inbox
    - Travels between networks and servers
        - Some may be vulnerable and unsecured.
        - Some may even be compromised even though the individual computer is secured.
- Cyber criminals can easily impersonate a sender
    - Can manipulate email content body, attachments, Uniform Resource Locators (URLs), or a sender’s email address.
    - Can manipulate the email headers containing information about the sender and recipients
    - Can change the metadata and forged email may give the impression of mail coming from a reputable entity

What kinds of attacks occur via email?

- Fraud
  - Aim to trick large enterprise accounting departments into transferring money to illegitimate accounts.
  - With the use of domain spoofing the attacker can easily vouch for a legitimate person or entity
- Phishing
  - A phishing is an attempt to steal sensitive information, for example, username, password, etc.
  - Direct users to a fake webpage that collects credentials
  - Create urgency and pressure to send the information to an email address secretly controlled by the attacker.
  - Domain spoofing is also common in such attacks
- Malware
  - Malicious code delivered over email include spyware, scareware, adware, and ransomware, among others.
  - For example, through an email attachment that contains malicious code

What kinds of attacks occur via email? contd..

- Account takeover for malicious purposes
  - such as monitoring their messages
  - stealing information
  - To forward malware attacks and spam to their contacts.
- Email interception
  - To steal the information
  - To carry out on-path attacks in which attackers impersonate both sides of a conversation to each other.
  - Generally done using monitoring network data packets on LANs.
- Spoofing
  - Spoofing involves fooling the recipient into thinking the email is coming from someone other than the apparent sender.

Email domain spoofing

- Allows attackers to send messages from legitimate-seeming addresses.
- Allows attackers to send an email with a forged "from" address
  - For example, an attacker can forge the “From” address that represent a trustable entity

What is a phishing attack?

- Phishing is an attempt to steal sensitive data
  - Usernames, passwords, other important account information, etc.
  - Phisher can use them to take over the user's accounts with their password or sells the stolen information.
- Attackers disguise themselves as a reputable entity.
- Bait the victims with an enticing or seemingly urgent request
  - Attacker lures the victim into providing information, just as a person uses bait while fishing.
- Phishers trick people into emailing sensitive information directly
  - Or through links to a webpage, they control

There are several types of phishing:

- Spear phishing is highly targeted and often personalized to be more convincing.
- Whaling targets important or influential persons within an organization, such as executives.
- Non-email phishing attacks include vishing (phishing via phone call), smishing (phishing via text message), and social media phishing.

Blocking phishing attacks

- Email security solutions can
  - Filter out emails from known bad IP addresses.
  - Block or remove links embedded within emails
  - Use DNS filtering to block phishing webpage
- An organization's employees should receive training on how to recognize a phishing email.
- Many email providers have some built-in phishing protection
  - However, phishing emails still regularly sneak into user inboxes.
- Many organizations employ additional phishing protection to better defend their users and networks.

How are email attachments used in attacks?

- Attaching the malicious software as an exe file, then tricking the recipient into opening the attachment.
- Common approach is to conceal malicious code within an innocent-seeming document, like a PDF or a Word file.
    - Both these file types support the inclusion of code such as macros
- Many ransomware infections in recent years have started with an email attachment
    - Ryuk ransomware often enters a network through a TrickBot or Emotet infection through attachments
    - Maze ransomware
    - Petya ransomware

What is spam and how to tackle it?

- Spam is a term for unwanted or inappropriate email messages, sent without the recipient's permission.
- Almost all email providers offer some degree of spam filtering.
  - Still some spam messages still reach user inboxes.
- Individuals and organizations can take several approaches to cut down on the spam they receive.
  - Reduce or eliminate public listings of their email addresses.
  - Can implement a third-party spam filter on top of the filtering provided by their email service.
  - Consistently mark spam emails as spam, in order to better train the filtering
  - If a large percentage of a sender’s emails are unopened or marked as spam or bounce too much
    - ISPs and email services downgrade email sender reputation

Email accounts takeover

- Attackers can use several methods to break into an email account:
    - Purchasing lists of previously stolen credentials
    - Brute force attacks: The attacker loads a login page and uses a bot to rapidly guess a user's credentials.
        - limits on password entry can effectively stop such attacks.
    - Phishing attacks
    - Web browser infections
    - Spyware
- Using multi-factor authentication (MFA) instead of single-factor password authentication is one way to protect inboxes from compromise.
- Usage of single sign-on (SSO) service instead of logging directly into email.

How do DNS records help prevent email attacks?

- The Domain Name System (DNS) stores public records about a domain, including that domain's IP address.
- There are specialized types of DNS records that help ensure emails are from a legitimate source, not an impersonator: SPF records, DKIM records, and DMARC records.
- Email service providers check emails against all three of these records to see if they are from the place they claim to be from and have not been altered in transit.

Email Security Best Practices

- Spam filter
- Email Encryption
- Antivirus protection
- Secure email gateway (SEG)
- Multi-factor authentication (MFA)
- Employee education
  - Educate the to recognize social engineering, phishing, and other types of attacks

Do

- ALWAYS… check the email “from” field to validate the sender.
  - This “from” address can be easily spoofed
- ALWAYS… check for files with a “double extension”. Although a text file named “safe.txt” is safe, a file called “safe.txt.exe” is not.
- ALWAYS… report suspicious emails to your Information Technology support(ITS) team, or engage them for guidance before proceeding
- ALWAYS… look closely at website addresses (URL) that are included in an email

DON’T

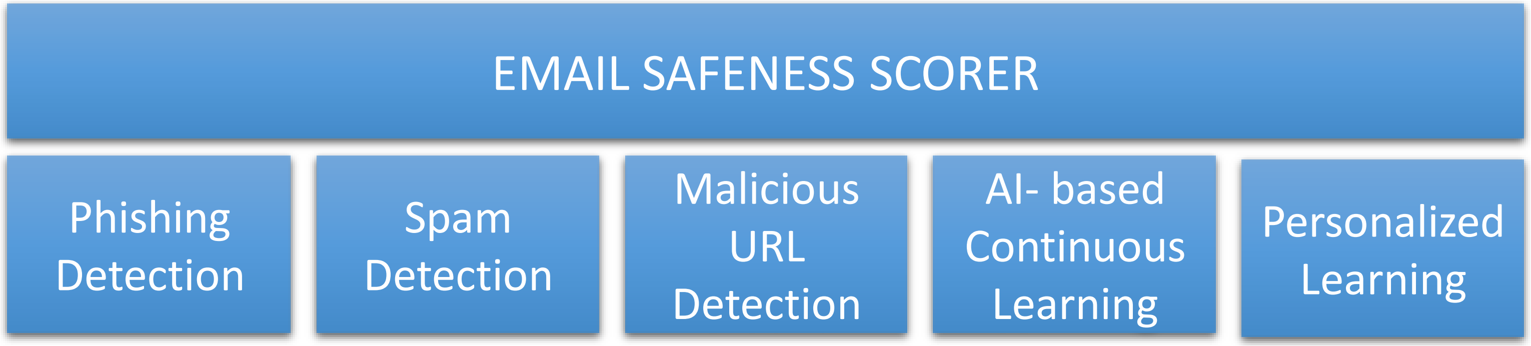
- DO NOT… open any email attachments that end with .exe, .scr, .bat, .com, or other executable files that you do not recognize.
  - Be very cautious about opening MS Word, MS Excel, and Adobe PDF files.
- DO NOT… ever click embedded hyperlinks within email messages without first hovering your mouse over them to see where they will take you
- DO NOT… respond or reply to spam in any way.
  - Instead mark the email as “SPAM” or “junk” in their email client
  - Else work with your IT department to adjust your SPAM filter to capture emails from this sender in the future.
- DO NOT… “unsubscribe” – it’s easier to mark the email as “SPAM” or “Junk” than deal with the security risks associated with clicking on the “unsubscribe” link or responding to an email.

5 REASONS WHY UNSUBSCRIBING IS A BAD IDEA:

- By clicking the link or responding via email you have confirmed to the sender that your email address is both valid and in active use.
- By responding to the email, you have positively confirmed that you have opened and read it
  - may be slightly interested in the subject matter
- By clicking unsubscribe and responding you are confirming that your email is active and information about email software too.
- If the response opens in a browser window and by visiting the spammer’s website, you may end up sharing your geographic location (calculated based on IP address), OS, and browser information.
- if you visit a website owned by a spammer, you’re giving them a chance to install malware on your computer, even if you don’t click anything.

AI/ML Based Email Safeness Scorer

- Email Safeness Scorer
  - A privacy-preserving machine learning-based client-side tool to provide a safeness score of an email for alerting the user about possible phishing, scam, etc.
  - AI-based aggregated global model for alerting users about unsafe emails and work non intrusively i.e., available as a plug-in for the Mozilla Thunderbird
  - Available at https://coednssecurity.in/#resources



EMAIL SAFENESS SCORER

Phishing Detection

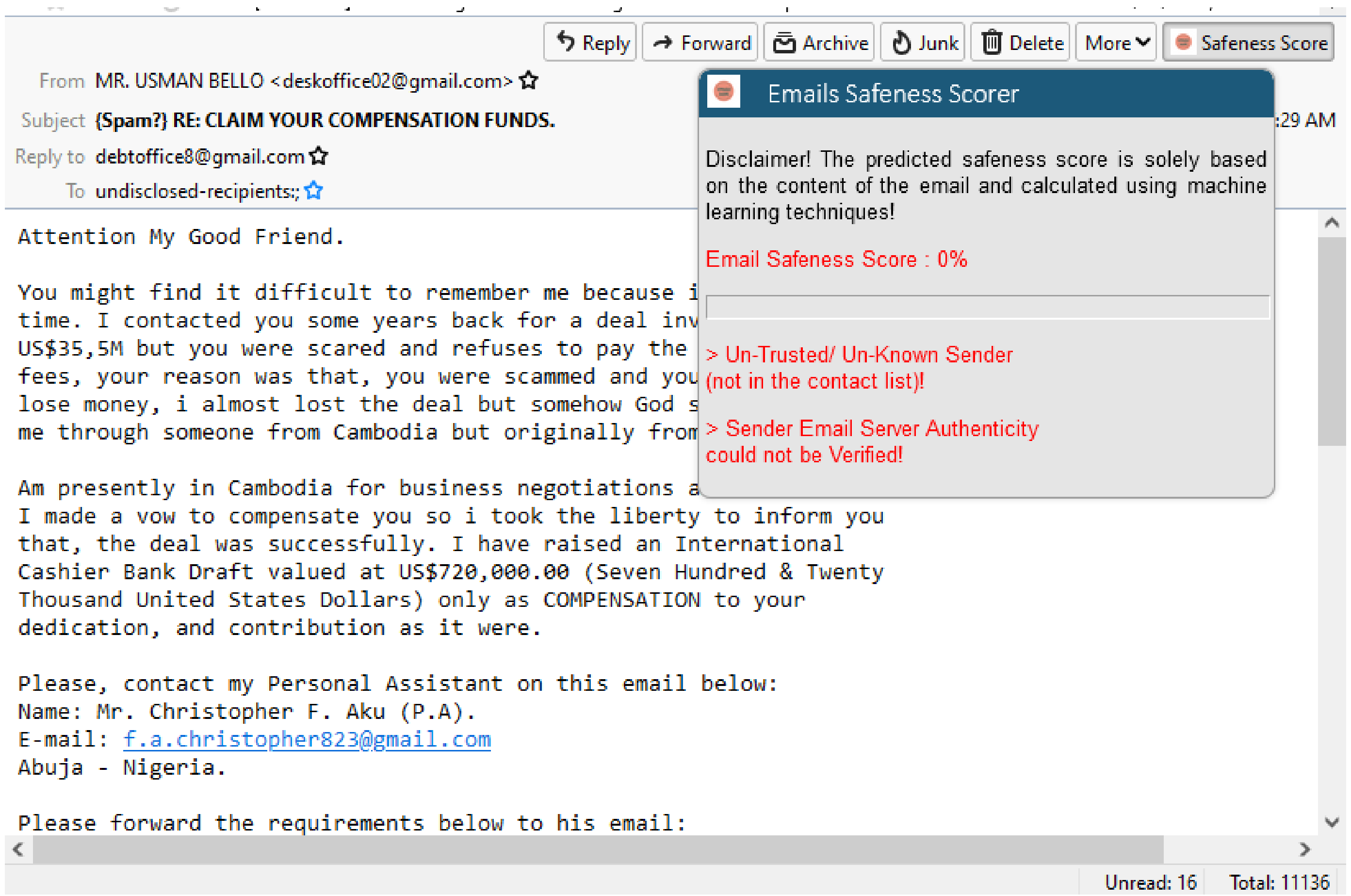
Spam Detection

Malicious URL Detection

AI- based Continuous Learning

Personalized Learning

A screenshot



From MR. USMAN BELLO <deskoffice02@gmail.com>

Subject {Spam?} RE: CLAIM YOUR COMPENSATION FUNDS.

Reply to debtoffice8@gmail.com

To undisclosed-recipients:;

:29 AM

Emails Safeness Scorer

Disclaimer! The predicted safeness score is solely based on the content of the email and calculated using machine learning techniques!

Email Safeness Score : 0%

> Un-Trusted/ Un-Known Sender (not in the contact list)!

> Sender Email Server Authenticity could not be Verified!

```
Attention My Good Friend.

You might find it difficult to remember me because i
time. I contacted you some years back for a deal inv
US$35,5M but you were scared and refuses to pay the
fees, your reason was that, you were scammed and you
lose money, i almost lost the deal but somehow God s
me through someone from Cambodia but originally from

Am presently in Cambodia for business negotiations a
I made a vow to compensate you so i took the liberty to inform you
that, the deal was successfully. I have raised an International
Cashier Bank Draft valued at US$720,000.00 (Seven Hundred & Twenty
Thousand United States Dollars) only as COMPENSATION to your
dedication, and contribution as it were.

Please, contact my Personal Assistant on this email below:
Name: Mr. Christopher F. Aku (P.A).
E-mail: f.a.christopher823@gmail.com
Abuja - Nigeria.

Please forward the requirements below to his email:
```

Unread: 16 Total: 11136

Thank You