



Phishing E-mails

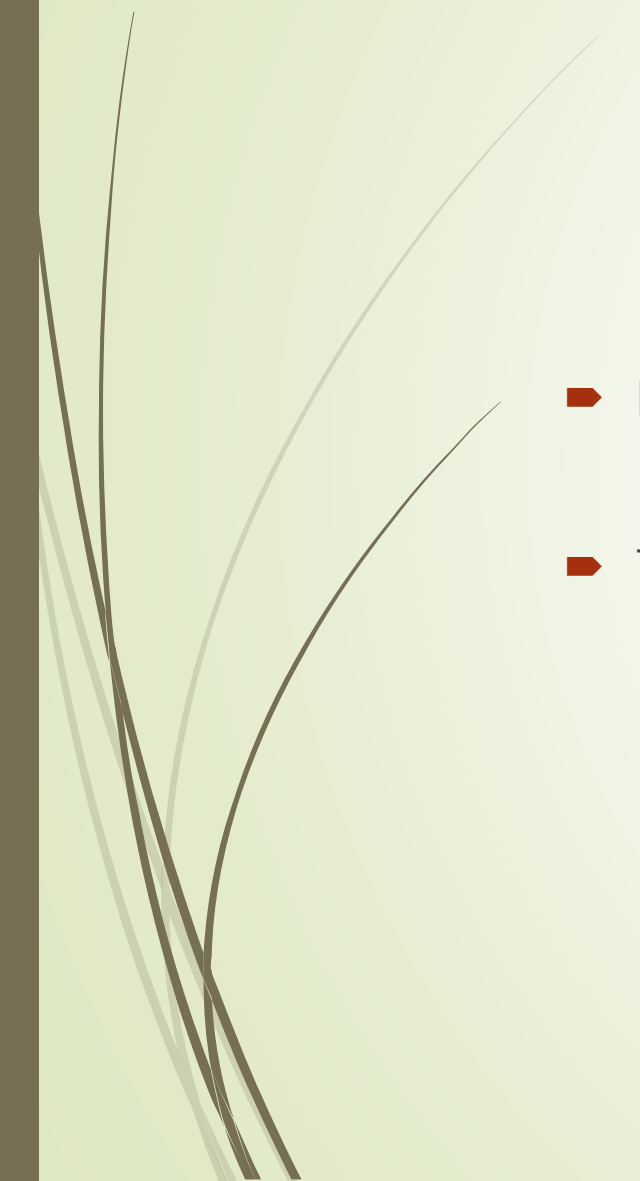


Topics

- Understand E-mail Security Incidents
- Explain different types of E-mail attacks and their impacts
- Discuss the preparation required to handle E-mail incidents
- Identify email attack indicator
- Detect phishing and spam mails
- Contain email attacks
- Device methods of eradicating email incidents
- Explain steps to follow to recover after email incidents



Overview of Email Security Incidents

- Introduction to Email Security Incidents
 - Types of Email Incidents
- 


Spamming

- Spam refers to undesired emails used to distribute malicious links and attachments, cause network congestion, perform phishing and financial frauds and so on.
- The spam may also consume bandwidth of the email servers causing DoS conditions.
- In the example the email address doesn't match the sender name or the content of message

<input type="checkbox"/>	☆	▷	R... (n) 2	24 Hours Left 🤖 Grab The Deal - Upto ...	Dec 7
<input type="checkbox"/>	☆	▷	S...	You have coupon worth Rs 200 inside. ...	Dec 6
<input type="checkbox"/>	☆	▷	F... (n) 2	Surprise Sale 🤖 A Deal Not to Miss 🤖 -	Dec 4
<input type="checkbox"/>	☆	▷	C... ra.	Save Big Up to 70% on your Car Insura...	Dec 3
<input type="checkbox"/>	☆	▷	R... (n) 2	Cyber Monday Sale Extended 🤖 - Cyb...	Nov 28
<input type="checkbox"/>	☆	▷	S...	Hurry! offer expiring today. Use Code: ...	Nov 27
<input type="checkbox"/>	☆	▷	T...	Pre-qualified* top-up loan on your 🚗 ...	Nov 23
<input type="checkbox"/>	☆	▷	D... ar	Choosing great stocks now - View this i...	Nov 22
<input type="checkbox"/>	☆	▷	M... s	You are missing out online! Property D...	Nov 22
<input type="checkbox"/>	☆	▷	D... k	🔒 Closing Tonight (Hindi Blogging Co...	Nov 19
<input type="checkbox"/>	☆	▷	U... R	Don't seize the day! - Especially not if'...	Nov 18

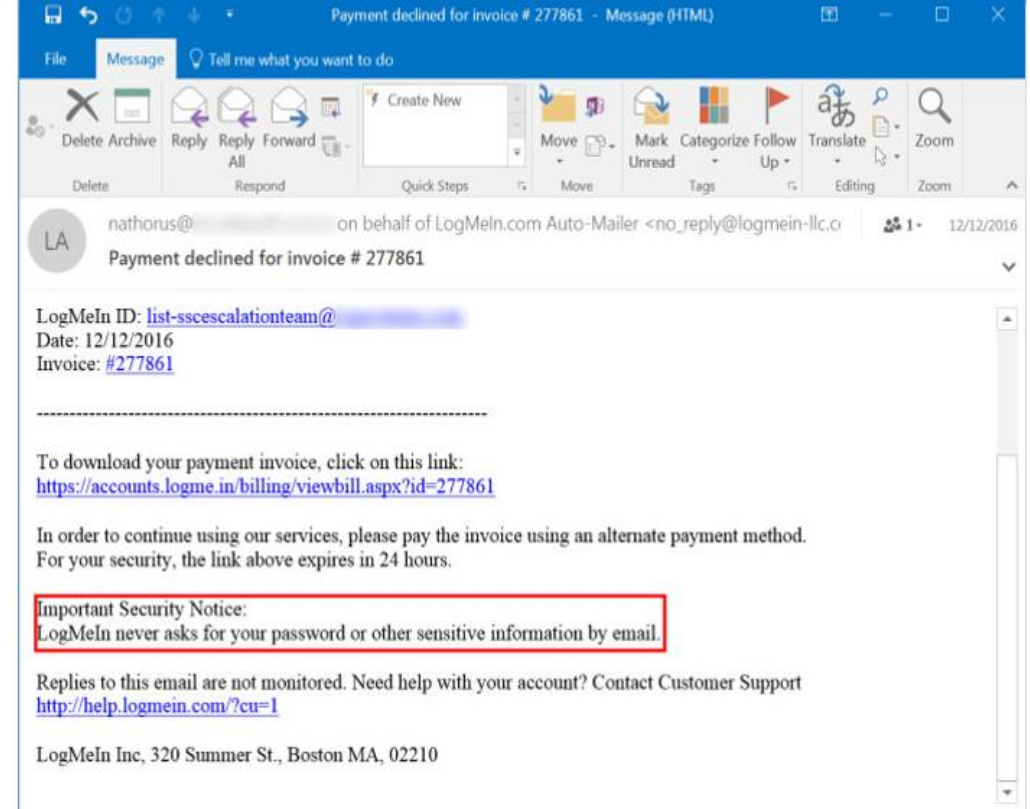
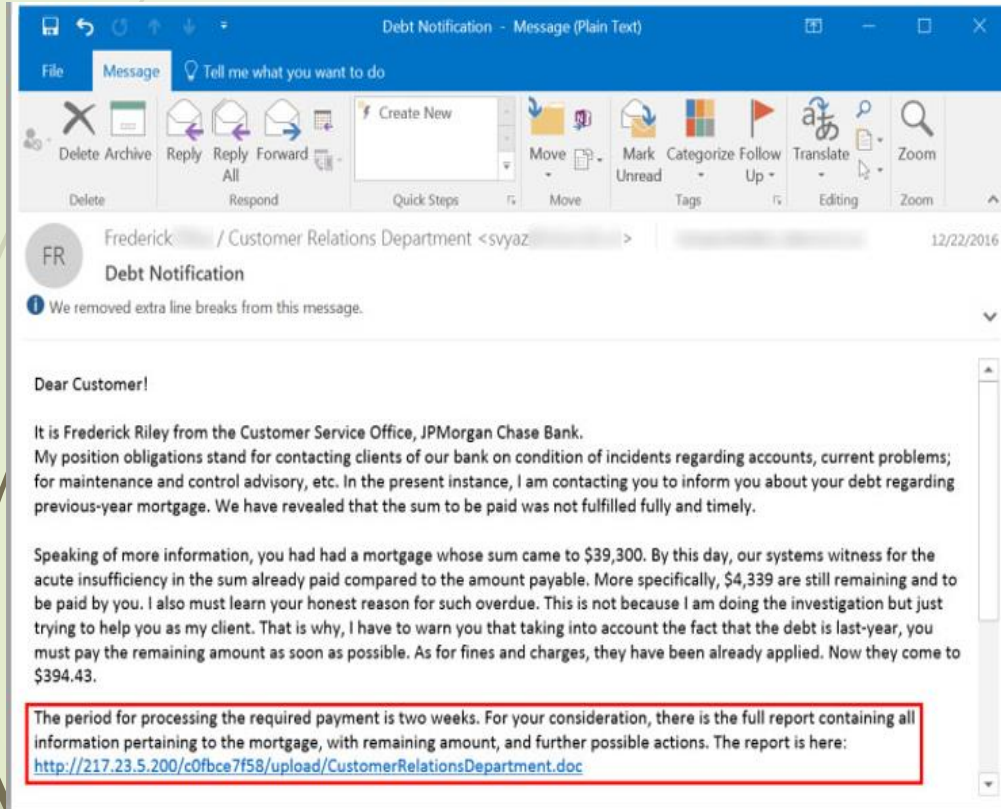


Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
 - The information is then used to access important accounts and can result in identity theft and financial loss.
- 

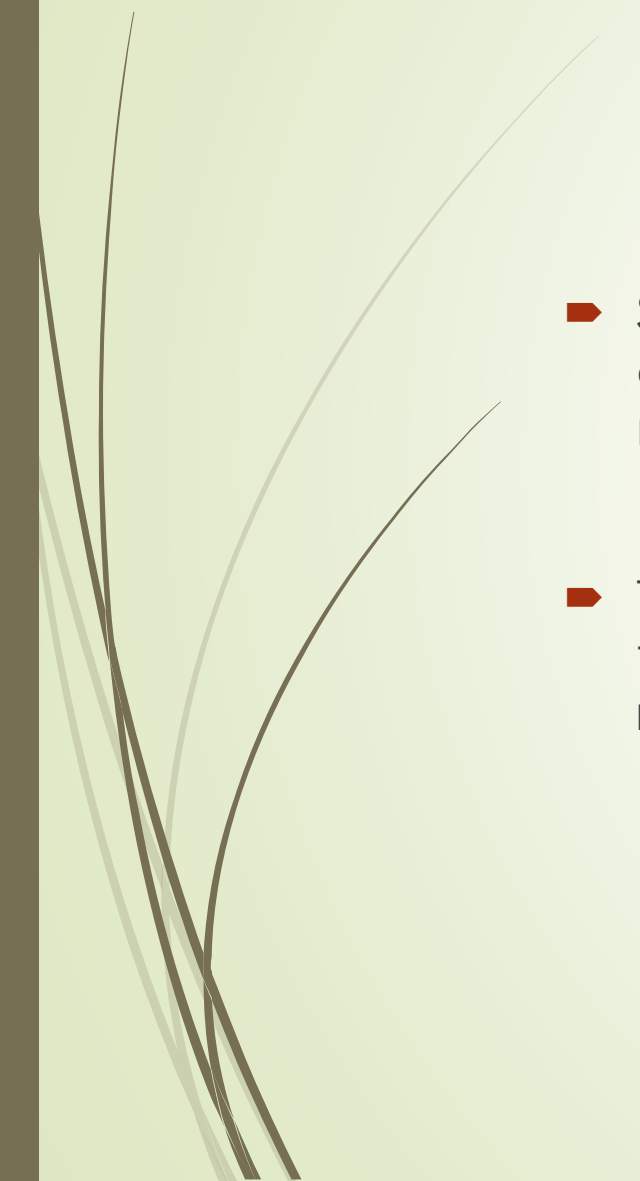
Examples of phishing

- Phishing involves fraudulently acquiring sensitive information (e.g., passwords, credit cards) by masquerading as a trusted entity.

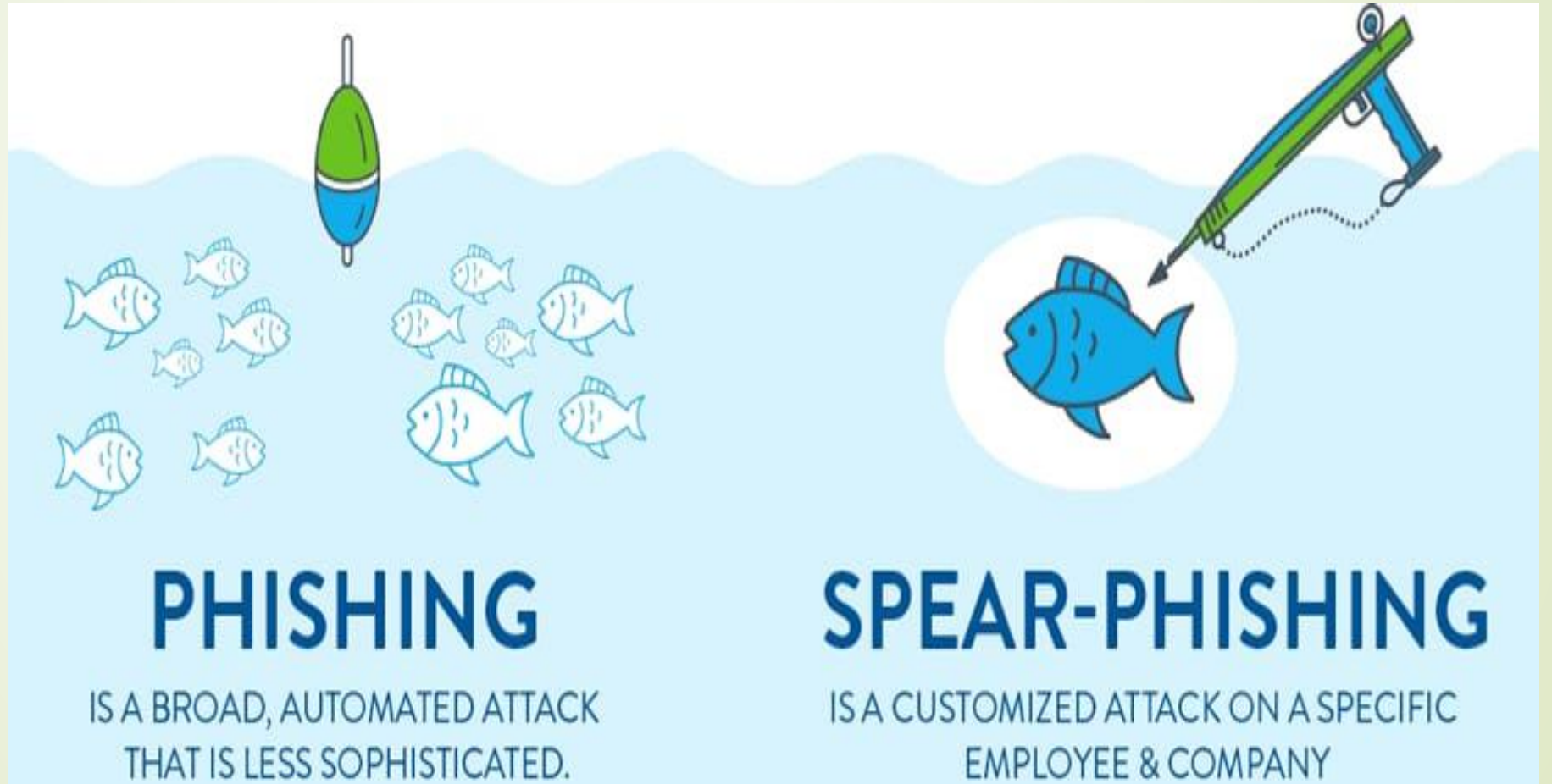




SPEAR-PHISHING

- Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.
 - This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online.
- 

SPEAR-PHISHING VS. PHISHING





Preparation for Handling Email Security Incidents

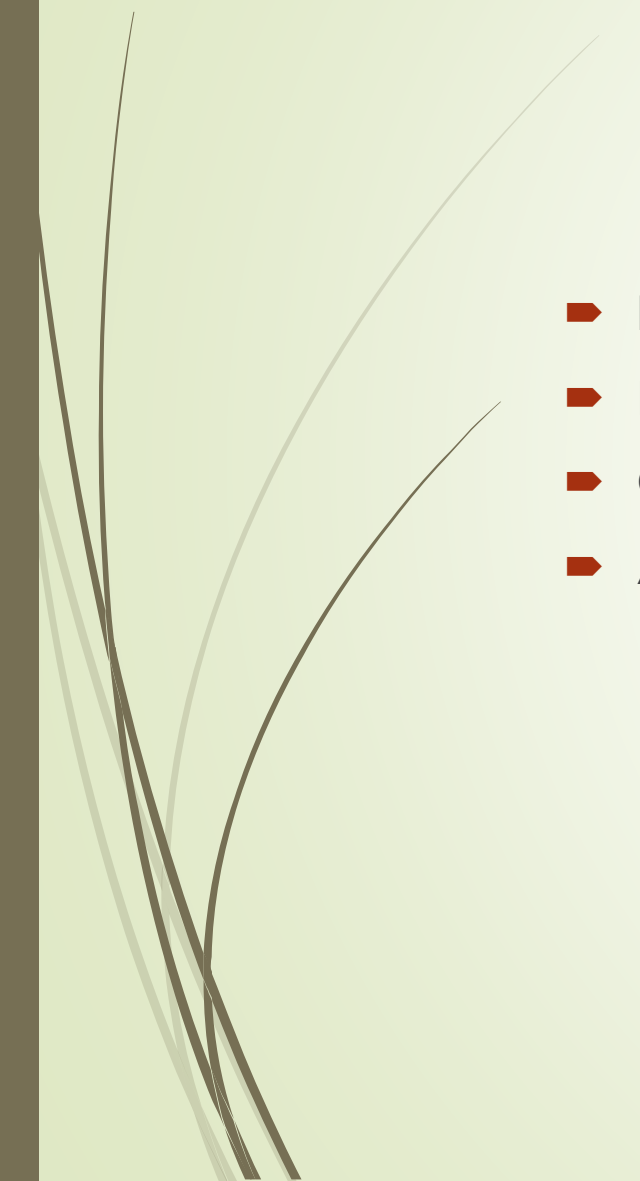


Preparation

- Email Filtering
- Email monitoring tools
- Communication
- Training and awareness to employees
- Acceptable usage policy
- Local archive or backups
- Email logs analysis tools



Detection and Containment of Email Security Incidents

- Indicators of Email attack
 - Detecting Phishing/Spam emails
 - Containing Email incidents
 - Analyzing Email Headers
- 



Indications of Email Attacks

- Unavailability of the email server.
- Inability to access the system or the email accounts after opening an email.
- System showing signs of malware attack after opening a link or attachment from an email such as finding suspicious process running on your system.
- Sudden increase of advertising and spam emails.
- Change to the theme or interface of the email web page.

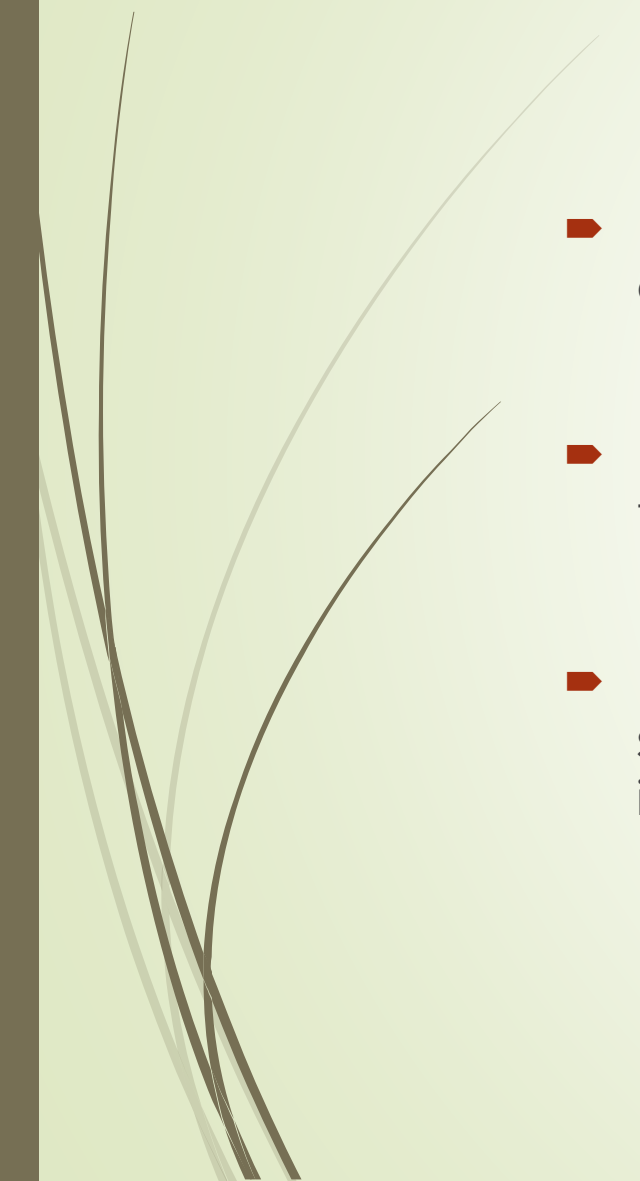


Detecting Phishing/Spam Emails

- Unexpected attachment from user, client, vendor, or peers.
- Attachments with unusual or unrecognized formats.
- Difference in the email ID of the sender and display name.
- Email format IDs that don't have incomplete or incorrect organization name or use numbers in the place of letters in the name.
- Having generic greetings such as dear customers.



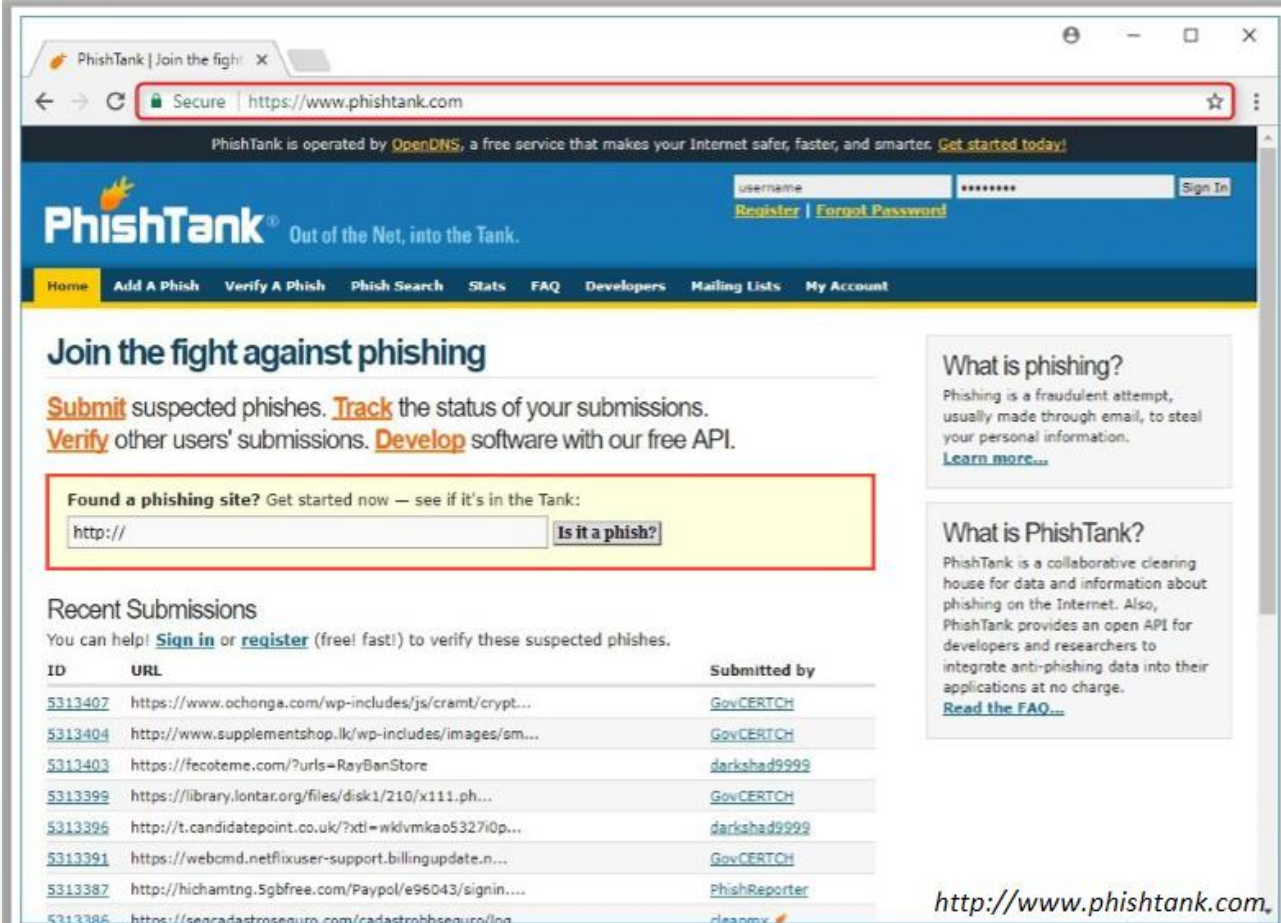
Detecting Phishing/Spam Emails

- 
- Emails with links, which display a different website or URL when hovered on or have URL with incorrect name or domain
 - Emails presenting offers that are too attractive to believe, such as winning the lottery, a competition, a free subscription, vacation, and job offers.
 - Emails that seem to be from user's bank, financial institution, organization, service provider, and other associate, which ask to reveal sensitive information or login to their accounts using provided links or install updates.

Tools for Detecting Phishing/Spam mails

➤ PhishTank

- Phishtank is a collaborative clearing house for data and information about phishing on the internet.
- It provides an open API for developers and researchers to integrate antiphishing data into their application.
- It helps in detecting phishing and spam emails easier as API is available for all developers.



PhishTank | Join the fight

Secure | <https://www.phishtank.com>

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

PhishTank® Out of the Net, into the Tank.

username [Sign In](#)
[Register](#) | [Forgot Password](#)

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
5313407	https://www.ochonga.com/wp-includes/js/cramt/crypt...	GovCERTCH
5313404	http://www.supplementsshop.lk/wp-includes/images/sm...	GovCERTCH
5313403	https://fecoteme.com/?urls=RayBanStore	darkshad9999
5313399	https://library.lontar.org/files/disk1/210/x111.ph...	GovCERTCH
5313396	http://t.candidatepoint.co.uk/?xtl=wklvmkao5327iOp...	darkshad9999
5313391	https://webcmd.netflixuser-support.billingupdate.n...	GovCERTCH
5313387	http://hichamtng.5gbfree.com/Paypol/e96043/signin...	PhishReporter
5313386	https://seccadastresequo.com/cadastrobhsequo/loq	cleanmy

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
[Learn more...](#)

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
[Read the FAQ...](#)

<http://www.phishtank.com>



Containing Email Incidents

- Isolate the targeted system from the functional network immediately after receiving the incident report.
- Interview the users or compliment about the email incident to find details of the attack and user actions.
- Ask if the user had downloaded the attachment, clicked the link, provided the requested information, and so on.

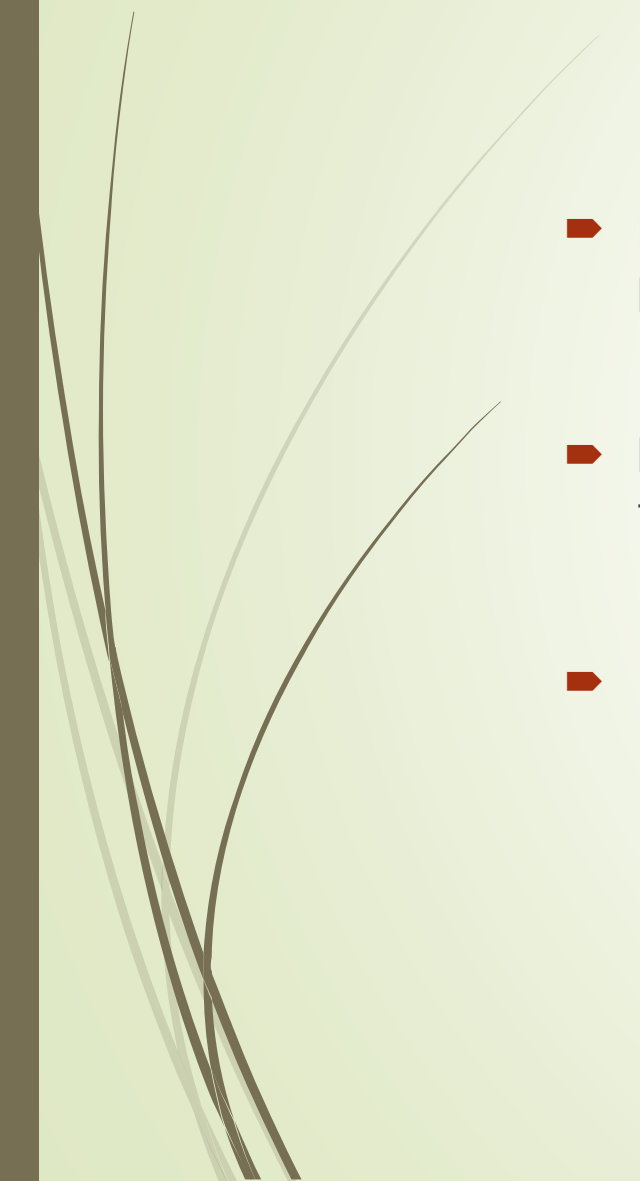


Containing Email Incidents

- If the email consist of links, find further details of the link by opening it in a sand box environment to perform behavior analysis.
- Report and block the malicious links in the server, network devices, and across all security solutions.
- In case of malicious attachment sent through email , incident responders must open the email account in sandbox environment, download the attachment and perform behavior analysis of the system and check if it has malicious code.



Containing Email Incidents

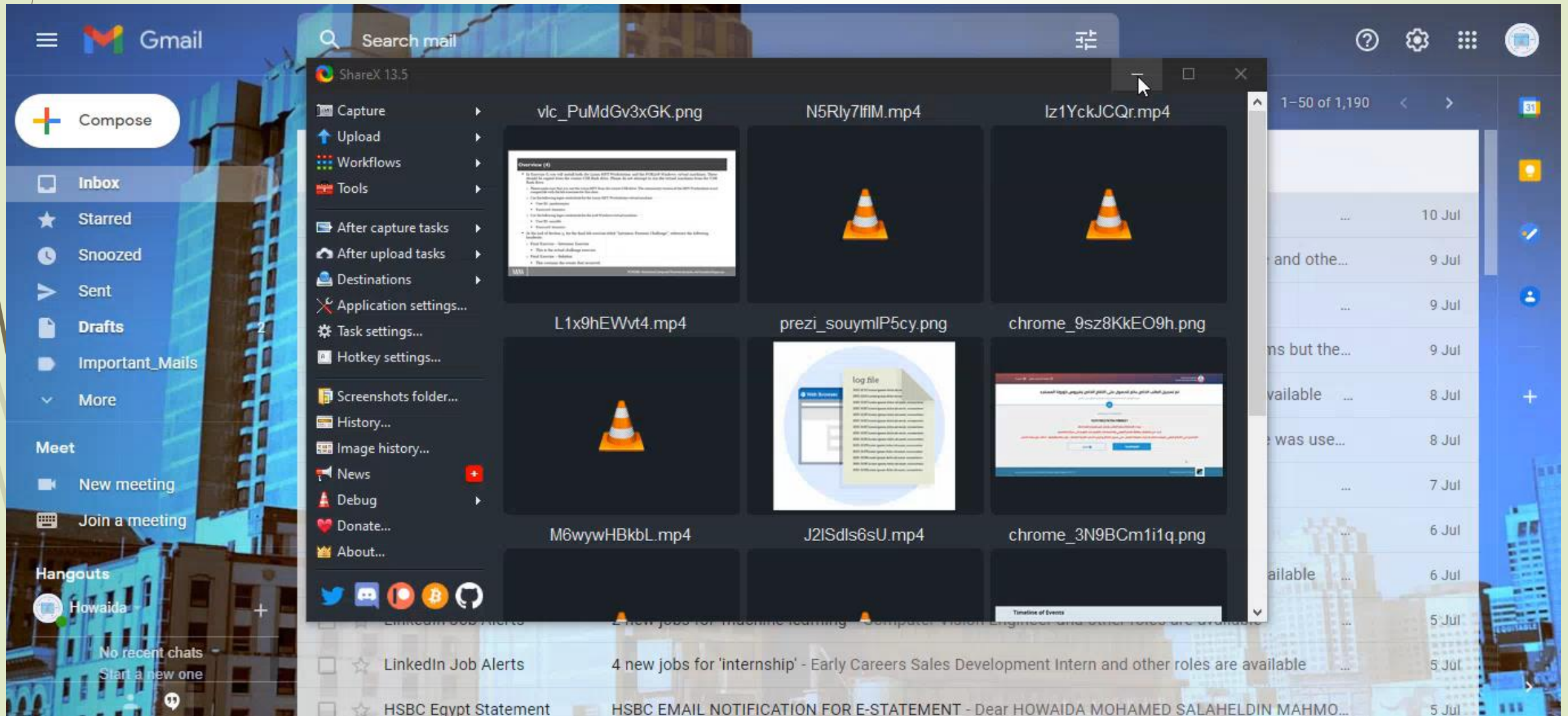
- Perform malware incident handling process if the email contain malicious programs.
 - In case of spam or phishing emails, issue a notification to all the employees to find if others have been facing the same issue.
 - Report the spam and phishing mail to service providers.
- 



What is an Email Header

- *The email header is a code snippet in an HTML 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.*

Email header Analysis Example





What purpose do email headers serve

- Providing information about the sender and recipient
- Preventing spam
- Identifying the email route

Example of Email Header

```
Return-Path: <BraylonHuff@metrowg.pronaceous.com>
Received: from metrowg.pronaceous.com (metrowg.pronaceous.com [138.128.6.57])
        by mail.identityvector.com (8.13.8/8.13.8) with ESMTTP id sA4Gcioh008308
        for <recip@identityvector.com>; Tue, 4 Nov 2014 11:38:45 -0500
Message-ID: <92861425.aLg7b0EBmFjmWCZ20141104083084444@mx1.metrowg.pronaceous.com>
Date: Tue, 04 Nov 2014 08:38:44 -0800
From: Lazy Weight Loss <Braylon@pronaceous.com>
To: <recip@identityvector.com>
Reply-to: <Braylon@pronaceous.com>
Subject: Too Self-Conscious about your body?
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
MIME-Version: 1.0
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on
        quaff.identityvector.com
X-Spam-Level:
X-Spam-Status: No, score=-1.8 required=5.0 tests=BAYES_00,HTML_MESSAGE,
        MIME_HTML_ONLY,RP_MATCHES_RCVD,SPF_HELO_PASS,SPF_PASS autolearn=no
        version=3.3.1
X-Virus-Scanned: clamav-milter 0.98.4 at mail.identityvector.com
X-Virus-Status: Clean
X-Greylist: Sender passed SPF test, not delayed by milter-greylist-4.4.3
        (mail.identityvector.com [205.186.148.46]);
        Tue, 04 Nov 2014 11:38:46 -0500 (EST)
```

New
"Received:"
header

Arbitrary "X-"
headers
added by MX
server

Header/body separator

This is some content that is supposed to look legit...
Completely Legit.
Click the link, because you do what you're supposed to do.
Just like a good little human does.
Obey your email master.
<http://hfdklashgfjkdlsghfdlsjhglksd.cz.cc/pwnme/please>

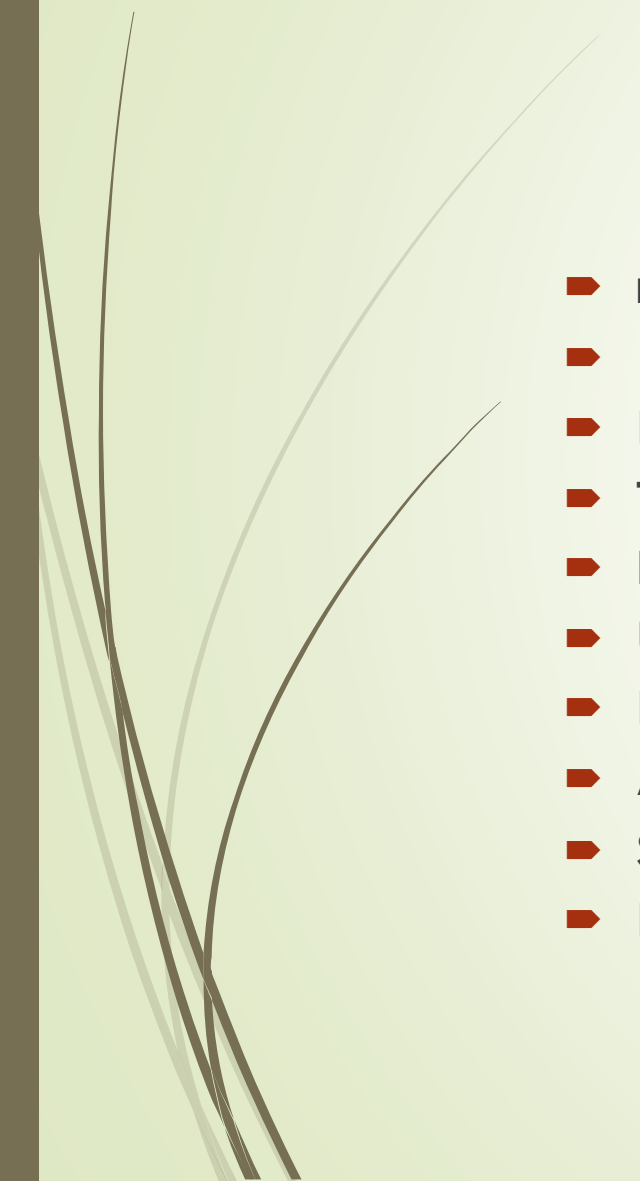


Analyzing an Email Header

- The appearance of the email header differs between ESPs. To analyze it, you need to find the email header and examine the lines of interest to you. All the code from the beginning, until the <body> tag, represents the header.



Analyzing an Email Header

- 
- return path
 - Recipient's email address
 - Name of the email server
 - Type of email sending server
 - IP address of sending server
 - Unique message number
 - Date and time of email was sent
 - Attachment file information
 - Sender Policy Framework (SPF)
 - Domain Key Identified Mail (DKIM)

Example of Email Header Analysis

Consider an example: Rudy sends an Email to Timmy

From: rudy@bieberdorf.edu (Rudy)
To: timmy@immense-isp.com
Date: Tue, Dec 11 2018 14:36:14 PST
X-Mailer: Loris v2.32
Subject: Lunch today?

Received: from mail.bieberdorf.edu
(mail.bieberdorf.edu [124.211.3.78]) by
mailhost.immense-isp.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for
<timmy@immense-isp.com>; Tue, Dec
11 2018 14:39:24 -0800 (PST)

Received: from alpha.bieberdorf.edu
(alpha.bieberdorf.edu
[124.211.3.11]) by
mail.bieberdorf.edu (8.8.5) id
004A21; Tue, Dec 11 2018 14:36:17 -
0800 (PST)
From: rudy@bieberdorf.edu (R.T.
Hood)
To: timmy@immense-isp.com
Date: Tue, Dec 11 2018 14:36:14 PST
Message-Id: <rth031897143614-
00000298@mail.bieberdorf.edu>
X-Mailer: Loris v2.32
Subject: Lunch today?

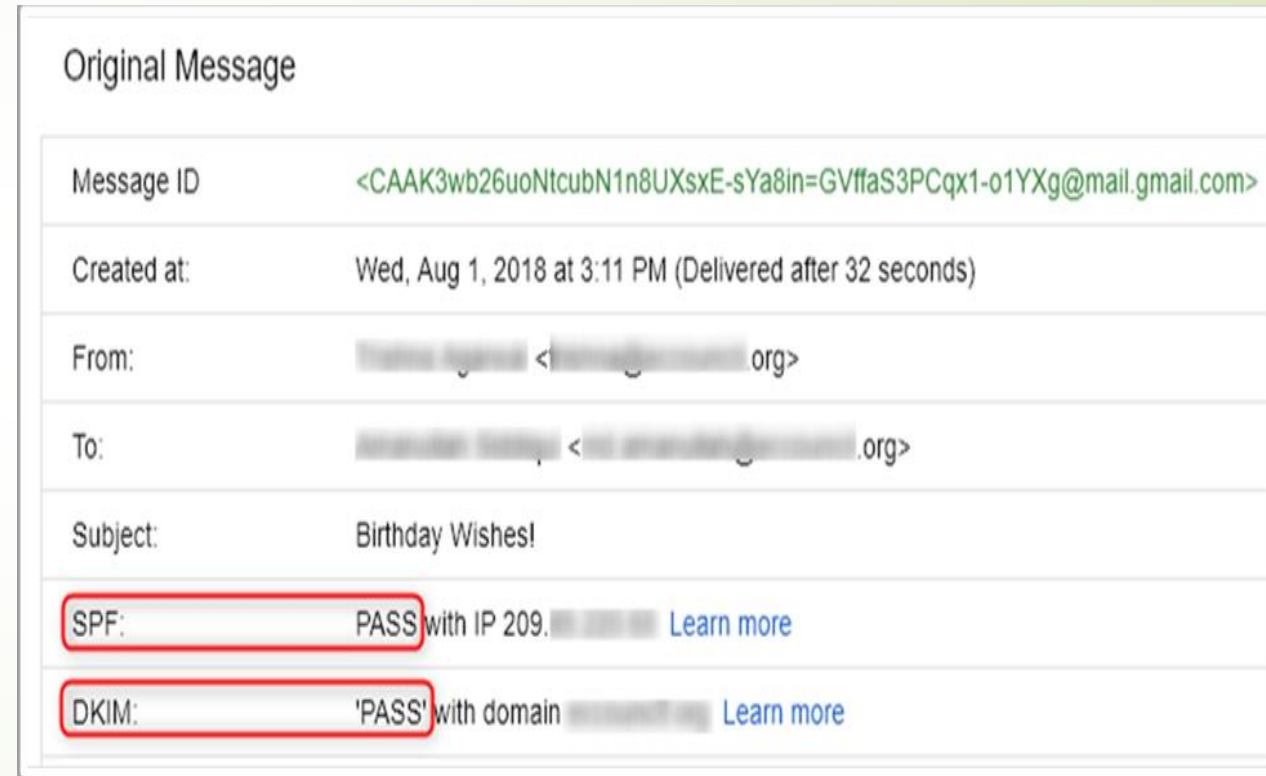


Sender Policy Framework (SPF)

- SPF is an email validation protocol used to by domain owners for preventing spoofing of email.
- Incident responders can analyze the authenticity of the sender using the SPF results.
- The SPF will display results mentioned in the following :
 1. **None** : no SPF records are found for this domain
 2. **Pass** : SPF records exist and IP address is authorized it include plus (+) sign in front of the IP
 3. **Fail** : IP address is not authorized to send email for this domain. This shown by a -all command in the record

Steps to Analyze Email in Gmail

- Open an email you want to analyze.
- Click "more" option (three vertical dots) from the top right of the message.
- From the drop down menu click "show original" option.
- The mail will open a new tab display the original message.



Steps to Analyze Email in Yahoo Mail

- Open the mail you want to analyze.
- Click the "more" option (three horizontal dots) from the top of message.
- From the drop-down menu click "view raw message" option to see the complete message source

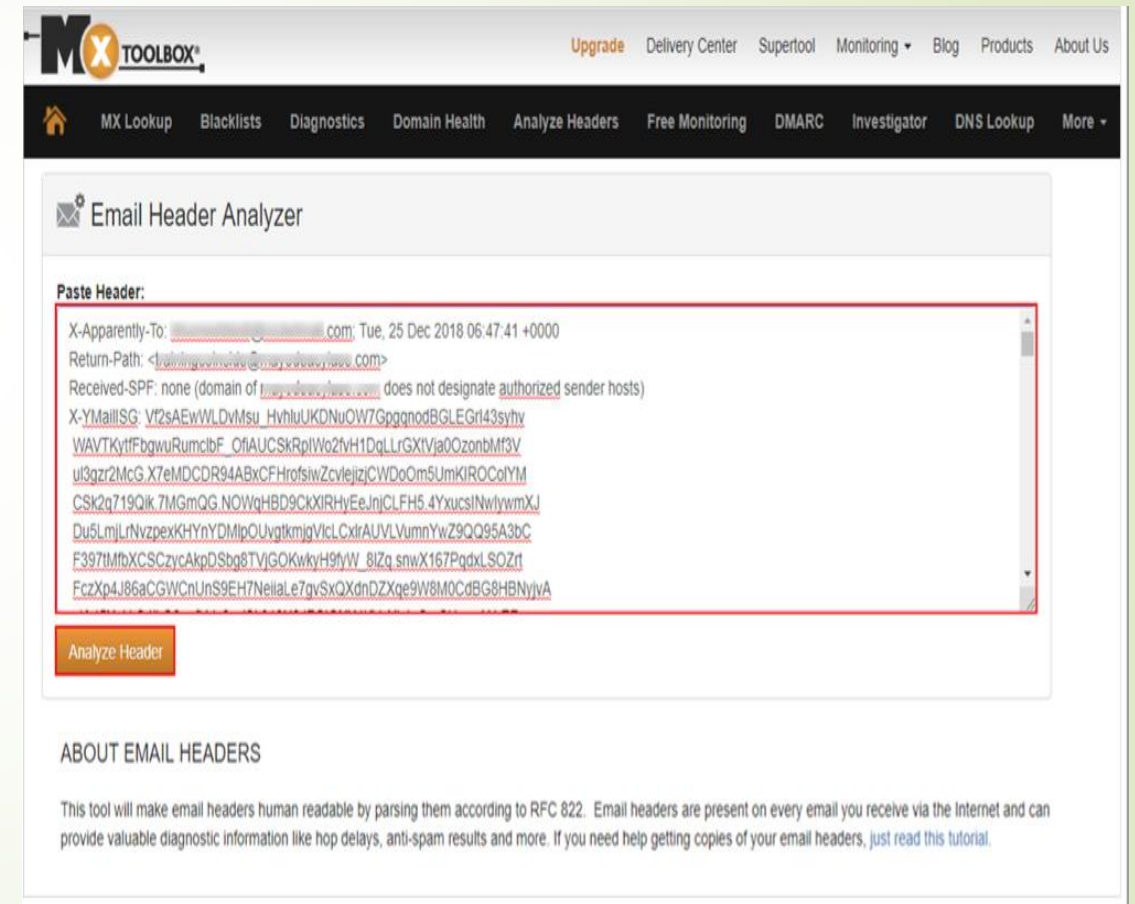
```
X-Apparently-To: [redacted]; Fri, 08 Jun 2018 06:26:48 +0000
Return-Path: <mail@product.communications.yahoo.com>
Received-SPF: fail (domain of product.communications.yahoo.com does not
designate 98.137.[redacted] as permitted sender)
X-YMailISG: baMCC94WLDuFmpnMHBbW5YU8InDSevNQ0tHn_tKvcFFzxUm4
```

```
X-Originating-IP: [98.137.[redacted]]
Authentication-Results: mta4449.mail.gq1.yahoo.com
from=product.communications.yahoo.com; domainkeys=neutral (no sig);
from=product.communications.yahoo.com; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO sonic331-54.consmr.mail.gq1.yahoo.com)
(98.137.[redacted])
by mta4449.mail.gq1.yahoo.com with SMTPS; Fri, 08 Jun 2018 06:26:47 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=product.communications.yahoo.com; s=201402-std-mrk-prd; t=1528439207;
bh=rXQbgUAznRDNjm7LCdWXv9cuKmvVF/yHKGyHimlx2Jg=; h=From:Reply-
To:To:Subject:From:Subject;
```


Tools to Analyze Email headers

➔ MxToolbox

This tool will make email headers human readable.



The screenshot shows the MxToolbox website's Email Header Analyzer tool. The page has a dark navigation bar with the MxToolbox logo and links like Upgrade, Delivery Center, Supertool, Monitoring, Blog, Products, and About Us. Below this is a secondary navigation bar with links for MX Lookup, Blacklists, Diagnostics, Domain Health, Analyze Headers, Free Monitoring, DMARC, Investigator, DNS Lookup, and More. The main content area is titled "Email Header Analyzer" and features a "Paste Header:" label above a large text input field. The input field contains a sample email header with various fields like X-Apparently-To, Return-Path, Received-SPF, and X-YMail-SG. Below the input field is an "Analyze Header" button. At the bottom, there is a section titled "ABOUT EMAIL HEADERS" which explains that the tool parses headers according to RFC 822 to provide human-readable information.

MxTOOLBOX Upgrade Delivery Center Supertool Monitoring Blog Products About Us

MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Monitoring DMARC Investigator DNS Lookup More

Email Header Analyzer

Paste Header:

```
X-Apparently-To: [redacted]@com, Tue, 25 Dec 2018 06:47:41 +0000
Return-Path: <[redacted]@com>
Received-SPF: none (domain of [redacted] does not designate authorized sender hosts)
X-YMail-SG: Vf2sAEwWLDvMsu HvhlUUKDNuOW7GpgqnodBGLEGrI43syhv
WAVTKytfFbgwuRumclbF_OfAUCSkRplWo2fvH1DqLLrGXIVja0OzonbMF3V
uI3gzr2McG.X7eMDCDR94ABxCFHrofsiwZcveijzjCjWDoOm5UmKIROCoYIM
CSK2q719Qik.7MGmQG.NOWqHBD9CkXIRHyEeJnjCLFH5.4YxucsINwlywmXJ
Du5LmjLrNvzpexKHYnYDMlpOUvgtkmjgViclCxrAUVLVumYwZ9QQ95A3bC
F397IMfbXCSCzycAkpDSbg8TVjGOKwkyH9yW 8IZq.snwX167PgdxLSOZrt
FcZxp4J86aCGWcnUnS9EH7NeilaLe7gvSxQXdnDZXqe9W8M0CdBG8HBnyivA
```

Analyze Header

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, [just read this tutorial](#).

Email Header Analysis using mxtoolbox

The screenshot shows a Gmail inbox with the search filter 'in:spam' applied. The left sidebar shows the 'Spam' folder selected with 2 messages. The main content area displays a list of spam messages. A Windows activation watermark is visible in the bottom right corner of the image.

Messages that have been in Spam for more than 30 days will be automatically deleted. [Delete all spam messages now](#)

Message	From	Sent	Time
<input type="checkbox"/> <input type="star"/> <input type="reply"/> Loai Ashraf Hosni	Fw: Emails - _____	From: Loai Ashraf Hosni	Sent: Sunday, July 11, 20... 19:55
<input type="checkbox"/> <input type="star"/> <input type="reply"/> Jeff	test - test		7 Jul
<input type="checkbox"/> <input type="star"/> <input type="reply"/> Hajar ElGhareeb	We brought you a whole week in a mailshot. - We Brought You A whole week In A Mailshot! Dea...		5 Jul
<input type="checkbox"/> <input type="star"/> <input type="reply"/> Quora Digest	During the Vietnam War, how did the Viet Cong manage to cook underground in tunnels w...? - A...		14 Jun

1.69 GB of 15 GB used

Terms - Privacy - Programme Policies

Last account activity: 0 minutes ago
[Details](#)

Activate Windows
Go to Settings to activate Windows.

Email Header Analysis using mxtoolbox

The screenshot displays a Gmail inbox interface with a ShareX application window overlaid. The ShareX window lists various email headers for analysis, organized into columns. The Gmail interface shows a list of emails in the inbox, with the first email selected. The email list includes columns for checkboxes, stars, senders, subjects, and timestamps.

ShareX Overlay Headers:

Primary	Social	Promotions	Updates	Forums
Upyk1hUWKe.mp4	h9AsiBXXhA.mp4	dXIJ9vg51p.mp4		
test - test				
Fw: [Daily News Report] Update Security: New Statement is Available				
Fw: Emails -				
Fake Mailer to				
Gmail to Hatma				
Re: [Daily News				
Db1772YSTi.mp4	wxC6lsvgZ2.mp4	HGnABR24yX.mp4		
test - test				
test - test				
Fw: [Cyber Chief Magazine] June 2021 - From: Netwrix [mailto:netwrix.emea@netwrix.com] Sen...				
test - Test Sent from Mail for Windows 10				
Dco417UiXR.mp4	HR7u6CwioO.mp4			
loai ashraf shared "Phishing Presentation 1" with you. - loai ashraf shared a file with you loai as...				
FW: [eBook] Kickstart Guide to Implementing the NIST Cybersecurity Framework - From: Netwrix...				
loai ashraf				
loai ashraf shared "Loai's Evaluation" with you. - loai ashraf shared a file with you loai ashraf sha				
loai ashraf				
loai ashraf shared "Loai's Evaluation 1" with you. - loai ashraf shared a file with you Loai's Evalua...				

Gmail Interface Elements:


- Search bar: Search mail
- Compose button
- Inbox list: Starred, Snoozed, Important, Sent, Drafts (2)
- Meet section: New meeting, Join a meeting
- Hangouts section: Loay, AASTMT-P1-1-Course, Orientation
- Email list: 1-50 of 173

Examining The originating IP Address

- Open the email to trace and find its header.
- Collect IP Address of the sender from the header of the received mail.
- Search for IP in the WHOIS database.
- Look for the geographic address of the sender in the WHOIS database

IP Information for 162.241.216.11

Quick Stats

IP Location	 United States Provo Unified Layer
ASN	 AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Resolve Host	box5331.bluehost.com
Whois Server	whois.arin.net
IP Address	162.241.216.11
Reverse IP	928 websites use this address.

NetRange: 162.240.0.0 - 162.241.255.255
CIDR: 162.240.0.0/15
NetName: UNIFIEDLAYER-NETWORK-16
NetHandle: NET-162-240-0-0-1
Parent: NET162 (NET-162-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS46606
Organization: Unified Layer (BLUEH-2)
RegDate: 2013-08-22
Updated: 2013-08-22
Ref: <https://rdap.arin.net/registry/ip/162.240.0.0>

OrgName: Unified Layer
OrgId: BLUEH-2
Address: 1958 South 950 East
City: Provo
StateProv: UT
PostalCode: 84606
Country: US
RegDate: 2006-08-08
Updated: 2018-07-31
Ref: <https://rdap.arin.net/registry/entity/BLUEH-2>

Example using WHOIS database

The screenshot shows a web browser with multiple tabs. The active tab is a Bing search for 'whois'. The search results show 'Whois.com' as the top result. A 'ShareX 13.5' window is overlaid on the browser, displaying a grid of video thumbnails. The thumbnails are arranged in three rows and three columns, each with a title and a play button icon. The titles are: 'GASzuysGQt.mp4', 'o5fiOS5O7U.mp4', 'CVn3662lbd.mp4' in the first row; 'Upyk1hUWKe.mp4', 'h9AsiBXXhA.mp4', 'dXIJ9vg51p.mp4' in the second row; and 'Db1772YSTi.mp4', 'wxC6lsvgZ2.mp4', 'HGnABR24yX.mp4' in the third row. The browser's address bar shows the URL 'https://www.bing.com/search?q=whois&cvid=cf18257586784bc2bf7aa0fcb52d1156&aqs=edge.0.017.1724j0j1&pgl=43&FORM=ANN...'. The browser's search bar contains the text 'whois'. The browser's sidebar shows the Microsoft Bing logo and the search results. The browser's top bar shows the tabs and the address bar. The browser's bottom bar shows the search results and the 'Activate Windows' watermark.

Microsoft Bing

whois

ALL

36,600,000 Results

Whois.com

<https://www.whois.com>

Get verified Whois

Domain Name

Whois L

A Whois domain ownership

Login

Login - Whois for Everyone

Website

Do it Yourself

See more

WHOIS Search, Domain Name, Website, and IP Tools - Who.is

<https://who.is>

Search the **whois** database, look up domain and IP owner information, and check out dozens of other statistics. On Demand Domain Data Get all the data you need about a domain and everything associated

Summary

Internet Standards

Activate Windows


Go to Settings to activate Windows

See all (5+)




Eradication of Email Security Incidents

- Eradicating Email attacks
- Report Phishing and Spam Emails to Email Service Provider
- Guidelines Against Spam
- Guidelines Against Phishing



Eradicating Email Attacks

- Collect details of an email security incident such as URL, subject, links, sender, and IP address, from email header analysis and block them across servers, security tools and network devices we can seek help from ISPs to help us performing these actions.
- Immediately alert employees about the incident and train them to diagnose it, inform Network administrators to guide employees who to deal with the current situation.
- Update antiphishing and antispam tools with the newly found signature and details of the attack to prevent similar attacks in the future.
- Find common pattern and signatures from the email to block them on the SMTP server.



Eradicating Email Attacks

- Check the SMTP logs to find if the same email is sent to other employees and remove them from the inboxes.
- Check if other users have been impacted with the attack and perform incident handling process on their system as well.
- Use DNS blocking to block IP addresses used to send the malicious emails.
- Harden the security of the email server and clients.



Eradicating Email Attacks

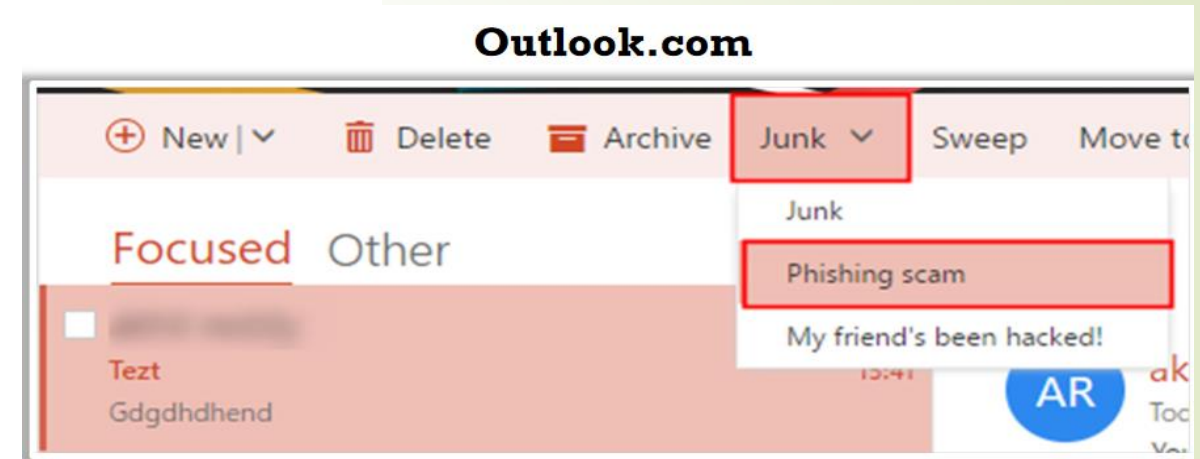
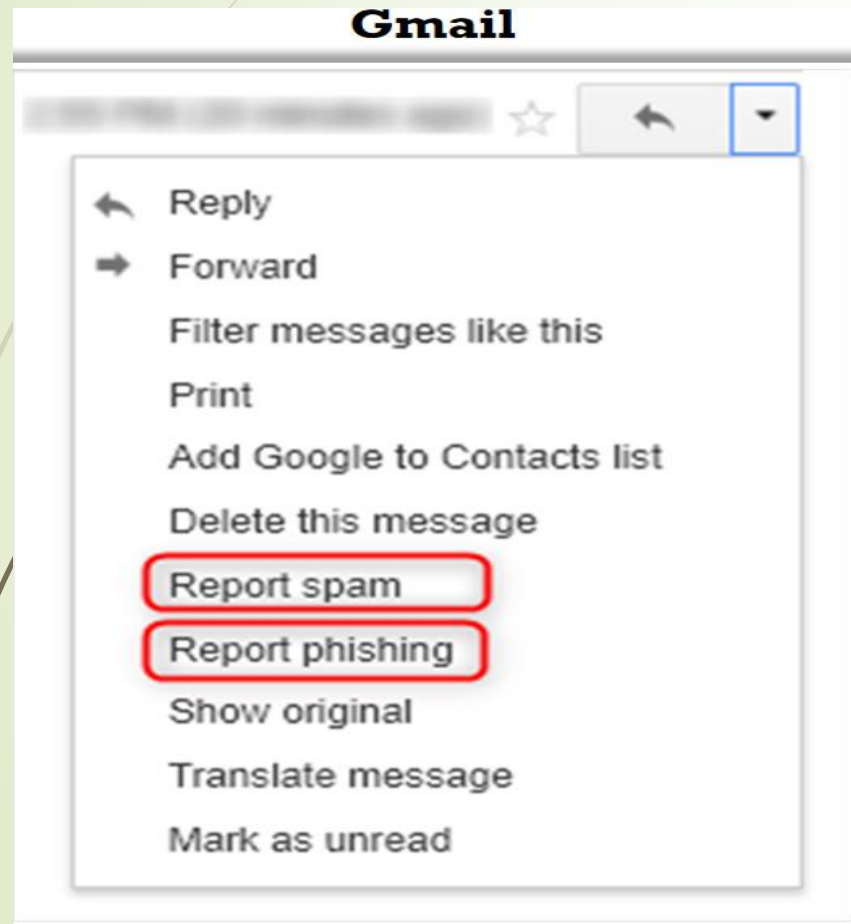
- Train the employees to check email headers from the email asking for immediate action such as financial transactions.
- Blacklist the malicious websites and disable automatic download across all the systems and devices.
- Ensure removal of malware related data from affected systems such as text files, process executed by the malware.
- Block and remove the impacted accounts and re-issue new accounts to the employees.



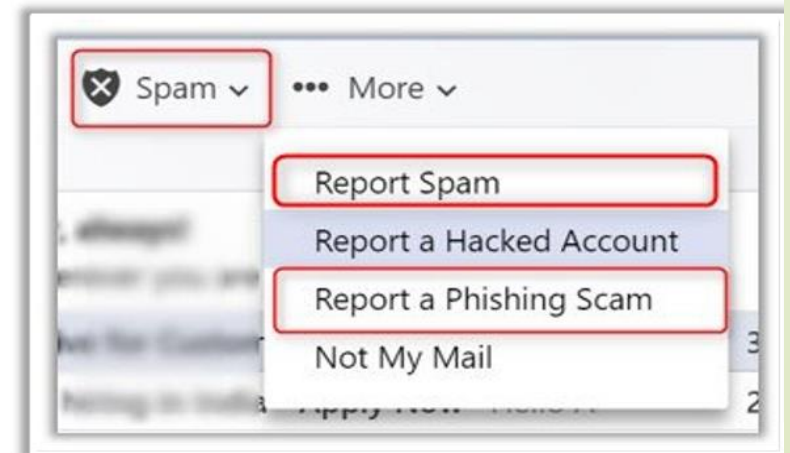
Eradicating Email Attacks

- Request all employees to change password ,ensure it's complicated password and implement multiple authentication for their accounts.
- Install browser extensions and tools that help in detecting and preventing phishing and spam emails.
- Blacklist the email using signature, sender's address, or other details of malicious email.
- Inform the organizations, bank, or entities whose email being spoofed by the attackers.

Reporting Phishing and Spam Emails to Email Service Providers

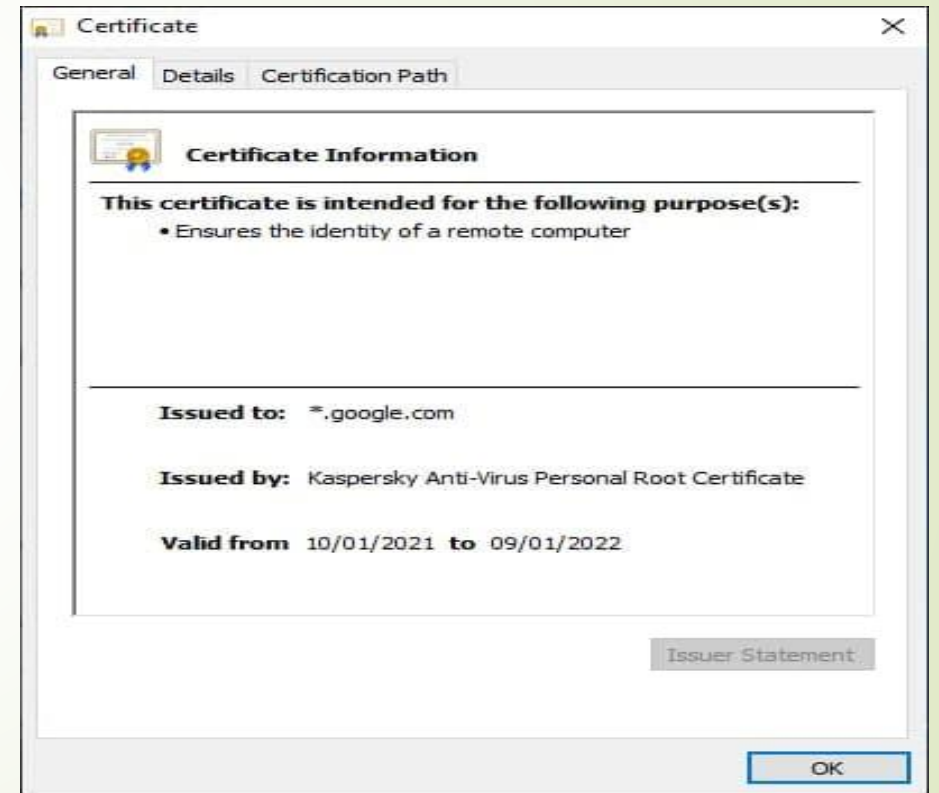


Yahoo Mail



Guidelines Against Spam

- Avoid giving email ID to unnecessary or unsecured websites.
- Before giving email ID to a website check its privacy policy and website certificate.
- Block spamming email IDs and regularly update recipient's address book.



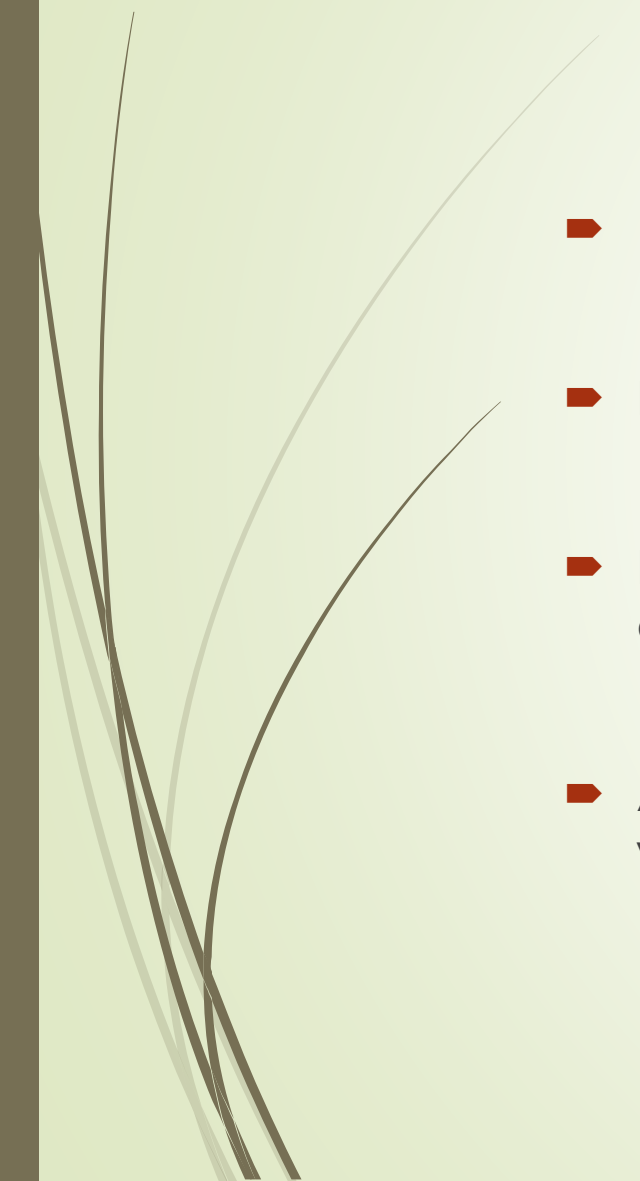


Guidelines Against Spam

- Block potential offensive images in email to prevent attack using luring technique.
- Never give your email ID in clickable form on the web to prevent spam bots from stealing your email ID.
- Maintain a personal email ID which is shared only with friends and family members and never use that email ID for any other purpose.
- Use long email ID with numbers and underscore to prevent spammers.



Guidelines Against Spam

- 
- ▶ Never use unsubscribe links in email messages.
 - ▶ Do not use or subscribe to sites that access email contact list.
 - ▶ Do not choose numbers that reflect personal identification information such as social security number, street address, and telephone number
 - ▶ Avoid buying products from web links in email to discourage them as well as to avoid bogus and fraud related issues.



Guidelines Against Phishing

- Do not transfer sensitive data such as credentials, personal and financial information through emails.
- Do not enter personal details in suspicious links sent in email form and pop-up screen.
- Protect the computer with a security software such antivirus, antispyware, antimalware, firewalls etc.
- Beware of the too good to be true or over attractive schemes and offers.



Guidelines Against Phishing

- Never open the email marked as spam even if the subject line seems to be interesting, and delete such email immediately.
- Avoid accessing the links from the instant messengers.
- Maintain different passwords for different accounts and change them frequently.
- Check the domain name/URL and security indicators before logging in to bank accounts.



Recovery After Email Security Incidents

- Recovery Steps to Follow after Email Incidents
- Recover of Deleted Emails
- Email Security Checklist



Recovery Steps to Follow After Email Incidents

- Change password of the email accounts related to it.
- Inform banks and financial institutions about the attack and block the compromised accounts.
- Restore the compromised systems using backups.
- Contact law enforcements.
- Claim insurance if there huge financial loss



Recovery of Deleted Emails



Gmail :

1. Log in to Gmail
1. In the left pan, scroll down and find the trash folder
2. Click the trash folder and you can view the list of all deleted emails in the right pane of the window



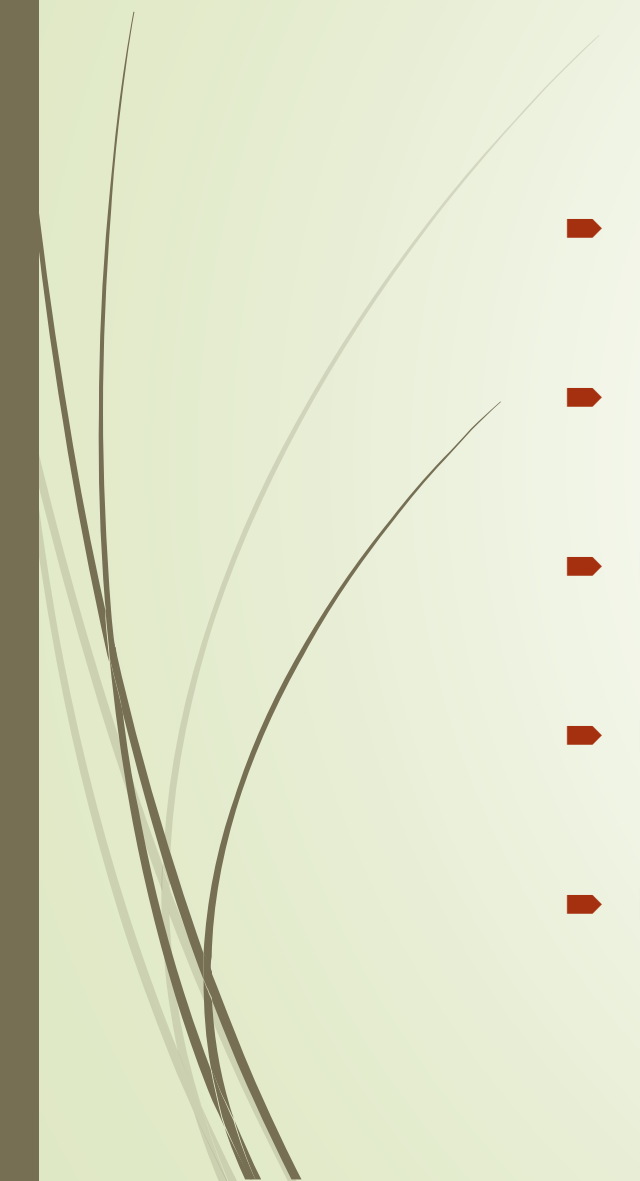
Recovery of Deleted Emails

➤ Outlook :

1. Login to MS outlook
2. The folder will contain recently deleted items
3. In the home tab click recover deleted items from server
4. Click on the email you want recover and select restore selected items button
5. Then click OK button
6. Now, navigate back to the deleted item folder ; you can find the recovered emails



Email Security Checklists

- 
- ▶ Enable HTTPS for secure connection/transactions.
 - ▶ Be delightful while opening email attachments.
 - ▶ Do not click the links provided in the email message.
 - ▶ Follow email etiquette while forwarding messages.
 - ▶ Do not forward or replay to spam and suspicious emails ; delete them.



Email Security Checklists

- Avoid accessing emails via unsecured public wireless.
- Avoid accessing email accounts on shared computers and sending large attachments in emails.
- Never save your password on web browser.
- Sort message by priority, subject date, sender, and other options.




Email Security Checklists

- Avoid sending confidential, sensitive, personal, and classified information in emails.
- Clean your inbox regularly.
- Create folders and move emails accordingly.
- Digital sign your outgoing emails.
- Send attachment in PDF format rather than word or excel.



Email Security Checklists

- 
- Scan email attachments for malware.
 - Use security certified email service provider.
 - Maintain separate email for personal and public communications.
 - Disable keep me signed in/ stay signed in functions.
 - Turn off the preview feature.



Thank You