Module 05

Handling and Responding to Email Security Incidents

This page is intentionally left blank.

Module Objectives

Email, with its ease-of-use and speed, has become one of the most preferred methods of personal as well as professional communications today. This massive adaptation and utilization of email by global corporations as well as the general public has made email one of hackers favorite attack vectors.

Studies reveal that phishing attacks and malicious email attachment attacks together have accounted for more than a quarter of all cybersecurity attacks. Therefore, among all the stakeholders in organizations, the IH&R teams must be aware of different types of email attacks and should develop suitable protocols for handling and responding to such email incidents.

This module will discuss the process of handling and responding to email security incidents. It will help you understand different types of email security incidents, such as phishing and spamming, along with their impact and the differences among them. The module will discuss the additional preparations required to respond to email incidents, including tools and skills. It will help you detect different types of email attacks using sole indicators as well as various other detection and analysis techniques. This module will also discuss the process of containing and eradicating incidents as well as helping to recover from such attacks.

At the end of this module, you will be able to do the following:

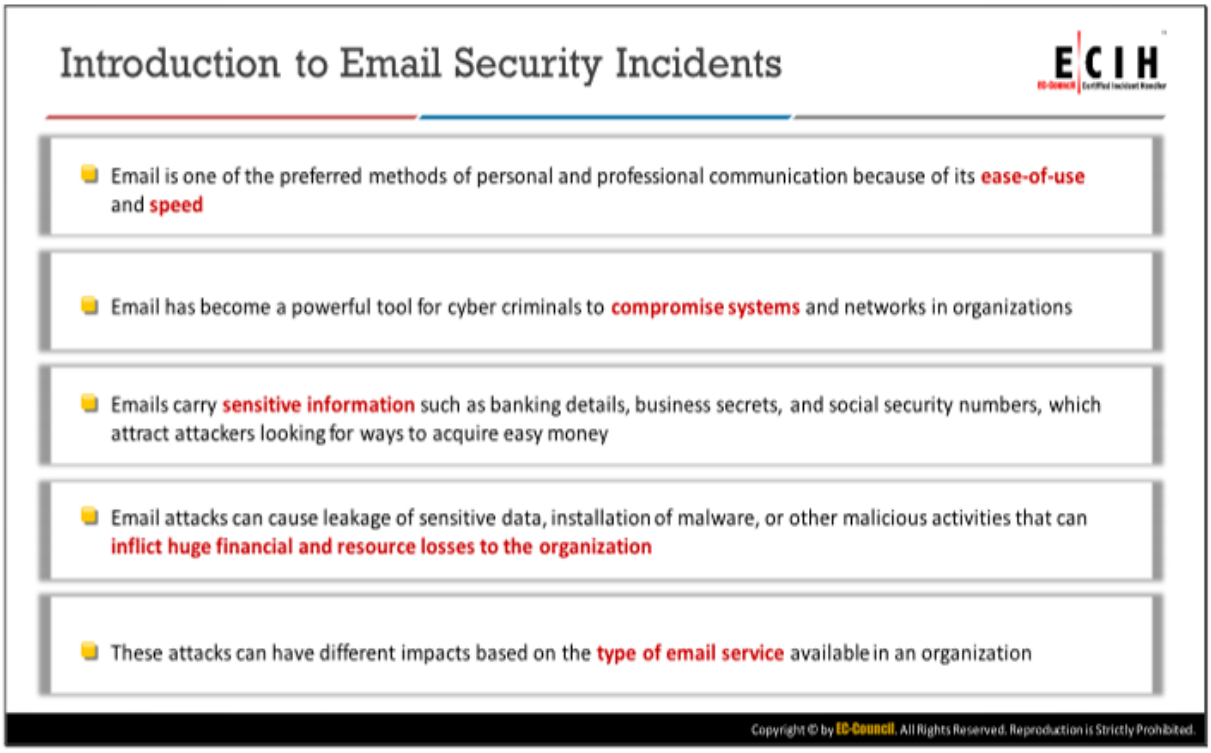
- Understand email security incidents
- Explain different types of email attacks and their impacts
- Discuss the preparation required to handle email security incidents
- Identify email attack indicators

- Detect phishing and spam email
- Contain email attacks
- Devise methods for eradicating email incidents
- Explain the steps to recover following email incidents

Overview of Email Security Incidents

Organizations and individuals use email to communicate, and sometimes their email carries sensitive information such as banking details, business secrets, and social security numbers, all of which has made the email services as a lucrative target for the attackers. Malicious emails are still considered valued weapons by the attackers in order to execute their attacks.

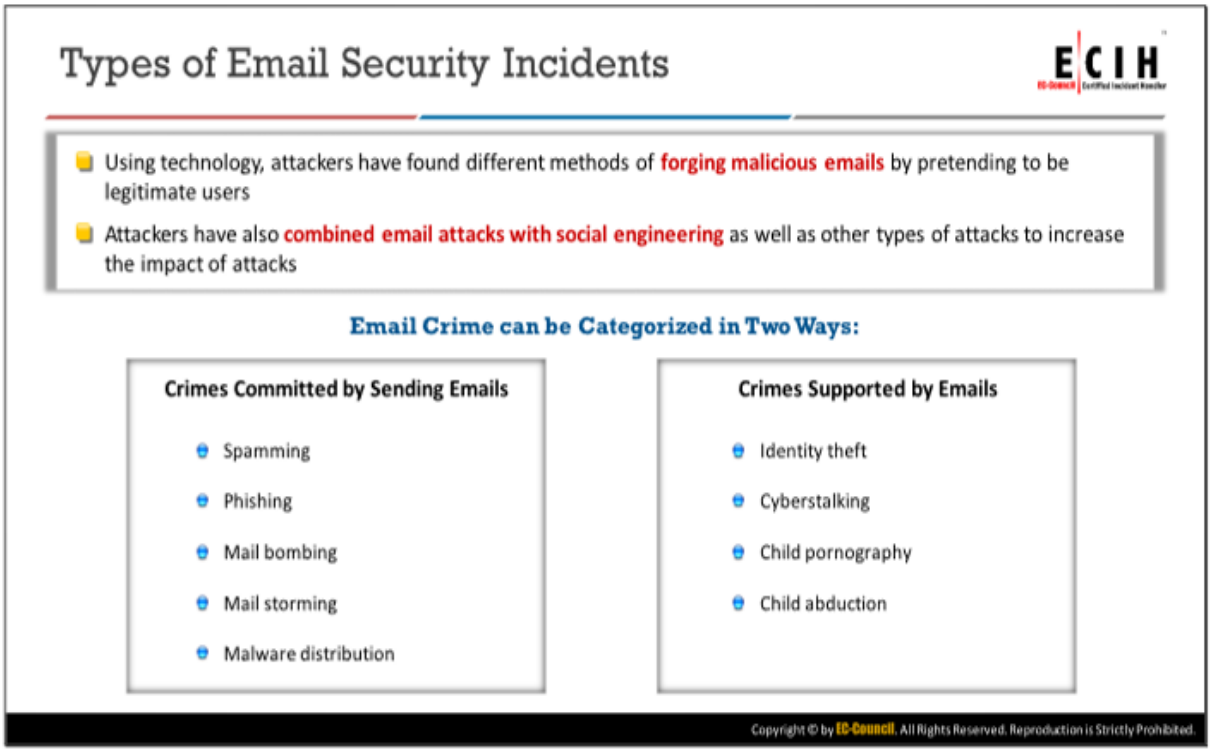
This section discusses email security incidents along with various types of email attacks, including identity theft, phishing, spamming, and malware distribution.



Introduction to Email Security Incidents

Attackers and cybercriminals use email as a powerful tool to compromise organizations' systems and networks. These attacks can have different types of impacts based on the different types of email services available in an organization. Sometimes, email carries sensitive information, which attracts threat actors and lures them to look for ways to exploit the information in the email. Some of the most common email security attacks include identity theft, malware distribution, phishing, and spamming.

Email attacks can cause leaks of sensitive data, installation of malware, or other malicious activities with the potential to inflict huge financial and resource losses on an organization. Containing email attacks or securing against them are essential tasks for IH&R teams. If an organization opts for a third-party email service provider, then the burden of containing the attacks falls completely on the service provider, while organizations using in-house email services and servers will have to implement their own security controls in order to handle and contain email security incidents.



Types of Email Security Incidents

Before starting an email investigation, one should understand the concept of "email crime." Attackers not only try to hack emails but also to use email for trapping and exploiting the target victims. Using this technology, attackers have established a variety of methods to forge malicious emails by posing as legitimate users. Attackers have also developed other types of techniques to increase the impact, including combining email attacks with social engineering.

Email crimes and violations depend on cyber laws created by the governments from the places where the emails originate. For example, spamming is a crime in Washington state but is not illegal in many surrounding states.

We can categorize email crime into two ways:

- **Crimes Committed by Sending Email**

  When an attacker sends an email in order to commit a specific crime, those types of attacks fall under this category.

  Attacks that fall under this category include the following:

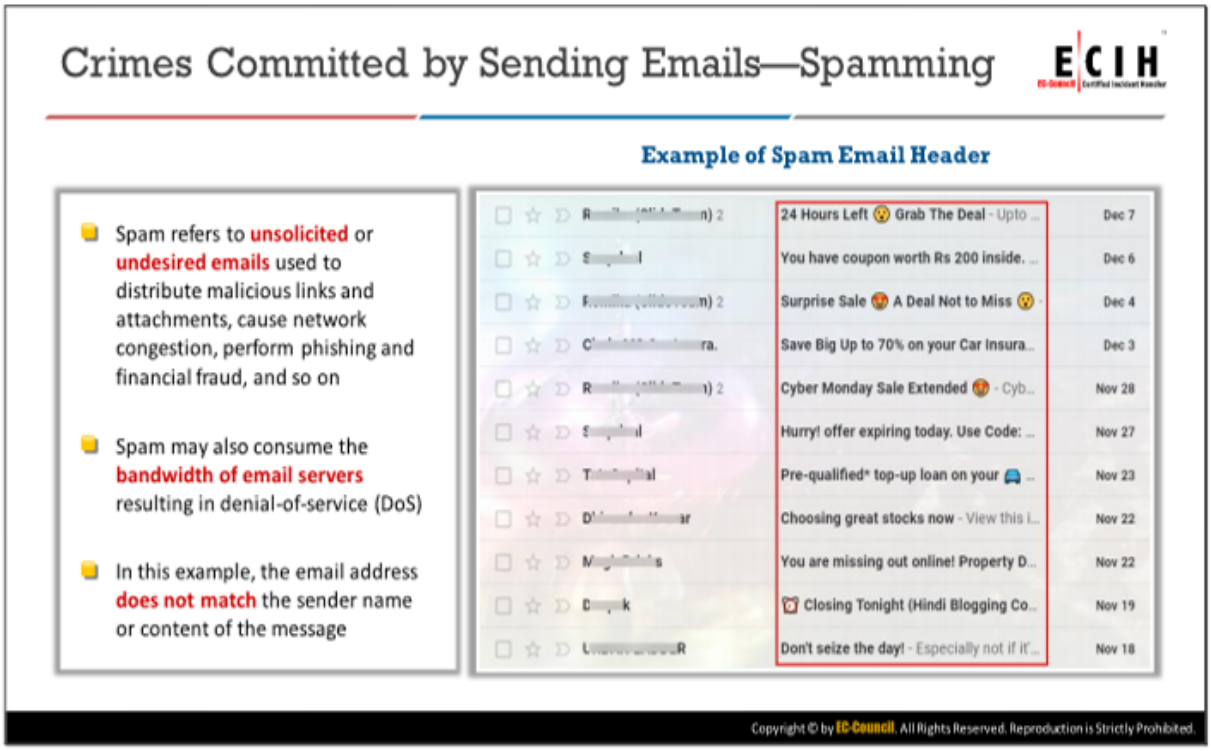
  - Spamming
  - Phishing
  - Mail bombing
  - Mail storms
  - Malware distribution

- **Crimes Supported by Email**

  The use of email for criminal acts such as stalking, committing fraud, and selling narcotics categorized as email that supports cybercrime.

  Attacks that fall under this category include the following:

  - Identity theft
  - Cyberstalking
  - Child pornography
  - Child abduction



Crimes Committed by Sending Emails—Spamming

Spam refers to unsolicited or undesired email used to distribute malicious links and attachments, cause network congestion, perform phishing and financial frauds, and so on. These communications include unsolicited commercial email (UCE) or junk mail. Spam involves sending the same content to a massive number of addresses at the same time. Spamming, or junk mailing, fills mailboxes and prevents users from accessing their regular email. Regular email starts bouncing back to the sender because the server exceeds its capacity. Spammers hide their identities by forging the email header. To avoid replies from infuriated recipients, spammers provide misleading information in the FROM and REPLY-TO fields and post them to a mailing list or newsgroup. In the example, the email address does not match either the name of the sender or the content of the message.

Spam refers in part to unsolicited commercial advertisements distributed online. Although email remains the most common way of sending spam, attackers also use online message boards and chat rooms to send spam. Not only does spam waste people's time, but it also uses up vast amounts of network bandwidth.

Spam also refers to the use of email systems to send undesired email. Attackers use spam to overload users' inboxes, render the email server unavailable, cause network congestion, send malware, perform financial fraud, and divert users' attention.

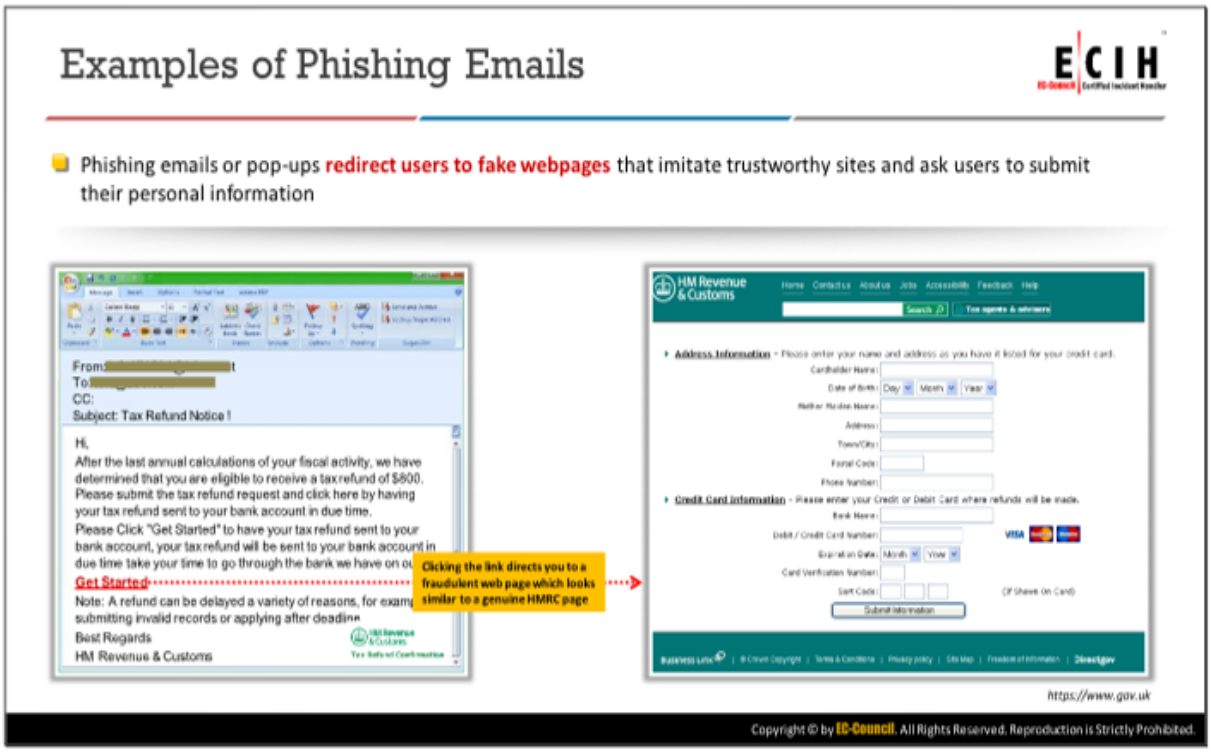
Most of the spam consists of email advertising that organizations send to their customers. These advertising emails redirect users to the product's website. Attackers use spam to distribute fake links and attachments, which download files containing malware or redirect users to malicious or compromised websites that perform malicious activities.

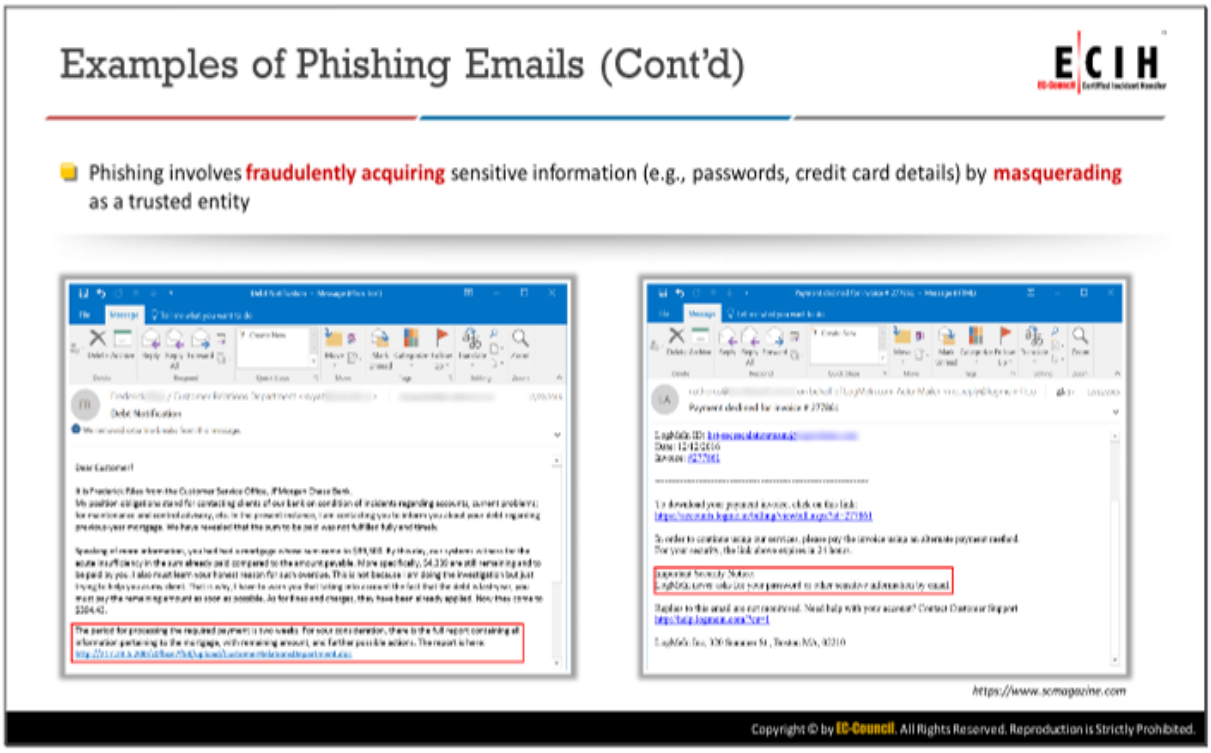
Attackers also add compelling messages to spam email in an attempt to lure or threaten users into downloading the attachment or clicking the links or visiting the mentioned websites, which can be malicious or compromised. All of these actions can lead to the compromise of any target resources, including email accounts, systems, servers, and networks. Furthermore, these actions can help the attacker steal personal information or take control of the user's machine.

Crimes Committed by Sending Emails—Phishing

Phishing refers to a psychological manipulation attack technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information. The attacker registers a fake domain name, builds a lookalike website, and then mails the fake website's link to several users. These phishing emails contain a message that threatens or attracts the user to perform actions such as clicking a link, downloading an attachment, or revealing sensitive details. When a user clicks on the phishing link, it redirects that user to the counterfeit webpage, where the user is lured to share sensitive details, such as address and credit card information, without knowing that it is a phishing site.

Attackers also use techniques such as social engineering to gather information about users and then employ that information to trick them. Attackers also impersonate the names of genuine, known institutions and people to perform this attack. Some of the reasons behind the success of phishing scams include users' having a lack of knowledge, being visually deceived, and not paying attention to security indicators. Phishing has emerged as an effective method of attack as it allows attackers to send email to a great number of users across the world.





Examples of Phishing Emails

Phishing is a practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information. Attackers perform phishing attacks by distributing malicious links via some communication channel or mail to obtain private information like account numbers; one client's application cloud could potentially allow attackers to access another client's data. Phishing emails or pop-ups redirect

users to fake webpages by mimicking trustworthy sites, which ask them to submit their personal information.

The types of email used for phishing usually contain a spoofed address and header, a message that directs users to follow the instructions that include a malicious link or attachment. To create the fake phishing emails, the attackers can also copy images and other components of emails from genuine senders. The messages used in phishing emails can also include offers that are too good to be true, such as winning a lottery or a financial prize from a very well-known organization. Alternatively, the phishing email could claim an emergency from known a known user, such as a friend admitted to hospital, a hacked account, or security implementations that require a change of password.

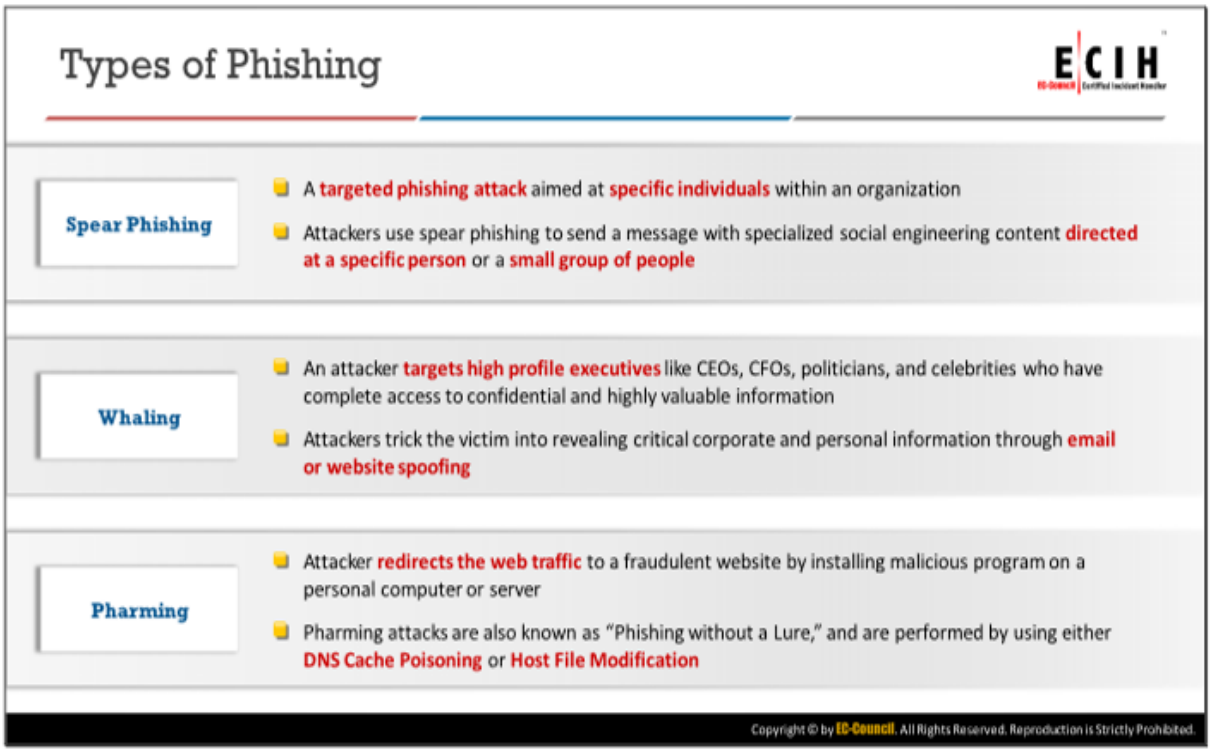
Following are some examples of phishing emails:

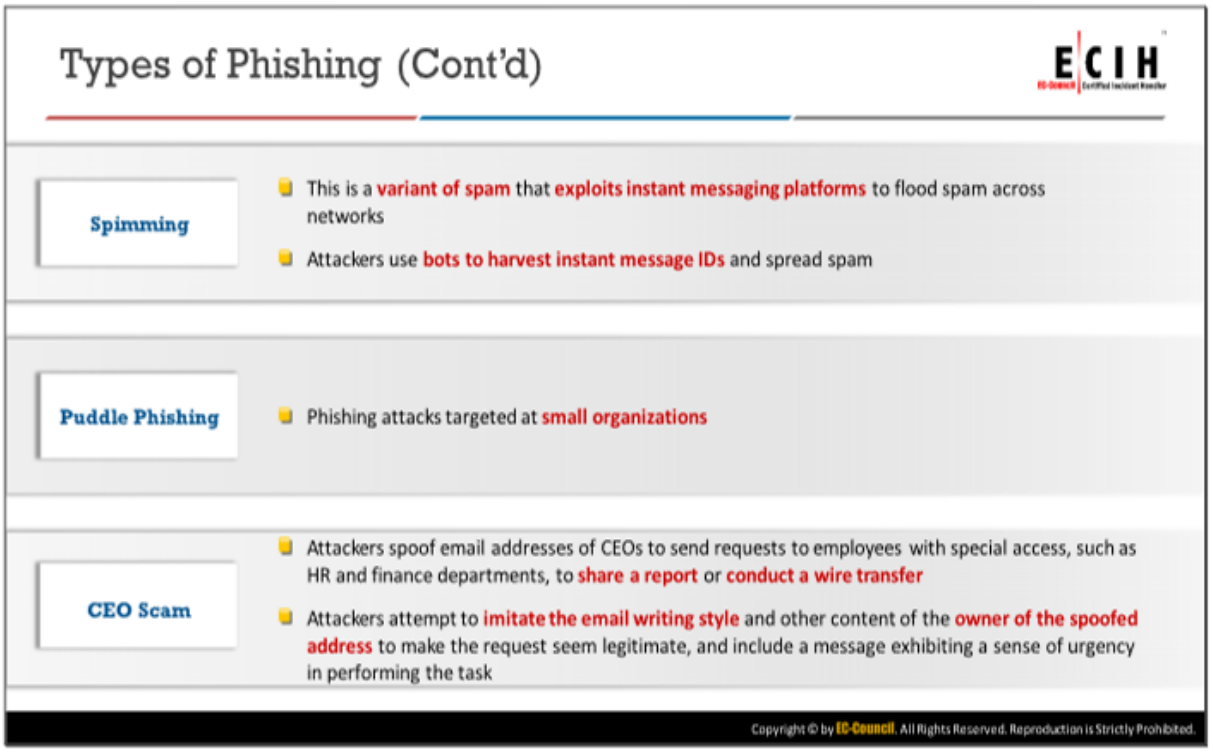
Source: *https://www.gov.uk*

The screenshots shown on the above slides represent an example of an illegitimate email that claims to be from a legitimate sender. The email link redirects users to a fake webpage and asks them to submit their personal or financial details.

Source: *https://www.scmagazine.com*

Today, most people use internet banking. In fact, many use internet banking for all their financial needs, such as online share trading and e-commerce. Phishing involves fraudulently acquiring sensitive information (e.g., passwords, credit card details) by masquerading as a trusted entity. The target receives an email that appears to be from the bank and that requests the user to click on the URL or the link provided. If the user is successfully tricked into providing his or her username, password, and other information, then the site will forward the information to the attacker, who will use it for nefarious purposes.





Types of Phishing

- **Spear Phishing**

  Instead of sending thousands of emails, some attackers opt for "spear phishing" and use specialized social engineering content directed at a specific employee or small group of employees in a particular organization to steal sensitive data such as financial information and trade secrets.

Spear phishing messages appear to be from a trusted source with an official-looking website. The email also appears to be from an individual within the recipient's company, generally someone in position of authority. But the message has actually been sent by an attacker attempting to obtain critical information about a specific recipient and the organization, including login credentials, credit card details, bank account numbers, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate when compared to a normal phishing attack, as it appears to be from a trusted company source.

- **Whaling**

  This is a type of phishing attack to obtain specific, valuable information or perform financial fraud that is targeted at selected high-profile executives, such as CEO, CFO, HR manager, accounts department personnel, politicians, or celebrities, who have complete access to confidential and highly valuable information. Whaling is a social engineering deception in which the attacker tricks the victim to reveal critical corporate and personal information (for example bank account details, employee details, customer information, and credit card details) through email or website spoofing. Whaling is different from a phishing attack; the email or website that is used for the attack is carefully designed to target someone at the executive leadership level.

- **Pharming**

  Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server. When the victim enters any URL or domain name, it automatically redirects the victim's traffic to a website controlled by the attacker. This attack is also known as "Phishing without a Lure." The attacker steals confidential information such as credentials, banking details, and other information related to web-based services. Pharming attacks can be performed in two ways: DNS Cache Poisoning and Host File Modification.

- **Spimming**

  SPIM (spam over instant messaging) exploits instant messaging platforms and uses IM as a tool to spread spam. A person who generates SPIM is called a spimmer. Spimmers generally make use of bots (an application that executes automated tasks over the network) to harvest instant message IDs and forward spam messages to them. SPIM messages, similar to email spams, generally include advertisements and malware as attachments or embedded hyperlinks. The user opens the attachment, which, in turn, redirects the user to a malicious website, which collects financial and personal information such as credentials, bank account numbers, and credit card details.

- **Puddle Phishing**

  It is a phishing attack that targets small organizations.

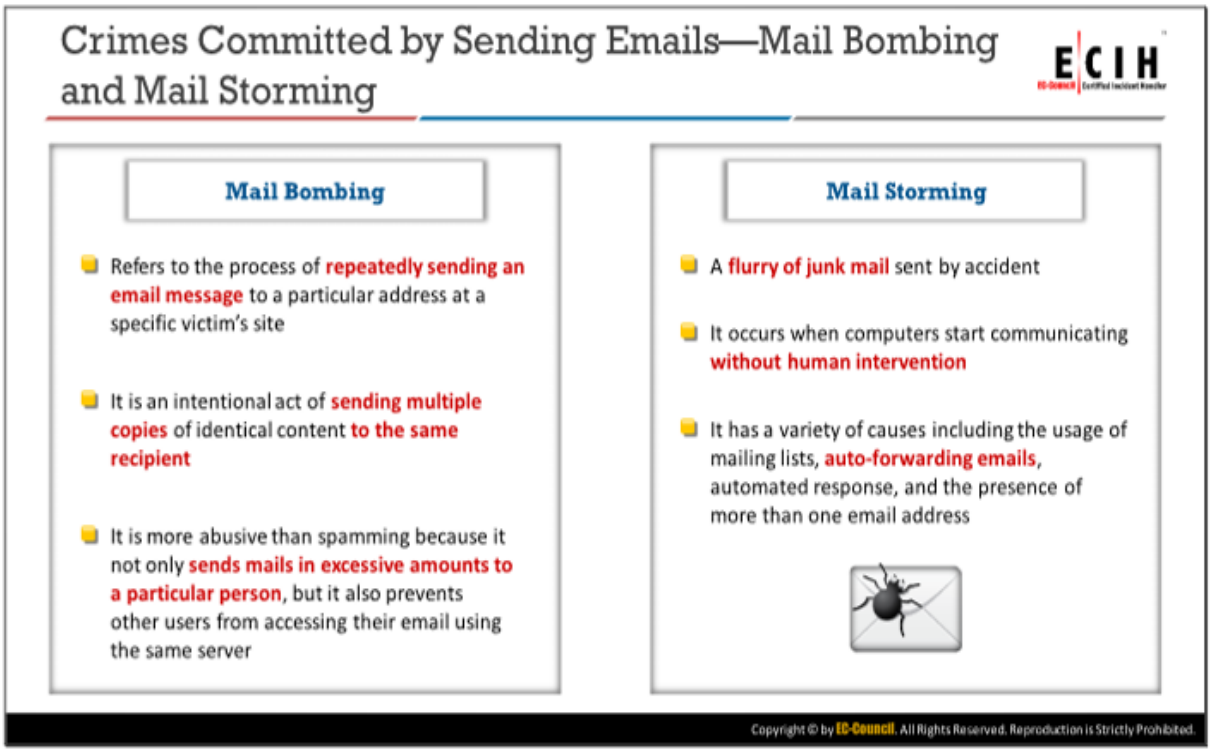
- **CEO Scam**

  The CEO scam is a type of phishing attack in which the perpetrators spoof email addresses of target organization CEOs and impersonate them to perform financial fraud.

They use the spoofed email IDs to send emails, which request the employees from accounting or HR departments to perform wire transfers to a particular user of specific amounts. The employees may believe that the email came from their CEO and then perform the requested transaction.

The attackers will attempt to imitate the CEO's style of email writing and content to make the scam email seem legitimate, and they will include a message presenting a sense of urgency to perform the task. Attackers can impersonate a vendor and use fake invoice, such as for payment of an overdue bill, or they can impersonate a legal firm and request fund transfer to settle a legal dispute.

Attackers may also perform these attacks on the organization's vendors, clients, and customers for financial benefits. Apart from financial losses, these attacks may also result in loss of customer and vendor trust.



Crimes Committed by Sending Emails—Mail Bombing and Mail Storming

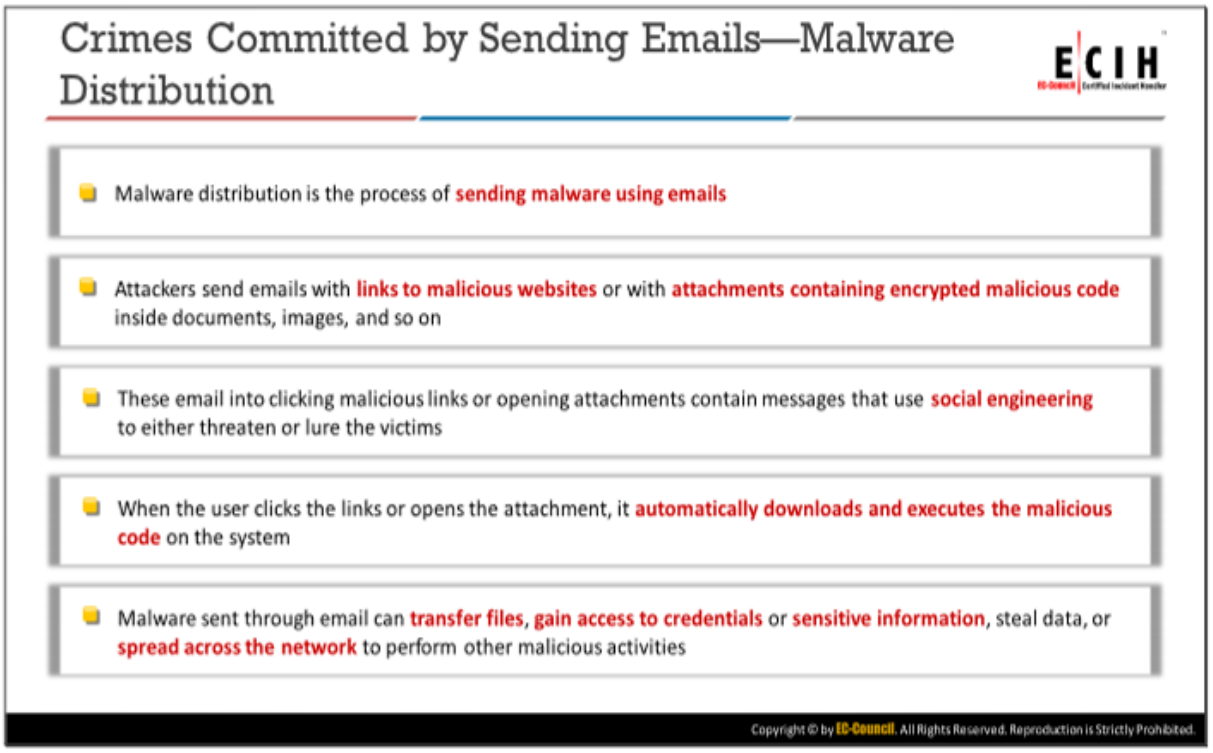
- **Mail Bombing**

  Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial-of-service impact.

  Mail bombing is an intentional act of sending multiple copies of identical content to the same recipient. The primary objective behind mail bombing is to overload the email server and degrade the communication system by making it unserviceable. Usually, a mail bomber and the victim know each other. Newsgroup postings that do not agree with the recipient's opinion also result in mail bombing. The target of a mail bomber can be either a specific machine or a particular person. Mail bombing is more abusive than spamming because it not only sends mails in excessive amounts to a particular person, but it also prevents other users from accessing their email using the same server.

- **Mail Storming**

  A mail storm occurs when computers start communicating without human intervention. The flurry of junk mail sent by accident is a type of mail storm. The use of mailing lists, auto-forwarding emails, automated response, and the presence of more than one email address are among the causes for a mail storm. Malicious software code is also written to create mail storms such as the "Melissa, I-Love-u" message. Mail storms hinder communication systems and can make them inoperable.



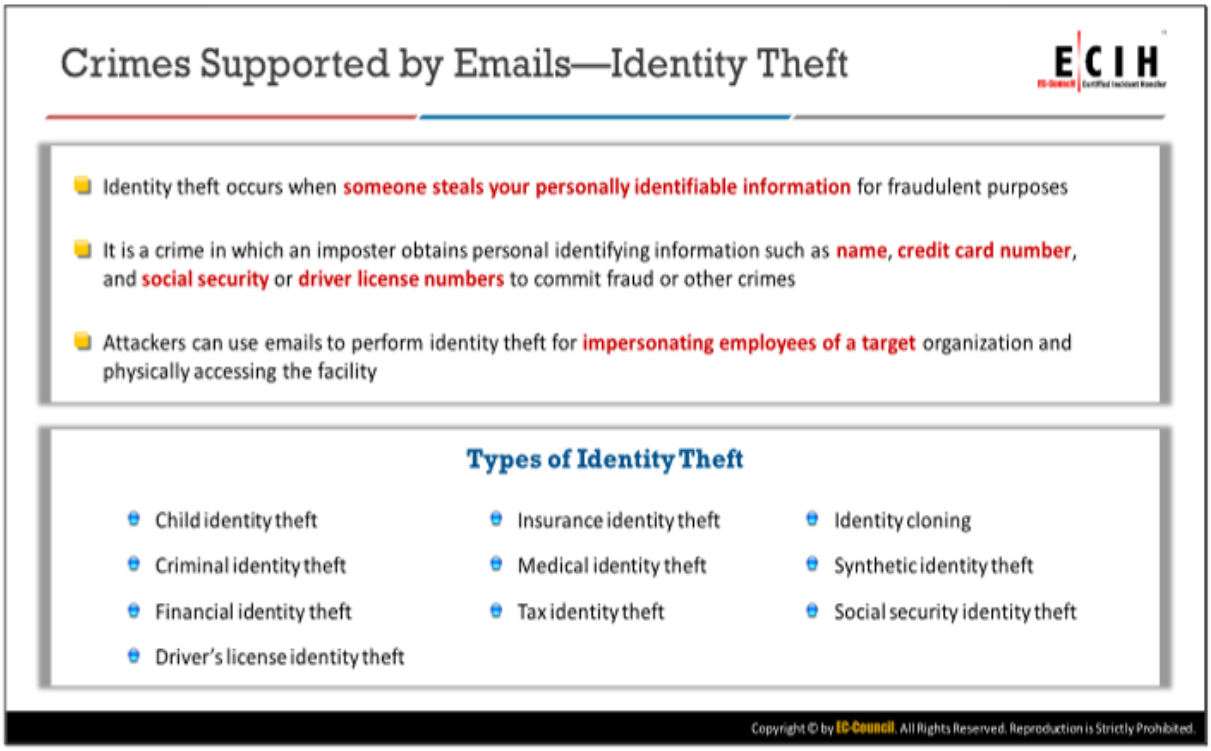
Crimes Committed by Sending Emails—Malware Distribution

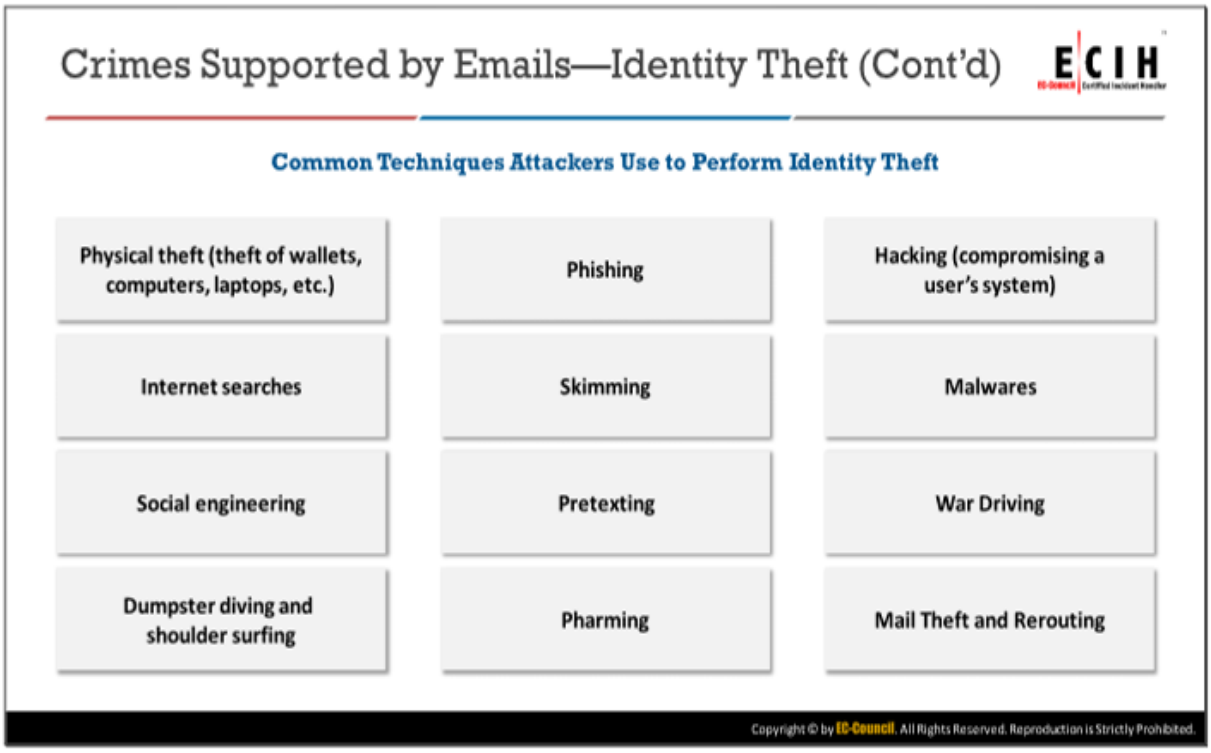
Malware distribution is the process of sending malware via email. Attackers can use techniques such as sending attachments that contain malware or links to websites that download malware. When the user clicks on the link or opens the attachment, it automatically downloads and executes the malicious code.

Such email also contains messages that use social engineering to either threaten or lure the victims into opening the attachments or clicking the provided malicious link. Malware sent through email can transfer files, gain access to credentials or sensitive information, steal data, or spread across the network to perform other malicious activities.

The basic email malware infection process includes the following steps:

- Attackers send emails with links to malicious websites or with attachments containing encrypted malicious code inside documents, images, invoice bills, package delivery, and so on.
- Emails contain a link or an attachment, typically a JavaScript file or a macro.
- When the user clicks on the link or the attachment, it will induce the user to execute the macro or automatically download PowerShell to execute the payload.
- The final payload can be a virus or ransomware or Trojan that steals information or attacks the organization's network, causing the intended harm.





Crimes Supported by Emails—Identity Theft

Identity theft is a problem that many consumers face today. In the United States, some state legislators have imposed laws restricting employees from providing their SSNs (Social Security numbers) during their recruitment. Identity theft frequently figures in news reports. Companies should be informed about identity theft so that they do not endanger their own anti-fraud initiatives.

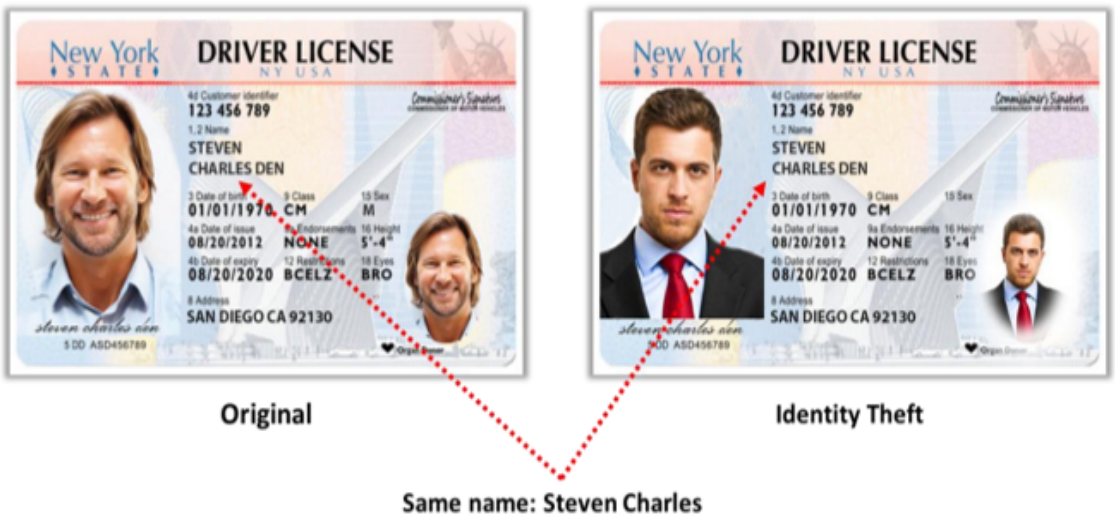


Figure 5.1: Identity theft example

The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone's identification. Identity theft occurs when someone steals another's personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts. Furthermore, attackers can use email to perform identity theft for the purpose of impersonating the target organization's employees and physically accessing the facility.

Types of personally identifiable information stolen by identity thieves:

- Names
- Home and office addresses
- Social security numbers
- Phone numbers
- Dates of birth
- Bank account numbers
- Credit card information
- Credit reports
- Driver's license numbers
- Passport numbers

Attackers steal people's identities for several fraudulent purposes:

- Opening new credit card accounts in users' names without paying the bills
- Opening new phone or wireless accounts in users' names, or running up charges on existing accounts
- Using victims' information to obtain utility services such as electricity, heating, or cable TV

- Opening bank accounts for writing bogus checks using victims' information
- Cloning ATM or debit cards to make electronic withdrawals from victims' accounts
- Obtaining loans for which victims are liable
- Obtaining driving licenses, passports, or other official ID cards that contain victims' data but have attackers' photos
- Using victims' names and Social Security numbers to steal their government benefits
- Impersonating employees of a target organization to physically access its facility
- Taking over insurance policies
- Selling personal information
- Ordering goods online using a drop-site
- Hijacking email accounts
- Obtaining health services
- Submitting fraudulent tax returns
- Committing other crimes and then providing victims' names to the authorities upon arrest, instead of their own

Types of Identity Theft

Identity theft is constantly increasing, and the identity thieves are finding new ways or techniques to steal different types of targets' information. Some of the identity theft types are as follows:

- **Child Identity Theft**

  This type of identity theft occurs when the identity of a minor is stolen, which usually goes undetected for a long time. After a child's birth, parents apply for a Social Security number (SSN) for their child. This number, along with an altered date of birth, is used by identity thieves to apply for credit accounts, loans or utility services, or to rent a place to live or apply for government benefits.

- **Criminal Identity Theft**

  This is one of the most common and damaging types of identity theft, in which a criminal uses someone else's identity and escapes criminal charges. When the criminal is caught or arrested, they provide the fake identity. The best means of protection against criminal identity theft is to keep personal information secure, including following safe internet practices and being cautious of "shoulder surfers."

- **Financial Identity Theft**

  This type of identity theft occurs when a victim's bank account and credit card information are stolen and used illegally by a thief. The criminal can max out credit cards and withdraw money from the account or can use the stolen identity to open a new account, get new credit cards, and take out loans. The information required to hack into

the victim's account and steal information is obtained by the thieves through viruses, phishing attacks, or data breaches.

- **Driver's License Identity Theft**

  This type of identity theft is the easiest as it requires little sophistication. A person can lose his/her driver's license, or it can be easily stolen. Once it falls into the wrong hands, the perpetrator can sell the driver's license or misuse the fake driver license by committing traffic violations, of which the victim is unaware, fails to pay the fines, and might ultimately have his/her license suspended or revoked.

- **Insurance Identity Theft**

  This type of identity theft is closely related to medical identity theft. It takes place when a perpetrator unlawfully takes the victim's medical information in order to access his/her insurance for a medical treatment. Its effects include difficulties for the victim in settling medical bills, higher insurance premiums, and probably trouble in acquiring medical coverage later on.

- **Medical Identity Theft**

  This is the most dangerous type of identity theft, in which the perpetrator uses a victim's name or information without the victim's consent or knowledge in order to obtain medical products and claim health insurance or healthcare services. Medical identity theft results in frequent erroneous entries in the victim's medical records, which could lead to false diagnosis and life-threatening decisions by the doctors.

- **Tax Identity Theft**

  This type of identity theft occurs when a perpetrator steals the victim's Social Security Number (SSN) in order to file fraudulent tax returns and obtain fraudulent tax refunds. It creates difficulties for the victim in accessing legitimate tax refunds and results in a loss of funds. Phishing emails are one of the main tricks used by the criminal to steal a target's information. Therefore, protection from such identity theft includes adoption of safe internet practices.

- **Identity Cloning and Concealment**

  This is a type of identity theft that encompasses all forms of identity theft, in which the perpetrators attempt to impersonate someone else in order to simply hide their identity. These perpetrators could be illegal immigrants or those hiding from creditors, or they simply want to become "anonymous" due to some other reasons.

- **Synthetic Identity Theft**

  This is one of the most sophisticated types of identity theft, in which the perpetrator obtains information from different victims to create a new identity. First, the perpetrator steals the Social Security number (SSN) and uses it with a combination of fake names, dates of birth, addresses, and other details required for creating new identities. The perpetrator then uses this new identity to open new accounts, loans, credit cards, phones, and other goods and services.

- **Social Identity Theft**

  This is another most common type of identity theft, in which the perpetrator steals victim's Social Security number (SSN) in order to derive various benefits such as selling it to some undocumented person, using it to defraud the government by getting a new bank account, loans, credit cards, or passport.

Common Techniques Attackers Use to Perform Identity Theft

Discussed below are some methods by which attackers steal targets' identities, which in turn allow them to commit fraud and other criminal activities.

- **Physical Theft**

  Physical theft is common. Attackers steal wallets, computers, laptops, cell phones, backup media, and other sources of personal information from public places such as hotels and recreational areas, including clubs, restaurants, parks, and beaches. Given adequate time, they can recover valuable data from these sources.

- **Internet Searches**

  Attackers can gather a considerable amount of sensitive information via legitimate internet sites, using search engines such as Google, Bing, and Yahoo!.

- **Social Engineering**

  Social engineering is the art of manipulating people into performing certain actions or divulging personal information, accomplishing the task without using cracking methods.

- **Dumpster Diving and Shoulder Surfing**

  Attackers rummage through household garbage and organizations' trash bins, ATMs, hotels, and other places to obtain personal and financial information for fraudulent purposes.

  Criminals may find user information by glancing at documents, personal identification numbers (PINs) typed into an automatic teller machine (ATM), or by overhearing conversations.

- **Phishing**

  The "fraudster" may pretend to be from a financial institution or other reputable organization and send spam or pop-up messages to trick users into revealing their personal information.

- **Skimming**

  Skimming refers to stealing credit/debit card numbers by using special storage devices called skimmers or wedges when processing the card.

- **Pretexting**

  Fraudsters may pose as executives from financial institutions, telephone companies, and so on, who rely on "smooth talking" and win the trust of an individual to reveal sensitive information.

- **Pharming**

  Pharming, also known as domain spoofing, is an advanced form of phishing, in which the attacker redirects the connection between the IP address and its target server. The attacker may use cache poisoning (modifying the internet address to that of a rogue address) to do so. When the users type in the internet address, pharming redirects them to a rogue website that resembles the original website.

- **Hacking**

  Attackers may compromise user systems and route information using listening devices such as sniffers and scanners. They gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

- **Key Loggers and Password Stealers (Malwares)**

  An attacker may infect the user's computer with Trojans, viruses, and so on, and then collect the keyword strokes to steal passwords, user names, and other sensitive information of personal, financial, or business importance.

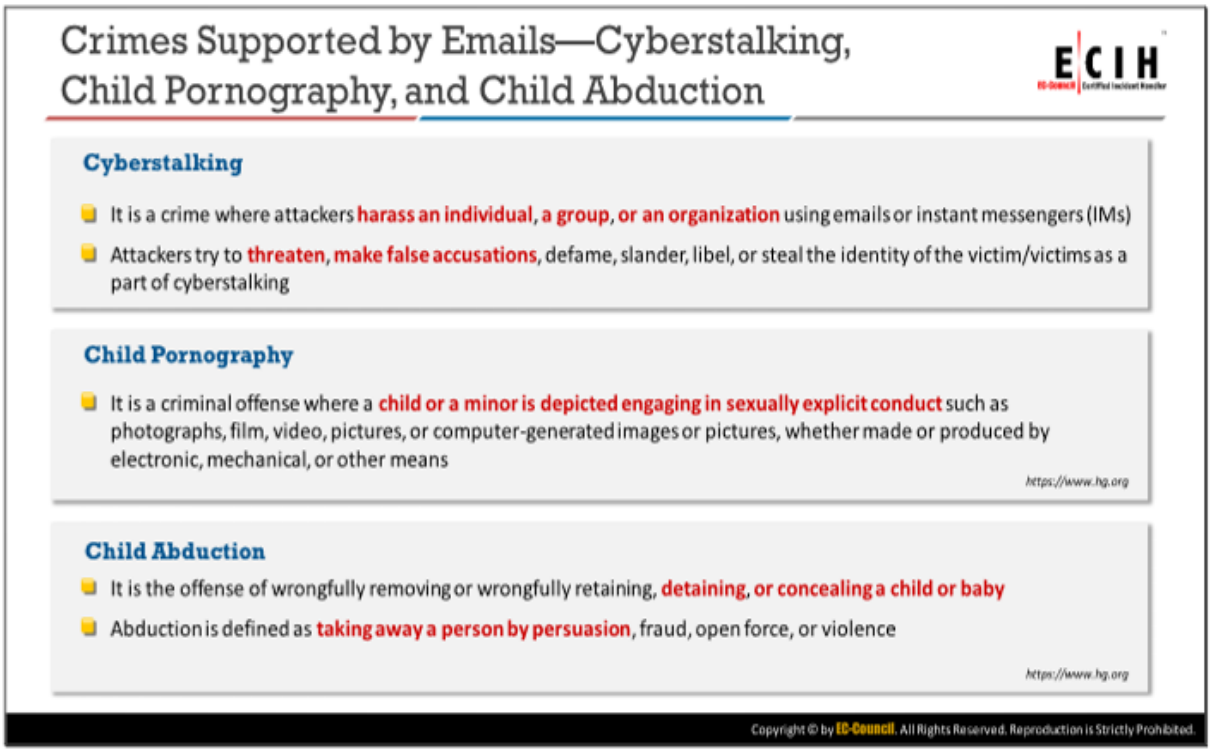
  Attackers may also use emails to send fake forms such as Internal Revenue Service (IRS) forms to gather information from the victims.

- **War Driving**

  Attackers search for unsecure Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecure networks, attackers access sensitive information stored in users' devices on those networks.

- **Mail Theft and Rerouting**

  Often, mailboxes contain bank documents (credit cards or account statements), administrative forms, and so on. Criminals use this information to obtain credit card information or to reroute the mail to a new address.



Crimes Supported by Emails—Cyberstalking, Child Pornography, and Child Abduction

- **Cyberstalking**

  Cyberstalking is a crime where attackers harass an individual, a group, or an organization using emails or IMs (instant messengers). Attackers try to threaten, make false accusations, defame, slander, libel, or steal the identity of the victim/victims as a part of cyberstalking. The stalker can be someone associated with the victim or a stranger.

- **Child Pornography**

  Source: *https://www.hg.org*

  Child pornography is a criminal offense where a child or a minor is depicted engaging in sexually explicit conduct in media such as photographs, film, video, pictures, or computer-generated images or pictures, whether made or produced by electronic, mechanical, or other means.

- **Child Abduction**

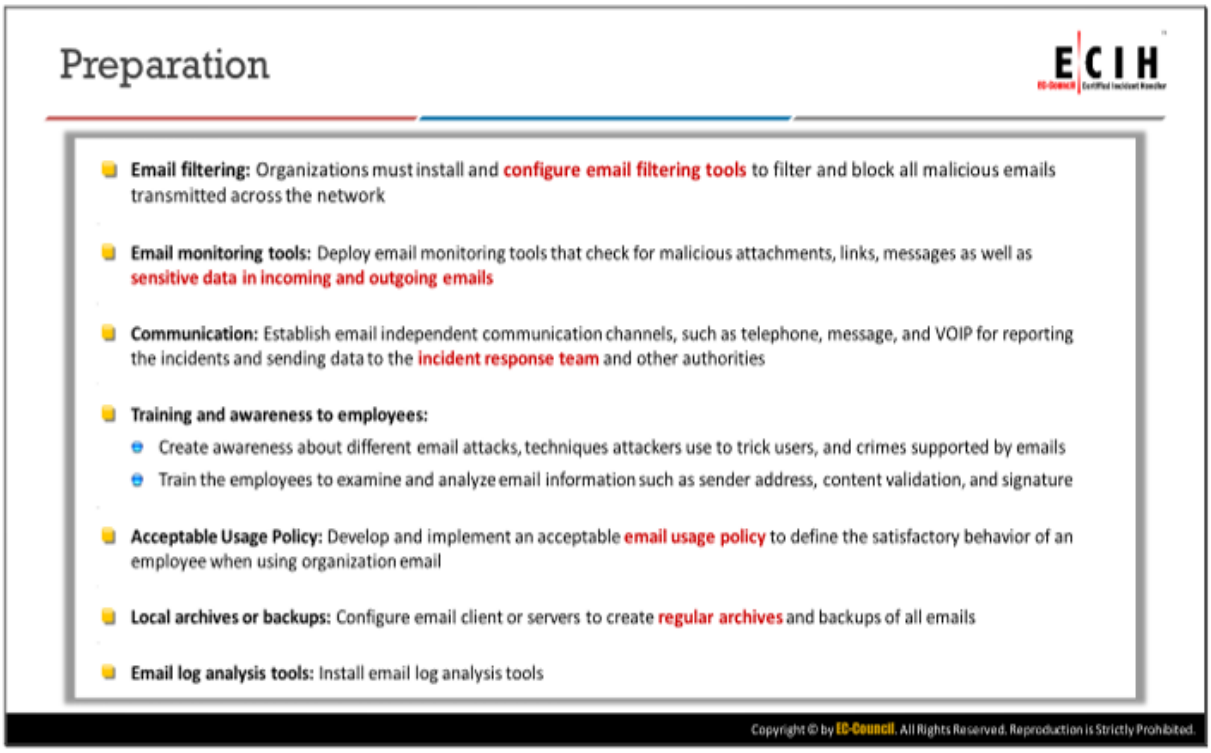
  Source: *https://www.hg.org*

  Child abduction is the offense of wrongfully removing or wrongfully retaining, detaining, or concealing a child or baby. Abduction is defined as taking away a person by persuasion, fraud, or open force or violence. There are two types of child abduction: parental child abduction and abduction by a stranger. Parental child abductions are the most common type, while abduction by stranger comes under kidnap.

Preparation for Handling Email Security Incidents

IH&R teams in the organizations must be well prepared for handling any kind of email security incident. Email incidents can cause severe damage to the organization, so organizations must take well-structured proactive measures in order to handle email security incidents.

This section discusses the preparation steps involved while handling email security incidents.



Preparation

Organizations must be able to handle and respond to various email attacks by developing and implementing proper incident response plans against the known attacks. Organizations must execute the following to handle and respond to the email incidents properly:

- **Email filtering**: Install and configure email filtering tools to filter and block all malicious emails transmitted across the network.
- **Email monitoring tools**: Deploy email monitoring tools that check for malicious attachments, links, messages as well as sensitive data in incoming and outgoing emails.
- **Communication**: Establish email-independent communication channels, such as telephone, message, and VOIP, for reporting incidents and sending data to the incident response teams and other authorities.
- **Training and awareness for employees**:
  - Create awareness about different email attacks, techniques attackers use to trick users, and crimes supported by emails.
  - Train the employees to analyze email information such as sender's address, content validation, and signature examining.
- **Acceptable usage policy**: Develop and implement an acceptable email usage policy to define satisfactory behavior of employees for using organization email.
- **Local archives or backups**: Configure email clients or servers to create regular archives and backups of all emails.
- **Email log analysis tools**: Install email log analysis tools.

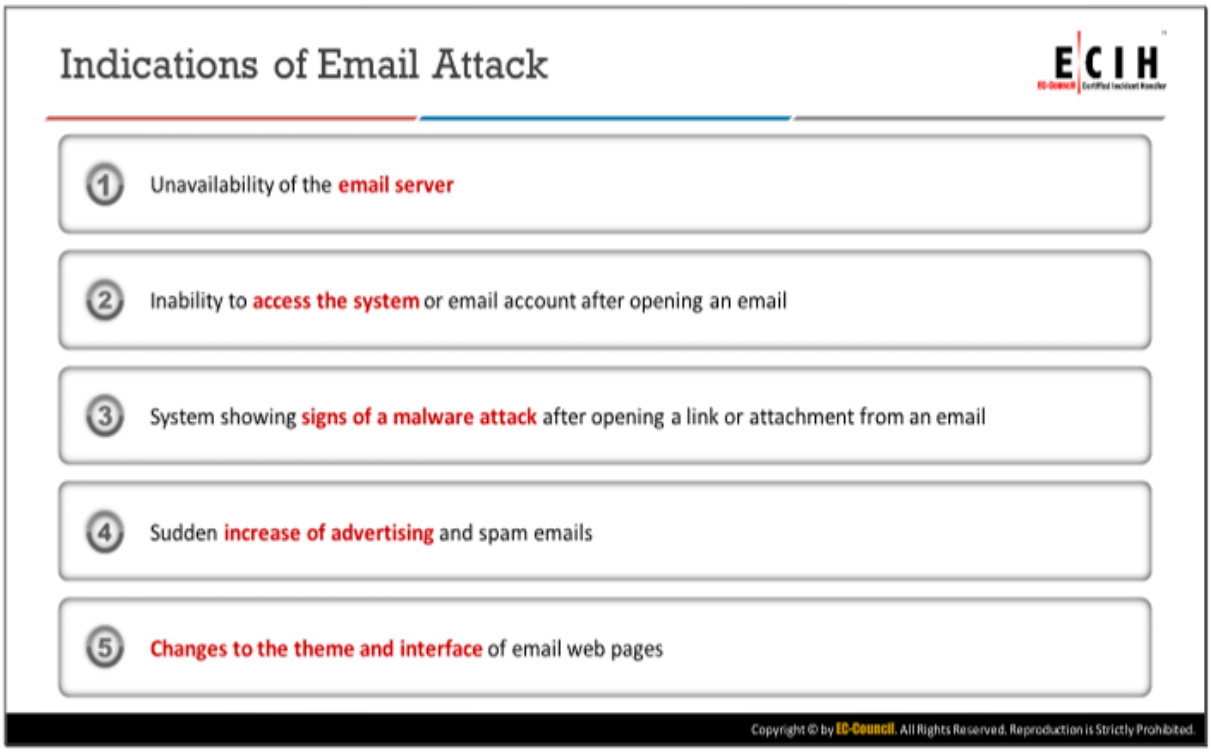
Apart from these, the organizations must provide the following to handle and respond to email security incidents:

- Provide proper information about the contact persons whom users can contact in case of an email security incident.
- Create a proper format for reporting and registering the complaints.
- Prepare a list of questions that the tech support must ask the complainants to analyze the type of email incident.

Detection and Containment of Email Security Incidents

Despite establishing various security measures, hackers explore various new means to perform attacks. IH&R team must be able to detect and contain the email security incidents in a spontaneous manner.

This section discusses various indications for detecting any email attack, identity theft, and phishing emails. This module also discusses analyzing email headers, email logs, and SMTP logs.

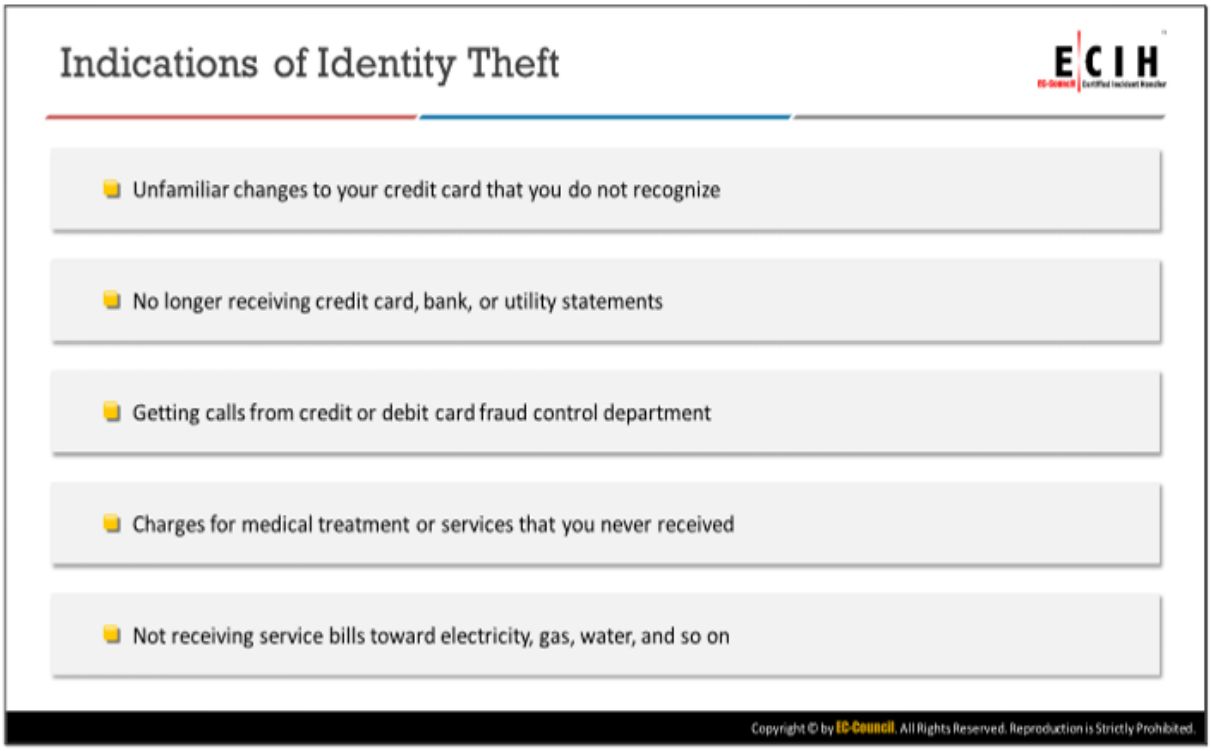


Indications of Email Attack

The organizations must train their employees in detecting email incidents by defining the indicators that relate to these attacks. The employees must identify these signs and immediately report them through a predefined process.

This helps the security team or IR team to contain and eradicate such incidents, and thus it reduces the losses. Some indicators of the email attacks include the following:

- Inability to access the system or the email account after opening an email
- System showing signs of malware attack after opening a link or attachment from an email
- Sudden increase of advertising and spam emails
- Unavailability of the email server
- Changes to the theme and interface of the email web pages
- Loss or unavailability of crucial emails and email folders
- Unusual or unidentified account activity
- Changes in email template and signature
- Data exfiltration alerts from security solutions
- Bouncing back of emails or reports of bounced emails
- Deletion of emails from the folders
- Reports and complaints from users, vendors, law firms, and third parties about spam and phishing emails from authorized email ID



Indications of Identity Theft

People do not realize that they are the victim of identity theft until they experience some unknown and unauthorized issues occurring due to their stolen identity. Therefore, it is of paramount importance that people should watch out for the warning signs for their identities that have been compromised.

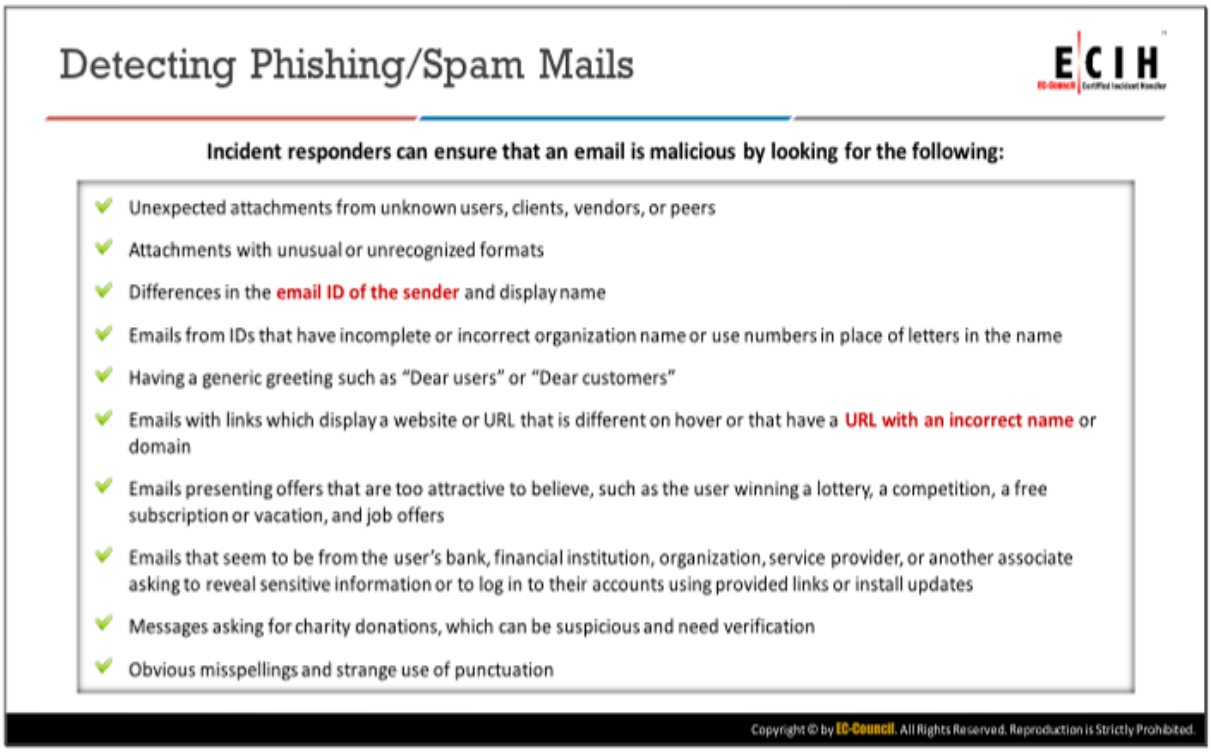
Listed below are some of signs showing you are a victim of an identity theft:

- Unfamiliar changes to your credit card that you do not recognize
- If creditors call asking about an unknown account in your name
- Numerous traffic violations under your name that you did not commit
- Charges for medical treatment or services you never received
- More than one tax return filed under your name
- Denial of your own account operation and of loans or other services
- Not receiving bills for services such as electricity, gas, water, and so on, an indication of your stolen mail
- Sudden changes in personal medical records showing a condition you do not have

Some additional indications of identity theft are as follows:

- Receiving a notification that your information was compromised or misused by a data breach in a company where you are an employer and have an account
- Inexplicable cash withdrawal from your bank account

- Calls from debit or credit card fraud control departments warning about suspicious activities on your accounts
- No claim of government benefits by you and your child because those benefits are already being received by some other account using the Social Security number (SSN) of your child
- Your medical insurance plan rejects your true medical claim because someone tampered your medical records and you reached your benefits limit

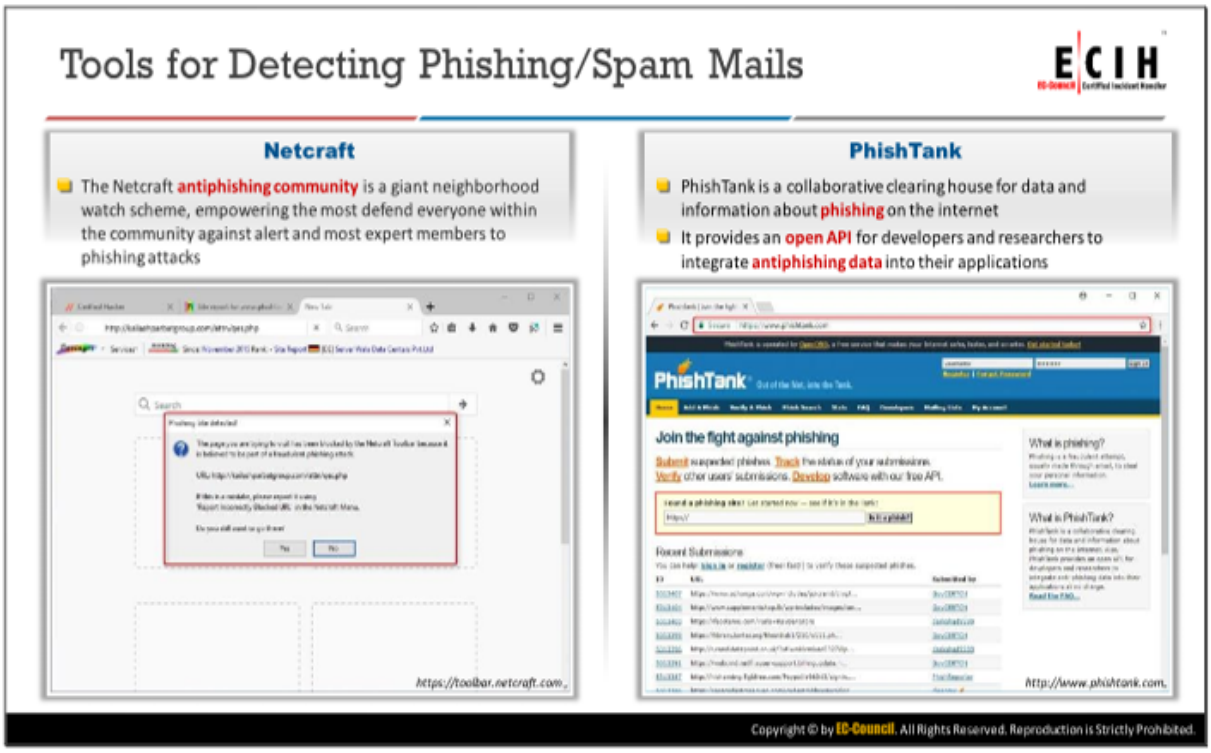


Detecting Phishing/Spam Mails

Incident responders can detect and verify if the email is malicious by looking for the following:

- Unexpected attachments from unknown users, clients, vendors, or peers
- Attachments with unusual or unrecognized formats
- Differences in the email ID of the sender and display names
- Emails from IDs that have incomplete or incorrect organization names or that use numbers in place of letters in the name
- Having generic greeting such as "Dear users" or "Dear customers"
- 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 the user winning a lottery, a competition, or a free subscription or vacation, and job offers
- Some emails try to arouse a sense of urgency and can seem to be from persons known to the users, such as relatives, family, and colleagues, and ask the user to immediately transfer funds to help them
- Emails that seem to be from the user's bank, financial institution, organization, service provider, or other associate, that ask to reveal sensitive information or log in to their accounts using provided links or install updates
- Messages asking for charity donations can be suspicious and need verification
- Obvious misspellings and strange uses of punctuation

- The mails that request personal information from the receivers is also a phishing or spam mail
- Emails that do not have a complete signature and contact details of the sender



Tools for Detecting Phishing/Spam Mails

Incident handlers can use various automated tools for detecting phishing and spam emails. Discussed below are some of the important tools for detecting phishing emails:

- **Netcraft**

  Source: *https://toolbar.netcraft.com*

  The Netcraft Toolbar provides updated information about the sites users visit regularly and blocks dangerous sites. The toolbar provides you with a wealth of information about the sites you visit. This information will help you make an informed choice about the integrity of those sites.

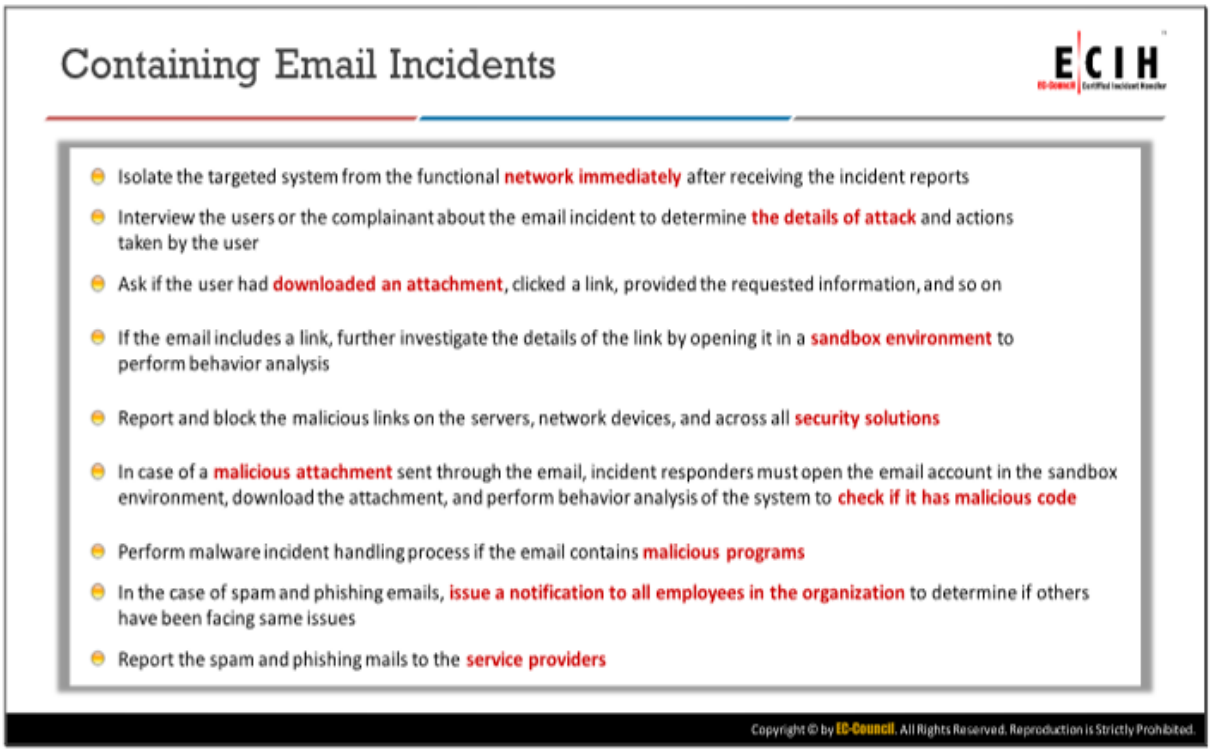
  Features:

  - Protects your savings from phishing attacks
  - Observes the hosting location and risk rating of every website visited (as well as other information)
  - Helps in defending the internet community from fraudsters
  - Checks if a website supports perfect forward secrecy (PFS)
  - Observes if a website is affected by the aftermath of the Heartbleed vulnerability

- **PhishTank**

  Source: *http://phishtank.com*

  PhishTank is a collaborative clearinghouse for data and information about phishing on the internet. It provides an open API for developers and researchers to integrate antiphishing data into their applications.



Containing Email Incidents

Immediately after detecting an incident, the incident responders must initiate the process of containment to reduce the impact. You must perform the following to detect and contain email incidents:

- Isolate the targeted system from the functional network immediately after receiving the incident reports and temporarily block the targeted email account.
- Interview the users or complainant about the email incident to determine the details of attack and user actions.
- Ask if the user had downloaded the attachment, clicked the link, provided the requested information, and so on.
- Gather information about the incident such as type of email attack, impact, and losses.
- If the email consists of a link, find further details of the link by opening it in a sandboxed environment to perform behavior analysis.
- Identify the source of the email and verify its authenticity.
- Gather complete details about the email such as its header information, including the source of the email and IP address.
- Perform investigation of the email by analyzing the URL, attachments, domain names, IP addresses, and other obtained details.
- Report and block the malicious links on the servers, network devices, and across all security solutions.

- In case of a malicious attachment sent through the email, incident responders must open the email account in the sandbox environment, download the attachment, and analyze the attachment to check if it has malicious code.
- Perform the malware incident handling process if the email contains malicious programs.
- In case of spam and phishing emails, issue a notification to all employees to learn if others have been facing the same issues.
- Report the spam and phishing mails to the service providers.
- Contain the impact of the email to other employees by identifying key objectives in the mail and implement filters to block similar signature mail.
- Check the firewall logs to identify the suspicious IP addresses and URLs.
- Check the DNS logs as some attackers hide their identity through frequent IP spoofing.
- Analyze and verify the DHCP logs to know the hosts associated with the suspicious IP addresses.
- Analyze the organization's mail server logs to obtain additional information about the email attack such as number of victim systems, message IDs, and IP addresses.
- Change the passwords and other sensitive information for affected email accounts and systems.
- Identify all the other active sessions related to the email from the victimized system and close them.

Analyzing Email Headers

01

"Received" headers show a detailed log of a message's history. These headers help to draw conclusions about the origin of an email, which also provides information on whether the headers have been forged

02

If, for instance, the machine xsecurity.com, whose IP address is 104.128.23.115, sends a message to mail.target.com, but falsely reports **HELO example.org**, the resultant "Received" line might start like this:

Received: from example.org ([104.128.23.115]) by mail.target.com (8.8.5)...

Analyzing Email Headers (Cont'd)

Gather the following items of supporting evidence from the email headers to track the suspect

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

Analyzing Email Headers (Cont'd)

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?
```


Analyzing Email Headers (Cont'd)

Sender Policy Framework (SPF)

- SPF is an email validation protocol used by domain owners for **preventing the spoofing of emails**
- Incident responders can analyze the **authenticity of the sender** using the SPF results
- The SPF will display results mentioned in the following table:

Result	Explanation
None	No SPF records are found for this domain
Pass	SPF record exits and IP address is authorized. It includes a plus (+) sign in front of the IP address
Neutral	This means that the domain owner does not want to disclose the specific IP address authorized in SPF record. It includes all commands specified in the SPF record
Fail	IP address is not authorized to send email for this domain. This is shown by a –all command in the record.
SoftFail	This result is between neutral and fail. This means that the mail is authorized but is tagged as suspicious or spam
TempError	Indicates the occurrence of a temporary error such as technical issue during verification
PermError	SPF record cannot be verified due to syntax or format errors in the record

Analyzing Email Headers (Cont'd)

Domain Keys Identified Mail (DKIM)

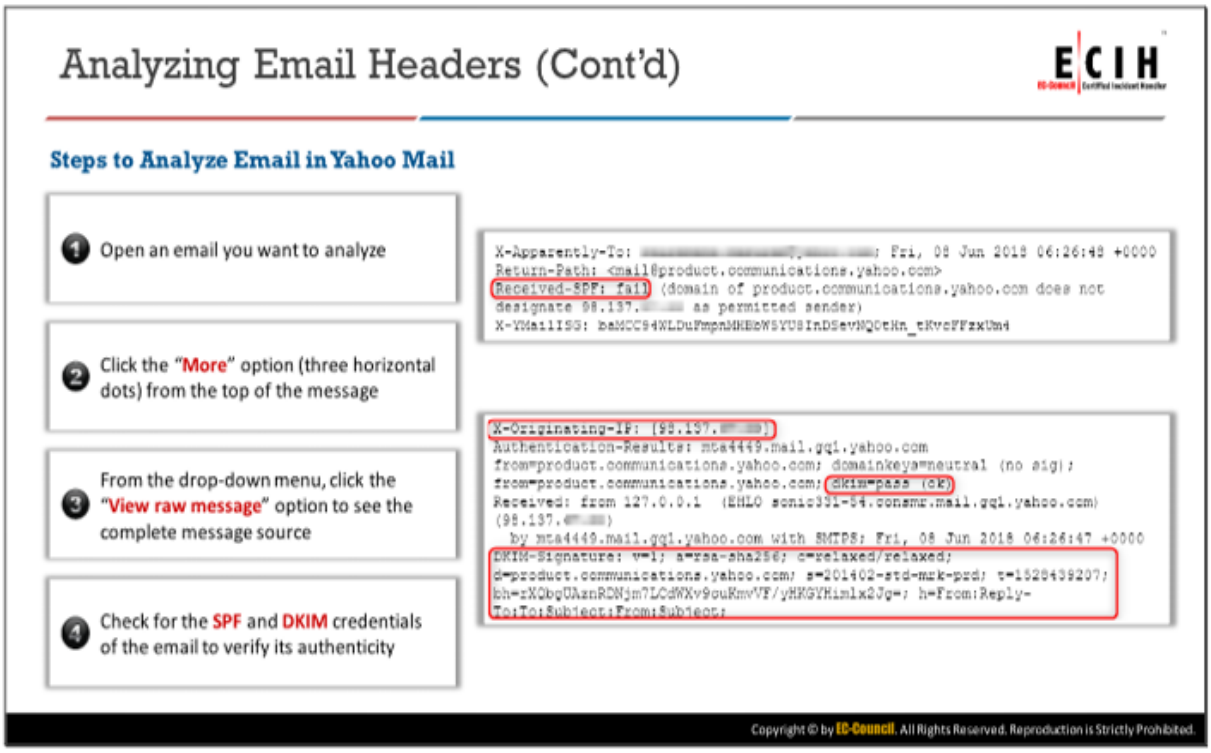
- DKIM is an **email authentication** standard designed to detect spoofing
- Using this standard, the domain owner can encrypt the domain's outgoing mail headers and add a **digital signature** to the outgoing emails for better authentication
- Incident responders can analyze the **integrity of the email** by analyzing its DKIM results
- The DKIM standard will display results mentioned in the following table:

Result	Explanation
Pass	Mail is signed and the signature passes the verification tests
Neutral	Mail is signed but the signature has syntax errors and therefore cannot be processed
Fail	Mail is signed and the signature does not pass the verification tests
Policy	Mail is signed and some part of signature is not acceptable by administrative management domains (ADMD)
TempError	Mail is not verified due to temporary errors such as cannot retrieve public key and transient in nature
PermError	Mail is not verified due to permanent errors such as absence of required header field

Analyzing Email Headers (Cont'd)

Steps to Analyze Email in Gmail

1. Open an email you want to analyze
2. Click the "**More**" option (three vertical dots) from the top-right of the message
3. From the drop-down menu, click the "**Show original**" option
4. The mail will **open a new tab** displaying the original message
5. Check for the **SPF** and **DKIM credentials** of the email to verify its authenticity



Analyzing Email Headers

Received headers of an email message provide information about the message origin, the route it took to reach the recipient, and the cause of delivery delays. It is important to examine this part of the email header once we identify that the email is spam.

When the SMTP Server receives an email message, a Received Header gets added to the email. Therefore, Received Headers are essentially in reverse order; in other words, the last Received Header added is the first one at the top. To understand the Received Headers correctly, read from the bottom (first Received Header) to the top (last Received Header).

Incident responders must be aware of the forged headers, which attackers make up to deceive the users, systems, security, and so on and enter the normal traffic.

If, for instance, the machine turmeric.com, whose IP address is 104.128.23.115, sends a message to mail bieberdorf.edu but falsely says HELO galangal.org, the resultant "Received" line might start like this:

Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...

This means that the email sent from turmeric.com might have "Received" lines that look something like this:

Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...

Received: from nowhere by outer space (8.8.3/8.7.2)...

Information to be Gathered from the Malicious Email Headers

The incident responder can track fraudulent email's originating location by examining the email header. The most valuable information for investigation is the originating email's domain

address or IP address. Other supporting data is the date and time of the message sent, attachment filenames, and the unique message number.

Gather the supporting evidence from the email headers and track the suspect as given below:

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

Example of Email Header Analysis

In the email header shown on the above slide, Received: from mail.bieberdorf.edu represents that a machine named mail.bieberdorf.edu sent the mail and bears the IP address 124.211.3.11 by using the Sendmail version 8.8.5 with assigned ID number 004A21.

The rth@bieberdorf.edu, who gives his real name as R.T. Hood, sent the mail to tmh@immense-isp.com with mail ID rth031897143614-00000298@mail.bieberdorf.edu.

This ID does not represent the SMTP and ESMTP ID numbers and is attached to this message for life. The sender used a program called Loris, version 2.32, to send the message.

Sender Policy Framework (SPF)

SPF is an email validation protocol used by domain owners for preventing spoofing of emails. It allows owners of the domain to create a public list of approved senders, who send emails on the owner's behalf. It contains IP addresses or hostnames of authorized senders. SPF does not validate the domain name mentioned in the from address, but verifies it using Return-Path value. Incident responders can analyze the authenticity of the sender using the SPF results. The SPF will display results mentioned in the table shown on the slide.

Domain Keys Identified Mail (DKIM)

DKIM is an email authentication standard designed to detect spoofing. Using this standard, the domain owner can add a digital signature to the outgoing emails for better authentication. They can also encrypt the domain's outgoing mail headers and add a public version of the key to the domain's DNS records in the email. The sending mail transfer agent (MTA) generates the signature using an algorithm and stores the public key used at the domain. The recipient MTA recovers the public key through DNS and uses it to decrypt and verify the DKIM signature to validate the integrity of the mail.

Incident responders can analyze the integrity of the email by analyzing its DKIM results. The DKIM standard will display results mentioned in the table shown on the slide.

The incident responders must analyze the headers to gather additional information about the email. Before analyzing, the responders must view the original content of the email or the source of the message. Different email service providers have different methods for viewing the original message. Now, we will observe the steps to analyze email in Gmail and Yahoo mail.

Steps to Analyze Email in Gmail

In Gmail,

1. Open the suspicious email.
2. Click the "**More**" option (three vertical dots) from the top-right of the message. It will display a drop-down menu.

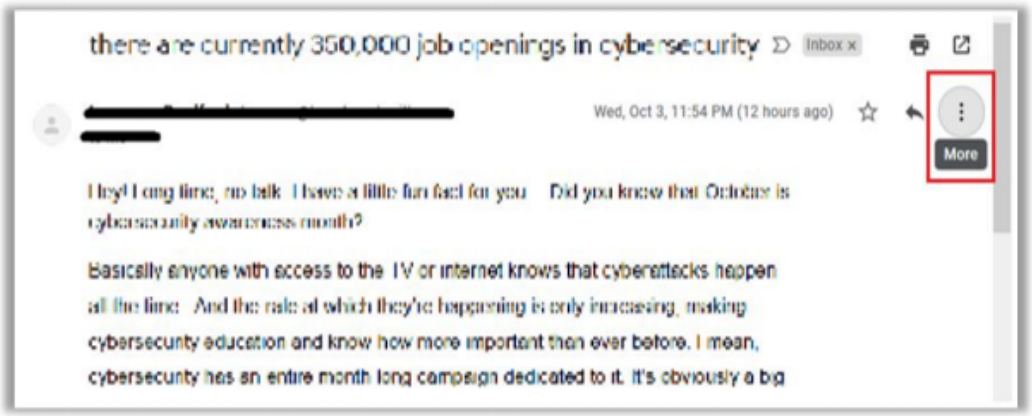


Figure 5.2: Spam mail

3. From the drop-down menu, click "**Show original**" option.

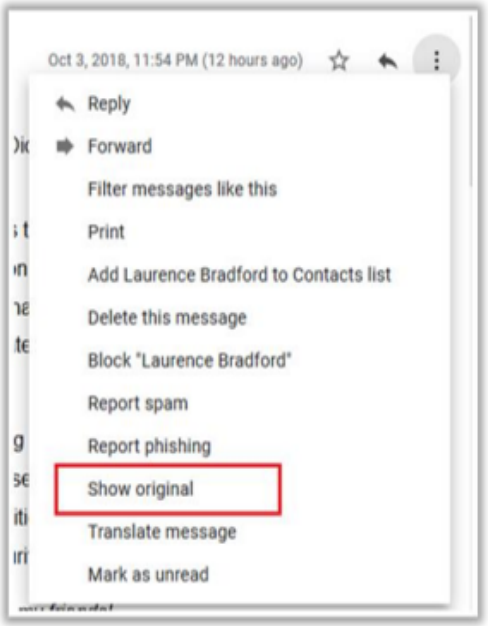


Figure 5.3: Show original option

4. The mail will open in a new tab displaying the original message.
5. Check for the **SPF** and **DKIM** credentials of the email to verify its authenticity.

Steps to Analyze Email in Yahoo Mail

In Yahoo mail,

1. Open the suspicious email.
2. Click the "**More**" option (three horizontal dots) from the top of the message. It will display a drop-down menu.

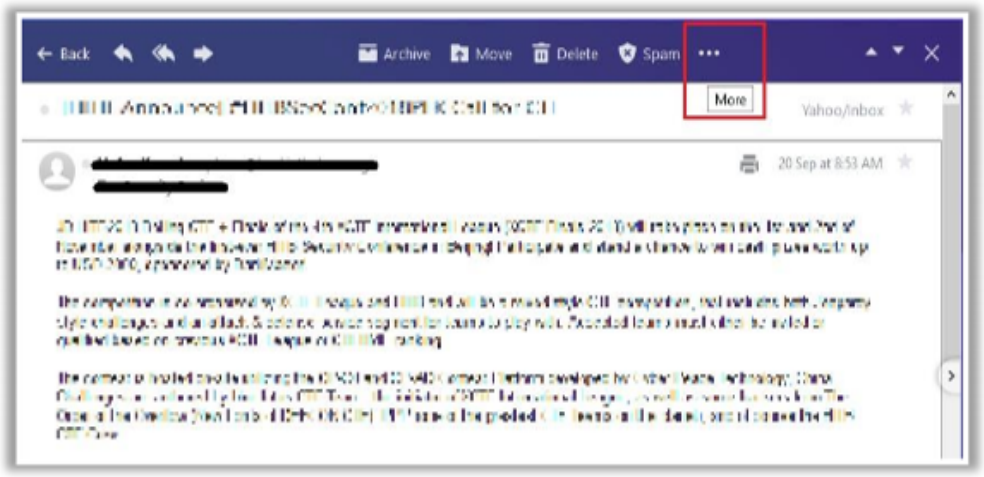


Figure 5.4: Spam mail

3. From the drop-down menu, click "**View raw message**" option to see the complete message source.

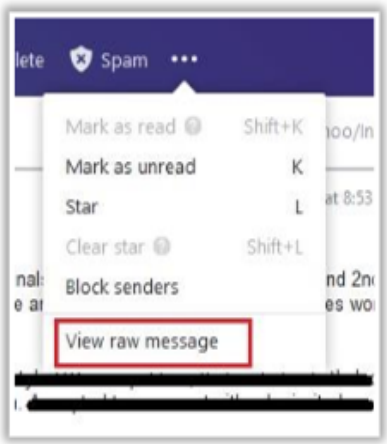


Figure 5.5: View raw message option

4. Check for the **SPF** and **DKIM** credentials of the email to verify its authenticity.

Tools for Analyzing Email Headers

Discussed below are some of the important email header analysis tools that help incident handlers to detect spam/malicious emails:

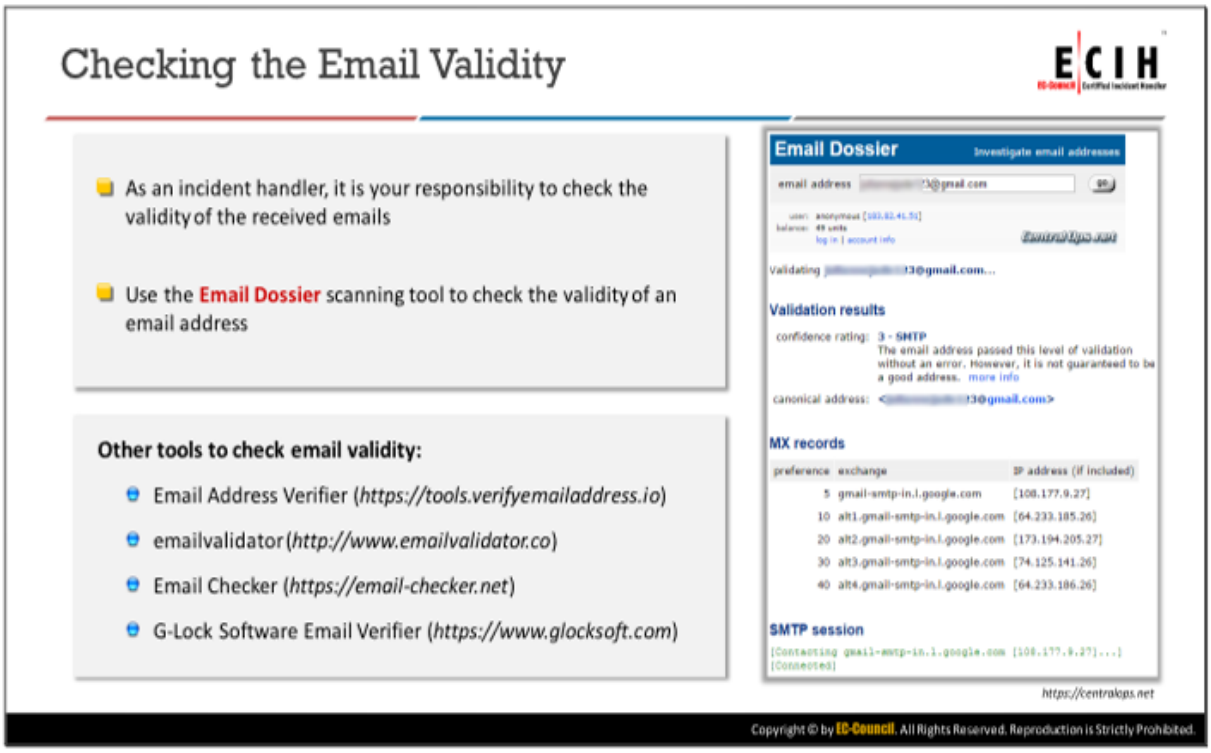
- **MxToolbox**

  Source: *https://mxtoolbox.com*

  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, including hop delays, and antispam results. Incident handlers can use this tool to analyze email headers and detect spam emails.

Listed below are some of the additional tools for analyzing email headers:

- E-Mail Header Analyzer (*https://www.gaijin.at*)
- Message Header Analyzer (*https://testconnectivity.microsoft.com*)
- ipTRACKEREonline.com (*https://www.iptrackeronline.com*)
- G Suite Toolbox (*https://toolbox.googleapps.com*)
- Email Header Analyzer (*https://www.whatismyip.com*)



Checking the Email Validity

A valid email address is the one to which we can send or receive emails. There are particular standards and guidelines for validating email addresses. In the process of detecting and containing malicious emails, as an incident handler, it is your responsibility to check the validity of the received emails. Among the tools that IH&R team can use to check the validity of emails are Email Dossier and Email Address Verifier.

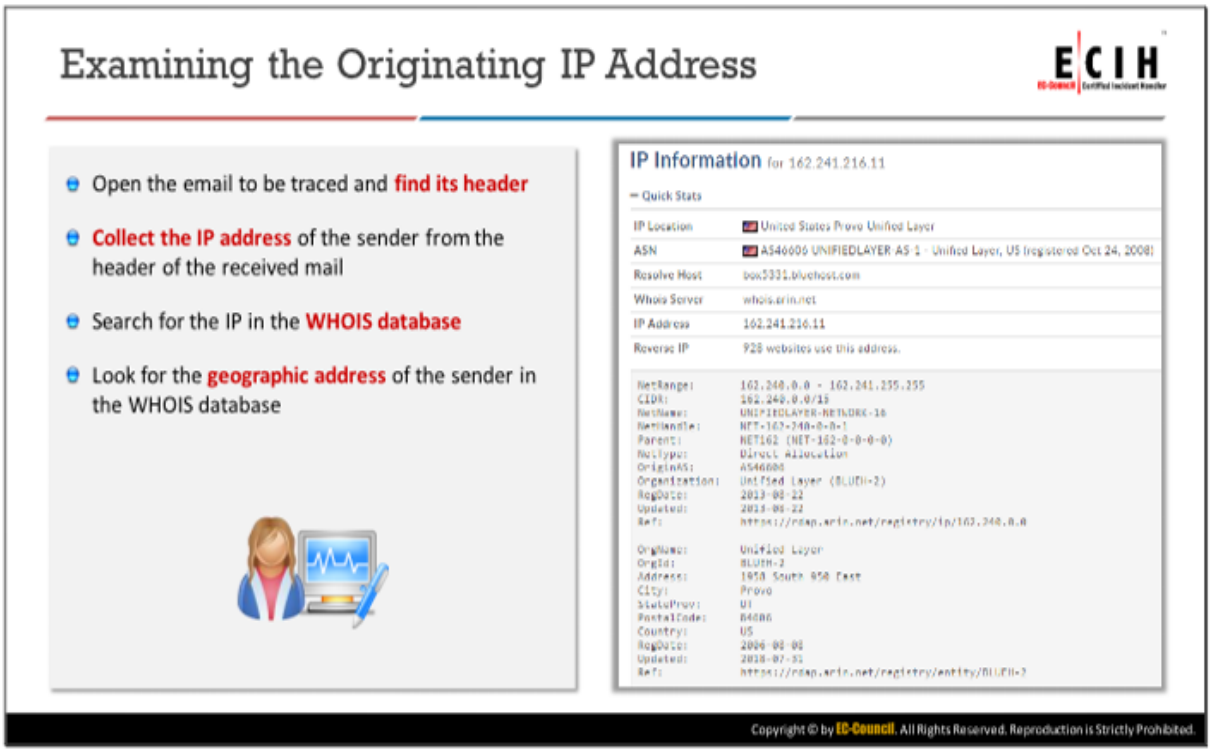
- **Email Dossier**

  Source: *https://centralops.net*

  Email Dossier is a part of the CentralOps.net suite of online network utilities. It is a scanning tool that the incident handler can use to check the validity of an email address. It provides information about the email address, including the mail exchange records. This tool initiates SMTP sessions to check address acceptance, but it never actually sends email.

Some of the other tools to check email validity are as follows:

- Email Address Verifier (*https://tools.verifyemailaddress.io*)
- emailvalidator (*http://www.emailvalidator.co*)
- Email Checker (*https://email-checker.net*)
- G-Lock Software Email Verifier (*https://www.glocksoft.com*)

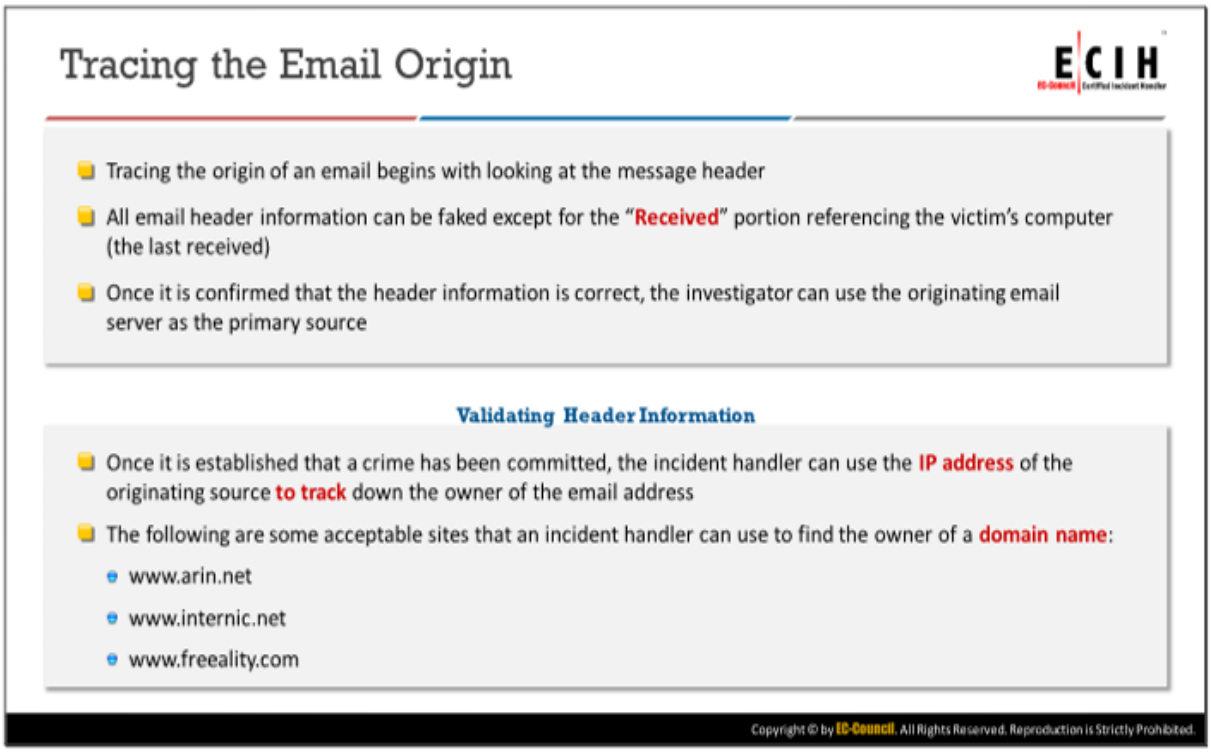


Examining the Originating IP Address

In the process of detecting and containing malicious emails, incident responders should examine the originating IP address of the emails.

The following steps are involved in the process of examining the originating IP address:

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



Tracing the Email Origin

Email origin refers to the details of the source used to send the email. It includes the IP address, mail server, username, domain name, and so on. These details will help the incident handlers in tracing the perpetrator or sender of an email as well as understanding the motive behind the attack. To achieve this, the incident handlers need to further examine the email message header with one of the free internet tools.

Validating Header Information

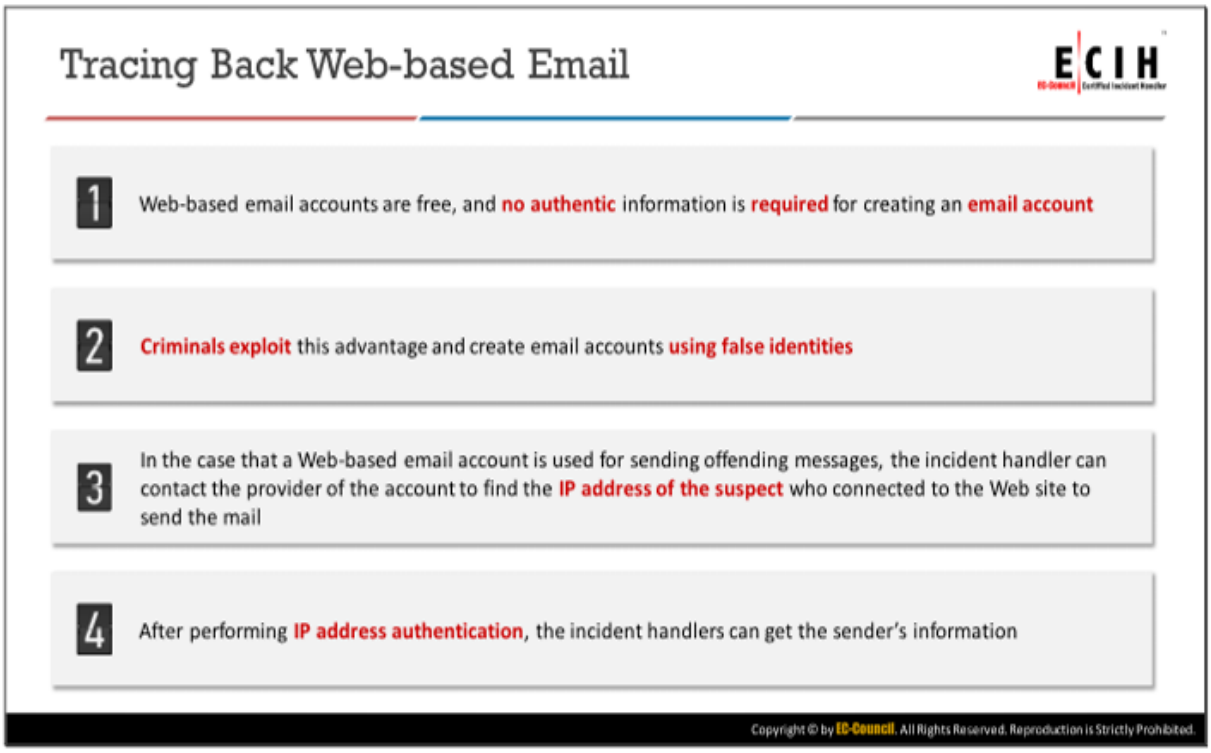
Tracing back email begins by looking at the message header information. The header has a subject, date, and the "From"/"Received" address. The "From" line contains the source of the email, and "Received" indicates every point the email passed through, along with the date and time. Attackers can fake all email header information except the "Received" portion referencing the victim's computer (the last received).

Once the incident handlers confirm that the header information is correct, they can use the originating email server as the primary source to trace back. The incident handlers can approach the court and get a court order served by law enforcement or a civil complaint filed by attorneys. The court order helps to obtain the log files from the server in order to determine the sender. After getting the contact information about the suspect, they can take punitive steps against the suspect.

The incident handlers may use the following registry sites to determine the Email origin:

- **www.arin.net:** It employs the American Registry for Internet Numbers (ARIN) to match the domain name for an IP address. It also provides the point of contact for the domain name.
- **www.internic.com:** It provides the identical information given by www.arin.net.

- **www.freeality.com:** This site provides the various options for searching such as email address, phone numbers, and names. One can do a reverse email search, which could reveal the subject's real name. This site can do other searches such as reverse phone number searches and address searches.



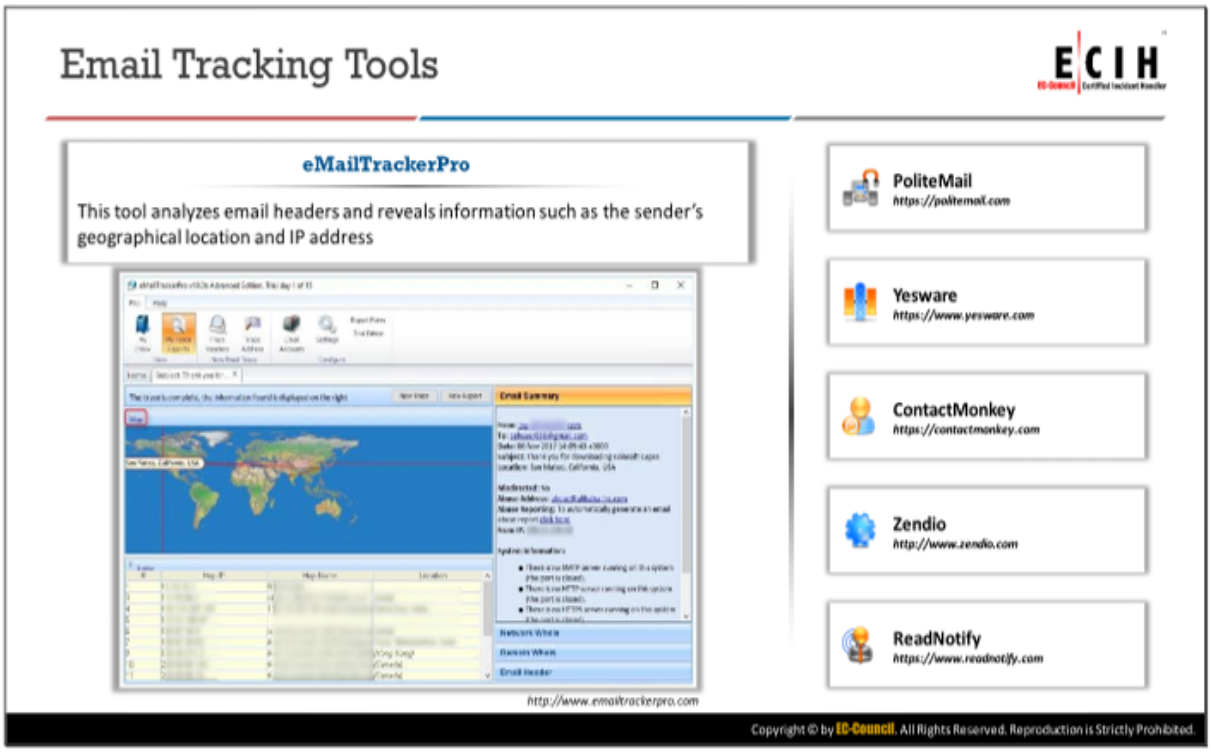
Tracing Back Web-based Email

There are two ways to transmit an email over the internet. One is by using the email program installed on the machine, and the other is an email service on the web.

Email programs such as Eudora and Outlook require configuration with the ISP, and if one wants to use the email program on another computer, he or she has to first install the email program on that computer. Tracing a suspect becomes far easier in this case.

On the other hand, if one is using web-based email, then it becomes difficult to trace the sender. One can read and send the email from any computer and from any part of the world. These web-based emails are free, and no authentic information is required for creating an email account. The criminals exploit this advantage and create fake email accounts using false details.

When the attacker sends offending messages through a web-based email account, the incident handler can contact the provider of the account to find the IP address of the suspect who connected to the website to send the mail. The online websites Yahoo!, Hotmail, and so on maintain the IP address of each machine accessing their email services. After IP address authentication, the examiner can contact an email provider to get the sender's information.



Email Tracking Tools

Email tracking tools help incident handlers track an email and extract information such as sender identity, mail server, sender's IP address, location, and so on. These tools send notifications automatically when the recipients open the mail and give status information about whether the email was successfully delivered or not.

Discussed below are some of the important email tracking tools:

- **eMailTrackerPro**

  Source: *http://www.emailtrackerpro.com*

  eMailTrackerPro analyzes email headers and reveals information such as sender's geographical location, IP address, and so on**.** It allows an attacker to review the traces later by saving past traces.

The following are a few of the most widely used email tracking tools:

- PoliteMail (*https://politemail.com*)
- Yesware (*https://www.yesware.com*)
- ContactMonkey (*https://contactmonkey.com*)
- Zendio (*http://www.zendio.com*)
- ReadNotify (*https://www.readnotify.com*)
- DidTheyReadIt (*https://www.didtheyreadit.com*)
- Trace Email (*https://whatismyipaddress.com*)

- Email Lookup – Free Email Tracker (*http://www.ipaddresslocation.org*)
- Pointofmail (*https://www.pointofmail.com*)
- WhoReadMe (*http://whoreadme.com*)
- GetNotify (*https://www.getnotify.com*)
- G-Lock Analytics (*https://glockanalytics.com*)

Analyzing Email Logs

- For analyzing emails in organizations having internal email servers, the responders must validate and **verify the email addresses**, sources, and paths related to the suspected emails
- It is important to **examine logs** to figure out if the attacker has tampered the email header after the incident
- Logs will also help in determining if the attacker has deleted the email after an attack

Examining System Logs

- By examining system logs, an incident handler can verify the path taken by an email
- Because the email logs are internet-based, the IRT can check the **IIS logs** of a system

Examining Network Equipment Logs

- By examining the router and firewall logs, it is possible for the incident handler to verify the times and the **IP addresses** contained within the email
- These logs provide the email message ID information, source address, and destination address of the servers used to send the email

Analyzing Email Logs (Cont'd)

Examining Microsoft Exchange Email Server Logs

- Microsoft Exchange uses the **Microsoft Extensible Storage Engine** (ESE)
- It uses **Messaging Application Programming Interface** (**MAPI**), which allows the collaboration of various email applications in an organization
- While investigating a Microsoft Exchange server for email crimes, an incident handler should primarily focus on the following files:
  - **.edb database** files (responsible for MAPI information)
  - **.stm database** files (responsible for non-MAPI information)
  - **checkpoint** files
  - **temporary** files

Examining Linux Email Server Logs

- `sendmail` is the command used to send emails via a Linux or UNIX system
- `sendmail` uses `syslog` to maintain logs for understanding what has exactly happened on the system
- `/etc/syslog.conf` is the syslog configuration file, which determines the location of service logs stored by syslog
- `syslog.conf` also contains information regarding the logging priority, where logs are sent, and what other actions may be taken
- `syslog.conf` also provides the location of the log file for email, which is usually `/var/log/mailog`
- The `/var/log/mailog` file contains source and destination IP addresses, date and time stamps, and other information necessary to validate the data within an email header
- As an incident responder, you must analyze all these logs to detect the traces of abnormal or malicious emails

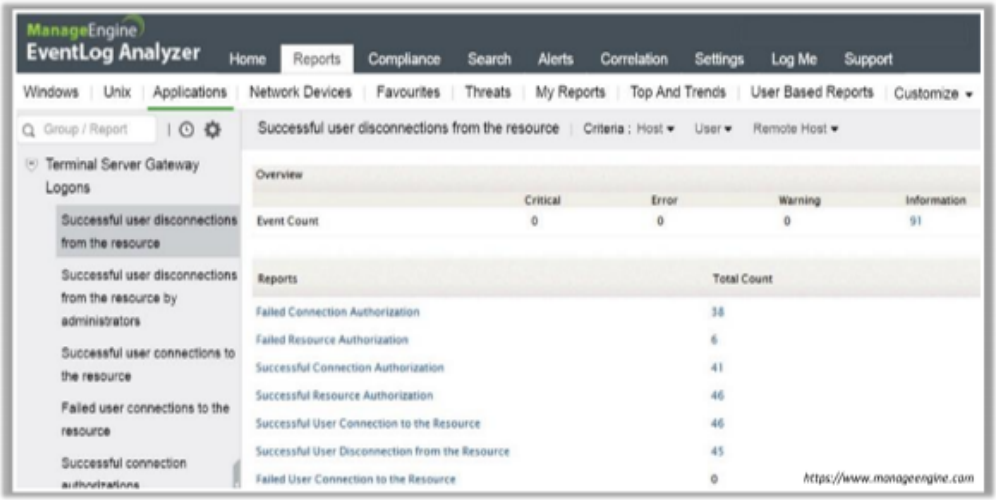
Analyzing Email Logs (Cont'd)

Examining Novell GroupWise Email Server Logs

- **GroupWise** is an **email service platform by the Novell NetWare**. It stores the user's messages in almost 25 proprietary databases
- Every database is stored in the **OFUSER Directory** object and is referenced by a username, followed by a unique ID and the .db extension
- The **NGWDFR.DB database**, present in the OFMSG directory object, is used for delayed or deferred emails
- **Guardian (Ngwguard.db)** is a specialized database that:
  - Maintains **centralized control** of the email services
  - **Tracks changes** in the GroupWise environment
  - Includes built-in safeguards like **Ngwguard.fbk**, **Ngwguard.rfl**, and **Ngwguard.db**, which helps in preventing data loss
- **GroupWise** generates log files (.log extension) maintained in GroupWise folders, which can be used to match an email header with a suspect's IP address

Analyzing Email Logs (Cont'd)

Use tools such as **EventLog Analyzer** to analyze **email logs at server level** and detect the emails used by attackers for phishing or spamming



Analyzing Email Logs

Email logs are very useful in email security incidents to reveal various activities of attackers. Although the attackers are capable of altering the email headers, they cannot change the logs across the network, routers, firewalls, system, and so on. Emails need to pass through all these devices. Incident handlers can use logs from various devices to check the email path and other details.

The incident handlers must analyze the email logs to identify the type of email incidents, their impact, timeline, source, and activities they perform.

They identify email messages through the following:

- The received account
- IP address of the system from which they were sent
- Time and date
- IP addresses

Examining System Logs

Systems store details of all the traffic they receive and send, along with details such as application, user, port, and protocol used to transfer the data. Therefore, system logs also contribute to the analysis of emails and provide detailed data about them. Incident handlers should examine the system logs to verify the email path. As the email logs are internet based, the IRT can check the IIS logs of a system.

Examining Network Equipment Logs

Network equipment, such as routers, switches, firewall, and server, store the transmission data and logs. Incident handlers can work in association with the administrators to gather the inbound and outbound traffic logs. The logs from the routers include details of the traffic they allow or deny, source or destination IP addresses, types of transmission, and so on. By examining the router and firewall logs, it is possible for the incident handler to verify the times and the IP addresses contained within the email. These logs provide email message ID information, source addresses, and destination addresses of the servers used to send the email.

Network admins also maintain firewall logs that filter internet traffic, and these logs may contain details of emails that have passed through the firewall. Gathering all the details and their cross-checking can help in finding the difference between header information and the information provided by the other sources to determine if there has been any tampering.

Examining Microsoft Exchange Email Server Logs

In organizations using the Microsoft Exchange email servers, the incident responders must understand that Microsoft Exchange uses the Microsoft Extensible Storage Engine (ESE), which in turn employs Messaging Application Programming Interface (MAPI) for the collaboration of various email applications in the organization. Thus, while investigating a Microsoft Exchange server for email crimes, an incident handler should primarily focus on the following files:

- .edb database files (responsible for MAPI information)
- .stm database files (responsible for non-MAPI information)
- checkpoint files
- temporary files

While analyzing logs, analyzing the checkpoints, temporary files, and transaction logs is a crucial task, for these reasons:

- Checkpoint files helps the incident responder determine if any data loss has occurred after the last backup, thus allowing the incident responder to recover lost or deleted messages.
- Temporary files store the information received by the server when it was too busy to process that information immediately. System retains these temporary files that may be recovered for investigation purposes.
- Transaction log preserves and processes modifications done in the database file. So, these logs can be used by the incident responder to determine if the email has been sent or received by the server.

Apart from the aforementioned:

- An incident responder can use Windows Event Viewer for the following:
  - Tracking log (allows to view message content associated with the email).
  - Troubleshooting or diagnostic logs (records a number of events for each email sent or received). In addition, an Event Properties dialog box provides more information in forensic investigations.
- Incident responder can also use the Performance Analysis of Logs (PAL) Tool (*https://github.com*) to monitor and analyze the logs for identifying phishing and malware distribution emails.
- An incident responder can use **`Get-MessageTrackingLog`** PowerShell command to trace the flow of email from sender to receiver.

Examining Linux Email Server Logs

`Sendmail` is the command used to send emails via Linux or UNIX system. It requires the information regarding the source and destination addresses, the sender and recipient addresses, and the email message ID. This sendmail uses **`Syslog`** to maintain logs for understanding what exactly happened on the system. The syslog configuration file, **`/etc/syslog.conf`** determines the location of syslog service logs. This syslog configuration file contains information on the logging priority, where logs are sent, and what other actions may be taken. The **`syslog.conf`** also provides the location of the log file for email, which is usually **`/var/log/mailog`**. The **`/var/log/mailog`** file contains source and destination IP addresses, date and time stamps, and other information necessary to validate the data within an email header. As an incident responder, you must analyze all the logs that are mentioned above to detect the traces of abnormal or malicious emails.

Examining Novell GroupWise Email Server Logs

GroupWise is an email service platform created by Novell NetWare. It stores the user's messages in almost 25 proprietary databases. It stores all the databases in the OFUSER Directory object and references them by username, followed by a unique ID and the .db

extension. The NGWDFR.DB database, present in the OFMSG directory object, is used for delayed or deferred emails. Guardian (Ngwguard.db) is a specialized database that

- Maintains centralized control of email services
- Tracks changes in the GroupWise environment
- Includes built-in safeguards like Ngwguard.fbk, Ngwguard.rfl, and Ngwguard.db, which help in preventing data loss

GroupWise generates log files (.log extension), maintained in GroupWise folders, which responders can use to match an email header with a suspect's IP address. Incident responders must analyze these logs to find the anomalous emails.

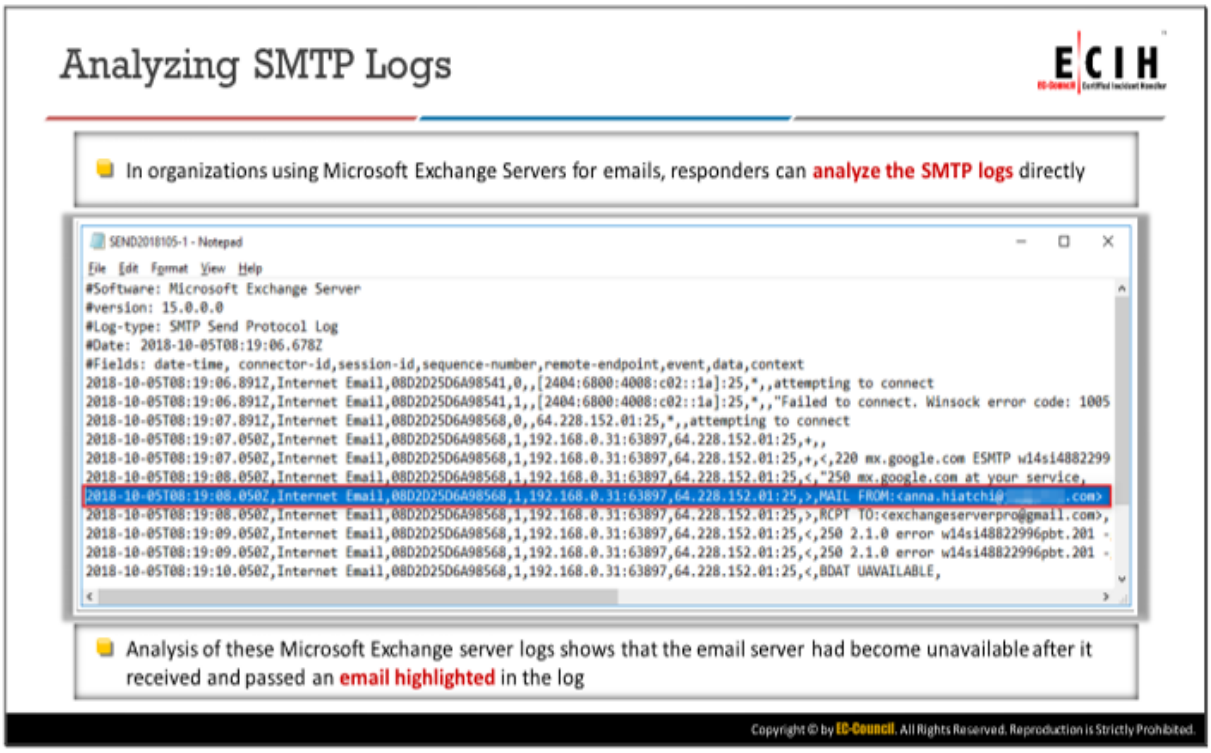
The responders can use tools such as EventLog Analyzer to analyze email logs at the server level and detect the emails that attackers used for phishing or spamming.

- **EventLog Analyzer**

  Source: *https://www.manageengine.com*

  EventLog Analyzer provides log management with agent and agentless methods of log collection, custom log parsing, and complete log analysis with reports and alerts. It allows you to audit all your critical application servers. With predefined reports for the applications listed here, the solution also allows you to monitor custom applications. Its custom log parser enables you to easily parse and validate custom log formats.

  The responders can use this tool to analyze email logs at server level and detect the emails that attackers used for phishing or spamming.



Analyzing SMTP Logs

SMTP is a TCP/IP mail delivery protocol. It transfers email across the internet and across the local network. It runs on the connection-oriented service provided by Transmission Control Protocol (TCP), and it uses the well-known port number 25.

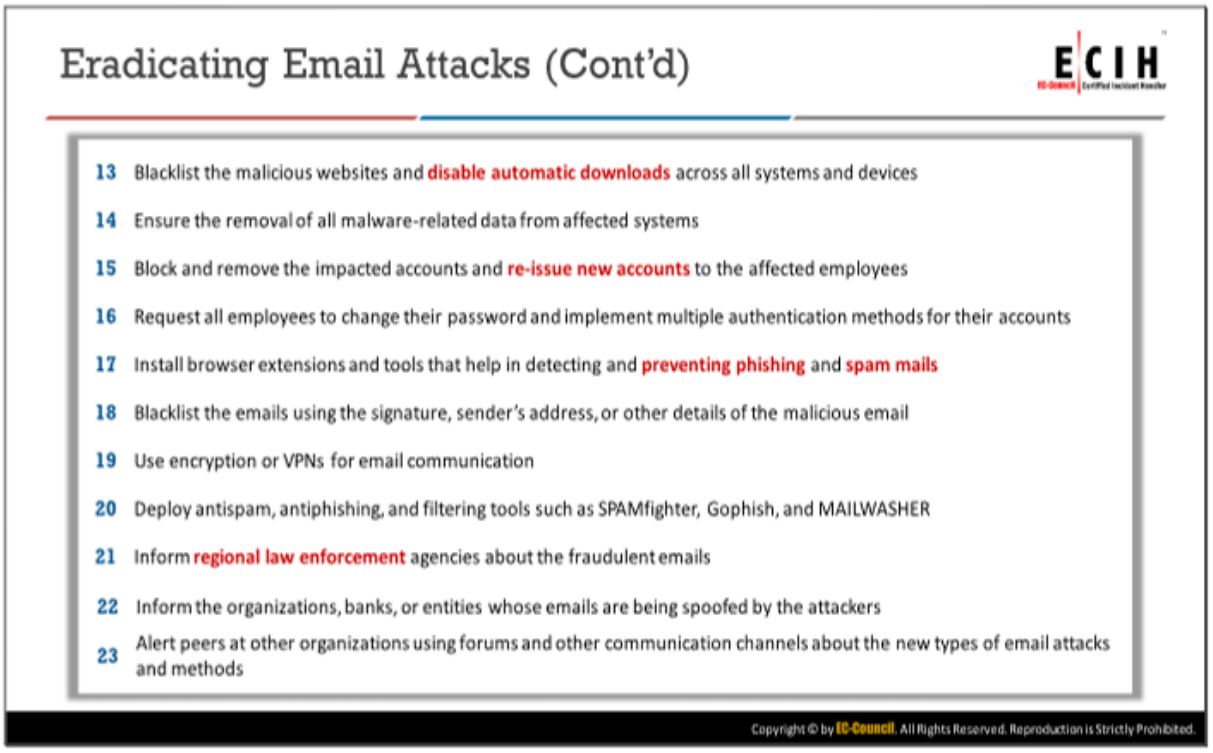
In organizations using Microsoft Exchange Servers for emails, responders can analyze the SMTP logs directly. Analysis of the Microsoft exchange server logs shows that the email server had gone unavailable after it received and passed an email highlighted in the log.

The screenshot shown on the above slide represents logs of Microsoft Exchange Server. In this, the responder has found a message from a non-existent website named abc.com.

Eradication of Email Security Incidents

After detecting, containing, and analyzing the email incident, the incident responder is responsible for eradicating the incident. The responder must take appropriate measures in eradicating the incident and not repeating it in the future.

This section discusses the steps and guidelines that are to be followed by the IH&R personnel in eradicating the email security incident.



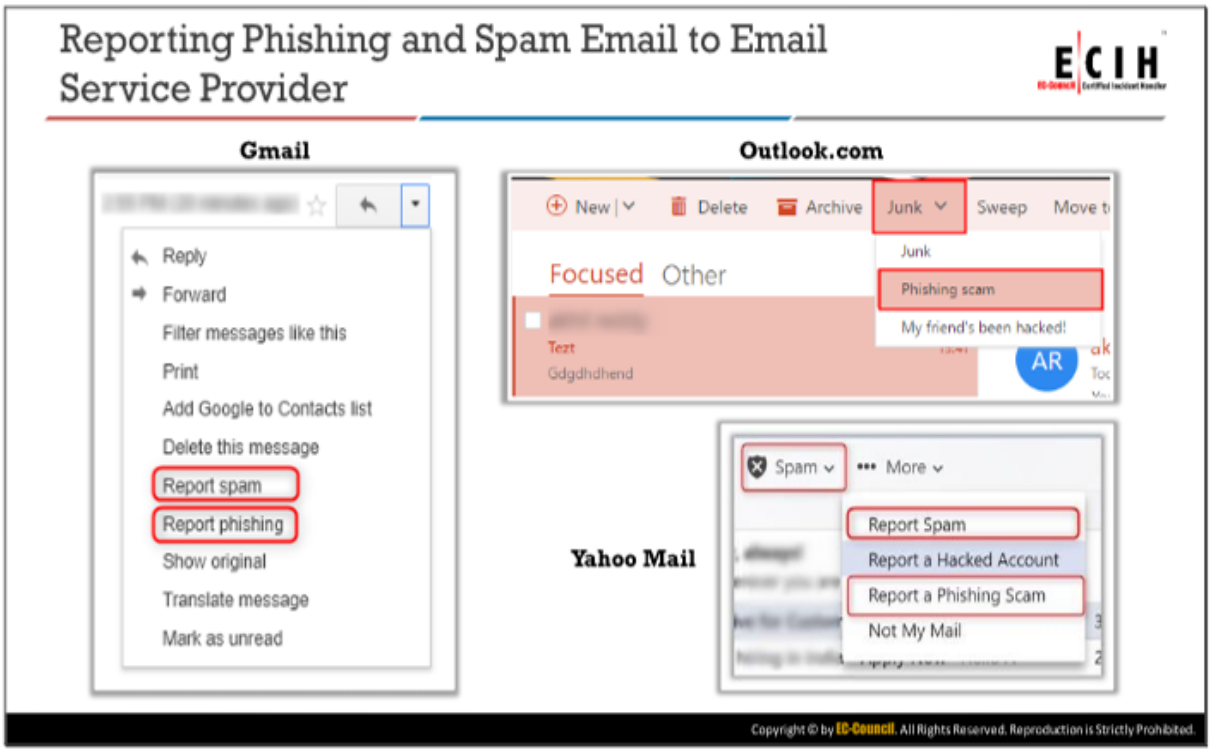
Eradicating Email Attacks

Eradication of email incidents involves removing malware, isolating the critical systems infected with malware, blocking the compromised email accounts, and performing other email security strengthening measures. During this, the responders must check whether the email server is experiencing any vulnerabilities that the attackers can use to exploit and resolve those as soon as possible.

Incident responders must perform the following to eradicate email incidents:

- Collect details of an email security incident, such as URL, hostname, subject link, sender, and IP address, from email header analysis and block them across servers, security tools, and network devices.
- Immediately alert employees about the incident and train them to diagnose them.
- Update antiphishing and antispam tools with the newly found signatures and details of the attackers to prevent similar attacks in future.
- Find common patterns and signatures from the emails to block them on the SMTP server.
- Check the SMTP logs to determine if the attackers have sent the same or similar emails to other employees and remove them from the inboxes.
- Check the impact of the attacks on other users and perform incident handling processes on their systems as well.
- Use DNS Black holing to block IP addresses used to send the malicious emails.
- Seek help from government agencies and antiphishing organization such as APWG.
- Harden the security of email servers and clients.
- Share the email incident reports with peers through forums and submit them to online databases and authorities.
- Train employees to check email headers for those emails asking for immediate actions such as financial transactions.
- Implement a multiple verification policy for financial transactions.
- Blacklist the malicious websites and disable automatic downloads across all the systems and devices.
- Ensure removal of all malware-related data from affected systems.
- Block and remove the impacted accounts and re-issue new accounts to the employees.
- Request all the employees to change their passwords and implement multiple authentication for their accounts.
- Install browser extensions and tools that help in detecting and preventing phishing and spam email.
- Blacklist the email using signatures, sender's addresses, or other details of any malicious email.
- Use encryption or VPNs to communicate using emails.
- Deploy antispam, antiphishing, and filtering tools such as, SPAMfighter, Gophish, and MAILWASHER.
- Inform regional law enforcement agencies about the fraudulent mails.

- Inform the organizations, banks, or entities whose emails have been spoofed by attackers.
- Alert peers at other organizations using forums and other communication channels about the new types of email attacks and methods.
- Patch the vulnerabilities exploited by the malware to corrupt the systems and other devices.



Reporting Phishing and Spam Email to Email Service Provider

The attackers create phishing or spamming emails to lure viewers and obtain sensitive information from readers. The email inbox become awash with fraudulent email that informs the reader about some actions to obtain money or prizes. The best way to deal with such emails is to stay away from them by ignoring and reporting them to local cybercrime police departments, email service providers, and internet service providers, and by sharing these details with peers.

Users or incident responders can report these malicious emails directly to the service providers through the following steps:

- **Gmail**

  1. Open the suspicious mail, click the "**More**" button (three vertical dots) at top-right corner of the email.

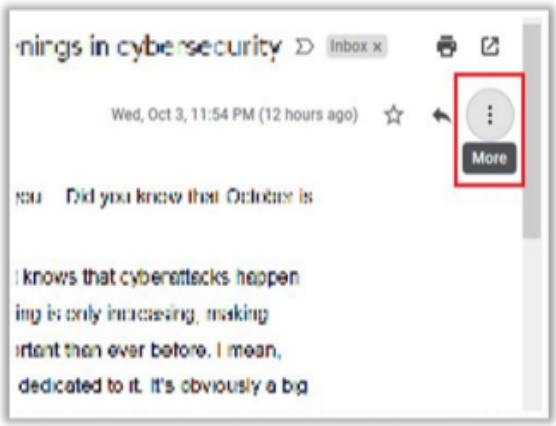


Figure 5.6: More option in Gmail

2. Select the options **Report spam** or **Report phishing** based on the type of email incident you want to report.

- **Hotmail**

1. Open the suspicious email, and click down-arrow beside the **Reply** button from the top-right corner to see the drop-down list or select the **Junk** option from the email tool bar.

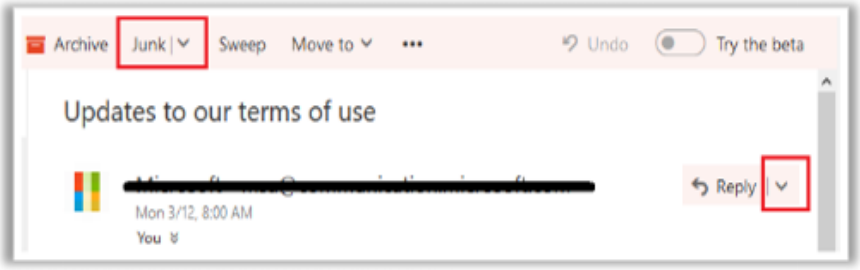


Figure 5.7: Junk option in Hotmail

2. Select the **Mark as junk** or **Phishing scam** options to send the report to the Microsoft security center.

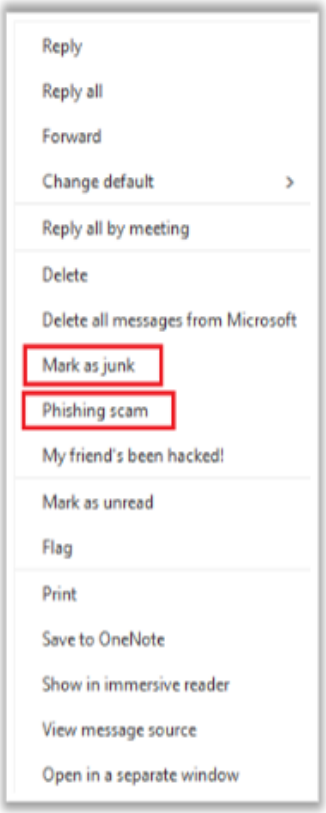
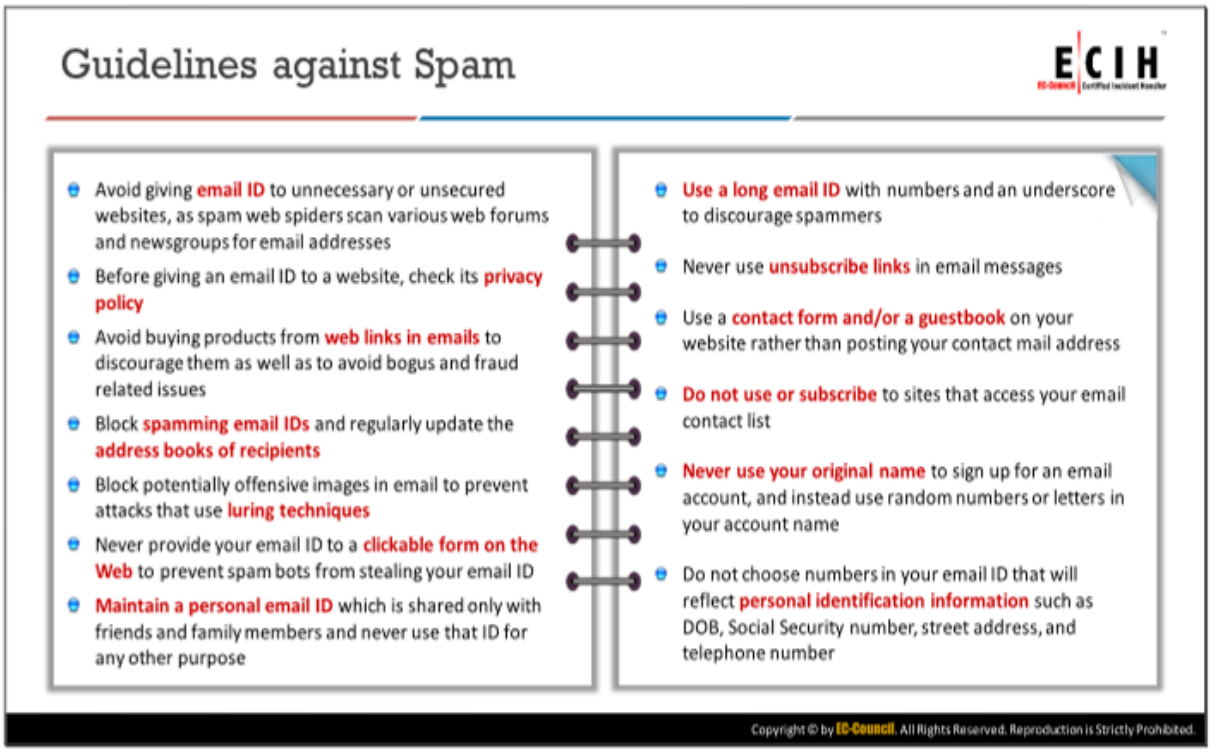


Figure 5.8: Mark as junk and Phishing scam options

- **Yahoo Mail**

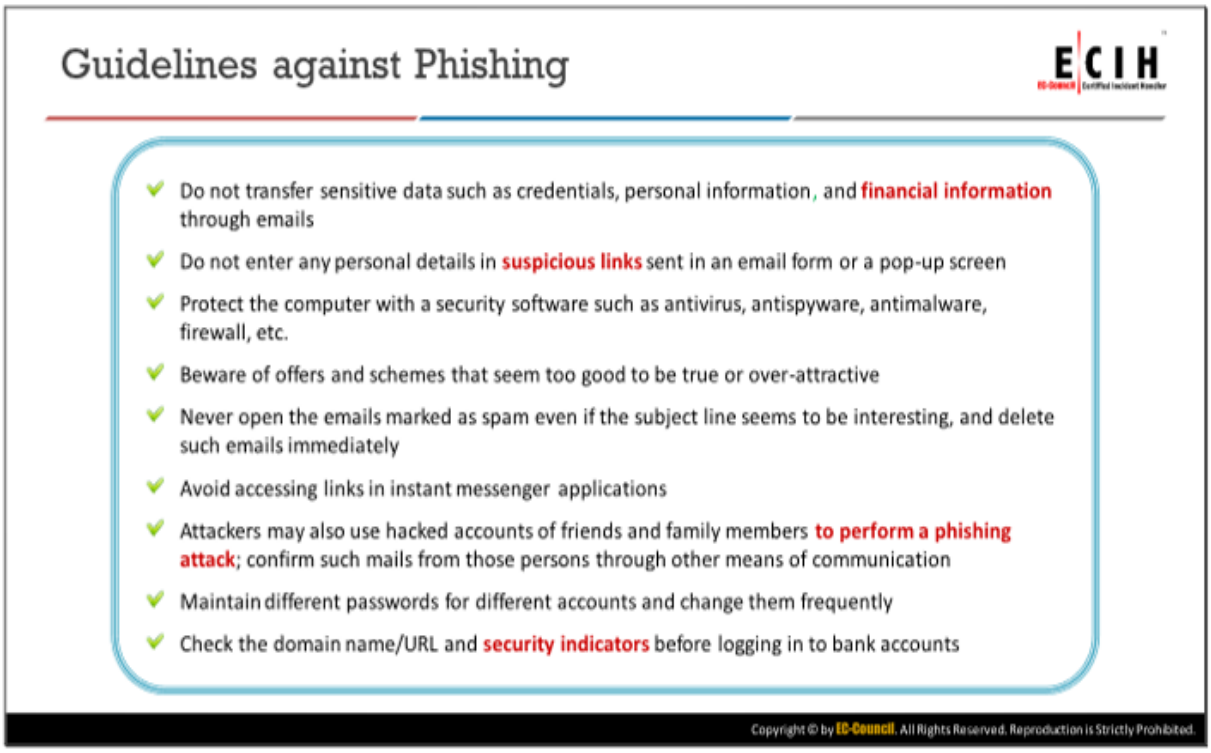
1. Open the suspicious email and then click on **Spam** at the top of the mail.
2. Select the **Report Spam** or **Report a Phishing Scam** option from the menu list.



Guidelines against Spam

The following are some of the guidelines to overcome spam email:

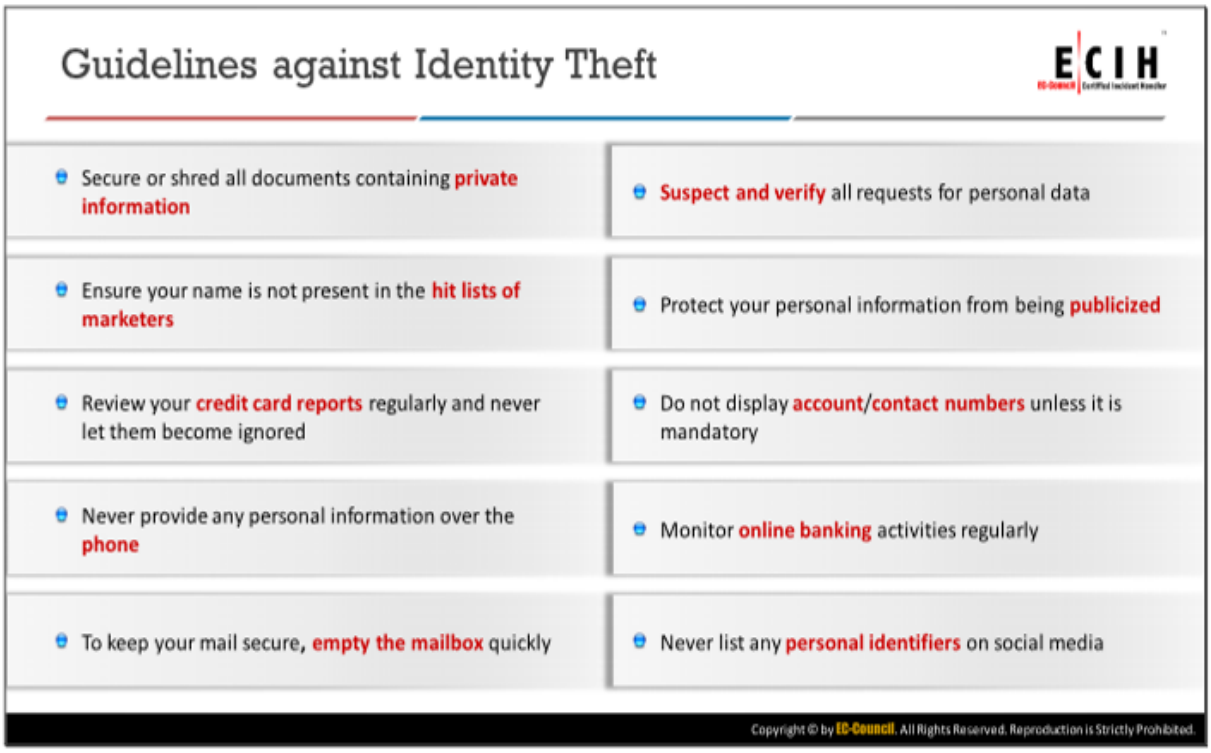
- Avoid giving email ID to unnecessary or unsecured websites, as spam web spiders scan various web forums and newsgroups for email addresses.
- Check a website's privacy policy before giving an email ID to a website.
- Avoid buying products from web links in emails to discourage them as well as to avoid bogus and fraudulent issues.
- Block spamming email IDs and regularly update recipient's address book.
- Block potentially offensive images in email to prevent attacks using luring techniques.
- 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 different from professional email ID, and share it only with friends and family members, and never use that ID for other purposes.
- Use long email IDs with numbers and underscore to prevent spammers.
- Never use unsubscribe links in email messages.
- Use a contact form and/or a guestbook on your website rather than posting your contact mail address.
- Do not use or subscribe to sites that access email contact list.
- Never use your original name to sign up for an email account; use instead random numbers or letters in it.
- Do not choose numbers that reflect personal identification information such as DOB, Social Security number, street address, and telephone number.



Guidelines against Phishing

The following are some of the guidelines to overcome phishing emails:

- Do not transfer sensitive data such as credentials or personal and financial information through emails.
- Do not enter any personal details in suspicious links sent in an email form or a pop-up screen.
- Protect the computer with a security software such as antivirus, antispyware, antimalware, and firewall.
- Beware of the too good to be true or overly attractive schemes and offers.
- Never open emails marked as spam, even if the subject line seems to be interesting, and delete such emails immediately.
- Avoid accessing the links from instant messengers.
- Attackers may also use hacked accounts of friends and family members to perform a phishing attack; confirm such mails are from the correct people through other means of communication.
- Maintain different passwords for different accounts and change them frequently.
- Check the domain name/URL and security indicators before logging in to bank accounts.



Guidelines against Identity Theft

Identity theft occurs when someone uses your personal information (e.g., name, Social Security number, date of birth, mother's maiden name, address) in a malicious way for credit card or loan services, or even for rentals and mortgages, without your knowledge or permission.

The following are some of the guidelines to avoid identity theft:

- Secure or shred all documents containing private information
- Ensure your name is not present in the marketers' hit lists
- Review your credit card reports regularly and never let it go out of sight
- Never give any personal information on the phone
- To keep your mail secure, empty the mailbox quickly
- Suspect and verify all the requests for personal data
- Protect your personal information from being publicized
- Do not display account/contact numbers unless mandatory
- Monitor online banking activities regularly
- Never list any personal identifiers on social media websites such as father's name, pet's name, address, and city of birth

Some additional countermeasures against identity theft are as follow:

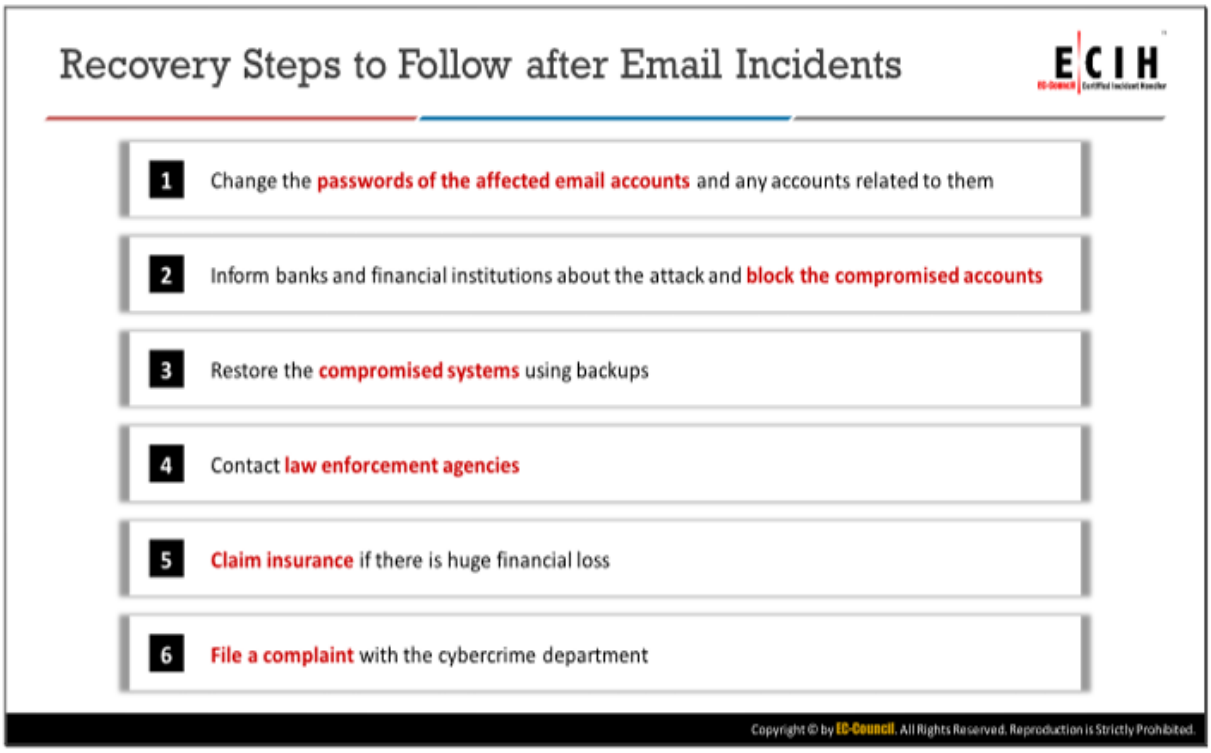
- To keep your mail secure, empty your mailbox quickly, and do not reply to unsolicited email requests asking for personal information.

- Shred credit card offers and "convenience checks" that are not useful.
- Do not store any financial information on the system and use strong passwords for all financial accounts.
- Check telephone and cell phone bills for calls you did not make.
- Keep your Social Security card, passport, license, and other valuable personal information hidden and locked.
- Read website privacy policies.
- Be cautious before clicking on the link provided in an email or instant message box.

Recovery after Email Security Incidents

After containment and eradication of the incident, the incident responder must recover the organization's systems, network, and other resources from the incident impact.

This section discusses various steps that the IH&R person or team needs to follow in recovering from email security incident to maintain business continuity. This module also discusses the recovery of deleted emails along with email recovery, antiphishing, and antispamming tools.



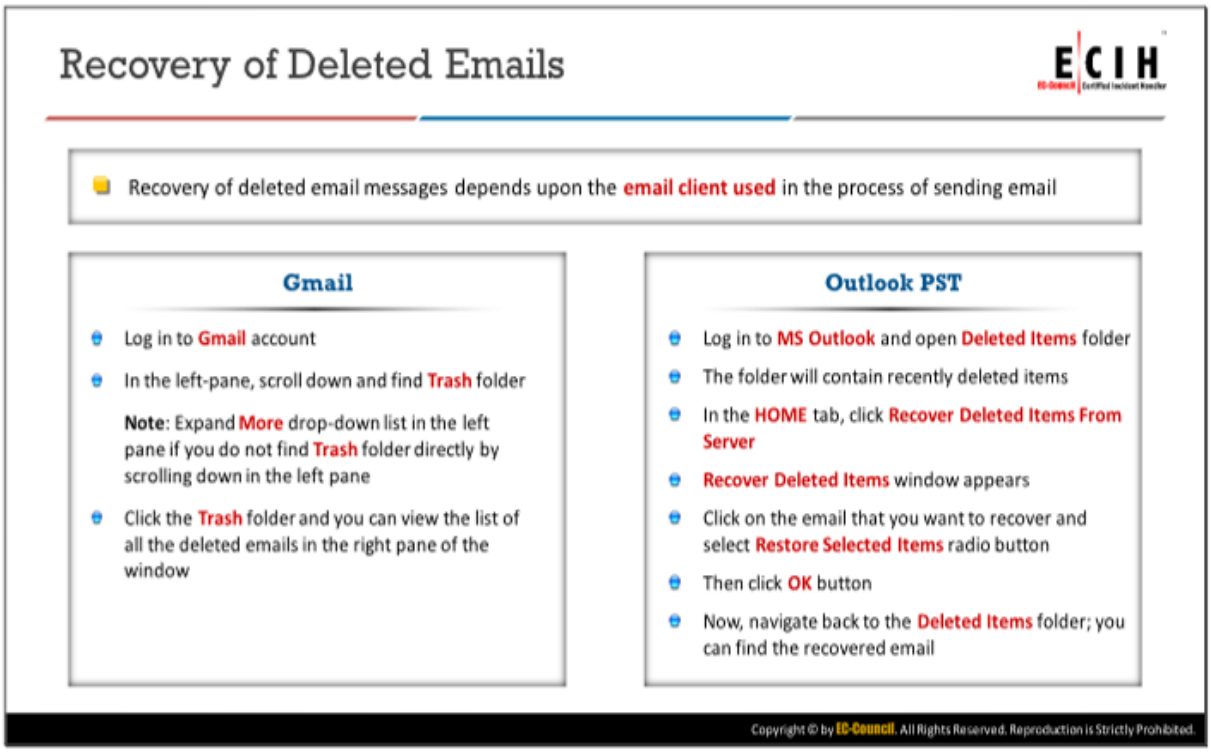
Recovery Steps to Follow after Email Incidents

Following are the some of the crucial tasks that help in recovering from an email security incident:

- **Change passwords of the emails account and accounts related to it**. Change credentials of the compromised accounts. The organization can also permanently delete the compromised accounts and issue new account to the users if possible.
- **Inform banks and financial institutions about the attack and block the compromised accounts**. Provide all proofs of the email attack and request banks to block the compromised accounts.
- **Restore the compromised systems using backups**. Thoroughly scan, update, and patch all compromised systems and perform a backup from reliable backup storage.
- **Contact law enforcement**. Contact law enforcement and brief them about the incident and provide these details:
  - Attacker email address
  - Recipient email address
  - Organization name
  - Organization location
  - Organization bank name
  - Organization bank account number
  - Recipient name

- Recipient bank name
- Recipient bank account number
- Recipient bank location (if available)
- Intermediary bank name (if available)
- SWIFT number
- Date and time of incident
- Amount of transaction
- Additional information (if available)—card numbers, in favor of details, and so on

- **Claim insurance.** If there is a huge financial loss, the organization can claim their insurance.
- **Enquire with the bank if it is possible to revert the transaction.** In case of a CEO scam, inform the bank authorities and cybersecurity team of that bank about the incident and details of the wire transfer so that they can stop the money transfer. Check if the bank has policies of blocking the transferred amount until further clarification or reverse a transaction that happened due to a proven attack.
- **File a complaint at cybercrime department.** File a complaint at the nearest or concerned cybercrime department regarding the data and amount lost and time of the incident. Provide the following details of incident for investigation purposes:
  - Date and time of incident
  - The total amount lost
  - IP/email address of the fraudulent mail
  - History of all the phishing activity
  - Fraudulent phone calls details



Recovery of Deleted Emails

An employee may delete emails accidentally or intentionally. The process of their recovery depends on the email client that the employee is using.

Gmail

After a user deletes mails in the Gmail, it does not remove them completely, but tags them for deletion and moves them to trash folder in the mailbox. These messages reside in the trash folder, until the user or the service provider clears the trash folder.

Recovering deleted emails in Gmail:

- Log in to **Gmail** account.
- In the left pane, scroll down and find **Trash** folder.

  Note: Expand the **More** drop-down list in the left pane if you do not find the **Trash** folder directly by scrolling down in the left pane.
- Click the **Trash** folder, and you can view the list of all the deleted emails in the right pane of the window.

Outlook PST

Outlook stores emails, contacts, calendar entries, and so on in the form of Personal Storage Table (PST). In MS Outlook, data deletion occurs in two categories:

- **Soft deletion**. When a user deletes mails from folders such as Inbox, Drafts, Sent Items, and Contacts, Outlook moves them into **Deleted Items** folder.
- **Hard deletion**. When a user deletes emails using **Shift+Delete**, Outlook deletes those permanently from the mailbox.

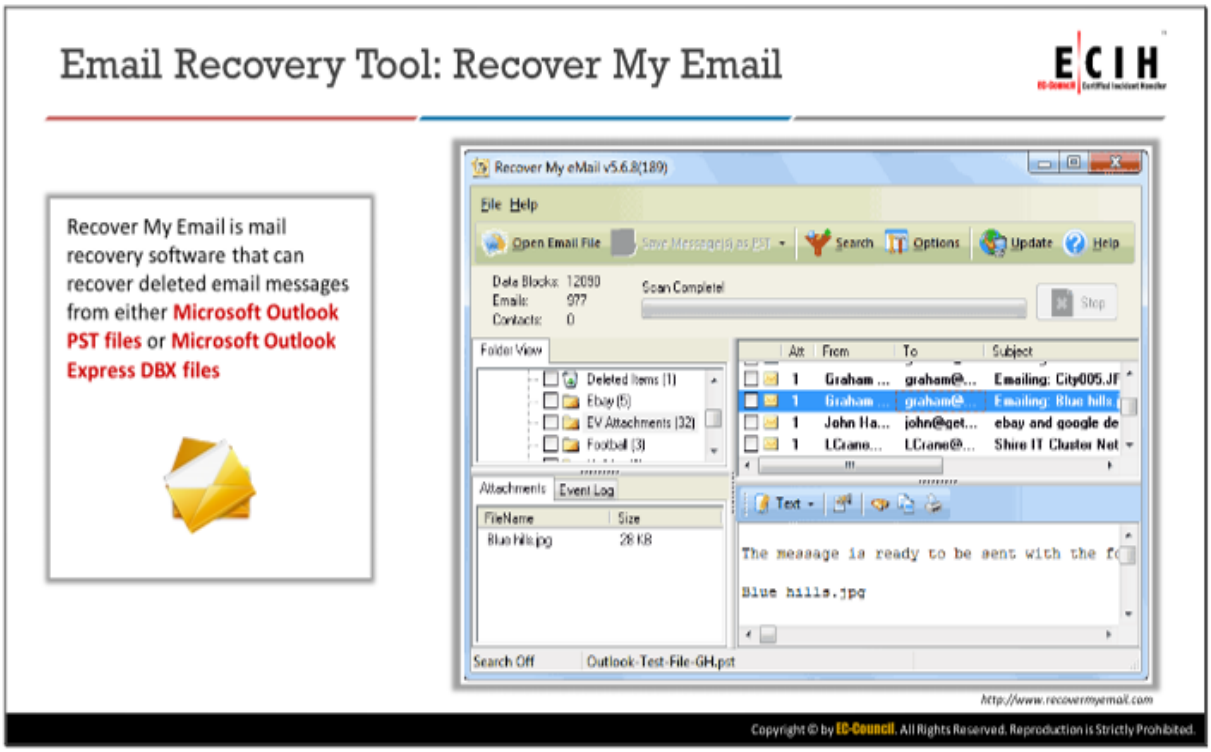
Recovering deleted emails in Outlook:

An incident responder may recover such deleted emails as follows:

- Log in to **MS Outlook** and open **Deleted Items** folder.

  Note: If you do not find Deleted Items folder, then your account does not support the recovery function.

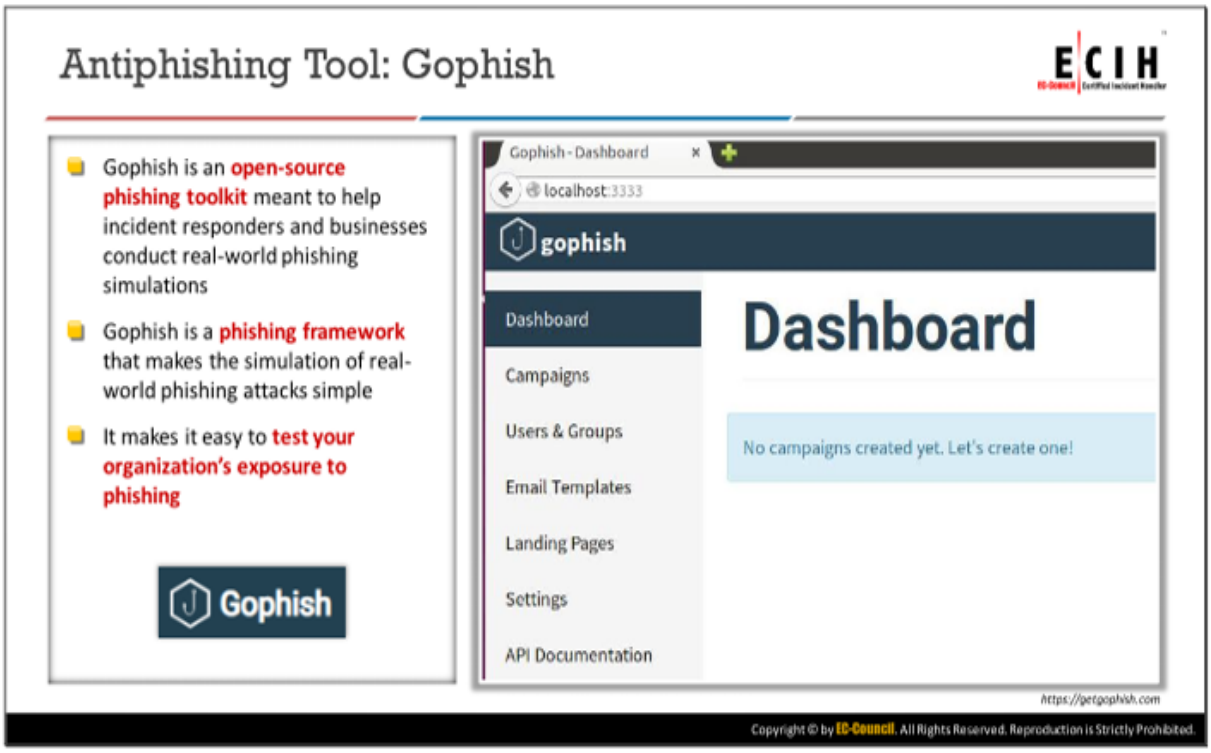
- The folder will contain recently deleted items.
- Then, in the **HOME** tab, click **Recover Deleted Items From Server**.
- **Recover Deleted Items** window appears.
- Click the email that you want to recover and select **Restore Selected Items** radio button.
- Then click **OK** button.
- Now, navigate back to the **Deleted Items** folder; you can find the recovered email.



Email Recovery Tool: Recover My Email

Source: *http://www.recovermyemail.com*

Recover My Email is mail recovery software that can recover deleted email messages from either Microsoft Outlook PST files or Microsoft Outlook Express DBX files.



Antiphishing Tool: Gophish

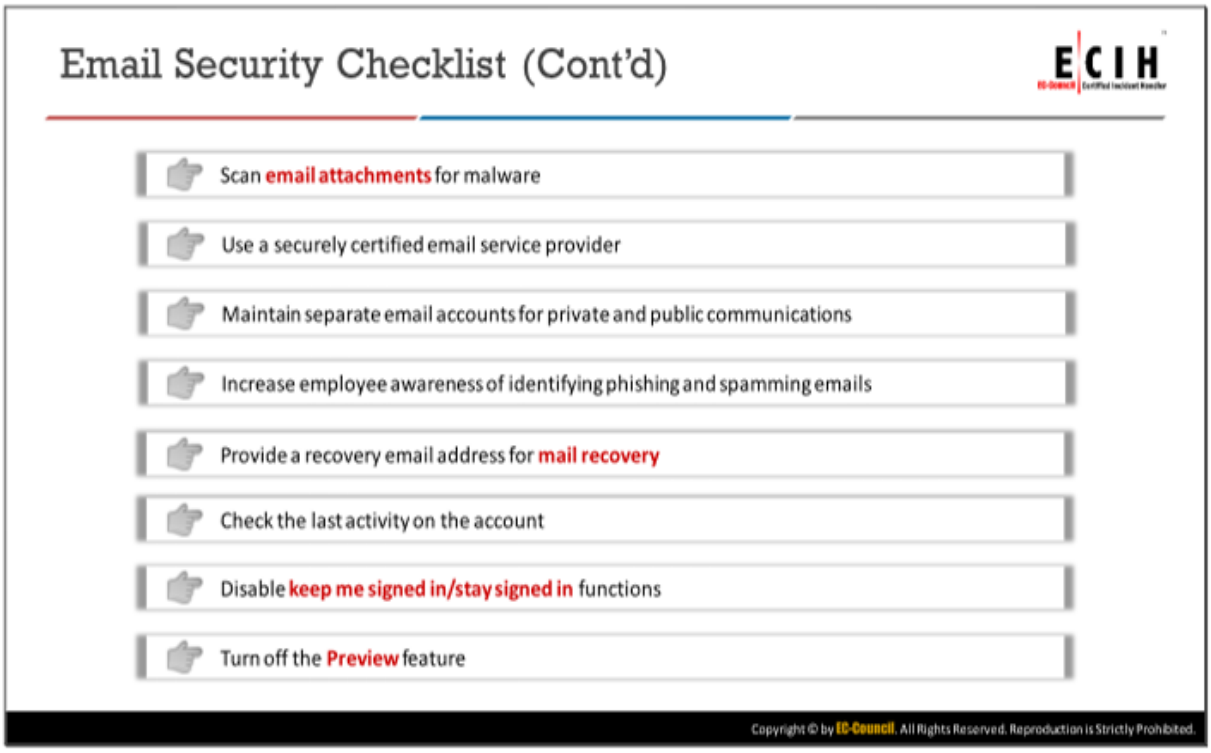
Source: *https://getgophish.com*

Gophish is an open-source phishing toolkit meant to help incident responders and businesses conduct real-world phishing simulations. Gophish is a phishing framework that makes the simulation of real-world phishing attacks simple. It makes it easy to test your organization's exposure to phishing.

Antispamming Tool: SPAMfighter

Source: *https://www.spamfighter.com*

SPAMfighter is a spam filter that works instantly by automatically removing the spam and phishing emails from your inbox.

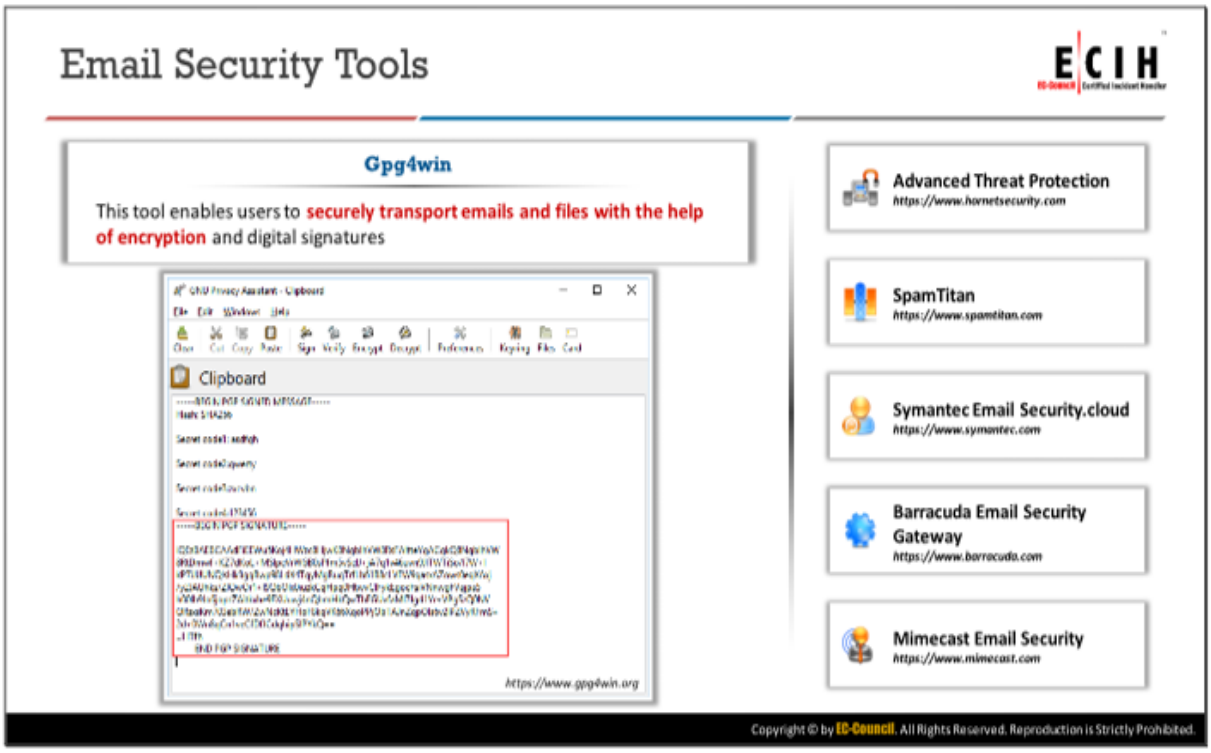


Email Security Checklist

Following are some of the elements of the email security checklist suggested by incident response teams for secure email communications:

- Enable HTTPS for secure communications/transactions.
- Be diligent while opening email attachments.

- Do not click the links provided in email messages.
- Follow email etiquette when forwarding messages.
- Do not forward or reply to spam and suspicious emails; delete them.
- Avoid accessing email via unsecured public wireless connection.
- Avoid accessing the email accounts on shared computers and sending large attachments in emails.
- Use the Bcc: option when sending mail to bulk recipients.
- Never save your password on the web browser.
- Sort messages by priority, subject, date, sender, and other options (helps in searching email).
- Avoid sending confidential, sensitive, personal, and classified information in emails.
- Clean your Inbox regularly.
- Create folders and move emails accordingly (Family, Friends, Work, etc.).
- Digitally sign your outgoing mails.
- Send attachments in PDF format rather than Word or Excel formats.
- Scan email attachments for malware.
- Use securely certified email service provider.
- Maintain separate email for private and public communications.
- Employee awareness of identifying phishing and spamming emails.
- Provide a recovery email address for mail recovery.
- Check the last account activity.
- Disable keep me signed in/stay signed in functions.
- Turn off the **Preview** feature.



Email Security Tools

Incident handlers can use various email security tools to prevent evolving email threats. Discussed below are some of the important email security tools:

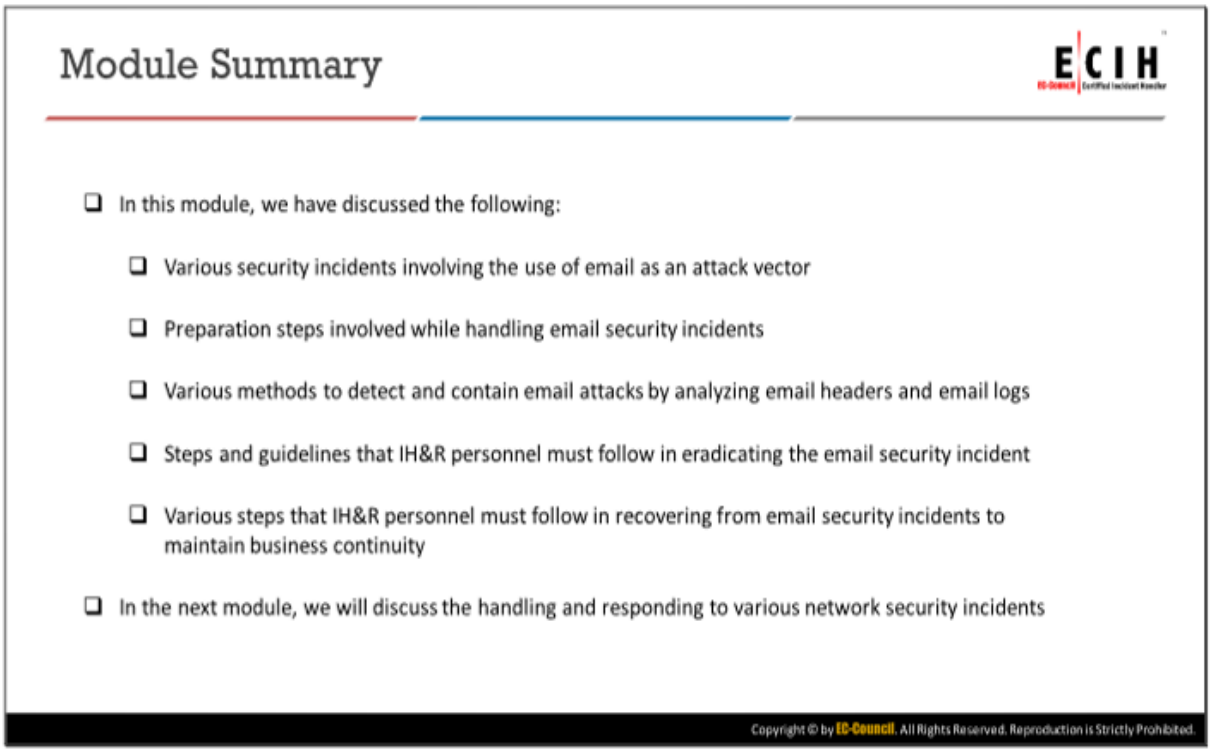
- **Gpg4win**

  Source: *https://www.gpg4win.org*

  Gpg4win enables users to securely transport emails and files with the help of encryption and digital signatures. Encryption protects the contents against an unwanted party reading it. Digital signatures make sure that the mails were not modified and come from a specific sender. Gpg4win supports both relevant cryptography standards, OpenPGP and S/MIME (X.509), and it is the official GnuPG distribution for Windows.

Listed below are some of the additional tools for securing email communication:

- Advanced Threat Protection (*https://www.hornetsecurity.com*)
- SpamTitan (*https://www.spamtitan.com*)
- Symantec Email Security.cloud (*https://www.symantec.com*)
- Barracuda Email Security Gateway (*https://www.barracuda.com*)
- Mimecast Email Security (*https://www.mimecast.com*)
- Comodo Dome Anti-spam (*https://www.comodo.com*)
- Spambrella (*https://www.spambrella.com*)
- The Email Laundry (*https://www.theemaillaundry.com*)
- GFI MailEssentials (*https://www.gfi.com*)
- Cisco Email Security (*https://www.cisco.com*)



Module Summary

In this module, we have discussed various security incidents involving the use of email as an attack vector. We have discussed the responsibilities of incident handlers and responders during an email incident. We have also discussed the preparation steps involved while handling email security incidents and have discussed various methods to detect and contain the email attacks by analyzing email headers and email logs. We then discussed the steps and guidelines that IH&R personnel have to follow in eradicating the email security incident as well as recovering from such an incident to maintain the business continuity.

In the next module, we will discuss in detail handling and responding to various network security incidents.