|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA CÔNG NGHỆ THÔNG TIN**  Logo HvKTMM  BÁO CÁO BÀI TẬP LỚN  **ĐIỀU TRA SỐ**  **Đề tài:**  **TÌM HIỂU VỀ ĐIỀU TRA TỘI PHẠM EMAIL**  Sinh viên thực hiện: VŨ HỒNG PHÚC AT160245  NGUYỄN VĂN A AT16  TRẦN THỊ B AT16  Nhóm 05    Hà Nội, 5-2023 |

**LỜI NÓI ĐẦU**

Email đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày của chúng ta, cả về mặt cá nhân và nghề nghiệp. Nó đã cách mạng hóa cách chúng ta giao tiếp và tiến hành kinh doanh, giúp kết nối với mọi người trên khắp thế giới nhanh hơn và dễ dàng hơn. Tuy nhiên, cùng với sự tiện lợi này là nguy cơ tội phạm Email, có thể gây hậu quả nghiêm trọng cho các cá nhân cũng như tổ chức.

Tội phạm Email có thể có nhiều hình thức, từ spam và lừa đảo trực tuyến đến các tội nghiêm trọng hơn như hack và đánh cắp danh tính. Những tội ác này có thể dẫn đến tổn thất tài chính, thiệt hại về uy tín và thậm chí là hậu quả pháp lý. Đó là lý do tại sao điều quan trọng là phải điều tra tội phạm Email kỹ lưỡng và đưa thủ phạm ra trước công lý.

Điều tra tội phạm Email đòi hỏi kiến thức chuyên môn và chuyên môn, bao gồm sự hiểu biết về các giao thức Email và kỹ thuật pháp y. Nó cũng liên quan đến việc hợp tác chặt chẽ với các cơ quan thực thi pháp luật, chuyên gia công nghệ và chuyên gia pháp lý để thu thập bằng chứng và xây dựng vụ việc.

Nội dung chi tiết của bài báo cáo sẽ được chia làm 3 chương:

**Chương 1: Tìm hiểu về Email**

**Chương 2: Điều tra tội phạm Email và các bước điều tra**

**Chương 3: Một số điều luật chống tội phạm Email của Việt Nam**

# TÌM HIỂU VỀ EMAIL

## Hệ thống Email

Email là từ viết tắt của “thư điện tử” được sử dụng để gửi, nhận và lưu thư trên các hệ thống liên lạc điện tử. Với sự phụ thuộc ngày càng tăng vào công nghệ, Email đã trở thành một trong những phương thức liên lạc phổ biến nhất.

Một hệ thống thư điện tử hoạt động trên kiến trúc client-server cơ bản. Nó cho phép khách hàng gửi/nhận thư thông qua các máy chủ Email giao tiếp với nhau. Hầu hết các hệ thống Email đều có trình soạn thảo văn bản với các tùy chọn định dạng cơ bản cho phép khách hàng soạn tin nhắn văn bản và gửi chúng đến một hoặc nhiều người nhận. Khi tin nhắn đã được gửi đi, nó sẽ đi qua một số máy chủ và được lưu trữ trong hộp thư của người nhận cho đến khi người đó lấy lại.

## Cách Email hoạt động

Cũng giống như các công nghệ điều tra kỹ thuật số khác, không dễ để tiến hành điều tra mà không hiểu cơ sở của các công nghệ cơ bản.

Email có thể được tạo từ nhiều phương tiện và cách tiếp cận khác nhau và do đó có nhiều công nghệ khác nhau được áp dụng.

Nói một cách thông thường, một người viết Email trên thiết bị kỹ thuật số của mình, có thể là điện thoại hoặc máy tính, rồi gửi đến người anh ta muốn. Mặc dù có vẻ như đã hoàn thành công việc của mình, nhưng công việc xử lý Email sau đó chỉ mới bắt đầu để gửi thành công và chính xác đến người nhận.

Khi một Email được gửi đi, vô số máy chủ thực sự đảm nhận toàn bộ thông tin của Email trước khi nó thực sự đến hộp thư đến của người nhận, điều này có nghĩa là chúng ta phải hiểu những gì đang diễn ra sau khi chúng ta nhấp vào nút “Gửi”.

## Các thành phần liên quan đến giao tiếp Email

Có một số thành phần của giao tiếp Email đóng vai trò cụ thể khi một Email được truyền từ người gửi đến người nhận.

### Mail User Agent

Còn được gọi là ứng dụng email (MUA) là một ứng dụng trên máy tính để đọc, gửi và sắp xếp email. Nó cung cấp giao diện để người dùng nhận, soạn hoặc gửi Email từ địa chỉ Email đã định cấu hình của họ.

Người dùng cần thiết lập và định cấu hình địa chỉ Email của họ trước khi sử dụng ứng dụng email. Cấu hình bao gồm cấp ID email, mật khẩu, Post Office Protocol 3 (POP3)/Internet Message Access Protocol (IMAP) và địa chỉ Simple Mail Transfer Protocol (SMTP), số cổng và các tùy chọn liên quan khác. Có nhiều ứng dụng Email độc lập và dựa trên web như Claws Mail, Thunderbird, Mailbird, Zimbra Desktop, Gmail và Outlook.com. Ứng dụng Email chỉ hoạt động khi người dùng chạy nó.

### Mail Transport Agent

Tác nhân chuyển thư (MTA) là một thành phần quan trọng của quá trình truyền tải thư điện tử. Nó chủ yếu là một loại máy chủ thư nhận thư Email từ tác nhân gửi thư và giải mã thông tin tiêu đề để xem thư sẽ đi đâu. Sau khi được xác định, nó sẽ chuyển thông báo đến máy chủ MTA tiếp theo.

Tất cả các máy chủ MTA giao tiếp với nhau thông qua giao thức SMTP. Một số ví dụ về MTA bao gồm Sendmail, Exim và Postfix.

### Mail Delivery Agent

Tác nhân chuyển phát thư (MDA) là máy chủ nhận thông báo Email từ MTA cuối cùng và giữ nó trong hộp thư của người nhận. Dovecot là một ví dụ về MDA.

### SMTP Server

SMTP là một máy chủ thư đi cho phép người dùng gửi Email đến một địa chỉ Email hợp lệ. Người dùng không thể sử dụng máy chủ SMTP để nhận Email; tuy nhiên, cùng với Post Office Protocol (POP) hoặc IMAP, họ có thể sử dụng SMTP để nhận Email với cấu hình phù hợp.

Bất kỳ máy chủ SMTP nào cũng được ứng dụng thư khách của người dùng gán một địa chỉ theo định dạng sau: smtp.serveraddress.com (ví dụ: địa chỉ máy chủ SMTP của Gmail sẽ là smtp.gmail.com).

Khi người dùng gửi Email đến một người nhận cụ thể, trước tiên, nó sẽ đến máy chủ SMTP xử lý thư để xác định địa chỉ của người nhận và sau đó chuyển tiếp nó đến máy chủ cụ thể. Tất cả các máy chủ SMTP thường lắng nghe cổng 25. Tuy nhiên, các máy chủ SMTP gửi đi sử dụng cổng 587 cho các kết nối bảo mật lớp truyền tải và cổng 465 cho các kết nối lớp cổng bảo mật (SSL).

### POP3 Server

POP3 là một giao thức đơn giản để truy xuất Email từ máy chủ Email. Khi máy chủ POP nhận Email, chúng sẽ được lưu trữ trên máy chủ cho đến khi và trừ khi người dùng yêu cầu.

Máy chủ POP3 không chấp nhận khái niệm thư mục; nó coi hộp thư trên máy chủ là nơi lưu trữ duy nhất của nó. Sau khi người dùng kết nối với máy chủ thư để khôi phục thư của họ bằng ứng dụng Email khách, thư sẽ tự động được tải xuống từ máy chủ thư vào ổ cứng của người dùng và không còn được lưu trữ trên máy chủ trừ khi người dùng chỉ định giữ một bản sao của nó.

Máy chủ POP3 có thể hiểu các lệnh đơn giản như sau:

* USER-nhập ID người dùng của bạn
* PASS - nhập mật khẩu của bạn
* QUIT - thoát khỏi máy chủ POP3
* LIST - liệt kê các tin nhắn và kích thước của chúng
* RETR - truy xuất tin nhắn, theo số tin nhắn
* DELETE - xóa tin nhắn, theo số tin nhắn

Kể từ khi POP3 triển khai các ứng dụng Email gửi thư xuống hệ thống, người dùng có thể đọc thư ngay cả khi không có kết nối Internet. Tuy nhiên, do thư được lưu trữ trên ổ cứng nên người dùng không thể truy cập chúng từ các máy từ xa.

### Máy chủ IMAP

Máy chủ IMAP tương tự như máy chủ POP3. Giống như POP3, IMAP xử lý thư đến. Theo mặc định, máy chủ IMAP lắng nghe cổng 143 và IMAPS (IMAP qua SSL) lắng nghe trên cổng 993.

IMAP lưu trữ Email trên máy chủ thư và cho phép người dùng xem và làm việc trên Email của họ, như thể thư được lưu trữ trong hệ thống cục bộ của họ. Điều này cho phép người dùng tổ chức tất cả các thư tùy thuộc vào yêu cầu của họ. Ngược lại với POP3, IMAP không di chuyển máy chủ thư đến hộp thư của người dùng.

Nó hoạt động như một máy chủ từ xa lưu trữ tất cả thư của người dùng trong máy chủ thư. IMAP cho phép ứng dụng Email truy xuất các phần mở rộng thư Internet đa mục đích (MIME) ở dạng toàn bộ thư hoặc ở dạng nhiều bit, cho phép ứng dụng khách chỉ truy xuất phần văn bản của thư mà không cần tải xuống tệp đính kèm. Giao thức này lưu trữ một bản sao của tất cả các Email trên máy chủ ngay cả khi người dùng tải chúng xuống hệ thống của họ. Do đó, người dùng có thể truy cập chúng từ bất kỳ hệ thống máy tính hoặc thiết bị nào.

## Cách thức hoạt động của giao tiếp qua Email

Khi người dùng gửi một Email đến bất kỳ người nhận nào, nó sẽ trải qua một số giai đoạn trước khi đến đích. Kịch bản dưới đây sẽ giải thích về các giai đoạn này:

* Giả sử rằng một người dùng Email tên Bob muốn gửi một Email đến một người dùng Email khác tên Alice. Anh ấy soạn thư bằng ứng dụng Email của mình (MUA) hoặc Email dựa trên web như Yahoo!, chỉ định địa chỉ Email của Alice và nhấn nút gửi.
* Thông báo Email được nhận bởi một máy chủ MTA thông qua SMTP để giải mã thông tin tiêu đề và tìm kiếm tên miền trong địa chỉ Email của Alice. Phương pháp này cho phép máy chủ MTA xác định máy chủ thư đích và chuyển thư đến MTA tương ứng.
* Mỗi khi máy chủ MTA nhận được một tin nhắn trong quá trình gửi thư, nó sẽ sửa đổi thông tin tiêu đề của nó. Khi đến MTA cuối cùng, nó sẽ được chuyển đến MDA, nơi giữ tin nhắn trong hộp thư của Alice.
* Ứng dụng Email (MUA) của Alice sau đó truy xuất tin nhắn bằng cách sử dụng POP3 hoặc IMAP và Alice cuối cùng có thể đọc tin nhắn.

## Các thành phần của một tin nhắn Email

Thông điệp email là một văn bản ngắn gọn và thân mật được gửi hoặc nhận qua mạng. Tin nhắn email là tin nhắn văn bản đơn giản cũng có thể bao gồm các tệp đính kèm như tệp hình ảnh và bảng tính. Nhiều công thức có thể nhận email cùng một lúc.

Hiện tại, RFC 5322 xác định định dạng thư điện tử trên Internet và RFC 2045 đến RFC 2049 xác định các tệp đính kèm nội dung đa phương tiện - chúng được gọi là phần mở rộng thư Internet đa mục đích (MIME).

Thông điệp email bao gồm ba phần chính:

* Tiêu đề thư

Tiêu đề thư bao gồm các trường sau:

* **To** chỉ định người gửi tin nhắn. Lưu ý rằng tiêu đề "To" không phải lúc nào cũng chứa địa chỉ của người nhận.
* **Cc** là viết tắt của "bản sao carbon." Tiêu đề này chỉ định những người nhận bổ sung ngoài những người được liệt kê trong tiêu đề "To". Sự khác biệt giữa "To" và "Cc" về cơ bản là có ý nghĩa; một số người gửi thư cũng xử lý chúng theo cách khác trong việc tạo thư trả lời.
* **Bcc** là viết tắt của "blind carbon copy." Tiêu đề này gửi các bản sao của email tới những người có thể không muốn nhận thư trả lời hoặc không muốn xuất hiện trong tiêu đề. Những bản sao mù phổ biến với những kẻ gửi thư rác vì chúng gây nhầm lẫn cho nhiều người dùng thiếu kinh nghiệm khi nhận được email không có địa chỉ của họ hoặc có vẻ như không dành cho họ.
* **From** chỉ định người gửi tin nhắn
* **Reply-To** chỉ định một địa chỉ để gửi trả lời. Mặc dù tiêu đề này có nhiều cách sử dụng hợp pháp nhưng nó cũng được những kẻ gửi thư rác sử dụng rộng rãi để làm chệch hướng những lời chỉ trích. Đôi khi, một người gửi thư rác gốc sẽ thu hút phản hồi qua email và sử dụng tiêu đề "Reply-To" để thu thập chúng, nhưng thường thì địa chỉ được chỉ định trong email rác không hợp lệ hoặc là địa chỉ của một nạn nhân vô tội.
* **Sender** không bình thường trong email ("X-Sender" thường được sử dụng thay thế) nhưng thỉnh thoảng xuất hiện, đặc biệt là trong các bản sao của bài đăng Usenet. Nó sẽ xác định người gửi; trong trường hợp các bài đăng trên Usenet, nó là một số nhận dạng đáng tin cậy hơn dòng "From".
* **Subject** là một trường có dạng hoàn toàn tự do do người gửi chỉ định để mô tả chủ đề của thư
* **Date** chỉ định ngày tạo và gửi email. Nếu máy tính của người gửi bỏ qua tiêu đề này, máy chủ thư hoặc một số máy khác có thể thêm nó, thậm chí dọc theo tuyến đường.
* **MIME-Version** là một tiêu đề MIME khác phản ánh phiên bản của giao thức MIME
* **Priority** về cơ bản là một tiêu đề dạng tự do chỉ định mức độ ưu tiên cho thư. Hầu hết các phần mềm bỏ qua nó. Những kẻ gửi thư rác thường sử dụng nó để cố gắng đọc tin nhắn của họ.
* Nội dung thư
* Phần thân của email truyền tải thông điệp và đôi khi bao gồm một khối chữ ký ở cuối. Một dòng trống ngăn cách phần đầu và phần thân. Trong một email, nội dung hoặc văn bản luôn xuất hiện sau các dòng tiêu đề.
* Nội dung email là thông điệp chính của email chứa văn bản, hình ảnh, siêu liên kết và dữ liệu khác (như tệp đính kèm). Nội dung email hiển thị các tệp đính kèm riêng biệt xuất hiện cùng dòng với văn bản. Tiêu chuẩn email trên Internet không đặt ra bất kỳ giới hạn nào về kích thước nội dung của email. Tuy nhiên, các máy chủ thư cá nhân có giới hạn kích thước thư.
* Chữ ký
* Chữ ký email là một lượng nhỏ thông tin bổ sung được đính kèm ở cuối thông báo email bao gồm tên và chi tiết liên hệ của người gửi email. Nó có thể chứa văn bản rõ hoặc hình ảnh.

# TÌM HIỂU VỀ ĐIỀU TRA TỘI PHẠM EMAIL VÀ CÁC BƯỚC

## Giới thiệu về tội phạm email

Điều tra tội phạm email liên quan đến việc trích xuất, thu thập, phân tích và phục hồi các email liên quan đến bất kỳ tội phạm mạng nào. Phân tích chi tiết các email giúp các điều tra viên thu thập bằng chứng hữu ích như ngày và giờ gửi email, địa chỉ IP thực của người gửi và người gửi, cũng như cơ chế giả mạo nào đã được sử dụng. Các điều tra viên cần sử dụng nhiều công cụ pháp y để trích xuất siêu dữ liệu từ các tiêu đề email. Điều này giúp họ xác định vị trí tội phạm đứng sau tội ác và báo cáo những phát hiện để truy tố họ trước tòa án.

Điều tra các hoạt động tội phạm hoặc vi phạm chính sách liên quan đến email cũng tương tự như các loại điều tra tội phạm máy tính khác. Tội phạm email có thể được phân loại theo hai cách: một được thực hiện bằng cách gửi email và cách kia được hỗ trợ bởi email. Khi bọn tội phạm sử dụng thư rác, email giả mạo, đánh bom thư hoặc bão thư để bán ma túy, theo dõi, lừa đảo, bắt cóc trẻ em hoặc thực hiện các hoạt động bất chính khác, có thể nói rằng những email đó đã hỗ trợ tội phạm mạng.

**Tội phạm thực hiện bằng cách gửi email.**

### Gửi thư rác qua email

Thư rác không được yêu cầu bởi email thương mại hoặc thư rác. Thư rác liên quan đến việc gửi cùng một nội dung đến một số lượng lớn địa chỉ cùng một lúc. Thư rác hoặc thư rác lấp đầy hộp thư và ngăn người dùng truy cập email thông thường của họ. Những email thông thường này bắt đầu bị trả lại do máy chủ vượt quá giới hạn dung lượng. Những kẻ gửi thư rác che giấu danh tính của họ bằng cách giả mạo tiêu đề email. Để tránh nhận được phản hồi từ những người nhận khó chịu, những kẻ gửi thư rác cung cấp thông tin sai lệch trong các trường FROM và REPLY-TO và đăng chúng lên danh sách gửi thư hoặc nhóm tin.

### Lừa đảo

Lừa đảo đã nổi lên như một phương pháp hiệu quả để đánh cắp dữ liệu cá nhân và bí mật của người dùng. Đây là một trò lừa đảo trên Internet lừa người dùng tiết lộ thông tin cá nhân và bí mật của họ bằng cách đưa ra những tuyên bố và lời đề nghị hấp dẫn. địa chỉ email trên toàn thế giới.

Cuộc tấn công lừa đảo lừa đảo và thuyết phục người dùng bằng nội dung kỹ thuật giả mạo cùng với các hoạt động kỹ thuật xã hội. Nhiệm vụ chính của những kẻ lừa đảo là khiến nạn nhân tin rằng các trang lừa đảo là hợp pháp. Các nguồn có thể bị mạo danh bao gồm các trang web, tin nhắn tức thời, email và Trò chuyện chuyển tiếp qua Internet. Hầu hết các cuộc tấn công lừa đảo được thực hiện thông qua email, trong đó người dùng nhận được email lừa người dùng để theo liên kết đã cho, điều hướng họ đến một trang web lừa đảo. Email có thể chứa thông báo cho biết rằng một giao dịch cụ thể đã xảy ra từ tài khoản của người dùng và có thể có liên kết để kiểm tra số dư của họ hoặc có thể chứa liên kết để thực hiện kiểm tra bảo mật cho tài khoản của người dùng.

Dưới đây là một số kiểu tấn công lừa đảo:

* **Spear Phishing** là khi, thay vì gửi hàng nghìn email, một số kẻ tấn công sử dụng nội dung kỹ thuật xã hội chuyên biệt nhắm vào một nhân viên cụ thể hoặc một nhóm nhỏ nhân viên trong một tổ chức cụ thể để đánh cắp dữ liệu nhạy cảm như thông tin tài chính và bí mật thương mại. Các tin nhắn lừa đảo có vẻ như đến từ một nguồn đáng tin cậy với một trang web có giao diện chính thức. Email cũng có vẻ là của một cá nhân trong công ty của người nhận, thường là một người nào đó ở vị trí có thẩm quyền. Tuy nhiên, tin nhắn thực sự được gửi bởi kẻ tấn công nhằm lấy thông tin quan trọng về một người nhận cụ thể và tổ chức của họ, chẳng hạn như thông tin đăng nhập, chi tiết thẻ tín dụng, số tài khoản ngân hàng, mật khẩu, tài liệu bí mật, thông tin tài chính và bí mật thương mại. Spear phishing tạo ra tỷ lệ phản hồi cao hơn so với một cuộc tấn công lừa đảo thông thường, vì nó dường như đến từ một nguồn công ty đáng tin cậy.
* **Whaling** là một kiểu tấn công lừa đảo nhằm vào các giám đốc điều hành cấp cao như CEO, CFO, chính trị gia và người nổi tiếng, những người có toàn quyền truy cập vào thông tin bí mật và có giá trị cao. Đây là một thủ thuật kỹ thuật xã hội trong đó kẻ tấn công lừa nạn nhân tiết lộ thông tin cá nhân và công ty quan trọng (chẳng hạn như chi tiết tài khoản ngân hàng, chi tiết nhân viên, thông tin khách hàng và chi tiết thẻ tín dụng), thường thông qua giả mạo email hoặc trang web. Đánh bắt cá voi khác với tấn công lừa đảo; trong trường hợp này, email hoặc trang web được sử dụng cho cuộc tấn công được thiết kế cẩn thận để nhắm mục tiêu cụ thể là ai đó trong ban lãnh đạo điều hành.
* **Pharming** là một kỹ thuật kỹ thuật xã hội trong đó kẻ tấn công thực thi các chương trình độc hại trên máy tính hoặc máy chủ của nạn nhân. Khi nạn nhân nhập bất kỳ URL hoặc tên miền nào, nó sẽ tự động chuyển hướng lưu lượng truy cập của nạn nhân đến một trang web do kẻ tấn công kiểm soát. Cuộc tấn công này còn được gọi là "Lừa đảo không có mồi nhử": Kẻ tấn công đánh cắp thông tin bí mật như thông tin xác thực, chi tiết ngân hàng và các thông tin khác liên quan đến các dịch vụ dựa trên web. Các cuộc tấn công bằng thuốc có thể được thực hiện theo hai cách, cụ thể là đầu độc bộ đệm của Hệ thống tên miền (DNS) và sửa đổi tệp máy chủ.
* **Spimming** hoặc "spam qua nhắn tin tức thời" (SPIM) khai thác các nền tảng nhắn tin tức thời và sử dụng IM làm công cụ để phát tán thư rác. Một người tạo thư rác qua IM được gọi là người tạo thư rác. Người gửi tin nhắn rác thường sử dụng bot (một ứng dụng thực thi các tác vụ tự động qua mạng) để thu thập ID tin nhắn tức thời và chuyển tiếp tin nhắn rác tới chúng. Tin nhắn SPIM, tương tự như thư rác email, thường bao gồm quảng cáo và phần mềm độc hại dưới dạng tệp đính kèm hoặc siêu liên kết được nhúng. Người dùng nhấp vào tệp đính kèm sẽ được chuyển hướng đến một trang web độc hại, trang này thu thập thông tin cá nhân và tài chính như thông tin xác thực, tài khoản ngân hàng và chi tiết thẻ tín dụng.thực, tài khoản ngân hàng và chi tiết thẻ tín dụng.

### Đánh bom thư

Đánh bom email đề cập đến quá trình gửi liên tục một email đến một địa chỉ cụ thể tại trang web của một nạn nhân cụ thể. Trong nhiều trường hợp, các tin nhắn sẽ chứa đầy dữ liệu rác nhằm tiêu tốn nhiều dung lượng mạng và hệ thống hơn.

Nhiều tài khoản tại trang đích có thể bị lạm dụng, làm tăng tác động từ chối dịch vụ. Đánh bom thư là một hành động cố ý gửi nhiều bản sao có nội dung giống hệt nhau đến cùng một người nhận. Mục tiêu chính đằng sau nó là làm quá tải máy chủ email và làm suy giảm hệ thống liên lạc bằng cách làm cho nó không thể sử dụng được. Thông thường, kẻ đánh bom thư và nạn nhân biết nhau. Các bài đăng trong nhóm tin tức không đồng ý với ý kiến của người nhận cũng dẫn đến đánh bom thư. Mục tiêu trong những trường hợp như vậy có thể là một máy cụ thể hoặc một người cụ thể. Ném bom thư bị lạm dụng nhiều hơn là gửi thư rác vì nó không chỉ gửi thư với số lượng quá lớn cho một cá nhân mà còn ngăn người dùng khác truy cập email của họ bằng cùng một máy chủ.

### Bão thư

Bão thư xảy ra khi các máy tính bắt đầu giao tiếp mà không có sự can thiệp của con người. Một loạt thư rác được gửi do vô tình là bão thư. Việc sử dụng danh sách gửi thư, email tự động chuyển tiếp, phản hồi tự động và sự hiện diện của nhiều địa chỉ email là những nguyên nhân khác nhau gây ra cơn bão thư. Mã phần mềm độc hại cũng được viết để tạo ra các cơn bão thư, chẳng hạn như thông báo "Melissa, I-Care-For-U". Bão thư cản trở các hệ thống thông tin liên lạc và khiến chúng không hoạt động được.

**Tội phạm được hỗ trợ bởi email.**

### Mạo danh

Mạo danh là hành vi truy xuất và sử dụng bất hợp pháp dữ liệu cá nhân của người khác để thu lợi bất chính và tiền bạc. Trộm cắp danh tính là một tội phạm đang nhanh chóng trở nên phổ biến. Đó là hành động cố ý đánh cắp danh tính của ai đó vì lợi ích tiền tệ. Tội phạm có được thông tin cá nhân về một người và lạm dụng nó, gây tổn thất tài chính nặng nề cho nạn nhân. Các trang web mua sắm trực tuyến có thông tin sai lệch và email spam chứa các ưu đãi không thể cưỡng lại là những phương tiện phổ biến được sử dụng để lấy số thẻ tín dụng của nạn nhân. Khi người dùng đã đặt hàng trực tuyến, bọn tội phạm có thể chặn email và sử dụng nó. Bọn tội phạm không chỉ rút số tiền khổng lồ từ tài khoản của nạn nhân mà còn có thể khiến nạn nhân phá sản.

### Theo dõi qua mạng

Theo dõi qua mạng là một tội phạm mà những kẻ tấn công quấy rối một cá nhân, một nhóm hoặc một tổ chức bằng email hoặc IM. Những kẻ tấn công cố gắng đe dọa, gạ gẫm quan hệ tình dục, buộc tội sai, phỉ báng, vu khống, bôi nhọ hoặc đánh cắp danh tính của nạn nhân/các nạn nhân như một phần của hành vi rình rập trên mạng. Kẻ rình rập có thể là người có quan hệ với nạn nhân hoặc người lạ.

### Bắt cóc trẻ em

Bắt cóc trẻ em là hành vi phạm tội lấy đi hoặc giữ lại, giam giữ hoặc che giấu một đứa trẻ hoặc em bé một cách sai trái. Bắt cóc được định nghĩa là lấy đi một người bằng cách thuyết phục, lừa đảo, hoặc cưỡng bức hoặc bạo lực. Có hai hình thức bắt cóc trẻ em: cha mẹ bắt cóc trẻ em và bắt cóc bởi người lạ. Bắt cóc trẻ em của cha mẹ là loại phổ biến nhất, trong khi bắt cóc bởi một người lạ sẽ được phân loại là bắt cóc.

## Các bước điều tra tội phạm email

Để có thể tìm, trích xuất và phân tích bằng chứng liên quan đến email, điều tra viên phải tuân theo một loạt các bước được xác định và thực hành. Điều này không chỉ giúp giảm bớt quá trình thu thập bằng chứng mà còn giúp điều tra viên duy trì sự tuân thủ và liêm chính.

Một số bước quan trọng cần tuân theo: nợ trong khi tiến hành điều tra tội phạm email như:

* Chiếm đoạt tài khoản máy tính và email
* Lấy dữ liệu email
* Kiểm tra email
* Truy xuất tiêu đề email
* Phân tích tiêu đề email
* Khôi phục email đã xóa

### Bước 1: Thu giữ tài khoản máy tính và email

Để tiến hành kiểm tra tại chỗ máy tính và máy chủ email, điều tra viên phải xin lệnh khám xét bằng ngôn ngữ thích hợp. Sau đó, họ nên tiến hành kiểm tra pháp y trên thiết bị được phép, như được đề cập trong lệnh. Tất cả các máy tính và tài khoản email bị nghi ngờ có liên quan đến tội phạm nên bị tịch thu. Điều tra viên có thể chiếm giữ các tài khoản email bằng cách thay đổi mật khẩu hiện tại của nó - bằng cách hỏi mật khẩu của nạn nhân hoặc lấy nó từ máy chủ thư.

Nếu nạn nhân là một tổ chức doanh nghiệp, thì điều tra viên nên xin phép các cơ quan hữu quan và cộng tác với quản trị viên hệ thống và mạng nội bộ để hiểu chính sách của họ và tuân thủ các quy định về an toàn dữ liệu của họ.

### Bước 2: Thu thập dữ liệu email

Khi tài khoản máy tính và email đã bị thu giữ, bước tiếp theo là thu thập dữ liệu email để phân tích pháp y. Việc thu thập dữ liệu email phụ thuộc vào các tình huống sau:

* Nghi phạm đã truy cập email thông qua các ứng dụng email dựa trên máy tính để bàn như Outlook và Mozilla Thunderbird.
* Nghi phạm có một tài khoản email dựa trên web mà họ đã truy cập thông qua trình duyệt.

Điều tra viên cần chọn quy trình thu thập tùy theo tình huống tại hiện trường vụ án.

#### Thu thập dữ liệu email từ ứng dụng email khách trên máy tính để bàn

Nhiều người dùng thích các ứng dụng email dựa trên máy tính để bàn như Microsoft Outlook, Mozilla Thunderbird và Apple mail để gửi/nhận email. Khi tội phạm email bị nghi ngờ đã xảy ra trên máy của người dùng sử dụng ứng dụng email khách, nguồn bằng chứng chính là các thư mục cục bộ và tệp lưu trữ được lưu trữ bởi các chương trình này chứa thông tin in đậm về tất cả các hoạt động email. Công việc của điều tra viên pháp y là xác định vị trí các thư mục cục bộ và trích xuất tất cả các email bằng công cụ pháp y phù hợp và lưu trữ các bản sao ở một vị trí an toàn.

Các tệp/cơ sở dữ liệu email cục bộ do ứng dụng email khách tạo ra có thể được lưu ở nhiều vị trí khác nhau trên máy tính của kẻ tình nghi. Điều tra viên cần xác định cẩn thận tất cả các tệp email cục bộ và thu thập các thông báo email có liên quan đến tội phạm.

#### Tệp email cục bộ trong Microsoft Outlook

Khi một tài khoản email được đồng bộ hóa với ứng dụng Microsoft Outlook trên máy tính, nó sẽ tạo một bản sao cục bộ của tất cả các thư mục email ở hai định dạng sau:

* Bảng lưu trữ cá nhân (.pst)

Nói chung, tài khoản pop lưu trữ tất cả thông tin email ở định dạng tệp .pst trong Outlook. Thông báo email, liên hệ, lịch và dữ liệu tác vụ khác được tự động tải xuống từ máy chủ thư và được lưu cục bộ trên đĩa cứng. Trong Outlook 2013 và các phiên bản cũ hơn, các tệp .pst đã được tài khoản IMAP sử dụng.

Tuy nhiên, trong Outlook 2016, thư email của tất cả các tài khoản IMAP được lưu ở định dạng tệp .ost. Vị trí mặc định của tệp .pst trong Outlook 2016 là như sau:

C:\Users\%USERNAME%\Documents\Outlook Files

* Bảng lưu trữ ngoại tuyến (.ost)

Các loại tài khoản như Outlook.com, Outlook cho Office 365, Microsoft Exchange và IMAP sao chép tất cả các thành phần hộp thư trong định dạng tệp .ost.

Dưới dạng email, liên hệ, lịch và và dữ liệu tác vụ khác không bị loại bỏ khỏi máy chủ như tài khoản pop mà người dùng có thể truy cập email của họ ngay cả khi họ không có kết nối Internet. Tất cả thông tin hộp thư được cập nhật khi kết nối được phục hồi

Mặc định, tệp .ost trong Outlook 2016 được lưu tại vị trí sau:

C:\User\%USERNAME%\AppData\Local\Microsoft\Outlook

Lưu trữ trong Microsoft Outlook

Điều tra viên cũng có thể trích xuất các mảng liên quan đến email từ lưu trữ, một thư mục mặc định được tạo bởi ứng dụng Outlook cho phép người dùng lưu email cũ. Các tính năng tự động có sẵn trong các phiên bản Outlook 2013, 2016, 2019 và chúng cho phép người dùng lưu trữ email tự động theo định kỳ. Các tệp lưu trữ này được lưu trữ trong định dạng .pst.

Để xác định vị trí của tệp lưu trữ Outlook, điều tra viên cần có được thông tin đăng nhập của nghi phạm, mở ứng dụng Outlook và điều hướng đến File 🡪 Options 🡪 Advanced 🡪 AutoArchive Settings.

#### Tệp email cục bộ ở Mozilla Thunderbird

Mozilla Thunderbird là một ứng dụng email phổ biến được sử dụng. Khi bất kỳ người dùng nào định cấu hình tài khoản email có Thunderbird, nó sẽ tạo một thư mục cấu hình ở vị trí sau theo mặc định:

C:\User\%USERNAME%\AppData\Roaming\Thunderbird\Profiles

Trong thư mục Profoles, Thunderbird lưu trữ một bản sao cục bộ của tất cả các thông báo email và bất kỳ thay đổi cấu hình nào được thực hiện bởi người dùng, chẳng hạn như các thay đổi được thực hiện trong cài đặt tài khoản. Thunderbird tạo một thư mục hồ sơ mặc định khi được cài đặt và có thể tạo nhiều tệp hồ sơ khác tùy thuộc vào việc sử dụng. Mỗi hồ sơ quy ước đặt tên sau: <chuỗi ngẫu nhiên gồm tám chữ số> <profile\_name>

Người dùng có thể định cấu hình cả tài khoản email POP3 và IMAP trong Thunderbird. Một thư mục con có tên là “Imapmail”, được tạo ra để lưu trữ hồ sơ thư IMAP, trong khi POP3 Mail và các thư mục khác được lưu trữ riêng trong một thư mục con khác có tên là “Mail”.

Trong Thunderbird, tất cả các tin nhắn email trong các thư mục thư khác nhau, như đã tìm thấy trên giao diện người dùng, được lưu trữ dưới dạng các tệp Mbox không có phần mở rộng. Có các tệp tóm tắt thư hoặc các tệp .msf được tìm thấy trong cùng tên với các tệp Mbox, được sử dụng các chỉ mục của thư. Ví dụ: nội dung của thư mục INBOX được lưu trữ trong hộp thư đến tệp MBOX không có phần mở rộng tệp.

Người dùng Thunderbird sử dụng 1 thư mục con hoặc tệp SBD để lưu trữ các chỉ mục thư và email ở định dạng Mbox và MSF. Tên của thư mục “SBD” phụ thuộc vào loại tài khoản được cấu hình trong Thunderbird. Ví dụ: nếu thư mục “SBD” được tạo ra cho Gmail, Thunderbird sẽ tạo ra một thư mục Gmail.sbd.

Nếu bất kỳ người dùng nào muốn lấy bất kỳ thư gì của máy chủ để tăng không gian lưu trữ, họ có thể lưu một bản sao cục bộ của email đó bằng cách chuyển nó vào thư mục cục bộ, một folder mặc định được tạo bởi Thunderbird. Có thể tìm thấy folder cục bộ trong mặc định nếu Thunderbird được cài đặt và cấu hình với bất kỳ tài khoản người dùng nào:

C:\User\%USERNAME%\AppData\Roaming\Thunderbird\Profiles\<Profile name>\Mail

Có hai thư mục chính bên trong các thư mục cục bộ:

* **Thùng rác**: Thường được sử dụng như một thư mục lưu trữ trên mạng để lưu trữ các tin nhắn email
* **Tin nhắn chưa được gửi**: Được sử dụng để lưu trữ nội dung của thư mục Outbox hoặc các tin nhắn được soạn thảo nhưng không được gửi

Trong trường hợp của bất kỳ tài khoản Thunderbird được cấu hình POP3 nào, tất cả các tin nhắn mới được tự động tải xuống và lưu trữ trong người theo dõi cục bộ và lấy ra máy chủ

Chủ tài khoản IMAP có thể chọn tạo một thư mục lưu trữ trên mạng trong Thunderbird để giữ một bản sao lưu cục bộ các tin nhắn email quan trọng. Tệp lưu trữ cục bộ được lưu trữ trong đường dẫn:

C:\User\%USERNAME%\AppData\Roaming\Thunderbird\Profiles\<Profile name>\Mail\Local Folder.

Tuy nhiên, người dùng cũng có thể lưu tệp lưu trữ này trong các đường dẫn khác.

Để xác định vị trí của thư mục lưu trữ trên mạng, điều tra viên có thể đăng nhập vào ứng dụng email Thunderbird bằng cách sử dụng thông tin đăng nhập của nghi phạm, điều hướng đến Setting 🡪 Account Setting 🡪 Copies and Folder và kiểm tra đường dẫn được đưa ra trong kho lưu trữ tin nhắn (như được mô tả Trong hình dưới đây).

#### Thu thập các các tệp email cục bộ Thunderbird SysTools MailPro+

Là một điều tra viên pháp y, bạn có thể sử dụng các công cụ như SysTools MailPro+ để có được dữ liệu tệp email cục bộ được lưu trữ bởi Thunderbird. Họ có thể chọn một hoặc nhiều tệp Mbox hoặc các thư mục email cục bộ cụ thể để thu thập và phân tích pháp y.

Để có được dữ liệu email cục bộ của Mozilla Thunderbird trên SysTools MailPro+, bạn có thể thực hiện các bước sau:

* Chọn tất cả các email có giá trị bằng chứng và nhấp vào nút 'Export' để có được chúng
* Bạn có thể chọn định dạng tên và loại tệp đã xuất và thu thập các thông báo email đã chọn trong thư mục đích đã chọn.

**SysTools mailpro+**

Source: [*https://www.systoolsgroup.com*](https://www.systoolsgroup.com)

Đây là một tiện ích đa năng và toàn diện để xem trước, tìm và xuất email từ nhiều ứng dụng email

**Đặc điểm**

* Hỗ trợ hơn 12 định dạng tệp email
* Đọc hộp thư của bất kỳ loại tệp email nào
* Tìm kiếm email trong các tệp email nguồn chỉ trong vài lần nhấp
* Tạo và trích xuất email từ ổ cứng hoặc lưu trữ ngoài
* Thêm tệp trong ba chế độ vào bảng điều khiển của phần mềm
* Xuất email thành các dạng tệp .pst, .pdf, .msg, .html, .eml, .tiff và .csv
* Xem trước các loại đính kèm như JPG, GIF, PNG, DOC và PDF

**Previewing Emails**

Công cụ này cung cấp bản xem trước các email ở các chế độ khác nhau như được đưa ra dưới đây:

* Chế độ xem Hex bình thường

Nó hiển thị email cùng với các thuộc tính như TO, CC, BCC, chủ đề, ngày và thời gian

* Chế độ xem Hex

Nó hiển thị email bằng mã hex theo cách từng chút một

* Chế độ xem thuộc tính

Nó hiển thị các thuộc tính được liên kết với các email như cờ tin nhắn, người nhận và người gửi

* Chế độ xem tiêu đề tin nhắn

Nó cung cấp các chi tiết xem như X-Priority, ID tin nhắn, chỉ số chủ đề, loại nội dung và thông tin khác

* Chế độ xem MIME

Nó hiển thị email ở định dạng mime với nhiều chi tiết khác nhau

* Chế độ xem HTML

Nó hiển thị email trong HTML với tất cả các thẻ và cơ thể

* Chế độ xem RTF

Điều này cung cấp bản xem trước các email ở định dạng văn bản đơn giản

* Chế độ xem tệp đính kèm

Điều này cho phép người dùng xem các tệp đính kèm trong email

* Chế độ xem phân cấp

Điều này hiển thị chế độ xem phân cấp của thư mục chứa tệp nguồn

#### Thu thập email Outlook: Chuyển đổi Tệp .ost sang pst

Chuyển đổi .ost thành các định dạng tệp .pst cung cấp cho một điều tra viên một cách dễ dàng để có được dữ liệu email được lưu trữ bởi ứng dụng email Outlook. Bạn có thể sử dụng các công cụ như kernel cho .ost to .pst cho mục đích này

**Kernel for OST to PST**

Nguồn: [*https://www.nucleustechnology.com*](https://www.nucleustechnology.com)

Kernel for OST to PST có thể dễ dàng chuyển đổi các tệp OST thành PST và các định dạng tệp khác như PST, EML, MSG, Office 365 và Exchange Server. Công cụ này lưu tệp OST cho máy chủ email khác nhau, ứng dụng email dựa trên web bao gồm Office 365. Nó đi kèm với các bộ lọc giúp chọn các mục cụ thể để di chuyển

**Đặc trưng**

* Chuyển đổi các tệp OST Orphaned thành PST (bất kỳ phiên bản Outlook nào)
* Chuyển đổi các tệp OST có kích thước lớn
* Lấy dữ liệu người dùng từ các tệp OST mồ côi
* Phục hồi các mục hộp thư Outlook đã xóa vĩnh viễn
* Hiển thị email OST và chuyển đổi chúng với tính toàn vẹn hoàn toàn
* Khôi phục email trao đổi cho tài khoản Gmail/Outlook.com
* Tìm và lưu các email cần thiết, ví dụ, PST, MBOX, PDF, DBX và EML/MSG
* Xuất dữ liệu OST để trao đổi trực tiếp và Office 365
* Phục hồi và xuất các tệp
* Sửa chữa các tệp OST bị hỏng trước khi chuyển đổi
* Cung cấp sự phục hồi hộp thư an toàn của các email, tệp đính kèm, mục lịch hiện có/đã bị xóa

**Phiên bản được hỗ trợ**

MS Exchange Server - 2019/2016/2013/2010/2007/2003/2000/5.5 và 5.0, MS Outlook - Office 365/2019/2016/2013/2010/2007/2003/2000/98 và 97 và Outlook Express - 6.0 /5.5/5.0 và 4.0

**Yêu cầu hệ điều hành**

Windows 10, 8.1, 8, 7, Vista, XP, 2000, 98, NT, 95, Windows Server 2016/ 2012/2008 R2/ 2008/2003 R2/ 2003

#### Thu thập tệp Outlook .pst qua SysTools MailPro+

Bạn cũng có thể sử dụng Systools MailPro+ để xem nội dung của tệp .pst và trích xuất tất cả các thông báo email. Có được tin nhắn email bằng cách nhấp vào nút ‘Export’ và lưu chúng vào một vị trí mong muốn.

Các số liệu bên dưới mô tả việc xem tất cả các thư mục và email của tệp .pst liên quan đến tài khoản email nghi ngờ bằng Systools MailPro+ và xuất các tin nhắn được chọn đến một vị trí mong muốn cho mục đích mua lại

#### Thu thập dữ liệu email từ các tài khoản Email trên mạng

Trong khi điều tra tội phạm email, bước đầu tiên là thu thập dữ liệu email để thực hiện phân tích pháp y. Tuy nhiên, điều tra viên pháp y cần phải có thông tin đăng nhập của nghi phạm để có thể có được dữ liệu email từ các tài khoản email trên mạng. Điều tra viên có thể sử dụng các phương pháp sau để có được bằng chứng email để điều tra:

* Sử dụng Google Takeout để tạo kho lưu trữ ngoại tuyến của tài khoản Gmail nghi phạm ở định dạng tệp mbox.
* Đồng bộ hóa tài khoản email dựa trên mạng cụ thể với các ứng dụng email như Outlook hoặc Thunderbird để ghi lại các bản sao cục bộ của dữ liệu email và mua lại chúng bằng các công cụ pháp y. Quá trình này sử dụng đồng bộ hóa POP3/IMAP. Điều quan trọng đối với một điều tra viên pháp y là đảm bảo rằng tính toàn vẹn của dữ liệu không bị thay đổi trong hoặc sau khi đồng bộ hóa với ứng dụng email.

Lưu ý: Email dựa trên mạng là một phần của dịch vụ đám mây và cuộc điều tra của họ cũng sẽ liên quan đến sự hợp tác từ dịch vụ đám mây cung cấp.

### Bước 3: Kiểm tra tin nhắn email

Các điều tra viên pháp y nên kiểm tra chặt chẽ các mục sau trong khi kiểm tra các tin nhắn email đã thu được:

1. **Chủ đề:** Trường này của một email thông báo cho người nhận về thông điệp mà email dự định sẽ truyền tải. Hầu hết các email giả mạo được thiết kế để tạo ra cảm giác hoảng loạn/cấp bách bao gồm nạn nhân để mở thư và đi qua nội dung của nó.
2. **Địa chỉ email của người gửi:** Kẻ tấn công lừa người dùng mục tiêu bằng cách thực hiện các email đáng ngờ Qphear xác thực. Ví dụ: một email xuất hiện dưới tên của ngân hàng, nhưng sử dụng tài khoản Gmail của tên miền của ngân hàng tương ứng, là một chỉ số mạnh mẽ của việc giả mạo
3. **Nội dung email:** Nội dung email chứa thông điệp chính của email. Một nội dung email giả mạo có thể bao gồm các liên kết/siêu liên kết trực tiếp thu hút người dùng cung cấp các chi tiết nhạy cảm. Nội dung của một email giả mạo thường có ngôn ngữ/câu có cấu trúc kém và có vẻ kém chuyên nghiệp.
4. **Tệp đính kèm email:** Những kẻ tấn công thường gửi tài liệu hoặc bản sao pdf có phần mở rộng như .exe, .vbs, .js, .wsf và .zip dưới dạng tệp đính kèm trong email. Các tệp đính kèm này được thiết kế để thực thi các chương trình ẩn như phần mềm gián điệp và phần mềm độc hại trên hệ thống máy tính của người dùng, những chương trình này có thể xâm phạm dữ liệu nhạy cảm.

### Bước 4: Truy xuất tiêu đề email

Tiêu đề email là một thành phần quan trọng của email có thể giúp các điều tra viên truy tìm nguồn gốc của email. Các tiêu đề này cung cấp thông tin về người gửi và nội dung của email. Các chi tiết này về nguồn và (những) người nhận được cung cấp bằng cách sử dụng tiêu đề "From" và "To," tương ứng.

Các tiêu đề cũng chứa thông tin về đường đi của một email trong khi chuyển tiếp. Mỗi MTA nhận được thông báo email, khi nó di chuyển từ nguồn đến đích, sẽ thay đổi phần tiêu đề email. Do đó, các điều tra viên nên kiểm tra phần tiêu đề email và do đó có được dữ liệu quan trọng có giá trị chứng cứ và truy tìm thủ phạm.

Các điều tra viên có thể truy xuất thông tin tiêu đề từ bất kỳ thư email nào sau khi thu thập được. Trong trường hợp họ có quyền truy cập vật lý vào hệ thống của nghi phạm, họ có thể sử dụng cùng một chương trình email mà nghi phạm đã sử dụng để xem email. Quy trình truy xuất tiêu đề email khác nhau trong mỗi chương trình email.

#### Truy xuất tiêu đề email trong Microfoft Outlook

Các bước dưới đây có liên quan đến ứng dụng máy tính để bàn Microsoft Outlook 2016:

1. Khởi chạy ứng dụng máy tính để bàn Microsoft Outlook
2. Xem lại tất cả các email của tài khoản email của nghi phạm và nhấp đúp vào email mà bạn muốn lưu.
3. Nhấp vào nút File nằm ở trên cùng bên trái, sau đó nhấp vào biểu tượng Properties.
4. Khi cửa sổ Properties mở ra, hãy chọn văn bản tiêu đề thư từ hộp Tiêu đề Internet
5. Sao chép và dán văn bản vào bất kỳ trình soạn thảo văn bản nào và lưu tệp

Do đó, bạn có thể lưu văn bản tiêu đề thư của tất cả các thư email cần thiết để tiến hành điều tra thêm về chúng.

#### Truy xuất tiêu đề email trong Microsoft Outlook.com

Các bước được trình bày dưới đây có liên quan đến ứng dụng web Microsoft Outlook:

1. Đăng nhập vào Microsoft Outlook.com
2. Nhấp vào thư mà bạn muốn xem tiêu đề
3. Nhấp vào nút thả xuống More actions, điều hướng đến tùy chọn View message details
4. Chọn văn bản tiêu đề thư từ hộp Message details, sao chép và dán văn bản vào bất kỳ trình soạn thảo văn bản nào và lưu tệp

#### Truy xuất tiêu đề email trong AOL

1. Đăng nhập vào thư AOL và nhấp chuột phải vào thư đã nhận hoặc thư mà bạn muốn xem tiêu đề
2. Điều hướng đến tùy chọn View Message Source
3. Chọn văn bản tiêu đề thư, sao chép và dán văn bản vào bất kỳ trình soạn thảo văn bản nào và lưu tệp

#### Truy xuất tiêu đề email trong Apple Mail

1. Khởi chạy Apple Mail.
2. Chọn thư đã nhận mà bạn muốn xem tiêu đề
3. Vào View → Message → All Headers
4. Chọn văn bản tiêu đề thư
5. Sao chép và dán văn bản vào bất kỳ trình soạn thảo văn bản nào và lưu tệp

#### Truy xuất tiêu đề email trong Gmail

1. Đăng nhập Gmail
2. Chọn thư đã nhận mà bạn muốn xem tiêu đề
3. Nhấp vào nút thả xuống More và điều hướng đến tùy chọn Show original
4. Chọn văn bản tiêu đề thư, sao chép và dán văn bản vào bất kỳ trình soạn thảo văn bản nào, rồi lưu tệp

#### Truy xuất tiêu đề email trong Yahoo Mail

1. Đăng nhập Yahoo Mail
2. Chọn email đã nhận mà bạn muốn xem tiêu đề
3. Nhấp chuột phải vào email và điều hướng đến tùy chọn View raw message
4. Chọn văn bản tệp tiêu đề thư, sao chép và dán văn bản vào bất kỳ trình soạn thảo văn bản nào và lưu tệp

### Bước 5: Phân tích tiêu đề email

Phân tích tiêu đề email là một khía cạnh quan trọng trong điều tra tội phạm email, vì chúng lưu trữ siêu dữ liệu email và các thông tin khác. Các chi tiết sau có trong tiêu đề email:

1. **Time stamp**

Điều này phản ánh ngày và thời gian khi một email được gửi

1. **From**

Tiêu đề này phản ánh ID email của người gửi như được thấy ở cuối người nhận. Tiêu đề "From" có thể bị giả mạo trong trường hợp email spam.

1. **To**

Tiêu đề này hiển thị ID email của người nhận

1. **Message ID**

Mỗi email có một ID duy nhất được liên kết với nó. Không có hai email nào, kể cả trong cùng một chuỗi email, có thể có cùng ID Thư. Các ID Thư này được tạo bởi máy chủ MTA/mail duy nhất trên toàn cầu của hệ thống gửi thư. ID tin nhắn duy nhất trên toàn cầu của một email là một chỉ báo về tính xác thực của nó. Phần trước "@" trong ID thư biểu thị dấu thời gian được liên kết với thông báo email cụ thể đó. Phần ID tin nhắn sau "@" biểu thị tên miền đủ điều kiện (FQDN) phản ánh tên miền của bất kỳ máy chủ lưu trữ nào đánh dấu sự hiện diện trực tuyến duy nhất của nó.

**Subject**

Tiêu đề này hiển thị chủ đề do người gửi cung cấp

1. **MIME**

Phần mở rộng thư Internet đa mục đích (MIME) cho phép người dùng email gửi các tệp phương tiện như âm thanh, video và hình ảnh như một phần của thông điệp email

**Ví dụ về tiêu đề MIME**

* **MIME-Version**: tiêu đề này cho biết thư được định dạng MIME. Theo giá trị mặc định là 1.0.
* **Content-Type**: Tiêu đề này chỉ định loại nội dung và loại phụ trong một thông báo, chẳng hạn như sau:
  + **Text/plain** hiển thị loại tin nhắn
  + **Audio/mp3, image/jpeg, video/mp4**, tương ứng, đại diện cho các email chứa tệp âm thanh, tệp hình ảnh và tệp video
  + **Multipart/signature** cho thấy rằng một email có chữ ký
  + **Multipart/mixed** cho biết email có văn bản cùng với tệp đính kèm
* **Content Disposition**: Tiêu đề này chỉ định cách một thông báo hoặc phần nội dung của nó phải được trình bày
* **Content-Transfer Encoding**: Tiêu đề này đại diện cho mã hóa có trong tin nhắn
* **Content Description**: Đây là tiêu đề MIME tùy chọn được sử dụng để cung cấp thông tin bổ sung liên quan đến nội dung của thông báo email

1. **Received Headers**

Tiêu đề nhận được chứa thông tin chi tiết về tất cả các máy chủ thư mà thư email đi qua đó trong khi chuyển tiếp. Các tiêu đề này được tạo mỗi khi email truyền qua máy chủ thư/MTA trên đường đến người nhận.

Bất cứ khi nào bất kỳ máy chủ SMTP nào nhận được thông báo email, tiêu đề nhận được sẽ được thêm vào email. Trong tiêu đề email, các tiêu đề đã nhận được đặt theo thứ tự ngược lại, tiêu đề nhận được gần đây nhất hoặc được tạo cuối cùng sẽ xuất hiện đầu tiên và tiêu đề đã nhận được tạo trước tiên xuất hiện sau cùng.

Do đó, các điều tra viên cần bắt đầu kiểm tra tiêu đề nhận được ở dưới cùng, vì nó phản ánh thông tin về máy chủ thư của người gửi. Sau đó, họ có thể tiếp tục lên trên cùng, phần này sẽ cung cấp cho họ dữ liệu về máy chủ thư và địa chỉ IP được liên kết với người nhận.

1. **Return-Path**

Tiêu đề này được sử dụng để chỉ định địa chỉ email mà một email sẽ được gửi/trả lại nếu nó không đến được người nhận dự định. Khi một email không đến được người nhận dự định, nó sẽ bị trả lại. Nghĩa là, nó được trả lại cho người gửi email, trừ khi người gửi chỉ định một địa chỉ email khác nơi các email bị trả lại sẽ được gửi. Nếu địa chỉ đường dẫn trả lại và địa chỉ email của người gửi khác nhau, thì đó là dấu hiệu gửi thư rác/giả mạo.

1. **Received-SPF**

Khung chính sách người gửi (SPF) ngăn chặn giả mạo địa chỉ người gửi. SPF cho phép các tổ chức chỉ định các máy chủ có thể gửi email thay mặt cho miền của họ. Khung triển khai bản ghi SPF, đề cập đến bản ghi DNS được thêm vào vùng DNS của miền của tổ chức. Trong bản ghi SPF, một tổ chức có thể xác định tên máy chủ và/hoặc địa chỉ IP được phép gửi email từ miền của họ. Thông qua việc triển khai SPF, kết quả trao đổi qua email có thể như sau.

* **Received-SPF: None:** Điều này có nghĩa là không tìm thấy bản ghi SPF nào cho miền.
* **Received-SPF: Neutral:** Điều này có nghĩa là địa chỉ IP của người gửi không được phép cũng như không bị hạn chế gửi email thay mặt cho miền của tổ chức. Kết quả trung lập được xử lý theo cách tương tự như kết quả "None".
* **Received-SPF: Pass:** Điều này có nghĩa là địa chỉ IP của người gửi được phép gửi email từ miền.
* **Received-SPF - fail, or hard fail**: Điều này có nghĩa là email đã bị bộ trao đổi thư của người nhận từ chối vì địa chỉ IP của người gửi không được phép gửi email từ miền. Lỗi cứng SPF được thực thi bằng cách thêm cơ chế "-all" vào bản ghi SPF.

**Ví dụ**: v=spf1 ip4: 207.84.200.37 -all

Trong ví dụ trên, "-all" có nghĩa là những người gửi không được liệt kê trong bản ghi DNS được đề cập (ví dụ: 207.84.200.37) sẽ được coi là không được phép và email từ họ sẽ bị từ chối. Chỉ có địa chỉ IP 207.84.200.37 là được phép gửi email.

* **Received-SPF: Softfail:** : Điều này có nghĩa là có khả năng các địa chỉ IP có thể có hoặc không có quyền gửi email thay mặt cho tên miền được đề cập.

**Ví dụ**: v=spf1 bao gồm: modprod.outlook.com ~all

Trong ví dụ trên, ký hiệu "~" cho biết rằng các thư đến từ bất kỳ máy chủ nào không được đề cập ở đây sẽ được gửi đi nhưng được coi là một lỗi mềm. Trong trường hợp này, nhà cung cấp hộp thư đánh dấu thư là thư rác hoặc email rác. Chỉ những thư đến từ Microsoft Office 365 sẽ được gắn thẻ là SPF PASS.

1. **Chữ ký thư được xác định bằng khóa tên miền:**

Thư được xác định bằng khóa miền (DKIM) đề cập đến một phương thức xác thực email giúp bảo vệ người gửi và người nhận email khỏi hành vi lừa đảo, giả mạo và gửi thư rác. Kỹ thuật này xác minh rằng thông điệp email mà người nhận nhận được đã được gửi từ một máy chủ thư hợp pháp. Phương pháp xác thực email này sử dụng mật mã khóa công khai để phát hiện và ngăn chặn việc gửi email độc hại. Chữ ký kỹ thuật số/DKIM này được bảo mật thông qua mã hóa. DKIM cũng đảm bảo rằng các email và nội dung của chúng không bị thay đổi trong khi chuyển tiếp giữa máy chủ của người gửi và người nhận. Hầu hết các nhà cung cấp dịch vụ email đều tìm chữ ký DKIM trong email.

Máy chủ thư nhận email có thể xác thực chữ ký DKIM của người gửi với sự trợ giúp của khóa mật mã công khai đã đăng ký trong DNS. Máy chủ thư đến sử dụng khóa công khai này để giải mã chữ ký (giá trị băm) và xác minh chữ ký đó bằng giá trị băm mới được tính toán. Nếu các giá trị hai hàm khớp nhau thì thông báo được coi là xác thực và không bị thay đổi.

**Ví dụ về Tiêu đề Chữ ký DKIM**

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

d=gmail.com; s=20161025pm;

h=mime-version:from:date:message-id:subject:to;

bh=RqlJ8naev02DhEPJtIFAsdUqiGR7RyzmJ9cSxw5KzCY=;

b=BYQQZk7S77sJJef1WEXGyTmfb8sUF6S7W8wi93/hh7WthcGjc2lk/NfpgqVpeXrhHPUjuv36G1DVe6TBzdHsjdDLzs4b3sATMSAZNZAEDA44Tm500GJbhBQ8iNjRgD7eYWEEPLCFOU/eBBU1Nteh9MOqxIBJYJ1ZHGB+dz9zyfsyQAiHik3Db1GLhXCvfYdkEWydjGN2CH7/1d031JCcF5z5sVwPYDz69dCKmyl3/WckXU/KU+xRVX4NjffZOWHBOXOK47H7YcJZyeaFoeirs/UJVZH2xKZcjSMhBS9Q/4GAuACp5ehT2GtM7B0QB/H4wVV7gdQrrHjBUEwJGXIDIQ=

Trong đó:

* **v=1:** Nó hiển thị phiên bản DKIM là 1
* **a=rsa-sha256**: Trường "a=" cho biết thuật toán băm được sử dụng để tạo khóa riêng hoặc khóa chung. rsa-sha1 và rsa-sha256 là hai thuật toán chữ ký được hỗ trợ chính thức để tạo giá trị băm cho khóa riêng tư/công khai
* **c=relaxed/relaxed**: Trường "c=" cho biết thuật toán chuẩn hóa được sử dụng. Nó hiển thị nếu có bất kỳ sửa đổi nào trong email về khoảng trắng hoặc dòng xuống dòng. Giá trị đầu tiên trước "/" là dành cho tiêu đề và phần còn lại dành cho phần thân.
* **d=gmail.com**: Trường "d=" đại diện cho tên miền email của người gửi
* **s=20161025pm**: Trường "s=" đề cập đến bộ chọn để xác định khóa DKIM công khai
* **bh=RqlJ8naev02DhEPJtIFAsdUqiGR7 RyzmJ9cSxw5KzCY=:** Giá trị này biểu thị giá trị băm cho nội dung theo thuật toán băm đang sử dụng và sau đó được mã hóa trong Base64
* **b=**: Điều này giữ chữ ký DKIM sẽ được tính theo trường tiêu đề được cung cấp trong trường "h="

#### Phân tích tiêu đề email: Kiểm tra tính xác thực của email

Địa chỉ email hợp lệ là địa chỉ mà email có thể được gửi thành công. Nó có thể xác thực danh tính của một người hoặc một thực thể/tổ chức.

Nếu các điều tra viên pháp y bắt gặp một địa chỉ email đáng ngờ trong quá trình điều tra tiêu đề email, họ nên sử dụng các công cụ như Email Dossier để xác minh tính xác thực của địa chỉ email.

**Email Dossier**

Nguồn: [*https://centralops.net*](https://centralops.net)

Công cụ này cung cấp một trường để nhập địa chỉ email để có thể xác minh tính hợp pháp của nó. Công cụ này cung cấp thông tin về địa chỉ email, bao gồm các bản ghi trao đổi thư.

Email Dossier khởi tạo các phiên SMTP để kiểm tra việc chấp nhận một địa chỉ email, nhưng nó không thực sự gửi email. Khi một địa chỉ email hợp lệ/xác thực, công cụ này sẽ cung cấp những thông tin sau:

* Hiển thị kết quả "3-SMTP" so với trường "xếp hạng độ tin cậy".
* Hiển thị các bản ghi Mail Exchange hoặc MX với các trường địa chỉ IP, trao đổi và tùy chọn
* Hiển thị các phiên SMTP mà nó đã bắt đầu để kiểm tra việc chấp nhận địa chỉ email

Một số công cụ khác để kiểm tra tính xác thực của địa chỉ email như sau:

**Email Address Verifier**

Nguồn: [*https://tools.verifyemailaddress.io*](https://tools.verifyemailaddress.io)

Công cụ xác minh email này thiết lập kết nối với hộp thư để xác định xem địa chỉ email có tồn tại hay không.

**Email Checker**

Nguồn: [*http://email-checker.net*](http://email-checker.net)

Công cụ này cung cấp một trường/hộp trong đó có thể nhập địa chỉ email để kiểm tra xem địa chỉ đó có hợp pháp hay không. Công cụ lấy các bản ghi trao đổi thư từ địa chỉ email và kết nối với máy chủ thư để xác minh rằng một hộp thư nhất định thực sự tồn tại cho địa chỉ email đã cho.

**G-Lock Software Email Verifier**

Nguồn: [*http://www.glocksoft.com*](http://www.glocksoft.com)

Công cụ này quét từng địa chỉ email được cung cấp từ danh sách gửi thư hoặc cơ sở dữ liệu để xác minh xem địa chỉ email có hợp lệ hay không.

#### Phân tích tiêu đề email: Kiểm tra địa chỉ IP gốc

Trong quá trình phân tích tiêu đề của một email đáng ngờ, các điều tra viên phải xác định địa chỉ IP của máy chủ thư nơi bắt nguồn thư email để truy tìm kẻ tấn công. Để làm điều này, các điều tra viên có thể sử dụng cơ sở dữ liệu trực tuyến như cơ sở dữ liệu Whois hoặc các trang web như whatismyipaddress.com. Sau đó, họ có thể tìm kiếm địa chỉ địa lý của người gửi trong cơ sở dữ liệu.

**Smart Whois Database**

Nguồn: [*https://whois.urih.com*](https://whois.urih.com)

Cơ sở dữ liệu Whois thông minh là cơ sở dữ liệu có sẵn công khai chứa thông tin chi tiết liên quan đến (những) chủ sở hữu hoặc (những) người liên hệ của mọi tên miền và dữ liệu máy chủ.

**Whatismyipaddress**

Nguồn: [*www.whatismyipaddress.com*](http://www.whatismyipaddress.com)

whatismyipaddress.com chứa phần tra cứu địa chỉ IP mà qua đó các điều tra viên có thể xác định địa chỉ IPv4 hoặc IPv6 của người dùng Internet hoặc biết được họ đang ở khu vực nào của quốc gia hoặc thế giới.

#### Điều tra một email đáng ngờ

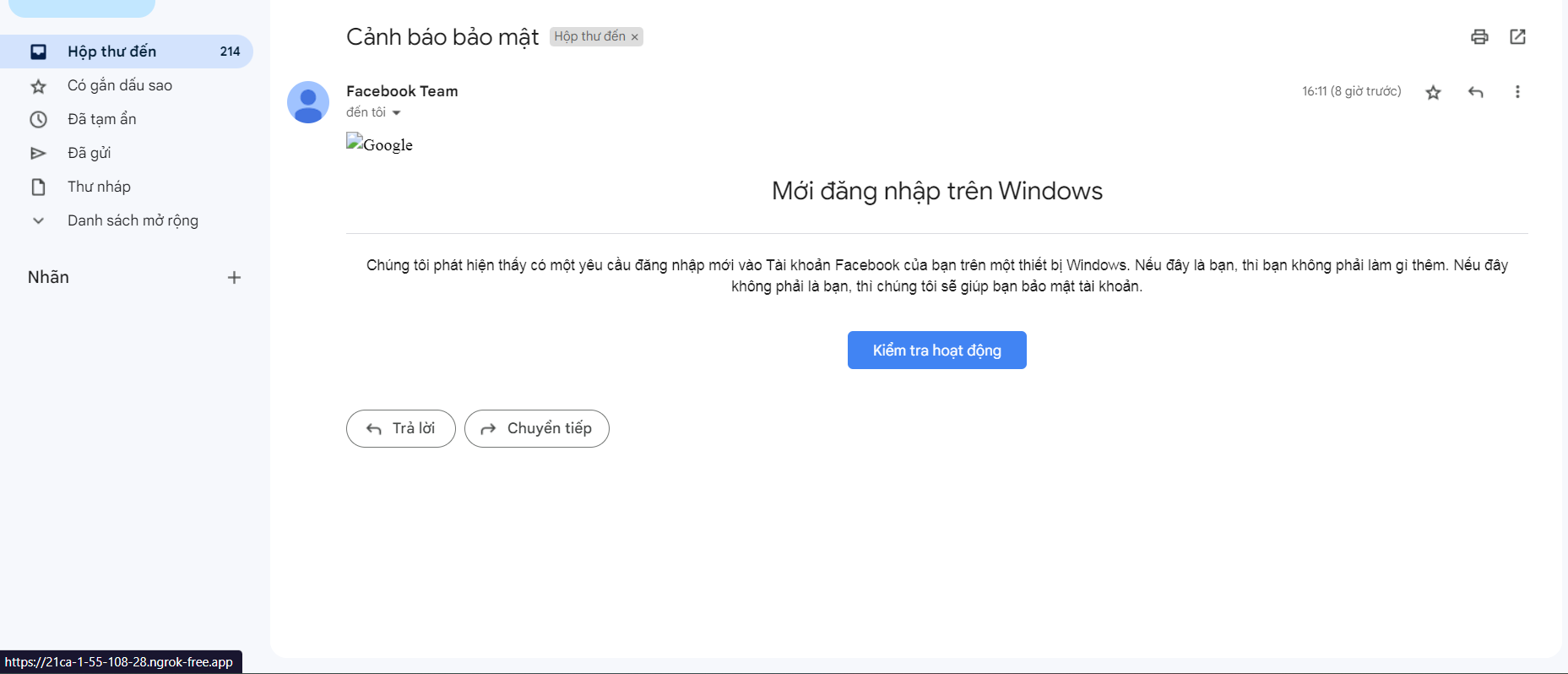
Nếu một email được xác định là đáng ngờ, các phần chính của nó, bao gồm trường chủ đề, nội dung email, các tiêu đề email như tiêu đề đã nhận, Đã nhận-SPF và ID Thư, phải được kiểm tra kỹ lưỡng để điều tra và xác định trong trường hợp email độc hại hoặc bị giả mạo.

Dưới đây là một số thành phần mà các điều tra viên phải kiểm tra để hiểu liệu một email là thật hay giả mạo:

1. **Kiểm tra Email**

Trong khi kiểm tra một email đáng ngờ, các điều tra viên phải theo sát chủ đề, nội dung và tệp đính kèm của email để trích xuất dữ liệu có giá trị bằng chứng. Ảnh chụp màn hình bên dưới hiển thị một thông báo email có dòng tiêu đề được viết theo cách tạo cảm giác cấp bách cho người nhận và do đó, lôi kéo người đọc nhấp vào thư để đọc thư.

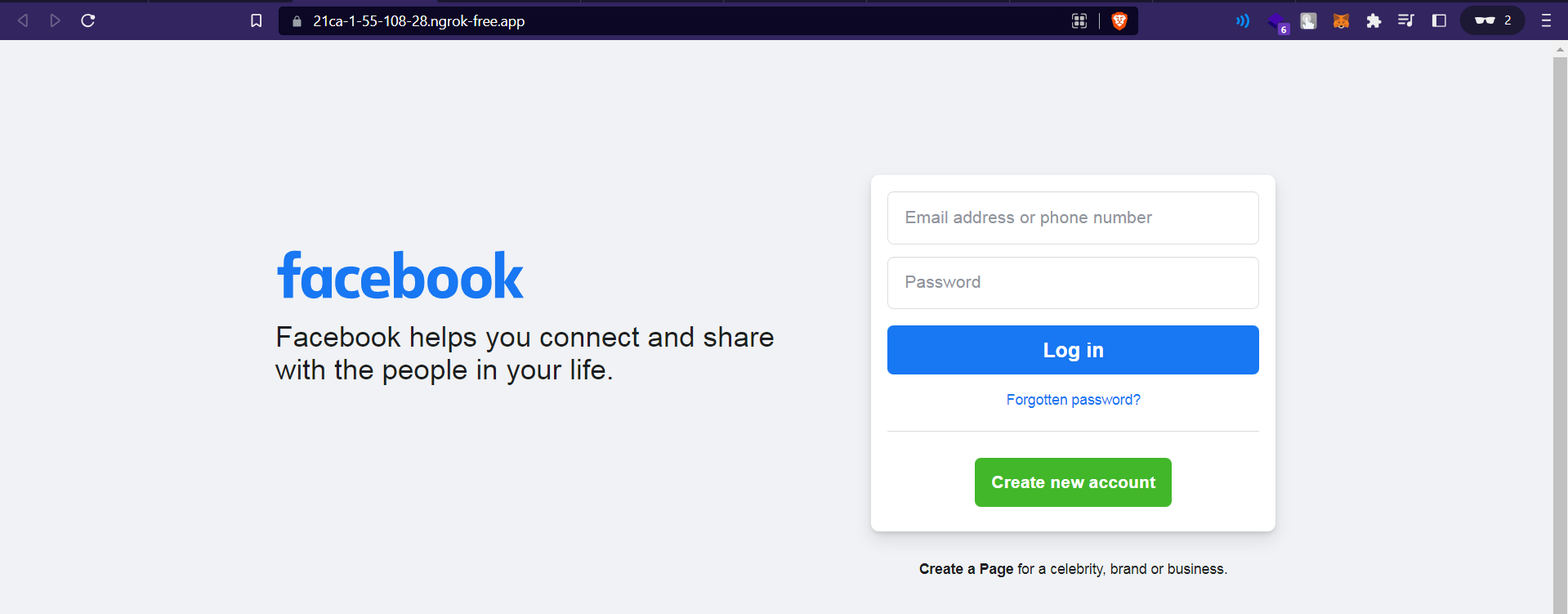
Ngoài ra, nội dung email chứa liên kết đến trang đăng nhập của Facebook. Tuy nhiên, khi di con trỏ chuột qua liên kết đã cho sẽ hiển thị địa chỉ (https://21ca-1-55-108-28.ngrok-free.app) ở dưới cùng bên trái của cửa sổ email có vẻ đáng ngờ.

****

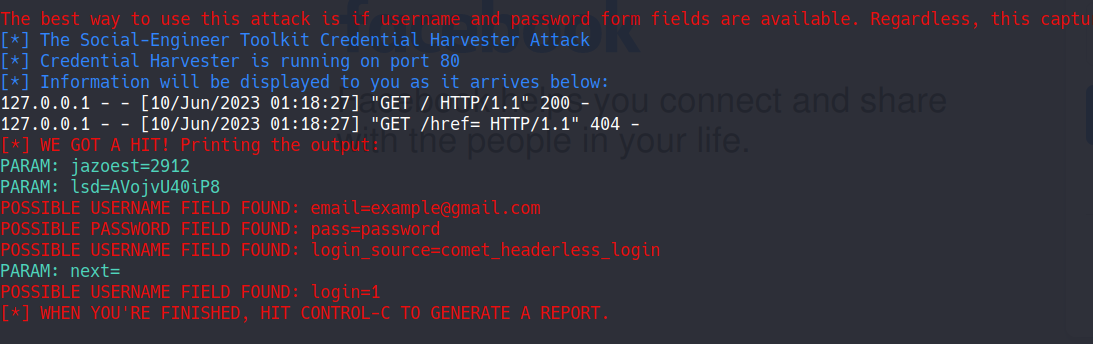
1. **Kiểm tra liên kết**

Nếu tìm thấy bất kỳ liên kết đáng ngờ nào trên nội dung email, điều tra viên có thể kiểm tra liên kết đó bằng cách mở liên kết đó trong môi trường pháp y được kiểm soát.

Ảnh chụp màn hình bên dưới cho thấy rằng liên kết, sau khi được nhấp vào, sẽ chuyển hướng đến một trang web nơi trình duyệt hiển thị "*https://21ca-1-55-108-28.ngrok-free.app*" trong khung URL thay vì URL cho trang đăng nhập của Facebook.

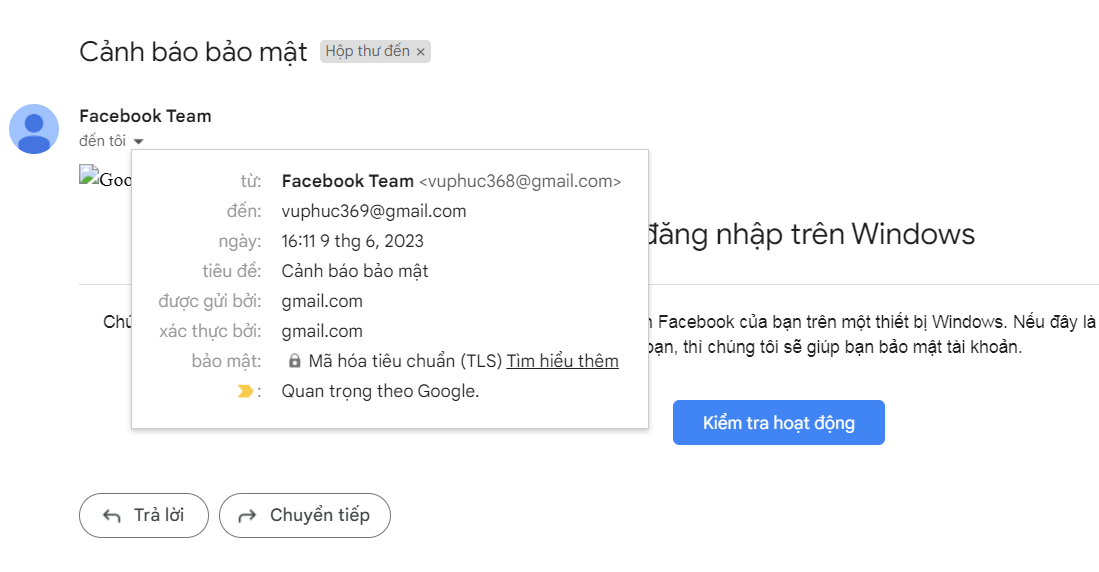


Tuy nhiên, trang đã mở có chứa các trường dành cho tên người dùng và mật khẩu Facebook. Nếu người dùng mục tiêu cung cấp nhầm thông tin đăng nhập của họ, kẻ tấn công sẽ ghi dấu ấn trên máy tấn công của họ.



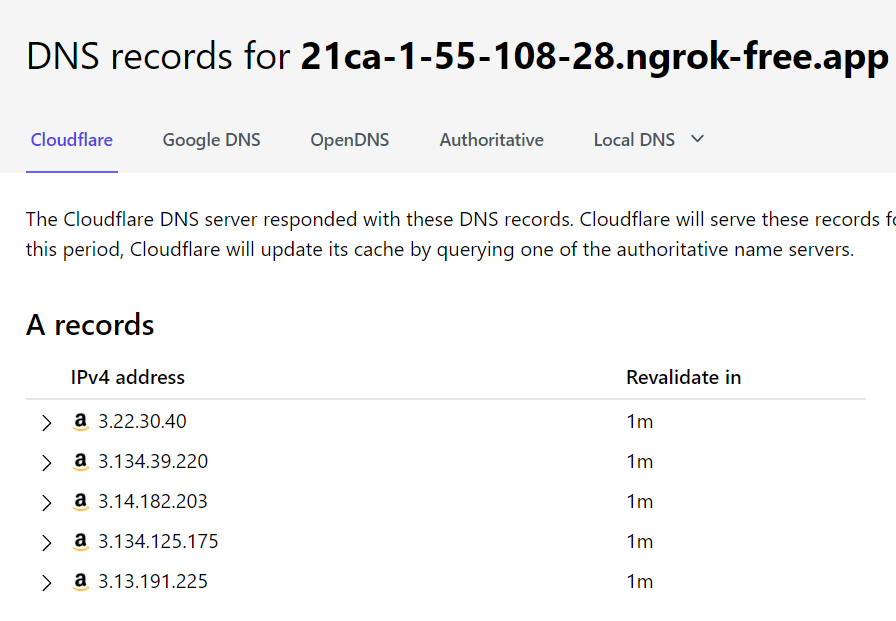
1. **Phân tích các mục tiêu đề đã nhận**

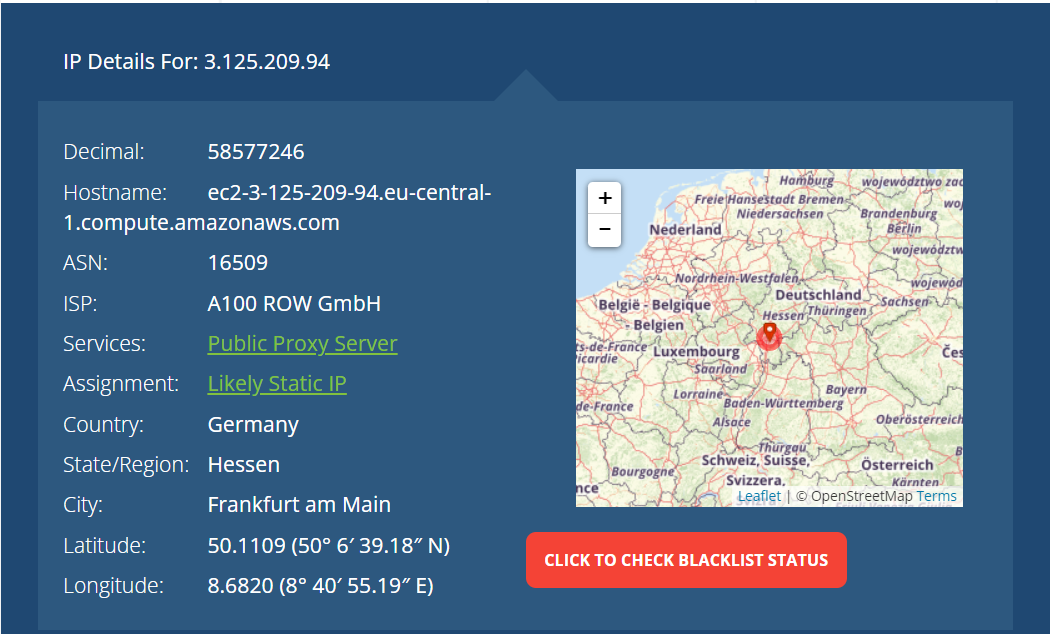
Để tìm thông tin trên máy chủ thư, địa chỉ IP và tên máy chủ được kẻ tấn công/người gửi sử dụng, điều tra viên cần kiểm tra các mục tiêu đề nhận được trong tiêu đề email. Chi tiết về tên máy chủ, máy chủ thư và địa chỉ IP mà kẻ tấn công sử dụng được tiết lộ trong tiêu đề nhận được ở dưới cùng.



1. **Kiểm tra địa chỉ IP ban đầu**

Các điều tra viên có thể nghiên cứu thêm địa chỉ IP thu được từ mục tiêu đề nhận được trên các trang web nslookup.io, whatismyipaddress.com.



****

1. **Kiểm tra trường Received-SPF**

Điều tra viên cũng nên kiểm tra trường tiêu đề Received-SPF để kiểm tra bất kỳ lỗi xác thực SPF nào.

Ảnh chụp màn hình dưới đây cho thấy trường Received-SPF đang hiển thị kết quả "pass", có nghĩa là tên miền vuphuc366@gmail.com (ID email của người gửi như trong email) đã cấp quyền cho địa chỉ IP 209.85.220.41 cho gửi email thay mặt nó.



1. **Kiểm tra tính hợp lệ của email của người gửi**

Sau khi có được ID email của người gửi, điều tra viên nên sử dụng Email Dossier để xác minh xem địa chỉ email của người gửi như được hiển thị trong thư có phải là xác thực hay không.

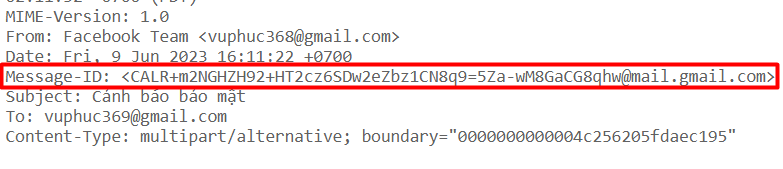
Ảnh chụp màn hình dưới đây được lấy từ Email Dossier, hiển thị địa chỉ email hợp lệ. Với phát hiện này, điều tra viên có thể xác định rằng tài khoản email của người dùng có tên vuphuc366 có thể đã bị kẻ tấn công xâm phạm hoặc ID đã được lấy thông qua các kỹ thuật kỹ thuật xã hội.



1. **Kiểm tra ID tin nhắn**

Kiểm tra ID thư cũng là một phần quan trọng của cuộc điều tra vì nó giúp xác định tính xác thực của thư email.

Ảnh chụp màn hình bên dưới làm nổi bật ID Thư cho thấy rằng tên miền đủ điều kiện (FQDN) là “mail.gmail.com” (là FQDN cho Gmail).



### Bước 6: Khôi phục tin nhắn email đã xóa

Quá trình khôi phục email đã xóa khác nhau dựa trên ứng dụng email được sử dụng để gửi email:

* Phục hồi thư điện tử đã xóa từ Outlook PST

Trong Outlook, thư email sau khi bị xóa sẽ được chuyển đến thư mục “Deleted Items”. Các email đã xóa được lưu trữ trong thư mục “Deleted Items” trong 14 ngày (thời gian lưu giữ mặc định có thể được sửa đổi), sau đó các thư sẽ tự động bị xóa khỏi thư mục đó. Trong trường hợp những email đã xóa này cũng bị xóa khỏi thư mục này, chúng sẽ trở nên vô hình đối với người dùng. Tuy nhiên, chúng không bị xóa hoàn toàn mà được chuyển đến không gian chưa phân bổ của ổ đĩa. Các email đã xóa có thể được khôi phục nếu không gian chưa phân bổ đó không được thay thế bằng dữ liệu mới. Những email này có thể được khôi phục bằng các công cụ pháp y như Trình kiểm tra bằng chứng điện tử của Paraben (E3), nếu nó chưa bị ghi đè.

* Khôi phục Email đã xóa từ Thunderbird

Thunderbird lưu trữ các email đã bị người dùng xóa trong thư mục “Trash”. Thư mục “Trash” lưu trữ các email đã xóa cho đến khi chúng bị xóa. Các công cụ pháp y như Trình kiểm tra bằng chứng điện tử của Paraben (E3) có thể khôi phục các email đã xóa đó tùy thuộc vào thời gian khôi phục được cố gắng. Nếu bất kỳ thư email nào được lưu trữ trong thư mục Thùng rác cục bộ của Thunderbird bị xóa, thì có thể khôi phục hoàn toàn thư đó.

Các điều tra viên pháp y có thể khôi phục dữ liệu email đã xóa vĩnh viễn khỏi tệp Outlook .pst và Thunderbird bằng các công cụ như Trình kiểm tra bằng chứng điện tử của Paraben. Ở đây, dữ liệu email đã xóa vĩnh viễn đề cập đến những email đã xóa đã bị xóa hoặc bị mất khỏi thư mục “Deleted Items” trong ngữ cảnh của Outlook và những email đã bị xóa hoặc bị mất khỏi thư mục “Trash” cũng như Thư mục “Local Trash” của Thunderbird.

**Paraben’s Electronic Evidence Examiner**

Nguồn: [*https://paraben.com*](https://paraben.com)

E3 là một công cụ phân tích pháp y kỹ thuật số toàn diện được thiết kế để xử lý dữ liệu hiệu quả hơn đồng thời tuân thủ Mô hình P2 của Paraben về trọng tâm chuyên biệt của toàn bộ quy trình kiểm tra pháp y. Nền tảng E3 sử dụng kiến trúc trình cắm nâng cao của Paraben để tạo các công cụ chuyên dụng kiểm tra các yếu tố như email, email mạng, nhật ký trò chuyện, dữ liệu di động, hệ thống tệp và phân tích tệp Internet - đồng thời tăng lượng dữ liệu có thể được xử lý và sử dụng tài nguyên thông qua lập lịch tác vụ và đa luồng. Electronic Evidence Examiner không chỉ có giá phải chăng mà còn chạy hiệu quả với yêu cầu phần cứng thấp hơn.

# MỘT SỐ ĐIỀU LUẬT CHỐNG TỘI PHẠM EMAIL

## Tại Hoa Kỳ

### Luật chống tội phạm email của Hoa Kỳ: Đạo luật CAN-SPAM

Đạo luật CAN-SPAM (Đạo luật kiểm soát hành vi tiếp thị và nội dung khiêu dâm không được yêu cầu) là luật đặt ra các quy tắc gửi email cho mục đích thương mại, thiết lập các yêu cầu tối thiểu đối với nhắn tin thương mại, cho phép người nhận email quyền yêu cầu người gửi ngừng gửi email cho họ và đưa ra các hình phạt trong trường hợp các quy tắc được đề cập bị vi phạm.

### Yêu cầu chính của CAN-SPAM đối với người gửi

* Không sử dụng thông tin tiêu đề sai hoặc gây nhầm lẫn
* Không sử dụng các dòng tiêu đề lừa đảo
* Email thương mại phải được xác định là quảng cáo
* Email phải có địa chỉ bưu chính thực hợp lệ của bạn
* Email phải chứa thông tin cần thiết về cách ngừng nhận email từ người gửi trong tương lai
* Tôn trọng yêu cầu từ chối của người nhận trong vòng 10 ngày làm việc
* Cả công ty có sản phẩm được quảng cáo trong tin nhắn và người gửi email được thuê theo hợp đồng để gửi tin nhắn đều phải tuân thủ luật pháp

### Hình phạt

Tất cả các email vi phạm pháp luật đều phải chịu hình phạt tài chính lên tới 16.000 đô la và tùy thuộc vào trường hợp, một hoặc nhiều người có thể phải chịu trách nhiệm về các vi phạm. Ví dụ: trong trường hợp vi phạm pháp luật thông qua email được gửi để quảng cáo sản phẩm và dịch vụ thương mại, cả công ty có sản phẩm đang được quảng cáo trong tin nhắn và công ty gửi tin nhắn ban đầu đều có thể phải chịu trách nhiệm pháp lý.

Theo Đạo luật CAN-SPAM, có một số vi phạm cụ thể có thể bị phạt bổ sung. Hình phạt hình sự và phạt tù có thể bị kết án cho những điều sau đây:

* Truy cập máy tính của người khác để gửi thư rác mà không được phép
* Sử dụng thông tin sai lệch để đăng ký nhiều tài khoản email hoặc tên miền
* Chuyển tiếp hoặc truyền lại nhiều tin nhắn rác qua một máy tính để đánh lừa người khác về nguồn gốc của tin nhắn
* Thu thập địa chỉ email hoặc tạo ra chúng thông qua một cuộc tấn công từ điển (thực hành gửi email đến các địa chỉ được tạo thành từ các chữ cái và số ngẫu nhiên với hy vọng đạt được những địa chỉ hợp lệ)
* Lợi dụng chuyển tiếp mở hoặc proxy mở mà không được phép

## Tại Việt Nam

Tại Việt Nam, không có một bộ luật hình sự cụ thể chỉ về lừa đảo qua email. Tuy nhiên, hành vi lừa đảo qua email thường xuyên được xem là một hành vi phạm tội và có thể bị xử lý theo các quy định trong Bộ Luật Hình sự của Việt Nam (Luật Số 100/2015/QH13, được sửa đổi và bổ sung). Dưới đây là một số điều mà bạn có thể tìm thấy trong Bộ Luật Hình sự liên quan đến hành vi lừa đảo:

### Khoản 1 Điều 174 Bộ luật Hình sự 2015 (sửa đổi, bổ sung năm 2017):

**Quy định**

“Người nào bằng thủ đoạn gian dối chiếm đoạt tài sản của người khác trị giá từ 2.000.000 đồng đến dưới 50.000.000 đồng hoặc dưới 2.000.000 đồng nhưng thuộc một trong các trường hợp sau đây, thì bị phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:

…”

### *Điều 288 Bộ luật Hình sự năm 2015*

**Quy định**

*“Người nào thực hiện một trong các hành vi sau đây, thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng hoặc gây thiệt hại từ 100.000.000 đồng đến dưới 500.000.000 đồng hoặc gây dư luận xấu làm giảm uy tín của cơ quan, tổ chức, cá nhân, thì bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc bị phạt tù từ 06 tháng đến 03 năm:*

1. *Đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật, nếu không thuộc một trong các trường hợp quy định tại các Điều 117, 155, 156 và 326 của Bộ luật này;*
2. *Mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin đó;*
3. *Hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông.*

*Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 200.000.000 đồng đến 1.000.000.000 đồng hoặc phạt tù từ 02 năm đến 07 năm:*

1. *Có tổ chức;*
2. *Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông;*
3. *Thu lợi bất chính 200.000.000 đồng trở lên;*
4. *Gây thiệt hại 500.000.000 đồng trở lên;*
5. *Xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát;*
6. *Gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội hoặc quan hệ đối ngoại của Việt Nam;*
7. *Dẫn đến biểu tình.*

*Người phạm tội còn có thể bị phạt tiền từ 20.000.000 đồng đến 200.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.”*