TRƯỜNG ĐẠI HỌC KHOA HỌC – ĐẠI HỌC HUẾ
KHOA CÔNG NGHỆ THÔNG TIN

Đề tài:

PHÂN TÍCH EMAIL PHISHING GỒM CÁC VẤN ĐỀ

THU THẬP MỘT EMAIL SCAM, PHÂN TÍCH HEADER NHẬN DIỆN DẤU HIỆU LỪA ĐẢO, ĐỀ XUẤT CÁCH PHÒNG TRÁNH

TÊN LỚP HỌC PHẦN: AN NINH MẠNG

MÃ HỌC PHẦN: TIN3163

GIẢNG VIÊN HƯỚNG DẪN:VÕ VIỆT DŨNG

HUẾ, THÁNG 1 NĂM 2026

TRƯỜNG ĐẠI HỌC KHOA HỌC
KHOA CÔNG NGHỆ THÔNG TIN

Đề tài:

PHÂN TÍCH EMAIL PHISHING GỒM CÁC VẤN ĐỀ

THU THẬP MỘT EMAIL SCAM, PHÂN TÍCH HEADER NHẬN DIỆN DẤU HIỆU LỪA ĐẢO, ĐỀ XUẤT CÁCH PHÒNG TRÁNH

TÊN LỚP HỌC PHẦN: AN NINH MẠNG

MÃ HỌC PHẦN: TIN3163

Giảng viên hướng dẫn : VÕ VIỆT DŨNG

Sinh viên thực hiện : NGUYỄN VĂN ĐẠI : MSV: 23T1020072

NGUYỄN VĂN NHẬT TÂN : MSV: 22T1020410

NGUYỄN THU QUỲNH : MSV: 23T1020443

NGUYỄN THỊ NHẬT QUỲNH: MSV: 21T1020067

NGUYỄN ĐÌNH TIẾN: MSV : 21T1020084

HUẾ, THÁNG 1 NĂM 2026

MỤC LỤC

LỜI CẢM ƠN

Trước tiên, nhóm chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến **thầy VÕ VIỆT DŨNG** – giảng viên hướng dẫn học phần **An ninh mạng**, người đã tận tình giảng dạy, truyền đạt những kiến thức quý báu cũng như tạo điều kiện để nhóm chúng em hoàn thành bài tiểu luận này.

Trong quá trình thực hiện đề tài, nhờ sự hướng dẫn và định hướng của thầy, nhóm chúng em đã hiểu rõ hơn về các nguy cơ an ninh mạng nói chung và Email phishing nói riêng, từ đó có thể tiếp cận đề tài một cách đúng đắn và thực tế hơn.

Nhóm chúng em cũng xin cảm ơn Khoa và Nhà trường đã tạo môi trường học tập thuận lợi, giúp sinh viên có điều kiện tiếp cận với các kiến thức chuyên ngành và thực hành gắn liền với thực tế.

Một lần nữa, nhóm chúng em xin kính chúc thầy luôn dồi dào sức khỏe, thành công trong sự nghiệp giảng dạy và nghiên cứu khoa học.

LỜI NÓI ĐẦU

Trong thời đại số hóa, Email là một trong những phương tiện giao tiếp quan trọng và phổ biến nhất, được sử dụng rộng rãi trong học tập, công việc và kinh doanh. Tuy nhiên, song song với sự phát triển mạnh mẽ đó, email cũng trở thành mục tiêu chính của các cuộc tấn công an ninh mạng như spam, phishing, giả mạo danh tính (email spoofing) và phát tán mã độc.

Theo nhiều báo cáo an ninh mạng, phần lớn các cuộc tấn công xâm nhập hệ thống đều bắt đầu từ email. Kẻ tấn công thường giả mạo địa chỉ email của các tổ chức uy tín để lừa người dùng nhấp vào liên kết độc hại hoặc cung cấp thông tin nhạy cảm. Vì vậy, việc xác thực nguồn gốc và tính toàn vẹn của email là yêu cầu vô cùng quan trọng.

Để giải quyết vấn đề này, nhiều cơ chế bảo mật email đã được xây dựng, trong đó nổi bật nhất là Received-From, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) và DMARC (Domain-based Message Authentication, Reporting & Conformance). Đây là các kỹ thuật cốt lõi giúp ngăn chặn email giả mạo và tăng độ tin cậy cho hệ thống email.

A. PHẦN NỘI DUNG

I.Lý thuyết về An ninh mạng

1. An ninh mạng là gì ?

- An ninh mạng (Cybersecurity) là tập hợp các phương pháp, công cụ và quy trình nhằm bảo vệ hệ thống máy tính, mạng, ứng dụng và dữ liệu khỏi các mối đe dọa kỹ thuật số, đảm bảo tính Bí mật (Confidentiality), Toàn vẹn (Integrity), và Sẵn sàng (Availability) của thông tin, bao gồm bảo vệ chống truy cập trái phép, đánh cắp, thay đổi hoặc phá hoại, thông qua các lớp phòng thủ kỹ thuật (mã hóa, tường lửa) và quy trình quản lý rủi ro, tuân thủ pháp lý.

2. Vai trò của các chuyên gia an ninh mạng.

- Vai trò chính của các chuyên gia an ninh mạng là bảo vệ cơ sở hạ tầng CNTT, mạng máy tính và dữ liệu khỏi các mối đe dọa này. Điều này liên quan đến:

- ***Ngăn chặn các mối đe dọa trên mạng*** : Triển khai các giao thức bảo mật nâng cao, tiến hành kiểm tra hệ thống thường xuyên và đảm bảo rằng tất cả các hệ thống đều được cập nhật các bản vá bảo mật mới nhất.
- ***Giảm thiểu các cuộc tấn công khi chúng xảy ra*** : Nhanh chóng xác định vi phạm, ngăn chặn thiệt hại và khôi phục mọi dữ liệu bị xâm phạm để giảm thiểu thời gian ngừng hoạt động và ngăn ngừa tổn thất thêm.

- ***Đảm bảo tính bảo mật, toàn vẹn và sẵn có của dữ liệu*** : Bảo vệ tính bí mật và tính chính xác của thông tin đồng thời đảm bảo rằng thông tin đó luôn sẵn có cho người dùng được ủy quyền.

- Các chuyên gia an ninh mạng phải cảnh giác và thích ứng, cập nhật thông tin về các xu hướng an ninh mạng mới và phát triển các chiến lược để giải quyết chúng. Sự nghiệp trong lĩnh vực an ninh mạng không chỉ đòi hỏi kỹ năng kỹ thuật mà còn phải có cam kết liên tục học hỏi và thích nghi trong điều kiện các rủi ro liên tục thay đổi.

3. Mục tiêu của an ninh mạng (Mô hình CIA):

- An ninh mạng hướng tới đảm bảo ba mục tiêu cơ bản sau:

3.1. Tính bảo mật (Confidentiality)

- Đảm bảo thông tin chỉ được truy cập bởi những người có thẩm quyền .
- Ví dụ : sử dụng mật khẩu , mã hóa dữ liệu .

3.2. Tính toàn vẹn (Integrity)

- Đảm bảo dữ liệu không bị thay đổi, chỉnh sửa trái phép trong quá trình lưu trữ và truyền tải.

- Ví dụ: chữ ký số, mã kiểm tra hash.

3.3 .Tính sẵn sàng (Availability)

- Đảm bảo hệ thống và dữ liệu luôn sẵn sàng cho người dùng hợp pháp khi cần. Ví dụ: sao lưu dữ liệu, chống tấn công DDoS.

4. Các lĩnh vực trong ngành An ninh mạng

- An ninh mạng là một thế giới rộng lớn với nhiều vai trò chuyên biệt, phục vụ cho các khía cạnh khác nhau. Việc chọn một lĩnh vực cụ thể có thể giúp các chuyên gia tập trung kỹ năng, và trở thành những chuyên gia uy tín trong ngành.

4.1. Lĩnh vực kiểm thử xâm nhập (Penetration Testing)

- Kiểm thử xâm nhập bao gồm việc mô phỏng các cuộc tấn công mạng để xác định và khai thác các lỗ hổng trong hệ thống, mạng hoặc ứng dụng web. Cách tiếp cận chủ động này rất quan trọng đối với các tổ chức vì nó giúp tăng cường khả năng phòng thủ của họ trước các cuộc tấn công thực tế.

- Lĩnh vực này rất quan trọng vì nó cho phép các tổ chức xác định các điểm yếu về bảo mật trước khi chúng có thể bị các tác nhân độc hại khai thác, từ đó ngăn ngừa các vi phạm dữ liệu và tổn thất tài chính tiềm ẩn.

- Những người kiểm thử xâm nhập cần có kỹ năng vững chắc bao gồm kiến thức về mạng, lập trình và các giao thức bảo mật. Các công cụ phổ biến được sử dụng trong thử nghiệm

thâm nhập bao gồm Metasploit, Burp Suite và OWASP ZAP. Kỹ năng giải quyết vấn đề và khả năng sáng tạo cũng rất cần thiết để suy nghĩ như một hacker và lường trước các lỗi bảo mật.

4.2. Điều tra số (Digital Forensics)

- Điều tra số liên quan đến việc khôi phục và điều tra tài liệu được tìm thấy trong các thiết bị kỹ thuật số, thường liên quan đến tội phạm máy tính. Các chuyên gia trong lĩnh vực này làm việc để theo dõi các vụ hack, khôi phục dữ liệu bị mất hoặc bị mã hóa và đóng góp vào các thủ tục pháp lý.
- Điều tra rất quan trọng để giải quyết tội phạm mạng và các vấn đề pháp lý khác liên quan đến bằng chứng kỹ thuật số. Các chuyên gia giúp duy trì tính toàn vẹn của dữ liệu và hỗ trợ thực thi công lý một cách suôn sẻ.
- Các chuyên gia điều tra số đòi hỏi sự kết hợp giữa kỹ năng phân tích và năng lực kỹ thuật, bao gồm sự hiểu biết thấu đáo về hệ thống tệp, hệ điều hành và lập trình. Chú ý đến chi tiết và cách tiếp cận có phương pháp để thu thập và phân tích dữ liệu là rất quan trọng.

4.3. Quản lý bảo mật thông tin (Information Security Management)

- Lĩnh vực này tập trung vào việc thiết lập và duy trì một bộ chính sách và thủ tục nhằm bảo vệ tài sản thông tin của tổ chức. Nó đảm bảo rằng dữ liệu vẫn được an toàn và không bị rò rỉ trái phép.
- Quản lý bảo mật thông tin hiệu quả là điều cần thiết để bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn có của dữ liệu công ty. Nó giúp các tổ chức tuân thủ các yêu cầu pháp lý và bảo vệ họ khỏi những tổn hại về tài chính và danh tiếng.
- Các chuyên gia trong lĩnh vực này cần có khả năng lãnh đạo và lập kế hoạch chiến lược, cùng với khả năng nắm bắt tốt các nguyên tắc cơ bản về an ninh mạng để thiết kế và thực thi các giao thức bảo mật.

4.4. Phân tích bảo mật (Security Analysis)

- Các nhà phân tích bảo mật đóng một vai trò quan trọng trong việc bảo vệ hệ thống và mạng máy tính của tổ chức. Họ giám sát, phân tích và giảm thiểu các mối đe dọa để duy trì tính toàn vẹn và bảo mật dữ liệu.

- Vai trò này rất quan trọng vì các nhà phân tích cung cấp tuyến phòng thủ đầu tiên chống lại các cuộc tấn công mạng thông qua việc thường xuyên cảnh giác và giám sát mối đe dọa.

Các nhà phân tích bảo mật phải có khả năng ứng phó sự cố mạnh mẽ, thành thạo về an ninh mạng và kỹ năng phân tích mạnh mẽ. Họ thường sử dụng các công cụ như phần mềm SIEM, hệ thống phát hiện xâm nhập và cấu hình tường lửa để phát hiện và ứng phó với các mối đe dọa tiềm ẩn.

5. Các biện pháp bảo mật

5.1. Biện pháp kỹ thuật

- Tường lửa (Firewall)
- Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)
- Mã hóa dữ liệu
- Xác thực đa yếu tố (MFA)
- Phần mềm diệt virus

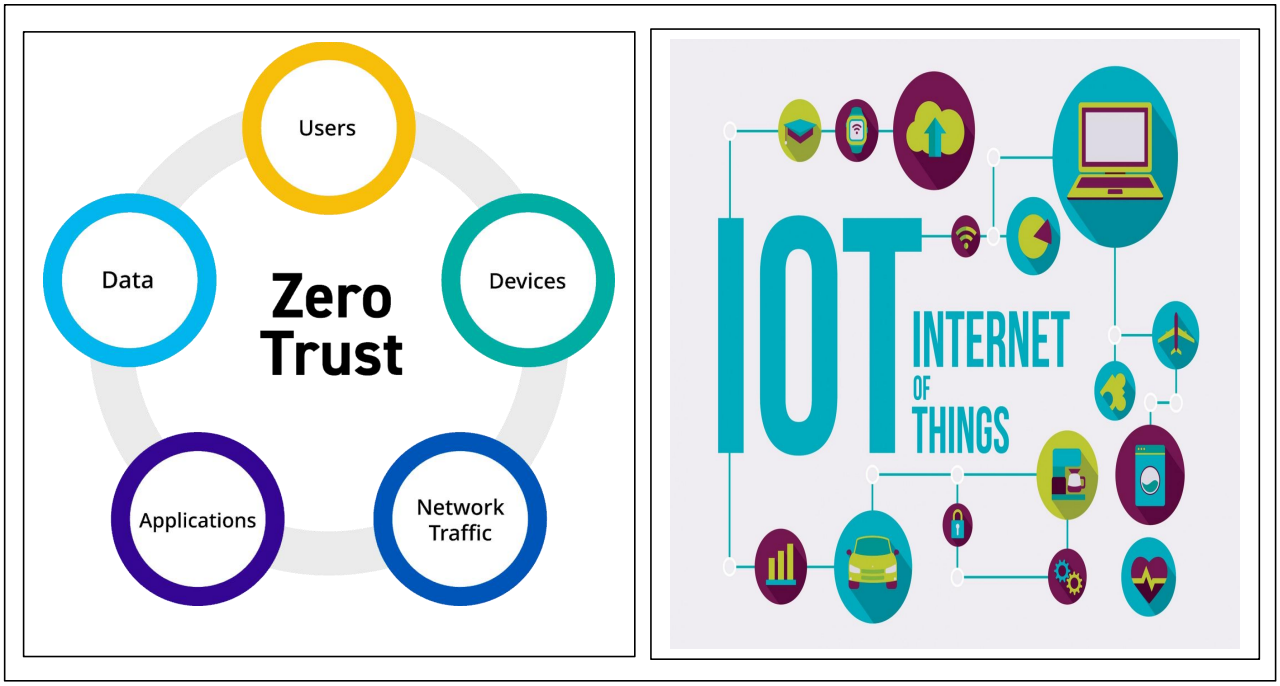
5.2. Biện pháp quản lý

- Xây dựng chính sách bảo mật
- Phân quyền truy cập người dùng

- Đào tạo nhận thức an ninh mạng

6. Xu hướng an ninh mạng hiện nay

- Mô hình Zero Trust
- Bảo mật điện toán đám mây
- Ứng dụng trí tuệ nhân tạo trong an ninh mạng
- Bảo mật Internet of Things (IoT)



II. Lý thuyết về Email Scam

1. *Email scam là gì?*

- ***Email scam là Email scam*** (hay còn gọi là lừa đảo qua ***Email*** hoặc ***Phishing Email***) là hình thức tội phạm mạng giả mạo email từ các tổ chức hợp pháp (ngân hàng, chính phủ, công ty) để lừa người nhận tiết lộ thông tin cá nhân nhạy cảm (mật khẩu, số thẻ tín dụng) hoặc click vào các liên kết/tệp đính kèm độc hại, nhằm mục đích đánh cắp tiền, thông tin hoặc xâm nhập hệ thống. Kẻ lừa đảo dùng chiêu trò tạo cảm giác khẩn cấp, mạo danh có thẩm quyền, và sao chép giao diện email thật để khiến người dùng tin tưởng. Cung cấp thông tin cá nhân (mật khẩu, OTP, số thẻ ngân hàng)

- Click vào liên kết độc hại

- Tải file chứa mã độc

- Chuyển tiền cho kẻ lừa đảo

2. *Mục đích của email scam*

- Đánh cắp thông tin cá nhân
- Chiếm đoạt tài sản
- Phát tán mã độc
- Xâm nhập hệ thống, đánh cắp dữ liệu tổ chức

3. *Các hình thức Email scam phổ biến*

3.1. Phishing Email

- Phishing liên quan đến tội phạm mạng giả dạng các tổ chức hợp pháp thông qua email hoặc nền tảng nhắn tin để dụ các cá nhân cung cấp dữ liệu nhạy cảm như mật khẩu, số thẻ tín dụng, số an sinh xã hội. Những cuộc tấn công này dựa vào các kỹ thuật lừa đảo đánh lừa người dùng mắc lỗi bảo mật hoặc tự nguyện cung cấp thông tin.

Phishing Email (email lừa đảo) là hình thức tấn công mạng qua email, trong đó hacker giả mạo tổ chức hoặc doanh nghiệp uy tín nhằm lừa người dùng cung cấp thông tin cá nhân hoặc truy cập vào các liên kết độc hại. Hậu quả là hệ thống mạng doanh nghiệp có thể bị xâm nhập, dẫn đến rủi ro về bảo mật và thiệt hại tài chính lớn.

- ***Giả mạo ngân hàng, mạng xã hội, sàn thương mại điện tử***
- ***Yêu cầu đăng nhập, xác minh tài khoản***

3.2. Spoofing Email

- Giả mạo địa chỉ người gửi
- Làm người nhận tưởng email đến từ nguồn đáng tin cậy

3.3. Malware Email

- Đính kèm file chứa virus, trojan, ransomware
- Khi mở file → máy bị nhiễm mã độc

3.4. Business Email Compromise (BEC)

- Giả mạo email sếp, kế toán
- Yêu cầu chuyển tiền gấp

3.5. Lottery / Prize scam

- Thông báo trúng thưởng giả
- Yêu cầu đóng phí để nhận thưởng

3.6. Hacking

- Hacking đề cập đến sự xâm nhập trái phép vào hệ thống hoặc mạng máy tính bởi các cá nhân hoặc nhóm muốn tìm cách khai thác các lỗ hổng hệ thống để thu lợi tài chính, thu thập thông tin hoặc làm gián đoạn các dịch vụ. Việc hack có thể được thực hiện thông qua nhiều chiến thuật khác nhau, bao gồm khai thác lỗ hổng phần mềm, bỏ qua mật khẩu hoặc sử dụng các mối đe dọa liên tục nâng cao ***(Advanced Persistent Threats – APTs).***

4. Dấu hiệu nhận biết Email Scam

- Địa chỉ email lạ hoặc gần giống email thật
- Nội dung tạo cảm giác khẩn cấp, đe dọa
- Lỗi chính tả, ngữ pháp
- Link dẫn đến website giả mạo
- File đính kèm không rõ nguồn gốc

5. Hậu quả của Email Scam

- Mất tiền
- Lộ thông tin cá nhân
- Nhiễm mã độc, mất dữ liệu
- Gây thiệt hại cho tổ chức, doanh nghiệp

6. Biện pháp phòng chống

6.1. Đối với cá nhân

- Không click link lạ
- Không cung cấp thông tin cá nhân qua Email
- Kiểm tra kỹ người gửi
- Bật xác thực 2 yếu tố (2FA)

6.2. Đối với tổ chức

- Sử dụng bộ lọc spam
- Áp dụng SPF, DKIM, DMARC
- Đào tạo nhận thức an ninh mạng cho nhân viên

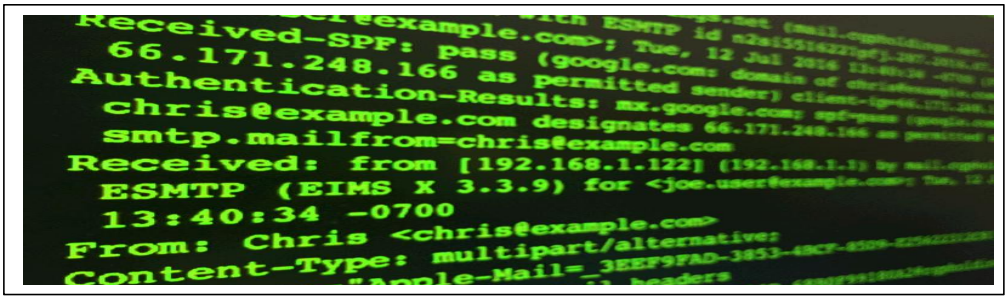
7. Email Scam và pháp luật

- Email scam là hành vi vi phạm pháp luật
- Có thể bị xử phạt hành chính hoặc truy cứu trách nhiệm hình sự
- Liên quan đến các tội danh lừa đảo chiếm đoạt tài sản, xâm nhập trái phép hệ thống thông tin

III. Received – From (Email Header)

1. Khái niệm

- **Received-From** là các dòng thông tin được thêm vào phần header của email mỗi khi email đi qua một mail server. Mỗi máy chủ trung gian đều ghi lại thông tin về nguồn gửi, địa chỉ IP, tên máy chủ và thời gian xử lý email.
- Các dòng Received-From được xếp theo thứ tự ngược, trong đó dòng dưới cùng thể hiện máy chủ gửi ban đầu.



2. *Vai trò trong an ninh mạng*

- Truy vết đường đi của email
- Phát hiện email giả mạo
- Phân tích nguồn tấn công trong các sự cố an ninh

3. *Ví dụ minh họa*

- Received: from mail.example.com (192.168.1.1)
- Dòng trên cho biết email được gửi từ máy chủ mail.example.com với địa chỉ IP tương ứng.

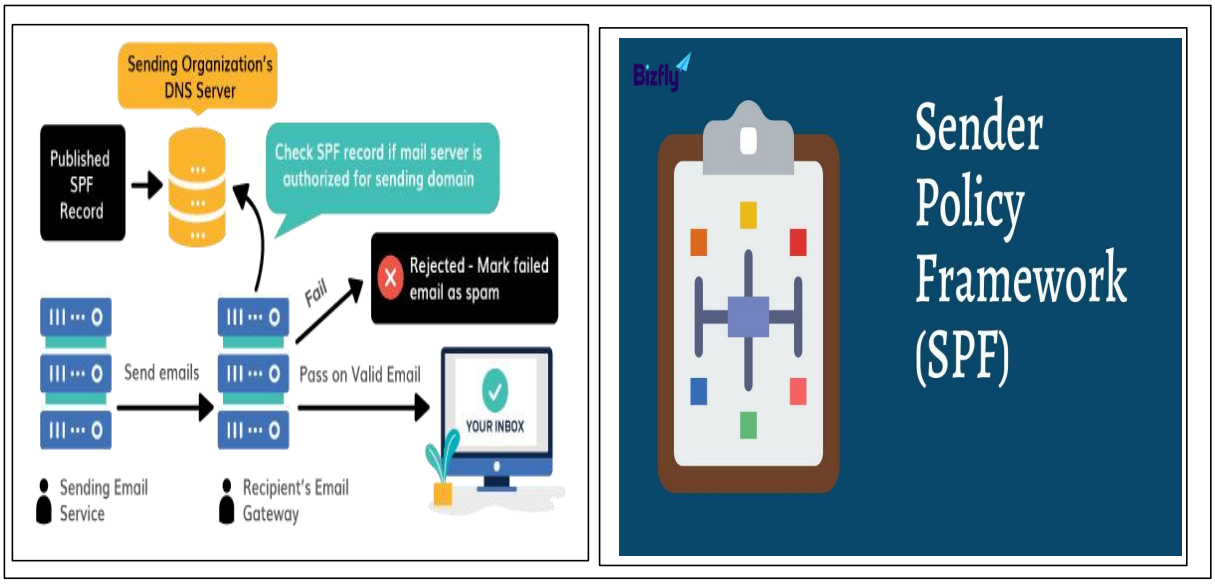
4. *Hỏi – đáp*

- Hỏi: Received-From có ngăn chặn được email giả mạo không?
- Đáp: Không trực tiếp ngăn chặn, nhưng giúp phân tích và phát hiện dấu hiệu bất thường.

IV. *SPF (SENDER POLICY FRAMEWORK)*

1. *Khái niệm*

- SPF là một cơ chế xác thực email dựa trên DNS, cho phép chủ sở hữu domain chỉ định những máy chủ nào được phép gửi email thay mặt cho domain đó.
- Khi một email được gửi đi, mail server nhận sẽ kiểm tra địa chỉ IP của máy gửi với bản ghi SPF trong DNS.



2. Cơ chế hoạt động

- Domain công bố bản ghi SPF trong DNS
- Server nhận kiểm tra IP gửi
- So khớp IP với danh sách cho phép

3. Ví dụ bản ghi SPF

- v=spf1 ip4:192.168.1.0/24 -all

4. Hỏi – đáp

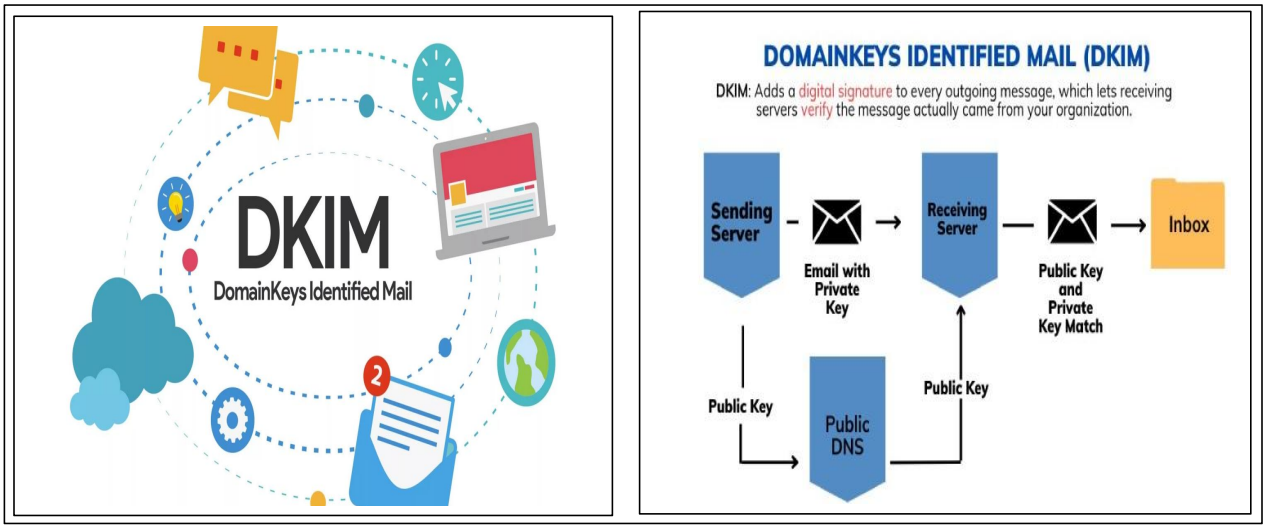
- Hỏi: SPF kiểm tra điều gì?
- Đáp: SPF kiểm tra địa chỉ IP của máy gửi email.
- Hỏi: SPF có bảo vệ nội dung email không?
- Đáp: Không, SPF chỉ xác thực nguồn gửi.

V. DKIM (DOMAINKEYS IDENTIFIED MAIL)

1. Khái niệm

- ***DKIM*** là cơ chế xác thực email sử dụng chữ ký số để đảm bảo rằng nội dung email không bị thay đổi trong quá trình truyền.

- Email được ký bằng khóa riêng (private key) của domain gửi, và máy chủ nhận sẽ xác minh chữ ký bằng khóa công khai (public key) lưu trong DNS.



2. Lợi ích

- Bảo vệ tính toàn vẹn nội dung
- Tăng độ tin cậy email

- Giảm nguy cơ giả mạo

3. Ví dụ

- DKIM-Signature: v=1; a=rsa-sha256; d=example.com;

4. Hỏi – đáp

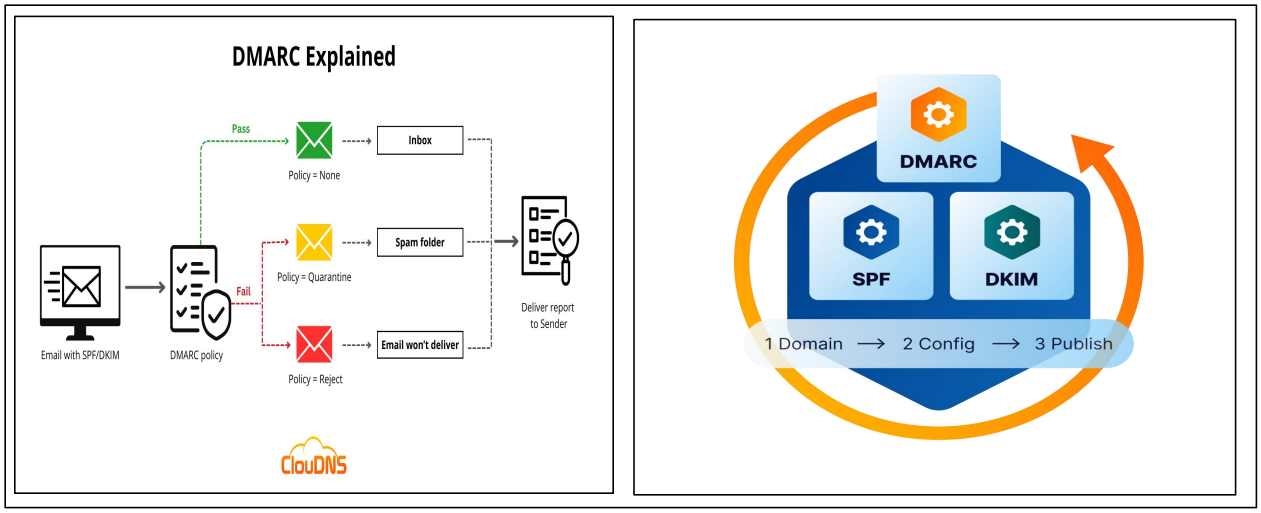
- Hỏi : DKIM bảo vệ điều gì?
- Đáp : DKIM bảo vệ nội dung email không bị chỉnh sửa.

VI. DMARC

1. Khái niệm

- DMARC là cơ chế kết hợp SPF và DKIM, cho phép domain đưa ra chính sách xử lý email không đạt xác thực như: từ chối, cách ly hoặc cho phép.

- Ngoài ra, DMARC còn cung cấp báo cáo chi tiết cho quản trị viên.



2. Chính sách DMARC

- none: chỉ giám sát
- quarantine: đưa vào spam
- reject: từ chối email

3. Ví dụ bản ghi DMARC :

- v=DMARC1; p=reject; rua=mailto:admin@example.com

4. Hỏi – đáp

- Hỏi: DMARC có bắt buộc không?
- Đáp: Không bắt buộc nhưng rất khuyến nghị sử dụng.

VII. So sánh các cơ chế

Cơ chế	Xác thực nguồn	Bảo vệ nội dung
Received - From	Có	Không
SPF	Có	Không
DKIM	Có	Có
DMARC	Có	Có

VIII. Phân tích tiêu đề Email lừa đảo

**** Bài tập nhỏ : Email dưới có phải là một email scam không ? Hãy phân tích Received-from, SPF,DKIM ?***

- Đường dẫn trở lại: 0101019a6e25344-863a0ee4-797e-498c-8dfb-1a9cfad6abce-000000@mail.phishyexample.com
- Từ: sender@trustedbank.com
- ĐẾN: victim@example.com
- Chủ đề: Khẩn cấp: Thông báo tạm ngưng tài khoản
- Ngày: Tue, 11 Nov 2025 09:00:00 +0000
- Mã tin nhắn:<unique-message-id@mail.phishyexample.com>
- Kết quả xác thực: spf=fail (sender IP is 192.0.2.123) smtp.mailfrom=trustedbank.com; dkim=none (no signature) header.d=trustedbank.com; dmarc=fail action=reject header.from=trustedbank.com

****GIẢI :***

1: Recceived- From

- Tên miền Return -Path :mail.phishyexample.com

- Tên miền from :trustedbank.com

-> 2 tên miền khác nhau -> email đáng ngờ

2: SPF

- SPF : Là cơ chế xác minh IP gửi email có được phép gửi thay mặt cho tên miền hay không

- Kết quả của SPF :

+ pass -> IP hợp lệ

+ Fail -> Ip không được phép -> nghi ngờ giả mạo

**** xét ở ví dụ trên ta thấy : spf=fail (sender IP is 192.0.2.123)***

-Địa chỉ IP bị thiếu trong bản ghi SPF (Fail) -> email trên đáng ngờ

<u>3 : DKIM</u>

- DKIM hoạt động như thế nào ?

+ Server gửi email dùng private key để ký

+ Server nhận email lấy public key trong DNS

+ So sánh chữ ký :

- Khớp -> email hợp lệ
- Khong có / sai -> email đáng ngờ.

**** xét ở ví dụ trên ta thấy : dkim=none (no signature) Không có chữ ký DKIM -***

=> Tổng kết :

- Miền From và Return-Path không khớp nhau

-- Xác thực SPF thất bại (fail) vì địa chỉ IP đó không được phép gửi email cho tên miền đó.

- Thiếu DKIM và DMARC bị lỗi, báo hiệu email này nên bị từ chối.

-Thiếu chữ ký DKIM

-Kết quả DMARC không thành công

-Dấu thời gian không theo trình tự

=> Email trên là email scam

IX. Nhận diện các dấu hiệu lừa đảo (indicators of compromise)

1. Tổng quan về nhận diện Phishing

- Việc nhận diện Email Phishing (Tấn công lừa đảo qua thư điện tử) là một quy trình phức tạp, đòi hỏi sự kết hợp giữa các giải pháp kỹ thuật tự động và nhận thức an toàn thông tin của người dùng cuối (End-user Awareness). Kẻ tấn công thường sử dụng kỹ thuật "Social Engineering" (Tấn công phi kỹ thuật) để thao túng tâm lý nạn nhân, khai thác các điểm yếu về sự sợ hãi, lòng tham hoặc sự thiếu hiểu biết về công nghệ.

- Để phân tích một email có phải là lừa đảo hay không, chúng ta cần xem xét toàn diện trên ba khía cạnh chính: Dấu hiệu định danh (Identity), Dấu hiệu nội dung (Content) và Dấu hiệu kỹ thuật (Technical Indicators).

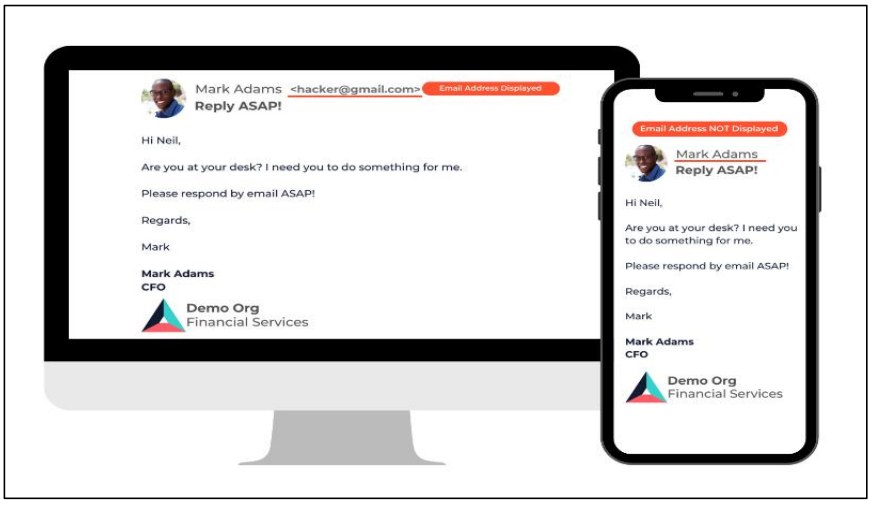
2. Phân tích các dấu hiệu bất thường từ định danh (sender identity)

- Đây là lớp phòng thủ đầu tiên và cũng là thành phần bị giả mạo thường xuyên nhất trong các chiến dịch Phishing.

2.1. Sự không đồng nhất giữa "Tên hiển thị" và "Địa chỉ Email"

- Kẻ tấn công thường thay đổi trường "Display Name" (Tên hiển thị) để tạo lòng tin giả tạo.

- **Cơ chế:** Hacker đặt tên hiển thị là các tổ chức uy tín (ví dụ: "Apple Support", "Giám đốc Nguyễn Văn A", "Bộ phận IT").
- **Dấu hiệu nhận biết:** Khi kiểm tra kỹ địa chỉ email thực tế gửi đến (Sender Address), ta thấy sự mâu thuẫn. Ví dụ: Tên hiển thị là "Ngân hàng Techcombank" nhưng địa chỉ gửi lại là support-team@gmail.com hoặc techcombank-security@hotmail.com.
- **Nguyên tắc bảo mật:** Các tổ chức lớn và chuyên nghiệp không bao giờ sử dụng các tên miền công cộng (public domain) như @gmail.com, @yahoo.com, @outlook.com cho các giao dịch chính thức.



2.2. Kỹ thuật giả mạo tên miền (Typosquatting / Cousin Domains)

- Đây là kỹ thuật tinh vi nhằm đánh lừa thị giác của người dùng.

- **Cơ chế:** Hacker đăng ký các tên miền có hình thức *nhìn thoáng qua* rất giống tên miền thật của tổ chức mục tiêu.
- **Các biến thể phổ biến:**
    - **Lỗi chính tả cố ý:** Thay vì amazon.com, hacker sử dụng amazom.com hoặc arnazon.com (chữ 'r' và 'n' dính nhau nhìn giống chữ 'm').
    - **Thay đổi phần mở rộng (TLD):** Sử dụng các đuôi tên miền rẻ tiền hoặc ít phổ biến. Ví dụ: support@facebook-security.top thay vì security@facebook.com.
    - **Thêm từ khóa phụ:** Sử dụng dấu gạch nối để thêm các từ khóa tạo uy tín như apple-id-verify.com hoặc google-login-alert.net.

2.3. Dấu hiệu từ danh sách người nhận (To/Cc fields)

- Email được gửi đến một danh sách rất dài các địa chỉ không liên quan hoặc để ở chế độ "Undisclosed-recipients" (Người nhận bị ẩn danh).
- Email thông báo các vấn đề cá nhân (như trúng thưởng, vi phạm tài khoản) nhưng lại gửi chung (CC) cho rất nhiều người trong cùng một tổ chức, cho thấy đây là một chiến dịch spam hàng loạt (Mass Spamming) chứ không phải email mục tiêu.

3.Phân tích dấu hiệu từ nội dung và văn phong (content & linguistics)

- Nội dung email là nơi chứa "bẫy" tâm lý (The Hook) nhằm thúc đẩy nạn nhân thực hiện hành động.

3.1. Lời chào chung chung (Generic Greetings)

- **Dấu hiệu:** Email bắt đầu bằng các cụm từ thiếu cụ thể như "Dear Customer", "Dear User", "Chào quý khách", "Chào bạn" thay vì đích danh tên thật của người nhận.
- **Lý do:** Do kẻ tấn công gửi email tới hàng triệu địa chỉ cùng lúc, chúng không có cơ sở dữ liệu để cá nhân hóa tên của từng nạn nhân. Các tổ chức uy tín thường sẽ chào đích danh (Ví dụ: "Chào ông Nguyễn Văn A").

3.2. Sai sót về Ngữ pháp và Chính tả (Grammar and Spelling Errors)

- **Dấu hiệu:** Câu cú lủng củng, sai cấu trúc ngữ pháp, sử dụng từ vựng không tự nhiên (dấu hiệu của việc dùng công cụ dịch tự động), lỗi chính tả cơ bản.
- **Phân tích chuyên sâu:** Đôi khi, hacker cố tình để sai sót chính tả nhằm mục đích lọc nạn nhân ("Self-selection"). Những người dùng tinh ý sẽ nhận ra lỗi sai và bỏ qua, hacker muốn tập trung vào nhóm người dùng "dễ dãi", ít kiến thức công nghệ để tăng tỷ lệ chuyển đổi thành công cho các bước lừa đảo tiếp theo. Ngoài ra, việc viết sai chính tả (ví dụ: "B.a.n.k" thay vì "Bank") còn giúp vượt qua các bộ lọc từ khóa của hệ thống chống Spam.

3.3. Tạo áp lực tâm lý khẩn cấp (Urgency) hoặc Sợ hãi (Fear)

- **Dấu hiệu:** Các cụm từ mang tính đe dọa hoặc thúc giục mạnh mẽ, yêu cầu hành động ngay lập tức.
    - "Tài khoản của bạn sẽ bị khóa vĩnh viễn trong 24 giờ tới nếu không xác minh."
    - "Phát hiện giao dịch lạ, bấm vào đây để hủy ngay."
    - "Hóa đơn quá hạn, thanh toán ngay để tránh các thủ tục pháp lý."

- **Cơ chế tâm lý:** Khi não bộ con người rơi vào trạng thái hoảng loạn hoặc gấp gáp (System 1 thinking), khả năng tư duy phản biện (System 2 thinking) bị suy giảm. Hacker lợi dụng điều này để khiến nạn nhân click chuột theo phản xạ mà không kịp kiểm chứng thông tin.

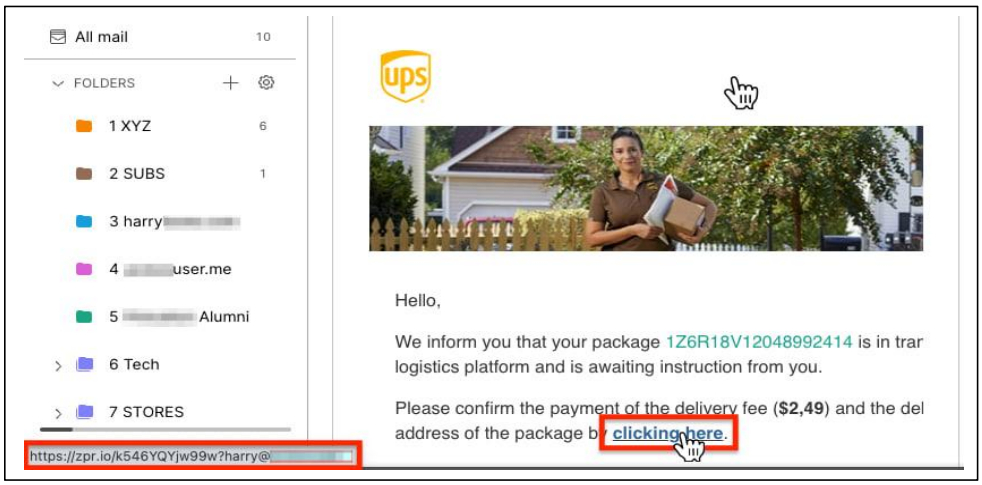
3.4. Lợi ích phi thực tế (Too Good To Be True)

- **Dấu hiệu:** Thông báo trúng thưởng iPhone, xe máy, trúng xổ số nước ngoài, hoặc nhận thừa kế tài sản khổng lồ từ những người không quen biết.
- **Nguyên tắc:** Nếu một đề nghị có vẻ quá tốt để là sự thật, thì khả năng cao đó là lừa đảo.

4. Phân tích kỹ thuật: đường dẫn và nút bấm (hyperlinks & cta)

4.1. Sự sai lệch giữa Văn bản hiển thị và Liên kết thực (Mismatch URLs)

- **Phương pháp kiểm tra:** Rê chuột (Hover) – tuyệt đối không click – vào đường link hoặc nút bấm trong email.
- **Dấu hiệu:** Văn bản hiển thị ghi là www.paypal.com/login nhưng đường dẫn thực tế (hiển thị ở góc dưới trình duyệt hoặc tooltip) lại trỏ về www.shady-website.com/login-stealer.php. Đây là dấu hiệu kỹ thuật rõ ràng nhất của tấn công Phishing.



4.2. Sử dụng dịch vụ rút gọn link (URL Shorteners)

- **Dấu hiệu:** Link đích có dạng bit.ly/xyz, tinyurl.com/abc, goo.gl/....

- **Mục đích:** Che giấu điểm đến thực sự của đường link, tránh bị người dùng phát hiện tên miền giả mạo ngay lập tức. Các tổ chức tài chính/ngân hàng hiếm khi sử dụng link rút gọn trong các email giao dịch quan trọng.

4.3. Kỹ thuật tấn công Homograph (Homograph Attacks)

- **Lý thuyết:** Hacker sử dụng các ký tự từ bảng chữ cái khác (ví dụ: Cyrillic - tiếng Nga) có hình dáng y hệt bảng chữ cái Latin để đăng ký tên miền.
- **Ví dụ:** Chữ "a" trong tiếng Cyrillic (U+0430) nhìn y hệt chữ "a" trong tiếng Anh (U+0061) nhưng máy tính hiểu là 2 ký tự khác nhau, dẫn đến 2 website hoàn toàn khác nhau.

5. Phân tích dấu hiệu từ tệp đính kèm (attachments)

5.1. Các định dạng tệp nguy hiểm

- **Dấu hiệu:** Email yêu cầu mở các file có đuôi thực thi hoặc script: .exe, .scr, .bat, .com, .cmd, .js, .vbs.
- **Lưu ý:** Hacker thường nén các file này trong định dạng .zip hoặc .rar và đặt mật khẩu để mã hóa nội dung, nhằm tránh sự quét tự động của các phần mềm diệt virus trên Mail Server.

5.2. Giả mạo phần mở rộng (Double Extension Tricks)

- **Cơ chế:** Lợi dụng tính năng mặc định ẩn phần mở rộng của Windows.
- **Ví dụ:** Tên file là invoice_document.pdf.exe. Người dùng chỉ nhìn thấy invoice_document.pdf (kèm icon PDF giả) và nghĩ đó là tài liệu an toàn, nhưng thực chất là file chạy mã độc.

5.3. File văn phòng chứa Macro độc hại (Malicious Macros)

- **Dấu hiệu:** File Word (.doc, .docm) hoặc Excel (.xls, .xlsm) khi mở ra chỉ hiện một nội dung mờ nhạt và yêu cầu người dùng bấm "Enable Content" hoặc "Enable Editing" để xem chi tiết.
- **Hậu quả:** Hành động này sẽ cấp quyền cho đoạn mã Visual Basic (VBA) độc hại chạy ngầm trên máy tính để tải và cài đặt mã độc (Malware/Ransomware).

6. Yêu cầu thông tin nhạy cảm bất thường

- **Dấu hiệu:** Email yêu cầu người dùng trả lời hoặc điền vào biểu mẫu (form) các thông tin:
    - Mật khẩu đăng nhập.
    - Mã xác thực OTP (One-Time Password).
    - Thông tin thẻ tín dụng (số thẻ, ngày hết hạn, mã CVV).
    - Số định danh cá nhân (CCCD/CMND/SSN).
- **Nguyên tắc vàng:** Các tổ chức hợp pháp (Ngân hàng, Cơ quan Chính phủ, Google, Facebook) **KHÔNG BAO GIỜ** yêu cầu người dùng cung cấp mật khẩu hoặc mã OTP thông qua email, tin nhắn hay điện thoại.

X. Đề xuất cách phòng tránh Email Phishing

- ***Email phishing*** là một trong những hình thức tấn công mạng phổ biến và nguy hiểm hiện nay. Do đó, việc trang bị kiến thức và áp dụng các biện pháp phòng tránh là vô cùng cần thiết nhằm giảm thiểu rủi ro mất mát thông tin và tài sản. Dưới đây là một số biện pháp phòng tránh Email phishing hiệu quả, được tổng hợp từ các khuyến nghị của chuyên gia an ninh mạng và thực tiễn sử dụng.

1. Luôn cảnh giác và kiểm tra kỹ trước khi hành động:

1. **Lý do:** Phishing khai thác sự vội vã, nên dừng lại 5 giây để nghĩ: "Đây có phải thật không?"

2. **Mẹo:** Nếu email từ ngân hàng, đừng click link – hãy mở app ngân hàng hoặc gõ tay URL chính thức (ví dụ: https://ibanking.vietcombank.com.vn). Kiểm tra bằng cách gọi hotline chính thức để xác nhận.
3. **Ví dụ:** Mình từng nhận email "cập nhật tài khoản Google", nhưng kiểm tra thấy URL dẫn đến site lạ – xóa ngay!

2. Không cung cấp thông tin nhạy cảm qua email:

1. **Lý do:** Email không an toàn, dễ bị hack. Thông tin như mật khẩu có thể bị dùng để trộm tiền.
2. **Mẹo:** Sử dụng trình quản lý mật khẩu (như LastPass miễn phí) để tạo mật khẩu mạnh, và không bao giờ chia sẻ OTP (One-Time Password) – OTP chỉ dùng trên app chính thức.
3. **Ví dụ:** Nếu email yêu cầu "nhập mã OTP để xác minh", đó là lừa – vì OTP chỉ gửi qua SMS/app, không qua email.

3. Sử dụng phần mềm bảo mật và chống phishing:

1. **Lý do:** Phần mềm phát hiện tự động, chặn email xấu trước khi đến hộp thư.
2. **Mẹo:** Cài antivirus như Avast (miễn phí) hoặc Bitdefender (trả phí), bật tính năng chống phishing. Trong Gmail: Bật "Bộ lọc nâng cao" và "Xác thực 2 lớp". Cập nhật phần mềm định kỳ để vá lỗ hổng.
3. **Ví dụ**: Windows Defender trên máy mình tự động quét email, từng chặn một file đính kèm chứa virus.

4. Kích hoạt xác thực hai yếu tố (2FA/MFA):

1. **Lý do:** Dù lộ mật khẩu, hacker vẫn cần yếu tố thứ hai (như mã SMS hoặc app authenticator) để đăng nhập.
2. **Mẹo:** Bật 2FA cho tất cả tài khoản: Gmail (qua Google Authenticator), ngân hàng (qua app), Facebook. Tránh dùng SMS nếu có thể, vì SIM swap attack có thể đánh cắp SMS.
3. **Ví dụ:** Tài khoản email của mình dùng 2FA, nên dù lỡ click link phishing, hacker không vào được mà không có mã từ điện thoại.

***5.Cập nhật phần mềm và hệ điều hành thường xuyên**:*

1. **Lý do:** Các bản cập nhật vá lỗ hổng mà hacker khai thác qua phishing (như lỗ hổng browser).
2. **Mẹo:** Bật tự động update trên Windows/Android/iOS. Kiểm tra hàng tuần qua Settings > Update.
3. **Ví dụ:** Bản update Chrome mới nhất từng vá lỗi cho phép phishing qua pop-up giả.

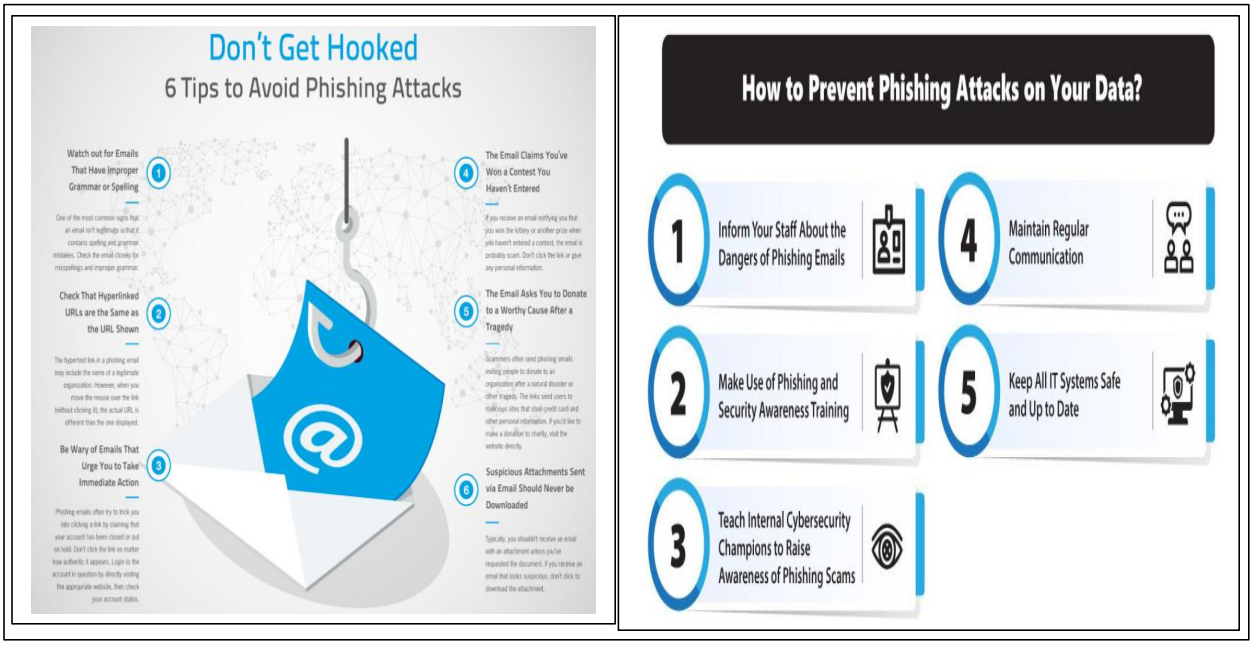
***6.Báo cáo và xử lý email đáng ngờ**:*

1. **Lý do:** Giúp ngăn chặn lan rộng và cảnh báo cộng đồng.
2. **Mẹo:** Trong Gmail/Outlook, click "Report Phishing". Forward email đến abuse@google.com hoặc Cục An toàn Thông tin Việt Nam (ais.gov.vn). Không forward trực tiếp để tránh lây lan.
3. **Ví dụ:** Mình từng báo cáo một email giả mạo Shopee, và họ xác nhận là phishing.

***7.Học hỏi và đào tạo liên tục**:*

1. **Lý do:** Phishing ngày càng tinh vi (như AI-generated email), nên cần cập nhật kiến thức.
2. **Mẹo:** Đọc blog như NCSC.gov.uk hoặc tham gia khóa học miễn phí trên Coursera (Cybersecurity for Beginners). Thực hành qua công cụ giả lập phishing như từ KnowBe4.
3. **Ví dụ:** Trường mình có workshop an ninh mạng, giúp nhận biết spear-phishing (phishing nhắm cá nhân).

- ***Dưới đây là infographic chi tiết về các bước phòng tránh:***



B. PHẦN KẾT LUẬN / NHẬN XÉT / ĐÁNH GIÁ / KIẾN NGHỊ

1. Kết luận

- Qua quá trình nghiên cứu và thực hiện đề tài **"Phân tích Email Phishing"**, nhóm đã tìm hiểu rõ hơn về bản chất, cách thức hoạt động cũng như mức độ nguy hiểm của các cuộc tấn công phishing qua email. Thông qua việc phân tích một email lừa đảo thực tế, đặc biệt là các trường thông tin trong Email Header như **Received**, **SPF** và **DKIM**, đề tài đã chỉ ra những dấu hiệu kỹ thuật quan trọng giúp nhận diện email giả mạo.
- Received-From, SPF, DKIM và DMARC đóng vai trò quan trọng trong việc bảo vệ hệ thống email hiện đại. Khi được triển khai đồng bộ, các cơ chế này giúp giảm thiểu đáng kể các cuộc tấn công phishing, giả mạo email và nâng cao độ an toàn thông tin.
- Bên cạnh đó, đề tài cũng tổng hợp và phân tích các biện pháp phòng tránh Email phishing hiệu quả, góp phần nâng cao nhận thức và kỹ năng tự bảo vệ của người dùng trong môi trường mạng ngày càng phức tạp.
- Tuy nhiên, đề tài vẫn còn hạn chế do phạm vi nghiên cứu chưa mở rộng nhiều loại email phishing khác nhau. Trong thời gian tới, có thể nghiên cứu sâu hơn về các kỹ thuật phishing nâng cao như spear phishing hoặc phishing sử dụng trí tuệ nhân tạo.

3. Nhận xét

- ***Email phishing*** là hình thức tấn công phổ biến, dễ thực hiện nhưng mang lại hậu quả nghiêm trọng. Nhiều email phishing hiện nay được thiết kế ngày càng tinh vi, nội dung giống email thật, khiến người dùng khó phân biệt nếu thiếu kiến thức và sự cảnh giác.

- Qua quá trình phân tích, có thể nhận thấy rằng việc kiểm tra kỹ Email Header và các cơ chế xác thực như SPF và DKIM là phương pháp hiệu quả để phát hiện email lừa đảo, tuy nhiên phương pháp này đòi hỏi người dùng phải có kiến thức cơ bản về an ninh mạng.

4. Đánh giá

- Đề tài đã đạt được mục tiêu đề ra là giúp người học hiểu rõ về Email phishing, cách phân tích email lừa đảo cũng như các biện pháp phòng tránh. Nội dung nghiên cứu bám sát thực tế, kết hợp giữa lý thuyết và thực hành phân tích kỹ thuật.

- Tuy nhiên, do giới hạn về thời gian và phạm vi nghiên cứu, đề tài chỉ tập trung vào phân tích một số trường hợp Email phishing cơ bản, chưa đi sâu vào các hình thức tấn công nâng cao như **spear phishing** hay **phishing sử dụng trí tuệ nhân tạo.**

5. Kiến nghị

- Trong thời gian tới, để nâng cao hiệu quả phòng chống Email phishing, cần chú trọng một số vấn đề sau:

- Tăng cường đào tạo và nâng cao nhận thức về an ninh mạng cho người dùng.
- Khuyến khích các tổ chức triển khai đầy đủ các cơ chế xác thực email như SPF, DKIM và DMARC.
- Người dùng cần chủ động trang bị kiến thức và áp dụng các biện pháp bảo mật như xác thực hai yếu tố và phần mềm bảo mật.
- Mở rộng nghiên cứu về các kỹ thuật phishing nâng cao để phù hợp với xu hướng tấn công mới.

C. TÀI LIỆU THAM KHẢO

[1]. https://ipmac.vn/an-ninh-mang-la-gi-tong-quan-kien-thuc-tu-a-z-ve-an-ninh-mang/

[2]. https://www.vnetwork.vn/news/phishing-email-la-gi/

[3]. https://viettelidc.com.vn/tin-tuc/spoofing-la-gi

[4]. https://www.cloudflare.com/learning/email-security/

[5]. https://support.google.com/mail/answer/180707

[6]. https://mailtrap.io/blog/email-headers/

[7]. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email

[8]. https://dmarc.org/overview/

*[9]. **C**ục An toàn thông tin (AIS). (2022). Cẩm nang nhận diện và phòng chống lừa đảo trực tuyến. Bộ Thông tin và Truyền thông.*

***[10]. H**iệp hội An toàn thông tin Việt Nam (VNISA). (2023). Báo cáo tình hình an toàn thông tin Việt Nam và chỉ số an toàn thông tin mạng.*

***[11]. T**rung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC). Cảnh báo các hình thức giả mạo email doanh nghiệp (BEC).*

***[12]. A**nti-Phishing Working Group (APWG). (2024). Phishing Activity Trends Report, 1st Quarter 2024.*

***[13]. D**hamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.*

[14]. F*ederal Trade Commission (FTC). How to Recognize and Avoid Phishing Scams.*

[15] . M*icrosoft Security. (2024). Global Security Intelligence Report: Phishing Trends and Techniques.*

[16]. N*ational Institute of Standards and Technology (NIST). (2016). NIST Special Publication 800-177: Trustworthy Email.*

[17]. V*erizon. (2023). Data Breach Investigations Report (DBIR). Verizon Enterprise Solutions.*

[18]. https://media.defense.gov/2018/Sep/24/2002043924/2000/2000/0/180924-D-D0441-001.PNG

[19]. https://www.ncsc.gov.uk/static-assets/images/guidance/Phishing-attacks-defending-your-organisation-infographic.png

[20]. https://timely-benefit-e63d540317.media.strapiapp.com/How_to_Prevent_Phishing_Attacks_on_Your_Data_v2_5113fd61d3.jpg

TRƯỜNG ĐẠI HỌC KHOA HỌC **KHOA CÔNG NGHỆ THÔNG TIN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

PHIẾU ĐÁNH GIÁ TIỂU LUẬN
Học kỳ 1 Năm học 2025-2026

Cán bộ chấm thi 1	Cán bộ chấm thi 2
Nhận xét: .... **Điểm đánh giá của CBChT1:** Bằng số: ..... Bằng chữ:	**Nhận xét**: .... **Điểm đánh giá của CBChT2:** Bằng số: ..... Bằng chữ: .....

Điểm kết luận: Bằng số..... Bằng chữ:.....

Thành Phố Huế, ngày …… tháng …… năm 20…

CBChT1	**CBChT2**
(Ký và ghi rõ họ tên)	*(Ký và ghi rõ họ tên)*