Họ tên: _____ Ngày: _____ Điểm: _____

Tấn công phishing và kỹ thuật xã hội

Spear phishing, lừa đảo whaling, các giao thức SPF/DKIM/DMARC, giả mạo người gửi và đào tạo bảo mật cho nhân viên.

TỔNG QUAN BÀI HỌC VỀ TẤN CÔNG PHISHING

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về các cuộc tấn công lừa đảo trực tuyến (phishing) và kỹ thuật tấn công phi kỹ thuật (social engineering). Bạn sẽ khám phá lừa đảo trực tuyến có chủ đích (spear phishing), whaling, giả mạo tên miền, các giao thức SPF/DKIM/DMARC, an toàn liên kết và đào tạo nâng cao nhận thức cho nhân viên.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- ☐ **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- ☐ **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- ☐ **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- ☐ **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- ☐ **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- ☐ **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/tan-cong-lua-dao/

Lộ trình học về giảm thiểu lừa đảo trực tuyến (phishing) của bạn

- Xác định các hình thức lừa đảo phổ biến như phishing, vishing và cửa sổ bật lên hỗ trợ giả.
- Triển khai quy trình xác minh giao dịch ngoài băng tần.
- Cấu hình các quy tắc SPF, DKIM và DMARC để chặn các tên miền giả mạo.

HƯỚNG DẪN VỀ TẤN CÔNG PHISHING

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về việc xác thực email. Kết thúc với hoạt động thưởng Nghĩ nhanh.

TẤN CÔNG PHISHING & KỸ THUẬT XÃ HỘI (GIỚI THIỆU)

Tấn công phishing dùng tin nhắn nhắm mục tiêu, lừa đảo whaling và giả mạo tên miền để thu thập thông tin đăng nhập của người dùng. Bảo vệ hệ thống doanh nghiệp đòi hỏi triển khai các quy tắc SPF, DKIM và DMARC tại cổng cùng các bước phê duyệt ngoài kênh.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1 **1. Spear phishing là gì?**

- A. Email lừa đảo có chủ đích được thiết kế riêng cho một cá nhân hoặc tổ chức cụ thể
- B. Email hàng loạt gửi đến hàng triệu địa chỉ ngẫu nhiên
- C. Một cuộc tấn công mạng làm ngập máy chủ web bằng lưu lượng
- D. Một kỹ thuật trích xuất cơ sở dữ liệu nhắm vào bản ghi người dùng

2 **2. Giao thức nào cho phép một tên miền liệt kê trong DNS các địa chỉ IP gửi thư được ủy quyền của mình để chống giả mạo?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. Tấn công whaling là gì?**

- A. Chiến dịch lừa đảo nhắm riêng vào các giám đốc điều hành doanh nghiệp nổi tiếng
- B. Tấn công SQL injection nhắm vào bản sao lưu cơ sở dữ liệu
- C. Hành vi trộm cắp vật lý thiết bị router mạng cục bộ
- D. Một lần quét vét cạn nhồi thông tin đăng nhập tự động

4 **4. DKIM làm gì?**

- A. Thêm chữ ký mật mã vào email để xác minh tính xác thực của người gửi
- B. Chặn lưu lượng gói tin mạng đến tại tường lửa
- C. Mã hóa các ổ lưu trữ cơ sở dữ liệu khi lưu trữ (at rest)
- D. Quét tệp đính kèm email để tìm phần mềm độc hại dựa trên chữ ký

5 **5. Vai trò của DMARC là gì?**

- A. Chỉ đạo máy chủ email nhận cách xử lý các kiểm tra SPF/DKIM thất bại
- B. Giải mã mật khẩu hệ thống bằng bảng cầu vồng tính sẵn
- C. Nén tệp đính kèm email trước khi gửi
- D. Cấu hình đặc quyền truy cập định tuyến mạng

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Spear phishing dựa vào các email hàng loạt chung chung gửi tới hàng triệu địa chỉ ngẫu nhiên.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Chính sách DMARC có thể chỉ thị máy chủ thư từ chối các thư giả mạo trái phép.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Xác minh SPF hoạt động bằng cách xác thực chữ ký mật mã của nội dung email.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Các cuộc tấn công whaling nhắm vào quản trị viên cấp thấp của doanh nghiệp để truy cập tệp cơ sở dữ liệu.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Xác minh ngoài kênh các yêu cầu thanh toán giúp ngăn chặn các vụ lừa đảo chuyển khoản tài chính.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Nhắm vào một nhân viên cụ thể bằng thông tin cá nhân hóa là kiểu phishing _____ .
2. Làm giả tiêu đề email để thư trông hợp lệ là hành vi _____ người gửi.
3. Danh sách IP máy chủ thư được ủy quyền trong DNS là _____ .
4. Chuẩn chữ ký email cung cấp khả năng xác minh người gửi là _____ .
5. Thiết lập chính sách từ chối các thư không vượt qua kiểm tra SPF/DKIM là dùng _____ .
6. Chiến dịch phishing nhắm vào lãnh đạo cấp cao được gọi là _____ .

NGÂN HÀNG TỪ VỰNG

BẢN GHI SPF | DKIM | DMARC | GIẢ MẠO | SMISHING | SPEAR | VISHING | WHALING

Viết câu trả lời của bạn tại đây:

1.
2.
3.
4.
5.
6.

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

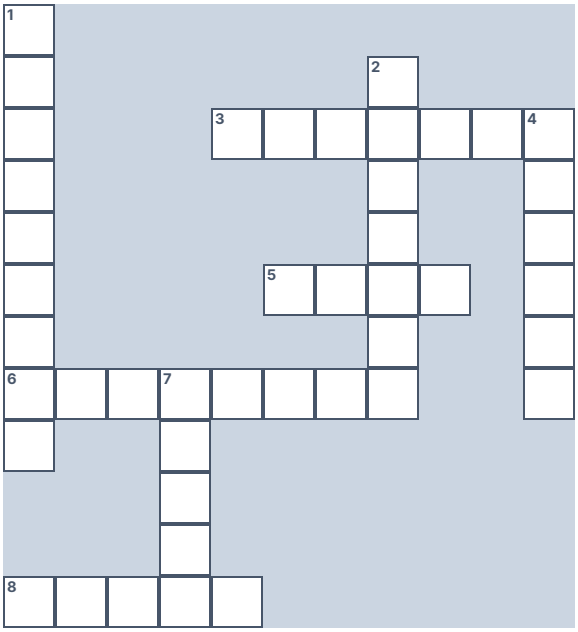
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. SPEAR	A	Các cuộc gọi lừa đảo bằng giọng nói.
☐	2. GIẢ MẠO	B	Nhắm vào các giám đốc cấp cao (C-level).
☐	3. SPF	C	Hướng dẫn từ chối theo chính sách.
☐	4. DKIM	D	Các IP người gửi được DNS ủy quyền.
☐	5. DMARC	E	Email kỹ thuật xã hội.
☐	6. TẤN CÔNG WHALING	F	Email nhắm mục tiêu được cá nhân hóa.
☐	7. PHISHING	G	Giả mạo địa chỉ email người gửi.
☐	8. VISHING	H	Chữ ký mật mã trong email.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

3. Các cuộc gọi lừa đảo bằng giọng nói (7)

5. Chữ ký mật mã trong email (4)

6. Email lừa đảo bằng tác động tâm lý (8)

8. Chính sách hướng dẫn từ chối thư (5)

HÀNG DỌC

1. Các IP người gửi được cấp phép trong DNS (9)

2. Nhắm vào lãnh đạo cấp cao (7)

4. Làm giả địa chỉ email người gửi (6)

7. Email cá nhân hóa nhắm vào mục tiêu cụ thể (5)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

3 hàng ngang: Các cuộc gọi lừa đảo bằng giọng nói (7 chữ cái):

5 hàng ngang: Chữ ký mật mã trong email (4 chữ cái):

6 hàng ngang: Email lừa đảo bằng tác động tâm lý (8 chữ cái):

8 hàng ngang: Chính sách hướng dẫn từ chối thư (5 chữ cái):

HÀNG DỌC

1 hàng dọc: Các IP người gửi được cấp phép trong DNS (9 chữ cái):

2 hàng dọc: Nhắm vào lãnh đạo cấp cao (7 chữ cái):

4 hàng dọc: Làm giả địa chỉ email người gửi (6 chữ cái):

7 hàng dọc: Email cá nhân hóa nhắm vào mục tiêu cụ thể (5 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

B P G Đ N P L Ô V Ơ O Â S Q R

D K R H Ă A Ă Â V O V K I V K

V S A I C Ơ M H C I G M M I Ơ

Ô E E O A M A I G M S M Ơ P Q

S R P E Â B Q Ơ O Ê Q H Â U C

G R S X T A Â P Y C U Đ I I Ê

N Y B M C N Ơ Ư H Ô R Â S N Ă

I A Y N C G K A C I O A C D G

L E G B P H Ơ L D G S Q M Y Q

A Đ Ơ U D I D A A Ơ O H M D Ô

H S V Ơ I S K P S Q B M I X Ă

W Đ Q Ư Ư P I H A P Y X X N K

E G M P I F M L L R O Ê Ơ Ơ G

E Y A O T Đ T Â X P X Ă Ê L Y

E H N Ô N Ư Â L Y X Đ V O U T

DANH SÁCH TỪ VỰNG

SPEAR GIAMAO BANGHISPF DKIM DMARC WHALING PHISHING VISHING

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG
A. SPEAR
B. GIAMAO
C. BANGHISPF
D. DKIM
E. DMARC
F. WHALING
G. PHISHING
H. VISHING

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
____ 1. Làm giả địa chỉ email người gửi.
____ 2. Email cá nhân hóa nhắm vào mục tiêu cụ thể.
____ 3. Các cuộc gọi lừa đảo bằng giọng nói.
____ 4. Các IP người gửi được cấp phép trong DNS.
____ 5. Email lừa đảo bằng tác động tâm lý.
____ 6. Chính sách hướng dẫn từ chối thư.
____ 7. Chữ ký mật mã trong email.
____ 8. Nhắm vào lãnh đạo cấp cao.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. **AESRP** _____

2. **FBPGAISHN** _____

3. **ADCRM** _____

4. **SNGIHPHI** _____

5. **MAOGAI** _____

6. **IMDK** _____

7. **WNIGHLA** _____

8. **IHGVNIS** _____

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những thiết bị có thể bị tấn công			
2	Những dấu hiệu của một email lừa đảo trực tuyến (phishing)			
3	Những dấu hiệu máy tính bị nhiễm			
4	Những từ tạo cảm giác khẩn cấp giả			
5	Những cách kiểm tra người gửi			
6	Những người bạn có thể nhờ giúp về CNTT			
7	Những thứ bạn sao lưu			
8	Những loài cá hoặc sinh vật biển bạn biết			
9	Những công ty mà kẻ lừa đảo giả danh			
10	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
11	Những việc cần làm sau khi nhấp vào liên kết giả			
12	Những việc cần làm sau khi dữ liệu bị rò rỉ			
13	Những kênh nơi phishing diễn ra			
14	Những thứ bạn không bao giờ gửi qua email			
15	Những cách bảo vệ tài khoản của bạn			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: XỬ LÝ VỤ TẤN CÔNG WHALING NHẮM VÀO LÃNH ĐẠO CẤP CAO

👨‍💼

Tình huống: Một Giám đốc Tài chính nhận được một email được cá nhân hóa cao, tự nhận là từ CEO, yêu cầu chuyển nhanh $50,000 để chốt một thương vụ mua tên miền bí mật.

Câu hỏi thảo luận: Hãy phân tích các rủi ro giả mạo thương hiệu, và trình bày chi tiết SPF/DKIM/DMARC cùng các biện pháp kiểm soát xác thực.

NGHIÊN CỨU TÌNH HUỐNG 2: TRIỂN KHAI CHÍNH SÁCH CỔNG SPF/DKIM/DMARC

👨‍💼

Tình huống: Một doanh nghiệp không đạt các cuộc kiểm toán bảo mật vì các email tiếp thị gửi đi thường bị gắn cờ là thư rác, và tin tặc đang chủ động giả mạo tên miền thương hiệu của công ty.

Câu hỏi thảo luận: Hãy thiết lập các biện pháp kiểm soát kỹ thuật và quản trị để xác minh tính xác thực của email.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

20	11	1	24	11	12	9	16	14	26	1	7	1	17	28	1	
11	18	12	21	25	1	13	12	9	15	24	17	1	16	5	18	16	10
24	11	26														

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Phishing là gì?

Phishing là một cuộc tấn công kỹ thuật xã hội trong đó tội phạm gửi tin nhắn lừa đảo để dụ người dùng chia sẻ dữ liệu nhạy cảm.

Q2: Sự khác biệt giữa phishing và spear phishing là gì?

Phishing nhắm vào các nhóm rộng với nội dung chung chung, còn spear phishing nhắm vào nạn nhân cụ thể bằng các chi tiết được tùy chỉnh.

Q3: Whaling là gì?

Whaling là kiểu tấn công lừa đảo trực tuyến (phishing) nhắm mục tiêu cao vào các lãnh đạo cấp cao nắm quyền quản trị.

Q4: Giả mạo email là gì?

Giả mạo email là việc tạo ra các thư email với địa chỉ người gửi bị làm giả để đánh lừa người nhận tin tưởng vào nguồn gửi.

Q5: SPF ngăn giả mạo như thế nào?

Nó công bố danh sách các địa chỉ IP gửi được ủy quyền trong DNS, cho phép máy chủ nhận xác minh nguồn thư. [1]

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: DKIM là gì?

DomainKeys Identified Mail thêm chữ ký mật mã vào tiêu đề email, chứng minh một tên miền đã chịu trách nhiệm và thư không bị thay đổi.

Q7: DMARC là viết tắt của gì?

Xác thực, báo cáo và tuân thủ thư dựa trên tên miền (Domain-based Message Authentication, Reporting, and Conformance). [2]

Q8: Chính sách DMARC là gì?

Chính sách cho máy chủ thư biết cách xử lý các thư không đạt SPF/DKIM (none, quarantine hoặc reject). [2]

Q9: Vishing là gì?

Lừa đảo qua giọng nói (vishing), trong đó kẻ tấn công dùng các cuộc gọi điện thoại gian lận để lấy dữ liệu quản trị hoặc tài chính.

Q10: Công cụ quét liên kết giúp ích như thế nào?

Chúng quét và viết lại các liên kết email đến để xác minh độ an toàn của trang web đích tại thời điểm nhấp.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Tấn công đồng dạng ký tự (homograph) hoạt động như thế nào?

Kẻ tấn công đăng ký tên miền bằng các ký tự Unicode không thuộc ASCII trông giống nhau để mô phỏng tên miền hợp pháp về mặt hình ảnh.

Q2: Biểu diễn punycode là gì?

Phép mã hóa chuyển tên miền Unicode thành chuỗi tương thích ASCII bắt đầu bằng 'xn--' để DNS xử lý được.

Q3: Vì sao 'p=reject' là trạng thái DMARC an toàn nhất?

Nó yêu cầu các máy chủ nhận từ chối thư không đạt DMARC (SPF/DKIM căn chỉnh) trong phiên SMTP, chặn việc giả mạo trực tiếp. [2]

Q4: Kẻ tấn công vượt qua các quy tắc SPF như thế nào?

Bằng cách lợi dụng các tên miền giống hệt (typosquatting) hoặc dùng các tài khoản bị chiếm đoạt trên dịch vụ thư của bên thứ ba hợp pháp.

Q5: Xâm phạm email doanh nghiệp (BEC) là gì?

Trò lừa đảo doanh nghiệp trong đó kẻ tấn công chiếm quyền hoặc mạo danh tài khoản email doanh nghiệp để ủy quyền các khoản thanh toán gian lận.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Xác thực đa yếu tố ngăn chặn lừa đảo trực tuyến (phishing) như thế nào?

Nó yêu cầu các mã thứ cấp (như khóa phần cứng) không thể bị đánh cắp chỉ qua các trang đích giả mạo.

Q7: Trang đích thu thập thông tin đăng nhập là gì?

Cổng đăng nhập giả mạo giống thật, được thiết kế để thu thập tên người dùng, mật khẩu và mã MFA được nhập theo thời gian thực.

Q8: Chiếm quyền tên miền phụ là gì?

Kẻ tấn công chiếm quyền điều khiển một con trỏ tên miền phụ DNS không dùng để lưu trữ các trang đích lừa đảo độc hại dưới một tên miền gốc đáng tin cậy.

Q9: Kiểm tra căn chỉnh DKIM hoạt động như thế nào?

Nó xác minh rằng tên miền trong tiêu đề 'From' khớp với tên miền đã ký mật mã thư trong tiêu đề DKIM.

Q10: Vai trò của cổng email (email gateway) là gì?

Lọc email đến, kiểm toán liên kết, chạy tệp đính kèm trong sandbox và xác thực việc tuân thủ SPF/DKIM/DMARC.

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

Phishing và giả mạo là loại tội phạm được báo cáo nhiều nhất cho IC3 của FBI năm 2025, với 191,561 khiếu nại. [4]

2. THÔNG TIN VỀ AN NINH

Business email compromise (BEC) gây ra thiệt hại hơn 3 tỷ đô la được báo cáo cho IC3 của FBI trong năm 2025. [4]

3. THÔNG TIN VỀ AN NINH

Tấn công đồng dạng (homograph) dùng các chữ cái Kirin trông giống nhau để nhân bản về mặt thị giác các tên miền thương hiệu khớp chính xác trong trình duyệt.

4. THÔNG TIN VỀ AN NINH

Với 'p=reject', một tên miền yêu cầu bên nhận từ chối thư không đạt trong lúc chuyển phát, thay vì xếp vào thư rác. [2]

5. THÔNG TIN VỀ AN NINH

Các cuộc tấn công whaling nhắm vào CEO thường yêu cầu thanh toán khẩn cấp cho các vụ sáp nhập bí mật hoặc mua tên miền.

6. THÔNG TIN VỀ AN NINH

Các cổng thu thập thông tin đăng nhập sao chép trang đăng nhập thật để nạn nhân nhập mật khẩu thẳng vào biểu mẫu của kẻ tấn công.

7. THÔNG TIN VỀ BẢO MẬT

Hướng dẫn chung của CISA về lừa đảo trực tuyến (phishing) khuyến nghị đào tạo người dùng cùng với DMARC, SPF, DKIM và MFA chống lừa đảo. [3]

8. THÔNG TIN VỀ BẢO MẬT

Việc đánh giá SPF bị giới hạn ở 10 thuật ngữ truy vấn DNS; vượt quá giới hạn sẽ trả về kết quả 'permerror'. [1]

9. THÔNG TIN VỀ BẢO MẬT

Khóa bảo mật phần cứng FIDO2 cung cấp khả năng bảo vệ được củng cố bằng mật mã trước việc thu thập thông tin đăng nhập từ xa.

10. THÔNG TIN VỀ AN NINH

Phishing là một trong những cách phổ biến nhất để kẻ tấn công thâm nhập vào tổ chức lần đầu, đó là lý do tập huấn nâng cao nhận thức thường xuyên là biện pháp phòng thủ hiệu quả.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[1] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Spear phishing là gì? → Email lừa đảo có chủ đích được thiết kế riêng cho một cá nhân hoặc tổ chức cụ thể

2 Câu hỏi 2 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

SPF công bố trong DNS các máy chủ gửi thư được ủy quyền của một tên miền để bên nhận có thể kiểm tra người gửi trong phong bì thư.

3 Câu hỏi 3 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Tấn công whaling là gì? → Chiến dịch lừa đảo nhắm riêng vào các giám đốc điều hành doanh nghiệp nổi tiếng

4 Câu hỏi 4 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

DKIM làm gì? → Thêm chữ ký mật mã vào email để xác minh tính xác thực của người gửi

5 Câu hỏi 5 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Vai trò của DMARC là gì? → Chỉ đạo máy chủ email nhận cách xử lý các kiểm tra SPF/DKIM thất bại

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: spear phishing được thiết kế riêng cho những người cụ thể, không giống phishing hàng loạt chung chung.

7 **Câu hỏi 7** **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Chính sách DMARC có thể chỉ thị máy chủ thư từ chối các thư giả mạo trái phép.

8 **Câu hỏi 8** **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: SPF kiểm tra IP gửi so với DNS; DKIM mới là cơ chế xác minh chữ ký mật mã.

9 **Câu hỏi 9** **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: whaling nhắm vào các lãnh đạo cấp cao, những người có thể phê duyệt thanh toán và truy cập dữ liệu nhạy cảm.

10 **Câu hỏi 10** **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đúng: xác nhận các yêu cầu thanh toán qua một kênh riêng, đã biết giúp ngăn chặn gian lận chuyển khoản.

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

F 1. SPEAR	G 2. GIẢ MẠO	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. TẤN CÔNG WHALING	E 7. PHISHING	A 8. VISHING

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 SPEAR	2 GIẢ MẠO	3 BẢN GHI SPF	4 DKIM
5 DMARC	6 WHALING		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 B – GIAMAO	2 A – SPEAR	3 H – VISHING	4 C – BANGHISPF
5 G – PHISHING	6 E – DMARC	7 D – DKIM	8 F – WHALING

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được SPEAR, GIẢ MẠO và SPF bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

B	P	G	Đ	N	P	L	Ô	V	Ơ	O	Â	S	Q	R
D	K	R	H	Ă	A	Ă	Â	V	O	V	K	I	V	K
V	S	A	I	C	Ơ	M	H	C	I	G	M	M	I	Ơ
Ô	E	E	O	A	M	A	I	G	M	S	M	Ơ	P	Q
S	R	P	E	Â	B	Q	Ơ	O	Ê	Q	H	Â	U	C
G	R	S	X	T	A	Â	P	Y	C	U	Đ	I	I	Ê
N	Y	B	M	C	N	Ơ	Ư	H	Ô	R	Â	S	N	Ă
I	A	Y	N	C	G	K	A	C	I	O	A	C	D	G
L	E	G	B	P	H	Ơ	L	D	G	S	Q	M	Y	Q
A	Đ	Ơ	U	D	I	D	A	A	Ơ	O	H	M	D	Ô
H	S	V	Ơ	I	S	K	P	S	Q	B	M	I	X	Ă
W	Đ	Q	Ư	Ư	P	I	H	A	P	Y	X	X	N	K
E	G	M	P	I	F	M	L	L	R	O	Ê	Ơ	Ơ	G
E	Y	A	O	T	Đ	T	Â	X	P	X	Ă	Ê	L	Y
E	H	N	Ô	N	Ư	Â	L	Y	X	Đ	V	O	U	T

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: VISHING Các cuộc gọi lừa đảo bằng giọng nói (7 chữ cái)

5 hàng ngang: DKIM Chữ ký mật mã trong email (4 chữ cái)

6 hàng ngang: PHISHING Email lừa đảo bằng tác động tâm lý (8 chữ cái)

8 hàng ngang: DMARC Chính sách hướng dẫn từ chối thư (5 chữ cái)

HÀNG DỌC

1 hàng dọc: BANGHISPF Các IP người gửi được cấp phép trong DNS (9 chữ cái)

2 hàng dọc: WHALING Nhắm vào lãnh đạo cấp cao (7 chữ cái)

4 hàng dọc: GIAMAO Làm giả địa chỉ email người gửi (6 chữ cái)

7 hàng dọc: SPEAR Email cá nhân hóa nhắm vào mục tiêu cụ thể (5 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1. AESRP	SPEAR	5. MAOGAI	GIAMAO
2. FBPGAISHN	BANGHISPF	6. IMDK	DKIM
3. ADCRM	DMARC	7. WNIGHLA	WHALING
4. SNGIHPHI	PHISHING	8. IHGVNIS	VISHING

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"PHAT HIÊN LƯA ĐAO XA HÔI QUA KIÊM TOAN CÔNG THƯ"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Xử lý vụ tấn công whaling nhắm vào lãnh đạo cấp cao

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một Giám đốc Tài chính nhận được email được cá nhân hóa cao, tự xưng là từ CEO, yêu cầu chuyển khoản nhanh 50.000 USD để chốt một vụ mua tên miền bí mật.
- Chiến lược và giải pháp đề xuất: Cấu hình DMARC với chính sách 'p=reject' để chặn các tên miền người gửi giả mạo. Thêm biểu ngữ cảnh báo người gửi bên ngoài tại cổng email và yêu cầu xác nhận bằng lời, ngoài băng tần cho mọi giao dịch tài chính.

B Nghiên cứu tình huống 2: Triển khai chính sách cổng SPF/DKIM/DMARC

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một doanh nghiệp không đạt các cuộc kiểm toán bảo mật vì email tiếp thị gửi đi thường bị gắn cờ là thư rác, và tin tặc đang chủ động giả mạo tên miền thương hiệu của công ty.
- Chiến lược và giải pháp đề xuất: Công bố bản ghi TXT cho SPF nêu các IP người gửi được ủy quyền. Cấu hình khóa ký DKIM trên các máy chủ thư đi và phân tích các báo cáo phản hồi XML DMARC đến để phát hiện hành vi lạm dụng.