Họ tên: _____ Ngày: _____ Điểm: _____

Lừa đảo trực tuyến và kỹ thuật xã hội Hướng dẫn bảo vệ

Lừa đảo qua email, tên miền giả mạo, lừa đảo qua điện thoại (vishing), lừa đảo hỗ trợ kỹ thuật, xác minh ngoài kênh, BEC

TỔNG QUAN BÀI HỌC VỀ LỪA ĐẢO TRỰC TUYẾN

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 cách phòng thủ trước lừa đảo trực tuyến. Bạn sẽ khám phá các trang web lừa đảo giả mạo, thủ đoạn tấn công phi kỹ thuật (social engineering), lừa đảo hỗ trợ, các vectơ gian lận chuyển khoản và phương pháp xác minh thanh toán.

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/lua-dao-truc-tuyen/

Lộ trình học về phòng chống lừa đảo trực tuyến của bạn

- Xác định các chỉ báo phổ biến của lừa đảo hỗ trợ kỹ thuật và tên miền typosquatting.
- Triển khai các giao thức xác minh email (SPF, DKIM, DMARC) chống giả mạo.
- Thiết lập xác minh giao dịch ngoài kênh để ngăn gian lận chuyển khoản doanh nghiệp.

HƯỚNG DẪN VỀ LỪA ĐẢO TRỰC TUYẾN

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 bảo vệ khỏi lừa đảo trực tuyến. Kết thúc với hoạt động thưởng Nghĩ nhanh.

LỪA ĐẢO TRỰC TUYẾN & BẢO VỆ CHỐNG KỸ THUẬT XÃ HỘI (GIỚI THIỆU)

Lừa đảo trực tuyến khai thác hành vi con người thông qua phishing, cửa sổ bật lên giả hỗ trợ, vishing và gian lận chuyển khoản. Áp dụng xác minh giao dịch ngoài kênh và các quy tắc tên miền SPF/DKIM/DMARC giúp chặn các hướng tấn công kỹ thuật xã hội ngay tại cổng.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **1. Dấu hiệu chính của một vụ lừa đảo hỗ trợ kỹ thuật là gì?**
   - A. Cửa sổ bật lên tuyên bố hệ thống của bạn bị nhiễm và yêu cầu bạn gọi một số điện thoại
   - B. Bản cập nhật bảo mật tự động tải từ một registry chính thức
   - C. Trình quản lý mật khẩu từ chối điền thông tin đăng nhập trên tên miền doanh nghiệp
   - D. Một tiến trình sao lưu tệp chạy nền trên cấu hình ổ đĩa ngoài

2. **2. Kỹ thuật nào dùng tên miền người gửi giả mạo để đánh cắp thông tin ngân hàng?**
   - A. Lừa đảo qua email
   - B. Quét cổng
   - C. Chèn vào bộ nhớ
   - D. Hủy bằng mật mã

3. **3. Điều gì đại diện cho gian lận chuyển khoản ngân hàng?**
   - A. Lừa nạn nhân gửi tiền vào các tài khoản công ty giả bằng kỹ thuật tấn công phi kỹ thuật
   - B. Mã hóa cơ sở dữ liệu hệ thống bằng tải trọng mã độc tống tiền
   - C. Truy vấn cơ sở dữ liệu bằng lệnh tấn công SQL injection
   - D. Sao lưu tệp hệ thống vào ổ đĩa lưu trữ ngoại tuyến

4. **4. Vì sao kẻ lừa đảo tạo các website mua sắm giả mạo?**
   - A. Để đánh cắp thông tin thẻ tín dụng và thông tin xác thực thanh toán của người mua
   - B. Lưu trữ các bảng cơ sở dữ liệu phân tích phần mềm độc hại trong hộp cát
   - C. Để đẩy nhanh việc giao đơn hàng trực tuyến
   - D. Để thử nghiệm miễn phí các thiết kế trang web mới

5. **5. Vishing nghĩa là gì?**
   - A. Lừa đảo bằng giọng nói qua mạng điện thoại để đánh cắp thông tin xác thực
   - B. Quét mạng cục bộ để tìm thiết bị hệ thống chưa được bảo mật
   - C. Khôi phục cơ sở dữ liệu hệ thống sau một vụ xâm phạm trái phép
   - D. Chạy mã không đáng tin cậy bên trong các container ảo an toàn

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Lừa đảo phishing chỉ nhắm vào người dùng cuối, không bao giờ nhắm vào các mục tiêu whaling cấp lãnh đạo.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Các tên miền giả mạo thường dùng lỗi chính tả nhỏ (như amaz0n.com) để bắt chước các thương hiệu đáng tin cậy.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Có thể giải quyết các vụ lừa đảo hỗ trợ kỹ thuật bằng cách cấp quyền truy cập từ xa cho người gọi.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Kỹ thuật xã hội khai thác tâm lý con người như nỗi sợ và sự khẩn cấp để qua mặt các quy tắc bảo mật.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Các yêu cầu chuyển khoản luôn nên được xác minh qua các kênh liên lạc ngoài băng tần (out-of-band).

○ 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. Các email gian lận đánh lừa người dùng được gọi là _____ .
2. Các địa chỉ web bắt chước thương hiệu đáng tin cậy là địa chỉ _____ .
3. Các vụ lừa đảo qua giọng nói nhắm vào thông tin ngân hàng được gọi là _____ .
4. Cửa sổ bật lên đòi tiền để gỡ virus là hình thức _____ hỗ trợ kỹ thuật.
5. Xác nhận một yêu cầu thanh toán cần _____ ngoài luồng.
6. Chuyển hướng các giao dịch của doanh nghiệp sang tài khoản của kẻ trộm là hình thức _____ .

NGÂN HÀNG TỪ VỰNG

GIẢ MẠO | LỪA CHUYỂN TIỀN | LỪA ĐẢO | PHISHING | SMISHING | VISHING | WHALING | XÁC MINH

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

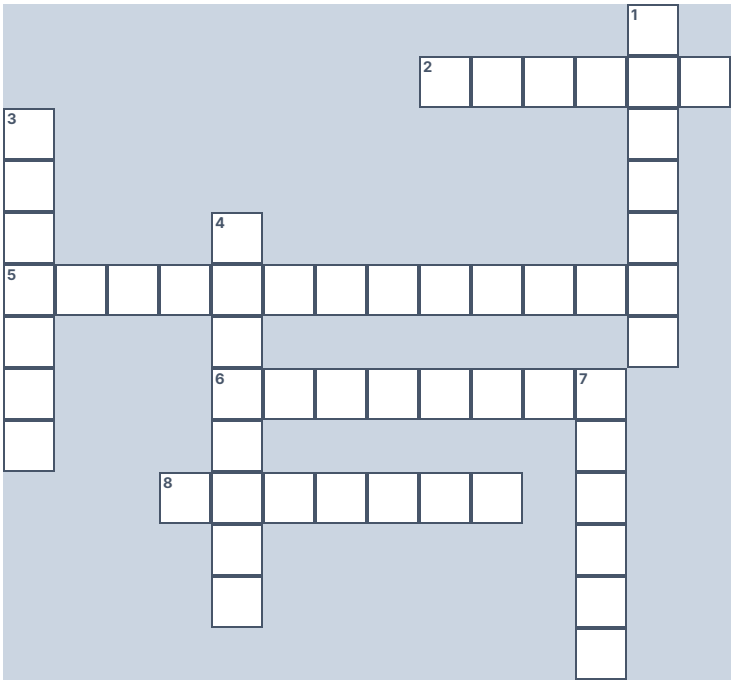
GHÉP ĐỊNH NGHĨA

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. PHISHING	A	Chuyển hướng gian lận các giao dịch ngân hàng sang tài khoản của tội phạm.
☐	2. BỊ GIẢ MẠO	B	Mánh khóe lừa đảo nhằm đánh cắp tiền hoặc thông tin đăng nhập của nạn nhân.
☐	3. VISHING	C	Gửi tin nhắn lừa đảo để đánh cắp thông tin đăng nhập tài khoản di động.
☐	4. LỪA ĐẢO	D	Các cuộc gọi thoại lừa đảo nhằm đánh cắp thông tin đăng nhập và chi tiết tài khoản.
☐	5. XÁC MINH	E	Các cuộc tấn công lừa đảo trực tuyến (phishing) có mục tiêu nhằm đánh cắp thông tin đăng nhập từ các giám đốc cấp cao (C-level).
☐	6. CHUYỂN KHOẢN	F	Địa chỉ người gửi email hoặc trang web bị giả mạo, được thiết kế để trông có vẻ hợp pháp.
☐	7. TẤN CÔNG WHALING	G	Các chiến dịch email lừa đảo nhằm đánh cắp thông tin đăng nhập và mật khẩu.
☐	8. SMISHING	H	Xác nhận thông tin thanh toán bằng một phương thức liên hệ thứ cấp đáng tin cậy.

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

2. Âm mưu gian lận nhằm đánh cắp tiền hoặc quyền truy cập thông tin đăng nhập của nạn nhân (6)

5. Chuyển hướng gian lận các giao dịch ngân hàng sang tài khoản của tội phạm (13)

6. Gửi tin nhắn văn bản lừa đảo để đánh cắp thông tin đăng nhập tài khoản di động (8)

8. Các cuộc gọi thoại gian lận nhằm đánh cắp thông tin đăng nhập và chi tiết tài khoản (7)

HÀNG DỌC

1. Xác nhận chi tiết thanh toán bằng một phương thức liên hệ phụ đáng tin cậy (7)

3. Các cuộc tấn công phishing có chủ đích nhằm đánh cắp thông tin đăng nhập của lãnh đạo cấp cao (7)

4. Các chiến dịch email gian lận nhằm đánh cắp thông tin đăng nhập và mật khẩu (8)

7. Địa chỉ người gửi email hoặc website bị bắt chước để trông có vẻ hợp pháp (6)

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

2 hàng ngang: Âm mưu gian lận nhằm đánh cắp tiền hoặc quyền truy cập thông tin đăng nhập của nạn nhân (6 chữ cái):

5 hàng ngang: Chuyển hướng gian lận các giao dịch ngân hàng sang tài khoản của tội phạm (13 chữ cái):

6 hàng ngang: Gửi tin nhắn văn bản lừa đảo để đánh cắp thông tin đăng nhập tài khoản di động (8 chữ cái):

8 hàng ngang: Các cuộc gọi thoại gian lận nhằm đánh cắp thông tin đăng nhập và chi tiết tài khoản (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Xác nhận chi tiết thanh toán bằng một phương thức liên hệ phụ đáng tin cậy (7 chữ cái):

3 hàng dọc: Các cuộc tấn công phishing có chủ đích nhằm đánh cắp thông tin đăng nhập của lãnh đạo cấp cao (7 chữ cái):

4 hàng dọc: Các chiến dịch email gian lận nhằm đánh cắp thông tin đăng nhập và mật khẩu (8 chữ cái):

7 hàng dọc: Địa chỉ người gửi email hoặc website bị bắt chước để trông có vẻ hợp pháp (6 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.

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

DANH SÁCH TỪ VỰNG

PHISHING GIAMAO VISHING LƯAĐAO XACMINH LƯACHUYÊNTIÊN WHALING SMISHING

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. PHISHING
B. GIAMAO
C. VISHING
D. LƯAĐAO
E. XACMINH
F. LƯACHUYÊNTIÊN
G. WHALING
H. SMISHING

	ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
	1. Địa chỉ người gửi email hoặc website bị bắt chước để trông có vẻ hợp pháp.
	2. Xác nhận chi tiết thanh toán bằng một phương thức liên hệ phụ đáng tin cậy.
	3. Chuyển hướng gian lận các giao dịch ngân hàng sang tài khoản của tội phạm.
	4. Gửi tin nhắn văn bản lừa đảo để đánh cắp thông tin đăng nhập tài khoản di động.
	5. Các cuộc tấn công phishing có chủ đích nhằm đánh cắp thông tin đăng nhập của lãnh đạo cấp cao.
	6. Các cuộc gọi thoại gian lận nhằm đánh cắp thông tin đăng nhập và chi tiết tài khoản.
	7. Các chiến dịch email gian lận nhằm đánh cắp thông tin đăng nhập và mật khẩu.
	8. Âm mưu gian lận nhằm đánh cắp tiền hoặc quyền truy cập thông tin đăng nhập của nạn nhân.

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. **NSHPIHGI** _____

2. **VSGNIHI** _____

3. **MXIHCNA** _____

4. **GHILNWA** _____

5. **MAOGAI** _____

6. **AĐLAOƯ** _____

7. **TIÊULƯNHNÊAYC** _____

8. **SMHGSNII** _____

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 cụm từ kẻ lừa đảo thường dùng			
3	Những hình thức thanh toán mà kẻ lừa đảo yêu cầu			
4	Những loại lừa đảo trực tuyến			
5	Những ưu đãi quá tốt để có thể là thật			
6	Những nơi để báo cáo một vụ lừa đảo			
7	Những từ liên quan đến an ninh mạng			
8	Những người bạn có thể cảnh báo về lừa đảo			
9	Những thứ bạn sao lưu			
10	Những dấu hiệu cảnh báo trong một email			
11	Những dấu hiệu máy tính bị nhiễm			
12	Những cách kiểm tra một cửa hàng trực tuyến			
13	Những cách bảo vệ tài khoản của bạn			
14	Những việc cần làm nếu bạn bị lừa đảo			
15	Những việc cần làm sau khi dữ liệu bị rò rỉ			

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: NGĂN CHẶN LỪA ĐẢO CHUYỂN KHOẢN CỦA DOANH NGHIỆP

👷

Tình huống: Phòng tài chính nhận được một email khẩn từ một địa chỉ nhà cung cấp bị giả mạo, yêu cầu các khoản chuyển tiền hóa đơn sau này được chuyển đến một số định tuyến ngân hàng mới.

Câu hỏi thảo luận: Hãy nêu chính sách xác minh gian lận chuyển khoản, và chỉ rõ các biện pháp chặn xác thực email.

NGHIÊN CỨU TÌNH HUỐNG 2: SỰ CỐ LỪA ĐẢO WHALING NHẮM VÀO LÃNH ĐẠO

👷

Tình huống: Một lãnh đạo đã nhấp vào một liên kết phishing tự nhận chứa tài liệu họp hội đồng quản trị bảo mật, và nhập thông tin đăng nhập công ty chính của mình trên một cổng thông tin giả mạo.

Câu hỏi thảo luận: Hãy trình bày chi tiết các bước ứng phó sự cố, và giải thích cách kiểm toán các lần đăng nhập của lãnh đạo.

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 20 11 12 23 11 12 16 10

4 2 16 10 28 1 5 15 12 16 11 21 25 1 15 1 29

21 25 8 24

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: Lừa đảo trực tuyến là gì?

Chiêu trò gian lận dùng các kênh kỹ thuật số để lừa nạn nhân gửi tiền hoặc cung cấp thông tin xác thực cá nhân.

Q2: Dấu hiệu chính của email phishing là gì?

Tin nhắn tạo cảm giác khẩn cấp (như tài khoản bị đình chỉ) và hướng bạn đến một liên kết không khớp với tên miền chính thức.

Q3: Typosquatting là gì?

Đăng ký các tên miền có lỗi chính tả phổ biến của các thương hiệu nổi tiếng (như amaz0n.com) để lưu trữ các trang lừa đảo trực tuyến (phishing) giả mạo.

Q4: Lừa đảo hỗ trợ kỹ thuật là gì?

Cửa sổ bật lên tuyên bố máy tính của bạn bị nhiễm, hướng bạn gọi một số điện thoại và trả tiền cho phần mềm dọn dẹp giả hoặc dịch vụ truy cập từ xa. [1]

Q5: Vishing là gì?

Tấn công phishing dùng cuộc gọi thoại để lừa nạn nhân cung cấp thông tin tài khoản ngân hàng hoặc đăng nhập.

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: Lừa đảo chuyển khoản (wire fraud) nghĩa là gì?

Chuyển hướng các giao dịch thanh toán đến tài khoản lừa đảo bằng cách mạo danh nhà cung cấp hoặc giám đốc điều hành.

Q7: Whaling là gì?

Hình thức lừa đảo có chủ đích rất cao, nhắm trực tiếp vào các mục tiêu giá trị cao như giám đốc điều hành cấp C của doanh nghiệp.

Q8: Smishing là gì?

Tin nhắn văn bản lừa đảo gửi tới thiết bị di động, chứa liên kết dẫn đến cổng giả mạo hoặc cập nhật theo dõi giả.

Q9: Vì sao xác minh ngoài băng tần lại quan trọng?

Nó xác nhận chi tiết giao dịch qua một kênh liên lạc riêng (như cuộc gọi điện thoại), tránh các chuỗi email bị xâm phạm.

Q10: Lừa đảo ký quỹ (escrow) giả hoạt động như thế nào?

Kẻ lừa đảo tạo một trang ký quỹ (escrow) giả mạo, tuyên bố tiền được giữ an toàn, rồi đánh cắp khoản tiền chuyển khoản của người mua.

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: Kẻ lừa đảo dùng BEC (xâm phạm email doanh nghiệp) để thực hiện gian lận chuyển khoản như thế nào?

Chúng chiếm quyền tài khoản email của một nhân viên hợp pháp, theo dõi các chuỗi hóa đơn và gửi thông tin thanh toán cập nhật kèm tài khoản ngân hàng lừa đảo.

Q2: Rủi ro của tấn công đồng dạng ký tự IDN trong lừa đảo trực tuyến là gì?

Dùng các ký tự không thuộc ASCII trông giống hệt chữ cái thông thường (ví dụ chữ Cyrillic 'a') để đăng ký các tên miền giả mạo bắt chước thương hiệu thật.

Q3: Vì sao việc kiểm tra tiêu đề email quan trọng trong phát hiện lừa đảo?

Nó tiết lộ IP máy chủ gốc thực tế và trạng thái xác thực SPF/DKIM, cho thấy tên miền người gửi có bị giả mạo hay không.

Q4: Kẻ lừa đảo hỗ trợ kỹ thuật khai thác phần mềm điều khiển máy tính từ xa như thế nào?

Chúng dùng các tiện ích như AnyDesk hoặc TeamViewer để kết nối với thiết bị của nạn nhân, cài phần mềm độc hại và đánh cắp mật khẩu đã lưu.

Q5: Mục tiêu của các vụ lừa đảo thu phí trước là gì?

Lừa nạn nhân trả phí xử lý trước để đổi lấy một phần thưởng tài chính lớn không hề tồn tại.

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: Kẻ lừa đảo dùng hồ sơ mạng xã hội để lừa đảo trực tuyến (phishing) có chủ đích như thế nào?

Chúng tổng hợp cơ cấu tổ chức doanh nghiệp và tên nhân viên để soạn các email lừa đảo nhắm mục tiêu (spear-phishing) thuyết phục.

Q7: Vì sao các cửa hàng web giả mạo đưa ra mức giảm giá sâu?

Để dụ người mua nhập thông tin thẻ tín dụng, thu thập thông tin đăng nhập để tái sử dụng hoặc bán lại trên các diễn đàn carding.

Q8: Bản ghi DMARC chặn các vụ lừa đảo trực tuyến (phishing) như thế nào?

DMARC cho phép chủ sở hữu tên miền yêu cầu bên nhận cách ly hoặc từ chối thư không vượt qua kiểm tra SPF và DKIM đã căn chỉnh, chặn hành vi giả mạo trực tiếp. [5]

Q9: Mối đe dọa của các cổng thông tin thu thập thông tin đăng nhập là gì?

Các trang đích giả mạo được thiết kế giống hệt Microsoft 365 hoặc không gian làm việc của Google, đánh cắp thông tin đăng nhập ngay khi được nhập.

Q10: Các nhóm bảo mật báo cáo và vô hiệu hóa tên miền lừa đảo như thế nào?

Bằng cách gửi bằng chứng gian lận đến email báo cáo lạm dụng của nhà đăng ký tên miền, nhà cung cấp lưu trữ và danh sách Google Safe Browsing.

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. [2]

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. [2]

3. THÔNG TIN VỀ AN NINH

Các tên miền giả mạo chính tả khác tên thương hiệu thật một hoặc hai ký tự, nên liếc nhanh có thể bỏ sót.

4. THÔNG TIN VỀ AN NINH

Các vụ lừa đảo hỗ trợ kỹ thuật gây ra thiệt hại hơn 2,1 tỷ USD được báo cáo cho IC3 của FBI trong năm 2025. [2]

5. THÔNG TIN VỀ AN NINH

Tấn công đồng dạng (homograph) trông giống hệt nhau trên thanh địa chỉ trình duyệt trừ khi trình duyệt hiển thị cấu hình punycode.

6. THÔNG TIN VỀ AN NINH

Lừa đảo qua tin nhắn SMS (smishing) dùng các tin nhắn ngắn, khẩn cấp kèm liên kết, khiến nạn nhân có ít ngữ cảnh để nhận ra gian lận.

7. THÔNG TIN VỀ BẢO MẬT

Các cuộc tấn công whaling nhắm vào email của lãnh đạo vì họ kiểm soát quyền truy cập các khoản chuyển khoản thanh toán lớn.

8. THÔNG TIN VỀ BẢO MẬT

Xác minh thay đổi thanh toán bằng cách gọi một số điện thoại đã biết, đã lưu là biện pháp phòng thủ quan trọng chống gian lận chuyển khoản BEC.

9. THÔNG TIN VỀ BẢO MẬT

Các trang web ký quỹ (escrow) giả mạo là chiêu lừa đảo phổ biến trên các chợ trực tuyến: chúng trông như dịch vụ thanh toán an toàn nhưng đánh cắp tiền chuyển khoản của người mua.

10. THÔNG TIN VỀ AN NINH

Google Safe Browsing cảnh báo người dùng trước khi họ mở các trang web mà nó đã gắn cờ là lừa đảo hoặc chứa phần mềm độc hại.

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] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

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

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

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

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

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

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

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Dấu hiệu chính của một vụ lừa đảo hỗ trợ kỹ thuật là gì? → Cửa sổ bật lên tuyên bố hệ thống của bạn bị nhiễm và yêu cầu bạn gọi một số điện thoại

2 Câu hỏi 2

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Kỹ thuật nào dùng tên miền người gửi giả mạo để đánh cắp thông tin ngân hàng? → Lừa đảo qua email

3 Câu hỏi 3

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Điều gì đại diện cho gian lận chuyển khoản ngân hàng? → Lừa nạn nhân gửi tiền vào các tài khoản công ty giả bằng kỹ thuật tấn công phi kỹ thuật

4 Câu hỏi 4

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Vì sao kẻ lừa đảo tạo các website mua sắm giả mạo? → Để đánh cắp thông tin thẻ tín dụng và thông tin xác thực thanh toán của người mua

5 Câu hỏi 5

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Vishing nghĩa là gì? → Lừa đảo bằng giọng nói qua mạng điện thoại để đánh cắp thông tin xác thực

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: lừa đảo trực tuyến (phishing) cũng nhắm vào các lãnh đạo; whaling là phishing nhắm vào các lãnh đạo cấp cao.

7 **Câu hỏi 7** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Các tên miền giả mạo thường dùng lỗi chính tả nhỏ (như amaz0n.com) để bắt chước các thương hiệu đáng tin cậy.

8 **Câu hỏi 8** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: cho kẻ lừa đảo giả danh hỗ trợ quyền truy cập từ xa cho phép chúng cài phần mềm độc hại và đánh cắp dữ liệu.

9 **Câu hỏi 9** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Kỹ thuật xã hội khai thác tâm lý con người như nỗi sợ và sự khẩn cấp để qua mặt các quy tắc bảo mật.

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

GHI CHÚ CHO GIÁO VIÊN

Các yêu cầu chuyển khoản luôn nên được xác minh qua các kênh liên lạc ngoài băng tần (out-of-band).

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

G 1. PHISHING	F 2. BỊ GIẢ MẠO	D 3. VISHING	B 4. LỪA ĐẢO
H 5. XÁC MINH	A 6. CHUYỂN KHOẢN	E 7. TẤN CÔNG WHALING	C 8. SMISHING

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 PHISHING	2 GIẢ MẠO	3 VISHING	4 LỪA ĐẢO
5 XÁC MINH	6 LỪA CHUYỂN TIỀN		

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

1 B – GIAMAO	2 E – XACMINH	3 F – LƯACHUYÊNTIÊN	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – LƯAĐAO

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được PHISHING, BỊ GIẢ MẠO và VISHING 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.

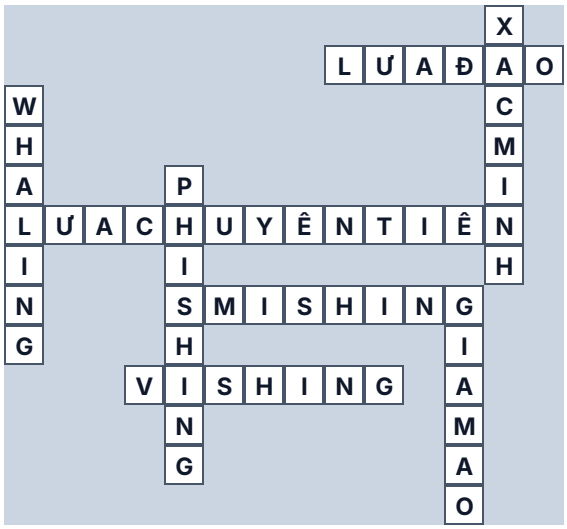
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

2 hàng ngang: LƯAĐAO Âm mưu gian lận nhằm đánh cắp tiền hoặc quyền truy cập thông tin đăng nhập của nạn nhân (6 chữ cái)

5 hàng ngang: LƯACHUYÊNTIÊN Chuyển hướng gian lận các giao dịch ngân hàng sang tài khoản của tội phạm (13 chữ cái)

6 hàng ngang: SMISHING Gửi tin nhắn văn bản lừa đảo để đánh cắp thông tin đăng nhập tài khoản di động (8 chữ cái)

8 hàng ngang: VISHING Các cuộc gọi thoại gian lận nhằm đánh cắp thông tin đăng nhập và chi tiết tài khoản (7 chữ cái)

HÀNG DỌC

1 hàng dọc: XACMINH Xác nhận chi tiết thanh toán bằng một phương thức liên hệ phụ đáng tin cậy (7 chữ cái)

3 hàng dọc: WHALING Các cuộc tấn công phishing có chủ đích nhằm đánh cắp thông tin đăng nhập của lãnh đạo cấp cao (7 chữ cái)

4 hàng dọc: PHISHING Các chiến dịch email gian lận nhằm đánh cắp thông tin đăng nhập và mật khẩu (8 chữ cái)

7 hàng dọc: GIAMAO Địa chỉ người gửi email hoặc website bị bắt chước để trông có vẻ hợp pháp (6 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.	NSHPIHGI	PHISHING	5.	MAOGAI	GIAMAO
2.	VSGNIHI	VISHING	6.	AĐLAOƯ	LƯAĐAO
3.	MXIHCNA	XACMINH	7.	TIÊULƯNHNÊAYC	LƯACHUYÊNTIÊN
4.	GHILNWA	WHALING	8.	SMHGSNII	SMISHING

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"PHAT HIÊN PHISHING BĂNG XAC MINH QUA MAY QUET"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Ngăn chặn lừa đảo chuyển khoản của doanh nghiệp

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: Bộ phận tài chính nhận được một email khẩn từ địa chỉ nhà cung cấp giả mạo, yêu cầu các khoản chuyển khoản hóa đơn sau này được gửi tới một số định tuyến mới.
- Chiến lược và giải pháp đề xuất: Áp dụng chính sách phê duyệt kép cho mọi khoản thanh toán. Thực hiện xác minh ngoài luồng bằng số điện thoại đã lưu sẵn và chặn email từ tên miền giả mạo tại cổng mạng.

B Nghiên cứu tình huống 2: Sự cố lừa đảo whaling nhắm vào lãnh đạo

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 điều hành nhấp vào liên kết lừa đảo trực tuyến (phishing) tự nhận chứa tài liệu họp hội đồng quản trị an toàn, rồi nhập thông tin đăng nhập doanh nghiệp chính trên một cổng giả mạo.
- Chiến lược và giải pháp đề xuất: Cô lập thiết bị của giám đốc điều hành. Đặt lại mọi mã thông báo phiên và thông tin xác thực của công ty. Xem lại nhật ký truy cập để tìm dữ liệu bị đưa ra ngoài, và triển khai MFA bằng phần cứng cho mọi lần đăng nhập.