Họ tên: _____ Ngày: _____ Điểm: _____

Phòng chống đánh cắp danh tính và tài sản
Hướng dẫn bảo mật

Rò rỉ thông tin đăng nhập, MFA, giám sát dark web, cảnh báo đóng băng tín dụng, kỹ thuật xã hội

TỔNG QUAN HỌC TẬP VỀ PHÒNG CHỐNG ĐÁNH CẮP DANH TÍNH

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 phòng ngừa và giảm thiểu hành vi đánh cắp danh tính. Bạn sẽ khám phá rò rỉ thông tin xác thực, xác thực đa yếu tố, giám sát web đen, cảnh báo đóng băng tín dụng và phòng thủ trước tấn công phi kỹ thuật (social engineering).

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/danh-cap-danh-tinh/

Lộ trình học về bảo vệ danh tính của bạn

- Hiểu về rủi ro lộ thông tin đăng nhập trên các diễn đàn dark web.
- Triển khai xác thực đa yếu tố (MFA) và cảnh báo đóng băng tín dụng.
- Thiết kế các biện pháp phòng thủ an ninh doanh nghiệp trước các chiêu lừa đảo kỹ thuật xã hội có chủ đích.

HƯỚNG DẪN VỀ PHÒNG CHỐNG ĐÁNH CẮP DANH TÍNH

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 danh tính. Kết thúc với hoạt động thưởng Nghĩ nhanh.

PHÒNG CHỐNG ĐÁNH CẮP DANH TÍNH VÀ BẢO VỆ TÀI SẢN (GIỚI THIỆU)

Đánh cắp danh tính khai thác thông tin đăng nhập bị lộ và đăng nhập yếu để chiếm quyền tài khoản cá nhân và doanh nghiệp. Triển khai MFA, đóng băng tín dụng, trình quét dark web và các khung SPF/DKIM/DMARC tạo thành lớp phòng thủ quan trọng chống lại việc mạo danh kỹ thuật số.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Phương pháp chính mà kẻ trộm danh tính dùng để đánh cắp thông tin đăng nhập là gì?

- A. Gửi cảnh báo email giả để lừa người dùng nhập mật khẩu trên các cổng giả mạo
- B. Nghe các chương trình phát thanh gần văn phòng công ty của người dùng
- C. Chống phân mảnh ổ lưu trữ máy chủ cục bộ của người dùng
- D. Ngắt các cấu hình sao lưu mạng bên ngoài

2. Biện pháp kiểm soát bảo mật nào cung cấp khả năng phòng vệ mạnh nhất trước việc rò rỉ thông tin đăng nhập?

- A. Xác thực đa yếu tố bằng khóa phần cứng
- B. Tạo mật khẩu dài bằng các định dạng mặc định của trình duyệt
- C. Đổi tên người dùng email sáu tháng một lần
- D. Xóa lịch sử duyệt web theo dõi bằng cookie đã lưu

3. Điều gì đại diện cho việc đóng băng tín dụng?

- A. Khóa báo cáo tín dụng để ngăn kẻ trộm mở các khoản vay trái phép
- B. Xóa lịch sử giao dịch tài khoản ngân hàng khỏi cơ sở dữ liệu
- C. Vô hiệu hóa đầu đọc thẻ từ trên máy quét
- D. Mã hóa ổ cứng cơ sở dữ liệu cục bộ khi lưu trữ

4. Vì sao việc giám sát dark web hữu ích?

- A. Cảnh báo người dùng nếu thông tin xác thực bị lộ của họ xuất hiện trên các cơ sở dữ liệu bất hợp pháp
- B. Ngăn phần mềm độc hại đang hoạt động chạy trong hộp cát ảo
- C. Nó tăng tốc độ định tuyến của trình duyệt trên mạng ảo
- D. Nó chặn các nỗ lực truy cập SQL injection vào cơ sở dữ liệu phía máy chủ

5. Kỹ thuật xã hội (social engineering) nghĩa là gì?

- A. Thao túng con người để họ tự nguyện tiết lộ thông tin xác thực bí mật
- B. Quét các cổng máy chủ doanh nghiệp để tìm lỗ hổng bảo mật đang bị khai thác
- C. Sao lưu các tệp cơ sở dữ liệu hệ thống vào ổ cứng ngoại tuyến
- D. Định tuyến gói tin mạng qua ba nút onion được mã hóa

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Đánh cắp danh tính chỉ ảnh hưởng đến các tài khoản kỹ thuật số trực tuyến, không ảnh hưởng đến thư tín qua đường bưu điện.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Áp dụng MFA cho mọi tài khoản cá nhân chặn được phần lớn các cuộc tấn công bot nhồi thông tin đăng nhập.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Đóng băng tín dụng chặn việc kiểm tra tín dụng nhưng ngăn bạn truy cập tài khoản ngân hàng của chính mình.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Trình quản lý mật khẩu bảo vệ người dùng khỏi phishing bằng cách từ chối tự động điền mật khẩu trên các tên miền giả mạo.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Email phishing thường dùng ngôn từ khẩn cấp để kích động phản ứng nhanh theo cảm xúc.

○ 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. Kẻ trộm danh tính nhắm đến mật khẩu cá nhân và _____ của người dùng.

2. Cảnh báo người dùng về các vụ vi phạm cơ sở dữ liệu giúp xác định các _____ tài khoản riêng tư.

3. Yêu cầu nhập một mã tạm thời để đăng nhập được gọi là _____ .

4. Quét các diễn đàn tin tặc để tìm dữ liệu bị đánh cắp là hoạt động _____ dark web.

5. Chặn các lượt kiểm tra tín dụng trái phép cần việc _____ hồ sơ tín dụng.

6. Đào tạo nhân viên nhận biết phishing xây dựng một tuyến _____ an ninh chủ động.

NGÂN HÀNG TỪ VỰNG

DỮ LIỆU ĐĂNG NHẬP | ĐÓNG BĂNG | GIẢ MẠO | GIÁM SÁT | LỪA ĐẢO PHISHING
PHÒNG THỦ | VỤ RÒ RỈ | XÁC THỰC MFA

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

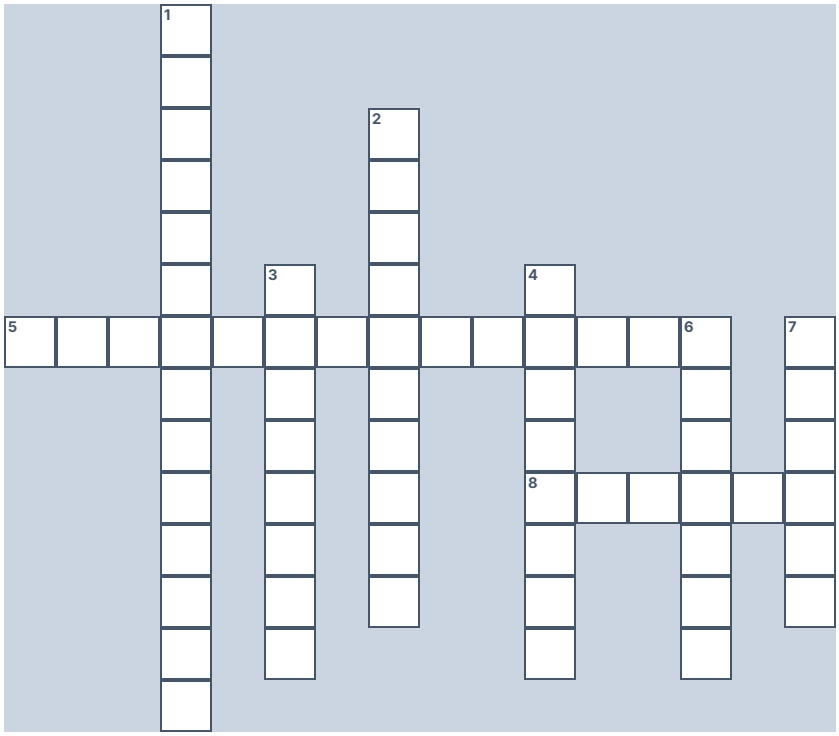
GHÉP ĐỊNH NGHĨA

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. THÔNG TIN ĐĂNG NHẬP	A	Bước xác minh thứ cấp (chẳng hạn khóa phần cứng) bảo vệ việc đăng nhập tài khoản.
☐	2. RÒ RỈ	B	Tạo trang web hoặc email giả để bắt chước một tổ chức hợp pháp.
☐	3. MFA	C	Hạn chế quyền truy cập hồ sơ tín dụng để ngăn các đơn vay gian lận.
☐	4. GIÁM SÁT	D	Việc cơ sở dữ liệu riêng tư chứa hồ sơ cá nhân của người dùng bị lộ trái phép.
☐	5. ĐÓNG BĂNG	E	Đào tạo và các biện pháp kiểm soát kỹ thuật dùng để bảo vệ trước hành vi đánh cắp danh tính.
☐	6. PHÒNG THỦ	F	Gửi tin nhắn gian lận để lừa người dùng tiết lộ thông tin đăng nhập.
☐	7. GIẢ MẠO	G	Quét các diễn đàn trực tuyến và kênh tin tặc để tìm dữ liệu doanh nghiệp bị đánh cắp.
☐	8. PHISHING	H	Tên người dùng, mật khẩu và token riêng tư dùng để xác thực danh tính số.

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

5. Gửi tin nhắn gian lận để lừa người dùng tiết lộ thông tin đăng nhập (14)

8. Tạo trang web hoặc email giả để bắt chước một tổ chức hợp pháp (6)

HÀNG DỌC

1. Tên người dùng, mật khẩu và mã thông báo riêng tư dùng để xác thực danh tính số (14)

2. Bước xác minh thứ cấp (chẳng hạn khóa phần cứng) bảo vệ việc đăng nhập tài khoản (10)

3. Hạn chế quyền truy cập hồ sơ tín dụng để ngăn các đơn vay gian lận (8)

4. Đào tạo và các biện pháp kiểm soát kỹ thuật dùng để chống lại hành vi đánh cắp danh tính (8)

6. Quét các diễn đàn trực tuyến và kênh của tin tặc để tìm dữ liệu doanh nghiệp bị đánh cắp (7)

7. Việc cơ sở dữ liệu riêng tư chứa hồ sơ cá nhân của người dùng bị lộ trái phép (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

5 hàng ngang: Gửi tin nhắn gian lận để lừa người dùng tiết lộ thông tin đăng nhập (14 chữ cái):

8 hàng ngang: Tạo trang web hoặc email giả để bắt chước một tổ chức hợp pháp (6 chữ cái):

HÀNG DỌC

1 hàng dọc: Tên người dùng, mật khẩu và mã thông báo riêng tư dùng để xác thực danh tính số (14 chữ cái):

2 hàng dọc: Bước xác minh thứ cấp (chẳng hạn khóa phần cứng) bảo vệ việc đăng nhập tài khoản (10 chữ cái):

3 hàng dọc: Hạn chế quyền truy cập hồ sơ tín dụng để ngăn các đơn vay gian lận (8 chữ cái):

4 hàng dọc: Đào tạo và các biện pháp kiểm soát kỹ thuật dùng để chống lại hành vi đánh cắp danh tính (8 chữ cái):

6 hàng dọc: Quét các diễn đàn trực tuyến và kênh của tin tặc để tìm dữ liệu doanh nghiệp bị đánh cắp (7 chữ cái):

7 hàng dọc: Việc cơ sở dữ liệu riêng tư chứa hồ sơ cá nhân của người dùng bị lộ trái phép (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.

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

DANH SÁCH TỪ VỰNG

DƯLIÊUĐĂNGNHÂP VURORI XACTHƯCMFA GIAMSAT ĐONGBĂNG PHONGTHU GIAMAO LƯAĐAOPHISHING

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. DỮLIỆUĐĂNGNHẬP
B. VURORI
C. XACTHƯCMFA
D. GIAMSAT
E. ĐONGBĂNG
F. PHONGTHU
G. GIAMAO
H. LƯAĐAOPHISHING

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
☐ 1. Gửi tin nhắn gian lận để lừa người dùng tiết lộ thông tin đăng nhập.
☐ 2. Tên người dùng, mật khẩu và mã thông báo riêng tư dùng để xác thực danh tính số.
☐ 3. Tạo trang web hoặc email giả để bắt chước một tổ chức hợp pháp.
☐ 4. Đào tạo và các biện pháp kiểm soát kỹ thuật dùng để chống lại hành vi đánh cắp danh tính.
☐ 5. Quét các diễn đàn trực tuyến và kênh của tin tặc để tìm dữ liệu doanh nghiệp bị đánh cắp.
☐ 6. Hạn chế quyền truy cập hồ sơ tín dụng để ngăn các đơn vay gian lận.
☐ 7. Việc cơ sở dữ liệu riêng tư chứa hồ sơ cá nhân của người dùng bị lộ trái phép.
☐ 8. Bước xác minh thứ cấp (chẳng hạn khóa phần cứng) bảo vệ việc đăng nhập tài khoản.

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. **NUĂGĐLƯNHD ÂPÊI** _____

2. **FTXAHACMƯC** _____

3. **GOĐBĂGNN** _____

4. **OMAAGI** _____

5. **ORIVRU** _____

6. **AASGMTI** _____

7. **PUGTHHNO** _____

8. **ĐHIOISƯGLPA NHA** _____

Hoạt động thưởng: Nghĩ nhanh

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

1	Những việc cần làm nếu danh tính của bạn bị đánh cắp			
2	Những điều không nên chia sẻ trên mạng xã hội			
3	Những thứ bạn sao lưu			
4	Những loại thẻ hoặc giấy tờ tùy thân trong ví của bạn			
5	Những giấy tờ bạn nên bảo vệ			
6	Những việc cần làm sau khi dữ liệu bị rò rỉ			
7	Lý do cập nhật phần mềm			
8	Những thông tin mà kẻ đánh cắp danh tính muốn có			
9	Những thiết bị có thể bị tấn công			
10	Những nơi dữ liệu của bạn có thể bị rò rỉ			
11	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
12	Những dấu hiệu máy tính bị nhiễm			
13	Những cách chứng minh bạn là ai			
14	Những dấu hiệu của hành vi đánh cắp danh tính			
15	Những dấu hiệu cảnh báo trong một email			

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: BẢO VỆ CHỐNG GIẢ MẠO DANH TÍNH LÃNH ĐẠO

👨‍💼

Tình huống: Một giám đốc cấp C nổi tiếng bị nhắm đến bởi các tên miền gõ sai chính tả giả mạo email cá nhân của họ để lừa đảo khách hàng. Hãy thiết kế một kế hoạch bảo vệ thương hiệu.

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: THÔNG TIN ĐĂNG NHẬP DOANH NGHIỆP BỊ LỘ TRÊN DARK WEB

👨‍💼

Tình huống: Một bản dữ liệu rò rỉ trên dark web chứa vài trăm thông tin đăng nhập của công ty thuộc về các quản trị viên hệ thống của một doanh nghiệp. Hãy thiết kế một chiến lược giảm thiểu.

Câu hỏi thảo luận: Hãy nêu quy trình dọn dẹp thông tin đăng nhập, và lập kế hoạch triển khai trình quản lý mật khẩu.

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

4 1 17 27 9 6 1 16 11 24 12 16 11 23 18

4 2 16 10 28 1 5 24 11 26 5 7 1 29 9 25

24 18

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: Trộm cắp danh tính là gì?

Tội phạm trong đó kẻ tấn công đánh cắp hồ sơ cá nhân (như mật khẩu hoặc số an sinh xã hội) để mạo danh người khác nhằm trục lợi tài chính.

Q2: Nguyên nhân phổ biến nhất của trộm cắp danh tính là gì?

Phishing là một trong những cách hàng đầu kẻ trộm lấy mật khẩu, dụ người dùng vào các trang web giả mạo.

Q3: Xác thực đa yếu tố (MFA) bảo vệ danh tính như thế nào?

MFA yêu cầu một bằng chứng thứ hai (như khóa phần cứng) để đăng nhập, chặn kẻ tấn công ngay cả khi họ đánh cắp mật khẩu của bạn.

Q4: Đóng băng tín dụng là gì?

Dịch vụ miễn phí chặn các văn phòng tín dụng chia sẻ hồ sơ tín dụng của bạn, ngăn kẻ trộm mở các khoản vay mới mang tên bạn. [2]

Q5: Giám sát dark web là gì?

Phần mềm kiểm tra các diễn đàn tin tặc để tìm email, mật khẩu và hồ sơ cá nhân bị rò rỉ, cảnh báo bạn nếu dữ liệu của bạn bị lộ.

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: Credential stuffing nghĩa là gì?

Các bot tự động thử danh sách mật khẩu bị rò rỉ trên hàng trăm trang web để chiếm quyền kiểm soát các tài khoản đang hoạt động.

Q7: Vì sao giả mạo email nguy hiểm?

Nó cho phép kẻ tấn công giả mạo tên người gửi trong email, khiến thư lừa đảo trông như đến từ đồng nghiệp đáng tin cậy.

Q8: Trình quản lý mật khẩu ngăn chặn đánh cắp danh tính như thế nào?

Chúng lưu mật khẩu phức tạp, duy nhất cho mọi tài khoản và từ chối tự động điền thông tin đăng nhập trên các tên miền lừa đảo giả mạo.

Q9: Lừa đảo trực tuyến (phishing) có chủ đích (spear phishing) là gì?

Cuộc tấn công lừa đảo có chủ đích cao, được cá nhân hóa bằng tên và thông tin của nạn nhân để tăng khả năng đánh lừa.

Q10: Cảnh báo tín dụng khác với đóng băng tín dụng như thế nào?

Cảnh báo yêu cầu các bên cho vay xác minh danh tính của bạn trước khi mở tài khoản, còn đóng băng chặn hoàn toàn quyền truy cập hồ sơ tín dụng của bạn. [2]

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: Hoán đổi SIM (SIM swapping) dẫn đến trộm cắp danh tính như thế nào?

Kẻ tấn công thuyết phục nhân viên nhà mạng chuyển số điện thoại của nạn nhân sang SIM mới, qua đó chiếm đoạt mã 2FA gửi qua SMS.

Q2: Vai trò của DMARC trong việc ngăn chặn trộm cắp danh tính là gì?

DMARC cho phép chủ sở hữu tên miền chặn email giả mạo vào hộp thư đến, ngăn email giả mạo tên miền doanh nghiệp.

Q3: Vì sao khó phát hiện hành vi đánh cắp danh tính tổng hợp?

Kẻ trộm kết hợp SSN thật với tên và ngày sinh giả để tạo hồ sơ tín dụng hoàn toàn mới, qua mặt các cảnh báo gian lận cơ bản.

Q4: Các nhà môi giới dữ liệu khai thác danh tính cá nhân như thế nào?

Các nhà môi giới dữ liệu thu thập hồ sơ công khai, hành vi web và lịch sử mua hàng để lập hồ sơ chi tiết về cá nhân, và những hồ sơ này có thể bị rò rỉ hoặc bị bán.

Q5: Vì sao MFA dựa trên SMS bị coi là dễ bị tấn công?

Lưu lượng SMS dễ bị chặn bắt, lừa đảo trực tuyến (phishing) và các hình thức khai thác hoán đổi SIM ở cấp nhà mạng.

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: Khóa hồ sơ tín dụng là gì?

Dịch vụ thương mại tương tự đóng băng, cho phép người dùng mở khóa hoặc khóa hồ sơ tín dụng ngay lập tức qua ứng dụng di động.

Q7: Các vụ rò rỉ dữ liệu doanh nghiệp tiếp tay cho đánh cắp danh tính như thế nào?

Các cơ sở dữ liệu bị rò rỉ làm lộ hàng triệu thông tin đăng nhập ở dạng văn bản thuần, cung cấp cho kẻ trộm dữ liệu thô để thực hiện hành vi gian lận danh tính có chủ đích.

Q8: Rủi ro của việc chia sẻ quá nhiều trên mạng xã hội là gì?

Chia sẻ công khai tên thú cưng, nơi sinh và họ thời con gái của mẹ cho kẻ trộm đáp án của các câu hỏi khôi phục tài khoản thông thường.

Q9: Đăng nhập sinh trắc học bảo vệ hồ sơ danh tính như thế nào?

Sinh trắc học gắn đăng nhập với đặc điểm như vân tay hoặc khuôn mặt; khi lưu trên thiết bị thì khó bị đánh cắp, nhưng dữ liệu sinh trắc học được lưu trữ có thể bị rò rỉ.

Q10: Quy tắc Red Flags chống trộm cắp danh tính như thế nào?

Quy định liên bang yêu cầu các tổ chức tài chính xây dựng chương trình bằng văn bản để phát hiện và ứng phó với các dấu hiệu cảnh báo trộm danh tính.

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

IdentityTheft.gov, do FTC điều hành, cho phép nạn nhân tại Hoa Kỳ báo cáo hành vi đánh cắp danh tính và nhận kế hoạch khắc phục cá nhân. [1]

2. THÔNG TIN VỀ AN NINH

Khóa bảo mật phần cứng là MFA chống lừa đảo, loại MFA mạnh nhất mà CISA khuyến nghị. [4]

3. THÔNG TIN VỀ AN NINH

Mật khẩu bị xâm phạm là điểm xâm nhập phổ biến trong các vụ rò rỉ dữ liệu, tiếp tay cho gian lận danh tính về sau.

4. THÔNG TIN VỀ AN NINH

Đóng băng tín dụng miễn phí theo luật liên bang, ngăn các bên cho vay kiểm tra hồ sơ tín dụng cho đến khi được mở khóa. [2]

5. THÔNG TIN VỀ AN NINH

DMARC cho phép chủ sở hữu tên miền yêu cầu máy chủ thư từ chối hoặc cách ly email giả mạo không vượt qua kiểm tra. [7]

6. THÔNG TIN VỀ AN NINH

Hoán đổi SIM cho phép tin tặc vượt qua xác thực hai yếu tố dựa trên SMS trên các cổng ngân hàng.

7. THÔNG TIN VỀ BẢO MẬT

Gian lận danh tính tổng hợp trộn lẫn thông tin thật và giả, khiến bên cho vay khó phát hiện.

8. THÔNG TIN VỀ BẢO MẬT

Nhiều người dùng lại cùng một mật khẩu cho các tài khoản trực tuyến, nên một vụ rò rỉ có thể làm lộ nhiều tài khoản.

9. THÔNG TIN VỀ BẢO MẬT

Các nhà môi giới dữ liệu tổng hợp hồ sơ chi tiết về số lượng lớn người tiêu dùng, tạo ra rủi ro quyền riêng tư tập trung.

10. THÔNG TIN VỀ AN NINH

Phục hồi sau vụ đánh cắp danh tính có thể mất nhiều tháng, chẳng hạn như khiếu nại các khoản phí và sửa báo cáo tín dụng.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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

Phương pháp chính mà kẻ trộm danh tính dùng để đánh cắp thông tin đăng nhập là gì? → Gửi cảnh báo email giả để lừa người dùng nhập mật khẩu trên các cổng giả mạo

2 Câu hỏi 2

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Biện pháp kiểm soát bảo mật nào cung cấp khả năng phòng vệ mạnh nhất trước việc rò rỉ thông tin đăng nhập? → Xác thực đa yếu tố bằng khóa phần cứng

3 Câu hỏi 3

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Điều gì đại diện cho việc đóng băng tín dụng? → Khóa báo cáo tín dụng để ngăn kẻ trộm mở các khoản vay trái phép

4 Câu hỏi 4

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Vì sao việc giám sát dark web hữu ích? → Cảnh báo người dùng nếu thông tin xác thực bị lộ của họ xuất hiện trên các cơ sở dữ liệu bất hợp pháp

5 Câu hỏi 5

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Kỹ thuật xã hội (social engineering) nghĩa là gì? → Thao túng con người để họ tự nguyện tiết lộ thông tin xác thực bí mật

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

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

GHI CHÚ CHO GIÁO VIÊN

Hành vi đánh cắp danh tính cũng có thể bắt đầu ngoài đời thực, chẳng hạn từ thư hoặc giấy tờ bị đánh cắp.

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

GHI CHÚ CHO GIÁO VIÊN

Áp dụng MFA cho mọi tài khoản cá nhân chặn được phần lớn các cuộc tấn công bot nhồi thông tin đăng nhập.

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

GHI CHÚ CHO GIÁO VIÊN

Đóng băng tín dụng chặn các lần kiểm tra tín dụng mới nhưng không ảnh hưởng đến các tài khoản hiện có của bạn.

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

GHI CHÚ CHO GIÁO VIÊN

Trình quản lý mật khẩu bảo vệ người dùng khỏi phishing bằng cách từ chối tự động điền mật khẩu trên các tên miền giả mạo.

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

GHI CHÚ CHO GIÁO VIÊN

Email phishing thường dùng ngôn từ khẩn cấp để kích động phản ứng nhanh theo cảm xúc.

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

H 1. THÔNG TIN ĐĂNG NHẬP	D 2. RÒ RỈ	A 3. MFA	G 4. GIÁM SÁT
C 5. ĐÓNG BĂNG	E 6. PHÒNG THỦ	B 7. GIẢ MẠO	F 8. PHISHING

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 DỮ LIỆU ĐĂNG NHẬP	2 VỤ RÒ RỈ	3 XÁC THỰC MFA	4 GIÁM SÁT
5 ĐÓNG BĂNG	6 PHÒNG THỦ		

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

1 H – LƯAĐAOPHISHING	2 A – DỮLIỆUĐĂNGNHẬP	3 G – GIAMAO	4 F – PHONGTHU
5 D – GIAMSAT	6 E – ĐONGBĂNG	7 B – VURORI	8 C – XACTHỰCMFA

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được THÔNG TIN ĐĂNG NHẬP, RÒ RỈ và MFA 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

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

ĐÁP ÁN Ô CHỮ

			D											
			Ư				X							
			L				A							
			I				C							
			Ê				T			P				
			U		Đ					H				
L	Ư	A	Đ	A	O	P	H	I	S	H	I	N	G	V
			Ă		N		Ư			O			I	U
			N		G		C			N			A	R
			G		B		M			G	I	A	M	A	O
			N		Ă		F			T			S	R
			H		N		A			H			A	I
			Â		G					U			T	
			P											

HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

5 hàng ngang: LƯAĐAOPHISHING Gửi tin nhắn gian lận để lừa người dùng tiết lộ thông tin đăng nhập (14 chữ cái)

8 hàng ngang: GIAMAO Tạo trang web hoặc email giả để bắt chước một tổ chức hợp pháp (6 chữ cái)

HÀNG DỌC

1 hàng dọc: DƯLIÊUĐĂNGNHẬP Tên người dùng, mật khẩu và mã thông báo riêng tư dùng để xác thực danh tính số (14 chữ cái)

2 hàng dọc: XACTHƯCMFA Bước xác minh thứ cấp (chẳng hạn khóa phần cứng) bảo vệ việc đăng nhập tài khoản (10 chữ cái)

3 hàng dọc: ĐONGBĂNG Hạn chế quyền truy cập hồ sơ tín dụng để ngăn các đơn vay gian lận (8 chữ cái)

4 hàng dọc: PHONGTHU Đào tạo và các biện pháp kiểm soát kỹ thuật dùng để chống lại hành vi đánh cắp danh tính (8 chữ cái)

6 hàng dọc: GIAMSAT Quét các diễn đàn trực tuyến và kênh của tin tặc để tìm dữ liệu doanh nghiệp bị đánh cắp (7 chữ cái)

7 hàng dọc: VURORI Việc cơ sở dữ liệu riêng tư chứa hồ sơ cá nhân của người dùng bị lộ trái phép (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. NUĂGĐLƯNHDÂPÊI — **DƯLIÊUĐĂNGNHÂP**
2. FTXAHACMƯC — **XACTHƯCMFA**
3. GOĐBĂGNN — **ĐONGBĂNG**
4. OMAAGI — **GIAMAO**
5. ORIVRU — **VURORI**
6. AASGMTI — **GIAMSAT**
7. PUGTHHNO — **PHONGTHU**
8. ĐHIOISƯGLPANHA — **LƯAĐAOPHISHING**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"BAO VÊ DANH TINH SÔ BĂNG XAC THƯC ĐA YÊU TÔ"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Bảo vệ chống giả mạo danh tính 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 cấp cao nổi tiếng bị nhắm mục tiêu bởi các tên miền đánh vần sai (typosquatting) giả mạo email cá nhân của họ để lừa khách hàng. Hãy thiết kế kế hoạch bảo vệ thương hiệu.
- Chiến lược và giải pháp đề xuất: Đăng ký mọi biến thể chính tả phổ biến của tên giám đốc điều hành. Triển khai các giao thức xác thực email (DMARC, DKIM, SPF) để ngăn giả mạo tên miền. Áp dụng MFA bằng phần cứng cho mọi lần đăng nhập của ban lãnh đạo cấp cao.

B Nghiên cứu tình huống 2: Thông tin đăng nhập doanh nghiệp bị lộ trên dark web

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 bản sao cơ sở dữ liệu dark web chứa hàng trăm thông tin xác thực doanh nghiệp thuộc về các quản trị viên hệ thống của một doanh nghiệp. Hãy thiết kế chiến lược giảm thiểu.
- Chiến lược và giải pháp đề xuất: Tiến hành đặt lại mật khẩu toàn công ty. Bắt buộc sử dụng trình quản lý mật khẩu doanh nghiệp. Thực thi MFA trên mọi cổng hệ thống và thiết lập cảnh báo giám sát dark web tự động liên tục.