ชื่อ-นามสกุล: _____ **วันที่:** _____ **คะแนน:** _____

การโจมตีแบบฟิชชิงและวิศวกรรมสังคม

สเปียร์ฟิชชิง การหลอกลวงแบบวาลลิง โปรโตคอล SPF/DKIM/DMARC การปลอมแปลงผู้ส่ง และการฝึกอบรมความปลอดภัยสำหรับพนักงาน

ภาพรวมการเรียนรู้เรื่องการโจมตีแบบฟิชชิง

ได้รับการรักษาความปลอดภัย
การเข้ารหัสข้อมูล
มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด
มาตรฐานสากล
กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์
นโยบายการเข้าถึง
การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการโจมตีแบบฟิชชิงและวิศวกรรมสังคม คุณจะได้สำรวจสเปียร์ฟิชชิง การล่าวาฬ (whaling) การปลอมแปลงโดเมน โปรโตคอล SPF/DKIM/DMARC ความปลอดภัยของลิงก์ และการฝึกอบรมสร้างความตระหนักรู้ให้พนักงาน

จุดตรวจสอบของใบงาน

- [ ] **ส่วนที่ 1-4: เรียนรู้ความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามให้เชี่ยวชาญ**
- [ ] **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- [ ] **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- [ ] **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- [ ] **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- [ ] **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความปลอดภัยไซเบอร์ของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/kan-yok-phishing/

เส้นทางการเรียนรู้การลดผลกระทบจากฟิชชิงของคุณ

- ระบุการหลอกลวงทั่วไปแบบฟิชชิง วิชชิง และป๊อปอัปสนับสนุนปลอม
- ใช้ขั้นตอนการยืนยันธุรกรรมผ่านช่องทางนอกแบนด์
- ตั้งค่ากฎ SPF, DKIM และ DMARC เพื่อบล็อกโดเมนที่ปลอมแปลง

คำแนะนำคู่มือการโจมตีแบบฟิชชิง

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การยืนยันตัวตนอีเมล ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การโจมตีแบบฟิชชิงและวิศวกรรมสังคม (บทนำ)

การโจมตีแบบฟิชชิงใช้ข้อความเจาะจงเป้าหมาย การหลอกลวงแบบ whaling และการปลอมแปลงโดเมนเพื่อเก็บข้อมูลเข้าสู่ระบบของผู้ใช้ การรักษาความปลอดภัยระบบองค์กรต้องใช้กฎ SPF, DKIM และ DMARC ที่เกตเวย์ควบคู่กับขั้นตอนการอนุมัตินอกช่องทางหลัก

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1 **1. สเปียร์ฟิชชิงคืออะไร?**

- A. อีเมลฟิชชิงเจาะจงเป้าหมายที่ปรับให้เหมาะกับบุคคลหรือองค์กรหนึ่งๆ
- B. อีเมลจำนวนมากที่ส่งถึงที่อยู่แบบสุ่มหลายล้านรายการ
- C. การโจมตีเครือข่ายที่ท่วมเว็บเซิร์ฟเวอร์ด้วยทราฟฟิก
- D. เทคนิคการดึงข้อมูลจากฐานข้อมูลที่มุ่งเป้าไปที่ระเบียนผู้ใช้

2 **2. โปรโตคอลใดให้โดเมนระบุที่อยู่ IP ผู้ส่งที่ได้รับอนุญาตใน DNS เพื่อต่อต้านการปลอมแปลง?**

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

3 **3. การโจมตีแบบฟิชชิงล่าวาฬคืออะไร?**

- A. แคมเปญฟิชชิงที่เจาะจงเป้าหมายผู้บริหารระดับสูงขององค์กร
- B. การโจมตีแบบ **SQL injection** ที่มุ่งเป้าไปที่การสำรองฐานข้อมูล
- C. การขโมยอุปกรณ์เราเตอร์เครือข่ายท้องถิ่นทางกายภาพ
- D. การสแกนแบบ **Brute-Force** ของ **Credential Stuffing** อัตโนมัติ

4 **4. DKIM ทำหน้าที่อะไร?**

- A. เพิ่มลายเซ็นการเข้ารหัสลงในอีเมลเพื่อยืนยันความถูกต้องของผู้ส่ง
- B. บล็อกแพ็กเก็ตเครือข่ายขาเข้าที่ไฟร์วอลล์
- C. เข้ารหัสวอลุ่มจัดเก็บฐานข้อมูลขณะพักข้อมูล
- D. สแกนไฟล์แนบอีเมลเพื่อหามัลแวร์ตามลายเซ็น

5 **5. DMARC มีบทบาทอะไร?**

- A. การสั่งเมลเซิร์ฟเวอร์ปลายทางว่าจะจัดการอย่างไรกับการตรวจสอบ **SPF/DKIM** ที่ไม่ผ่าน
- B. การถอดรหัสรหัสผ่านระบบด้วยตาราง **rainbow** ที่คำนวณไว้ล่วงหน้า
- C. การบีบอัดไฟล์แนบอีเมลก่อนส่ง
- D. การกำหนดค่าสิทธิ์การเข้าถึงการกำหนดเส้นทางเครือข่าย

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. สเปียร์ฟิชชิงอาศัยอีเมลจำนวนมากทั่วไปที่ส่งถึงที่อยู่แบบสุ่มนับล้าน

○ จริง ○ เท็จ

7 คำถาม 7

7. นโยบาย DMARC สามารถสั่งให้เมลเซิร์ฟเวอร์ปฏิเสธข้อความปลอมที่ไม่ได้รับอนุญาตได้

○ จริง ○ เท็จ

8 คำถาม 8

8. การตรวจสอบ SPF ทำงานโดยตรวจสอบลายเซ็นการเข้ารหัสของเนื้อหาอีเมล

○ จริง ○ เท็จ

9 คำถาม 9

9. การโจมตีแบบฟิชชิงล่าวาฬมุ่งเป้าไปที่ผู้ดูแลระบบระดับล่างขององค์กรเพื่อเข้าถึงไฟล์ฐานข้อมูล

○ จริง ○ เท็จ

10 คำถาม 10

10. การยืนยันคำขอชำระเงินผ่านช่องทางแยกต่างหากช่วยหยุดการหลอกลวงโอนเงินทางการเงิน

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การเจาะจงพนักงานคนหนึ่งด้วยข้อมูลเฉพาะบุคคลคือฟิชชิงแบบ _____
2. การปลอมแปลงส่วนหัวอีเมลให้ข้อความดูน่าเชื่อถือคือการ _____ ผู้ส่ง
3. รายการเรคคอร์ด DNS ของไอพีเมลเซิร์ฟเวอร์ที่ได้รับอนุญาตคือ _____
4. มาตรฐานลายเซ็นอีเมลที่ยืนยันผู้ส่งคือ _____
5. การกำหนดนโยบายปฏิเสธการตรวจสอบ SPF/DKIM ที่ล้มเหลวใช้ _____
6. แคมเปญฟิชชิงที่มุ่งเป้าผู้บริหารระดับ C เรียกว่า _____

คลังคำศัพท์

ดีเคไอเอ็ม ดีมาร์ก วิชชิง เวลลิง สปูฟฟิง สเปียร์ สมิชชิง เอสพีเอฟ

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

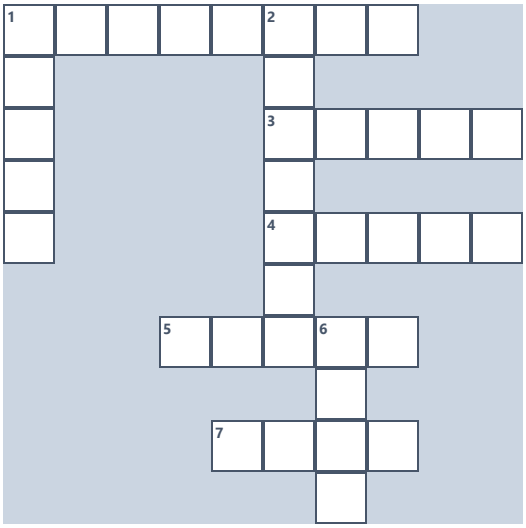
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. สเปียร์**	**A**	การโทรหลอกลวงด้วยเสียง
☐	**2. การปลอมแปลง**	**B**	กำหนดเป้าหมายผู้บริหารระดับ C
☐	**3. SPF**	**C**	คำสั่งปฏิเสธตามนโยบาย
☐	**4. DKIM**	**D**	IP ผู้ส่งที่ได้รับอนุญาตของ DNS
☐	**5. DMARC**	**E**	อีเมลวิศวกรรมสังคม
☐	**6. ฟิชชิงล่าวาฬ**	**F**	อีเมลเจาะจงเป้าหมายแบบปรับให้เหมาะกับแต่ละบุคคล
☐	**7. ฟิชชิง**	**G**	การปลอมที่อยู่อีเมลผู้ส่ง
☐	**8. วิชชิง**	**H**	ลายเซ็นดิจิทัลในอีเมล

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

1. ลายเซ็นเข้ารหัสลับในอีเมล (8)

3. อีเมลเจาะจงเป้าหมายที่ปรับแต่งเฉพาะบุคคล (5)

4. เจาะจงผู้บริหารระดับ C (5)

5. การปลอมแปลงที่อยู่อีเมลผู้ส่ง (5)

7. การโทรหลอกลวงด้วยเสียง (4)

แนวตั้ง

1. คำสั่งนโยบายให้ปฏิเสธ (5)

2. ไอพีของผู้ส่งที่ได้รับอนุญาตใน DNS (7)

6. อีเมลวิศวกรรมสังคม (4)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

1 แนวนอน: ลายเซ็นเข้ารหัสลับในอีเมล (8 ตัวอักษร):

3 แนวนอน: อีเมลเจาะจงเป้าหมายที่ปรับแต่งเฉพาะบุคคล (5 ตัวอักษร):

4 แนวนอน: เจาะจงผู้บริหารระดับ C (5 ตัวอักษร):

5 แนวนอน: การปลอมแปลงที่อยู่อีเมลผู้ส่ง (5 ตัวอักษร):

7 แนวนอน: การโทรหลอกลวงด้วยเสียง (4 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: คำสั่งนโยบายให้ปฏิเสธ (5 ตัวอักษร):

2 แนวตั้ง: ไอพีของผู้ส่งที่ได้รับอนุญาตใน DNS (7 ตัวอักษร):

6 แนวตั้ง: อีเมลวิศวกรรมสังคม (4 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ผ	ฟ	รี	ก	ท	กี	ท	วิ	นี	ร	ด	ง	ร	ดี	ข
ป	ร์	ย	ลี	ม	ฟ	า	ช	ดี	กี	ร	า	ข	า	ร
ด	ย	ร	ต	อ	า	นี	ชิ	า	ม	น	นี	ส	ช	มี
ฟ	ปี	บ	า	า	ห	นี	ง	า	ม	า	กี	จ	า	า
รี	เ	ต	ว	ย	ดี	ง	ก	ค	จ	น	ร์	ตี	เ	ว
ร	ส	ดี	ว	า	เ	ล	เ	ล	ด	า	อ	ก	ว	ย
ง	ชิ	ช	ฟิ	ซ	ค	ฟ	ก	อ	ก	ล	ม	า	ล	ป
ง	อ	อ	ม	มี	ไ	า	ล	ล	ส	ป	จ	า	ลิ	นี
ฟิ	กี	พ	ร	ง	อ	า	ช	า	า	พี	ลี	จ	ง	ดี
ฟ	า	น	ล	ผ	เ	ดี	ช	ก	ด	า	เ	ต	า	จ
ปู	า	ค	ก	ดี	อ็	า	ช	ว	ก	ด	กี	อ	ด	ท
ส	ผ	ฟ	ซ	มี	ม	ม	อ	ต	ฟ	ร	ดี	า	ฟ	ท
า	ส	ท	ข	ข	า	น	ก	า	ล	า	ม	ร	มี	า
ร	ช	ก	ด	ง	น	ร	ต	สี	ย	ข	มี	ดี	ด	ด
ว	บ	ฟ	อ	า	ร	ห	ห	รี	น	ผ	นี	ม	ผ	ดี

รายการคำศัพท์

สเปียร์ สปูฟฟิง เอสพีเอฟ ดีเคไอเอ็ม ดีมาร์ก เวลลิง ฟิชชิง วิชชิง

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. สเปียร์

B. สปูฟฟิง

C. เอสพีเอฟ

D. ดีเคไอเอ็ม

E. ดีมาร์ก

F. เวลลิง

G. ฟิชชิง

H. วิชชิง

คำนิยามและช่องจับคู่

1. การปลอมแปลงที่อยู่อีเมลผู้ส่ง
2. อีเมลเจาะจงเป้าหมายที่ปรับแต่งเฉพาะบุคคล
3. การโทรหลอกลวงด้วยเสียง
4. ไอพีของผู้ส่งที่ได้รับอนุญาตใน DNS
5. อีเมลวิศวกรรมสังคม
6. คำสั่งนโยบายให้ปฏิเสธ
7. ลายเซ็นเข้ารหัสลับในอีเมล
8. เจาะจงผู้บริหารระดับ C

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ยปีสร์เ
2. เสฟอเพือ
3. าดีกร์ม
4. งชิฟช
5. ฟงสฟิปู
6. อ็มไเดือเค
7. ลิงเลว
8. วิงชิช

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	อุปกรณ์ที่ถูกแฮกได้			
2	สัญญาณของอีเมลฟิชชิง			
3	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
4	คำที่สร้างความเร่งด่วนปลอม			
5	วิธีตรวจสอบผู้ส่ง			
6	บุคคลที่คุณขอความช่วยเหลือด้าน IT ได้			
7	สิ่งที่คุณสำรองข้อมูล			
8	ปลาหรือสัตว์ทะเลที่คุณรู้จัก			
9	บริษัทที่มิจฉาชีพแอบอ้าง			
10	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
11	สิ่งที่ควรทำหลังคลิกลิงก์ปลอม			
12	สิ่งที่ควรทำหลังข้อมูลรั่วไหล			
13	ช่องทางที่เกิดฟิชชิง			
14	สิ่งที่คุณไม่ส่งทางอีเมลเด็ดขาด			
15	วิธีปกป้องบัญชีของคุณ			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การแก้ไขหลังการโจมตีแบบเวลลิงต่อผู้บริหารระดับสูง



สถานการณ์: ประธานเจ้าหน้าที่ฝ่ายการเงินได้รับอีเมลที่ปรับแต่งเฉพาะบุคคลอย่างมากซึ่งอ้างว่ามาจาก CEO ขอให้โอนเงินด่วน $50,000 เพื่อปิดการซื้อโดเมนลับ

คำถามอภิปราย: จงวิเคราะห์ความเสี่ยงจากการปลอมแปลงแบรนด์ และอธิบายการควบคุม SPF/DKIM/DMARC และการยืนยันตัวตนโดยละเอียด

กรณีศึกษาที่ 2: การปรับใช้นโยบายเกตเวย์ SPF/DKIM/DMARC



สถานการณ์: องค์กรไม่ผ่านการตรวจสอบความปลอดภัยเพราะอีเมลการตลาดขาออกถูกแจ้งเป็นสแปมบ่อยครั้ง และแฮกเกอร์กำลังปลอมแปลงโดเมนแบรนด์ของบริษัทอยู่

คำถามอภิปราย: จงกำหนดมาตรการควบคุมทางเทคนิคและการบริหารเพื่อตรวจสอบความถูกต้องของอีเมล

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ปกป้องทรัพย์สินเครือข่ายจากผู้ก่อภัยคุกคามออนไลน์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ◌ั=48
า=49 ◌ำ=50 ◌ิ=51 ◌ี=52 ◌ึ=53 ◌ื=54 ◌ุ=55 ◌ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ◌็=62 ◌่=63 ◌้=64 ◌๊=65 ◌๋=66 ◌์=67

21	35	39	8	8	48	26

39	51	40	39	1	35	35	33	42	48	7	4	33	20	64	39	34

1	49	35	21	35	39	8	42	45	26

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ◌์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: ฟิชชิงคืออะไร?

ฟิชชิงเป็นการโจมตีด้วยวิศวกรรมสังคมที่อาชญากรส่งข้อความหลอกลวงเพื่อหลอกให้ผู้ใช้แชร์ข้อมูลสำคัญ

Q2: ฟิชชิงกับสเปียร์ฟิชชิงต่างกันอย่างไร?

ฟิชชิงมุ่งเป้ากลุ่มกว้างด้วยเนื้อหาทั่วไป ส่วนสเปียร์ฟิชชิงมุ่งเป้าเหยื่อเฉพาะรายโดยใช้รายละเอียดที่ปรับแต่ง

Q3: whaling คืออะไร?

ฟิชชิงล่าวาฬคือการโจมตีแบบฟิชชิงที่มุ่งเป้าสูงต่อผู้บริหารระดับสูงที่มีอำนาจด้านการบริหาร

Q4: การปลอมแปลงอีเมล (email spoofing) คืออะไร?

การปลอมแปลงอีเมล (email spoofing) คือการสร้างข้อความอีเมลที่ปลอมที่อยู่ผู้ส่งเพื่อหลอกให้ผู้รับเชื่อถือแหล่งที่มา

Q5: SPF ป้องกันการปลอมแปลงได้อย่างไร?

เผยแพร่รายการที่อยู่ IP ผู้ส่งที่ได้รับอนุญาตใน DNS ให้เซิร์ฟเวอร์ปลายทางตรวจสอบต้นทางของอีเมลได้ [1]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: DKIM คืออะไร?

DomainKeys Identified Mail เพิ่มลายเซ็นการเข้ารหัสลงในส่วนหัวอีเมล เพื่อพิสูจน์ว่าโดเมนรับผิดชอบและข้อความไม่ถูกแก้ไข

Q7: DMARC ย่อมาจากอะไร?

Domain-based Message Authentication, Reporting, and Conformance [2]

Q8: นโยบาย DMARC คืออะไร?

นโยบายที่บอกเมลเซิร์ฟเวอร์ว่าจะจัดการข้อความที่ไม่ผ่าน SPF/DKIM อย่างไร (none, quarantine หรือ reject) [2]

Q9: vishing คืออะไร?

ฟิชชิงทางเสียง ซึ่งผู้โจมตีใช้การโทรศัพท์หลอกลวงเพื่อดึงข้อมูลด้านการบริหารหรือการเงิน

Q10: เครื่องมือสแกนลิงก์ช่วยได้อย่างไร?

สแกนและเขียนลิงก์ในอีเมลขาเข้าใหม่เพื่อตรวจสอบความปลอดภัยของเว็บเพจปลายทางในขณะที่คลิก

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: การโจมตีแบบ homograph ทำงานอย่างไร?

ผู้โจมตีจดทะเบียนชื่อโดเมนโดยใช้อักขระ Unicode ที่ไม่ใช่ ASCII ซึ่งดูคล้ายกัน เพื่อเลียนแบบโดเมนที่ถูกต้องให้ดูเหมือนจริง

Q2: การแสดงแบบ punycode คืออะไร?

การเข้ารหัสที่แปลงชื่อโดเมน Unicode เป็นสตริงที่เข้ากันได้กับ ASCII ซึ่งขึ้นต้นด้วย 'xn--' เพื่อให้ DNS จัดการได้

Q3: เหตุใด 'p=reject' จึงเป็นสถานะ DMARC ที่ปลอดภัยที่สุด?

ขอให้เซิร์ฟเวอร์ปลายทางปฏิเสธอีเมลที่ไม่ผ่าน DMARC (SPF/DKIM ที่สอดคล้องกัน) ระหว่างเซสชัน SMTP เพื่อบล็อกการปลอมแปลงโดยตรง [2]

Q4: ผู้โจมตีหลบเลี่ยงกฎ SPF ได้อย่างไร?

ด้วยการใช้โดเมนที่เลียนแบบ (typosquatting) หรือใช้บัญชีที่ถูกเจาะในบริการอีเมลของบุคคลที่สามที่ถูกต้อง

Q5: การโจมตีอีเมลธุรกิจ (BEC) คืออะไร?

การหลอกลวงในองค์กรที่ผู้โจมตีแย่งชิงหรือปลอมเป็นบัญชีอีเมลธุรกิจเพื่ออนุมัติการชำระเงินที่เป็นการฉ้อโกง

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การยืนยันตัวตนแบบหลายปัจจัยหยุดฟิชชิงได้อย่างไร?

ต้องใช้โทเค็นชั้นที่สอง (เช่น คีย์ฮาร์ดแวร์) ที่ไม่สามารถถูกขโมยได้ด้วยหน้าเว็บปลอมเพียงอย่างเดียว

Q7: หน้า landing เก็บข้อมูลรับรอง (credential harvesting) คืออะไร?

พอร์ทัลเข้าสู่ระบบปลอมที่ออกแบบมาเพื่อดักชื่อผู้ใช้ รหัสผ่าน และโทเค็น MFA ที่กรอกแบบเรียลไทม์

Q8: การแย่งชิงซับโดเมน (subdomain hijacking) คืออะไร?

ผู้โจมตียึดตัวชี้โดเมนย่อย DNS ที่ไม่ได้ใช้งานเพื่อโฮสต์หน้า Landing Page ฟิชชิงอันตรายภายใต้โดเมนหลักที่เชื่อถือได้

Q9: การตรวจสอบ DKIM alignment ทำงานอย่างไร?

ตรวจสอบว่าโดเมนในส่วนหัว 'From' ตรงกับโดเมนที่ลงนามข้อความด้วยการเข้ารหัสลับในส่วนหัว DKIM

Q10: อีเมลเกตเวย์มีบทบาทอย่างไร?

การกรองอีเมลขาเข้า การตรวจสอบลิงก์ การทดสอบไฟล์แนบในแซนด์บ็อกซ์ และการตรวจสอบการปฏิบัติตาม SPF/DKIM/DMARC

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ฟิชชิงและการปลอมแปลงเป็นอาชญากรรมประเภทที่มีผู้แจ้งต่อ IC3 ของ FBI มากที่สุดในปี 2025 โดยมี 191,561 เรื่อง [4]

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การโจรกรรมทางอีเมลธุรกิจ (BEC) ก่อให้เกิดความสูญเสียกว่า 3 พันล้านดอลลาร์ที่รายงานต่อ IC3 ของ FBI ในปี 2025 [4]

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การโจมตีแบบ Homograph ใช้ตัวอักษรซีริลลิกที่หน้าตาคล้ายกันเพื่อทำซ้ำโดเมนแบรนด์ที่ตรงกันทุกประการในเบราว์เซอร์ให้ดูเหมือนกัน

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

เมื่อใช้ 'p=reject' โดเมนจะขอให้ผู้รับปฏิเสธอีเมลที่ไม่ผ่านการตรวจสอบระหว่างการส่ง ไม่ใช่จัดเก็บเป็นสแปม [2]

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การโจมตีแบบฟิชชิงล่าวาฬที่มุ่งเป้าไปที่ CEO มักขอให้ชำระเงินด่วนสำหรับการควบรวมกิจการที่เป็นความลับหรือการซื้อโดเมน

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

พอร์ทัลเก็บเกี่ยวข้อมูลรับรองคัดลอกหน้าเข้าสู่ระบบจริง เพื่อให้เหยื่อพิมพ์รหัสผ่านลงในแบบฟอร์มของผู้โจมตีโดยตรง

7. ข้อมูลเชิงลึกด้านความปลอดภัย

คำแนะนำร่วมเรื่องฟิชชิงของ CISA แนะนำให้อบรมผู้ใช้ควบคู่กับ DMARC, SPF, DKIM และ MFA ที่ต้านทานฟิชชิง [3]

8. ข้อมูลเชิงลึกด้านความปลอดภัย

การประเมิน SPF จำกัดที่ 10 เงื่อนไขที่ใช้การค้นหา DNS หากเกินขีดจำกัดจะได้ผลลัพธ์ 'permerror' [1]

9. ข้อมูลเชิงลึกด้านความปลอดภัย

คีย์ความปลอดภัยฮาร์ดแวร์ FIDO2 ให้การป้องกันที่หนุนด้วยการเข้ารหัสต่อการเก็บเกี่ยวข้อมูลรับรองจากระยะไกล

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ฟิชชิงเป็นหนึ่งในวิธีที่พบบ่อยที่สุดที่ผู้โจมตีใช้เข้าสู่องค์กรเป็นครั้งแรก การอบรมสร้างความตระหนักรู้อย่างสม่ำเสมอจึงเป็นการป้องกันที่มีประสิทธิภาพ

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **คำถาม 1** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

สเปียร์ฟิชชิงคืออะไร? → อีเมลฟิชชิงเจาะจงเป้าหมายที่ปรับให้เหมาะกับบุคคลหรือองค์กรหนึ่งๆ

2 **คำถาม 2** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

SPF เผยแพร่โฮสต์ผู้ส่งที่ได้รับอนุญาตของโดเมนใน DNS เพื่อให้ผู้รับตรวจสอบผู้ส่งซองจดหมาย (envelope sender) ได้

3 **คำถาม 3** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

การโจมตีแบบฟิชชิงล่าวาฬคืออะไร? → แคมเปญฟิชชิงที่เจาะจงเป้าหมายผู้บริหารระดับสูงขององค์กร

4 **คำถาม 4** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

DKIM ทำหน้าที่อะไร? → เพิ่มลายเซ็นการเข้ารหัสลงในอีเมลเพื่อยืนยันความถูกต้องของผู้ส่ง

5 **คำถาม 5** — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

DMARC มีบทบาทอะไร? → การสั่งเมลเซิร์ฟเวอร์ปลายทางว่าจะจัดการอย่างไรกับการตรวจสอบ SPF/DKIM ที่ไม่ผ่าน

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6**

คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: สเปียร์ฟิชชิงถูกปรับแต่งให้เหมาะกับบุคคลเฉพาะ ต่างจากฟิชชิงจำนวนมากทั่วไป

7 **คำถาม 7**

คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

นโยบาย DMARC สามารถสั่งให้เมลเซิร์ฟเวอร์ปฏิเสธข้อความปลอมที่ไม่ได้รับอนุญาตได้

8 **คำถาม 8**

คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: SPF ตรวจ IP ผู้ส่งกับ DNS ส่วน DKIM คือโปรโตคอลที่ตรวจสอบลายเซ็นการเข้ารหัส

9 **คำถาม 9**

คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: whaling มุ่งเป้าผู้บริหารระดับสูง ซึ่งอนุมัติการชำระเงินและเข้าถึงข้อมูลสำคัญได้

10 **คำถาม 10**

คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: การยืนยันคำขอชำระเงินผ่านช่องทางที่แยกต่างหากและเป็นที่รู้จักช่วยหยุดการฉ้อโกงการโอนเงิน

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

F 1. สเปียร์	G 2. การปลอมแปลง	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. ฟิชชิงล่าวาฬ	E 7. ฟิชชิง	A 8. วิชชิง

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 สเปียร์	2 สปูฟฟิง	3 เอสพีเอฟ	4 ดีเคไอเอ็ม
5 ดีมาร์ก	6 เวลลิง		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 B – สปูฟฟิง	2 A – สเปียร์	3 H – วิชชิง	4 C – เอสพีเอฟ
5 G – ฟิชชิง	6 E – ดีมาร์ก	7 D – ดีเคไอเอ็ม	8 F – เวลลิง

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย สเปียร์ การปลอมแปลง และ SPF ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ผ	ฟ	รี	ก	ท	กี	ท	วิ	นี	ร	ด	ง	ร	ดี	ข
ป	ร์	ย	ลี	ม	ฟ	า	ช	ดี	กี	ร	า	ข	า	ร
ด	ย	ร	ต	อ	า	นี	ชิ	า	ม	น	นี	ส	ช	มี
ฟ	ปี	บ	า	า	ห	นี	ง	า	ม	า	กี	จ	า	า
รี	เ	ต	ว	ย	ดี	ง	ก	ค	จ	น	ร์	ดี	เ	ว
ร	ส	ตี	ว	า	เ	ล	เ	ล	ด	า	อ	ก	ว	ย
ง	ชิ	ช	ฟิ	ช	ค	ฟ	ก	อ	ก	ล	ม	า	ล	ป
ง	อ	อ	ม	มี	ไ	า	ล	ล	ส	ป	จ	า	ลิ	นี
ฟิ	กี	พ	ร	ง	อ	า	ช	า	า	พี	ลี	จ	ง	ดี
ฟ	า	น	ล	ผ	เ	ดี	ช	ก	ด	า	เ	ต	า	จ
ปู	า	ค	ก	ดี	อ็	า	ช	ว	ก	ด	กี	อ	ด	ท
ส	ผ	ฟ	ช	มี	ม	ม	อ	ต	ฟ	ร	ดี	า	ฟ	ท
า	ส	ท	ข	ข	า	น	ก	า	ล	า	ม	ร	มี	า
ร	ช	ก	ด	ง	น	ร	ต	สี	ย	ข	มี	ดี	ด	ด
ว	บ	ฟ	อ	า	ร	ห	ห	รี	น	ผ	นี	ม	ผ	ดี

เฉลยปริศนาอักษรไขว้

ดี	เ	ค	ไ	อ	เ	อ็	ม			
ม				อ						
า				ส	เ	ปี	ย	ร์		
ร์				พี						
ก				เ	ว	ล	ลิ	ง		
				อ						
			ส	ปู	ฟ	ฟิ	ง			
						ช				
				วิ	ช	ชิ	ง			
						ง				

คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

1 แนวนอน: ดีเค้ไอเอ็ม ลายเซ็นเข้ารหัสลับในอีเมล (8 ตัวอักษร)

3 แนวนอน: สเปียร์ อีเมลเจาะจงเป้าหมายที่ปรับแต่งเฉพาะบุคคล (5 ตัวอักษร)

4 แนวนอน: เวลลิง เจาะจงผู้บริหารระดับ C (5 ตัวอักษร)

5 แนวนอน: สปูฟฟิง การปลอมแปลงที่อยู่อีเมลผู้ส่ง (5 ตัวอักษร)

7 แนวนอน: วิชชิง การโทรหลอกลวงด้วยเสียง (4 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ดีมาร์ก คำสั่งนโยบายให้ปฏิเสธ (5 ตัวอักษร)

2 แนวตั้ง: เอสพีเอฟ ไอพีของผู้ส่งที่ได้รับอนุญาตใน DNS (7 ตัวอักษร)

6 แนวตั้ง: ฟิชชิง อีเมลวิศวกรรมสังคม (4 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ยปีสร์เ → สเปียร์
2. เสฟอเพือ → เอสพีเอฟ
3. าดีกร์ม → ดีมาร์ก
4. งชิฟิช → ฟิชชิง
5. ฟงสฟิปู → สปูฟฟิง
6. อ็มไเดือเค → ดีเคไอเอ็ม
7. ลิงเลว → เวลลิง
8. วิงชิช → วิชชิง

เฉลยภารกิจรหัสลับ

"ตรวจจับ วิศวกรรมสังคม ด้วย การตรวจสอบ"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การแก้ไขหลังการโจมตีแบบเวลลิงต่อผู้บริหารระดับสูง

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ผู้อำนวยการฝ่ายการเงินได้รับอีเมลที่เจาะจงตัวมาก อ้างว่ามาจาก CEO ขอให้โอนเงินด่วน 50,000 ดอลลาร์เพื่อปิดการซื้อโดเมนที่เป็นความลับ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ตั้งค่า DMARC ด้วยนโยบาย 'p=reject' เพื่อบล็อกโดเมนผู้ส่งที่ถูกปลอมแปลง เพิ่มแบนเนอร์เตือนผู้ส่งภายนอกที่เกตเวย์ และกำหนดให้ยืนยันด้วยวาจานอกช่องทางสำหรับธุรกรรมทางการเงินทั้งหมด

B กรณีศึกษาที่ 2: การปรับใช้นโยบายเกตเวย์ SPF/DKIM/DMARC

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: องค์กรไม่ผ่านการตรวจสอบความปลอดภัยเพราะอีเมลการตลาดขาออกถูกทำเครื่องหมายเป็นสแปมบ่อยครั้ง และแฮกเกอร์กำลังปลอมแปลงโดเมนแบรนด์ของบริษัทอยู่
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เผยแพร่เรคคอร์ด TXT สำหรับ SPF ที่ระบุ IP ของผู้ส่งที่ได้รับอนุญาต กำหนดค่าคีย์ลงนาม DKIM บนเซิร์ฟเวอร์อีเมลขาออก และวิเคราะห์รายงานข้อเสนอแนะ DMARC แบบ XML ที่เข้ามาเพื่อระบุการละเมิด