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

# การหลอกลวงออนไลน์และวิศวกรรมสังคม คู่มือการป้องกัน

ฟิชชิงทางอีเมล โดเมนปลอม วิชชิง การหลอกลวงด้านการสนับสนุน การยืนยันนอกช่องทาง BEC

## ภาพรวมการเรียนรู้เรื่องการหลอกลวงออนไลน์

**ได้รับการรักษาความปลอดภัย**
**การเข้ารหัสข้อมูล**
มาตรฐาน AES 256 บิต

**เป็นไปตามข้อกำหนด**
**มาตรฐานสากล**
กรอบกฎหมาย GDPR และ CCPA

**ซีโร่ทรัสต์**
**นโยบายการเข้าถึง**
การยืนยันตัวตนหลายปัจจัย

**ยินดีต้อนรับ!** ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการป้องกันการหลอกลวงออนไลน์ คุณจะได้สำรวจเว็บไซต์ฟิชชิงปลอม กลวิธีวิศวกรรมสังคม การหลอกลวงด้านการสนับสนุน ช่องทางการฉ้อโกงทางการโอนเงิน และวิธีการตรวจสอบการชำระเงิน

**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/hlok-luang-ongkhan/

# เส้นทางการเรียนรู้การป้องกันการหลอกลวงออนไลน์ของคุณ

- ระบุตัวบ่งชี้ทั่วไปของการหลอกลวงด้านการสนับสนุนและโดเมนสะกดผิดเพื่อหลอกลวง
- ใช้โปรโตคอลการยืนยันอีเมล (SPF, DKIM, DMARC) เพื่อป้องกันการปลอมแปลง
- กำหนดการยืนยันธุรกรรมนอกช่องทางเพื่อป้องกันการฉ้อโกงโอนเงินทางธุรกิจ

### คำแนะนำคู่มือการหลอกลวงออนไลน์

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การป้องกันการหลอกลวงออนไลน์ ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

### การป้องกันการหลอกลวงออนไลน์และวิศวกรรมสังคม (บทนำ)

การหลอกลวงออนไลน์ใช้ประโยชน์จากพฤติกรรมมนุษย์ผ่านฟิชชิง ป๊อปอัปฝ่ายสนับสนุน วิชชิง และการฉ้อโกงทางการโอนเงิน การบังคับใช้การยืนยันธุรกรรมนอกช่องทางหลักและกฎโดเมน SPF/DKIM/DMARC ช่วยบล็อกช่องทางวิศวกรรมสังคมที่เกตเวย์ได้

**อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง**

## จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **1. ตัวบ่งชี้หลักของการหลอกลวงแบบแอบอ้างฝ่ายสนับสนุนคืออะไร?**
   - A. ป๊อปอัปที่อ้างว่าระบบของคุณติดไวรัสและเรียกร้องให้คุณโทรไปยังหมายเลขโทรศัพท์
   - B. การอัปเดตความปลอดภัยอัตโนมัติที่ดาวน์โหลดจากรีจิสทรีทางการ
   - C. ตัวจัดการรหัสผ่านที่ปฏิเสธการกรอกข้อมูลรับรองบนโดเมนขององค์กร
   - D. การสำรองไฟล์เบื้องหลังที่รันบนการกำหนดค่าไดรฟ์ภายนอก

2. **2. เทคนิคใดที่ใช้โดเมนผู้ส่งปลอมเพื่อขโมยรายละเอียดบัญชีธนาคาร?**
   - A. ฟิชชิงทางอีเมล
   - B. การสแกนพอร์ต
   - C. การฉีดหน่วยความจำ
   - D. การทำลายข้อมูลด้วยการเข้ารหัส

3. **3. อะไรแสดงถึงการฉ้อโกงการโอนเงิน?**
   - A. การหลอกให้เหยื่อโอนเงินไปยังบัญชีองค์กรปลอมโดยใช้วิศวกรรมสังคม
   - B. การเข้ารหัสฐานข้อมูลระบบด้วยเพย์โหลดแรนซัมแวร์
   - C. สืบค้นฐานข้อมูลด้วยคำสั่ง SQL injection
   - D. สำรองไฟล์ระบบไปยังดิสก์จัดเก็บข้อมูลแบบออฟไลน์

4. **4. เหตุใดมิจฉาชีพจึงสร้างเว็บไซต์ช้อปปิ้งปลอม?**
   - A. เพื่อขโมยรายละเอียดบัตรเครดิตและข้อมูลรับรองการชำระเงินจากผู้ซื้อ
   - B. เพื่อโฮสต์ตารางฐานข้อมูลวิเคราะห์มัลแวร์ในแซนด์บ็อกซ์
   - C. เพื่อเร่งการจัดส่งคำสั่งซื้อออนไลน์
   - D. เพื่อทดสอบการออกแบบเว็บไซต์ใหม่ฟรี

5. **5. วิชชิงหมายถึงอะไร?**
   - A. การหลอกลวงแบบฟิชชิงทางเสียงผ่านเครือข่ายโทรศัพท์เพื่อขโมยข้อมูลรับรอง
   - B. การสแกนเครือข่ายภายในเพื่อหาอุปกรณ์ระบบที่ไม่ปลอดภัย
   - C. กู้คืนฐานข้อมูลระบบหลังการละเมิดที่ไม่ได้รับอนุญาต
   - D. การรันโค้ดที่ไม่น่าเชื่อถือภายในคอนเทนเนอร์เสมือนที่ปลอดภัย

## จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

**6 คำถาม 6**

6. การหลอกลวงแบบฟิชชิงมุ่งเป้าเฉพาะผู้ใช้ปลายทาง ไม่เคยมุ่งเป้าผู้บริหารแบบ whaling

○ จริง ○ เท็จ

**7 คำถาม 7**

7. โดเมนปลอมมักใช้การพิมพ์ผิดเล็กน้อย (เช่น amaz0n.com) เพื่อเลียนแบบแบรนด์ที่เชื่อถือได้

○ จริง ○ เท็จ

**8 คำถาม 8**

8. การหลอกลวงด้านการสนับสนุนแก้ไขได้ด้วยการให้ผู้โทรเข้าถึงเครื่องจากระยะไกล

○ จริง ○ เท็จ

**9 คำถาม 9**

9. วิศวกรรมสังคมใช้จิตวิทยาของมนุษย์ เช่น ความกลัวและความเร่งด่วน เพื่อหลีกเลี่ยงกฎความปลอดภัย

○ จริง ○ เท็จ

**10 คำถาม 10**

10. ควรยืนยันคำขอโอนเงินทางไกลด้วยช่องทางการสื่อสารนอกช่องทางหลัก (out-of-band) เสมอ

○ จริง ○ เท็จ

## จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. อีเมลหลอกลวงที่ล่อให้ผู้ใช้หลงเชื่อเรียกว่า _____
2. ที่อยู่เว็บที่เลียนแบบแบรนด์ที่น่าเชื่อถือคือการ _____
3. การหลอกลวงทางเสียงที่มุ่งเป้าข้อมูลธนาคารเรียกว่า _____
4. ป๊อปอัปที่เรียกเงินเพื่อลบไวรัสคือการ _____ ปลอมฝ่ายสนับสนุน
5. การตรวจสอบความถูกต้องของคำขอชำระเงินต้องมีการ _____ นอกช่องทาง
6. การเปลี่ยนเส้นทางธุรกรรมธุรกิจไปยังบัญชีของโจรคือการ _____

**คลังคำศัพท์**

ปลอมแปลง | เปลี่ยนบัญชี | ฟิชชิง | ยืนยัน | วิชชิง | เวลลิง | สมิชชิง | หลอกลวง

**เขียนคำตอบของคุณที่นี่:**

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

# จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

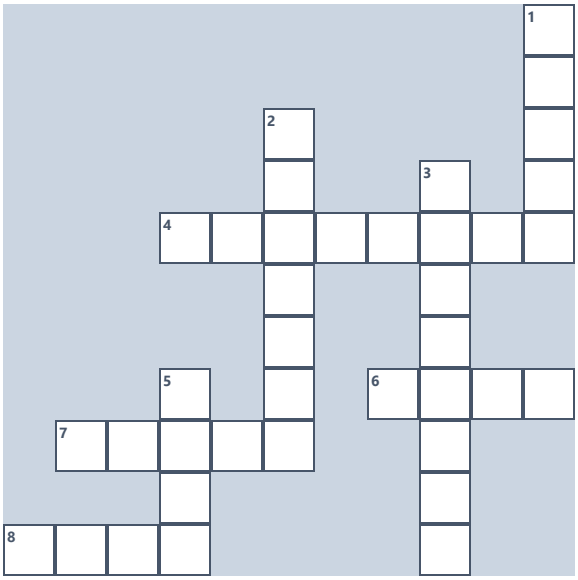
**การจับคู่คำนิยาม**

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

| | | | |
|---|---|---|---|
| ☐ | **1. ฟิชชิง** | **A** | การเปลี่ยนเส้นทางธุรกรรมธนาคารอย่างฉ้อฉลไปยังบัญชีของอาชญากร |
| ☐ | **2. ถูกปลอมแปลง** | **B** | แผนการหลอกลวงที่ออกแบบมาเพื่อขโมยเงินหรือข้อมูลเข้าสู่ระบบจากเหยื่อ |
| ☐ | **3. วิชชิง** | **C** | การส่งข้อความ SMS หลอกลวงเพื่อขโมยข้อมูลรับรองบัญชีมือถือ |
| ☐ | **4. การหลอกลวง** | **D** | การโทรด้วยเสียงหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลเข้าสู่ระบบและรายละเอียดบัญชี |
| ☐ | **5. การตรวจสอบยืนยัน** | **E** | การโจมตีฟิชชิงแบบเจาะจงเป้าหมายที่มุ่งขโมยข้อมูลรับรองจากผู้บริหารระดับ C |
| ☐ | **6. การโอนเงิน (Wire Transfer)** | **F** | ที่อยู่อีเมลผู้ส่งหรือเว็บไซต์ที่ลอกเลียนแบบเพื่อให้ดูน่าเชื่อถือ |
| ☐ | **7. ฟิชชิงล่าวาฬ** | **G** | แคมเปญอีเมลหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลเข้าสู่ระบบและรหัสผ่าน |
| ☐ | **8. สมิชชิง** | **H** | การยืนยันรายละเอียดการชำระเงินผ่านช่องทางติดต่อสำรองที่เชื่อถือได้ |

# จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



## แนวนอน

**4. ที่อยู่ผู้ส่งอีเมลหรือเว็บไซต์ที่เลียนแบบให้ดูน่าเชื่อถือ (8)**

**6. การตรวจสอบรายละเอียดการชำระเงินผ่านช่องทางติดต่อสำรองที่เชื่อถือได้ (4)**

**7. การส่งข้อความหลอกลวงเพื่อขโมยข้อมูลประจำตัวของบัญชีมือถือ (5)**

**8. การโทรด้วยเสียงหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลประจำตัวและรายละเอียดบัญชี (4)**

## แนวตั้ง

**1. การโจมตีฟิชชิงแบบเจาะจงเป้าหมายที่มุ่งขโมยข้อมูลประจำตัวของผู้บริหารระดับ C (5)**

**2. แผนการฉ้อโกงที่ออกแบบมาเพื่อขโมยเงินหรือสิทธิ์เข้าถึงข้อมูลประจำตัวจากเหยื่อ (7)**

**3. การเปลี่ยนเส้นทางธุรกรรมธนาคารไปยังบัญชีของอาชญากรอย่างหลอกลวง (8)**

**5. แคมเปญอีเมลหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลเข้าสู่ระบบและรหัสผ่าน (4)**

# จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

## แนวนอน

**4 แนวนอน: ที่อยู่ผู้ส่งอีเมลหรือเว็บไซต์ที่เลียนแบบให้ดูน่าเชื่อถือ (8 ตัวอักษร):**

**6 แนวนอน: การตรวจสอบรายละเอียดการชำระเงินผ่านช่องทางติดต่อสำรองที่เชื่อถือได้ (4 ตัวอักษร):**

**7 แนวนอน: การส่งข้อความหลอกลวงเพื่อขโมยข้อมูลประจำตัวของบัญชีมือถือ (5 ตัวอักษร):**

**8 แนวนอน: การโทรด้วยเสียงหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลประจำตัวและรายละเอียดบัญชี (4 ตัวอักษร):**

## แนวตั้ง

**1 แนวตั้ง: การโจมตีฟิชชิงแบบเจาะจงเป้าหมายที่มุ่งขโมยข้อมูลประจำตัวของผู้บริหารระดับ C (5 ตัวอักษร):**

**2 แนวตั้ง: แผนการฉ้อโกงที่ออกแบบมาเพื่อขโมยเงินหรือสิทธิ์เข้าถึงข้อมูลประจำตัวจากเหยื่อ (7 ตัวอักษร):**

**3 แนวตั้ง: การเปลี่ยนเส้นทางธุรกรรมธนาคารไปยังบัญชีของอาชญากรอย่างหลอกลวง (8 ตัวอักษร):**

**5 แนวตั้ง: แคมเปญอีเมลหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลเข้าสู่ระบบและรหัสผ่าน (4 ตัวอักษร):**

## จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า นี า น นี ส ช ฟิ มี ฟ บ า า ห นี
า ม กี จ า า รี ช เ ต ว ย ง ก ค
จ น ง ตี ว ร ตี ชิ ว ว า ล ล ด า
อ ย ชิ ช ฟ ก ก ง ล ม ล า ป อ อ
ม มี ช า ล ป ล ป จ า นี ลิ กี ส พ
ง ร วิ ง า ล ช เ า า ลี จ ง มิ ดี
ว า น ล ผ อ ดี ช ป ก ด า ต ช า
ล จ า ค ก ม ดี า ช ลิ่ ว ก ด ชิ กี
ก ด ท ผ ฟ แ ช มี ม อ ย ต ฟ ง ร
อ ดี า ท า ป ส ท ข ข า น น ก า
ล ล า ม ร ล มี า ร ช น ก บั ด ง
ห น ร ต สี ง ย ข มี ยั ดี ด ด ญ ว
บ ฟ อ า ร ห ห รี น น ผ นี ม ผ ชี
ดี ข กี ส บ ลี ง ยื ด ร ด ค ผ ห ดี
ป ร กี นี า ต จ ห ดี ด บ ตี น สี ลี

**รายการคำศัพท์**

ฟิชชิง ปลอมแปลง วิชชิง หลอกลวง ยืนยัน เปลี่ยนบัญชี เวลลิง สมิชชิง

# จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

**ศัพท์สำคัญ**

**A. ฟิชชิง**

**B. ปลอมแปลง**

**C. วิชชิง**

**D. หลอกลวง**

**E. ยืนยัน**

**F. เปลี่ยนบัญชี**

**G. เวลลิง**

**H. สมิชชิง**

**คำนิยามและช่องจับคู่**

1. ที่อยู่ผู้ส่งอีเมลหรือเว็บไซต์ที่เลียนแบบให้ดูน่าเชื่อถือ
2. การตรวจสอบรายละเอียดการชำระเงินผ่านช่องทางติดต่อสำรองที่เชื่อถือได้
3. การเปลี่ยนเส้นทางธุรกรรมธนาคารไปยังบัญชีของอาชญากรอย่างหลอกลวง
4. การส่งข้อความหลอกลวงเพื่อขโมยข้อมูลประจำตัวของบัญชีมือถือ
5. การโจมตีฟิชชิงแบบเจาะจงเป้าหมายที่มุ่งขโมยข้อมูลประจำตัวของผู้บริหารระดับ C
6. การโทรด้วยเสียงหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลประจำตัวและรายละเอียดบัญชี
7. แคมเปญอีเมลหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลเข้าสู่ระบบและรหัสผ่าน
8. แผนการฉ้อโกงที่ออกแบบมาเพื่อขโมยเงินหรือสิทธิ์เข้าถึงข้อมูลประจำตัวจากเหยื่อ

## จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ซิฟิงช _____
2. วิชิงช _____
3. นยียัน _____
4. ลงลิเว _____
5. แปลงมปลอ _____
6. วอลหกงล _____
7. เซินบัญปยลี่ _____
8. งสชซิมิ _____

# กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

| | | | | |
|---|---|---|---|---|
| 1 | อุปกรณ์ที่ถูกแฮกได้ | | | |
| 2 | วลีที่มิจฉาชีพมักใช้ | | | |
| 3 | วิธีชำระเงินที่มิจฉาชีพขอ | | | |
| 4 | ประเภทของการหลอกลวงออนไลน์ | | | |
| 5 | ข้อเสนอที่ดีเกินจริง | | | |
| 6 | สถานที่แจ้งเรื่องการหลอกลวง | | | |
| 7 | คำที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ | | | |
| 8 | บุคคลที่คุณเตือนเรื่องการหลอกลวงได้ | | | |
| 9 | สิ่งที่คุณสำรองข้อมูล | | | |
| 10 | สัญญาณเตือนในอีเมล | | | |
| 11 | สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ | | | |
| 12 | วิธีตรวจสอบร้านค้าออนไลน์ | | | |
| 13 | วิธีปกป้องบัญชีของคุณ | | | |
| 14 | สิ่งที่ควรทำหากคุณถูกหลอก | | | |
| 15 | สิ่งที่ควรทำหลังข้อมูลรั่วไหล | | | |

# จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

### กรณีศึกษาที่ 1: การป้องกันการหลอกให้โอนเงินในองค์กร



**สถานการณ์:** แผนกการเงินได้รับอีเมลด่วนจากที่อยู่ผู้ขายที่ถูกปลอมแปลง ขอให้โอนเงินตามใบแจ้งหนี้ในอนาคตไปยังหมายเลขบัญชีใหม่

**คำถามอภิปราย:** จงสรุปนโยบายการตรวจสอบการฉ้อโกงการโอนเงิน และระบุมาตรการยืนยันตัวตนของอีเมล

### กรณีศึกษาที่ 2: เหตุการณ์ฟิชชิงแบบเวลลิงต่อผู้บริหาร



**สถานการณ์:** ผู้บริหารคลิกลิงก์ฟิชชิงที่อ้างว่ามีเอกสารการประชุมคณะกรรมการที่ปลอดภัย และป้อนข้อมูลประจำตัวหลักขององค์กรบนพอร์ทัลปลอม

**คำถามอภิปราย:** จงอธิบายขั้นตอนการตอบสนองต่อเหตุการณ์โดยละเอียด และอธิบายวิธีตรวจสอบการเข้าสู่ระบบของผู้บริหาร

## 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 | | 31 | 51 | 10 | 10 | 51 | 7 | | 20 | 64 | 39 | 34 | |
| | | | | | | | | | | | | | | | | | | | |
| 1 | 49 | 35 | 42 | 58 | 1 | 25 | | 34 | 54 | 25 | 34 | 48 | 25 | | | | | | |
| | | | | | | | | | | | | | | | | | | | |

**ข้อความที่ถอดรหัสแล้ว:**

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

# จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

**Q1: การหลอกลวงออนไลน์คืออะไร?**

แผนการฉ้อโกงที่ใช้ช่องทางดิจิทัลหลอกให้เหยื่อโอนเงินหรือเปิดเผยข้อมูลรับรองส่วนบุคคล

**Q2: ตัวบ่งชี้หลักของอีเมลฟิชชิงคืออะไร?**

ข้อความที่อ้างว่าเร่งด่วน (เช่น บัญชีถูกระงับ) และนำคุณไปยังลิงก์ที่ไม่ตรงกับโดเมนอย่างเป็นทางการ

**Q3: typosquatting คืออะไร?**

การจดทะเบียนโดเมนที่สะกดผิดบ่อยของแบรนด์ยอดนิยม (เช่น amaz0n.com) เพื่อโฮสต์เว็บไซต์ฟิชชิงปลอม

**Q4: การหลอกให้ช่วยแก้ปัญหา (support scam) คืออะไร?**

ป๊อปอัปที่อ้างว่าพีซีของคุณติดไวรัส และให้คุณโทรไปยังหมายเลขหนึ่งและจ่ายเงินซื้อซอฟต์แวร์ทำความสะอาดปลอมหรือบริการเข้าถึงระยะไกล [1]

**Q5: vishing คืออะไร?**

การโจมตีแบบฟิชชิงที่ใช้โทรศัพท์เสียงหลอกให้เหยื่อให้ข้อมูลบัญชีธนาคารหรือข้อมูลเข้าสู่ระบบ

# จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

**Q6: การฉ้อโกงทางสายโทรเลขหรือการโอนเงิน (wire fraud) หมายความว่าอะไร?**

การเปลี่ยนเส้นทางธุรกรรมการชำระเงินไปยังบัญชีหลอกลวงโดยแอบอ้างเป็นผู้ขายหรือผู้บริหาร

**Q7: whaling คืออะไร?**

ฟิชชิงแบบเจาะจงเป้าหมายสูงรูปแบบหนึ่ง ที่มุ่งเป้าไปยังบุคคลมูลค่าสูงโดยตรง เช่น ผู้บริหารระดับ C ขององค์กร

**Q8: smishing คืออะไร?**

ข้อความหลอกลวงที่ส่งไปยังอุปกรณ์มือถือ มีลิงก์ที่ชวนให้ไปยังพอร์ทัลปลอมหรือการอัปเดตการติดตามพัสดุ

**Q9: ทำไมการยืนยันนอกช่องทาง (out-of-band) จึงสำคัญยิ่ง?**

ยืนยันรายละเอียดธุรกรรมผ่านช่องทางสื่อสารแยกต่างหาก (เช่น การโทรศัพท์) หลีกเลี่ยงกระทู้อีเมลที่ถูกบุกรุก

**Q10: การหลอกลวงเอสโครว์ปลอมทำงานอย่างไร?**

มิจฉาชีพสร้างเว็บไซต์เอสโครว์ปลอมโดยอ้างว่าเก็บเงินไว้อย่างปลอดภัย แล้วขโมยเงินที่ผู้ซื้อโอนมัดจำ

# จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

**Q1: มิจฉาชีพใช้ BEC (Business Email Compromise) ทำการฉ้อโกงทางการโอนเงินได้อย่างไร?**

ยึดบัญชีอีเมลของพนักงานที่ถูกต้อง เฝ้าดูเธรดใบแจ้งหนี้ และส่งรายละเอียดการเรียกเก็บเงินที่อัปเดตพร้อมบัญชีธนาคารหลอกลวง

**Q2: ความเสี่ยงของการโจมตีแบบ IDN homograph ในการหลอกลวงออนไลน์คืออะไร?**

การใช้อักขระที่ไม่ใช่ ASCII ซึ่งดูเหมือนตัวอักษรปกติทุกประการ (เช่น 'а' ซีริลลิก) เพื่อจดทะเบียนโดเมนปลอมที่เลียนแบบแบรนด์จริง

**Q3: เหตุใดการตรวจสอบส่วนหัวอีเมลจึงสำคัญในการตรวจจับการหลอกลวง?**

เผยที่อยู่ IP ของเซิร์ฟเวอร์ต้นทางจริงและสถานะการตรวจสอบ SPF/DKIM แสดงให้เห็นว่าโดเมนผู้ส่งถูกปลอมหรือไม่

**Q4: มิจฉาชีพหลอกให้ช่วยแก้ปัญหา (support scam) ใช้ซอฟต์แวร์รีโมตเดสก์ท็อปในทางมิชอบอย่างไร?**

ใช้ยูทิลิตี เช่น AnyDesk หรือ TeamViewer เชื่อมต่อกับอุปกรณ์ของเหยื่อ ฝังมัลแวร์ และขโมยรหัสผ่านที่บันทึกไว้

**Q5: เป้าหมายของการหลอกลวงแบบเก็บเงินล่วงหน้า (advance-fee scam) คืออะไร?**

หลอกให้เหยื่อจ่ายค่าธรรมเนียมดำเนินการล่วงหน้าเพื่อแลกกับรางวัลทางการเงินก้อนใหญ่ที่ไม่มีอยู่จริง

# จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

### Q6: มิจฉาชีพใช้การทำโปรไฟล์จากโซเชียลมีเดียเพื่อฟิชชิงแบบเจาะจงเป้าหมายอย่างไร?

รวบรวมโครงสร้างองค์กรและรายชื่อพนักงานเพื่อร่างอีเมลสเปียร์ฟิชชิงที่น่าเชื่อถือ

### Q7: ทำไมเว็บช็อปปลอมจึงเสนอส่วนลดสูงมาก?

เพื่อหลอกให้ผู้ซื้อกรอกรายละเอียดบัตรเครดิต และเก็บข้อมูลรับรองไปใช้ซ้ำหรือขายต่อในฟอรัมขโมยบัตร

### Q8: เรคอร์ด DMARC บล็อกการหลอกลวงแบบฟิชชิงได้อย่างไร?

DMARC ช่วยให้เจ้าของโดเมนขอให้ผู้รับกักกันหรือปฏิเสธอีเมลที่ไม่ผ่านการตรวจสอบ SPF และ DKIM ที่สอดคล้องกัน เพื่อบล็อกการปลอมแปลงโดยตรง [5]

### Q9: ภัยคุกคามจากพอร์ทัลเก็บข้อมูลรับรอง (credential harvesting) คืออะไร?

หน้าเข้าสู่ระบบปลอมที่ออกแบบให้เหมือน Microsoft 365 หรือ Google workspace ทุกประการ เพื่อขโมยข้อมูลเข้าสู่ระบบขณะที่ผู้ใช้กรอก

### Q10: ทีมรักษาความปลอดภัยรายงานและปิดโดเมนหลอกลวงได้อย่างไร?

ด้วยการส่งหลักฐานการฉ้อโกงไปยังอีเมลรับแจ้งการละเมิดของผู้รับจดทะเบียน ผู้ให้บริการโฮสติ้ง และทะเบียน Google Safe Browsing

# ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

**1. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

ฟิชชิงและการปลอมแปลงเป็นอาชญากรรมประเภทที่มีผู้แจ้งต่อ IC3 ของ FBI มากที่สุดในปี 2025 โดยมี 191,561 เรื่อง [2]

**2. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

การโจรกรรมทางอีเมลธุรกิจ (BEC) ก่อให้เกิดความสูญเสียกว่า 3 พันล้านดอลลาร์ที่รายงานต่อ IC3 ของ FBI ในปี 2025 [2]

**3. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

โดเมนที่สะกดผิดเลียนแบบต่างจากชื่อแบรนด์จริงเพียงหนึ่งหรือสองตัวอักษร จึงอาจมองพลาดได้หากดูผ่านๆ

**4. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

การหลอกลวงด้านการสนับสนุนทางเทคนิคก่อให้เกิดความสูญเสียกว่า 2.1 พันล้านดอลลาร์ที่รายงานต่อ IC3 ของ FBI ในปี 2025 [2]

**5. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

การโจมตีแบบ Homograph มีลักษณะเหมือนกันทุกประการในแถบที่อยู่ของเบราว์เซอร์ เว้นแต่เบราว์เซอร์จะแสดงการกำหนดค่า punycode

**6. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

การหลอกลวงทางข้อความ SMS (สมิชชิง) ใช้ข้อความสั้นเร่งด่วนพร้อมลิงก์ ทำให้เหยื่อมีบริบทน้อยในการสังเกตการฉ้อโกง

**7. ข้อมูลเชิงลึกด้านความปลอดภัย**

การโจมตีแบบฟิชชิงล่าวาฬมุ่งเป้าไปที่อีเมลของผู้บริหารเพราะพวกเขาควบคุมการเข้าถึงการโอนเงินจำนวนมาก

**8. ข้อมูลเชิงลึกด้านความปลอดภัย**

การตรวจสอบการเปลี่ยนแปลงการชำระเงินโดยโทรไปยังหมายเลขโทรศัพท์ที่ทราบและบันทึกไว้เป็นการป้องกันหลักต่อการฉ้อโกงโอนเงิน BEC

**9. ข้อมูลเชิงลึกด้านความปลอดภัย**

เว็บไซต์เอสโครว์ปลอมเป็นการหลอกลวงที่พบบ่อยในตลาดออนไลน์ โดยดูเหมือนบริการชำระเงินที่ปลอดภัยแต่ขโมยเงินโอนของผู้ซื้อ

**10. ข้อมูลเชิงลึกเรื่องความปลอดภัย**

Google Safe Browsing เตือนผู้ใช้ก่อนเปิดเว็บไซต์ที่ถูกระบุว่าเป็นฟิชชิงหรือมัลแวร์

# แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

## เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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

## เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

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

### หมายเหตุสำหรับผู้สอน

ตัวบ่งชี้หลักของการหลอกลวงแบบแอบอ้างฝ่ายสนับสนุนคืออะไร? → ป๊อปอัปที่อ้างว่าระบบของคุณติดไวรัสและเรียกร้องให้คุณโทรไปยังหมายเลขโทรศัพท์

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

### หมายเหตุสำหรับผู้สอน

เทคนิคใดที่ใช้โดเมนผู้ส่งปลอมเพื่อขโมยรายละเอียดบัญชีธนาคาร? → ฟิชชิงทางอีเมล

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

### หมายเหตุสำหรับผู้สอน

อะไรแสดงถึงการฉ้อโกงการโอนเงิน? → การหลอกให้เหยื่อโอนเงินไปยังบัญชีของค์กรปลอมโดยใช้วิศวกรรมสังคม

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

### หมายเหตุสำหรับผู้สอน

เหตุใดมิจฉาชีพจึงสร้างเว็บไซต์ช้อปปิ้งปลอม? → เพื่อขโมยรายละเอียดบัตรเครดิตและข้อมูลรับรองการชำระเงินจากผู้ซื้อ

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

### หมายเหตุสำหรับผู้สอน

วิชชิงหมายถึงอะไร? → การหลอกลวงแบบฟิชชิงทางเสียงผ่านเครือข่ายโทรศัพท์เพื่อขโมยข้อมูลรับรอง

## เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

**6 คำถาม 6** — คำตอบที่ถูกต้อง: เท็จ

### หมายเหตุสำหรับผู้สอน

เท็จ: ฟิชชิงยังมุ่งเป้าผู้บริหารด้วย การโจมตีแบบ whaling คือฟิชชิงที่มุ่งเป้าผู้นำระดับสูง

**7 คำถาม 7** — คำตอบที่ถูกต้อง: จริง

### หมายเหตุสำหรับผู้สอน

โดเมนปลอมมักใช้การพิมพ์ผิดเล็กน้อย (เช่น amaz0n.com) เพื่อเลียนแบบแบรนด์ที่เชื่อถือได้

**8 คำถาม 8** — คำตอบที่ถูกต้อง: เท็จ

### หมายเหตุสำหรับผู้สอน

เท็จ: การให้มิจฉาชีพที่แอบอ้างฝ่ายสนับสนุนเข้าถึงจากระยะไกลทำให้พวกเขาฝังมัลแวร์และขโมยข้อมูลได้

**9 คำถาม 9** — คำตอบที่ถูกต้อง: จริง

### หมายเหตุสำหรับผู้สอน

วิศวกรรมสังคมใช้จิตวิทยาของมนุษย์ เช่น ความกลัวและความเร่งด่วน เพื่อหลีกเลี่ยงกฎความปลอดภัย

**10 คำถาม 10** — คำตอบที่ถูกต้อง: จริง

### หมายเหตุสำหรับผู้สอน

ควรยืนยันคำขอโอนเงินทางไกลด้วยช่องทางการสื่อสารนอกช่องทางหลัก (out-of-band) เสมอ

# เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

## จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

| | | | |
|---|---|---|---|
| G 1. ฟิชชิง | F 2. ถูกปลอมแปลง | D 3. วิชชิง | B 4. การหลอกลวง |
| H 5. การตรวจสอบยืนยัน | A 6. การโอนเงิน (Wire Transfer) | E 7. ฟิชชิงล่าวาฬ | C 8. สมิชชิง |

## จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

| | | | |
|---|---|---|---|
| 1 ฟิชชิง | 2 ปลอมแปลง | 3 วิชชิง | 4 หลอกลวง |
| 5 ยืนยัน | 6 เปลี่ยนบัญชี | | |

## จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

| | | | |
|---|---|---|---|
| 1 B – ปลอมแปลง | 2 E – ยืนยัน | 3 F – เปลี่ยนบัญชี | 4 H – สมิชชิง |
| 5 G – เวลลิง | 6 C – วิชชิง | 7 A – ฟิชชิง | 8 D – หลอกลวง |

### หมายเหตุการอภิปรายสำหรับผู้สอน

**คำศัพท์สำคัญ:**
ตรวจสอบว่าผู้เรียนอธิบาย ฟิชชิง ถูกปลอมแปลง และ วิชชิง ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

**กรณีศึกษา:**
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

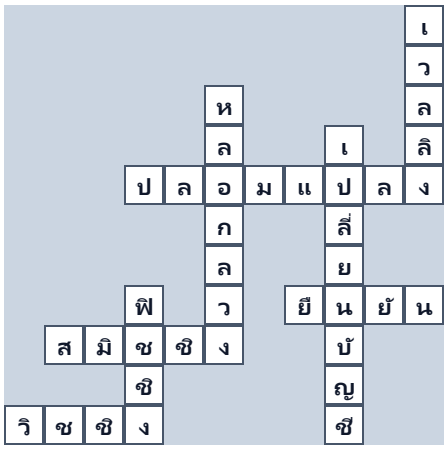
**การประเมินแหล่งข้อมูล:**
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

# เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

## เฉลยการค้นหาคำศัพท์

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| า | นี | า | น | นี | ส | ช | ฟิ | มี | ฟ | บ | า | า | ห | นี |
| า | ม | กี | จ | า | า | รี | ช | เ | ต | ว | ย | ง | ก | ค |
| จ | น | ง | ดี | ว | ร | ตี | ชิ | ว | ว | า | ล | ล | ด | า |
| อ | ย | ชิ | ช | ฟ | ก | ก | ง | ล | ม | ล | า | ป | อ | อ |
| ม | มี | ช | า | ล | ป | ล | ป | จ | า | นี | ลิ | กี | ส | พ |
| ง | ร | วิ | ง | า | ล | ช | เ | า | า | ลี | จ | ง | มิ | ดี |
| ว | า | น | ล | ผ | อ | ดี | ช | ป | ก | ด | า | ต | ช | า |
| ล | จ | า | ค | ก | ม | ดี | า | ช | ลี่ | ว | ก | ด | ชิ | กี |
| ก | ด | ท | ผ | ฟ | แ | ช | มี | ม | อ | ย | ต | ฟ | ง | ร |
| อ | ดี | า | ท | า | ป | ส | ท | ข | ข | า | น | น | ก | า |
| ล | ล | า | ม | ร | ล | มี | า | ร | ช | น | ก | บั | ด | ง |
| ห | น | ร | ต | สี | ง | ย | ข | มี | ยั | ดี | ด | ด | ญ | ว |
| บ | ฟ | อ | า | ร | ห | ห | รี | น | น | ผ | นี | ม | ผ | ชี |
| ดี | ข | กี | ส | บ | ลี | ง | ยี | ด | ร | ต | ค | ผ | ห | ดี |
| ป | ร | กี | นี | า | ต | จ | ห | ดี | ด | บ | ตี | น | สี | ลี |

## เฉลยปริศนาอักษรไขว้




## คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

### แนวนอน

**4 แนวนอน: ปลอมแปลง** ที่อยู่ผู้ส่งอีเมลหรือเว็บไซต์ที่เลียนแบบให้ดูน่าเชื่อถือ (8 ตัวอักษร)

**6 แนวนอน: ยืนยัน** การตรวจสอบรายละเอียดการชำระเงินผ่านช่องทางติดต่อสำรองที่เชื่อถือได้ (4 ตัวอักษร)

**7 แนวนอน: สมิชชิง** การส่งข้อความหลอกลวงเพื่อขโมยข้อมูลประจำตัวของบัญชีมือถือ (5 ตัวอักษร)

**8 แนวนอน: วิชชิง** การโทรด้วยเสียงหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลประจำตัวและรายละเอียดบัญชี (4 ตัวอักษร)

### แนวตั้ง

**1 แนวตั้ง: เวลลิง** การโจมตีฟิชชิงแบบเจาะจงเป้าหมายที่มุ่งขโมยข้อมูลประจำตัวของผู้บริหารระดับ C (5 ตัวอักษร)

**2 แนวตั้ง: หลอกลวง** แผนการฉ้อโกงที่ออกแบบมาเพื่อขโมยเงินหรือสิทธิ์เข้าถึงข้อมูลประจำตัวจากเหยื่อ (7 ตัวอักษร)

**3 แนวตั้ง: เปลี่ยนบัญชี** การเปลี่ยนเส้นทางธุรกรรมธนาคารไปยังบัญชีของอาชญากรอย่างหลอกลวง (8 ตัวอักษร)

**5 แนวตั้ง: ฟิชชิง** แคมเปญอีเมลหลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลเข้าสู่ระบบและรหัสผ่าน (4 ตัวอักษร)

# เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

## เฉลยการเรียงคำที่สลับตัวอักษร

1. ชิฟิงช → ฟิชชิง
2. วิชิงช → วิชชิง
3. นยียัน → ยืนยัน
4. ลงลิเว → เวลลิง
5. แปลงมปลอ → ปลอมแปลง
6. วอลหกงล → หลอกลวง
7. เซินบัญปยลี่ → เปลี่ยนบัญชี
8. งสชชิมิ → สมิชชิง

### เฉลยภารกิจรหัสลับ

**"ตรวจจับ ฟิชชิง ด้วย การสแกน ยืนยัน"**

# เฉลยกรณีศึกษา

## A กรณีศึกษาที่ 1: การป้องกันการหลอกให้โอนเงินในองค์กร

เฉลยสำหรับผู้สอน

**แนวทางการให้คะแนน**

**คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:**

- การวิเคราะห์สถานการณ์: ฝ่ายการเงินได้รับอีเมลด่วนจากที่อยู่ผู้ขายปลอม ขอให้โอนเงินใบแจ้งหนี้ในอนาคตไปยังเลขที่เส้นทางโอนเงินใหม่
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: บังคับใช้นโยบายการอนุมัติสองชั้นสำหรับการชำระเงินทุกรายการ ใช้การยืนยันนอกช่องทางหลักผ่านหมายเลขโทรศัพท์ที่บันทึกไว้ล่วงหน้า และบล็อกอีเมลจากโดเมนปลอมที่เกตเวย์

## B กรณีศึกษาที่ 2: เหตุการณ์ฟิชชิงแบบเวลลิงต่อผู้บริหาร

เฉลยสำหรับผู้สอน

**แนวทางการให้คะแนน**

**คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:**

- การวิเคราะห์สถานการณ์: ผู้บริหารคลิกลิงก์ฟิชชิงที่อ้างว่ามีเอกสารการประชุมบอร์ดที่ปลอดภัย แล้วกรอกข้อมูลเข้าสู่ระบบหลักขององค์กรบนพอร์ทัลปลอม
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: แยกอุปกรณ์ของผู้บริหาร รีเซ็ตโทเค็นเซสชันและข้อมูลรับรององค์กรทั้งหมด ตรวจสอบบันทึกการเข้าถึงว่ามีข้อมูลรั่วไหลออกหรือไม่ และใช้ MFA แบบฮาร์ดแวร์กับการเข้าสู่ระบบทั้งหมด