ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

การป้องกันการโจรกรรมข้อมูลประจำตัวและทรัพย์สิน คู่มือความปลอดภัย

ข้อมูลรับรองรั่วไหล MFA การเฝ้าระวังดาร์กเว็บ การแจ้งเตือนการแซ่แช็งเครดิต วิศวกรรมสังคม

ภาพรวมการเรียนรู้การป้องกันการโจรกรรมข้อมูลประจำตัว

ได้รับการรักษาความปลอดภัย
การเข้ารหัสข้อมูล
มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด
มาตรฐานสากล
กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์
นโยบายการเข้าถึง
การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการป้องกันและลดผลกระทบจากการขโมยข้อมูลระบุตัวตน คุณจะได้สำรวจการรั่วไหลของข้อมูลรับรอง การพิสูจน์ตัวตนหลายปัจจัย การเฝ้าติดตามดาร์กเว็บ การแจ้งเตือนการอายัดเครดิต และการป้องกันวิศวกรรมสังคม

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-luak-lon-tatua/

เส้นทางการเรียนรู้การปกป้องข้อมูลระบุตัวตนของคุณ

- ทำความเข้าใจความเสี่ยงของการเปิดเผยข้อมูลรับรองบนฟอรัมดาร์กเว็บ
- ใช้การยืนยันตัวตนหลายปัจจัย (MFA) และการแจ้งเตือนการอายัดเครดิต
- ออกแบบการป้องกันความปลอดภัยขององค์กรจากการหลอกลวงด้วยวิศวกรรมสังคมแบบเจาะจงเป้าหมาย

คำแนะนำคู่มือการโจรกรรมข้อมูลประจำตัว

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การปกป้องอัตลักษณ์ ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การป้องกันการโจรกรรมข้อมูลประจำตัวและความปลอดภัยของทรัพย์สิน (บทนำ)

การโจรกรรมข้อมูลประจำตัวอาศัยข้อมูลเข้าสู่ระบบที่รั่วไหลและการล็อกอินที่อ่อนแอเพื่อยึดบัญชีส่วนบุคคลและขององค์กร การใช้ MFA การอายัดเครดิต เครื่องมือสแกนดาร์กเว็บ และกรอบงาน SPF/DKIM/DMARC เป็นการป้องกันที่สำคัญต่อการแอบอ้างตัวตนทางดิจิทัล

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1 **1. วิธีหลักที่โจรขโมยตัวตนใช้ขโมยข้อมูลเข้าสู่ระบบคืออะไร?**

- A. การส่งการแจ้งเตือนทางอีเมลปลอมเพื่อหลอกให้ผู้ใช้กรอกรหัสผ่านบนพอร์ทัลปลอม
- B. การฟังการกระจายเสียงทางวิทยุใกล้สำนักงานองค์กรของผู้ใช้
- C. การจัดเรียงข้อมูลบนไดรฟ์จัดเก็บเซิร์ฟเวอร์ภายในของผู้ใช้
- D. การตัดการเชื่อมต่อการกำหนดค่าสำรองข้อมูลเครือข่ายภายนอก

2 **2. มาตรการควบคุมความปลอดภัยใดที่ให้การป้องกันที่แข็งแกร่งที่สุดต่อการรั่วไหลของข้อมูลเข้าสู่ระบบ?**

- A. การยืนยันตัวตนหลายปัจจัยโดยใช้คีย์ฮาร์ดแวร์
- B. การสร้างรหัสผ่านยาวโดยใช้รูปแบบเริ่มต้นของเบราว์เซอร์
- C. การเปลี่ยนชื่อผู้ใช้อีเมลทุกหกเดือน
- D. การลบประวัติการติดตามคุกกี้ที่เก็บไว้ในเบราว์เซอร์

3 **3. อะไรแสดงถึงการอายัดเครดิต?**

- A. การล็อกรายงานเครดิตเพื่อป้องกันโจรเปิดสินเชื่อโดยไม่ได้รับอนุญาต
- B. การลบประวัติธุรกรรมบัญชีธนาคารออกจากฐานข้อมูล
- C. การปิดเครื่องอ่านรูดแถบแม่เหล็กบัตรเครดิตบนสแกนเนอร์
- D. การเข้ารหัสฮาร์ดไดรฟ์ฐานข้อมูลในเครื่องขณะจัดเก็บ

4 **4. เหตุใดการเฝ้าระวังดาร์กเว็บจึงมีประโยชน์?**

- A. แจ้งเตือนผู้ใช้หากข้อมูลรับรองที่รั่วไหลของตนปรากฏในฐานข้อมูลผิดกฎหมาย
- B. ป้องกันมัลแวร์ที่ทำงานอยู่ไม่ให้รันในแซนด์บ็อกซ์เสมือน
- C. ช่วยเร่งความเร็วการกำหนดเส้นทางของเบราว์เซอร์บนเครือข่ายเสมือน
- D. บล็อกความพยายามเข้าถึงฐานข้อมูลแบ็กเอนด์ด้วย **SQL injection**

5 **5. วิศวกรรมสังคมหมายถึงอะไร?**

- A. การบงการผู้คนให้เปิดเผยข้อมูลรับรองที่เป็นความลับด้วยความสมัครใจ
- B. การสแกนพอร์ตเซิร์ฟเวอร์ขององค์กรเพื่อหาช่องโหว่ด้านความปลอดภัยที่กำลังถูกใช้
- C. การสำรองไฟล์ฐานข้อมูลระบบไปยังฮาร์ดไดรฟ์ออฟไลน์
- D. การกำหนดเส้นทางแพ็กเก็ตเครือข่ายผ่านโหนด **onion** ที่เข้ารหัสสามโหนด

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. การโจรกรรมข้อมูลประจำตัวส่งผลกระทบเฉพาะบัญชีดิจิทัลออนไลน์ ไม่ใช่จดหมายทางไปรษณีย์จริง

- ○ จริง
- ○ เท็จ

7 คำถาม 7

7. การบังคับใช้ MFA กับบัญชีส่วนตัวทั้งหมดบล็อกการโจมตีด้วยบอตแบบ credential stuffing ได้เป็นส่วนใหญ่

- ○ จริง
- ○ เท็จ

8 คำถาม 8

8. การอายัดเครดิตบล็อกการตรวจสอบเครดิต แต่ทำให้คุณเข้าถึงบัญชีธนาคารของตนเองไม่ได้

- ○ จริง
- ○ เท็จ

9 คำถาม 9

9. ตัวจัดการรหัสผ่านปกป้องผู้ใช้จากฟิชชิงด้วยการปฏิเสธกรอกรหัสผ่านอัตโนมัติบนโดเมนปลอม

- ○ จริง
- ○ เท็จ

10 คำถาม 10

10. อีเมลฟิชชิงมักใช้ถ้อยคำเร่งด่วนเพื่อกระตุ้นการตอบสนองทางอารมณ์ที่รวดเร็ว

- ○ จริง
- ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. มิจฉาชีพฟิชชิงมุ่งเป้าไปที่รหัสผ่านส่วนบุคคลและ _____ ของผู้ใช้
2. การแจ้งเตือนผู้ใช้เรื่องฐานข้อมูลถูกละเมิดช่วยระบุ _____ ของบัญชีส่วนตัว
3. การกำหนดให้ใช้รหัสชั่วคราวเพื่อเข้าสู่ระบบเรียกว่า _____
4. การสแกนฟอรัมแฮกเกอร์เพื่อหาข้อมูลที่ถูกขโมยคือการ _____ ดาร์กเว็บ
5. การบล็อกการตรวจสอบเครดิตโดยไม่ได้รับอนุญาตต้องมีการ _____ เครดิต
6. การฝึกพนักงานให้ตระหนักเรื่องฟิชชิงสร้าง _____ ด้านความปลอดภัยเชิงรุก

คลังคำศัพท์

การป้องกัน | ข้อมูลประจำตัว | เฝ้าระวัง | ฟิชชิง | รั่วไหล | สปูฟฟิง | อายัด | เอ็มเอฟเอ

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

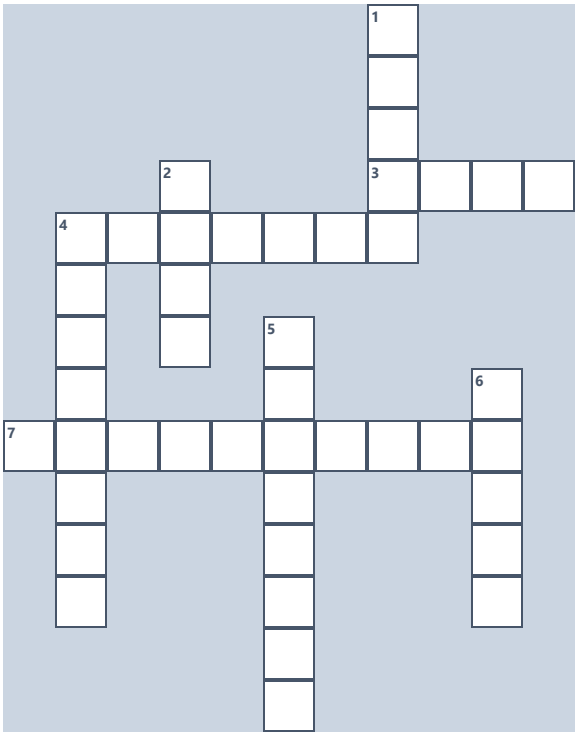
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. ข้อมูลรับรอง**	**A**	ขั้นตอนการยืนยันตัวตนขั้นที่สอง (เช่น กุญแจฮาร์ดแวร์) ที่ปกป้องการเข้าสู่ระบบบัญชี
☐	**2. การรั่วไหล**	**B**	การสร้างเว็บไซต์หรืออีเมลปลอมเพื่อเลียนแบบองค์กรที่ถูกต้อง
☐	**3. MFA**	**C**	การจำกัดการเข้าถึงแฟ้มเครดิตเพื่อป้องกันการยื่นขอสินเชื่ออันเป็นการฉ้อโกง
☐	**4. การตรวจสอบ**	**D**	การเปิดเผยฐานข้อมูลส่วนตัวที่มีระเบียนข้อมูลส่วนบุคคลของผู้ใช้โดยไม่ได้รับอนุญาต
☐	**5. การแซ่แซ็ง**	**E**	การฝึกอบรมและมาตรการทางเทคนิคที่ใช้ป้องกันการขโมยข้อมูลประจำตัว
☐	**6. การป้องกัน**	**F**	การส่งข้อความหลอกลวงเพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูลรับรอง
☐	**7. การปลอมแปลง**	**G**	การสแกนฟอรัมออนไลน์และช่องทางแฮกเกอร์เพื่อหาข้อมูลองค์กรที่ถูกขโมย
☐	**8. ฟิชชิง**	**H**	ชื่อผู้ใช้ รหัสผ่าน และโทเค็นส่วนตัวที่ใช้ยืนยันตัวตนดิจิทัล

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

3. การส่งข้อความหลอกลวงเพื่อล่อให้ผู้ใช้ให้ข้อมูลประจำตัว (4)

4. การสแกนเว็บบอร์ดและช่องทางของแฮกเกอร์เพื่อหาข้อมูลองค์กรที่ถูกขโมย (7)

7. ชื่อผู้ใช้ รหัสผ่าน และโทเค็นส่วนตัวที่ใช้ยืนยันตัวตนดิจิทัล (10)

แนวตั้ง

1. การสร้างเว็บไซต์หรืออีเมลปลอมเพื่อเลียนแบบองค์กรที่ถูกต้อง (5)

2. การจำกัดการเข้าถึงแฟ้มเครดิตเพื่อป้องกันการยื่นกู้เงินโดยทุจริต (4)

4. ขั้นตอนยืนยันตัวตนเพิ่มเติม (เช่น กุญแจฮาร์ดแวร์) ที่ปกป้องการเข้าสู่ระบบบัญชี (8)

5. การฝึกอบรมและมาตรการทางเทคนิคที่ใช้ป้องกันการขโมยข้อมูลประจำตัว (8)

6. การเปิดเผยฐานข้อมูลส่วนตัวที่มีบันทึกข้อมูลส่วนบุคคลของผู้ใช้โดยไม่ได้รับอนุญาต (5)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

3 แนวนอน: การส่งข้อความหลอกลวงเพื่อล่อให้ผู้ใช้ให้ข้อมูลประจำตัว (4 ตัวอักษร):

4 แนวนอน: การสแกนเว็บบอร์ดและช่องทางของแฮกเกอร์เพื่อหาข้อมูลองค์กรที่ถูกขโมย (7 ตัวอักษร):

7 แนวนอน: ชื่อผู้ใช้ รหัสผ่าน และโทเค็นส่วนตัวที่ใช้ยืนยันตัวตนดิจิทัล (10 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: การสร้างเว็บไซต์หรืออีเมลปลอมเพื่อเลียนแบบองค์กรที่ถูกต้อง (5 ตัวอักษร):

2 แนวตั้ง: การจำกัดการเข้าถึงแฟ้มเครดิตเพื่อป้องกันการยื่นกู้เงินโดยทุจริต (4 ตัวอักษร):

4 แนวตั้ง: ขั้นตอนยืนยันตัวตนเพิ่มเติม (เช่น กุญแจฮาร์ดแวร์) ที่ปกป้องการเข้าสู่ระบบบัญชี (8 ตัวอักษร):

5 แนวตั้ง: การฝึกอบรมและมาตรการทางเทคนิคที่ใช้ป้องกันการขโมยข้อมูลประจำตัว (8 ตัวอักษร):

6 แนวตั้ง: การเปิดเผยฐานข้อมูลส่วนตัวที่มีบันทึกข้อมูลส่วนบุคคลของผู้ใช้โดยไม่ได้รับอนุญาต (5 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า นี า น นี ส ช รั่ มี ฟ บ า า ห นี
า ม กี จ า า รี ว เ ต ว ย ง ก ค
จ น ด ตี ว ร ตี ไ ว ฝ า ล ล ด า
อ ย ยั ช ฟ ก ก ห ล ม า า ป อ อ
น ม า มี า ข้ ล ล ล ป ส ร จ า นี
กั กี อ พ ร อ ง เ า ซ า ปู ะ า ลี
ง จ ดี า น มู ล ผ อ็ ดี ซ ก ฟ วั ด
อ า ต า จ ล า ค ก ม ดี า ช ฟิ ง
ป้ ว ก ด กี ป ด ท ผ ฟ เ ซ มี ม ง
ร อ ต ฟ ร ร ดี า ท า ส อ ท ข ข
า า น ก า ะ ล า ม ร ง มี ฟ า ร
ก ช ก ด ง จำ น ร ต ชิ สี ย ข เ มี
ดี ด ด ว บ ตั ฟ อ ช า ร ห ห รี อ
น ผ นี ม ผ ว ดี ฟิ ข กี ส บ ลี ง ด
ร ด ค ผ ห ดี ป ร กี นี า ต จ ห ดี

รายการคำศัพท์

ข้อมูลประจำตัว | รั่วไหล | เอ็มเอฟเอ | เฝ้าระวัง | อายัด | การป้องกัน | สปูฟฟิง | ฟิชชิง

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. ข้อมูลประจำตัว

B. รั่วไหล

C. เอ็มเอฟเอ

D. เฝ้าระวัง

E. อายัด

F. การป้องกัน

G. สปูฟฟิง

H. ฟิชชิง

คำนิยามและช่องจับคู่

1. การส่งข้อความหลอกลวงเพื่อล่อให้ผู้ใช้ให้ข้อมูลประจำตัว
2. ชื่อผู้ใช้ รหัสผ่าน และโทเค็นส่วนตัวที่ใช้ยืนยันตัวตนดิจิทัล
3. การสร้างเว็บไซต์หรืออีเมลปลอมเพื่อเลียนแบบองค์กรที่ถูกต้อง
4. การฝึกอบรมและมาตรการทางเทคนิคที่ใช้ป้องกันการขโมยข้อมูลประจำตัว
5. การสแกนเว็บบอร์ดและช่องทางของแฮกเกอร์เพื่อหาข้อมูลองค์กรที่ถูกขโมย
6. การจำกัดการเข้าถึงแฟ้มเครดิตเพื่อป้องกันการยื่นกู้เงินโดยทุจริต
7. การเปิดเผยฐานข้อมูลส่วนตัวที่มีบันทึกข้อมูลส่วนบุคคลของผู้ใช้โดยไม่ได้รับอนุญาต
8. ขั้นตอนยืนยันตัวตนเพิ่มเติม (เช่น กุญแจฮาร์ดแวร์) ที่ปกป้องการเข้าสู่ระบบบัญชี

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ตัะรปอข้จำวลมู
2. เเออ็เฟอม
3. ดอย้า
4. ฟงฟิสปู
5. ไลรั่หว
6. ว้าะเรงฝ้
7. กนองก้าป้ร
8. ฟิงซิช

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สิ่งที่ควรทำหากข้อมูลประจำตัวของคุณถูกขโมย			
2	สิ่งที่ไม่ควรแชร์บนโซเชียลมีเดีย			
3	สิ่งที่คุณสำรองข้อมูล			
4	บัตรหรือบัตรประจำตัวในกระเป๋าสตางค์ของคุณ			
5	เอกสารที่คุณควรปกป้อง			
6	สิ่งที่ควรทำหลังข้อมูลรั่วไหล			
7	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
8	ข้อมูลที่ผู้ขโมยข้อมูลประจำตัวต้องการ			
9	อุปกรณ์ที่ถูกแฮกได้			
10	แหล่งที่ข้อมูลของคุณอาจรั่วไหล			
11	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
12	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
13	วิธีพิสูจน์ว่าคุณเป็นใคร			
14	สัญญาณของการขโมยข้อมูลประจำตัว			
15	สัญญาณเตือนในอีเมล			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การป้องกันการปลอมแปลงตัวตนผู้บริหาร



สถานการณ์: ผู้บริหารระดับ C-suite ที่มีชื่อเสียงตกเป็นเป้าหมายของชื่อโดเมนที่สะกดผิดซึ่งเลียนแบบอีเมลส่วนตัวของเขาเพื่อฉ้อโกงลูกค้า จงออกแบบแผนการปกป้องแบรนด์

คำถามอภิปราย: จงวิเคราะห์ความเสี่ยงจากการปลอมแปลงแบรนด์ และอธิบายการควบคุม SPF/DKIM/DMARC และการยืนยันตัวตนโดยละเอียด

กรณีศึกษาที่ 2: ข้อมูลรับรององค์กรเผยแพร่บนดาร์กเว็บ



สถานการณ์: ชุดข้อมูลรั่วไหลบน Dark Web มีข้อมูลประจำตัวขององค์กรหลายร้อยรายการที่เป็นของผู้ดูแลระบบของบริษัท จงออกแบบกลยุทธ์การลดผลกระทบ

คำถามอภิปราย: จงสรุปกระบวนการล้างข้อมูลประจำตัว และวางแผนการเปิดใช้ตัวจัดการรหัสผ่าน

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

27	1	27	64	45	7		21	48	39	21	25		20	64	39	34			
1	49	35	34	54	25	34	48	25		43	37	49	34	10	48	64	25		

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: การโจรกรรมข้อมูลประจำตัวคืออะไร?

อาชญากรรมที่ผู้โจมตีขโมยข้อมูลส่วนบุคคล (เช่น รหัสผ่านหรือ SSN) เพื่อปลอมตัวเป็นผู้อื่นเพื่อผลประโยชน์ทางการเงิน

Q2: สาเหตุที่พบบ่อยที่สุดของการโจรกรรมข้อมูลประจำตัวคืออะไร?

ฟิชชิงเป็นวิธีหลักวิธีหนึ่งที่โจรใช้ขโมยรหัสผ่าน โดยล่อให้ผู้ใช้เข้าเว็บไซต์ปลอม

Q3: การยืนยันตัวตนแบบหลายปัจจัย (MFA) ปกป้องตัวตนอย่างไร?

MFA ต้องใช้หลักฐานยืนยันชั้นที่สอง (เช่น กุญแจฮาร์ดแวร์) เพื่อเข้าสู่ระบบ จึงบล็อกผู้โจมตีได้แม้พวกเขาขโมยรหัสผ่านของคุณไป

Q4: การอายัดเครดิต (credit freeze) คืออะไร?

บริการฟรีที่ป้องกันไม่ให้สำนักงานเครดิตแชร์แฟ้มเครดิตของคุณ ช่วยหยุดโจรไม่ให้เปิดสินเชื่อใหม่ในชื่อของคุณ [2]

Q5: การเฝ้าระวังดาร์กเว็บคืออะไร?

ซอฟต์แวร์ที่ตรวจสอบฟอรัมแฮกเกอร์เพื่อหาอีเมล รหัสผ่าน และบันทึกส่วนบุคคลที่รั่วไหล และแจ้งเตือนคุณหากข้อมูลของคุณถูกเปิดเผย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: credential stuffing หมายความว่าอะไร?

บอตอัตโนมัติที่ลองใช้รายการรหัสผ่านที่รั่วไหลกับเว็บไซต์หลายร้อยแห่งเพื่อยึดบัญชีที่ใช้งานอยู่

Q7: ทำไมการปลอมแปลงอีเมลจึงเป็นอันตราย?

ช่วยให้ผู้โจมตีปลอมชื่อผู้ส่งในอีเมล ทำให้ข้อความฟิชชิงดูเหมือนมาจากเพื่อนร่วมงานที่เชื่อถือได้

Q8: โปรแกรมจัดการรหัสผ่านหยุดการขโมยตัวตนได้อย่างไร?

เก็บรหัสผ่านที่ซับซ้อนและไม่ซ้ำกันสำหรับทุกบัญชี และปฏิเสธการกรอกข้อมูลรับรองอัตโนมัติบนโดเมนฟิชชิงปลอม

Q9: สเปียร์ฟิชชิง (spear phishing) คืออะไร?

การโจมตีแบบฟิชชิงเจาะจงเป้าหมายสูงที่ปรับแต่งด้วยชื่อและรายละเอียดของเหยื่อเพื่อเพิ่มโอกาสในการหลอกลวง

Q10: การแจ้งเตือนเครดิตแตกต่างจากการอายัดอย่างไร?

การแจ้งเตือนบอกให้ผู้ให้กู้ตรวจสอบตัวตนของคุณก่อนเปิดบัญชี ส่วนการอายัดบล็อกการเข้าถึงแฟ้มเครดิตของคุณโดยสิ้นเชิง [2]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: SIM swapping นำไปสู่การโจรกรรมข้อมูลประจำตัวได้อย่างไร?

ผู้โจมตีโน้มน้าวพนักงานของผู้ให้บริการเครือข่ายให้ย้ายหมายเลขโทรศัพท์ของเหยื่อไปยังซิมการ์ดใหม่ เพื่อแย่งรหัส 2FA ทาง SMS

Q2: DMARC มีบทบาทอย่างไรในการป้องกันการโจรกรรมข้อมูลประจำตัว?

DMARC ช่วยให้เจ้าของโดเมนบล็อกอีเมลปลอมไม่ให้เข้ากล่องจดหมาย และหยุดอีเมลปลอมที่เลียนแบบโดเมนขององค์กร

Q3: เหตุใดการขโมยตัวตนแบบสังเคราะห์ (synthetic identity theft) จึงตรวจจับได้ยาก?

หัวขโมยรวม SSN จริงกับชื่อและวันเกิดปลอมเพื่อสร้างโปรไฟล์เครดิตใหม่เอี่ยม หลบการแจ้งเตือนการฉ้อโกงพื้นฐาน

Q4: ผู้ค้าข้อมูล (data broker) แสวงหาประโยชน์จากข้อมูลตัวตนส่วนบุคคลอย่างไร?

ผู้รวบรวมข้อมูล (data broker) รวบรวมบันทึกสาธารณะ พฤติกรรมบนเว็บ และประวัติการซื้อเพื่อจัดทำแฟ้มข้อมูลโปรไฟล์ ซึ่งอาจรั่วไหลหรือถูกขายได้

Q5: ทำไม MFA ผ่าน SMS จึงถือว่ามีช่องโหว่?

ทราฟฟิก SMS เสี่ยงต่อการถูกดักจับ ฟิชชิง และการโจมตีสลับซิมในระดับผู้ให้บริการเครือข่าย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การล็อกแฟ้มเครดิต (credit file lock) คืออะไร?

บริการเชิงพาณิชย์ที่คล้ายการอายัด ช่วยให้ผู้ใช้ปลดล็อกหรือล็อกแฟ้มเครดิตของตนได้ทันทีผ่านแอปมือถือ

Q7: การรั่วไหลของข้อมูลองค์กรกระตุ้นการขโมยตัวตนได้อย่างไร?

ฐานข้อมูลที่รั่วไหลเปิดเผยข้อมูลประจำตัวแบบข้อความธรรมดานับล้านรายการ ทำให้มิจฉาชีพมีข้อมูลดิบสำหรับก่อการฉ้อโกงโดยแอบอ้างตัวตนแบบเจาะจงเป้าหมาย

Q8: การแชร์ข้อมูลบนโซเชียลมีเดียมากเกินไปมีความเสี่ยงอะไร?

การเปิดเผยชื่อสัตว์เลี้ยง สถานที่เกิด และนามสกุลเดิมของมารดาต่อสาธารณะทำให้โจรได้คำตอบของคำถามกู้คืนบัญชีทั่วไป

Q9: การล็อกอินด้วยไบโอเมตริกซ์ปกป้องโปรไฟล์ตัวตนอย่างไร?

ไบโอเมตริกซ์ผูกการเข้าสู่ระบบกับลักษณะเฉพาะ เช่น ลายนิ้วมือหรือใบหน้า หากเก็บไว้บนอุปกรณ์จะขโมยได้ยาก แต่ข้อมูลไบโอเมตริกซ์ที่เก็บไว้อาจรั่วไหลได้

Q10: กฎ Red Flags Rule ต่อสู้กับการโจรกรรมข้อมูลประจำตัวได้อย่างไร?

กฎระเบียบของรัฐบาลกลางที่กำหนดให้สถาบันการเงินพัฒนาโปรแกรมเป็นลายลักษณ์อักษรเพื่อตรวจจับและตอบสนองต่อสัญญาณเตือนของการขโมยข้อมูลประจำตัว

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

IdentityTheft.gov ดำเนินการโดย FTC ช่วยให้เหยื่อในสหรัฐฯ รายงานการโจรกรรมข้อมูลประจำตัวและรับแผนการฟื้นฟูส่วนบุคคล [1]

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

คีย์ความปลอดภัยแบบฮาร์ดแวร์เป็น MFA ที่ต้านทานฟิชชิง ซึ่งเป็น MFA ประเภทที่แข็งแกร่งที่สุดที่ CISA เรียกร้องให้ใช้ [4]

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

รหัสผ่านที่ถูกบุกรุกเป็นจุดเข้าที่พบบ่อยในการละเมิดข้อมูล และเป็นต้นเหตุของการฉ้อโกงข้อมูลตัวตนในภายหลัง

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การอายัดเครดิตไม่มีค่าใช้จ่ายตามกฎหมายของรัฐบาลกลาง และป้องกันไม่ให้ผู้ให้กู้ตรวจสอบแฟ้มเครดิตจนกว่าจะปลดล็อก [2]

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

DMARC ช่วยให้เจ้าของโดเมนบอกเมลเซิร์ฟเวอร์ให้ปฏิเสธหรือกักกันอีเมลปลอมที่ไม่ผ่านการตรวจสอบ [7]

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การสลับซิม (SIM swapping) ช่วยให้แฮกเกอร์ข้ามการยืนยันตัวตนสองปัจจัยทาง SMS บนพอร์ทัลธนาคารได้

7. ข้อมูลเชิงลึกด้านความปลอดภัย

การฉ้อโกงข้อมูลตัวตนสังเคราะห์ผสมรายละเอียดจริงและปลอมเข้าด้วยกัน ทำให้ผู้ให้กู้ตรวจจับได้ยาก

8. ข้อมูลเชิงลึกด้านความปลอดภัย

หลายคนใช้รหัสผ่านเดียวกันซ้ำกับหลายบัญชีออนไลน์ ดังนั้นการรั่วไหลครั้งเดียวอาจเปิดเผยหลายบัญชีได้

9. ข้อมูลเชิงลึกด้านความปลอดภัย

ดาต้าโบรกเกอร์รวบรวมแฟ้มข้อมูลโดยละเอียดของผู้บริโภคจำนวนมาก ทำให้เกิดความเสี่ยงด้านความเป็นส่วนตัวที่กระจุกตัว

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การกู้คืนจากการขโมยข้อมูลประจำตัวอาจใช้เวลาทำงานหลายเดือน เช่น การโต้แย้งรายการเรียกเก็บเงินและการแก้ไขรายงานเครดิต

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

วิธีหลักที่โจรขโมยตัวตนใช้ขโมยข้อมูลเข้าสู่ระบบคืออะไร? → การส่งการแจ้งเตือนทางอีเมลปลอมเพื่อหลอกให้ผู้ใช้กรอกรหัสผ่านบนพอร์ทัลปลอม

2 คำถาม 2 — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

มาตรการควบคุมความปลอดภัยใดที่ให้การป้องกันที่แข็งแกร่งที่สุดต่อการรั่วไหลของข้อมูลเข้าสู่ระบบ? → การยืนยันตัวตนหลายปัจจัยโดยใช้คีย์ฮาร์ดแวร์

3 คำถาม 3 — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

อะไรแสดงถึงการอายัดเครดิต? → การล็อกรายงานเครดิตเพื่อป้องกันโจรเปิดสินเชื่อโดยไม่ได้รับอนุญาต

4 คำถาม 4 — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

เหตุใดการเฝ้าระวังดาร์กเว็บจึงมีประโยชน์? → แจ้งเตือนผู้ใช้หากข้อมูลรับรองที่รั่วไหลของตนปรากฏในฐานข้อมูลผิดกฎหมาย

5 คำถาม 5 — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

วิศวกรรมสังคมหมายถึงอะไร? → การบงการผู้คนให้เปิดเผยข้อมูลรับรองที่เป็นความลับด้วยความสมัครใจ

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** — คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

การขโมยข้อมูลประจำตัวอาจเริ่มจากนอกระบบออนไลน์ได้เช่นกัน เช่น จดหมายหรือเอกสารที่ถูกขโมย

7 **คำถาม 7** — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การบังคับใช้ MFA กับบัญชีส่วนตัวทั้งหมดบล็อกการโจมตีด้วยบอตแบบ credential stuffing ได้เป็นส่วนใหญ่

8 **คำถาม 8** — คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

การอายัดเครดิต (credit freeze) หยุดการตรวจสอบเครดิตใหม่ แต่ไม่กระทบบัญชีที่มีอยู่ของคุณ

9 **คำถาม 9** — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ตัวจัดการรหัสผ่านปกป้องผู้ใช้จากฟิชชิงด้วยการปฏิเสธกรอกรหัสผ่านอัตโนมัติบนโดเมนปลอม

10 **คำถาม 10** — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

อีเมลฟิชชิงมักใช้ถ้อยคำเร่งด่วนเพื่อกระตุ้นการตอบสนองทางอารมณ์ที่รวดเร็ว

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

H 1. ข้อมูลรับรอง	D 2. การรั่วไหล	A 3. MFA	G 4. การตรวจสอบ
C 5. การแซ่แซ้ง	E 6. การป้องกัน	B 7. การปลอมแปลง	F 8. ฟิชชิง

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ข้อมูลประจำตัว	2 รั่วไหล	3 เอ็มเอฟเอ	4 เฝ้าระวัง
5 อายัด	6 การป้องกัน		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 H – ฟิชชิง	2 A – ข้อมูลประจำตัว	3 G – สปูฟฟิง	4 F – การป้องกัน
5 D – เฝ้าระวัง	6 E – อายัด	7 B – รั่วไหล	8 C – เอ็มเอฟเอ

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย ข้อมูลรับรอง การรั่วไหล และ MFA ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

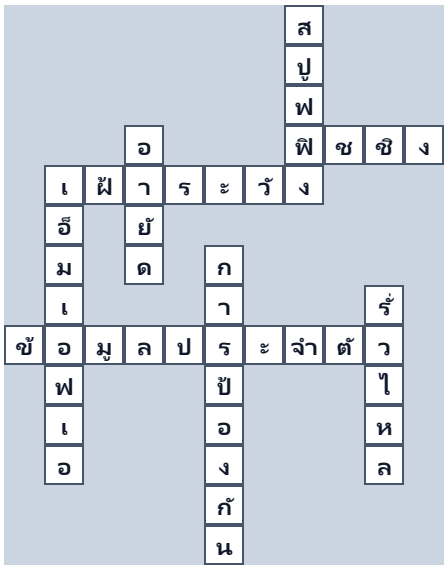
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	นี	า	น	นี	ส	ช	รั่	มี	ฟ	บ	า	า	ห	นี
า	ม	กี	จ	า	า	รี	ว	เ	ต	ว	ย	ง	ก	ค
จ	น	ด	ตี	ว	ร	ตี	ไ	ว	ฝ้	า	ล	ล	ด	า
อ	ย	ย้	ช	ฟ	ก	ก	ห	ล	ม	า	า	ป	อ	อ
น	ม	า	มี	า	ข้	ล	ล	ล	ป	ส	ร	จ	า	นี
ก้	กี	อ	พ	ร	อ	ง	เ	า	ช	า	ปู	ะ	า	ลี
ง	จ	ดี	า	น	มู	ล	ผ	อ็	ดี	ช	ก	ฟ	ว้	ด
อ	า	ต	า	จ	ล	า	ค	ก	ม	ดี	า	ช	ฟิ	ง
ป้	ว	ก	ด	กี	ป	ด	ท	ผ	ฟ	เ	ช	มี	ม	ง
ร	อ	ต	ฟ	ร	ร	ดี	า	ท	า	ส	อ	ท	ข	ข
า	า	น	ก	า	ะ	ล	า	ม	ร	ง	มี	ฟ	า	ร
ก	ช	ก	ด	ง	จำ	น	ร	ต	ชิ	สี	ย	ข	เ	มี
ดี	ด	ด	ว	บ	ตั	ฟ	อ	ช	า	ร	ห	ห	รี	อ
น	ผ	นี	ม	ผ	ว	ดี	ฟิ	ข	กี	ส	บ	ลี	ง	ด
ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

3 แนวนอน: ฟิชชิง การส่งข้อความหลอกลวงเพื่อล่อให้ผู้ใช้ให้ข้อมูลประจำตัว (4 ตัวอักษร)

4 แนวนอน: เฝ้าระวัง การสแกนเว็บบอร์ดและช่องทางของแฮกเกอร์เพื่อหาข้อมูลองค์กรที่ถูกขโมย (7 ตัวอักษร)

7 แนวนอน: ข้อมูลประจำตัว ชื่อผู้ใช้ รหัสผ่าน และโทเค็นส่วนตัวที่ใช้ยืนยันตัวตนดิจิทัล (10 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: สปูฟฟิง การสร้างเว็บไซต์หรืออีเมลปลอมเพื่อเลียนแบบองค์กรที่ถูกต้อง (5 ตัวอักษร)

2 แนวตั้ง: อายัด การจำกัดการเข้าถึงแฟ้มเครดิตเพื่อป้องกันการยื่นกู้เงินโดยทุจริต (4 ตัวอักษร)

4 แนวตั้ง: เอ็มเอฟเอ ขั้นตอนยืนยันตัวตนเพิ่มเติม (เช่น กุญแจฮาร์ดแวร์) ที่ปกป้องการเข้าสู่ระบบบัญชี (8 ตัวอักษร)

5 แนวตั้ง: การป้องกัน การฝึกอบรมและมาตรการทางเทคนิคที่ใช้ป้องกันการขโมยข้อมูลประจำตัว (8 ตัวอักษร)

6 แนวตั้ง: รั่วไหล การเปิดเผยฐานข้อมูลส่วนตัวที่มีบันทึกข้อมูลส่วนบุคคลของผู้ใช้โดยไม่ได้รับอนุญาต (5 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ตะรปอข้จำวลมู — ข้อมูลประจำตัว
2. แออ็เฟอม — เอ็มเอฟเอ
3. ดอย้า — อายัด
4. ฟงฟิสปู — สปูฟฟิง
5. ไลรั่หว — รั่วไหล
6. ว้ำะเรงฝ้ — เฝ้าระวัง
7. กนองก้าป้ร — การป้องกัน
8. ฟิงซิช — ฟิชชิง

เฉลยภารกิจรหัสลับ

"ปกป้อง ตัวตน ด้วย การยืนยัน หลายชั้น"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การป้องกันการปลอมแปลงตัวตนผู้บริหาร

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ผู้บริหารระดับ C-suite ที่มีชื่อเสียงตกเป็นเป้าหมายของชื่อโดเมน typosquatting ที่เลียนแบบอีเมลส่วนตัวเพื่อหลอกลวงลูกค้า จงออกแบบแผนปกป้องแบรนด์
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: จดทะเบียนชื่อสะกดแบบต่างๆ ที่พบบ่อยของชื่อผู้บริหารทั้งหมด ใช้โปรโตคอลยืนยันตัวตนอีเมล (DMARC, DKIM, SPF) เพื่อป้องกันการปลอมโดเมน และบังคับใช้ MFA แบบฮาร์ดแวร์กับการเข้าสู่ระบบองค์กรของผู้บริหารระดับ C-suite ทั้งหมด

B กรณีศึกษาที่ 2: ข้อมูลรับรององค์กรเผยแพร่บนดาร์กเว็บ

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ฐานข้อมูลที่รั่วไหลบน dark web มีข้อมูลรับรององค์กรหลายร้อยรายการของผู้ดูแลระบบขององค์กร จงออกแบบกลยุทธ์การลดผลกระทบ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ดำเนินการรีเซ็ตรหัสผ่านทั้งบริษัท กำหนดให้ใช้โปรแกรมจัดการรหัสผ่านระดับองค์กร บังคับใช้ MFA ในทุกพอร์ทัลของระบบ และตั้งค่าการแจ้งเตือนเฝ้าระวังดาร์กเว็บอัตโนมัติอย่างต่อเนื่อง