ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

ความปลอดภัยและการเข้ารหัสของ Wi-Fi สาธารณะ

การโจมตีแบบ man-in-the-middle, จุดเข้าใช้งานปลอม, การดักจับแพ็กเก็ต, อุโมงค์ VPN และการเข้ารหัส HTTPS

ภาพรวมการเรียนรู้ความปลอดภัย Wi-Fi สาธารณะ

ได้รับการรักษาความปลอดภัย

การเข้ารหัสข้อมูล

มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด

มาตรฐานสากล

กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์

นโยบายการเข้าถึง

การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับความปลอดภัยของ Wi-Fi สาธารณะ คุณจะได้สำรวจเครือข่ายที่ไม่เข้ารหัส การโจมตีแบบ man-in-the-middle (MitM) จุดเข้าใช้งานปลอม การดักจับแพ็กเก็ต อุโมงค์ VPN และความปลอดภัยในการส่งผ่านข้อมูลด้วย HTTPS

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/khwam-plodphai-wifi-satharana/

เส้นทางการเรียนรู้ความปลอดภัยของ Wi-Fi สาธารณะของคุณ

- ระบุความเสี่ยงทั่วไปของ Wi-Fi สาธารณะ รวมถึงการดักจับแพ็กเก็ตและแอกเซสพอยต์ปลอม
- ใช้อุโมงค์เข้ารหัส VPN เพื่อรักษาความปลอดภัยข้อมูลระหว่างส่ง
- บังคับใช้ HTTPS และการตั้งค่าเว็บเบราว์เซอร์ที่ปลอดภัยสำหรับพนักงานที่ทำงานระยะไกล

คำแนะนำคู่มือความปลอดภัย Wi-Fi สาธารณะ

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ ความปลอดภัยของการเข้าถึงระยะไกล ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

ความปลอดภัยของ Wi-Fi สาธารณะและการปกป้องข้อมูลระหว่างส่ง (บทนำ)

ฮอตสปอต Wi-Fi สาธารณะที่ไม่เข้ารหัสทำให้ทราฟฟิกเครือข่ายเสี่ยงต่อการดักจับแพ็กเก็ตและการปลอมแบบ Evil Twin การบังคับให้ทราฟฟิกผ่านอุโมงค์เข้ารหัส VPN ที่ปลอดภัยและบังคับใช้กฎ HSTS แบบ HTTPS เท่านั้นช่วยปกป้องเซสชันจากการดักในเครือข่ายท้องถิ่น

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. การโจมตีแบบ Man-in-the-Middle (MitM) คืออะไร?
   - A. การดักและแก้ไขการสื่อสารระหว่างสองฝ่ายบนเครือข่ายที่ใช้ร่วมกัน
   - B. เทคนิคการดึงข้อมูลจากฐานข้อมูลที่มุ่งเป้าไปที่ระเบียนผู้ใช้
   - C. ท่วมเว็บเซิร์ฟเวอร์ด้วยคำขอทราฟฟิกเครือข่ายจำนวนมาก
   - D. การล้างวอลุ่มจัดเก็บข้อมูลของฮาร์ดไดรฟ์ในเครื่อง

2. จุดเข้าใช้งานปลอม (Evil Twin) คืออะไร?
   - A. ฮอตสปอต Wi-Fi อันตรายที่ตั้งค่า SSID เดียวกับเครือข่ายที่ถูกต้อง
   - B. เครื่องมือผู้ดูแลระบบที่ใช้ตรวจสอบการสำรองฐานข้อมูล
   - C. การกำหนดค่าเกตเวย์ VPN ที่ปลอดภัย
   - D. ระเบียน DNS ที่แมปเมลเซิร์ฟเวอร์ที่ได้รับอนุญาต

3. VPN ปกป้องทราฟฟิก Wi-Fi สาธารณะได้อย่างไร?
   - A. ห่อแพ็กเก็ตเครือข่ายทั้งหมดไว้ในอุโมงค์เข้ารหัส ทำให้สนิฟเฟอร์อ่านไม่ได้
   - B. บล็อกคำขอเชื่อมต่อขาเข้าทั้งหมดโดยอัตโนมัติ
   - C. เปลี่ยนที่อยู่ MAC ของการ์ดเครือข่ายจริง
   - D. ลบคุกกี้ที่แคชไว้ในเว็บเบราว์เซอร์

4. การดักจับแพ็กเก็ต (packet sniffing) คืออะไร?
   - A. การใช้เครื่องมือฮาร์ดแวร์หรือซอฟต์แวร์เพื่อดักและบันทึกแพ็กเก็ตเครือข่าย
   - B. การสแกนไดเรกทอรีในเครื่องเพื่อหาไฟล์ซ้ำ
   - C. จำกัดสิทธิ์การอ่านฐานข้อมูลตามบทบาทของผู้ใช้
   - D. การเข้ารหัสไดรฟ์จัดเก็บข้อมูลด้วยกุญแจ AES-256

5. HTTPS มีบทบาทอะไร?
   - A. การเข้ารหัสทราฟฟิกของเซสชันระหว่างเบราว์เซอร์กับเว็บเซิร์ฟเวอร์
   - B. การกรองข้อความอีเมลขาเข้าที่เกตเวย์
   - C. การบีบอัดรูปภาพเพื่อให้โหลดหน้าเร็วขึ้น
   - D. การจัดการโครงสร้างไฟล์ในอุปกรณ์จัดเก็บข้อมูลแบบเชื่อมต่อเครือข่าย

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. ผู้ใช้ที่เชื่อมต่ออยู่สามารถดักจับข้อมูลข้อความธรรมดาบนเครือข่าย Wi-Fi สาธารณะแบบเปิดได้อย่างง่ายดาย

○ จริง ○ เท็จ

7 คำถาม 7

7. จุดเข้าถึงปลอม (Evil Twin) ได้รับอนุญาตจากผู้ดูแลเครือข่ายเสมอ

○ จริง ○ เท็จ

8 คำถาม 8

8. VPN ไม่มีประสิทธิภาพในการปกป้องทราฟฟิกจากการดักจับแพ็กเก็ตบนเครือข่ายสาธารณะ

○ จริง ○ เท็จ

9 คำถาม 9

9. HTTPS เข้ารหัสเฉพาะเส้นทาง URL และปล่อยเพย์โหลดของแพ็กเก็ตเป็นข้อความธรรมดา

○ จริง ○ เท็จ

10 คำถาม 10

10. ฮอตสปอต Wi-Fi ที่ใช้ความปลอดภัย WPA3 ให้การป้องกันที่แข็งแกร่งกว่าเครือข่ายเปิดที่ไม่มีรหัสผ่าน

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การดักรหัสผ่านส่วนตัวบน Wi-Fi สาธารณะคือการ _____ การสื่อสาร
2. การวิเคราะห์แพ็กเก็ตดิบบนเครือข่ายท้องถิ่นใช้การ _____ แพ็กเก็ต
3. ฮอตสปอตปลอมที่เลียนแบบ Wi-Fi ของโรงแรมคือ _____
4. การรักษาความปลอดภัยการส่งทราฟฟิกเว็บต้องเข้ารหัสด้วย _____
5. การเข้ารหัสเอาต์พุตเครือข่ายทั้งหมดใช้ไคลเอนต์ _____
6. เส้นทางสื่อสารที่เข้ารหัสผ่านเครือข่ายสาธารณะคือ _____

คลังคำศัพท์

ดักจับ | ดับเบิลยูพีเอ | ไฟร์วอลล์ | วีพีเอ็น | สนิฟฟิง | อีวิลทวิน | อุโมงค์ | เอชทีทีพีเอส

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

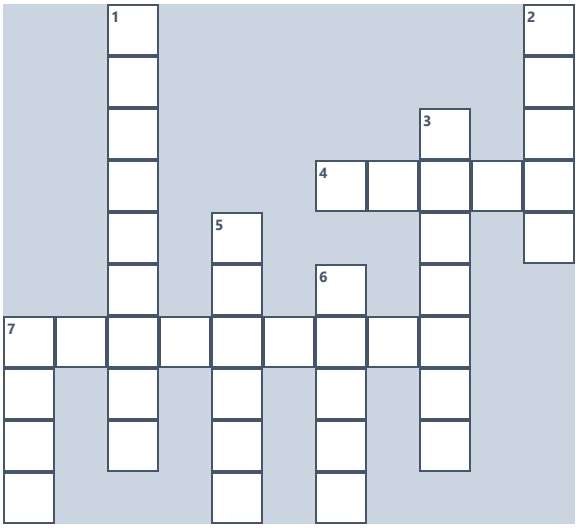
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. การดักข้อมูล**	**A**	มาตรฐานความปลอดภัย Wi-Fi สมัยใหม่
☐	**2. การดักจับแพ็กเก็ต**	**B**	เส้นทางข้อมูลที่ปลอดภัยระหว่างการส่ง
☐	**3. อีวิลทวิน**	**C**	การกรองทราฟฟิกขาเข้า
☐	**4. HTTPS**	**D**	ฮอตสปอตปลอมที่เลียนแบบ Wi-Fi
☐	**5. VPN**	**E**	การอ่านทราฟฟิกขณะส่งผ่าน
☐	**6. อุโมงค์**	**F**	การดักจับแพ็กเก็ตข้อมูลเครือข่าย
☐	**7. WPA3**	**G**	เครือข่ายส่วนตัวเสมือนที่เข้ารหัส
☐	**8. ไฟร์วอลล์**	**H**	การส่งข้อมูลบนเว็บอย่างปลอดภัย

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

4. การจับแพ็กเก็ตข้อมูลเครือข่าย (5)

7. มาตรฐานความปลอดภัย Wi-Fi สมัยใหม่ (9)

แนวตั้ง

1. การส่งข้อมูลเว็บอย่างปลอดภัย (9)

2. เส้นทางข้อมูลที่ปลอดภัยระหว่างส่ง (5)

3. การกรองทราฟฟิกขาเข้า (7)

5. ฮอตสปอตปลอมที่เลียนแบบ Wi-Fi (6)

6. เครือข่ายส่วนตัวเสมือนที่เข้ารหัส (5)

7. การอ่านทราฟฟิกระหว่างส่ง (4)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

4 แนวนอน: การจับแพ็กเก็ตข้อมูลเครือข่าย (5 ตัวอักษร):

7 แนวนอน: มาตรฐานความปลอดภัย Wi-Fi สมัยใหม่ (9 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: การส่งข้อมูลเว็บอย่างปลอดภัย (9 ตัวอักษร):

2 แนวตั้ง: เส้นทางข้อมูลที่ปลอดภัยระหว่างส่ง (5 ตัวอักษร):

3 แนวตั้ง: การกรองทราฟฟิกขาเข้า (7 ตัวอักษร):

5 แนวตั้ง: ฮอตสปอตปลอมที่เลียนแบบ Wi-Fi (6 ตัวอักษร):

6 แนวตั้ง: เครือข่ายส่วนตัวเสมือนที่เข้ารหัส (5 ตัวอักษร):

7 แนวตั้ง: การอ่านทราฟฟิกระหว่างส่ง (4 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า นี า น นี ส ช วี มี ฟ บ า า ห นี
า ม ค์ กี จ า า พี ไ รี ต ว ย ง ก
ค จ ง น ตี ว ร เ ดี ฟ ว า ล ล ด
อ า ม อ ย ช ฟ อ็ ก ก ร์ ล ม า ป
เ อ โ อ ม เ มี น า ล ล ว ป อี จ
พี า อุ นี กี อ พ ร ง า ซ า อ วิ า
ยู ลี จ ดี า ช น ล ส ผ ดี ช ก ล ด
ล า ต า จ ที า ค นิ ก ดี า ช ท ล์
บิ ว ก ด กี ที ด ท ฟ ผ ฟ ซ มี วิ ม
เ อ ต ฟ ร พี ดี า ฟิ ท า ส ท น ข
บ ข า น ก เ า ล ง า บ ม ร มี า
ดั ร ช ก ด อ ง น ร จั ต สี ย ข มี
ดี ด ด ว บ ส ฟ อ ก า ร ห ห รี น
ผ นี ม ผ ดี ข กี ดั ส บ ลี ง ด ร ด
ค ผ ห ดี ป ร กี นี า ต จ ห ดี ด บ

รายการคำศัพท์

ดักจับ สนิฟฟิง อีวิลทวิน เอชทีทีพีเอส วีพีเอ็น อุโมงค์ ดับเบิลยูพีเอ ไฟร์วอลล์

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ดักจับ
B. สนิฟฟิง
C. อีวิลทวิน
D. เอชทีทีพีเอส
E. วีพีเอ็น
F. อุโมงค์
G. ดับเบิลยูพีเอ
H. ไฟร์วอลล์

คำนิยามและช่องจับคู่
____ 1. มาตรฐานความปลอดภัย Wi-Fi สมัยใหม่
____ 2. ฮอตสปอตปลอมที่เลียนแบบ Wi-Fi
____ 3. การจับแพ็กเก็ตข้อมูลเครือข่าย
____ 4. เส้นทางข้อมูลที่ปลอดภัยระหว่างส่ง
____ 5. การกรองทราฟฟิกขาเข้า
____ 6. การอ่านทราฟฟิกระหว่างส่ง
____ 7. เครือข่ายส่วนตัวเสมือนที่เข้ารหัส
____ 8. การส่งข้อมูลเว็บอย่างปลอดภัย

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. จัดับก
2. นอีลวิทวิ
3. เวินอ็พี
4. ลอเบิพียูดับเ
5. ฟงสฟินิ
6. อทีอเพีเทีสช
7. งค์อุมโ
8. ฟวล์ไลอร์

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
2	อุปกรณ์ที่เชื่อมต่อ Wi-Fi โดยอัตโนมัติ			
3	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
4	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
5	วิธีรักษาความปลอดภัยที่ร้านกาแฟ			
6	อุปกรณ์ที่ถูกแฮกได้			
7	สิ่งที่แฮกเกอร์เห็นได้บน Wi-Fi แบบเปิด			
8	สัญญาณของเครือข่าย Wi-Fi ปลอม			
9	ทางเลือกแทน Wi-Fi สาธารณะ			
10	สัญญาณเตือนในอีเมล			
11	สิ่งที่คุณไม่ทำบน Wi-Fi สาธารณะ			
12	สถานที่ที่มี Wi-Fi ฟรี			
13	วิธีปกป้องบัญชีของคุณ			
14	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
15	ชื่อ Wi-Fi ที่ดูน่าสงสัย			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การจำกัดการดักดูแพ็กเก็ตบน Wi-Fi สาธารณะ



สถานการณ์: ผู้บริหารฝ่ายขายทางไกลที่เชื่อมต่อ Wi-Fi สาธารณะของสนามบินสังเกตเห็นว่าอีเมลธุรกิจที่ละเอียดอ่อนหลายฉบับรั่วไหลไม่นานหลังจากส่งเป็นข้อความธรรมดา

คำถามอภิปราย: จงวิเคราะห์ความเสี่ยงของเครือข่ายสาธารณะ และสรุปโซลูชันการเข้ารหัสทราฟฟิก

กรณีศึกษาที่ 2: การป้องกันฮอตสปอตปลอมแบบ Evil Twin



สถานการณ์: ผู้โจมตีติดตั้งจุดเข้าถึงไร้สายที่เป็นอันตรายชื่อ "CoffeeShop_Guest" เลียนแบบฮอตสปอตของร้านกาแฟที่ถูกต้อง เพื่อดักจับทราฟฟิกเครือข่ายจากแขกที่ไม่ระวัง

คำถามอภิปราย: จงอธิบายขั้นตอนการตรวจสอบเพื่อตรวจจับและบล็อกจุดเข้าถึงที่เป็นอันตรายโดยละเอียด

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

57	2	64	49	35	43	48	42		23	35	49	31	31	51	1		61	39	61	31

42	49	24	49	35	19	47

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: ทำไม Wi-Fi สาธารณะจึงไม่ปลอดภัย?

Wi-Fi สาธารณะแบบเปิดไม่เข้ารหัสทราฟฟิกขณะส่งผ่านอากาศ ผู้อื่นที่อยู่ใกล้จึงอาจดักจับข้อมูลที่ไม่ได้รับการป้องกันได้ [2]

Q2: การดักจับแพ็กเก็ตคืออะไร?

แพ็กเก็ตสนิฟเฟอร์ดักข้อมูลดิบที่ไหลผ่านอินเทอร์เฟซเครือข่าย ทำให้รหัสผ่านและรายละเอียดทราฟฟิกแบบข้อความธรรมดาถูกเปิดเผย

Q3: Evil Twin คืออะไร?

จุดเข้าถึงปลอมที่แฮกเกอร์ตั้งขึ้น เลียนแบบชื่อและการตั้งค่าของฮอตสปอต Wi-Fi ในพื้นที่ที่เชื่อถือได้

Q4: VPN ปกป้องฉันได้อย่างไร?

กำหนดเส้นทางทราฟฟิกของคุณผ่านอุโมงค์เข้ารหัส ซ่อนกิจกรรมการท่องเว็บของคุณจากตัวดักจับในเครือข่ายท้องถิ่น

Q5: HTTPS ปกป้องฉันบน Wi-Fi สาธารณะหรือไม่?

ได้ เข้ารหัสข้อมูลที่แลกเปลี่ยนระหว่างเบราว์เซอร์กับเว็บไซต์ และ VPN เพิ่มการป้องกันอีกชั้นหนึ่ง

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: WPA3 คืออะไร?

มาตรฐาน Wi-Fi Protected Access สมัยใหม่ ให้การเข้ารหัสที่แข็งแกร่งกว่าและป้องกันการโจมตีแบบพจนานุกรมออฟไลน์ [1]

Q7: Wi-Fi สาธารณะส่งมัลแวร์ได้หรือไม่?

ใช่ ผู้โจมตีสามารถดักทราฟฟิกและแทรกข้อความแจ้งดาวน์โหลดที่เป็นอันตราย (drive-by download) ลงในเซสชันเบราว์เซอร์ของคุณได้

Q8: การแชร์ไฟล์มีความเสี่ยงอะไร?

หากเปิดการแชร์ไฟล์ ผู้ใช้อื่นบนเครือข่ายสาธารณะอาจอ่านหรือแก้ไขไดเรกทอรีโฟลเดอร์ในเครื่องของคุณได้

Q9: captive portal คืออะไร?

หน้าเข้าสู่ระบบที่เครือข่ายโรงแรมหรือร้านกาแฟใช้เพื่ออนุญาตการเข้าถึงอินเทอร์เน็ต ซึ่งบางครั้งผู้โจมตีอาจปลอมแปลงได้

Q10: ฉันควรปิด Wi-Fi เมื่อไม่ได้ใช้งานหรือไม่?

ได้ การปิด Wi-Fi ช่วยป้องกันไม่ให้อุปกรณ์ของคุณเชื่อมต่อกับเครือข่ายที่ไม่น่าเชื่อถือโดยอัตโนมัติ

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: การโจมตีแบบ Man-in-the-Middle ใช้ประโยชน์จาก DNS ได้อย่างไร?

ด้วยการใช้ DNS spoofing บนเราเตอร์ปลอมเพื่อนำเบราว์เซอร์เป้าหมายไปยังหน้าเว็บฟิชชิงที่เลียนแบบ แทนโดเมนเป้าหมายจริง

Q2: การแย่งเซสชันคืออะไร?

ผู้โจมตีแอบดักคุกกี้เซสชันที่ไม่ได้เข้ารหัสบน Wi-Fi สาธารณะและนำเข้ามาใช้เพื่อข้ามการเข้าสู่ระบบด้วยข้อมูลรับรอง

Q3: SSL stripping คืออะไร?

การโจมตีแบบ MitM ที่ผู้โจมตีลดระดับคำขอ HTTPS ที่ปลอดภัยของผู้ใช้เป็น HTTP ที่ไม่เข้ารหัส เพื่อดักข้อมูลเข้าสู่ระบบเป็นข้อความธรรมดา

Q4: HSTS ป้องกัน SSL stripping ได้อย่างไร?

HTTP Strict Transport Security บังคับให้เบราว์เซอร์เชื่อมต่อผ่าน HTTPS เท่านั้นและปฏิเสธการถอยกลับไปใช้ HTTP ที่ไม่เข้ารหัส [3]

Q5: VPN แบบ split-tunnel คืออะไร?

การกำหนดค่าที่ส่งเฉพาะทราฟฟิกองค์กรผ่าน VPN และส่งข้อมูลอินเทอร์เน็ตสาธารณะโดยตรง ซึ่งอาจเสี่ยงต่อการเปิดเผยผ่านเส้นทางรั่วไหล

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: ทำไม WPA2 จึงมีช่องโหว่ต่อ KRACK?

Key Reinstallation Attack ใช้ช่องโหว่ใน four-way handshake ของ WPA2 เพื่อถอดรหัสแพ็กเก็ตโดยไม่ต้องใช้รหัสผ่าน Wi-Fi

Q7: client isolation คืออะไร?

การตั้งค่าความปลอดภัยของเราเตอร์ที่ป้องกันไม่ให้อุปกรณ์ Wi-Fi ที่เชื่อมต่ออยู่สื่อสารกันโดยตรง เพื่อบล็อกการดักข้อมูลในเครือข่ายภายใน

Q8: ผู้โจมตีใช้เซิร์ฟเวอร์ DNS ปลอมอย่างไร?

ตั้งค่าเราเตอร์ปลอมให้กำหนดเซิร์ฟเวอร์ DNS ปลอมแก่ไคลเอนต์ เพื่อดักและเขียนทับการค้นหาเว็บทั้งหมด

Q9: VPN ซ่อนที่อยู่ MAC ภายในเครื่องของฉันได้หรือไม่?

ไม่ ที่อยู่ MAC เป็นตัวระบุเลเยอร์ 2 ภายในเครือข่าย ให้ใช้การตั้งค่าสุ่มที่อยู่ MAC (ที่อยู่ส่วนตัว) ที่มีในอุปกรณ์ของคุณแทน

Q10: การโจมตีแบบปลอม captive portal คืออะไร?

ผู้โจมตีที่โฮสต์พอร์ทัลยืนยันตัวตนปลอมบนฮอตสปอตอันตรายเพื่อขโมยข้อมูลรับรองโดยอ้างว่าเป็นการเข้าถึง Wi-Fi ฟรี

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

พนักงานระยะไกลมักใช้ Wi-Fi ในคาเฟ่ โรงแรม และสนามบิน ซึ่งไม่สามารถควบคุมความปลอดภัยของเครือข่ายได้

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

จุดเข้าถึงปลอม Evil Twin สามารถคัดลอกชื่อและ MAC address ของเครือข่ายที่เชื่อถือได้อย่างตรงตัว ทำให้อุปกรณ์สับสน

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ซอฟต์แวร์ดักจับแพ็กเก็ตอย่าง Wireshark ใช้ฟรีและสามารถแสดงรหัสผ่าน HTTP ที่ไม่ได้เข้ารหัสเป็นข้อความธรรมดา

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ความปลอดภัยของ WPA3 ใช้ Simultaneous Authentication of Equals (SAE) เพื่อป้องกันการโจมตีแบบบรูตฟอร์ซภายในเครือข่าย

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การโจมตีแบบ SSL stripping ข้ามการป้องกัน HTTPS พื้นฐานโดยดักการเปลี่ยนเส้นทาง HTTP เริ่มต้นที่เกตเวย์

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ส่วนหัวการตอบกลับ HTTP Strict Transport Security (HSTS) ป้องกันไม่ให้เบราว์เซอร์ถอยกลับไปใช้การเชื่อมต่อ HTTP ที่ไม่เข้ารหัส [3]

7. ข้อมูลเชิงลึกด้านความปลอดภัย

การปิด 'เชื่อมต่ออัตโนมัติ' ช่วยป้องกันไม่ให้สมาร์ทโฟนเชื่อมต่อกับเครือข่ายปลอมที่เลียนแบบในที่สาธารณะ

8. ข้อมูลเชิงลึกด้านความปลอดภัย

การกำหนดค่า VPN แบบ 'always-on' ระดับองค์กรบังคับให้ทราฟฟิกเครือข่ายของพนักงานระยะไกลทั้งหมดผ่านไฟร์วอลล์ขององค์กร

9. ข้อมูลเชิงลึกด้านความปลอดภัย

จุดเข้าถึงปลอมสามารถส่งคำตอบ DNS ปลอมเพื่อเปลี่ยนเส้นทางโดเมนเป้าหมายไปยังเซิร์ฟเวอร์ฟิชชิง

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

หากไม่มี VPN ผู้ใช้คนอื่นบนฮอตสปอตแบบเปิดสามารถเห็นว่าอุปกรณ์ของคุณติดต่อเว็บไซต์และเซิร์ฟเวอร์ใดบ้าง

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[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

การโจมตีแบบ Man-in-the-Middle (MitM) คืออะไร? → การดักและแก้ไขการสื่อสารระหว่างสองฝ่ายบนเครือข่ายที่ใช้ร่วมกัน

2 คำถาม 2

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

จุดเข้าใช้งานปลอม (Evil Twin) คืออะไร? → ฮอตสปอต Wi-Fi อันตรายที่ตั้งค่า SSID เดียวกับเครือข่ายที่ถูกต้อง

3 คำถาม 3

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

VPN ปกป้องทราฟฟิก Wi-Fi สาธารณะได้อย่างไร? → ห่อแพ็กเก็ตเครือข่ายทั้งหมดไว้ในอุโมงค์เข้ารหัส ทำให้สนิฟเฟอร์อ่านไม่ได้

4 คำถาม 4

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การดักจับแพ็กเก็ต (packet sniffing) คืออะไร? → การใช้เครื่องมือฮาร์ดแวร์หรือซอฟต์แวร์เพื่อดักและบันทึกแพ็กเก็ตเครือข่าย

5 คำถาม 5

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

HTTPS มีบทบาทอะไร? → การเข้ารหัสทราฟฟิกของเซสชันระหว่างเบราว์เซอร์กับเว็บเซิร์ฟเวอร์

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ผู้ใช้ที่เชื่อมต่ออยู่สามารถดักจับข้อมูลข้อความธรรมดาบนเครือข่าย Wi-Fi สาธารณะแบบเปิดได้อย่างง่ายดาย

7 **คำถาม 7** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: Evil Twin คือฮอตสปอตที่ไม่ได้รับอนุญาตซึ่งผู้โจมตีตั้งขึ้นเพื่อเลียนแบบฮอตสปอตจริง

8 **คำถาม 8** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: VPN เข้ารหัสทราฟฟิกในอุโมงค์ ตัวดักจับในเครือข่ายท้องถิ่นจึงอ่านไม่ได้

9 **คำถาม 9** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: HTTPS เข้ารหัสการแลกเปลี่ยน HTTP ทั้งหมด รวมถึงพาธของ URL และเนื้อหาของหน้า

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ฮอตสปอต Wi-Fi ที่ใช้ความปลอดภัย WPA3 ให้การป้องกันที่แข็งแกร่งกว่าเครือข่ายเปิดที่ไม่มีรหัสผ่าน

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

E 1. การดักข้อมูล	F 2. การดักจับแพ็กเก็ต	D 3. อีวิลทวิน	H 4. HTTPS
G 5. VPN	B 6. อุโมงค์	A 7. WPA3	C 8. ไฟร์วอลล์

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ดักจับ	2 สนิฟฟิง	3 อีวิลทวิน	4 เอชทีทีพีเอส
5 วีพีเอ็น	6 อุโมงค์		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 G – ดับเบิลยูพีเอ	2 C – อีวิลทวิน	3 B – สนิฟฟิง	4 F – อุโมงค์
5 H – ไฟร์วอลล์	6 A – ดักจับ	7 E – วีพีเอ็น	8 D – เอชทีทีพีเอส

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย การดักข้อมูล การดักจับแพ็กเก็ต และ อีวิลทวิน ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

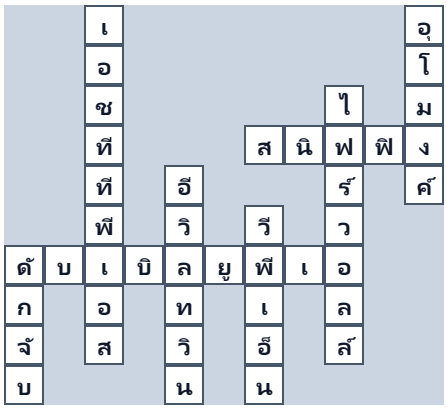
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	นี	า	น	นี	ส	ช	วี	มี	ฟ	บ	า	า	ห	นี
า	ม	ค์	กี	จ	า	า	พี	ไ	รี	ต	ว	ย	ง	ก
ค	จ	ง	น	ดี	ว	ร	เ	ดี	ฟ	ว	า	ล	ล	ด
อ	า	ม	อ	ย	ช	ฟ	อ็	ก	ก	ร์	ล	ม	า	ป
เ	อ	โ	อ	ม	เ	มี	น	า	ล	ล	ว	ป	อี	จ
พี	า	อุ	นี	กี	อ	พ	ร	ง	า	ช	า	อ	วิ	า
ยู	ลี	จ	ดี	า	ช	น	ล	ส	ผ	ดี	ช	ก	ล	ด
ล	า	ต	า	จ	ที	า	ค	นิ	ก	ดี	า	ช	ท	ล์
บิ	ว	ก	ด	กี	ที	ด	ท	ฟ	ผ	ฟ	ช	มี	วิ	ม
เ	อ	ต	ฟ	ร	พี	ดี	า	ฟิ	ท	า	ส	ท	น	ข
บ	ข	า	น	ก	เ	า	ล	ง	า	บ	ม	ร	มี	า
ดั	ร	ช	ก	ด	อ	ง	น	ร	จั	ต	สี	ย	ข	มี
ดี	ด	ด	ว	บ	ส	ฟ	อ	ก	า	ร	ห	ห	รี	น
ผ	นี	ม	ผ	ดี	ข	กี	ดั	ส	บ	ลี	ง	ด	ร	ด
ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

4 แนวนอน: สนิฟฟิง การจับแพ็กเก็ตข้อมูลเครือข่าย (5 ตัวอักษร)

7 แนวนอน: ดับเบิลยูพีเอ มาตรฐานความปลอดภัย Wi-Fi สมัยใหม่ (9 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: เอชทีทีพีเอส การส่งข้อมูลเว็บอย่างปลอดภัย (9 ตัวอักษร)

2 แนวตั้ง: อุโมงค์ เส้นทางข้อมูลที่ปลอดภัยระหว่างส่ง (5 ตัวอักษร)

3 แนวตั้ง: ไฟร์วอลล์ การกรองทราฟฟิกขาเข้า (7 ตัวอักษร)

5 แนวตั้ง: อีวิลทวิน ฮอตสปอตปลอมที่เลียนแบบ Wi-Fi (6 ตัวอักษร)

6 แนวตั้ง: วีพีเอ็น เครือข่ายส่วนตัวเสมือนที่เข้ารหัส (5 ตัวอักษร)

7 แนวตั้ง: ดักจับ การอ่านทราฟฟิกระหว่างส่ง (4 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. จัดับก — ดักจับ
2. นอีลวิทวิ — อีวิลทวิน
3. เวินอ็พี — วีพีเอ็น
4. ลอเบิพียูดับเ — ดับเบิลยูพีเอ
5. ฟงสฟินิ — สนิฟฟิง
6. อทีอเพีเทีสช — เอชทีทีพีเอส
7. งค์อุมโ — อุโมงค์
8. ฟวส์ไลอร์ — ไฟร์วอลล์

เฉลยภารกิจรหัสลับ

"เข้ารหัส ทราฟฟิก ไวไฟ สาธารณะ"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การจำกัดการดักดูแพ็กเก็ตบน Wi-Fi สาธารณะ

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ผู้บริหารฝ่ายขายระยะไกลที่เชื่อมต่อ Wi-Fi สนามบินสาธารณะสังเกตว่าอีเมลธุรกิจที่ละเอียดอ่อนหลายฉบับรั่วไหลไม่นานหลังส่งเป็นข้อความธรรมดา
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: กำหนดให้ใช้ไคลเอนต์ VPN ระดับองค์กรบนเวิร์กสเตชันระยะไกลทั้งหมด บังคับใช้ส่วนขยายเบราว์เซอร์แบบ HTTPS เท่านั้น และบล็อกโปรโตคอลที่ไม่เข้ารหัส (เช่น HTTP และ FTP) ที่ไฟร์วอลล์ฝั่งไคลเอนต์

B กรณีศึกษาที่ 2: การป้องกันฮอตสปอตปลอมแบบ Evil Twin

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ผู้โจมตีติดตั้งแอคเซสพอยต์ไร้สายปลอมชื่อ 'CoffeeShop_Guest' เลียนแบบฮอตสปอตของร้านกาแฟจริง เพื่อดักจับทราฟฟิกเครือข่ายจากแขกที่ไม่ทันระวัง
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ตรวจสอบที่อยู่ MAC ของ BSSID ของจุดเข้าใช้งานเพื่อยืนยันความถูกต้องของเครือข่าย บังคับใช้การตรวจสอบสถานะไคลเอนต์เพื่อบล็อกการเชื่อมต่อเครือข่ายแบบเปิด และกำหนดให้ใช้ฮอตสปอตเซลลูลาร์สำหรับงานที่ละเอียดอ่อน