ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

วิธีซ่อนที่อยู่ IP ของคุณ ใบงาน

การซ่อนที่อยู่ IP การปกปิดตำแหน่ง พร็อกซี Tor และการป้องกันการรั่วไหลของ DNS/WebRTC

ภาพรวมการเรียนรู้ VPN

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับหลักการพื้นฐานของเครือข่ายส่วนตัวเสมือน (VPN) คุณจะได้สำรวจว่าอุโมงค์ที่เข้ารหัสปกป้องข้อมูลของคุณอย่างไร โปรโตคอลเครือข่ายทำงานอย่างไร และวิธีระบุและลดการรั่วไหลของความเป็นส่วนตัว

จุดตรวจสอบของใบงาน

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

เปิดคู่มือ VPN ของ VPN.com

URL: https://www.vpn.com/th/vpn/

เส้นทางการเรียนรู้ VPN ของคุณ

- อธิบายว่าที่อยู่ IP ทำงานอย่างไรและรั่วไหลตำแหน่งที่ตั้งได้อย่างไร
- เปรียบเทียบพร็อกซี Tor และ VPN ในการปกปิดที่อยู่เครือข่าย
- ระบุวิธีตรวจจับและป้องกันการรั่วไหลของ DNS และ WebRTC
- ทำความเข้าใจว่าเว็บไซต์ติดตามผู้ใช้ผ่าน IP สาธารณะของพวกเขาอย่างไร
- ประเมินการกำหนดเส้นทางแบบ multi-hop และอุโมงค์ที่เข้ารหัสเพื่อปกป้อง IP

คำแนะนำใบงานการป้องกัน IP

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การซ่อนที่อยู่ IP ของคุณและการป้องกันการรั่วไหล ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การซ่อน IP ของคุณ (บทนำ)

IP ของคุณเปรียบเสมือนที่อยู่ไปรษณีย์ดิจิทัลที่เผยตำแหน่งที่ตั้งจริงและพฤติกรรมการใช้เครือข่ายของคุณ การซ่อน IP เป็นด่านป้องกันแรกจากการติดตามออนไลน์ การสร้างโปรไฟล์เป้าหมาย และการบล็อกตามตำแหน่งที่ตั้ง การเข้าใจวิธีปกปิดที่อยู่ของคุณอย่างปลอดภัยช่วยปกป้องความเป็นส่วนตัวของคุณทางออนไลน์

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. ที่อยู่ IP สาธารณะของอุปกรณ์เปิดเผยอะไรให้เว็บไซต์ที่คุณเข้าชมทราบ?

- A. หมายเลขบัตรเครดิตของผู้ใช้
- B. ตำแหน่งโดยประมาณของคุณและชื่อ ISP ของคุณ
- C. ไดเรกทอรีไฟล์ภายในเครื่องทั้งหมด
- D. การตั้งค่าภาษาของแป้นพิมพ์

2. วิธีใดที่ซ่อน IP ของคุณและเข้ารหัสทราฟฟิกทั้งหมดทั่วทั้งระบบ?

- A. เว็บพร็อกซีมาตรฐาน
- B. การล้างคุกกี้ของเบราว์เซอร์ของคุณ
- C. เครือข่ายส่วนตัวเสมือน (VPN)
- D. การปิดไฟร์วอลล์ในเครื่องของคุณ

3. ข้อจำกัดด้านความเป็นส่วนตัวที่สำคัญของการใช้พร็อกซีเว็บฟรีคืออะไร?

- A. ไม่เข้ารหัสทราฟฟิกข้อมูลบนเครือข่ายสาธารณะ
- B. ต้องติดตั้งระบบปฏิบัติการภายนอก
- C. ผิดกฎหมายอย่างสิ้นเชิงในสหรัฐอเมริกา
- D. ต้องใช้การเชื่อมต่อสายโทรศัพท์เฉพาะ

4. เครือข่าย Tor ให้ความไม่เปิดเผยตัวตนระดับสูงแก่ผู้ใช้ได้อย่างไร?

- A. โดยการเร่งความเร็วการเชื่อมต่อ
- B. โดยการส่งทราฟฟิกผ่านรีเลย์สามตัวที่ดำเนินการโดยอาสาสมัคร
- C. โดยการลงทะเบียนชื่อของคุณในฐานข้อมูลระดับโลก
- D. โดยการจำกัดการเข้าถึงเฉพาะหน่วยงานรัฐบาล

5. DNS leak คืออะไร?

- A. ข้อผิดพลาดในการส่งอีเมลไปยังที่อยู่ผิด
- B. เมื่อคำขอ DNS ข้ามอุโมงค์ VPN ไปยัง ISP
- C. ความล้มเหลวของฮาร์ดแวร์ในแหล่งจ่ายไฟของเราเตอร์ภายใน
- D. การอัปเดตไดรเวอร์อะแดปเตอร์เครือข่ายภายใน

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. เซิร์ฟเวอร์พร็อกซีเข้ารหัสทราฟฟิกเบื้องหลังของระบบปฏิบัติการเหมือน VPN

○ จริง ○ เท็จ

7 คำถาม 7

7. การกำหนดเส้นทางของ Tor ปลอดภัยสูงแต่ลดความเร็วในการท่องเครือข่าย

○ จริง ○ เท็จ

8 คำถาม 8

8. การรั่วไหลของ WebRTC อาจเปิดเผย IP จริงของคุณระหว่างเซสชัน VPN ที่ทำงานอยู่

○ จริง ○ เท็จ

9 คำถาม 9

9. เมื่อเปิด VPN และไม่มีการรั่วไหล ISP ของคุณจะมองไม่เห็นว่าคุณเข้าชมเว็บไซต์ใด

○ จริง ○ เท็จ

10 คำถาม 10

10. การซ่อนที่อยู่ IP ของคุณบล็อกการติดตามผ่านลายนิ้วมือเบราว์เซอร์

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การข้ามอุโมงค์ที่ปลอดภัยจนเผยคิวรีโดเมนของคุณเรียกว่า _____
2. API สื่อสารบนเบราว์เซอร์แบบ _____ อาจทำให้ที่อยู่ไอพีดั้งเดิมของคุณรั่วไหลโดยไม่ตั้งใจ
3. _____ เปลี่ยนเส้นทางทราฟฟิกของเบราว์เซอร์แต่ไม่เข้ารหัสเพย์โหลดของแพ็กเก็ต
4. การเข้ารหัสหลายชั้นของเครือข่าย _____ ให้ความเป็นนิรนามในระดับสูง
5. _____ สาธารณะของคุณถูกกำหนดโดยผู้ให้บริการโทรคมนาคมและเผยพื้นที่ของคุณ
6. การข้ามการปิดกั้นสื่อตามภูมิภาคทำได้ผ่านการ _____

คลังคำศัพท์

การติดตาม ทอร์ ที่อยู่ไอพี ปกปิดตำแหน่ง รั่วดีเอ็นเอส เว็บพร็อกซี เว็บอาร์ทีซี อุโมงค์

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องเครือข่าย

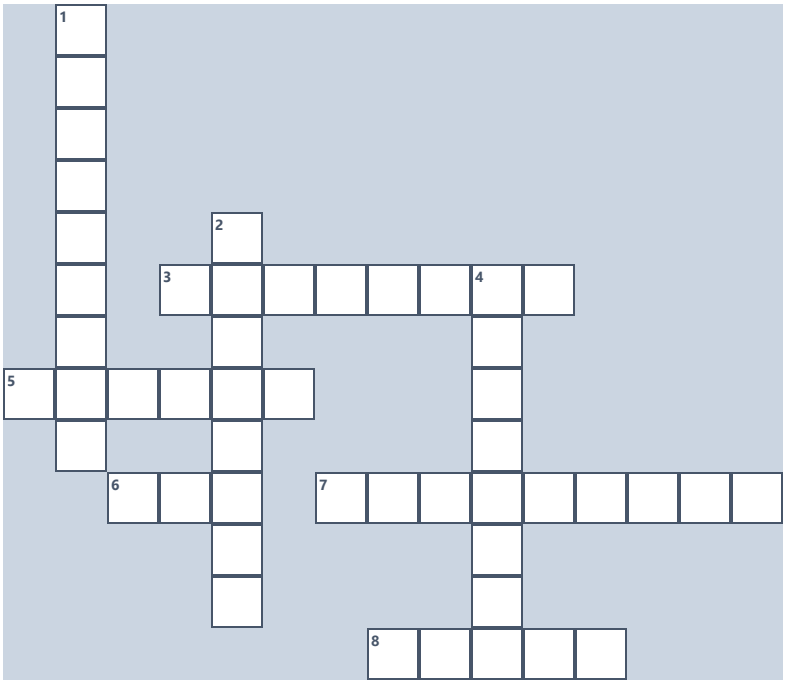
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. ที่อยู่ IP**	**A**	เข้ารหัสทราฟฟิกทั้งหมดของอุปกรณ์และส่งผ่านเซิร์ฟเวอร์ VPN
☐	**2. อุโมงค์ VPN**	**B**	ส่งข้อมูลผ่านเซิร์ฟเวอร์อาสาสมัครสามตัว โดยเข้ารหัสเป็นชั้นๆ ในแต่ละชั้น
☐	**3. เครือข่าย Tor**	**C**	การกำหนดเส้นทางการเชื่อมต่อผ่านเซิร์ฟเวอร์ของประเทศอื่นเพื่อเลี่ยงการบล็อกตามภูมิศาสตร์
☐	**4. เว็บพร็อกซี**	**D**	ป้ายกำกับตัวเลขเฉพาะที่ระบุอินเทอร์เฟซของอุปกรณ์บนอินเทอร์เน็ต
☐	**5. DNS รั่วไหล**	**E**	เปลี่ยนเส้นทางทราฟฟิกเบราว์เซอร์ที่ชั้นแอปพลิเคชันโดยไม่มีการเข้ารหัสระดับระบบ
☐	**6. WebRTC API**	**F**	การบันทึกปลายทางทราฟฟิกอินเทอร์เน็ตที่ไม่ได้เข้ารหัสโดยผู้ให้บริการโทรคมนาคมของคุณ
☐	**7. การปกปิดตำแหน่งที่ตั้ง**	**G**	คำค้นหาที่ถูกแก้ไขนอกอุโมงค์ VPN ทำให้โดเมนที่เข้าชมถูกเปิดเผยต่อ ISP
☐	**8. การติดตามโดย ISP**	**H**	ฟีเจอร์ของเบราว์เซอร์สำหรับเสียง/วิดีโอที่สามารถข้ามอุโมงค์และเปิดเผยที่อยู่ IP จริงได้

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

3. เปลี่ยนเส้นทางทราฟฟิกของเบราว์เซอร์ที่ชั้นแอปพลิเคชันโดยไม่เข้ารหัสระดับระบบ (8)

5. ป้ายกำกับตัวเลขเฉพาะที่ระบุอินเทอร์เฟซของอุปกรณ์บนอินเทอร์เน็ต (6)

6. ส่งข้อมูลผ่านเซิร์ฟเวอร์อาสาสมัครสามเครื่อง โดยเข้ารหัสเป็นชั้นในแต่ละชั้น (3)

7. การกำหนดเส้นทางการเชื่อมต่อผ่านเซิร์ฟเวอร์ของประเทศอื่นเพื่อข้ามการบล็อกตามภูมิศาสตร์ (9)

8. เข้ารหัสทราฟฟิกทั้งหมดของอุปกรณ์และส่งผ่านเซิร์ฟเวอร์ VPN (5)

แนวตั้ง

1. คิวรีที่ถูกแปลงนอกอุโมงค์ VPN ทำให้ ISP เห็นโดเมนที่เข้าชม (9)

2. ฟีเจอร์เบราว์เซอร์สำหรับเสียงและวิดีโอที่อาจข้ามอุโมงค์และเผยที่อยู่ไอพีจริง (8)

4. การบันทึกปลายทางของทราฟฟิกอินเทอร์เน็ตที่ไม่เข้ารหัสโดยผู้ให้บริการโทรคมนาคมของคุณ (8)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

3 แนวนอน: เปลี่ยนเส้นทางทราฟฟิกของเบราว์เซอร์ที่ชั้นแอปพลิเคชันโดยไม่เข้ารหัสระดับระบบ (8 ตัวอักษร):

5 แนวนอน: ป้ายกำกับตัวเลขเฉพาะที่ระบุอินเทอร์เฟซของอุปกรณ์บนอินเทอร์เน็ต (6 ตัวอักษร):

6 แนวนอน: ส่งข้อมูลผ่านเซิร์ฟเวอร์อาสาสมัครสามเครื่อง โดยเข้ารหัสเป็นชั้นในแต่ละชั้น (3 ตัวอักษร):

7 แนวนอน: การกำหนดเส้นทางการเชื่อมต่อผ่านเซิร์ฟเวอร์ของประเทศอื่นเพื่อข้ามการบล็อกตามภูมิศาสตร์ (9 ตัวอักษร):

8 แนวนอน: เข้ารหัสทราฟฟิกทั้งหมดของอุปกรณ์และส่งผ่านเซิร์ฟเวอร์ VPN (5 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: คิวรีที่ถูกแปลงนอกอุโมงค์ VPN ทำให้ ISP เห็นโดเมนที่เข้าชม (9 ตัวอักษร):

2 แนวตั้ง: ฟีเจอร์เบราว์เซอร์สำหรับเสียงและวิดีโอที่อาจข้ามอุโมงค์และเผยที่อยู่ไอพีจริง (8 ตัวอักษร):

4 แนวตั้ง: การบันทึกปลายทางของทราฟฟิกอินเทอร์เน็ตที่ไม่เข้ารหัสโดยผู้ให้บริการโทรคมนาคมของคุณ (8 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	ฟ	บ	า	า	ห	ก	นี	า	ม	กี	จ	า	า
รี	ต	ค์	ว	ย	ง	ก	า	ค	จ	ที่	น	ตี	ว	ร
ตี	ว	ง	า	ล	ล	ด	ร	า	อ	อ	ย	ช	ฟ	ก
ง	ก	ม	ล	ม	า	ป	ติ	อ	อ	ยู่	ม	มี	า	ล
น่	ล	โ	ป	จ	รั่	า	ด	นี	กี	ไ	พ	ร	เ	ง
ห	า	อุ	ช	า	ว	า	ต	ลี	จ	อ	ดี	า	ว็	น
แ	ล	ผ	ดี	ช	ดี	ก	า	เ	ด	พี	า	ต	บ	า
ตำ	จ	า	ค	ก	เ	ดี	ม	ว็	า	ช	ว	ก	พ	ด
ด	กี	ด	ท	ผ	อ็	ฟ	ช	บ	มี	ม	อ	ต	ร็	ฟ
ปิ	ร	ดี	า	ท	น	ท	า	อ	ส	ท	ข	ข	อ	า
ก	น	ก	า	ล	เ	อ	า	า	ม	ร	มี	า	ก	ร
ป	ช	ก	ด	ง	อ	ร์	น	ร์	ร	ต	สี	ย	ซี	ข
มี	ดี	ด	ด	ว	ส	บ	ฟ	ที	อ	า	ร	ห	ห	รี
น	ผ	นี	ม	ผ	ดี	ข	กี	ซี	ส	บ	ลี	ง	ด	ร
ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด

รายการคำศัพท์

ที่อยู่ไอพี อุโมงค์ ทอร์ เว็บพร็อกซี รั่วดีเอ็นเอส เว็บอาร์ทีซี ปกปิดตำแหน่งการติดตาม

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. ที่อยู่ไอพี

B. อุโมงค์

C. ทอร์

D. เว็บพร็อกซี

E. รั่วดีเอ็นเอส

F. เว็บอาร์ทีซี

G. ปกปิดตำแหน่ง

H. การติดตาม

คำนิยามและช่องจับคู่

1. เปลี่ยนเส้นทางทราฟฟิกของเบราว์เซอร์ที่ชั้นแอปพลิเคชันโดยไม่เข้ารหัสระดับระบบ

2. การกำหนดเส้นทางการเชื่อมต่อผ่านเซิร์ฟเวอร์ของประเทศอื่นเพื่อข้ามการบล็อกตามภูมิศาสตร์

3. ฟีเจอร์เบราว์เซอร์สำหรับเสียงและวิดีโอที่อาจข้ามอุโมงค์และเผยที่อยู่ไอพีจริง

4. ป้ายกำกับตัวเลขเฉพาะที่ระบุอินเทอร์เฟซของอุปกรณ์บนอินเทอร์เน็ต

5. ส่งข้อมูลผ่านเซิร์ฟเวอร์อาสาสมัครสามเครื่อง โดยเข้ารหัสเป็นชั้นในแต่ละชั้น

6. การบันทึกปลายทางของทราฟฟิกอินเทอร์เน็ตที่ไม่เข้ารหัสโดยผู้ให้บริการโทรคมนาคมของคุณ

7. คิวรีที่ถูกแปลงนอกอุโมงค์ VPN ทำให้ ISP เห็นโดเมนที่เข้าชม

8. เข้ารหัสทราฟฟิกทั้งหมดของอุปกรณ์และส่งผ่านเซิร์ฟเวอร์ VPN

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของ VPN เขียนคำตอบของคุณในช่องกรอกที่กรอกได้

1. ยู่ที่ไอพีอ
2. ร์อท
3. รั่นอ็วเสเอดี
4. ตำงน่ดหแปกปิ
5. มค์อุงโ
6. กซีพอเร็ว็บ
7. เซีาร์ทีว็อบ
8. ติาดมกาตร

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	เหตุผลที่ควรใช้ VPN ขณะเดินทาง			
2	เบราว์เซอร์ที่คุณรู้จัก			
3	สิ่งที่ VPN ซ่อนได้			
4	คำที่เกี่ยวข้องกับความเป็นส่วนตัว			
5	คำจากใบงานนี้ที่คุณอยากจำ			
6	สิ่งที่เว็บไซต์เดาได้จาก IP ของคุณ			
7	ตัวเลขหรือสัญลักษณ์ในที่อยู่ IP			
8	ความเชื่อผิด ๆ เกี่ยวกับ VPN			
9	บริการ VPN ที่คุณรู้จัก			
10	สิ่งที่ผู้ให้บริการอินเทอร์เน็ตของคุณมองเห็นได้			
11	คำมั่นสัญญาที่ผู้ให้บริการ VPN ที่ดีให้ไว้			
12	สิ่งที่ทำให้ IP จริงของคุณรั่วไหลได้			
13	เหตุผลที่ควรซ่อนตำแหน่งของคุณ			
14	วิธีซ่อนที่อยู่ IP ของคุณ			
15	อุปกรณ์ที่ใช้ VPN ได้			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

ซาราห์ (นักเรียนร้านกาแฟ)

👷 "สวัสดี! ฉันนั่งอยู่ที่ Coffee & Bytes มีเครือข่ายสาธารณะที่ไม่ปลอดภัยชื่อ 'Free_Wi-Fi_No_Password' ฉันอยากล็อกอินอีเมลโรงเรียนและอัปโหลดงานที่ได้รับมอบหมาย แต่กังวลเรื่องแฮกเกอร์ การใช้เครือข่ายนี้โดยไม่มี VPN มีความเสี่ยงอะไรบ้าง และ VPN ช่วยรักษาความปลอดภัยของข้อมูลฉันได้อย่างไร?"

อเล็กซ์ (นักเรียนนักท่องเที่ยว)

👷 "แย่แล้ว! ฉันเดินทางไปต่างประเทศเพื่อทำโปรเจกต์ และกำลังพยายามดูสารคดีชีววิทยาที่โฮสต์บนเซิร์ฟเวอร์ในประเทศบ้านเกิด แต่เว็บไซต์ขึ้นข้อความว่า 'วิดีโอนี้ไม่พร้อมใช้งานในตำแหน่งที่ตั้งปัจจุบันของคุณ' ทำไมฉันถึงถูกบล็อก และ VPN ช่วยให้ฉันดูได้อย่างไร?"

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

เพื่อให้การฝึกอบรมการปกปิด IP ของคุณเสร็จสมบูรณ์ ให้ถอดรหัสข้อความลับนี้เกี่ยวกับการซ่อนร่องรอยดิจิทัลของคุณ

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

11	63	45	25		23	52	63	45	34	56	63		2	45	7	4	55	19

20	64	39	34		35	47	26	26		37	48	26

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q1: VPN คืออะไรและทำงานอย่างไร?

Virtual Private Network (VPN) เข้ารหัสการเชื่อมต่ออินเทอร์เน็ตของคุณและส่งทราฟฟิกผ่านเซิร์ฟเวอร์ระยะไกลที่ปลอดภัย ซึ่งปกปิดที่อยู่ IP สาธารณะของคุณและจำกัดสิ่งที่ผู้สังเกตการณ์ในเครือข่ายท้องถิ่นและ ISP ของคุณมองเห็นเกี่ยวกับทราฟฟิกที่ผ่านอุโมงค์ VPN

Q2: ทำไมฉันควรใช้ VPN?

VPN ปกป้องความเป็นส่วนตัวทางดิจิทัลของคุณ รักษาความปลอดภัยของการเชื่อมต่อบนเครือข่าย Wi-Fi สาธารณะ (เช่น ร้านกาแฟหรือสนามบิน) อาจลดการหน่วงความเร็วตามกิจกรรมเมื่อ ISP ระบุประเภทของทราฟฟิกที่เข้ารหัสไม่ได้ ข้ามข้อจำกัดทางภูมิศาสตร์เพื่อเข้าถึงเนื้อหาทั่วโลก และช่วยรักษาความปลอดภัยของทรัพยากรการทำงานระยะไกล

Q3: VPN ทำให้ฉันไม่เปิดเผยตัวตนบนออนไลน์โดยสมบูรณ์หรือไม่?

ไม่ แม้ VPN จะซ่อนที่อยู่ IP ของคุณและเข้ารหัสการรับส่งข้อมูล แต่คุณก็ยังถูกติดตามได้ผ่านคุกกี้ของเบราว์เซอร์ บัญชีที่ล็อกอินอยู่ (เช่น Google หรือ Facebook) การพิมพ์ลายนิ้วมือเบราว์เซอร์ หรือหากผู้ให้บริการ VPN ของคุณบันทึกข้อมูลของคุณ

Q4: เว็บพร็อกซีซ่อน IP address ของฉันได้หรือไม่?

ใช่ แต่เฉพาะทราฟฟิกที่ส่งผ่านพร็อกซีเท่านั้น ซึ่งโดยปกติคือเบราว์เซอร์ของคุณ พร็อกซีเว็บส่วนใหญ่ไม่เข้ารหัสข้อมูลของคุณ ดังนั้น ISP หรือผู้ให้บริการเครือข่ายของคุณยังเห็นสิ่งที่คุณส่งและรับได้

Q5: การซ่อน IP ของฉันถูกกฎหมายหรือไม่?

ในหลายประเทศใช่ แต่บางประเทศจำกัดหรือห้าม VPN และเครื่องมืออื่นที่ใช้ซ่อนที่อยู่ IP การซ่อน IP ของคุณไม่ทำให้การกระทำที่ผิดกฎหมายกลายเป็นถูกกฎหมาย ดังนั้นควรตรวจสอบกฎหมายท้องถิ่นก่อนใช้

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดที่ผู้สนใจมีเกี่ยวกับการใช้เครือข่ายส่วนตัวเสมือน

Q6: Tor ซ่อน IP ของฉันหรือไม่?

ได้ Tor ส่งทราฟฟิกของคุณผ่านรีเลย์อาสาสมัครสามจุด (guard, middle และ exit) เว็บไซต์จึงเห็นที่อยู่ของรีเลย์ exit และไม่มีรีเลย์ใดรู้ทั้งตัวตนของคุณและจุดหมายปลายทาง [1]

Q7: IP ของฉันเปิดเผยอะไรบ้าง?

IP สาธารณะของคุณมักเผย ISP และตำแหน่งโดยประมาณ เช่น ประเทศหรือเมืองของคุณ เว็บไซต์ยังใช้ IP นี้เชื่อมโยงการเข้าชมของคุณเข้าด้วยกันและใช้บล็อกตามภูมิภาคได้

Q8: ฉันตรวจสอบได้อย่างไรว่าถูกซ่อนอยู่?

เชื่อมต่อ VPN จากนั้นเข้าเว็บไซต์ตรวจสอบ IP และรันการทดสอบการรั่วไหลของ DNS และ WebRTC IP และเซิร์ฟเวอร์ DNS ที่แสดงควรเป็นของ VPN ไม่ใช่ของ ISP ของคุณ หากปรากฏ IP จริงของคุณ ให้เปิดการป้องกันการรั่วไหล

Q9: ฉันใช้ VPN บนโทรศัพท์และสมาร์ททีวีได้หรือไม่?

ได้ ผู้ให้บริการ VPN สมัยใหม่มีแอปเฉพาะสำหรับ iOS, Android, macOS, Windows, Linux และสมาร์ททีวี รวมถึงการตั้งค่าบนเราเตอร์เพื่อปกป้องทุกอุปกรณ์ในเครือข่ายบ้านของคุณ

Q10: Kill Switch คืออะไร?

Kill Switch คือฟีเจอร์ความปลอดภัยที่ตัดการเชื่อมต่ออุปกรณ์ของคุณจากอินเทอร์เน็ตโดยอัตโนมัติหากการเชื่อมต่อ VPN หลุด ช่วยป้องกันไม่ให้ข้อมูลที่ไม่ได้เข้ารหัสหรือที่อยู่ IP จริงของคุณรั่วไหล

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคและโครงสร้างของเครือข่ายส่วนตัวเสมือนและโปรโตคอลอุโมงค์ที่ปลอดภัย

Q1: ทำไมเว็บไซต์ยังติดตามฉันได้หลังจากซ่อนที่อยู่ IP แล้ว?

การซ่อน IP ของคุณไม่ได้หยุดลายนิ้วมือเบราว์เซอร์ ตัวติดตามสามารถรวมรายละเอียดอย่างความละเอียดหน้าจอ ฟอนต์ที่ติดตั้ง และการตั้งค่าเบราว์เซอร์ของคุณให้เป็นตัวระบุได้ และคุกกี้หรือบัญชีที่ลงชื่อเข้าใช้ก็ระบุตัวคุณได้เช่นกัน ดังนั้นควรใช้เบราว์เซอร์ที่เน้นความเป็นส่วนตัวด้วย [3]

Q2: การกำหนดเส้นทางแบบ double VPN หรือ Multi-Hop คืออะไร?

Multi-Hop ส่งการรับส่งข้อมูลของคุณผ่านเซิร์ฟเวอร์ VPN สองเครื่องขึ้นไปตามลำดับ ซึ่งเพิ่มการเข้ารหัสชั้นที่สองและช่วยซ่อนที่อยู่ IP จริงของคุณจากฮอปที่สองหากเซิร์ฟเวอร์ใดเครื่องหนึ่งถูกบุกรุก

Q3: การรั่วไหลของ WebRTC คืออะไร และ VPN ป้องกันได้อย่างไร?

WebRTC คือโปรโตคอลของเบราว์เซอร์ที่อาจเปิดเผยที่อยู่ IP ภายในและสาธารณะจริงของคุณ แม้จะเปิดใช้ VPN อยู่ VPN ระดับพรีเมียมจะบล็อกหรือปลอมคำขอ WebRTC ในแอปเดสก์ท็อป/มือถือและส่วนขยายเบราว์เซอร์

Q4: ทราฟฟิก IPv6 ทำให้ IP address จริงของฉันรั่วไหลได้หรือไม่?

ได้ หาก VPN ของคุณทำอุโมงค์เฉพาะ IPv4 อุปกรณ์ของคุณอาจส่งทราฟฟิก IPv6 ออกนอกอุโมงค์ ทำให้เผยที่อยู่ที่ ISP กำหนดให้ ควรใช้ VPN ที่ทำอุโมงค์หรือบล็อก IPv6 และยืนยันด้วยการทดสอบการรั่วไหลของ IPv6

Q5: การพรางทราฟฟิก (Obfuscation) หลบเลี่ยงการบล็อก VPN ได้อย่างไร?

การอำพราง (หรือ "Stealth VPN") ทำให้แพ็กเก็ตทราฟฟิก VPN ดูเหมือนทราฟฟิกเว็บ HTTPS ปกติ (พอร์ต 443) ช่วยให้ผ่านการตรวจสอบแพ็กเก็ตเชิงลึก (DPI) ที่รัฐบาลหรือเครือข่ายโรงเรียน/สำนักงานใช้บล็อก VPN

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคและโครงสร้างของเครือข่ายส่วนตัวเสมือนและโปรโตคอลอุโมงค์ที่ปลอดภัย

Q6: split tunneling เปิดเผย IP address จริงของฉันหรือไม่?

ได้ สำหรับแอปที่คุณยกเว้น ทราฟฟิกที่ส่งออกนอกอุโมงค์จะใช้ IP จริงของคุณ และ RFC 8828 ระบุว่า WebRTC อาจเผยที่อยู่ของ ISP ที่อยู่ใต้ VPN แบบแยกอุโมงค์ได้ หากเบราว์เซอร์ไม่จำกัด [2]

Q7: IP address ที่ใช้ร่วมกันคืออะไร และช่วยความเป็นส่วนตัวอย่างไร?

เมื่อใช้ IP ร่วมกัน ผู้ใช้ VPN จำนวนมากจะปรากฏออนไลน์ด้วยที่อยู่เดียวกันในเวลาเดียวกัน ทำให้เว็บไซต์เชื่อมโยงการเข้าชมครั้งใดครั้งหนึ่งกับคุณได้ยากกว่า IP เฉพาะที่ใช้เพียงคนเดียวมาก

Q8: ISP ของฉันเห็นได้หรือไม่ว่าฉันใช้ VPN เพื่อซ่อน IP?

โดยปกติใช่ ISP ของคุณมองเห็นได้ว่าคุณเชื่อมต่อกับที่อยู่ IP ของเซิร์ฟเวอร์ VPN เมื่อใดที่คุณเชื่อมต่อ และคุณส่งข้อมูลมากเท่าใด แต่ไม่เห็นเว็บไซต์ที่คุณเยี่ยมชมหรือเนื้อหาภายในอุโมงค์ที่เข้ารหัส

Q9: การป้องกัน DNS Leak คืออะไร?

การป้องกันการรั่วไหลของ DNS บังคับให้อุปกรณ์ของคุณส่งคำค้นหาเว็บไซต์ (คำขอ DNS) ผ่านเซิร์ฟเวอร์ DNS ส่วนตัวที่เข้ารหัสของ VPN แทนเซิร์ฟเวอร์ของ ISP ซึ่งช่วยป้องกันไม่ให้ ISP ติดตามว่าคุณเข้าเว็บไซต์ใด

Q10: พร็อกซีหรือ VPN ดีกว่าสำหรับการซ่อน IP ของฉัน?

โดยทั่วไป VPN ดีกว่า เพราะซ่อน IP ของคุณสำหรับทุกแอปบนอุปกรณ์และเข้ารหัสทราฟฟิก ขณะที่พร็อกซีบนเว็บมักครอบคลุมเฉพาะเบราว์เซอร์และมักไม่เพิ่มการเข้ารหัส

ส่วนที่ 11: ข้อเท็จจริงน่าสนใจเกี่ยวกับ VPN 10 ข้อและข้อมูลเชิงลึกในโลกจริง

ทบทวนข้อเท็จจริงและข้อมูลเชิงลึกในโลกจริงที่มีคุณค่าสูงเกี่ยวกับประวัติ ตลาด และเทคโนโลยีของ VPN

1. โปรโตคอล VPN แรก

PPTP (Point-to-Point Tunneling Protocol) โปรโตคอล VPN ยุคแรกจากกลุ่มที่นำโดย Microsoft ในทศวรรษ 1990 ปัจจุบันถือว่าไม่ปลอดภัย VPN สมัยใหม่จึงใช้ WireGuard หรือ OpenVPN

2. การระบุลายนิ้วมือดิจิทัล

การซ่อน IP ของคุณไม่ได้หยุดลายนิ้วมือเบราว์เซอร์ ซึ่งสามารถระบุตัวคุณได้จากรายละเอียดอย่างความละเอียดหน้าจอและฟอนต์ที่ติดตั้ง [3]

3. การปฏิวัติ WireGuard

WireGuard มีโค้ดที่เรียบง่ายมากซึ่งออกแบบมาเพื่อประสิทธิภาพ ทำให้ตรวจสอบช่องโหว่ด้านความปลอดภัยได้ง่ายกว่าโปรโตคอลแบบดั้งเดิม

4. การเปิดเผยที่อยู่ WebRTC

RFC 8828 เตือนว่า WebRTC อาจค้นพบทั้งที่อยู่สาธารณะของ VPN และที่อยู่ ISP ที่ VPN ทำงานอยู่ เว้นแต่เบราว์เซอร์จะจำกัดไว้ [2]

5. จุดกำเนิดของพันธมิตร 5-Eyes

ความร่วมมือด้านข่าวกรอง Five Eyes ของสหรัฐฯ สหราชอาณาจักร แคนาดา ออสเตรเลีย และนิวซีแลนด์ เติบโตมาจากความร่วมมือด้านข่าวกรองสัญญาณระหว่างฝ่ายสัมพันธมิตรในยุคสงครามโลกครั้งที่สอง

6. การตรวจสอบแพ็กเก็ตเชิงลึก

ไฟร์วอลล์ขั้นสูงใช้ Deep Packet Inspection (DPI) เพื่อวิเคราะห์เมทาดาทาของแพ็กเก็ตเครือข่ายและบล็อกลักษณะการเชื่อมต่อ VPN มาตรฐาน

7. การใช้วงจร Tor ซ้ำ

Tor ใช้วงจรเดิมประมาณสิบนาทีแล้วสร้างวงจรใหม่ ซึ่งทำให้เชื่อมโยงกิจกรรมการท่องเว็บของคุณได้ยากขึ้น [1]

8. VPN แบบกระจายศูนย์

VPN แบบกระจายศูนย์ (dVPN) กระจายทราฟฟิกไปทั่วเครือข่ายโหนดที่ผู้ใช้ดูแลเอง ช่วยลดการพึ่งพาผู้ให้บริการส่วนกลางรายเดียว

9. ความเป็นนิรนามของ TOR เทียบกับ VPN

VPN ส่งทราฟฟิกผ่านผู้ให้บริการรายเดียว ส่วน Tor (The Onion Router) ส่งทราฟฟิกผ่านรีเลย์อาสาสมัครสามตัว (guard, middle, exit) เพื่อเพิ่มความเป็นส่วนตัวสูงสุด [1]

10. พร็อกซีเทียบกับอุโมงค์ VPN

เว็บพร็อกซีเปลี่ยนที่อยู่ IP ที่เว็บไซต์เห็นสำหรับทราฟฟิกเบราว์เซอร์ของคุณ แต่ต่างจาก VPN ตรงที่มักไม่เข้ารหัสทราฟฟิกนั้นหรือครอบคลุมแอปอื่นบนอุปกรณ์ของคุณ [5]

แหล่งอ้างอิงทางเทคนิค

สิ่งพิมพ์ที่อ้างอิง ข้อกำหนดด้านการเข้ารหัส และมาตรฐานเอกสารทางการที่ใช้ตลอดทั้งใบงานนี้

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

เฉลย: การซ่อนที่อยู่ IP การปกปิดตำแหน่ง พร็อกซี Tor และการป้องกันการรั่วไหลของ DNS/WebRTC

1 คำถาม 1

คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

ที่อยู่ IP สาธารณะของอุปกรณ์เปิดเผยอะไรให้เว็บไซต์ที่คุณเข้าชมทราบ? → ตำแหน่งโดยประมาณของคุณและชื่อ ISP ของคุณ

2 การเข้ารหัสระบบของ VPN เวลาแฝง

คำตอบที่ถูกต้อง: C

หมายเหตุสำหรับผู้สอน

ต่างจากพร็อกซีที่เปลี่ยนเส้นทางเฉพาะทราฟฟิกของเบราว์เซอร์ VPN สร้างอุโมงค์เข้ารหัสทั่วทั้งระบบ ปกป้องแอปเบื้องหลัง เกม และคำขอของระบบปฏิบัติการ อ้างอิง: Tor Project Relays, W3C WebRTC API.

3 การขาดการเข้ารหัสของพร็อกซี ความปลอดภัย Wi-Fi

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

พร็อกซีเว็บเพียงส่งต่อทราฟฟิกของเบราว์เซอร์โดยไม่เข้ารหัสเพย์โหลดของแพ็กเก็ต ซึ่งหมายความว่าผู้ให้บริการเครือข่ายหรือ ISP ของคุณยังคงติดตามทราฟฟิกเนื้อหาของคุณได้ การอ้างอิง: IETF Proxy Vulnerabilities.

4 คำถาม 4

คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

เครือข่าย Tor ให้ความไม่เปิดเผยตัวตนระดับสูงแก่ผู้ใช้ได้อย่างไร? → โดยการส่งทราฟฟิกผ่านรีเลย์สามตัวที่ดำเนินการโดยอาสาสมัคร

5 การรั่วไหลของ DNS Tunnel ความเป็นส่วนตัว

คำตอบที่ถูกต้อง: B

หมายเหตุสำหรับผู้สอน

DNS รั่วไหลเกิดขึ้นเมื่อคำขอแปลงชื่อโดเมนหลบอุโมงค์ VPN และไปยังรีโซลเวอร์ของ ISP โดยตรง ทำให้บันทึกโดเมนที่เข้าชมถูกเปิดเผย อ้างอิง: DNSSEC Tunnel Testing, EFF Tracking Evasion.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **รายละเอียดข้อจำกัดของพร็อกซี** การปกปิด IP — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

พร็อกซีทำงานที่ชั้นแอปพลิเคชันและไม่มีการผสานไดรเวอร์เครือข่ายทั้งระบบเหมือนอุโมงค์ VPN อ้างอิง: IETF Proxy Vulnerabilities.

7 **คำถาม 7** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

การส่งทราฟฟิกผ่านรีเลย์อาสาสมัครสามตัวพร้อมการเข้ารหัสหลายชั้นเพิ่มเวลาแฝง Tor จึงมักช้ากว่าการเชื่อมต่อโดยตรง

8 **คำถาม 8** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

WebRTC อาจเปิดเผยที่อยู่ภายในเครื่อง และในการตั้งค่า VPN บางแบบ อาจเปิดเผยที่อยู่ IP สาธารณะที่ ISP กำหนดให้ซึ่งอยู่ใต้อุโมงค์ (RFC 8828)

9 **คำถาม 9** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

หากไม่มีการรั่วไหลของ DNS หรือ WebRTC ISP จะเห็นเพียงทราฟฟิกที่เข้ารหัสไปยังเซิร์ฟเวอร์ VPN ไม่เห็นเว็บไซต์ที่คุณเข้าชม

10 **ข้อจำกัดของการสร้างลายนิ้วมือ** ไม่เก็บล็อก — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

การสร้างลายนิ้วมือ (fingerprinting) มุ่งเป้าไปที่เมตริกการกำหนดค่าอุปกรณ์ (ความละเอียดหน้าจอ ฟอนต์ ปลั๊กอิน) ซึ่งยังมองเห็นได้แม้ซ่อน IP แหล่งอ้างอิง: EFF Tracking Evasion.

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

D 1. ที่อยู่ IP	A 2. อุโมงค์ VPN	B 3. เครือข่าย Tor	E 4. เว็บพร็อกซี
G 5. DNS รั่วไหล	H 6. WebRTC API	C 7. การปกปิดตำแหน่งที่ตั้ง	F 8. การติดตามโดย ISP

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 รั่วดีเอ็นเอส	2 เว็บอาร์ทีซี	3 เว็บพร็อกซี	4 ทอร์
5 ที่อยู่ไอพี	6 ปกปิดตำแหน่ง		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 D – เว็บพร็อกซี	2 G – ปกปิดตำแหน่ง	3 F – เว็บอาร์ทีซี	4 A – ที่อยู่ไอพี
5 C – ทอร์	6 H – การติดตาม	7 E – รั่วดีเอ็นเอส	8 B – อุโมงค์

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย ที่อยู่ IP อุโมงค์ VPN และ เครือข่าย Tor ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

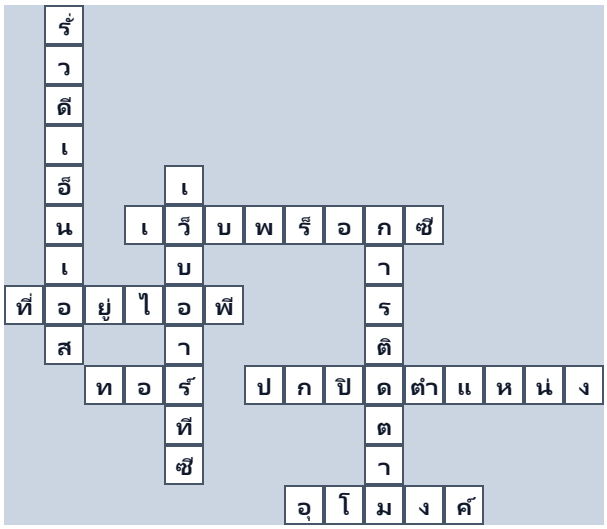
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ฟ	บ	า	า	ห	ก	นี	า	ม	กี	จ	า	า
รี	ต	ค์	ว	ย	ง	ก	า	ค	จ	ที่	น	ตี	ว	ร
ดี	ว	ง	า	ล	ล	ด	ร	า	อ	อ	ย	ช	ฟ	ก
ง	ก	ม	ล	ม	า	ป	ดิ	อ	อ	ยู่	ม	มี	า	ล
น่	ล	โ	ป	จ	รั่	า	ด	นี	กี	ไ	พ	ร	เ	ง
ห	า	อุ	ช	า	ว	า	ต	ลี	จ	อ	ดี	า	ว็	น
แ	ล	ผ	ดี	ช	ดี	ก	า	เ	ด	พี	า	ต	บ	า
ตำ	จ	า	ค	ก	เ	ดี	ม	ว็	า	ช	ว	ก	พ	ด
ด	กี	ด	ท	ผ	อ็	ฟ	ช	บ	มี	ม	อ	ต	ร็	ฟ
ปิ	ร	ดี	า	ท	น	ท	า	อ	ส	ท	ข	ข	อ	า
ก	น	ก	า	ล	เ	อ	า	า	ม	ร	มี	า	ก	ร
ป	ช	ก	ด	ง	อ	ร์	น	ร์	ร	ต	สี	ย	ซี	ข
มี	ดี	ด	ด	ว	ส	บ	ฟ	ที	อ	า	ร	ห	ห	รี
น	ผ	นี	ม	ผ	ดี	ข	กี	ซี	ส	บ	ลี	ง	ด	ร
ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

3 แนวนอน: เว็บพร็อกซี เปลี่ยนเส้นทางทราฟฟิกของเบราว์เซอร์ที่ชั้นแอปพลิเคชันโดยไม่เข้ารหัสระดับระบบ (8 ตัวอักษร)

5 แนวนอน: ที่อยู่ไอพี ป้ายกำกับตัวเลขเฉพาะที่ระบุอินเทอร์เฟซของอุปกรณ์บนอินเทอร์เน็ต (6 ตัวอักษร)

6 แนวนอน: ทอร์ ส่งข้อมูลผ่านเซิร์ฟเวอร์อาสาสมัครสามเครื่อง โดยเข้ารหัสเป็นชั้นในแต่ละชั้น (3 ตัวอักษร)

7 แนวนอน: ปกปิดตำแหน่ง การกำหนดเส้นทางการเชื่อมต่อผ่านเซิร์ฟเวอร์ของประเทศอื่นเพื่อข้ามการบล็อกตามภูมิศาสตร์ (9 ตัวอักษร)

8 แนวนอน: อุโมงค์ เข้ารหัสทราฟฟิกทั้งหมดของอุปกรณ์และส่งผ่านเซิร์ฟเวอร์ VPN (5 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: รั่วดีเอ็นเอส คิวรีที่ถูกแปลงนอกอุโมงค์ VPN ทำให้ ISP เห็นโดเมนที่เข้าชม (9 ตัวอักษร)

2 แนวตั้ง: เว็บอาร์ทีซี ฟีเจอร์เบราว์เซอร์สำหรับเสียงและวิดีโอที่อาจข้ามอุโมงค์และเผยที่อยู่ไอพีจริง (8 ตัวอักษร)

4 แนวตั้ง: การติดตาม การบันทึกปลายทางของทราฟฟิกอินเทอร์เน็ตที่ไม่เข้ารหัสโดยผู้ให้บริการโทรคมนาคมของคุณ (8 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ยู่ที่ไอพือ — ที่อยู่ไอพี
2. ร์อท — ทอร์
3. รั่นอ็วเสเอดี — รั่วดีเอ็นเอส
4. ตำงน่ดหแปกปิ — ปกปิดตำแหน่ง
5. มศ์อุงโ — อุโมงศ์
6. กซีพอเร็วิบ — เว็บพร็อกซี
7. เซ้าร์ทีวิอบ — เว็บอาร์ทีซี
8. ติาดมกาตร — การติดตาม

เฉลยภารกิจรหัสลับ

"ซ่อน ที่อยู่ ของคุณ ด้วย ระบบ ลับ"

เฉลยกรณีศึกษา

A สถานการณ์ A: ความปลอดภัยของเครือข่ายสาธารณะ

การดักจับแพ็กเก็ตและการเข้ารหัส | ความกังวลของซาราห์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- ความเสี่ยง: การดักจับแพ็กเก็ต การสกัดกั้นข้อมูล และการโจมตีแบบ man-in-the-middle ผู้ที่อยู่ในเครือข่ายร้านกาแฟเดียวกันอาจดักจับรายละเอียดการล็อกอินหรือไฟล์การบ้านของเธอได้
- การป้องกันของ VPN: เข้ารหัสเพย์โหลดของแพ็กเก็ตเครือข่าย ทำให้ทราฟฟิกอุโมงค์ที่ถูกดักอ่านไม่ได้สำหรับผู้แอบดูในเครือข่ายท้องถิ่นแบบพาสซีฟ เมื่อตั้งค่า VPN อย่างถูกต้อง

B สถานการณ์ B: การเข้าถึงทรัพยากรที่ถูกบล็อก

การบล็อกตามภูมิศาสตร์และ IP | ปัญหาของอเล็กซ์

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- เหตุผลที่ถูกบล็อก: โฮสต์สตรีมมิงใช้การบล็อกตามภูมิศาสตร์ ซึ่งจับคู่ที่อยู่ IP ท้องถิ่นของผู้เดินทางกับประเทศจริงของเขาและบล็อกตามการอนุญาตให้ใช้สิทธิ์ตามอาณาเขต
- VPN ช่วยได้อย่างไร: ปกปิดตำแหน่งจริงของเขาโดยกำหนดเส้นทางทราฟฟิกผ่านเซิร์ฟเวอร์ในประเทศบ้านเกิดของเขา เว็บไซต์จะเห็น IP ของประเทศบ้านเกิด ทำให้เข้าถึงได้