ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

ความปลอดภัยของ CyberGhost

การประเมินโครงสร้างพื้นฐานความปลอดภัยของ CyberGhost อาร์เรย์เซิร์ฟเวอร์ NoSpy ที่เป็นเจ้าของเองในโรมาเนีย โหนดเซิร์ฟเวอร์ไร้ดิสก์ที่ใช้เฉพาะ RAM การเข้ารหัส AES-256 และการป้องกันด้วย kill switch อัตโนมัติ

ภาพรวมการเรียนรู้ความปลอดภัย CYBERGHOST

ผู้เรียน
สถานะนักเรียน
สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย
สถานะการเชื่อมต่อ
การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน
การป้องกันการรั่วไหล
การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับฟีเจอร์ความปลอดภัยของ CyberGhost คุณจะได้สำรวจชุดเซิร์ฟเวอร์ NoSpy ที่เป็นเจ้าของเอง ฮาร์ดแวร์แบบ RAM เท่านั้นที่ไม่มีดิสก์ ชุดรหัส และ kill switch

จุดตรวจสอบของใบงาน

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

เปิดคู่มือ VPN ที่ดีที่สุดของ VPN.com

URL: https://www.vpn.com/th/vpn/cyberghost/khwam-plodphai/

เส้นทางการเรียนรู้ความปลอดภัยของ CyberGhost ของคุณ

- วิเคราะห์สถาปัตยกรรมทางเทคนิคและกฎการกำหนดค่าของความปลอดภัยของ CyberGhost
- ตั้งค่าไคลเอนต์เพื่อป้องกันการรั่วไหลของทราฟฟิก IP, DNS และ WebRTC
- เปรียบเทียบราคากำหนดเอง ช่วงทดลอง และฟีเจอร์ด้านประสิทธิภาพกับรุ่นมาตรฐาน

คำแนะนำคู่มือความปลอดภัย CYBERGHOST

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การเข้ารหัสและเซิร์ฟเวอร์ NoSpy ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

โครงสร้างพื้นฐานเซิร์ฟเวอร์ NoSpy ที่เป็นเจ้าของเองและโหนดแบบไร้ดิสก์ (บทนำ)

CyberGhost ดำเนินการเซิร์ฟเวอร์ NoSpy ที่บริหารจัดการเองจากสำนักงานใหญ่ที่บูคาเรสต์ ประเทศโรมาเนีย จึงหลีกเลี่ยงความเสี่ยงจากโฮสต์เชิงพาณิชย์ ความปลอดภัยบังคับใช้ผ่านชุดรหัส AES-256 ฮาร์ดแวร์ RAM-only ไร้ดิสก์ และ Kill Switch อัตโนมัติ

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **1. CyberGhost มีโปรโตคอลใดให้ใช้บนทุกแพลตฟอร์มหลัก?**
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) L2TP

2. **2. การเชื่อมต่อ OpenVPN และ IKEv2 ของ CyberGhost ใช้รหัสลับ (cipher) ใด?**
   - A) AES-256
   - B) Blowfish-128
   - C) DES-56
   - D) RC4

3. **3. เซิร์ฟเวอร์ NoSpy ที่ CyberGhost ดำเนินการเองตั้งอยู่ที่ใด?**
   - A) โรมาเนีย
   - B) เยอรมนี
   - C) สหรัฐอเมริกา
   - D) สวิตเซอร์แลนด์

4. **4. โครงสร้างพื้นฐานแบบใดที่ไม่เก็บบันทึกลงดิสก์เมื่อปิดเครื่อง?**
   - A) เซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น
   - B) เซิร์ฟเวอร์ HDD
   - C) เซิร์ฟเวอร์เสมือน
   - D) เซิร์ฟเวอร์ไฮบริด

5. **5. ฟีเจอร์ใดที่บล็อกการเชื่อมต่อระหว่างที่ VPN หลุด?**
   - A) Kill Switch
   - B) Split tunneling
   - C) Smart DNS
   - D) ส่งต่อพอร์ต

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. CyberGhost มีสำนักงานใหญ่ในโรมาเนีย ซึ่งอยู่นอกกลุ่ม 14-Eyes

○ จริง ○ เท็จ

7 คำถาม 7

7. เซิร์ฟเวอร์ NoSpy เช่าจากดาต้าเซ็นเตอร์เชิงพาณิชย์ของบุคคลที่สาม

○ จริง ○ เท็จ

8 คำถาม 8

8. เซิร์ฟเวอร์แบบ RAM-only เขียนข้อมูลเซสชันของผู้ใช้ลงในไดรฟ์ SSD ถาวร

○ จริง ○ เท็จ

9 คำถาม 9

9. แอปไคลเอนต์มีการป้องกันการรั่วไหลของ DNS ในตัว

○ จริง ○ เท็จ

10 คำถาม 10

10. นโยบาย zero-logs ของ CyberGhost ได้รับการยืนยันโดยการตรวจสอบอิสระ

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. โพรโทคอลประสิทธิภาพสูงที่แนะนำสำหรับการเชื่อมต่อบนมือถือคือ _____
2. ทราฟฟิกถูกเข้ารหัสด้วยรหัสลับแบบสมมาตรที่ปลอดภัยสูงมาตรฐาน _____ 256
3. สำนักงานใหญ่ของบริษัทตั้งอยู่ในเขตอำนาจของ _____
4. เซิร์ฟเวอร์ความปลอดภัยสูงที่บริษัทเป็นเจ้าของและบริหารเองเรียกว่า _____
5. เพื่อไม่ให้ข้อมูลคงอยู่หลังปิดเครื่อง พวกเขาใช้เซิร์ฟเวอร์ไร้ดิสก์แบบ _____
6. การรั่วไหลของทราฟฟิกที่ไม่เข้ารหัสขณะเชื่อมต่อหลุดป้องกันได้ด้วยสวิตช์กันพลาดแบบ _____

คลังคำศัพท์

คิลสวิตช์ ตรวจสอบ โนสปาย รั่วไหล แรมล้วน โรมาเนีย ไวร์การ์ด เอเอส

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่อง VPN และเครือข่าย

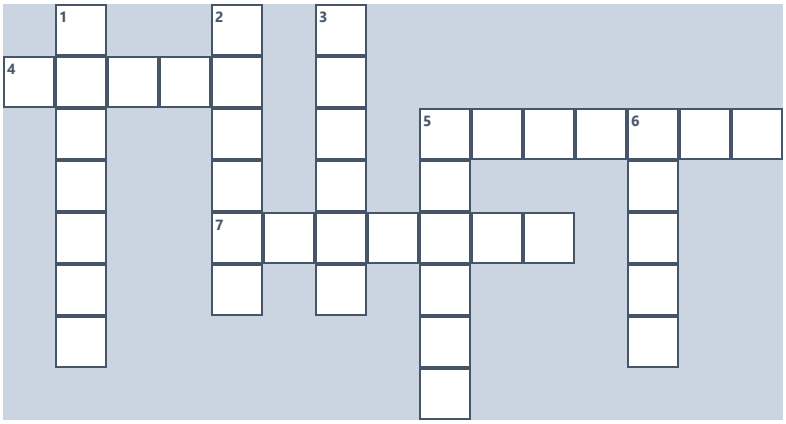
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. WireGuard**	**A**	เขตอำนาจศาลด้านความเป็นส่วนตัวระดับประเทศที่ตั้งอยู่นอกพันธมิตร 14 Eyes
☐	**2. AES-256**	**B**	โครงสร้างพื้นฐานเซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เขียนบันทึกถาวรเลย
☐	**3. โรมาเนีย**	**C**	การเปิดเผยคำขอ resolver นอก VPN โดยไม่ตั้งใจ
☐	**4. NoSpy**	**D**	โปรโตคอลโอเพนซอร์สความเร็วสูงที่มีในแอป CyberGhost ทุกแพลตฟอร์ม
☐	**5. เฉพาะ RAM**	**E**	การตรวจสอบยืนยันโดยบุคคลที่สามที่ทบทวนข้ออ้างเรื่องการปฏิบัติตามนโยบายไม่เก็บบันทึก
☐	**6. KILL SWITCH**	**F**	มาตรฐานรหัสสมมาตรที่ปกป้องเพย์โหลดที่ส่งผ่านอุโมงค์
☐	**7. การรั่วไหล**	**G**	กลุ่มเซิร์ฟเวอร์ความปลอดภัยสูงที่เป็นเจ้าของเองทั้งหมดซึ่งดำเนินการในโรมาเนีย
☐	**8. การตรวจสอบ**	**H**	ยูทิลิตี้ไคลเอนต์ป้องกันความล้มเหลวที่ตัดทราฟฟิกอินเทอร์เน็ตเมื่อหลุด

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

4. การเปิดเผยคำขอตัวแปลงชื่อออกนอก VPN โดยไม่ตั้งใจ (5)

5. เขตอำนาจด้านความเป็นส่วนตัวของประเทศที่อยู่นอกพันธมิตร 14-Eyes (7)

7. การตรวจสอบโดยบุคคลที่สามที่ทบทวนคำกล่าวอ้างเรื่องการไม่เก็บบันทึก (7)

แนวตั้ง

1. โพรโทคอลโอเพนซอร์สความเร็วสูงที่มีในแอป CyberGhost ทุกตัว (7)

2. ยูทิลิตีกันพลาดของไคลเอนต์ที่ตัดทราฟฟิกอินเทอร์เน็ตเมื่อการเชื่อมต่อหลุด (6)

3. โครงสร้างพื้นฐานเซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เขียนบันทึกถาวรเลย (6)

5. กลุ่มเซิร์ฟเวอร์ความปลอดภัยสูงที่บริษัทเป็นเจ้าของและบริหารเองในโรมาเนีย (6)

6. มาตรฐานรหัสลับแบบสมมาตร (256 บิต) ที่ปกป้องข้อมูลที่ส่งผ่านอุโมงค์ (5)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

4 แนวนอน: การเปิดเผยคำขอตัวแปลงชื่อออกนอก VPN โดยไม่ตั้งใจ (5 ตัวอักษร):

5 แนวนอน: เขตอำนาจด้านความเป็นส่วนตัวของประเทศที่อยู่นอกพันธมิตร 14-Eyes (7 ตัวอักษร):

7 แนวนอน: การตรวจสอบโดยบุคคลที่สามที่ทบทวนคำกล่าวอ้างเรื่องการไม่เก็บบันทึก (7 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: โพรโทคอลโอเพนซอร์สความเร็วสูงที่มีในแอป CyberGhost ทุกตัว (7 ตัวอักษร):

2 แนวตั้ง: ยูทิลิตีกันพลาดของไคลเอนต์ที่ตัดทราฟฟิกอินเทอร์เน็ตเมื่อการเชื่อมต่อหลุด (6 ตัวอักษร):

3 แนวตั้ง: โครงสร้างพื้นฐานเซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เขียนบันทึกถาวรเลย (6 ตัวอักษร):

5 แนวตั้ง: กลุ่มเซิร์ฟเวอร์ความปลอดภัยสูงที่บริษัทเป็นเจ้าของและบริหารเองในโรมาเนีย (6 ตัวอักษร):

6 แนวตั้ง: มาตรฐานรหัสลับแบบสมมาตร (256 บิต) ที่ปกป้องข้อมูลที่ส่งผ่านอุโมงค์ (5 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	ฟ	บ	า	า	ห	นี	า	ม	กี	จ	า	า	รี
ต	ว	ส	ย	ง	ก	ค	จ	โ	น	คิ	ตี	ว	ร	ตี
ว	า	อ	ล	ล	ด	า	อ	ย	น	ล	ช	ฟ	ก	ก
ล	ม	เ	น	ว	ล้	ม	ร	แ	า	ส	ป	อ	อ	ม
มี	า	อ	ล	ล	ไ	ป	จ	า	นี	วิ	ป	กี	พ	ร
บ	ง	เ	า	ช	ว	า	โ	า	ลี	ต	จ	า	ดี	า
อ	น	ล	ผ	ดี	ร์	ช	ก	ร	ด	ช์	า	ต	ย	า
ส	จ	า	ค	ก	ก	ดี	า	ช	ม	ว	ก	ด	กี	ด
จ	ท	ผ	ฟ	ช	า	มี	ม	อ	ต	า	ฟ	ร	ดี	า
ว	ท	า	ส	ท	ร์	รั่	ข	ข	า	น	เ	ก	า	ล
ร	า	ม	ร	มี	ด	ว	า	ร	ช	ก	ด	นี	ง	น
ต	ร	ต	สี	ย	ข	ไ	มี	ดี	ด	ด	ว	บ	ย	ฟ
อ	า	ร	ห	ห	รี	ห	น	ผ	นี	ม	ผ	ดี	ข	กี
ส	บ	ลี	ง	ต	ร	ล	ด	ค	ผ	ห	ดี	ป	ร	กี
นี	า	ต	จ	ห	ดี	ด	บ	ตี	น	สี	ลี	ว	ลี	า

รายการคำศัพท์

ไวร์การ์ด เอเอส โรมาเนีย โนสปาย แรมล้วน คิลสวิตช์ รั่วไหล ตรวจสอบ

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ไวร์การ์ด
B. เอเอส
C. โรมาเนีย
D. โนสปาย
E. แรมล้วน
F. คิลสวิตช์
G. รั่วไหล
H. ตรวจสอบ

คำนิยามและช่องจับคู่	
	1. การเปิดเผยคำขอตัวแปลงชื่อออกนอก VPN โดยไม่ตั้งใจ
	2. โพรโทคอลโอเพนซอร์สความเร็วสูงที่มีในแอป CyberGhost ทุกตัว
	3. กลุ่มเซิร์ฟเวอร์ความปลอดภัยสูงที่บริษัทเป็นเจ้าของและบริหารเองในโรมาเนีย
	4. ยูทิลิตีกันพลาดของไคลเอนต์ที่ตัดทราฟฟิกอินเทอร์เน็ตเมื่อการเชื่อมต่อหลุด
	5. มาตรฐานรหัสลับแบบสมมาตร (256 บิต) ที่ปกป้องข้อมูลที่ส่งผ่านอุโมงค์
	6. เขตอำนาจด้านความเป็นส่วนตัวของประเทศที่อยู่นอกพันธมิตร 14-Eyes
	7. การตรวจสอบโดยบุคคลที่สามที่ทบทวนคำกล่าวอ้างเรื่องการไม่เก็บบันทึก
	8. โครงสร้างพื้นฐานเซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เขียนบันทึกถาวรเลย

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของเครือข่ายส่วนตัวเสมือน (VPN) เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ก ร์ ไ า ด ร์ ว
2. โ ม ย นี เ า ร
3. แ ม ล้ น ว ร
4. ไ ล ห รั่ ว
5. เ ส เ อ อ
6. า ป โ ส ย น
7. ต คิ ว ิ ซ์ ส ล
8. ร จ บ ต อ ส ว

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	บริการสตรีมมิงที่คุณรับชม			
2	ปุ่มหรือเมนูในแอป VPN			
3	การตั้งค่าที่คุณเปิดเพื่อความปลอดภัยเพิ่มเติม			
4	บริการ VPN อื่นที่ไม่ใช่ CyberGhost			
5	สิ่งที่การเข้ารหัสปกป้อง			
6	สิ่งที่ CyberGhost ซ่อนจากเครือข่ายของคุณได้			
7	ภัยคุกคามบน Wi-Fi สาธารณะ			
8	ประเภทของการรั่วไหลของ VPN			
9	ฟีเจอร์ด้านความปลอดภัยใน CyberGhost			
10	สิ่งที่การตรวจสอบ (audit) ตรวจได้			
11	สถานการณ์ที่ kill switch ช่วยได้			
12	ประเทศที่มีชื่อเสียงด้านกฎหมายความเป็นส่วนตัวที่เข้มแข็ง			
13	คำที่อธิบายแอป VPN ที่ดี			
14	ประเทศที่คุณอยากได้เซิร์ฟเวอร์ CyberGhost			
15	วิธีสร้างรหัสผ่านที่รัดกุม			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การตรวจสอบความเป็นส่วนตัวตามเขตอำนาจศาล



สถานการณ์: บริษัทสื่อต้องการให้แน่ใจว่าบันทึกข่าวกรององค์กรไม่สามารถถูกเจ้าหน้าที่บังคับใช้กฎหมายต่างประเทศออกหมายเรียกได้

คำถามอภิปราย: สำนักงานใหญ่ของ CyberGhost ในโรมาเนียปกป้องบริษัทจากหมายเฝ้าติดตามอย่างไร?

กรณีศึกษาที่ 2: ความปลอดภัยเมื่อฮาร์ดแวร์ถูกยึด



สถานการณ์: สถานที่ตั้งเซิร์ฟเวอร์ถูกบุกรุกทางกายภาพโดยไม่ได้รับอนุญาต และแร็คเซิร์ฟเวอร์ VPN ถูกยึด

คำถามอภิปราย: การออกแบบฮาร์ดแวร์แบบใดที่ป้องกันไม่ให้ผู้บุกรุกดึงคีย์เซสชันหรือประวัติผู้ใช้ออกมาได้?

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

วิศวกรเครือข่ายรักษาความปลอดภัยของช่องทางกำหนดเส้นทางและอุโมงค์ของไคลเอนต์ 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	11	51	35	67	31	57	39	45	35	67		59	25	42	27	49	34

27	1	27	64	45	7		2	64	45	33	56	37

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: CyberGhost ปลอดภัยหรือไม่?

ได้ ใช้การเข้ารหัส AES-256 โปรโตคอลที่ปลอดภัย และดำเนินงานภายใต้กฎหมายความเป็นส่วนตัวของโรมาเนีย

Q2: เซิร์ฟเวอร์ NoSpy คืออะไร?

เซิร์ฟเวอร์ NoSpy เป็นเจ้าของ สร้าง และดูแลโดย CyberGhost เพียงผู้เดียวที่สำนักงานใหญ่ในโรมาเนียเพื่อความปลอดภัยสูงสุด

Q3: CyberGhost เก็บล็อกหรือไม่?

ไม่ บังคับใช้นโยบายไม่เก็บล็อกอย่างเข้มงวด หมายความว่าไม่มีการจัดเก็บประวัติการท่องเว็บหรือล็อกการเชื่อมต่อ

Q4: CyberGhost มีฐานอยู่ที่ไหน?

CyberGhost ตั้งอยู่ที่บูคาเรสต์ ประเทศโรมาเนีย ซึ่งศาลรัฐธรรมนูญเคยตัดสินให้กฎหมายเก็บรักษาข้อมูลแบบครอบคลุมเป็นโมฆะในปี 2009 และ 2014 แม้กฎหมายปี 2015 จะกำหนดให้ผู้ให้บริการสื่อสารอิเล็กทรอนิกส์เก็บข้อมูลทราฟฟิกบางส่วนอีกครั้ง

Q5: ใช้โปรโตคอลอะไรบ้าง?

รองรับโปรโตคอล WireGuard, OpenVPN (TCP/UDP) และ IKEv2 ขึ้นอยู่กับประเภทอุปกรณ์

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: บล็อกโฆษณาหรือไม่?

ได้ แอปไคลเอนต์มีตัวบล็อกเนื้อหาในตัวสำหรับโฆษณา สคริปต์ติดตาม และโดเมนมัลแวร์

Q7: มี kill switch หรือไม่?

ได้ มี kill switch อัตโนมัติที่บล็อกการเข้าถึงอินเทอร์เน็ตหากการเชื่อมต่อ VPN หลุด

Q8: CyberGhost ป้องกันการรั่วไหลหรือไม่?

ได้ แอปมีการป้องกันการรั่วไหลของ DNS และ IP ในตัวที่ซ่อน IP จริงของคุณ

Q9: เซิร์ฟเวอร์ได้รับการตรวจสอบหรือไม่?

ใช่ นโยบายไม่เก็บบันทึกและโครงสร้างพื้นฐานของ CyberGhost ได้รับการตรวจสอบอิสระโดย Deloitte [2]

Q10: ใช้เซิร์ฟเวอร์ RAM หรือไม่?

ใช่ CyberGhost อธิบายว่าเครือข่ายเซิร์ฟเวอร์ของตนทำงานบนฮาร์ดแวร์ที่ไม่มีดิสก์และใช้ RAM เท่านั้น

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: ใช้โปรโตคอลใดเป็นค่าเริ่มต้น?

แอปเลือกโปรโตคอลที่ดีที่สุดให้โดยอัตโนมัติ แต่คุณสลับได้ทุกเมื่อ

Q2: split tunneling ทำงานอย่างไร?

ช่วยให้คุณเลือกได้ว่าแอปและเว็บไซต์ใดใช้ VPN และแอปใดข้ามอุโมงค์

Q3: คิวรี DNS ไปที่ไหน?

ถูกส่งผ่านอุโมงค์ VPN ไปยังเซิร์ฟเวอร์ DNS ของ CyberGhost เอง ไม่ใช่ของ ISP ของคุณ

Q4: ใครเป็นเจ้าของ CyberGhost?

CyberGhost เป็นของ Kape Technologies ซึ่งเป็นเจ้าของ ExpressVPN และ Private Internet Access ด้วย [7]

Q5: WireGuard ใช้ไซเฟอร์อะไร?

WireGuard ใช้มาตรฐานรหัสเข้ารหัสแบบสมมาตร ChaCha20-Poly1305 สมัยใหม่ [9]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: เซิร์ฟเวอร์ NoSpy แตกต่างอย่างไร?

มีฮาร์ดแวร์แบนด์วิดท์สูงกว่า อัปลิงก์เฉพาะ และตั้งอยู่ในดาต้าเซ็นเตอร์ส่วนตัว

Q7: Dedicated IP ไม่ระบุตัวตนหรือไม่?

ได้ IP จะถูกจับคู่กับโทเค็นแบบสุ่มแทนบัญชีของคุณ และโทเค็นจะถูกลบ

Q8: ใครตรวจสอบนโยบาย no-logs?

Deloitte Audit Romania ซึ่งตรวจสอบระบบไม่เก็บบันทึกของ CyberGhost เป็นครั้งที่สามเสร็จสิ้นในปี 2025

Q9: ตัวบล็อกโฆษณาถอดรหัส HTTPS หรือไม่?

ไม่ ตัวบล็อกโฆษณาทำงานที่ระดับ DNS โดยแปลงโดเมนโฆษณาไปยังหลุมดำ

Q10: ฉันใช้ CyberGhost บนเราเตอร์ได้หรือไม่?

ได้ ตั้งค่า CyberGhost บนเราเตอร์ที่รองรับ VPN เพื่อครอบคลุมทุกอุปกรณ์ในบ้าน

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

CyberGhost มีสำนักงานใหญ่ในโรมาเนีย ซึ่งอยู่นอกพันธมิตรแบ่งปันข่าวกรอง Five Eyes [1]

2. ข้อมูลเชิงลึกเรื่อง VPN

OpenVPN และ IKEv2 ใช้ AES-256 ส่วน WireGuard ใช้ ChaCha20-Poly1305 [5]

3. ข้อมูลเชิงลึกเรื่อง VPN

เซิร์ฟเวอร์ NoSpy เป็นเจ้าของและดูแลภายในองค์กรโดยพนักงาน CyberGhost [3]

4. ข้อมูลเชิงลึกเรื่อง VPN

Deloitte ตรวจสอบและยืนยันนโยบายการดำเนินงานแบบไม่เก็บบันทึกของพวกเขาอย่างสม่ำเสมอ [2]

5. ข้อมูลเชิงลึกเรื่อง VPN

อาร์เรย์เซิร์ฟเวอร์ไร้ดิสก์ที่ใช้เฉพาะ RAM ป้องกันการคงอยู่ของข้อมูลเมื่อปิดเครื่อง [1]

6. ข้อมูลเชิงลึกเรื่อง VPN

แอปไคลเอนต์มี Kill Switch อัตโนมัติสำหรับกรณีการเชื่อมต่อ VPN หลุด

7. ข้อมูลเชิงลึกด้าน VPN

การป้องกันการรั่วไหลของ DNS และ IP ในตัวช่วยซ่อนที่อยู่ IP จริงของคุณ

8. ข้อมูลเชิงลึกด้าน VPN

ไคลเอนต์รองรับโปรโตคอล WireGuard, OpenVPN และ IKEv2 แบบเนทีฟ [4]

9. ข้อมูลเชิงลึกด้าน VPN

IP เฉพาะถูกกำหนดให้โดยใช้ระบบโทเคินแบบ zero-knowledge ที่ปลอดภัย [8]

10. ข้อมูลเชิงลึกเรื่อง VPN

ตัวกรองมัลแวร์ในตัวสแกนการค้นหาโดเมนเพื่อบล็อกเป้าหมายที่เป็นอันตราย [6]

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] CyberGhost VPN. (n.d.). No-Logs VPN: Secure & Private VPN with Zero Tracking.
https://www.cyberghostvpn.com/features/no-logs-vpn

[2] CyberGhost VPN. (2025). Third Deloitte Romania Audit Verifies Our Commitment to Privacy.
https://www.cyberghostvpn.com/privacyhub/privacy-audit-2025/

[3] CyberGhost VPN. (n.d.). CyberGhost's NoSpyServers: Complete Privacy & Anonymity.
https://www.cyberghostvpn.com/features/nospy

[4] CyberGhost VPN Support Center. (n.d.). Which VPN Protocols Do You Support?
https://support.cyberghostvpn.com/hc/en-us/articles/213983829-Which-VPN-Protocols-Do-You-Support

[5] CyberGhost VPN. (n.d.). VPN Encryption: How VPNs Help Secure Your Browsing.
https://www.cyberghostvpn.com/features/vpn-encryption

[6] CyberGhost VPN. (n.d.). VPN Features and Use Cases.
https://www.cyberghostvpn.com/features

[7] Kape Technologies. (n.d.). Our Brands.
https://www.kape.com/our-brands/

[8] CyberGhost VPN. (n.d.). Dedicated IP VPN | Get a Secure Static IP Address.
https://www.cyberghostvpn.com/dedicated-ip-vpn

[9] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[10] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[11] National Institute of Standards and Technology. (n.d.). FIPS 197: Advanced Encryption Standard (AES).
https://csrc.nist.gov/pubs/fips/197/final

[12] European Digital Rights (EDRi). (2014). Romania: The aftermath of the second CCR data retention ruling.
https://edri.org/our-work/romania-aftermath-of-second-ccr-data-retention-ruling/

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

CyberGhost มีโปรโตคอลใดให้ใช้บนทุกแพลตฟอร์มหลัก? → A) WireGuard

2 คำถาม 2 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การเชื่อมต่อ OpenVPN และ IKEv2 ของ CyberGhost ใช้รหัสลับ (cipher) ใด? → A) AES-256

3 คำถาม 3 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

เซิร์ฟเวอร์ NoSpy ที่ CyberGhost ดำเนินการเองตั้งอยู่ที่ใด? → โรมาเนีย

4 คำถาม 4 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

โครงสร้างพื้นฐานแบบใดที่ไม่เก็บบันทึกลงดิสก์เมื่อปิดเครื่อง? → เซิร์ฟเวอร์ที่ใช้ RAM เท่านั้น

5 คำถาม 5 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ฟีเจอร์ใดที่บล็อกการเชื่อมต่อระหว่างที่ VPN หลุด? → Kill Switch

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

CyberGhost มีสำนักงานใหญ่ในโรมาเนีย ซึ่งอยู่นอกกลุ่ม 14-Eyes

7 **คำถาม 7** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เซิร์ฟเวอร์ NoSpy เช่าจากดาต้าเซ็นเตอร์เชิงพาณิชย์ของบุคคลที่สาม

8 **คำถาม 8** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เซิร์ฟเวอร์แบบ RAM-only เขียนข้อมูลเซสชันของผู้ใช้ลงในไดรฟ์ SSD ถาวร

9 **คำถาม 9** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

แอปไคลเอนต์มีการป้องกันการรั่วไหลของ DNS ในตัว

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

นโยบาย zero-logs ของ CyberGhost ได้รับการยืนยันโดยการตรวจสอบอิสระ

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

D 1. WireGuard	F 2. AES-256	A 3. โรมาเนีย	G 4. NoSpy
B 5. เฉพาะ RAM	H 6. KILL SWITCH	C 7. การรั่วไหล	E 8. การตรวจสอบ

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ไวร์การ์ด	2 เอเอส	3 โรมาเนีย	4 โนสปาย
5 แรมล้วน	6 คิลสวิตช์		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 G – รั่วไหล	2 A – ไวร์การ์ด	3 D – โนสปาย	4 F – คิลสวิตช์
5 B – เอเอส	6 C – โรมาเนีย	7 H – ตรวจสอบ	8 E – แรมล้วน

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย WireGuard AES-256 และ โรมาเนีย ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

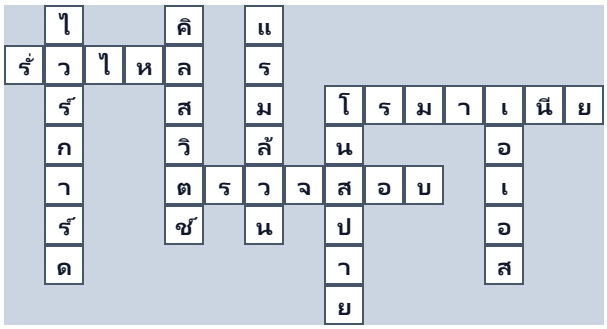
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ฟ	บ	า	า	ห	นี	า	ม	กี	จ	า	า	รี
ต	ว	ส	ย	ง	ก	ค	จ	โ	น	คิ	ตี	ว	ร	ตี
ว	า	อ	ล	ล	ด	า	อ	ย	น	ล	ซ	ฟ	ก	ก
ล	ม	เ	น	ว	ล้	ม	ร	แ	า	ส	ป	อ	อ	ม
มี	า	อ	ล	ล	ไ	ป	จ	า	นี	วิ	ป	กี	พ	ร
บ	ง	เ	า	ช	ว	า	โ	า	ลี	ต	จ	า	ดี	า
อ	น	ล	ผ	ดี	ร์	ช	ก	ร	ด	ช์	า	ต	ย	า
ส	จ	า	ค	ก	ก	ดี	า	ช	ม	ว	ก	ด	กี	ด
จ	ท	ผ	ฟ	ช	า	มี	ม	อ	ต	า	ฟ	ร	ดี	า
ว	ท	า	ส	ท	ร์	รั่	ข	ข	า	น	เ	ก	า	ล
ร	า	ม	ร	มี	ด	ว	า	ร	ช	ก	ด	นี	ง	น
ต	ร	ต	สี	ย	ข	ไ	มี	ดี	ด	ด	ว	บ	ย	ฟ
อ	า	ร	ห	ห	รี	ห	น	ผ	นี	ม	ผ	ดี	ข	กี
ส	บ	ลี	ง	ด	ร	ล	ด	ค	ผ	ห	ดี	ป	ร	กี
นี	า	ต	จ	ห	ดี	ด	บ	ดี	น	สี	ลี	ว	ลี	า

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

4 แนวนอน: รั่วไหล การเปิดเผยคำขอตัวแปลงชื่อออกนอก VPN โดยไม่ตั้งใจ (5 ตัวอักษร)

5 แนวนอน: โรมาเนีย เขตอำนาจด้านความเป็นส่วนตัวของประเทศที่อยู่นอกพันธมิตร 14-Eyes (7 ตัวอักษร)

7 แนวนอน: ตรวจสอบ การตรวจสอบโดยบุคคลที่สามที่ทบทวนคำกล่าวอ้างเรื่องการไม่เก็บบันทึก (7 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ไวร์การ์ด โพรโทคอลโอเพนซอร์สความเร็วสูงที่มีในแอป CyberGhost ทุกตัว (7 ตัวอักษร)

2 แนวตั้ง: คิลสวิตช์ ยูทิลิตีกันพลาดของไคลเอนต์ที่ตัดทราฟฟิกอินเทอร์เน็ตเมื่อการเชื่อมต่อหลุด (6 ตัวอักษร)

3 แนวตั้ง: แรมล้วน โครงสร้างพื้นฐานเซิร์ฟเวอร์ไร้ดิสก์ที่ไม่เขียนบันทึกถาวรเลย (6 ตัวอักษร)

5 แนวตั้ง: โนสปาย กลุ่มเซิร์ฟเวอร์ความปลอดภัยสูงที่บริษัทเป็นเจ้าของและบริหารเองในโรมาเนีย (6 ตัวอักษร)

6 แนวตั้ง: เอเอส มาตรฐานรหัสลับแบบสมมาตร (256 บิต) ที่ปกป้องข้อมูลที่ส่งผ่านอุโมงค์ (5 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. กร์ไดร์ว → ไวร์การ์ด
2. โมยนีเาร → โรมาเนีย
3. แมล้นวร → แรมล้วน
4. ไลหรั่ว → รั่วไหล
5. เสเออ → เอเอส
6. าปโสยน → โนสปาย
7. ตคิวิซ์สล → คิลสวิตช์
8. รจบตอสว → ตรวจสอบ

เฉลยภารกิจรหัสลับ

"เซิร์ฟเวอร์โนสปาย ปกป้อง ข้อมูล"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การตรวจสอบความเป็นส่วนตัวตามเขตอำนาจศาล

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บริษัทสื่อต้องการให้แน่ใจว่าบันทึกข่าวกรององค์กรไม่สามารถถูกเรียกโดยหมายศาลจากหน่วยงานบังคับใช้กฎหมายต่างประเทศ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: โรมาเนียมีกฎหมายความเป็นส่วนตัวที่เข้มแข็งและไม่ได้เป็นสมาชิกของเครือข่ายแบ่งปันข่าวกรอง Five-Eyes หรือ Fourteen-Eyes

B กรณีศึกษาที่ 2: ความปลอดภัยเมื่อฮาร์ดแวร์ถูกยึด

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ศูนย์เซิร์ฟเวอร์ถูกบุกรุกทางกายภาพโดยไม่ได้รับอนุญาต และแร็คเซิร์ฟเวอร์ VPN ถูกยึด
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เซิร์ฟเวอร์ทำงานบนสถาปัตยกรรมแบบ RAM-only ซึ่งหมายความว่าข้อมูลทั้งหมดจะสูญหายทันทีเมื่อตัดไฟ