ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

รีวิว TunnelBear

การวิเคราะห์ทางเทคนิคของ TunnelBear ที่มีสำนักงานใหญ่ในแคนาดา การปกปิดทราฟฟิก GhostBear kill switch VigilantBear การตรวจสอบความปลอดภัยอิสระประจำปี และการไม่เก็บบันทึก

ภาพรวมการเรียนรู้การรีวิว TunnelBear

ผู้เรียน

สถานะนักเรียน

สายงานผู้พิทักษ์เครือข่าย

ปลอดภัย

สถานะการเชื่อมต่อ

การปกป้องแพ็กเก็ตข้อมูล

เปิดใช้งาน

การป้องกันการรั่วไหล

การป้องกันการรั่วไหลของ DNS และ IPv6

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการรีวิวทางเทคนิคของ TunnelBear คุณจะได้สำรวจการอำพราง GhostBear การตั้งค่า kill switch ของ VigilantBear และการยืนยันผลการตรวจสอบความปลอดภัยประจำปี

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/tunnelbear/

เส้นทางการเรียนรู้ TunnelBear ของคุณ

- วิเคราะห์สถาปัตยกรรมทางเทคนิคและมาตรฐานการเข้ารหัสของรีวิว TunnelBear
- ตั้งค่าไคลเอนต์เพื่อป้องกันการรั่วไหลของทราฟฟิก IP, DNS และ WebRTC
- เปรียบเทียบโปรโตคอลอุโมงค์ที่เป็นกรรมสิทธิ์เฉพาะกับการใช้งานมาตรฐาน

คำแนะนำการรีวิว TunnelBear

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การพรางทราฟฟิก GhostBear และสวิตช์ VigilantBear ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การพรางตัว GhostBear และการตรวจสอบยืนยันโดยหน่วยงานอิสระประจำปี

TunnelBear มีชื่อเสียงจากการตรวจสอบความปลอดภัยอิสระประจำปีโดย Cure53 มีสำนักงานใหญ่ในแคนาดา มีการพรางโปรโตคอล GhostBear เพื่อหลบเลี่ยงการเซ็นเซอร์ DPI การป้องกันการรั่วไหลของการเชื่อมต่อ VigilantBear และการเชื่อมต่ออุปกรณ์ไม่จำกัด

(บทนำ)

TunnelBear มีชื่อเสียงจากการตรวจสอบความปลอดภัยอิสระประจำปีโดย Cure53 มีสำนักงานใหญ่ในแคนาดา มีการพรางโปรโตคอล GhostBear เพื่อหลบเลี่ยงการเซ็นเซอร์ DPI การป้องกันการรั่วไหลของการเชื่อมต่อ VigilantBear และการเชื่อมต่ออุปกรณ์ไม่จำกัด

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **1. นิติบุคคลของ TunnelBear จดทะเบียนในประเทศใด?**
   - A) แคนาดา
   - B) สหรัฐอเมริกา
   - C) สวิตเซอร์แลนด์
   - D) เยอรมนี

2. **2. การพรางตัวเพื่อหลีกเลี่ยงการเซ็นเซอร์ของ TunnelBear ชื่ออะไร?**
   - A) GhostBear
   - B) Chameleon
   - C) Stealth
   - D) ShadowSocks

3. **3. ฟีเจอร์ kill switch ในตัวของ TunnelBear ชื่ออะไร?**
   - A) VigilantBear
   - B) Secure Core
   - C) NetShield
   - D) SafePath

4. **4. บริษัทความปลอดภัยไซเบอร์รายใดที่เข้าซื้อ TunnelBear ในปี 2018?**
   - A) McAfee
   - B) Avast
   - C) NortonLifeLock
   - D) Kape Technologies

5. **5. TunnelBear แนะนำโปรโตคอลใดสำหรับอุโมงค์ความเร็วสูงสมัยใหม่?**
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) PPTP

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. GhostBear สลับเมทาดาทาของ VPN เพื่อช่วยเลี่ยงไฟร์วอลล์ที่ตรวจสอบแพ็กเก็ตเชิงลึก

○ จริง ○ เท็จ

7 คำถาม 7

7. แพ็กเกจฟรีของ TunnelBear รวมข้อมูลการเรียกดูรายเดือนแบบไม่จำกัด

○ จริง ○ เท็จ

8 คำถาม 8

8. VigilantBear ช่วยรักษาข้อมูลให้ปลอดภัยขณะแอปกำลังเชื่อมต่อหรือเชื่อมต่อใหม่

○ จริง ○ เท็จ

9 คำถาม 9

9. TunnelBear เป็น VPN สำหรับผู้บริโภครายแรกที่เผยแพร่ผลการตรวจสอบความปลอดภัยประจำปีต่อสาธารณะ

○ จริง ○ เท็จ

10 คำถาม 10

10. ผู้ให้บริการดำเนินงานภายใต้เขตอำนาจศาลที่เข้มงวดของกฎหมายปานามา

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. **TunnelBear มีสำนักงานใหญ่และดำเนินงานจาก _____ ซึ่งมีกฎหมายเข้มงวด**
2. **เทคโนโลยีพรางตัวขับเคลื่อนด้วยการตั้งค่าระบบ _____**
3. **การป้องกันการรั่วไหลระดับระบบจัดการด้วยการตั้งค่า _____**
4. **ผู้ให้บริการ VPN ถูกเข้าซื้อโดยนักพัฒนาด้านความปลอดภัย _____ ในปี 2018**
5. **ความเร็วการส่งข้อมูลสูงทำได้ผ่านโปรโตคอล _____**
6. **การเชื่อมต่อไคลเอนต์เดสก์ท็อปแบบดั้งเดิมอาศัยโปรโตคอล _____**

คลังคำศัพท์

โกสต์แบร์ **แคนาดา** **ตรวจสอบ** **แมคคาฟี** **ไม่เก็บล็อก** **วิจิแลนต์แบร์** **ไวร์การ์ด** **โอเพนวีพีเอ็น**

เขียนคำตอบของคุณที่นี่:

1. **2.**

3. **4.**

5. **6.**

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่อง VPN และเครือข่าย

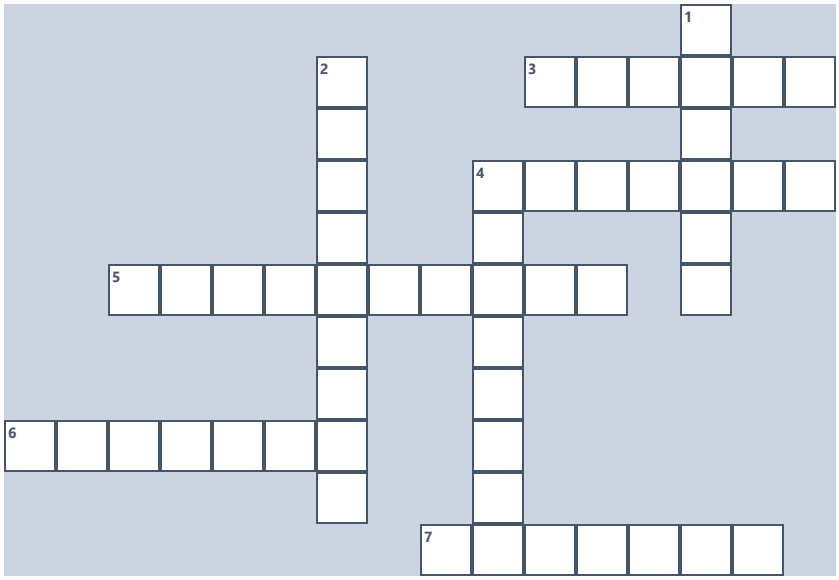
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. แคนาดา**	**A**	นโยบายความเป็นส่วนตัวที่บังคับไม่ให้เก็บประวัติทราฟฟิก
☐	**2. GhostBear**	**B**	ประเทศที่จดทะเบียนและสำนักงานใหญ่ของบริษัท
☐	**3. VigilantBear**	**C**	การประเมินความปลอดภัยโดยบุคคลที่สามที่ดำเนินการทุกปี
☐	**4. McAfee**	**D**	โปรโตคอลอุโมงค์โอเพนซอร์สมาตรฐานที่ใช้บนเดสก์ทอป
☐	**5. WireGuard**	**E**	บริษัทแม่ด้านความปลอดภัยที่เข้าซื้อ TunnelBear
☐	**6. OpenVPN**	**F**	โปรโตคอลประสิทธิภาพสูงที่ใช้การเข้ารหัสลับสมัยใหม่
☐	**7. การตรวจสอบ**	**G**	เทคโนโลยีสับเปลี่ยนเมทาดาทาที่ใช้หลบการตรวจสอบแพ็กเก็ตเชิงลึก
☐	**8. ไม่เก็บล็อก**	**H**	Kill switch ในตัวที่ปกป้องการเชื่อมต่อเมื่อหลุด

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

3. บริษัทแม่ด้านความปลอดภัยที่เข้าซื้อ TunnelBear (6)

4. โปรโตคอลประสิทธิภาพสูงที่ใช้การเข้ารหัสลับสมัยใหม่ (7)

5. โปรโตคอลอุโมงค์โอเพนซอร์สมาตรฐานที่ใช้บนเดสก์ท็อป (10)

6. การประเมินความปลอดภัยโดยบุคคลที่สามที่ทำเป็นประจำทุกปี (7)

7. เทคโนโลยีสับเมตาดาตาที่ใช้ข้ามการตรวจสอบแพ็กเก็ตเชิงลึก (7)

แนวตั้ง

1. ประเทศที่จดทะเบียนและเป็นที่ตั้งสำนักงานใหญ่ขององค์กร (6)

2. คิลสวิตช์ในตัวที่ปกป้องการเชื่อมต่อเมื่อหลุด (9)

4. นโยบายความเป็นส่วนตัวที่บังคับไม่เก็บประวัติทราฟฟิก (8)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

3 แนวนอน: บริษัทแม่ด้านความปลอดภัยที่เข้าซื้อ TunnelBear (6 ตัวอักษร):

4 แนวนอน: โปรโตคอลประสิทธิภาพสูงที่ใช้การเข้ารหัสลับสมัยใหม่ (7 ตัวอักษร):

5 แนวนอน: โปรโตคอลอุโมงค์โอเพนซอร์สมาตรฐานที่ใช้บนเดสก์ท็อป (10 ตัวอักษร):

6 แนวนอน: การประเมินความปลอดภัยโดยบุคคลที่สามที่ทำเป็นประจำทุกปี (7 ตัวอักษร):

7 แนวนอน: เทคโนโลยีสับเมตาดาตาที่ใช้ข้ามการตรวจสอบแพ็กเก็ตเชิงลึก (7 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ประเทศที่จดทะเบียนและเป็นที่ตั้งสำนักงานใหญ่ขององค์กร (6 ตัวอักษร):

2 แนวตั้ง: คิลสวิตช์ในตัวที่ปกป้องการเชื่อมต่อเมื่อหลุด (9 ตัวอักษร):

4 แนวตั้ง: นโยบายความเป็นส่วนตัวที่บังคับไม่เก็บประวัติทราฟฟิก (8 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช	มี	า	ฟ	บ	า	า	ไ	ห	นี	า	ม	กี	จ	า
า	รี	ด	ต	ว	ย	ง	ว	ก	ค	ต	จ	น	ตี	ว
ร	ตี	า	ว	า	ล	ล	ร์	ด	า	ร	อ	ย	ช	ฟ
ร์	ก	น	ก	ล	ม	า	ก	ป	อ	ว	อ	ม	มี	า
บ	ล	ค	ล	ป	โ	จ	า	า	นี	จ	กี	พ	ไ	ร
แ	ง	แ	า	ช	อ	า	ร์	า	ลี	ส	จ	ดี	ม่	า
ต์	น	ล	ผ	ดี	เ	ช	ด	โ	ก	อ	ด	า	เ	ต
น	า	จ	า	ค	พ	ก	ดี	ก	า	บ	ช	ว	ก็	ก
ล	ด	กี	ด	ท	น	ผ	ฟ	ส	ช	มี	ม	อ	บ	ต
แ	ฟ	ร	ดี	า	วี	แ	ท	ต์	า	ส	ท	ข	ล็	ข
จิ	า	น	ก	า	พี	ม	ล	แ	า	ม	ร	มี	อ	า
วิ	ร	ช	ก	ด	เ	ค	ง	บ	น	ร	ต	สี	ก	ย
ข	มี	ดี	ด	ด	อ็	ค	ว	ร์	บ	ฟ	อ	า	ร	ห
ห	รี	น	ผ	นี	น	า	ม	ผ	ดี	ข	กี	ส	บ	ลี
ง	ด	ร	ด	ค	ผ	ฟี	ห	ดี	ป	ร	กี	นี	า	ต

รายการคำศัพท์

แคนาดา โกสต์เบร์ วิจิแลนต์แบร์ แมคคาฟี ไวร์การ์ด โอเพนวีพีเอ็น ตรวจสอบ ไม่เก็บล็อก

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. แคนาดา
B. โกสต์แบร์
C. วิจิแลนต์แบร์
D. แมคคาฟี
E. ไวร์การ์ด
F. โอเพนวีพีเอ็น
G. ตรวจสอบ
H. ไม่เก็บล็อก

คำนิยามและช่องจับคู่
1. โปรโตคอลอุโมงค์โอเพนซอร์สมาตรฐานที่ใช้บนเดสก์ท็อป
2. นโยบายความเป็นส่วนตัวที่บังคับไม่เก็บประวัติทราฟฟิก
3. โปรโตคอลประสิทธิภาพสูงที่ใช้การเข้ารหัสลับสมัยใหม่
4. ประเทศที่จดทะเบียนและเป็นที่ตั้งสำนักงานใหญ่ขององค์กร
5. การประเมินความปลอดภัยโดยบุคคลที่สามที่ทำเป็นประจำทุกปี
6. เทคโนโลยีสับเมตาดาตาที่ใช้ข้ามการตรวจสอบแพ็กเก็ตเชิงลึก
7. บริษัทแม่ด้านความปลอดภัยที่เข้าซื้อ TunnelBear
8. คิลสวิตช์ในตัวที่ปกป้องการเชื่อมต่อเมื่อหลุด

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของเครือข่ายส่วนตัวเสมือน (VPN) เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. น แ า ด า ค _____

2. ร์ ว บ ล จ ิ ต์ แ น แ _____

3. ก ไ า ด ร์ ร์ ว _____

4. บ ร ส จ อ ต ว _____

5. แ ร์ ต์ ส โ บ ก _____

6. า ค แ ค ฟ ี ม _____

7. อ พ โ พ ี ว ี เ อ็ น น เ _____

8. ก็ ม่ บ ก ไ อ ล็ เ _____

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	ประเทศที่คุณอยากได้เซิร์ฟเวอร์ TunnelBear			
2	สิ่งที่ TunnelBear ซ่อนจากเครือข่ายของคุณได้			
3	สถานการณ์ที่ kill switch ช่วยได้			
4	คำศัพท์ด้านความปลอดภัยที่คุณเรียนรู้จากใบงานนี้			
5	โปรโตคอล VPN ที่คุณรู้จัก			
6	อุปกรณ์ที่คุณจะติดตั้ง TunnelBear			
7	สถานที่ที่คุณจะเปิดใช้ TunnelBear			
8	แอปที่คุณจะใช้ร่วมกับ TunnelBear			
9	สัญญาณที่บ่งบอกว่าการเชื่อมต่อ VPN ของคุณช้า			
10	สิ่งที่ควรตรวจสอบก่อนซื้อ VPN			
11	คำที่อธิบายแอป VPN ที่ดี			
12	ปุ่มหรือเมนูในแอป VPN			
13	บริการสตรีมมิงที่คุณรับชม			
14	ข้อมูลที่ VPN ไม่ควรเก็บ			
15	สิ่งที่คุณมองหาใน TunnelBear			

จุดตรวจสอบที่ 8: กรณีศึกษา VPN และเครือข่าย

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การหลีกเลี่ยงการเซ็นเซอร์



สถานการณ์: นักวิจัยที่เดินทางผ่านประเทศที่บล็อกโปรโตคอล VPN ต้องการเข้าถึงเอกสารวิจัย

คำถามอภิปราย: ควรเปิดใช้การตั้งค่า TunnelBear ใดเพื่อข้ามการตรวจสอบแพ็กเก็ตเชิงลึก?

กรณีศึกษาที่ 2: ฮอตสปอตสาธารณะที่ไม่ปลอดภัย



สถานการณ์: วิศวกรเชื่อมต่อกับฮอตสปอต Wi-Fi สนามบินแบบเปิดและพบการเชื่อมต่อหลุดบ่อย

คำถามอภิปราย: VigilantBear ปกป้องอุปกรณ์ของวิศวกรระหว่างที่การเชื่อมต่อหลุดได้อย่างไร?

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

58	45	27		23	48	25	57	25	37	58	26	35	67		33	52

39	51	8	51	58	37	25	21	67	58	26	35	67

27	64	45	7	1	48	25

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q1: TunnelBear ปลอดภัยหรือไม่?

ได้ ใช้การเข้ารหัส AES-256 และแอปได้รับการตรวจสอบโดยอิสระทุกปี [1]

Q2: GhostBear คืออะไร?

GhostBear เป็นฟีเจอร์พรางตัวที่ซ่อนทราฟฟิก VPN เพื่อเลี่ยงการบล็อกจากการเซ็นเซอร์

Q3: มีแพ็กเกจฟรีหรือไม่?

ใช่ TunnelBear มีแพ็กเกจฟรีแบบจำกัดที่ให้แบนด์วิดท์ 2GB ต่อเดือน [1]

Q4: TunnelBear มีฐานอยู่ที่ไหน?

TunnelBear มีสำนักงานใหญ่ที่โตรอนโต แคนาดา ภายใต้เขตอำนาจศาลของแคนาดา

Q5: VigilantBear คืออะไร?

VigilantBear เป็น kill switch ในตัวของ TunnelBear ที่บล็อกการรั่วไหลเมื่อการเชื่อมต่อหลุด

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยที่สุดเกี่ยวกับเครือข่ายส่วนตัวเสมือน (VPN) และการทำอุโมงค์

Q6: ฉันเชื่อมต่อหลายอุปกรณ์ได้หรือไม่?

ได้ แพ็กเกจแบบชำระเงินรองรับการเชื่อมต่อพร้อมกันไม่จำกัดภายใต้บัญชีเดียว

Q7: TunnelBear รองรับ WireGuard หรือไม่?

ใช่ รองรับ WireGuard สำหรับการเชื่อมต่อประสิทธิภาพสูงที่ประหยัดแบตเตอรี่

Q8: นโยบาย zero-logs ของพวกเขาคืออะไร?

TunnelBear ไม่บันทึกที่อยู่ IP คำค้น DNS หรือกิจกรรมการท่องเว็บของผู้ใช้

Q9: ใครเป็นเจ้าของ TunnelBear?

TunnelBear ถูกซื้อโดยบริษัทความปลอดภัยไซเบอร์รายใหญ่ McAfee ในปี 2018 [8]

Q10: บล็อกโฆษณาได้หรือไม่?

TunnelBear เน้นการเข้ารหัส การบล็อกโฆษณาไม่ได้มีมาในไคลเอนต์ VPN หลัก [4]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q1: GhostBear หลบ DPI ได้อย่างไร?

ทำให้ทราฟฟิก VPN ที่เข้ารหัสดูเหมือน HTTPS ธรรมดา ตัวกรอง DPI จึงตรวจพบได้ยาก

Q2: แคนาดาเป็นประเทศ 5-Eyes หรือไม่?

ใช่ แคนาดาเป็นสมาชิกพันธมิตร Five-Eyes ซึ่งทำให้ต้องพิจารณาเรื่องเขตอำนาจศาล

Q3: VigilantBear บล็อกการรั่วไหลของข้อมูลอย่างไร?

บล็อกทราฟฟิกขาเข้าและขาออกทั้งหมดจนกว่าจะเชื่อมต่อ VPN ได้อีกครั้ง

Q4: การตรวจสอบของพวกเขาตรวจสอบอะไรบ้าง?

Cure53 ตรวจสอบโค้ดแอป การกำหนดค่าเซิร์ฟเวอร์ โครงสร้างพื้นฐาน และการควบคุมการบันทึก

Q5: WireGuard ทำงานแบบเนทีฟหรือไม่?

ใช่ แอป TunnelBear มี WireGuard เพื่อการเชื่อมต่อที่เร็วและเสถียร

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับ VPN ระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของโปรโตคอลอุโมงค์ VPN การผสานรวมไคลเอนต์มือถือ และการติดตั้งใช้งานระดับองค์กร

Q6: มีเซิร์ฟเวอร์เฉพาะสำหรับ P2P หรือไม่?

ไม่ รองรับการรับส่งข้อมูล P2P บนโหนดเซิร์ฟเวอร์ทั่วโลกทั้งหมดโดยไม่มีข้อจำกัด

Q7: ป้องกันการรั่วไหลของ WebRTC หรือไม่?

ได้ ไคลเอนต์ดักจับและส่งคำขอ WebRTC เพื่อป้องกันการเปิดเผย IP ภายในเครื่อง

Q8: การจัดการความปลอดภัยของ DNS ทำอย่างไร?

คำขอ DNS ถูกส่งผ่านรีโซลเวอร์ DNS ส่วนตัวที่เข้ารหัสของ TunnelBear

Q9: ฉันใช้บน Linux ได้หรือไม่?

TunnelBear ไม่มีแอป Linux อย่างเป็นทางการ แอปของบริการรองรับ Windows, macOS, iOS และ Android [5]

Q10: ฐานข้อมูลการเรียกเก็บเงินถูกแยกออกจากกันอย่างไร?

ระเบียนการเรียกเก็บเงินจัดเก็บแยกจากล็อกทราฟฟิกของเซิร์ฟเวอร์เพื่อรักษาการไม่เปิดเผยตัวตน

ส่วนที่ 11: ข้อเท็จจริง VPN ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับความเร็วการเข้ารหัส VPN การตรวจสอบโปรโตคอล การเชื่อมต่อบนมือถือ และการทำงานระยะไกลขององค์กร

1. ข้อมูลเชิงลึกเรื่อง VPN

TunnelBear มีสำนักงานใหญ่ที่โตรอนโต แคนาดา และดำเนินงานภายใต้เขตอำนาจศาลของแคนาดา [2]

2. ข้อมูลเชิงลึกเรื่อง VPN

McAfee เข้าซื้อบริการนี้ในปี 2018 เพื่อเสริมพอร์ตโฟลิโอด้านความปลอดภัย [3]

3. ข้อมูลเชิงลึกเรื่อง VPN

GhostBear พรางลายเซ็นโปรโตคอล VPN ให้ดูเหมือนแพ็กเก็ต HTTP/S มาตรฐาน [4]

4. ข้อมูลเชิงลึกเรื่อง VPN

VigilantBear ทำหน้าที่เป็น kill switch การเชื่อมต่อระดับไฟร์วอลล์ของไคลเอนต์ [4]

5. ข้อมูลเชิงลึกเรื่อง VPN

Cure53 ตรวจสอบสาธารณะประจำปีเพื่อยืนยันความปลอดภัยของแอปและเซิร์ฟเวอร์ [6]

6. ข้อมูลเชิงลึกเรื่อง VPN

การสมัครใช้งานแบบชำระเงินรองรับการเชื่อมต่อพร้อมกันได้ไม่จำกัดจำนวนอุปกรณ์ [1]

7. ข้อมูลเชิงลึกด้าน VPN

เครือข่ายใช้การเข้ารหัส AES-256 ซึ่งเป็นมาตรฐานความปลอดภัยระดับโลก [1]

8. ข้อมูลเชิงลึกด้าน VPN

รองรับอุโมงค์โปรโตคอล OpenVPN, IKEv2 และ WireGuard [5]

9. ข้อมูลเชิงลึกด้าน VPN

ไม่มีการเก็บล็อกเกี่ยวกับที่อยู่ IP ปลายทางหรือประวัติการท่องเว็บของผู้ใช้

10. ข้อมูลเชิงลึกเรื่อง VPN

มีส่วนติดต่อผู้ใช้ธีมหมีสนุกสนานเพื่อให้จัดการ VPN ได้ง่าย

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานทางเทคนิค ข้อกำหนดเฉพาะ และกรอบการกำกับดูแลระดับโลก

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] TunnelBear, LLC. (2026). TunnelBear VPN - Apps on Google Play.
https://play.google.com/store/apps/details?id=com.tunnelbear.android&hl=en_US

[2] TunnelBear, LLC. (n.d.). TunnelBear: Safe and Fast VPN App - App Store.
https://apps.apple.com/us/app/tunnelbear-secure-vpn-wifi/id564842283

[3] TechCrunch. (2018). McAfee acquires VPN company TunnelBear.
https://techcrunch.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[4] PCWorld. (2024). TunnelBear VPN review: It's just right for beginners.
https://www.pcworld.com/article/406999/tunnelbear-vpn-review-2.html

[5] CyberInsider. (2026). TunnelBear Review & Test Results 2026 — Pros and Cons.
https://cyberinsider.com/vpn/reviews/tunnelbear/

[6] Cure53. (2024). Pentest-Report TunnelBear VPN Clients & Servers 10-11.2023.
https://cure53.de/pentest-report_tunnelbear_2023.pdf

[7] Cure53. (2020). TunnelBear Security Assessment Summary 11.2019.
https://cure53.de/summary-report_tunnelbear_2019.pdf

[8] VentureBeat. (2018). McAfee acquires VPN provider TunnelBear.
https://venturebeat.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

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

[10] Office of the Privacy Commissioner of Canada. (n.d.). The Personal Information Protection and Electronic Documents Act (PIPEDA).
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

นิติบุคคลของ TunnelBear จดทะเบียนในประเทศใด? → แคนาดา

2 คำถาม 2 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การพรางตัวเพื่อหลีกเลี่ยงการเซ็นเซอร์ของ TunnelBear ชื่ออะไร? → GhostBear

3 คำถาม 3 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ฟีเจอร์ kill switch ในตัวของ TunnelBear ชื่ออะไร? → VigilantBear

4 คำถาม 4 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

บริษัทความปลอดภัยไซเบอร์รายใดที่เข้าซื้อ TunnelBear ในปี 2018? → McAfee

5 คำถาม 5 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

TunnelBear แนะนำโปรโตคอลใดสำหรับอุโมงค์ความเร็วสูงสมัยใหม่? → WireGuard

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: GhostBear พรางทราฟฟิก VPN เพื่อช่วยให้ผ่านการตรวจสอบแพ็กเก็ตเชิงลึกได้

7 **คำถาม 7** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: แพ็กเกจฟรีให้ข้อมูลการเรียกดู 2GB ต่อเดือน

8 **คำถาม 8** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

VigilantBear ช่วยรักษาข้อมูลให้ปลอดภัยขณะแอปกำลังเชื่อมต่อหรือเชื่อมต่อใหม่

9 **คำถาม 9** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: TunnelBear ระบุว่าเป็น VPN สำหรับผู้บริโภครายแรกที่ผ่านการตรวจสอบสาธารณะโดยบุคคลที่สามเป็นประจำทุกปี

10 **คำถาม 10** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: TunnelBear ตั้งอยู่ในโทรอนโตและดำเนินงานภายใต้กฎหมายแคนาดา

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

B 1. แคนาดา	G 2. GhostBear	H 3. VigilantBear	E 4. McAfee
F 5. WireGuard	D 6. OpenVPN	C 7. การตรวจสอบ	A 8. ไม่เก็บล็อก

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 แคนาดา	2 โกสต์แบร์	3 วิจิแลนต์แบร์	4 แมคคาฟี
5 ไวร์การ์ด	6 โอเพนวีพีเอ็น		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 F – โอเพนวีพีเอ็น	2 H – ไม่เก็บล็อก	3 E – ไวร์การ์ด	4 A – แคนาดา
5 G – ตรวจสอบ	6 B – โกสต์แบร์	7 D – แมคคาฟี	8 C – วิจิแลนต์แบร์

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย แคนาดา GhostBear และ VigilantBear ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

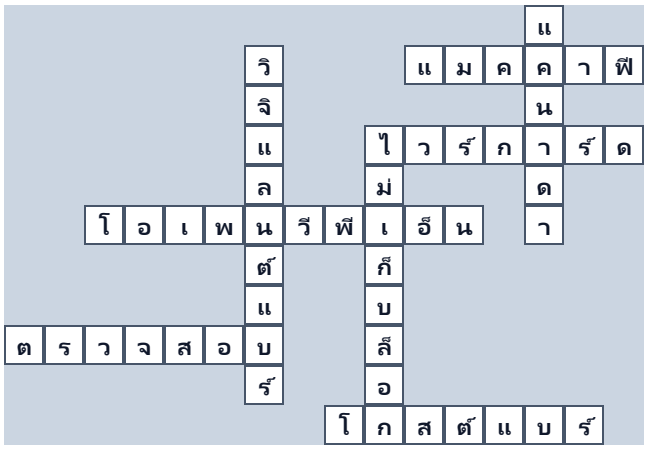
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	า	ฟ	บ	า	า	ไ	ห	นี	า	ม	กี	จ	า
า	รี	ด	ต	ว	ย	ง	ว	ก	ค	ต	จ	น	ตี	ว
ร	ตี	า	ว	า	ล	ล	ร์	ด	า	ร	อ	ย	ช	ฟ
ร์	ก	น	ก	ล	ม	า	ก	ป	อ	ว	อ	ม	มี	า
บ	ล	ค	ล	ป	โ	จ	า	า	นี	จ	กี	พ	ไ	ร
แ	ง	แ	า	ช	อ	า	ร์	า	ลี	ส	จ	ตี	ม่	า
ต์	น	ล	ผ	ดี	เ	ช	ด	โ	ก	อ	ด	า	เ	ต
น	า	จ	า	ค	พ	ก	ดี	ก	า	บ	ช	ว	ก็	ก
ล	ด	กี	ด	ท	น	ผ	ฟ	ส	ช	มี	ม	อ	บ	ต
แ	ฟ	ร	ดี	า	วี	แ	ท	ต์	า	ส	ท	ข	ล็	ข
จิ	า	น	ก	า	พี	ม	ล	แ	า	ม	ร	มี	อ	า
วิ	ร	ช	ก	ด	เ	ค	ง	บ	น	ร	ต	สี	ก	ย
ข	มี	ตี	ด	ด	อ็	ค	ว	ร์	บ	ฟ	อ	า	ร	ห
ห	รี	น	ผ	นี	น	า	ม	ผ	ดี	ข	กี	ส	บ	ลี
ง	ด	ร	ด	ค	ผ	ฟี	ห	ดี	ป	ร	กี	นี	า	ต

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

3 แนวนอน: แมคคาฟี บริษัทแม่ด้านความปลอดภัยที่เข้าซื้อ TunnelBear (6 ตัวอักษร)

4 แนวนอน: ไวร์การ์ด โปรโตคอลประสิทธิภาพสูงที่ใช้การเข้ารหัสลับสมัยใหม่ (7 ตัวอักษร)

5 แนวนอน: โอเพนวีพีเอ็น โปรโตคอลอุโมงค์โอเพนซอร์สมาตรฐานที่ใช้บนเดสก์ท็อป (10 ตัวอักษร)

6 แนวนอน: ตรวจสอบ การประเมินความปลอดภัยโดยบุคคลที่สามที่ทำเป็นประจำทุกปี (7 ตัวอักษร)

7 แนวนอน: โกสต์แบร์ เทคโนโลยีสับเมตาดาตาที่ใช้ข้ามการตรวจสอบแพ็กเก็ตเชิงลึก (7 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: แคนาดา ประเทศที่จดทะเบียนและเป็นที่ตั้งสำนักงานใหญ่ขององค์กร (6 ตัวอักษร)

2 แนวตั้ง: วิจิแลนต์แบร์ คิลสวิตช์ในตัวที่ปกป้องการเชื่อมต่อเมื่อหลุด (9 ตัวอักษร)

4 แนวตั้ง: ไม่เก็บล็อก นโยบายความเป็นส่วนตัวที่บังคับไม่เก็บประวัติทราฟฟิก (8 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. นแาดาค → **แคนาดา**
2. รวิบลจิต์แนแ → **วิจิแลนต์แบร์**
3. กไาดร์ร์ว → **ไวร์การ์ด**
4. บรสจอตว → **ตรวจสอบ**
5. แร์ต์สโบก → **โกสต์แบร์**
6. าคแคฟีม → **แมคคาฟี**
7. อฟโพีวีเอ็นนเ → **โอเพนวีพีเอ็น**
8. ก็มบกไอล็เ → **ไม่เก็บล็อก**

เฉลยภารกิจรหัสลับ

"แอป ทันเนลแบร์ มี วิจิแลนต์แบร์ ป้องกัน"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การหลีกเลี่ยงการเซ็นเซอร์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: นักวิจัยที่เดินทางผ่านประเทศที่บล็อกโปรโตคอล VPN ต้องเข้าถึงเอกสารวิจัย
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ต้องเปิดใช้ GhostBear เพื่อปกปิดเมทาดาทาของแพ็กเก็ต VPN ให้ดูเหมือนทราฟฟิก HTTPS ปกติ

B กรณีศึกษาที่ 2: ฮอตสปอตสาธารณะที่ไม่ปลอดภัย

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: วิศวกรเชื่อมต่อกับฮอตสปอต Wi-Fi สาธารณะที่สนามบินและพบว่าการเชื่อมต่อหลุดบ่อย
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: VigilantBear ตรึงอินเทอร์เฟซเครือข่ายทั้งหมด บล็อกการรั่วไหลของทราฟฟิกที่ไม่เข้ารหัสจนกว่าจะกู้คืนอุโมงค์ VPN ได้