ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

การปกป้องข้อมูลส่วนบุคคลและสิทธิ์ของคุณ

ข้อมูลส่วนบุคคล สิทธิความเป็นส่วนตัว (GDPR, CCPA) ตัวแทนค้าข้อมูล คุกกี้ ฟิชชิง VPN และบัญชีที่ปลอดภัยกว่า

ภาพรวมการเรียนรู้เรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคล

ได้รับข้อมูลครบถ้วน

รู้จักข้อมูลของคุณ

ข้อมูลที่เก็บรวบรวมและเหตุผล

เสริมพลัง

สิทธิความเป็นส่วนตัว

สิทธิตาม GDPR และ CCPA/CPRA

ระแวดระวัง

นิสัยที่ชาญฉลาด

MFA การอัปเดต และการสังเกตกลโกง

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับมาตรฐานความเป็นส่วนตัวของข้อมูลระดับโลก คุณจะได้สำรวจความยินยอมแบบ opt-in ของ GDPR สิทธิ์ opt-out ของ CCPA การลดข้อมูลให้น้อยที่สุด การเข้ารหัสทั้งดิสก์ และ TLS ขณะส่งข้อมูล

จุดตรวจสอบของใบงาน

- ☐ **ส่วนที่ 1-4: เรียนรู้สิทธิความเป็นส่วนตัวและนิสัยที่ปลอดภัยของคุณ**
- ☐ **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- ☐ **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- ☐ **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- ☐ **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- ☐ **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความเป็นส่วนตัวของข้อมูลของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/khwam-pen-suan-tua-khong-khomun/

เส้นทางการเรียนรู้ความเป็นส่วนตัวของข้อมูลส่วนบุคคลของคุณ

- ทำความเข้าใจสิทธิ์ความเป็นส่วนตัวของคุณภายใต้ GDPR และ CCPA ของแคลิฟอร์เนีย
- ทำความเข้าใจว่าผู้ค้าข้อมูล คุกกี้ และแอปเก็บข้อมูลส่วนบุคคลได้อย่างไร
- ใช้หลักการลดข้อมูลให้น้อยที่สุดโดยแชร์เฉพาะสิ่งที่บริการต้องใช้จริง
- ตัดสินใจอย่างรอบรู้เกี่ยวกับแบนเนอร์คุกกี้และข้อความขอสิทธิ์ของแอป
- ลดความเสี่ยงจากฟิชชิง การรั่วไหลของข้อมูล และ Wi-Fi สาธารณะด้วย MFA และการอัปเดต

คำแนะนำคู่มือความเป็นส่วนตัวของข้อมูล

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การปกป้องข้อมูลส่วนบุคคลของคุณเอง ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

ความเป็นส่วนตัวของข้อมูลส่วนบุคคลและสิทธิของคุณ (บทนำ)

ความเป็นส่วนตัวของข้อมูลคือความสามารถของคุณในการควบคุมวิธีที่ข้อมูลส่วนบุคคลของคุณถูกเก็บรวบรวม ใช้ จัดเก็บ และแบ่งปัน กฎหมายอย่าง GDPR และ CCPA ให้สิทธิแก่คุณ ขณะที่นิสัยอย่างการใช้รหัสผ่านที่รัดกุม MFA และการแบ่งปันข้อมูลอย่างระมัดระวังสามารถช่วยลดความเสี่ยงได้

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **ตัวเลือกใดสะท้อนหลักการลดข้อมูลให้น้อยที่สุด (data minimization) ได้ดีที่สุด?**
   - A. การแชร์เฉพาะข้อมูลที่บริการต้องใช้ตามวัตถุประสงค์
   - B. การให้สิทธิ์เข้าถึงเต็มรูปแบบแก่ทุกแอปเพื่อให้ตั้งค่าง่ายขึ้น
   - C. กรอกทุกช่องที่ไม่บังคับในแบบฟอร์มสมัครสมาชิก
   - D. การใช้รหัสผ่านเดียวซ้ำเพื่อให้จัดการบัญชีได้ง่ายขึ้น

2. **ควรทำขั้นตอนใดหากเว็บไซต์ที่คุณใช้รายงานว่าเกิดการละเมิดข้อมูล?**
   - A. เปลี่ยนรหัสผ่านนั้นและเปิดใช้ MFA หากมีให้ใช้
   - B. ใช้รหัสผ่านเดิมซ้ำกับบัญชีใหม่
   - C. ตอบกลับอีเมลแจ้งการละเมิดโดยแนบ PIN ของคุณ
   - D. เพิกเฉย เพราะการละเมิดข้อมูลไม่ค่อยสำคัญ

3. **ตามกฎของ EU ข้อใดคือความยินยอมที่ถูกต้องต่อคุกกี้ติดตาม?**
   - A. การติ๊กช่องที่ยังไม่ได้ติ๊กอย่างจงใจหลังได้รับข้อมูลที่ชัดเจน
   - B. ช่องที่ติ๊กไว้ล่วงหน้าบนแบนเนอร์คุกกี้หรือแบนเนอร์สมัครสมาชิก
   - C. เพียงแค่เลื่อนหรือท่องเว็บไซต์ต่อไป
   - D. ประกาศที่ซ่อนอยู่ในข้อกำหนดและเงื่อนไขของเว็บไซต์

4. **ผู้บริโภคในแคลิฟอร์เนียมีสิทธิ์ใดภายใต้ CCPA?**
   - A. เพื่อเลือกไม่ให้มีการขายหรือแชร์ข้อมูลของตน
   - B. เพื่อรับค่าธรรมเนียมคงที่ทุกครั้งที่มีคำขอข้อมูล
   - C. เพื่อเรียกร้องให้ลบแอปใดๆ ออกจากร้านแอป
   - D. เพื่อบล็อกการเก็บข้อมูลทั้งหมดโดยทุกบริษัท

5. **VPN ทำหน้าที่หลักอะไรเมื่อคุณเชื่อมต่อ Wi-Fi สาธารณะ?**
   - A. เข้ารหัสทราฟฟิกระหว่างอุปกรณ์ของคุณกับเซิร์ฟเวอร์ VPN
   - B. หยุดเว็บไซต์ไม่ให้ตั้งคุกกี้ใดๆ
   - C. มาแทนที่ MFA
   - D. ลบมัลแวร์ที่มีอยู่แล้วบนอุปกรณ์

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถามจริง/เท็จ 6

6. ความเป็นส่วนตัวของข้อมูลและความปลอดภัยของข้อมูลมีความหมายเหมือนกัน

○ จริง ○ เท็จ

7 คำถามจริง/เท็จ 7

7. GDPR อาจใช้กับบริษัทนอกสหภาพยุโรปที่เสนอบริการให้แก่ผู้คนในสหภาพยุโรป

○ จริง ○ เท็จ

8 คำถามจริง/เท็จ 8

8. การใช้ VPN ทำให้เว็บไซต์หยุดติดตามคุณด้วยคุกกี้

○ จริง ○ เท็จ

9 คำถามจริง/เท็จ 9

9. การแชร์ข้อมูลส่วนบุคคลออนไลน์ให้น้อยลงอาจลดความเสียหายจากการรั่วไหลของข้อมูลได้

○ จริง ○ เท็จ

10 คำถามจริง/เท็จ 10

10. CCPA ช่วยให้ผู้บริโภคเลือกไม่ให้มีการขายหรือแบ่งปันข้อมูลของตนได้

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. ภายใต้ GDPR ต้องให้ _____ โดยอิสระ เฉพาะเจาะจง รับทราบข้อมูล และชัดเจน ดังนั้นช่องที่ติ๊กไว้ล่วงหน้าจึงไม่นับ

2. _____ รวบรวมรายละเอียดจากบันทึกสาธารณะ แอป และการซื้อ เพื่อสร้างและขายโปรไฟล์ของบุคคล

3. ข้อความที่อ้างว่าพัสดุของคุณถูกระงับและขอให้ "ยืนยัน" รายละเอียดบัตรเป็นตัวอย่างทั่วไปของการ _____ แบบฟิชชิง

4. HTTPS ใช้ _____ เพื่อช่วยปกป้องข้อมูลระหว่างทางระหว่างเบราว์เซอร์กับเว็บไซต์

5. การให้ข้อมูลเฉพาะรายละเอียดที่แบบฟอร์มสมัครต้องการจริงๆ คือการใช้หลักการ _____

6. สิทธิที่จะ _____ ช่วยให้คุณขอให้องค์กรลบข้อมูลส่วนบุคคลของคุณ แม้จะมีข้อยกเว้น

คลังคำศัพท์

เข้ารหัส | ความยินยอม | ติดตาม | ถูกลืม | นายหน้าข้อมูล | ลดข้อมูล | เลือกออก | หลอกลวง

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความเป็นส่วนตัว

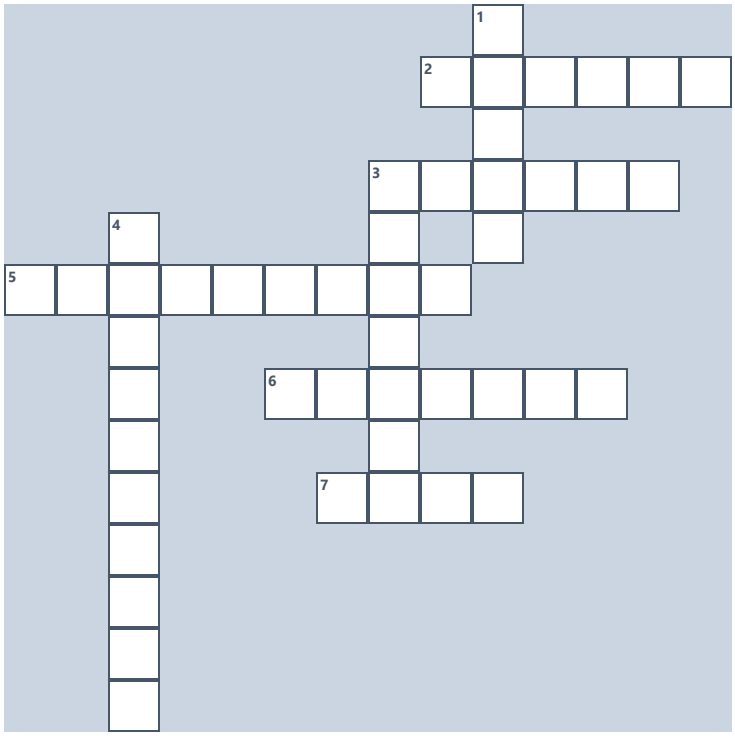
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. สิทธิในการลบข้อมูล**	**A**	สิทธิ์ของชาวแคลิฟอร์เนียในการให้ธุรกิจหยุดขายหรือแชร์ข้อมูลของคุณ
☐	**2. สิทธิ์ปฏิเสธ**	**B**	สิทธิภายใต้ GDPR ในการขอให้ลบข้อมูลส่วนบุคคลของคุณ โดยมีข้อยกเว้นบางประการ
☐	**3. การลดข้อมูลให้น้อยที่สุด**	**C**	ไฟล์ขนาดเล็กในเบราว์เซอร์ที่ใช้ติดตามกิจกรรมของคุณข้ามเว็บไซต์
☐	**4. การเข้ารหัส**	**D**	ความยินยอมที่ให้โดยอิสระ เฉพาะเจาะจง ได้รับข้อมูลครบถ้วน และไม่คลุมเครือ
☐	**5. โบรกเกอร์ข้อมูล**	**E**	การเก็บรวบรวมเฉพาะข้อมูลส่วนบุคคลที่จำเป็นต่อวัตถุประสงค์ที่ระบุไว้
☐	**6. ความยินยอม**	**F**	ข้อความปลอมที่หลอกให้คนเปิดเผยข้อมูลหรือข้อมูลล็อกอิน
☐	**7. ฟิชชิง**	**G**	การสลับข้อมูลให้ยุ่งเหยิงเพื่อให้เฉพาะผู้ที่มีกุญแจที่ถูกต้องเท่านั้นที่อ่านได้
☐	**8. คุกกี้ติดตาม**	**H**	บริษัทที่รวบรวมและขายโปรไฟล์ส่วนบุคคลจากหลายแหล่ง

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. การเก็บรวบรวมเฉพาะสิ่งที่จำเป็นต่อวัตถุประสงค์ที่ระบุไว้ (data minimization) (6)

3. การสับเปลี่ยนข้อมูลเพื่อให้เฉพาะผู้ที่มีคีย์ที่ถูกต้องอ่านได้ (6)

5. ความตกลงที่ให้โดยอิสระ เฉพาะเจาะจง รับทราบข้อมูล และชัดเจนต่อการใช้ข้อมูล (9)

6. ข้อความปลอมที่ล่อให้คุณเปิดเผยข้อมูลเข้าสู่ระบบหรือรายละเอียดบัตร (ฟิชชิง) (7)

7. สิทธิที่ให้คุณขอให้องค์กรลบข้อมูลส่วนบุคคลของคุณ (4)

แนวตั้ง

1. ไฟล์คุกกี้ขนาดเล็กของเบราว์เซอร์ที่ติดตามกิจกรรมของคุณข้ามเว็บไซต์ได้ (5)

3. สิทธิตาม CCPA ในการหยุดการขายหรือแบ่งปันข้อมูลของคุณ (7)

4. บริษัทที่รวบรวมและขายโปรไฟล์ของบุคคล (10)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: การเก็บรวบรวมเฉพาะสิ่งที่จำเป็นต่อวัตถุประสงค์ที่ระบุไว้ (data minimization) (6 ตัวอักษร):

3 แนวนอน: การสับเปลี่ยนข้อมูลเพื่อให้เฉพาะผู้ที่มีคีย์ที่ถูกต้องอ่านได้ (6 ตัวอักษร):

5 แนวนอน: ความตกลงที่ให้โดยอิสระ เฉพาะเจาะจง รับทราบข้อมูล และชัดเจนต่อการใช้ข้อมูล (9 ตัวอักษร):

6 แนวนอน: ข้อความปลอมที่ล่อให้คุณเปิดเผยข้อมูลเข้าสู่ระบบหรือรายละเอียดบัตร (ฟิชชิง) (7 ตัวอักษร):

7 แนวนอน: สิทธิที่ให้คุณขอให้องค์กรลบข้อมูลส่วนบุคคลของคุณ (4 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ไฟล์คุกกี้ขนาดเล็กของเบราว์เซอร์ที่ติดตามกิจกรรมของคุณข้ามเว็บไซต์ได้ (5 ตัวอักษร):

3 แนวตั้ง: สิทธิตาม CCPA ในการหยุดการขายหรือแบ่งปันข้อมูลของคุณ (7 ตัวอักษร):

4 แนวตั้ง: บริษัทที่รวบรวมและขายโปรไฟล์ของบุคคล (10 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า	นี	า	น	นี	ส	ช	เ	มี	ฟ	บ	า	า	ห	นี
า	ม	ม	กี	จ	า	า	ข้	เ	รี	ต	ว	ย	ง	ก
ค	จ	า	น	ตี	ว	ร	า	ตี	ลึ	ว	า	ล	ล	ด
ม	า	ต	อ	ย	ช	ฟ	ร	ก	ก	อ	ล	ม	า	ป
อ	อ	ด	อ	ม	น	มี	ห้	า	ล	ล	ก	ป	ห	จ
ย	า	ติ	นี	กี	า	พ	ส	ร	ง	า	ช	อ	ล	า
น	า	ลึ	จ	ดี	ย	า	น	ล	ล	ผ	ดี	ช	อ	ก
ยิ	ด	า	ต	า	ห	จ	า	ด	ค	ก	ดี	า	ก	ก
ม	ช	ว	ก	ด	น้	กี	ด	ข้	ท	ผ	ฟ	ช	ล	มี
า	ม	อ	ต	ฟ	า	ร	ดี	อ	า	ท	า	ส	ว	ท
ว	ข	ข	า	น	ข้	ก	า	มู	ล	ม	า	ม	ง	ร
ค	มี	า	ร	ช	อ	ก	ด	ล	ลึ	ง	น	ร	ต	สี
ย	ข	มี	ดี	ด	มู	ด	ว	ก	บ	ฟ	อ	า	ร	ห
ห	รี	น	ผ	นี	ล	ม	ถู	ผ	ดี	ข	กี	ส	บ	ลึ
ง	ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ

รายการคำศัพท์

ถูกลืม เลือกออก ลดข้อมูล เข้ารหัส นายหน้าข้อมูล ความยินยอม หลอกลวง ติดตาม

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. ถูกลืม

B. เลือกออก

C. ลดข้อมูล

D. เข้ารหัส

E. นายหน้าข้อมูล

F. ความยินยอม

G. หลอกลวง

H. ติดตาม

คำนิยามและช่องจับคู่

1. สิทธิตาม CCPA ในการหยุดการขายหรือแบ่งปันข้อมูลของคุณ
2. ความตกลงที่ให้โดยอิสระ เฉพาะเจาะจง รับทราบข้อมูล และชัดเจนต่อการใช้ข้อมูล
3. บริษัทที่รวบรวมและขายโปรไฟล์ของบุคคล
4. สิทธิที่ให้คุณขอให้องค์กรลบข้อมูลส่วนบุคคลของคุณ
5. การเก็บรวบรวมเฉพาะสิ่งที่จำเป็นต่อวัตถุประสงค์ที่ระบุไว้ (data minimization)
6. ข้อความปลอมที่ล่อให้คุณเปิดเผยข้อมูลเข้าสู่ระบบหรือรายละเอียดบัตร (ฟิชชิง)
7. ไฟล์คุกกี้ขนาดเล็กของเบราว์เซอร์ที่ติดตามกิจกรรมของคุณข้ามเว็บไซต์ได้
8. การสับเปลี่ยนข้อมูลเพื่อให้เฉพาะผู้ที่มีคีย์ที่ถูกต้องอ่านได้

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ล ถ ู ม ก
2. ล ล ข้ ม ู อ ด
3. น า ม ู ข้ า น้ ล ห อ ย
4. ง ล ล ก ว ห อ
5. อ ก ก อ เ อ ล ื
6. ห ั ร เ า ส ข้
7. น ค อ ม ย ม ว ย ิ า
8. ม ต ิ ต า ด

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	ขั้นตอนที่ควรทำหลังเกิดการละเมิดข้อมูล			
2	แอปที่ขอตำแหน่งของคุณ			
3	การตั้งค่าความเป็นส่วนตัวที่ควรตรวจสอบบนโทรศัพท์เครื่องใหม่			
4	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
5	สัญญาณที่บ่งบอกว่าข้อความอาจเป็นฟิชชิง			
6	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
7	ข้อมูลส่วนตัวที่ไม่ควรโพสต์บนโซเชียลมีเดีย			
8	วิธีปกป้องบัญชีของคุณ			
9	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
10	บัญชีที่ควรเปิดใช้ MFA			
11	สิ่งที่คุณสำรองข้อมูล			
12	สถานที่ที่คุณอาจใช้ Wi-Fi สาธารณะ			
13	สิ่งที่ควรทำหลังข้อมูลรั่วไหล			
14	บริษัทที่อาจเก็บข้อมูลการเรียกดูของคุณ			
15	สัญญาณเตือนในอีเมล			

จุดตรวจสอบที่ 8: กรณีศึกษาความเป็นส่วนตัวของข้อมูล

นำแนวคิดที่คุณได้เรียนรู้ไปใช้กับสถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การขอให้เว็บไซต์ลบข้อมูล



สถานการณ์: มายา ผู้อาศัยอยู่ในฝรั่งเศส ปิดบัญชีบนแอปช้อปปิ้งเมื่อสองปีก่อน แต่ยังคงได้รับอีเมลการตลาดจากแอปนั้น เธอต้องการให้แอปลบข้อมูลส่วนบุคคลของเธอตามสิทธิในการลบข้อมูล (right to erasure) ของ GDPR

คำถามอภิปราย: มายาทำขั้นตอนใดได้บ้าง และแอปอาจเก็บข้อมูลใดไว้ได้โดยชอบด้วยกฎหมาย?

กรณีศึกษาที่ 2: แอปแบบทดสอบและการอนุญาต



สถานการณ์: แอปแบบทดสอบบุคลิกภาพฟรีขอตำแหน่งที่ตั้ง รายชื่อติดต่อ ไมโครโฟน และวันเกิดของลีโอก่อนที่เขาจะเริ่มใช้งานได้

คำถามอภิปราย: สิทธิ์ใดดูไม่จำเป็น และลีโอมีทางเลือกใดบ้างเพื่อลดปริมาณข้อมูลที่เขาแชร์?

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้ที่ตระหนักถึงความเป็นส่วนตัวจะหยุดคิดก่อนแชร์รายละเอียดส่วนตัวทางออนไลน์ ใช้รหัสจับคู่ตัวอักษรกับตัวเลขด้านล่างเพื่อถอดรหัสข้อความโดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง ข้อความความปลอดภัยไซเบอร์ที่ถอดรหัสแล้ว:

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

4	51	20		1	63	45	25		58	10	35	67		2	64	45	33	56	37

45	45	25	61	37	25	67

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความเป็นส่วนตัวของข้อมูลระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลของคุณ

Q1: ความเป็นส่วนตัวของข้อมูลกับความปลอดภัยของข้อมูลต่างกันอย่างไร?

ความเป็นส่วนตัวคือการควบคุมของคุณว่าข้อมูลส่วนบุคคลถูกเก็บ ใช้ และแชร์อย่างไร ส่วนความปลอดภัยคือการป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตเข้าถึงข้อมูลนั้น

Q2: GDPR คืออะไร?

ระเบียบ GDPR ของสหภาพยุโรป ซึ่งบังคับใช้ตั้งแต่ 25 พฤษภาคม 2018 กำหนดกฎการประมวลผลข้อมูลส่วนบุคคลและให้สิทธิแก่บุคคลเหนือข้อมูลนั้น [1]

Q3: CCPA คืออะไร?

กฎหมายความเป็นส่วนตัวของผู้บริโภคแห่งรัฐแคลิฟอร์เนีย ตามที่แก้ไขโดย CPRA ให้สิทธิ์ผู้อยู่อาศัยในการรับรู้ ลบ แก้ไข และเลือกไม่ให้ขายหรือแชร์ข้อมูล [4]

Q4: การลดข้อมูลให้น้อยที่สุด (data minimization) หมายความว่าอย่างไร?

ใช้เฉพาะข้อมูลส่วนบุคคลที่เพียงพอ เกี่ยวข้อง และจำกัดเท่าที่จำเป็นต่อวัตถุประสงค์ ในฐานะผู้ใช้ คุณนำไปใช้ได้ด้วยการแบ่งปันให้น้อยลง [1]

Q5: App Permissions คืออะไร?

การตั้งค่าที่ให้แอปเข้าถึงตำแหน่งที่ตั้ง รายชื่อติดต่อ หรือรูปภาพของคุณ การตรวจสอบและปิดการตั้งค่าที่ไม่จำเป็นอาจช่วยจำกัดการเก็บข้อมูลได้ [8]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความเป็นส่วนตัวของข้อมูลระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลของคุณ

Q6: HTTPS ช่วยความเป็นส่วนตัวของฉันอย่างไร?

HTTPS เข้ารหัสข้อมูลระหว่างเบราว์เซอร์ของคุณกับเว็บไซต์ แต่เว็บไซต์หลอกลวงก็ใช้ HTTPS ได้เช่นกัน ดังนั้นไอคอนแม่กุญแจจึงไม่ได้พิสูจน์ว่าเว็บไซต์น่าเชื่อถือ [10]

Q7: สิทธิในการลบข้อมูล (Right to Erasure) คืออะไร?

ภายใต้ GDPR มาตรา 17 คุณขอให้องค์กรลบข้อมูลของคุณได้ในบางกรณี สิทธินี้ไม่เด็ดขาดและมีข้อยกเว้น [1]

Q8: อะไรถือเป็นความยินยอมที่ถูกต้อง?

การกระทำยืนยันที่ชัดเจน เช่น การติ๊กช่องที่ยังไม่ได้ติ๊กหลังได้รับข้อมูลที่ชัดเจน ช่องที่ติ๊กไว้ล่วงหน้า การนิ่งเฉย หรือการเลื่อนหน้าจอไม่นับ [2]

Q9: อะไรทำให้รหัสผ่านแข็งแกร่ง?

ความยาวสำคัญที่สุด: NIST ขอให้เว็บไซต์กำหนดรหัสผ่านที่ใช้เพียงอย่างเดียวให้มีอย่างน้อย 15 ตัวอักษร และอนุญาตให้ใช้ตัวจัดการรหัสผ่าน [11]

Q10: ฉันควรทำอย่างไรหลังข้อมูลรั่วไหล?

เปลี่ยนรหัสผ่านที่ได้รับผลกระทบ เปิดใช้ MFA ติดตามบัญชีของคุณ และพิจารณาแช่แข็งเครดิตฟรี IdentityTheft.gov รวบรวมขั้นตอนการกู้คืนไว้ [9]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความเป็นส่วนตัวระดับสูง (ส่วน C)

สำรวจคำถามเชิงลึกเกี่ยวกับฐานทางกฎหมาย คุกกี้ การติดตาม ดาต้าโบรกเกอร์ และสิทธิ์ของคุณทางออนไลน์

Q1: การประมวลผลข้อมูลทั้งหมดต้องได้รับความยินยอมจากฉันภายใต้ GDPR หรือไม่?

ไม่ ความยินยอมเป็นหนึ่งในหกฐานทางกฎหมายตามมาตรา 6 ส่วนฐานอื่น ได้แก่ สัญญา ภาระผูกพันทางกฎหมาย และผลประโยชน์โดยชอบด้วยกฎหมาย [1]

Q2: GDPR ใช้บังคับที่ไหน?

กับองค์กรที่ก่อตั้งใน EU และองค์กรนอก EU ที่เสนอสินค้าหรือบริการให้ หรือติดตามพฤติกรรมของผู้คนใน EU [1]

Q3: เว็บไซต์ต้องขอความยินยอมสำหรับคุกกี้ทุกประเภทหรือไม่?

ไม่เสมอไป คุกกี้ที่จำเป็นอย่างยิ่งโดยทั่วไปได้รับการยกเว้น แต่คุกกี้ที่ไม่จำเป็น เช่น คุกกี้ติดตาม ต้องได้รับความยินยอมที่ถูกต้องล่วงหน้า [3]

Q4: ตัวติดตามของบุคคลที่สามมีความเสี่ยงต่อความเป็นส่วนตัวอย่างไร?

ตัวติดตามของบุคคลที่สามสามารถติดตามคุณข้ามเว็บไซต์จำนวนมากเพื่อแสดงโฆษณาเฉพาะกลุ่ม การลบคุกกี้และปรับการตั้งค่าความเป็นส่วนตัวอาจช่วยได้ [8]

Q5: ผู้ค้าข้อมูล (data broker) คืออะไร?

ธุรกิจที่รวบรวมข้อมูลส่วนบุคคลจากหลายแหล่งและขายให้บริษัทอื่น ผู้อยู่อาศัยในแคลิฟอร์เนียสามารถใช้แพลตฟอร์ม DROP ของรัฐเพื่อขอให้ลบข้อมูลได้ [5]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความเป็นส่วนตัวระดับสูง (ส่วน D)

สำรวจคำถามเชิงลึกเกี่ยวกับฐานทางกฎหมาย คุกกี้ การติดตาม ดาต้าโบรกเกอร์ และสิทธิ์ของคุณทางออนไลน์

Q6: ลิงก์ 'Do Not Sell or Share' ของ CCPA คืออะไร?

ธุรกิจที่ขายหรือแบ่งปันข้อมูลโดยทั่วไปต้องมีลิงก์ 'Do Not Sell or Share My Personal Information' และเคารพสัญญาณการไม่ยินยอม เช่น GPC [4]

Q7: VPN ทำให้ฉันไม่ระบุตัวตนหรือไม่?

ไม่ VPN เข้ารหัสการรับส่งข้อมูลไปยังเซิร์ฟเวอร์ VPN และซ่อน IP ของคุณจากเว็บไซต์ แต่ผู้ให้บริการมองเห็นได้ และคุกกี้กับการพิมพ์ลายนิ้วมืออุปกรณ์ยังคงติดตามคุณได้ [12]

Q8: ฉันสังเกตข้อความฟิชชิงได้อย่างไร?

ระวังคำขอเร่งด่วนให้คลิกลิงก์ ยืนยันรายละเอียดการชำระเงิน หรือแก้ไขปัญหาบัญชี ให้ติดต่อบริษัทโดยใช้หมายเลขโทรศัพท์หรือเว็บไซต์ที่คุณรู้ว่าเป็นของจริง [7]

Q9: Wi-Fi สาธารณะปลอดภัยที่จะใช้หรือไม่?

อาจมีความเสี่ยง เว็บไซต์ส่วนใหญ่ใช้การเข้ารหัส ดังนั้นให้ตรวจสอบ HTTPS อัปเดตซอฟต์แวร์ให้ทันสมัย และใช้ MFA [10] VPN อาจเพิ่มการป้องกันบนเครือข่ายที่ไม่น่าเชื่อถือ [12]

Q10: บทลงโทษทางการเงินสูงสุดภายใต้ GDPR คืออะไร?

สำหรับการละเมิดที่ร้ายแรงที่สุด ค่าปรับอาจสูงถึง 20 ล้านยูโรหรือ 4% ของยอดขายรายปีทั่วโลก แล้วแต่จำนวนใดจะสูงกว่า [1]

ส่วนที่ 11: ข้อเท็จจริงด้านความเป็นส่วนตัวของข้อมูลในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับกฎหมายความเป็นส่วนตัว ผู้ค้าข้อมูล การฉ้อโกง การรั่วไหลของข้อมูล และนิสัยออนไลน์ที่ปลอดภัยกว่า

1. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

GDPR บังคับใช้ตั้งแต่ 25 พฤษภาคม 2018 และให้สิทธิแก่ผู้คนในการเข้าถึง แก้ไข และลบข้อมูลส่วนบุคคลของตน [1]

2. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

ภายใต้ GDPR การละเมิดที่ร้ายแรงที่สุดอาจถูกปรับสูงสุด 20 ล้านยูโรหรือ 4% ของรายได้ทั่วโลก [1]

3. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

การแก้ไข CPRA ต่อ CCPA ของรัฐแคลิฟอร์เนียมีผลบังคับใช้เมื่อวันที่ 1 มกราคม 2023 โดยเพิ่มสิทธิ์ในการแก้ไขข้อมูลและจำกัดการใช้ข้อมูลอ่อนไหว [4]

4. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

ผู้บริโภครายงานว่าสูญเสียเงิน 15.9 พันล้านดอลลาร์จากการฉ้อโกงในปี 2025 เพิ่มขึ้นจากกว่า 12 พันล้านดอลลาร์ในปีก่อนหน้า ตามข้อมูลของ FTC [6]

5. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

ตั้งแต่ 1 มกราคม 2026 ชาวแคลิฟอร์เนียสามารถใช้แพลตฟอร์ม DROP ฟรีเพื่อขอให้นายหน้าข้อมูลลบข้อมูลส่วนบุคคลของตนได้ [5]

6. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

ตามกฎคุ้มครองข้อมูลของ EU ช่องที่ติ๊กไว้ล่วงหน้า การนิ่งเฉย หรือการไม่ทำอะไร ไม่นับเป็นความยินยอมที่ถูกต้อง [2]

7. ข้อมูลเชิงลึกด้านความเป็นส่วนตัว

ในสหราชอาณาจักร เว็บไซต์ต้องให้วิธีแก่คุณในการให้ความยินยอมต่อคุกกี้ใดๆ ที่ไม่จำเป็นอย่างเคร่งครัดต่อเว็บไซต์ [3]

8. ข้อมูลเชิงลึกด้านความเป็นส่วนตัว

GDPR กำหนดให้การละเมิดข้อมูลส่วนบุคคลบางกรณีต้องรายงานต่อหน่วยงานภายใน 72 ชั่วโมง หากทำได้ [1]

9. ข้อมูลเชิงลึกด้านความเป็นส่วนตัว

NIST ระบุว่าเว็บไซต์ไม่ควรบังคับเปลี่ยนรหัสผ่านเป็นระยะ และควรตรวจสอบรหัสผ่านใหม่เทียบกับรายการที่ถูกบุกรุก [11]

10. ข้อมูลเชิงลึกเรื่องความเป็นส่วนตัว

VPN ซ่อนที่อยู่ IP ของคุณจากเว็บไซต์ แต่ผู้ให้บริการ VPN ยังคงเห็นทราฟฟิกของคุณได้ ดังนั้นควรเลือกอย่างรอบคอบ [12]

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาอ้างอิงแนวทางด้านความเป็นส่วนตัวอย่างเป็นทางการของ EU สหราชอาณาจักร แคลิฟอร์เนีย FTC NIST และ EFF

แหล่งอ้างอิงอย่างเป็นทางการและจากผู้เชี่ยวชาญ

[1] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119.

https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[3] Information Commissioner's Office. (n.d.). Cookies. ICO for the public.

https://ico.org.uk/for-the-public/online/cookies/

[4] California Privacy Protection Agency. (n.d.). Frequently asked questions (FAQs).

https://cppa.ca.gov/faq.html

[5] California Privacy Protection Agency. (2025). Delete Request and Opt-out Platform (DROP).

https://privacy.ca.gov/drop/

[6] Federal Trade Commission. (2026, March 25). FTC testifies before the Joint Economic Committee on agency's efforts to combat fraud [Press release].

https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud

[7] Federal Trade Commission. (2022). How to recognize and avoid phishing scams. Consumer Advice.

https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[8] Federal Trade Commission. (2023). How websites and apps collect and use your information. Consumer Advice.

https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information

[9] Federal Trade Commission. (2024). What to know about identity theft. Consumer Advice.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[10] Federal Trade Commission. (2023). Are public Wi-Fi networks safe? What you need to know. Consumer Advice.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[11] National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4).

https://csrc.nist.gov/pubs/sp/800/63/b/4/final

[12] Electronic Frontier Foundation. (2026). Choosing the VPN that's right for you. Surveillance Self-Defense.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **การใช้ข้อมูลให้น้อยที่สุด** การลดข้อมูลให้น้อยที่สุด **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

มาตรา 5 ของ GDPR กำหนดให้ข้อมูลส่วนบุคคลต้องเพียงพอ เกี่ยวข้อง และจำกัดเท่าที่จำเป็น ผู้ใช้สามารถทำตามแนวคิดนี้ได้โดยแบ่งปันข้อมูลให้น้อยลง [1]

2 **การรับมือเมื่อเกิดการรั่วไหลของข้อมูล** การละเมิดข้อมูล **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

หลังเกิดการละเมิดข้อมูล ให้เปลี่ยนรหัสผ่านที่ถูกเปิดเผย เปิดใช้ MFA และเฝ้าติดตามบัญชี IdentityTheft.gov มีขั้นตอนการกู้คืนที่ปรับให้เหมาะกับแต่ละกรณี [9]

3 **ความยินยอมที่ถูกต้อง** ความยินยอมเรื่องคุกกี้ **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

ความยินยอมที่ถูกต้องต้องมีการกระทำยืนยันที่ชัดเจนหลังได้รับข้อมูลที่ชัดเจน ช่องที่ติ๊กไว้ล่วงหน้าและการเลื่อนหน้าต่อไปไม่เข้าเกณฑ์ [2]

4 **สิทธิ์ตาม CCPA** กฎหมาย CCPA **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

ผู้บริโภคในรัฐแคลิฟอร์เนียสามารถเลือกไม่ให้มีการขายหรือแชร์ข้อมูลส่วนบุคคลได้ รวมถึงผ่านสัญญาณ Global Privacy Control [4]

5 **การป้องกันของ VPN** อุโมงค์ VPN **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

VPN เข้ารหัสทราฟฟิกไปยังเซิร์ฟเวอร์ VPN และซ่อน IP ของคุณจากเว็บไซต์ แต่คุกกี้และการระบุลายนิ้วมืออุปกรณ์ยังคงติดตามคุณได้ [12]

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **ความเป็นส่วนตัวเทียบกับความปลอดภัย** ความเป็นส่วนตัว — คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เกี่ยวข้องแต่ต่างกัน: มาตรา 5 ของ GDPR กำหนดกฎเกี่ยวกับการใช้ข้อมูล ส่วนมาตรา 32 กำหนดมาตรการรักษาความปลอดภัยแยกต่างหาก [1]

7 **ขอบเขตเชิงพื้นที่ของ GDPR** ขอบเขตของ GDPR — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

มาตรา 3(2) ครอบคลุมองค์กรนอก EU ที่เสนอสินค้าหรือบริการแก่ หรือเฝ้าติดตามพฤติกรรมของ บุคคลใน EU [1]

8 **VPN และคุกกี้** ขีดจำกัดของ VPN — คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

VPN ซ่อนที่อยู่ IP ของคุณ แต่คุกกี้ พิกเซลติดตาม และการระบุลายนิ้วมืออุปกรณ์ยังคงติดตามคุณข้ามเว็บไซต์ได้ [12]

9 **แชร์ให้น้อยลง** การลดข้อมูลให้น้อยที่สุด — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การปิดสิทธิ์แอปที่ไม่จำเป็นและแบ่งปันข้อมูลให้น้อยลงจะจำกัดสิ่งที่ถูกเก็บรวบรวมและอาจถูกเปิดเผยในภายหลังจากการรั่วไหลของข้อมูล [8]

10 **เลือกไม่ให้ขายหรือแบ่งปัน** กฎหมาย CCPA — คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ธุรกิจที่ขายหรือแบ่งปันข้อมูลต้องมีลิงก์ไม่ยินยอมที่ชัดเจน เช่น 'Do Not Sell or Share My Personal Information' [4]

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

B 1. สิทธิในการลบข้อมูล	A 2. สิทธิ์ปฏิเสธ	E 3. การลดข้อมูลให้น้อยที่สุด	G 4. การเข้ารหัส
H 5. โบรกเกอร์ข้อมูล	D 6. ความยินยอม	F 7. ฟิชชิง	C 8. คุกกี้ติดตาม

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ความยินยอม	2 นายหน้าข้อมูล	3 หลอกลวง	4 เข้ารหัส
5 ลดข้อมูล	6 ถูกลืม		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 B – เลือกออก	2 F – ความยินยอม	3 E – นายหน้าข้อมูล	4 A – ถูกลืม
5 C – ลดข้อมูล	6 G – หลอกลวง	7 H – ติดตาม	8 D – เข้ารหัส

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย สิทธิในการลบข้อมูล สิทธิ์ปฏิเสธ และ การลดข้อมูลให้น้อยที่สุด ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

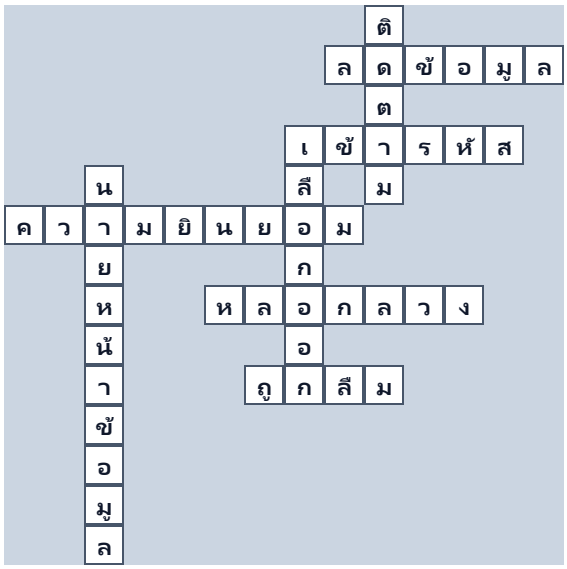
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	นี	า	น	นี	ส	ช	เ	มี	ฟ	บ	า	า	ห	นี
า	ม	ม	กี	จ	า	า	ข้	เ	รี	ต	ว	ย	ง	ก
ค	จ	า	น	ดี	ว	ร	า	ดี	ลื	ว	า	ล	ล	ด
ม	า	ต	อ	ย	ช	ฟ	ร	ก	ก	อ	ล	ม	า	ป
อ	อ	ด	อ	ม	น	มี	ห้	า	ล	ล	ก	ป	ห	จ
ย	า	ติ	นี	กี	า	พ	ส	ร	ง	า	ช	อ	ล	า
น	า	ลื	จ	ดี	ย	า	น	ล	ล	ผ	ดี	ช	อ	ก
ยิ	ด	า	ต	า	ห	จ	า	ด	ค	ก	ดี	า	ก	ก
ม	ช	ว	ก	ด	น้	กี	ด	ข้	ท	ผ	ฟ	ช	ล	มี
า	ม	อ	ต	ฟ	า	ร	ดี	อ	า	ท	า	ส	ว	ท
ว	ข	ข	า	น	ข้	ก	า	มู	ล	ม	า	ม	ง	ร
ค	มี	า	ร	ช	อ	ก	ด	ล	ลื	ง	น	ร	ต	สี
ย	ข	มี	ดี	ด	มู	ด	ว	ก	บ	ฟ	อ	า	ร	ห
ห	รี	น	ผ	นี	ล	ม	ถู	ผ	ดี	ข	กี	ส	บ	ลื
ง	ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: ลดข้อมูล การเก็บรวบรวมเฉพาะสิ่งที่จำเป็นต่อวัตถุประสงค์ที่ระบุไว้ (data minimization) (6 ตัวอักษร)

3 แนวนอน: เข้ารหัส การสับเปลี่ยนข้อมูลเพื่อให้เฉพาะผู้ที่มีคีย์ที่ถูกต้องอ่านได้ (6 ตัวอักษร)

5 แนวนอน: ความยินยอม ความตกลงที่ให้โดยอิสระ เฉพาะเจาะจง รับทราบข้อมูล และชัดเจนต่อการใช้ข้อมูล (9 ตัวอักษร)

6 แนวนอน: หลอกลวง ข้อความปลอมที่ล่อให้คุณเปิดเผยข้อมูลเข้าสู่ระบบหรือรายละเอียดบัตร (ฟิชชิง) (7 ตัวอักษร)

7 แนวนอน: ถูกลืม สิทธิที่ให้คุณขอให้องค์กรลบข้อมูลส่วนบุคคลของคุณ (4 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ติดตาม ไฟล์คุกกี้ขนาดเล็กของเบราว์เซอร์ที่ติดตามกิจกรรมของคุณข้ามเว็บไซต์ได้ (5 ตัวอักษร)

3 แนวตั้ง: เลือกออก สิทธิตาม CCPA ในการหยุดการขายหรือแบ่งปันข้อมูลของคุณ (7 ตัวอักษร)

4 แนวตั้ง: นายหน้าข้อมูล บริษัทที่รวบรวมและขายโปรไฟล์ของบุคคล (10 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ลืถูมก — **ถูกลืม**
2. ลลข้มูอด — **ลดข้อมูล**
3. นามูข้าน้ลหอย — **นายหน้าข้อมูล**
4. งลลกวหอ — **หลอกลวง**
5. อกกอเอลื — **เลือกออก**
6. หัรเาสข้ — **เข้ารหัส**
7. นคอมยมาวยิา — **ความยินยอม**
8. มติตาด — **ติดตาม**

เฉลยภารกิจรหัสลับ

"คิด ก่อน แชร์ ข้อมูล ออนไลน์"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การขอให้เว็บไซต์ลบข้อมูล

แนวทางสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: มายาซึ่งอาศัยอยู่ในฝรั่งเศสปิดบัญชีแอปช้อปปิ้งเมื่อสองปีก่อน แต่ยังได้รับอีเมลการตลาดของแอปนั้น เธอต้องการให้แอปลบข้อมูลส่วนบุคคลของเธอตามสิทธิในการลบข้อมูลภายใต้ GDPR
- แนวทางที่แนะนำ: ตัวเลือกที่ 1: Maya ส่งคำขอลบข้อมูลเป็นลายลักษณ์อักษรและคัดค้านการตลาดทางตรง ซึ่งจะต้องหยุดหลังจากนั้น โดยทั่วไปแอปควรตอบกลับภายในหนึ่งเดือน [1] ตัวเลือกที่ 2: เธอยกเลิกการสมัครรับข้อความก่อนเพื่อบรรเทาอย่างรวดเร็ว เหตุผล: การลบข้อมูลไม่ใช่สิทธิ์เด็ดขาด แอปจึงอาจเก็บข้อมูลที่จำเป็นต่อภาระผูกพันทางกฎหมายหรือการเรียกร้องทางกฎหมายไว้ได้ [1] หากแอปไม่ตอบกลับ เธอสามารถร้องเรียนต่อหน่วยงานคุ้มครองข้อมูลของเธอได้ [1]

B กรณีศึกษาที่ 2: แอปแบบทดสอบและการอนุญาต

แนวทางสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: แอปแบบทดสอบบุคลิกภาพฟรีขอตำแหน่ง รายชื่อติดต่อ ไมโครโฟน และวันเกิดจากลีโอก่อนที่เขาจะเริ่มใช้งานได้
- แนวทางที่แนะนำ: ตัวเลือกที่ 1: ปฏิเสธการเข้าถึงตำแหน่งที่ตั้ง รายชื่อติดต่อ และไมโครโฟน แล้วตรวจสอบว่าแบบทดสอบยังใช้งานได้หรือไม่ [8] ตัวเลือกที่ 2: หากแอปยืนกราน ให้เลือกแอปอื่นหรือลบแอปนั้น [8] เหตุผล: แบบทดสอบแทบไม่จำเป็นต้องใช้ข้อมูลเหล่านั้น และการแชร์ให้น้อยลงช่วยจำกัดสิ่งที่อาจถูกเก็บ ขาย หรือเปิดเผย Leo ยังสามารถตรวจสอบสิทธิ์เป็นประจำได้ในการตั้งค่าความเป็นส่วนตัวของโทรศัพท์ [8]