

บทเรียนที่ 2

WE THINK DIGITAL

พื้นฐานด้านดิจิทัล



 Meta

We Think Digital

หัวข้อที่ 1

ความรู้พื้นฐาน ความเป็นส่วนตัวบน โลกอินเทอร์เน็ต



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.



กิจกรรม

เกมความเป็น ส่วนตัว



ความเป็นส่วนตัวคืออะไร
ในมุมมองของเรา



อะไรคือความเป็นส่วนตัว

ความเป็นส่วนตัว คือ วิธีการที่
เราเลือกจัดการข้อมูลของเรา

สิ่งสำคัญ คือ เราต้องตระหนักถึง
ความเข้าใจในความเป็นส่วนตัว
ของตนเอง และเราคิดว่าเราพึง
พอใจกับความเข้าใจนั้นหรือไม่

มีอย่างอื่นอีกหรือไม่ที่ไม่จำเป็นต้องเก็บ
เป็นความลับ แต่เราต้องการเก็บเป็นส่วนตัว
จากคนที่ไม่รู้จักดีพอหรือคนที่เพิ่งเจอกัน

มีอะไรที่เราไม่ยอมให้ผู้
ปกครองหรือเพื่อนรู้หรือ
ไม่

เราได้เรียนรู้อะไร
เกี่ยวกับความเข้าใจ
ส่วนตัวของตนเองที่
ทำให้เรารู้สึกแปลก
ใจ

มีอะไรที่เราเก็บเป็นความ
ลับจากคุณครูหรือคุณครู
คนอื่น ๆ หรือไม่



กิจกรรม

ความเข้าใจ ส่วนบุคคลเกี่ยวกับ ความเป็นส่วนตัว

กิจกรรมที่ 1



หาตัวอย่างออนไลน์ 3 ตัวอย่างที่มีคนแชร์หรือโพสต์ข้อมูลซึ่งถ้าเป็นเราจะเก็บข้อมูลนั้นไว้ส่วนตัว

กิจกรรมที่ 2



ในแต่ละตัวอย่างให้เขียนอธิบายว่าเพราะเหตุใดเราจึงเลือกที่จะเก็บข้อมูลนี้เป็นส่วนตัว

กิจกรรมที่ 3



อธิบายว่า ถ้าหากความคิดเห็นส่วนตัวของเราเกี่ยวกับการแบ่งปันข้อมูลนี้จะเปลี่ยนแปลงไปตามบริบทหรือไม่ อย่างไร

หัวข้อที่ 2

ความเป็นส่วนตัว และตัวเรา



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.



กิจกรรม

เกมลองทาย

- มีข้อมูลบางส่วนที่เราไม่เปิดเผยกับใครหรือไม่? เรื่องใด? และเพราะเหตุใด ?
- ทุกคนเลือกตัดสินใจเหมือนกันหรือไม่ว่าจะเปิดเผยเรื่องอะไร เพราะเหตุใดจึงเป็นเช่นนั้น? เพราะเหตุใดจึงไม่เป็นเช่นนั้น?
- เพราะเหตุใดเราจึงไม่แชร์ข้อมูลประเภทนี้ให้มากหรือน้อยกว่านี้ เราจะแชร์ข้อมูลในกรณีใด ทั้งนี้ ขึ้นอยู่กับว่าเราแชร์ข้อมูลกับใคร



กิจกรรม

เกมลองทาย

- การเชื่อมโยงข้อมูลแต่ละส่วนกับบุคคลที่เขียน/พูดนั้นง่ายแค่ไหน
- มีกรณีใดหรือไม่ ที่คำตอบที่กำหนดไว้อาจสื่อถึงบางสิ่งที่อยู่นอกเหนือคำตอบจริง
- เราคิดว่าคนอื่นอาจตั้งสมมติฐานอะไรเกี่ยวกับตัวเราหรือไม่ ถ้าเราแชร์ข้อมูลที่เขียนไว้เป็นส่วนหนึ่งของเกมลองทาย



เราจะแบ่งปันข้อมูลหรือ ไม่ว่าอาศัยอยู่ที่ใด

ผู้ปกครอง ผู้คุ้มครอง หรือผู้ใหญ่ที่สำคัญใน
ครอบครัว

เพื่อน

คุณครู

คนแปลกหน้า คนที่ไม่ได้รู้จักดี

เพื่อนของเพื่อน

องค์กรหรือบริษัท

การสื่อสารโดยการส่งข้อความ:
แตกต่างจากการสื่อสาร
กันแบบพบหน้าหรือไม่



เราจะจัดการความเป็นส่วนตัวและ ชื่อเสียงในโลกออนไลน์ของเรา อย่างไร



รู้หรือไม่ว่าการตั้งค่าความเป็น
ส่วนตัวในปัจจุบันของเราเป็น
อย่างไรในแต่ละแพลตฟอร์ม
โซเชียลมีเดีย





กิจกรรม

- ▶ การตั้งค่านโยบายโดยรวมของเราเป็นสาธารณะส่วนตัว หรืออย่างอื่นหรือไม่
- ▶ เราตัดสินใจอย่างไรในการตั้งค่าแบบนั้น
- ▶ การตั้งค่านโยบายในปัจจุบันของเราเป็นแบบที่เราต้องการหรือไม่





กิจกรรม

- ▶ เมื่อใดที่การแชร์แบบสาธารณะมีความเหมาะสม และเมื่อใดที่การตั้งค่าส่วนตัวอาจเป็นที่ต้องการมากกว่า
- ▶ รู้สึกสะดวกใจหรือไม่ที่ต้องแชร์ข้อมูลบนโซเชียลมีเดียที่เราใช้ หรือบริษัทที่โฆษณาบนโซเชียลมีเดียเหล่านี้
- ▶ การสนทนาในเรื่องนี้ทำให้เรามีความคิดเห็นที่แตกต่างเกี่ยวกับการตั้งค่าความเป็นส่วนตัวหรือไม่





กิจกรรม

สถานการณ์ที่

#1

อรนภา อายุ 13 ปี และเธอชอบร้องเพลง

เธอรู้สึกว่าเธอยังไม่เก่งมากพอในเรื่องนี้ แต่เธอต้องการแชร์ความชอบของเธอ กับเพื่อน ๆ และรับความคิดเห็นจากพวกเขา เธอกำลังพิจารณาที่จะเพิ่มวิดีโอที่ เธอร้องเพลงโปรดของเธอบน โซเชียลมีเดีย

- เราจะแนะนำแพลตฟอร์มประเภทใด
- เราคิดว่าการตั้งค่าความเป็นส่วนตัวที่ดีที่สุดที่ควรจะเป็นแบบใดสำหรับ แพลตฟอร์มนั้น
- **โปรดอธิบายเหตุผล**



กิจกรรม

สถานการณ์ที่

#2

เก่ง อายุ 16 ปี และเขาหลงใหลในการทำอาหารและสร้างสูตรอาหารใหม่ ๆ

เขาเคยทำงานเกี่ยวกับเมนูไก่หลายเมนูซึ่งเขารู้สึกตื่นเต้นมาก และเขาชอบที่จะแชร์ส่วนผสมและวิธีที่พวกเขาเตรียมกับเพื่อน ๆ ของเขาและคนอื่น ๆ ที่สนใจในการทำอาหาร

- เราจะแนะนำแพลตฟอร์มประเภทใด
- เราคิดว่าการตั้งค่าความเป็นส่วนตัวที่ดีที่สุดควรจะเป็นแบบใดสำหรับแพลตฟอร์มนั้น
- **โปรดอธิบายเหตุผล** และอธิบายว่าความคิดเห็นส่วนตัวในการแชร์ข้อมูลนี้จะเปลี่ยนแปลงไปตามบริบทหรือไม่/หรือจะเปลี่ยนแปลงไปอย่างไร



กิจกรรม

สถานการณ์ที่

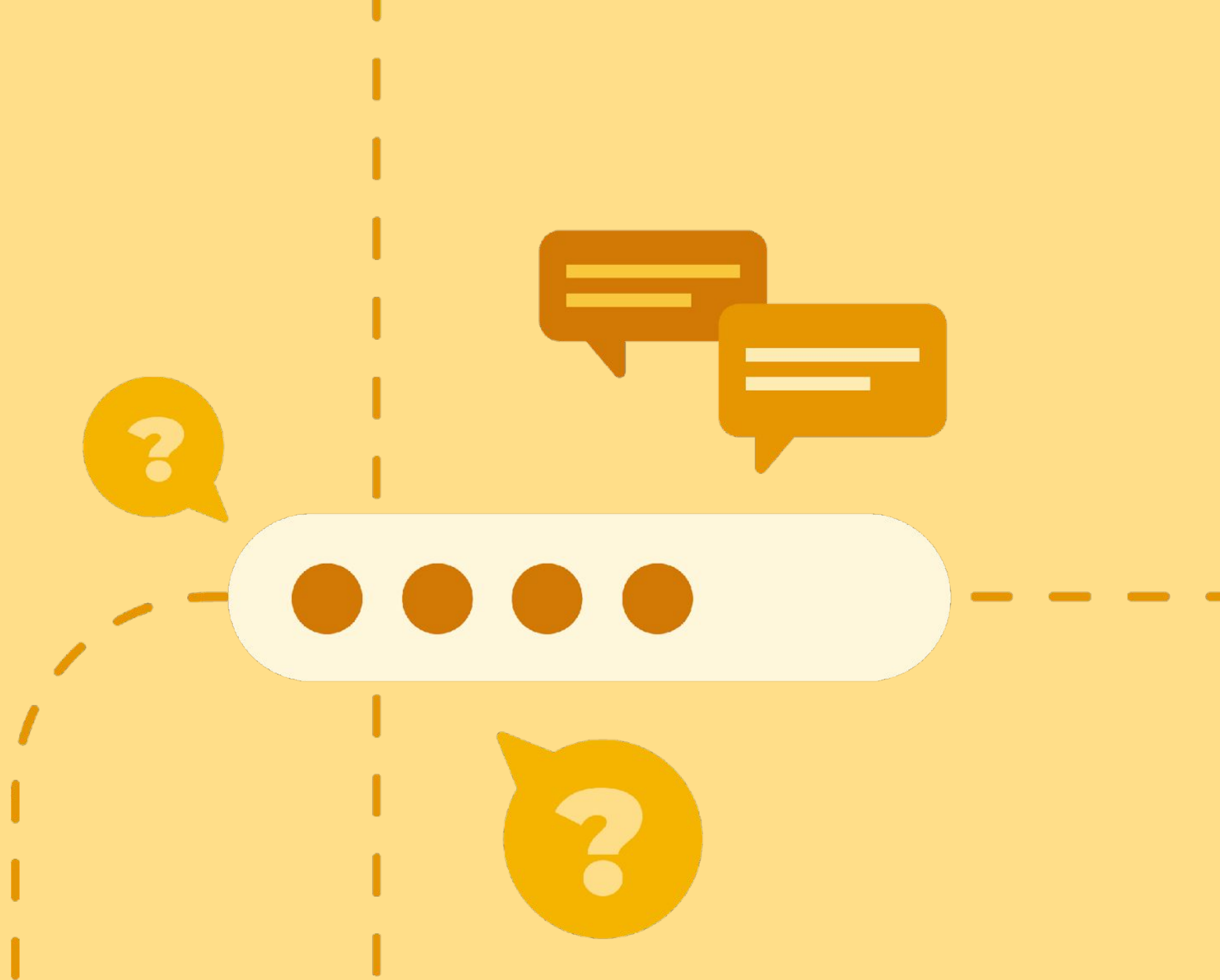
#3

ปวีณา อายุ 18 ปี และกำลังมองหางานที่จะทำในเดือนหน้า

เธอรักคอมพิวเตอร์และต้องการงานในแผนกไอที อย่างไรก็ตาม เธอไม่รู้ว่ามีงานอะไรบ้างที่เหมาะสมกับเธอ เธอทราบดีว่านายจ้างต้องการดูประวัติย่อ แต่เธอไม่รู้ว่าจะเขียนประวัติย่ออย่างไรให้มีประสิทธิภาพ เธอต้องการพบกับผู้คนที่มีความคล้ายคลึงกัน เพื่อที่เธอจะได้ขอคำแนะนำและการชี้แนะเกี่ยวกับวิธีการดำเนินการ

- โซเชียลมีเดียประเภทไหนที่เราจะแนะนำให้ยูนา
- เราคิดว่าการตั้งค่าความเป็นส่วนตัวแบบไหนที่เหมาะสมสำหรับแพลตฟอร์มนั้น เพื่อให้เธอสามารถบรรลุเป้าหมายของเธอได้
- **โปรดอธิบายสาเหตุ**

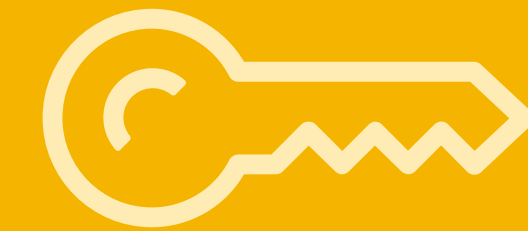
รหัสผ่าน



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.

มาคุยกันเกี่ยวกับรหัสผ่าน!

คำเตือน: สำคัญมาก! ไม่ควรเปิดเผยรหัสผ่านจริงของเราในระหว่าง
แบบฝึกหัดนี้หรือแบบฝึกหัดอื่น ๆ



กิจกรรมในชั้นเรียน

จะเกิดอะไรขึ้นหากมีคนต้องการ
จะสร้างปัญหา แล้วเขาคอนนั้นรหัส
ผ่านในการเข้าถึง
บัญชีโซเชียลมีเดียของเรา

จะเกิดอะไรขึ้นหากแฮกเกอร์รู้รหัส
ผ่านที่เข้าถึงบัญชีธนาคารผ่านช่อง
ทางออนไลน์ของผู้ปกครอง/ผู้
คุ้มครองของเรา

แฮกเกอร์เข้าถึงรหัสผ่านส่วนตัว ได้อย่างไร

รหัสผ่าน



รหัสผ่านที่รัดกุมคืออะไร



รหัสผ่านที่คาดเดาได้ง่ายคืออะไร

สร้างรหัสผ่านที่รัดกุมได้อย่างไร: เคล็ดลับการตั้งรหัสผ่าน

- ▶ มีตัวเลขอย่างน้อย 1 ตัว
- ▶ มีสัญลักษณ์อย่างน้อย 1 ตัว
- ▶ มีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็กอย่างน้อย 1 ตัว
- ▶ รหัสผ่านต้องมีอย่างน้อย 7 ตัวอักษร
- ▶ รหัสผ่านควรจำง่าย (เว้นแต่จะใช้ตัวจัดการรหัสผ่าน)
- ▶ ตัวจัดการรหัสผ่านคือ เว็บไซต์/แอปพลิเคชันที่ช่วยให้ผู้ใช้บันทึกและจัดระเบียบรหัสผ่านของตน
- ▶ รหัสผ่านไม่ควรเป็นคำทั่วไปหรือข้อมูลส่วนบุคคล (วันเกิด ชื่อผู้ปกครอง ฯลฯ)
- ▶ รหัสผ่านจะต้องไม่มีการแชร์ระหว่างเว็บไซต์

สร้างรหัสผ่านที่รัดกุมอย่างไร: ความยาวของรหัสผ่าน

เชื่อมต่อชุดคำที่ไม่เกี่ยวข้องกัน 4 คำ หรือมากกว่านั้นที่ทำให้เดาได้ยากขึ้น



26cheese + horse + train + table! = **26cheesehorsetrainable!**



กิจกรรม

สร้างรหัสผ่านโดยการใช้ “เคล็ดลับการตั้งรหัสผ่าน”

- ▶ มีตัวเลขอย่างน้อย 1 ตัว
- ▶ มีสัญลักษณ์อย่างน้อย 1 ตัว
- ▶ มีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็กอย่างน้อย 1 ตัว
- ▶ รหัสผ่านต้องมีอย่างน้อย 7 ตัวอักษร
- ▶ รหัสผ่านควรจำง่าย (เว้นแต่จะใช้ตัวจัดการรหัสผ่าน)
- ▶ ตัวจัดการรหัสผ่านคือ เว็บไซต์/แอปพลิเคชันช่วยให้ผู้ใช้บันทึกและจัดระเบียบรหัสผ่านของตน
- ▶ รหัสผ่านไม่ควรเป็นคำทั่วไปหรือข้อมูลส่วนบุคคล (วันเกิด ชื่อ ผู้ปกครอง ฯลฯ)
- ▶ รหัสผ่านจะต้องไม่มีการแชร์ระหว่างเว็บไซต์



กิจกรรม

สร้างรหัสผ่านโดยใช้: ความยาวของรหัสผ่าน

เชื่อมต่อชุดคำ 4 คำ หรือมากกว่านั้นที่ไม่เกี่ยวข้องกันที่ทำให้เดาได้ยากขึ้น



26cheese + horse + train + table! = **26cheesehorsetrainatable!**



การรับรองความถูกต้อง โดยใช้หลายปัจจัย (หรือ 2 ปัจจัย)



วิธีอื่นที่รหัสผ่านของเราอาจเดาได้ง่าย



การใช้รหัสผ่านซ้ำสำหรับหลายบัญชี



ใช้รหัสผ่านเดิมซ้ำมาหลายปี



ใช้รหัสผ่านที่มีข้อมูลส่วนบุคคล

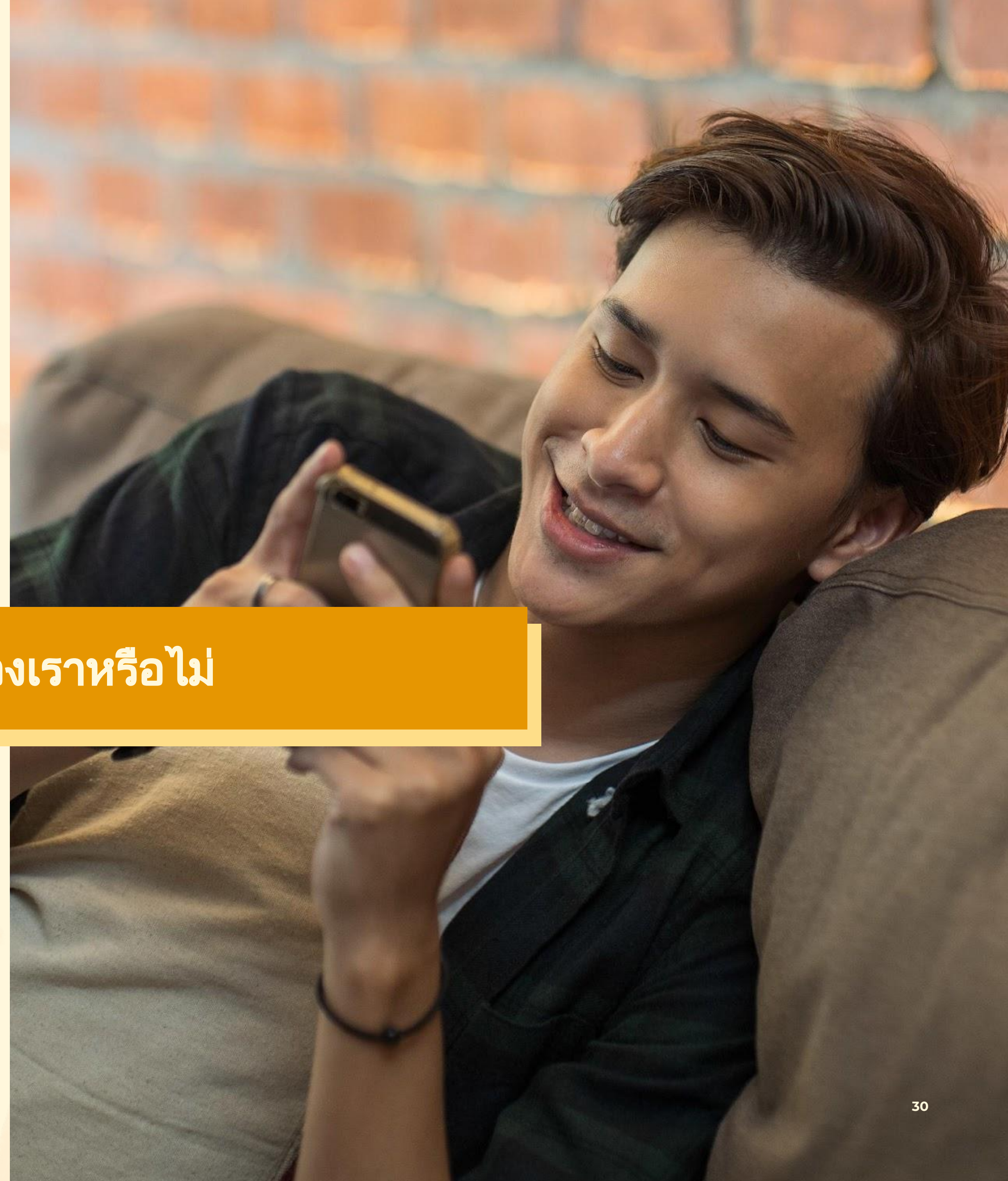


ลืมหรหัสผ่าน



เราใช้การจัดการรหัสผ่านหรือไม่

เราใช้ฟีเจอร์ “การบันทึกรหัสผ่าน” ในเบราว์เซอร์ของเราหรือไม่





การแบ่งปันรหัสผ่าน:
**เราเคยแชร์รหัสผ่านกับ
คนอื่นหรือไม่**

เคยมีกรณีใดหรือไม่ที่การแชร์รหัส
ผ่านเป็นเรื่องสามารถทำได้

เราแชร์รหัสผ่านกับใครหรือไม่

หากเราเป็นเพื่อนสนิทกับใครสักคน
พวกเขาจะพูดว่า “ถ้าเธอเห็นแกฉัน
...” สิ่งนี้อาจจะเป็นแรงจูงใจให้เรา
แชร์รหัสผ่านหรือไม่

การแฮกทางสังคม/ วิศวกรรมสังคม

ถ้ามีใครรู้ข้อมูลส่วนตัวของผู้เรียนมากพอ
เขาอาจเดารหัสผ่านของเราได้



กิจกรรม

เรียนรู้เกี่ยวกับรหัสผ่าน

1

อะไรคือข้อมูลเชิงลึกสามประการจากบทเรียนนี้
ที่เราจะนำไปใช้ในการสร้างรหัสผ่านครั้งต่อไป

3

กลยุทธ์สามประการที่เราสามารถใช้แชร์รหัส
ผ่านของเรากับผู้อื่นได้อย่างปลอดภัยมีอะไร
บ้าง

2

ยกตัวอย่างที่เราารู้สึกว่าสามารถแชร์รหัสผ่าน
ของเรากับคนอื่นได้



4

ยกตัวอย่างสามตัวอย่างที่อาจผิดพลาดหาก
รหัสผ่านตกไปอยู่ในมือของผู้อื่น

วิธีการยืนยันตัวตนแบบ 2 ขั้นตอนบน Facebook

- ▶ ไปที่การตั้งค่าความปลอดภัยและการเข้าสู่ระบบ โดยคลิก ที่มุมบนขวาของ Facebook แล้วคลิก การตั้งค่า > ความปลอดภัยและการเข้าสู่ระบบ
- ▶ เลื่อนลงไปที่ การยืนยันตัวตนแบบ 2 ขั้นตอน แล้วคลิกแก้ไข
- ▶ เลือกวิธีการรับรองความถูกต้องที่ต้องการเพิ่มและทำตามคำแนะนำบนหน้าจอ
- ▶ คลิกเปิดใช้เมื่อเราเลือกและเปิดวิธีการรับรองความถูกต้อง

วิธีการยืนยันตัวตนแบบ 2 ขั้นตอนบน Instagram

- ▶ กด  หรือกดไปที่รูปโปรไฟล์ในมุมล่างขวาของโปรไฟล์เรา
- ▶ กด  ที่ด้านบนขวา แล้วแตะการตั้งค่า
- ▶ กดไปที่ความปลอดภัย จากนั้นกดการยืนยันตัวตนแบบ 2 ขั้นตอน
- ▶ กดเริ่มต้นที่ด้านล่าง
- ▶ เลือกวิธีการรักษาความปลอดภัยที่เราต้องการเพิ่มและทำตามคำแนะนำด้านบนหน้าจอ

วิธีใช้การยืนยันตัวตนแบบ 2 ขั้นตอนบน WhatsApp

- ▶ เปิดการตั้งค่าใน WhatsApp
- ▶ กดที่บัญชี > การยืนยันตัวตนแบบ 2 ขั้นตอน > เปิดใช้งาน
- ▶ ป้อน PIN หกหลักที่เราเลือกและยืนยัน.
- ▶ ระบุอีเมลที่เราสามารถเข้าถึงได้ หรือแตะข้าม หากเราไม่ต้องการเพิ่มอีเมล
- ▶ กด ถัดไป
- ▶ ยืนยันอีเมลแล้วกดบันทึกหรือเสร็จสิ้น

หมายเหตุ: แนะนำให้เพิ่มที่อยู่อีเมล เนื่องจากจะทำให้เราสามารถรีเซ็ตการยืนยันตัวตนแบบ 2 ขั้นตอนได้และช่วยปกป้องบัญชีของเรา

Wi-Fi

สาธารณะ



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.

เราสามารถเชื่อมต่ออินเทอร์เน็ตได้อย่างไร



แล็ปท็อปและโทรศัพท์เชื่อมต่อกับอินเทอร์เน็ตได้อย่างไร



จุดเชื่อมต่อ

จุดเชื่อมต่อคือสิ่งที่ส่งสัญญาณ Wi-Fi และให้เข้าถึงอินเทอร์เน็ต



เราเตอร์ไร้สาย AP

เราเตอร์คือ อุปกรณ์ที่สร้างเครือข่ายระหว่างอุปกรณ์ทั้งหมดในตำแหน่งที่กำหนด



โมเด็ม

โมเด็มเป็นอุปกรณ์ที่สร้างและรักษาการเชื่อมต่อกับผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อให้เราเข้าถึงอินเทอร์เน็ตได้



ประโยชน์ของ Wi-Fi คืออะไร

ข้อเสียของ Wi-Fi คืออะไร

เราคิดว่ามีข้อกังวลด้านความปลอดภัยใดหรือไม่ เมื่อใช้ Wi-Fi กับการเชื่อมต่ออินเทอร์เน็ตแบบมีสาย เพราะเหตุใด

เพราะเหตุใดสัญญาณ Wi-Fi จึงขาดหายเมื่อเราออกจาก บ้านหรือตึกบริเวณที่มี Wi-Fi



เครือข่าย Wi-Fi ปลอดภัยทุกเครือข่ายหรือไม่



3 มาตรการทั่วไปที่ใช้ใน การเข้ารหัสสำหรับเครือข่าย ข่าย Wi-Fi

การเข้ารหัสแบบ WEP (Wired
Equivalent Privacy)

การเข้ารหัสแบบ WPA (Wi-Fi
Protected Access)

การเข้ารหัสแบบ WPA2 (Wi-Fi
Protected Access 2)

การเข้ารหัส

การเข้ารหัสสร้างขึ้นเพื่อให้แฮกเกอร์ติดตามข้อมูลเราได้ยากขึ้น



เครื่องมือรักษาความปลอดภัย

HTTPS เป็นมาตรฐานที่เว็บไซต์ใช้เพื่อเข้ารหัสข้อมูลที่ส่งผ่านอินเทอร์เน็ต

ควรป้องกันเฉพาะข้อมูลที่ละเอียดอ่อน (เช่น รหัสผ่าน ข้อมูลบัตรเครดิต) บนหน้าเว็บที่มี HTTPS:// นำหน้า

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) เป็นชื่อของเทคโนโลยีที่ช่วยให้ HTTPS ปลอดภัย

เครื่องมือรักษาความปลอดภัย

ตัวบ่งชี้ความปลอดภัยของเบราว์เซอร์จะแสดงถึงข้อมูลของการรับรอง Extended Validation (EV) ด้วย ใบรับรอง EV มอบให้กับเว็บไซต์ที่ยืนยันตัวตนต่อผู้ออกใบรับรอง

การเชื่อมต่อไปยัง Wi-Fi

ควรคำนึงถึงสิ่งใดเมื่อเชื่อมต่อกับเครือข่ายใหม่

- ▶ ใครเป็นเจ้าของเครือข่าย Wi-Fi
- ▶ รู้จักคนเหล่านี้เป็นการส่วนตัวหรือไม่
- ▶ เชื่อคนเหล่านี้หรือไม่

เราควรจะเชื่อมต่อกับเครือข่าย Wi-Fi ที่เจ้าของเป็น **คนที่เรารู้จักและเชื่อถือได้**

เราควรทำสิ่งนี้บนเครือข่าย Wi-Fi (บ้าน/โรงเรียน/ร้านกาแฟ) ของเราหรือไม่



อ่านข่าวออนไลน์/บล็อก



ส่งหมายเลขบัตรเครดิต



เช็คอีเมลส่วนตัว



การเชื่อมต่อ อย่างปลอดภัย





กิจกรรม

วาดช่วงเวลาของวันทั่ว ๆ ไป
ทำเครื่องหมายเครือข่าย
Wi-Fi ที่เราเชื่อมต่อในแต่ละ
ช่วงเวลา

ระบุเครือข่ายได้หรือไม่

มีใครอื่นเชื่อมต่ออีกหรือไม่

ปลอดภัยมากน้อยแค่ไหน

โอกาสและความเสี่ยงคือ
อะไร

ความปลอดภัยทางไซเบอร์ (Cybersecurity) ฟิชชิ่ง (Phishing) และ สแปม (Spam)



Source: This content is hosted by Meta and currently includes learning drawn from youth and media at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons Attribution-ShareAlike 4.0 International license. You can make use of them, including copying and preparing derivative works, whether commercial or non-commercial, so long as you attribute Youth and Media as the original source and follow the other terms of the license, sharing any further works under the same terms.

เราใช้อินเทอร์เน็ตเมื่อใด

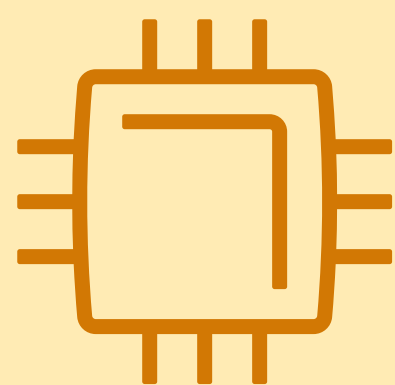
เราอาจมีความเสี่ยงเพียงแค่ว่าเราเข้าเว็บเพจ สื่อสารออนไลน์ หรือดาวน์โหลดข้อมูล

มันเป็นเรื่องที่สามารถเกิดขึ้นได้บนเว็บไซต์ที่เราเข้าถึง ผู้คนในเครือข่ายเดียวกัน หรือแม้กระทั่งกลุ่มบุคคลที่จะรู้ข้อมูลที่อยู่หรือข้อมูลอื่น ๆ ของเรา เมื่อเราทำการค้นหา



- เพราะเหตุใดแฮกเกอร์ที่ประสงค์ร้ายจึงพยายามเข้าถึงข้อมูลของเราทางออนไลน์
- เพราะเหตุใดเว็บไซต์ที่เราไม่ได้เข้าสู่ระบบต้องการติดตามว่าเราเป็นใคร
- ข้อมูลอะไรที่ผู้คนมองหา
- มีใครทราบหรือไม่ว่ามัลแวร์คืออะไร และมันทำอะไรได้บ้าง





มัลแวร์ คืออะไร

มัลแวร์ คือ รหัสอันตรายที่ทำงานบนคอมพิวเตอร์ของเรา มัลแวร์บางตัวสามารถรวบรวมข้อมูลจากคอมพิวเตอร์ของเราได้ นอกจากนี้ยังสามารถอนุญาตให้แฮกเกอร์ควบคุมคอมพิวเตอร์ของเราได้อีกด้วย

มัลแวร์ส่วนใหญ่นั้นธรรมดาอย่างมาก เช่น เว็บไซต์ที่เลียนแบบพอร์ทัลที่ปลอดภัย เช่น ธนาคาร หรือส่วนขยายที่วางโฆษณาในเบราว์เซอร์ของเราเพื่อสร้างรายได้



ความเสี่ยง ทางออนไลน์

โปรดระมัดระวังเมื่อคลิกลิงค์ โฆษณา หรือโพสต์บนโซเชียลมีเดีย

URL ตรงกับสิ่งที่เราจะเข้าหรือไม่

เราไปที่หน้าเดิมเมื่อพิมพ์ URL อีกครั้งด้วยตัวเองหรือค้นหาเว็บไซต์หรือไม่

กฎที่ดีคือ SSL/TLS ควรปกป้องหน้าการ
เข้าสู่ระบบสำหรับบัญชีที่สำคัญ (เช่น
Google, Facebook, Twitter หรือ
บัญชีธนาคาร) SSL/TLS ทำให้แฮกเกอร์
ในเครือข่ายเดียวกันส่งเว็บไซต์ปลอมให้
เราได้ยากมากขึ้น



เครื่องมือรักษาความปลอดภัย

ดาวน์โหลดหรือติดตั้งซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น และระมัดระวังเมื่อเราดาวน์โหลดไฟล์ปฏิบัติการ (.exe, .pkg, .sh, .dll หรือ .dmg)

เราสามารถใช้อซอฟต์แวร์ป้องกันไวรัสเพื่อป้องกันไม่ให้คอมพิวเตอร์ของเราเรียกใช้มัลแวร์

เราอาจพิจารณาถึงส่วนขยายของเบราว์เซอร์ที่สามารถบล็อกปลั๊กอินที่ทำให้เว็บไซต์ค้นหาว่าเราเป็นใครหรือติดตามเราได้ยากขึ้น



เราปลอดภัยเมื่อใช้อินเทอร์เน็ตหรือไม่



เราสามารถดำเนินการอะไรได้บ้างเพื่อป้องกันตัวเองจากการดาวน์โหลดไฟล์ที่เป็นอันตรายต่อคอมพิวเตอร์ของเราโดยไม่ตั้งใจ



การแชร์รหัสผ่าน

คิดว่าการแชร์รหัสผ่านเป็นสิ่งที่สมควรทำหรือไม่

มีความเสี่ยงอะไรบ้างที่อาจได้รับเมื่อเราแชร์รหัสผ่าน





กิจกรรม

สแปม (Spam)



จะสังเกตสแปมได้อย่างไร

บทเรียนที่ 2

WE THINK DIGITAL

พื้นฐานทางดิจิทัล



 Meta

We Think Digital