Wi-Fi สาธารณะ

ผู้เข้าร่วมจะได้เรียนรู้เกี่ยวกับเครือข่าย Wi-Fi สาธารณะ
รวมถึงประโยชน์และความเสี่ยงจากการใช้ Wi-Fi สาธารณะ
บทเรียนนี้จะมุ่งเน้นให้ผู้เข้าร่วมได้ศึกษาวิธีจำแนก Wi-Fi ที่ไม่ปลอดภัยเมื่อ Wi-Fi ประเภทนี้ปรากฏให้ใช้งาน ทำความเข้าใจสิ่งที่ต้องแลกซึ่งมาพร้อมกับการใช้งาน Wi-Fi ที่ไม่ปลอดภัย และทำการตัดสินใจหลังไตร่ตรองข้อมูลอย่างถี่ถ้วนว่าควรเชื่อมต่อและใช้งาน Wi-Fi ที่ไม่ปลอดภัยเมื่อใด

แหล่งข้อมูล

รูปโมเดมไร้สาย
ใบงานเกี่ยวกับความปลอดภัยในการเชื่อมต่อ

Wi-Fi คืออะไร

ส่วนที่หนึ่ง

ถามนักเรียนของคุณ

คุณใช้อุปกรณ์ใดเข้าถึงอินเทอร์เน็ต

อุปกรณ์เหล่านั้นเชื่อมต่อกับอินเทอร์เน็ตอย่างไร

การปฏิสัมพันธ์ในชั้นเรียนภาพลักษณ์

Wi-Fi เป็นวิธีการทั่วไปในการเชื่อมต่ออุปกรณ์กับอินเทอร์เน็ต Wi-Fi ใช้สัญญาณวิทยุในการเชื่อมต่อกับอุปกรณ์โดยไม่ต้องใช้การเชื่อมต่อทางกายภาพหรือการเชื่อมต่อผ่านสาย

ลองจินตนาการว่าคุณมีแล็ปท็อปสามเครื่องในบ้านที่คุณต้องการเชื่อมต่ออินเทอร์เน็ต
คุณจะต้องมีสิ่งต่อไปนี้เพื่อเชื่อมต่ออินเทอร์เน็ต

1. จุดเข้าใช้งานเครือข่ายไร้สาย (Access Point: AP):
จุดเข้าใช้งานเครือข่ายไร้สายคือสิ่งใดก็ตามที่ถ่ายทอดสัญญาณ (หรือแพร่สัญญาณ) Wi-Fi และมอบการเข้าถึงอินเทอร์เน็ต
อุปกรณ์ของคุณจะต้องหาสัญญาณเหล่านี้เพื่อเชื่อมต่ออินเทอร์เน็ต ในบางครั้ง
คุณอาจจำเป็นต้องได้รับสิทธิ์การอนุญาตพิเศษ (เช่น ชื่อผู้ใช้และรหัสผ่าน)
เพื่อลงชื่อเข้าใช้และใช้สัญญาณไร้สายที่จุดเข้าใช้งานเครือข่ายไร้สายแพร่ออกมา

2. เราเตอร์: เราเตอร์คืออุปกรณ์ที่สร้างเครือข่ายระหว่างอุปกรณ์ทั้งหมด (เช่น คอมพิวเตอร์ แท็บเล็ต โทรศัพท์มือถือ) ในตำแหน่งที่ตั้งหนึ่งๆ (เช่น โรงเรียน ห้องสมุด หรือบ้านของคุณ)
โดยปกติแล้วเราเตอร์จะมีจุดเข้าใช้งานเครือข่ายไร้สายติดตั้งมาในเครื่องอยู่แล้ว
(ดูแผนภาพด้านบน)

> เราเตอร์มีขอบเขตสัญญาณจำกัด (ซึ่งขอบเขตนี้มักจะแคบ)
> จึงเป็นเหตุผลที่ทำให้คุณได้รับสัญญาณ Wi-Fi
> ที่อ่อนหรือไม่ได้รับเลยหากอุปกรณ์อยู่ไกลจากเราเตอร์เกินไป นอกจากนี้
> หากมีอะไรคั่นระหว่างคุณและเราเตอร์ (เช่น อาคารหรือผนังอิฐ)
> สัญญาณก็จะอ่อนลงเช่นกัน
>
> ถึงแม้การเชื่อมต่อเราเตอร์จะช่วยให้คุณเข้าถึงเครือข่ายได้
> แต่ก็ไม่ได้หมายความว่าคุณจะเข้าถึงอินเทอร์เน็ตได้ เราเตอร์จะต้องเชื่อมต่อกับโมเด็มเพื่อให้อุปกรณ์หลายเครื่องบนเครือข่ายเชื่อมต่ออินเทอร์เน็ตได้

3. โมเด็ม: โมเด็มคืออุปกรณ์ที่สร้างและรักษาการเชื่อมต่อระหว่างคุณกับผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อช่วยให้คุณเข้าถึงอินเทอร์เน็ตได้ โมเด็มจะเปลี่ยนสัญญาณที่อยู่ภายนอกตำแหน่งที่ตั้งเป็นสัญญาณที่คอมพิวเตอร์และอุปกรณ์ดิจิทัลอื่นๆ ของคุณอ่านได้

> ในการตั้งค่าทั่วๆ ไป จุดเข้าใช้งานเครือข่ายไร้สายและเราเตอร์คืออุปกรณ์เครื่องเดียวกันที่

เชื่อมต่อกับโมเด็มทางกายภาพ โดยใช้สายพิเศษที่เรียกว่าสายอีเธอร์เน็ตในการเชื่อมต่อ การเชื่อมต่อแบบนี้คือการเชื่อมต่อที่เรียกว่าการเชื่อมต่ออินเทอร์เน็ต “ผ่านสาย”

อุปกรณ์มือถือสามารถใช้การเชื่อมต่อทางโทรศัพท์เพื่อเชื่อมต่ออินเทอร์เน็ตได้เช่นกัน โดยเฉพาะเมื่ออุปกรณ์ไม่ได้อยู่ในเครือข่ายของโรงเรียน ห้องสมุด หรือบ้าน การเชื่อมต่อทางโทรศัพท์เป็นสัญญาณวิทยุไร้สายประเภทหนึ่งที่มีพื้นที่ครอบคลุมสัญญาณกว้างกว่าเราเตอร์มาก การเชื่อมต่อทางโทรศัพท์ใช้เครื่องรับส่งเฉพาะที่เรียกว่าเสาสัญญาณเชื่อมต่ออุปกรณ์มือถือเข้ากับอินเทอร์เน็ต

ส่วนที่สอง

ถามนักเรียนของคุณ

ประโยชน์ของ Wi-Fi มีอะไรบ้าง

ข้อเสียของ Wi-Fi มีอะไรบ้าง

ข้อกังวลด้านความปลอดภัยที่อาจมีเมื่อใช้งาน Wi-Fi มีอะไรบ้าง
และข้อกังวลด้านความปลอดภัยที่อาจมีเมื่อใช้งานการเชื่อมต่ออินเทอร์เน็ตผ่านสายมีอะไรบ้าง

เหตุใดโทรศัพท์ของคุณจึงเสียการเข้าถึง Wi-Fi เมื่อคุณออกจากอาคาร

การเลือกเครือข่าย Wi-Fi

ส่วนที่หนึ่ง

ถามนักเรียนของคุณ

เครือข่าย Wi-Fi ทั้งหมดปลอดภัยหรือไม่ เพราะเหตุใดจึงเป็น/ไม่เป็นเช่นนั้น

บอกนักเรียนของคุณ

ในบางครั้ง คุณสามารถเลือกเครือข่าย Wi-Fi ที่ต้องการใช้ได้ คุณจำเป็นต้องระลึกไว้ว่าการเชื่อมต่อเครือข่ายที่ไม่เหมาะสมอาจทำให้คุณต้องเผชิญกับความเสี่ยงใหญ่หลวง ตัวอย่างเช่น เครือข่าย Wi-Fi ที่ไม่ปลอดภัยคือเครือข่ายที่ไม่จำเป็นต้องใช้รหัสผ่านในการเข้าสู่ระบบ หากคุณใช้งานเครือข่ายที่ไม่ปลอดภัย
เป็นไปได้ว่าผู้อื่นที่ใช้เครือข่ายเดียวกันจะเห็นข้อมูลของคุณได้
คนเหล่านั้นอาจขโมยข้อมูลที่คุณส่งผ่านเครือข่ายหรือคอยติดตามกิจกรรมทางออนไลน์ของคุณ

ในทางกลับกัน เครือข่าย Wi-Fi ที่ปลอดภัยและเชื่อถือได้คือเครือข่ายที่จำเป็นต้องใช้รหัสผ่านเปิดใช้การเข้ารหัส รวมถึงเครือข่ายที่คุณแน่ใจได้ว่าเป็นของเครือข่ายที่แสดงชื่ออยู่จริงๆ ตัวอย่างเช่น การลงชื่อเข้าใช้เครือข่ายที่แอบอ้างใช้ชื่อเครือข่ายโรงเรียนของคุณอาจทำให้ข้อมูลในบัญชีผู้ใช้ของคุณรั่วไหลได้ ดังนั้น
เครือข่ายที่ปลอดภัยและเชื่อถือได้จึงเป็นเครือข่ายที่มอบการคุ้มครองให้คุณมากที่สุด

สิ่งหนึ่งที่คุณควรพิจารณาก็คือบริบทหรือตำแหน่งที่ตั้งของเครือข่าย Wi-Fi ตัวอย่างเช่น หากคุณอยู่ที่โรงภาพยนตร์และคุณเห็นชื่อเครือข่ายของโรงเรียนบนโทรศัพท์เมื่อค้นหาการเชื่อมต่อ Wi-Fi คุณอาจสันนิษฐานว่าเครือข่ายดังกล่าวพยายามเลียนแบบหรือ “แกล้งปลอม” เป็นเครือข่ายของโรงเรียนเพื่อเก็บรหัสผ่านของนักเรียนที่ไม่ทันฉุกคิด

เมื่อตั้งค่าเครือข่าย Wi-Fi ที่ปกป้องด้วยรหัสผ่าน
เจ้าของเครือข่ายจะต้องเปิดโปรโตคอลการเข้ารหัสของเราเตอร์
โปรโตคอลการเข้ารหัสที่ใช้กันทั่วไปคือ Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) หรือ WPA2 โปรโตคอลเหล่านี้ทำหน้าที่เข้ารหัส (หรือ “ขยำรวม”) ข้อมูลที่ส่งผ่านเครือข่ายไร้สาย

การเข้ารหัสสร้างขึ้นเพื่อทำให้แฮ็กเกอร์เห็นข้อมูลที่คุณส่งได้ยากขึ้น อย่างไรก็ตาม
มีการพิสูจน์ให้เห็นแล้วว่าโปรโตคอลเหล่านี้ (WEP, WPA และ WPA2) ถูกแฮ็กได้ง่าย ดังนั้น
การใช้การเชื่อมต่อผ่านเว็บที่ปลอดภัยเมื่อส่งข้อมูลทางออนไลน์จึงเป็นสิ่งสำคัญเช่นกัน

HTTPS คือมาตรฐานที่เว็บไซต์ต่างๆ ใช้เข้ารหัสข้อมูลที่มีการรับส่งผ่านอินเทอร์เน็ต
การเข้ารหัสช่วยป้องกันไม่ให้บุคคลที่สามดูข้อมูลจากการเชื่อมต่อของคุณได้ง่ายนัก HTTPS มอบการรักษาความปลอดภัยอีกชั้นหนึ่งและสามารถนำไปใช้ในเบราว์เซอร์ใดก็ได้โดยการเพิ่ม “https://” หน้า URL ที่คุณใช้ (เช่น https://www.mysite.com) อย่างไรก็ตาม
บางเว็บไซต์ก็ไม่รองรับ HTTPS

1. คุณควรป้อนข้อมูลที่ละเอียดอ่อน (เช่น รหัสผ่านหรือข้อมูลบัตรเครดิต) บนเว็บเพจที่มี HTTPS:// นำหน้าเว็บเท่านั้น

2. เบราว์เซอร์หลักๆ ส่วนมากมีตัวชี้วัดความปลอดภัยหน้าตาเหมือนแม่กุญแจอยู่ใกล้กับแถบที่อยู่เพื่อระบุว่ามีการเชื่อมต่อ HTTPS

3. แต่น่าเสียดายที่ HTTPS ไม่อาจช่วยรับประกันว่าคุณจะปลอดภัย เนื่องจากเว็บไซต์อันตรายบางเว็บก็รองรับ HTTPS ได้เช่นกัน HTTPS ช่วยคุ้มครองการเชื่อมต่อ แต่ไม่ได้รับรองว่าเว็บไซต์นั้นเป็นเว็บไซต์ที่ดี

บอกนักเรียนของคุณ

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
คือชื่อของเทคโนโลยีที่ช่วยรักษาความปลอดภัยให้กับ HTTPS SSL/TLS
ใช้คีย์การเข้ารหัสดิจิทัลซึ่งทำหน้าที่เหมือนกุญแจจริงๆ มาก
หากคุณเขียนความลับของคุณใส่กระดาษเพื่อส่งให้เพื่อน
ทุกคนที่พบกระดาษแผ่นนี้ก็จะดูความลับของคุณได้ กลับกัน
ให้จินตนาการว่าคุณยื่นกุญแจสำรองให้เพื่อนเองกับมือ
จากนั้นจึงเอาความลับใส่กล่องปิดล็อกซึ่งเป็นคู่ของกุญแจที่เพื่อนของคุณมีแล้วจึงส่งให้เพื่อน
หากมีผู้ขัดขวางการส่งกล่อง
คนเหล่านั้นก็คงจะต้องลำบากกับการหาวิธีดูความลับของคุณโดยไม่มีกุญแจ
หากมีผู้พยายามเปลี่ยนกล่องดังกล่าวกับกล่องที่หน้าตาเหมือนกัน
คุณก็จะสังเกตได้ว่ากุญแจของคุณใช้กับกล่องนั้นไม่ได้ SSL/TLS ทำงานในรูปแบบเดียวกัน
แต่ทำงานกับเว็บไซต์

ตัวชี้วัดความปลอดภัยของเบราว์เซอร์จะทำหน้าที่สื่อสารใบรับรอง Extended Validation (EV) ด้วยเช่นกัน
เว็บไซต์ที่ตรวจสอบยืนยันตัวตนกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะได้รับใบรับรอง EV ในเบราว์เซอร์ บางครั้งตัวชี้วัด EV จะอยู่ในรูปแบบของชื่อเว็บไซต์หรือผู้จดทะเบียน
ซึ่งจะอยู่ข้างแถบที่อยู่ หากคุณสงสัยเนื้อหาบนเว็บไซต์บางเว็บ
คุณสามารถตรวจสอบได้โดยการดูว่า URL ในใบรับรองตรงกับ URL
ในเบราว์เซอร์หรือไม่โดยการคลิกที่ “ดูใบรับรอง” [การสาธิตวิธีหาส่วน “ดูใบรับรอง” ให้ผู้เข้าร่วมดูบนจอโปรเจคเตอร์อาจมีประโยชน์]
วิธีดูใบรับรองนี้จะแตกต่างกันไปตามเบราว์เซอร์ ตัวอย่างเช่น หากคุณใช้ Chrome ให้คลิก “ผู้พัฒนา” ในส่วน “ดู” จากนั้นจึงเลือก “เครื่องมือสำหรับผู้พัฒนา” จากส่วน “เครื่องมือสำหรับผู้พัฒนา” ให้คลิกแท็บ “ความปลอดภัย” จากนั้นคลิก “ดูใบรับรอง”

ถามนักเรียนของคุณ

คุณควรคำนึงถึงสิ่งใดเมื่อเชื่อมต่อกับเครือข่ายใหม่

1. คำตอบที่เป็นไปได้ ได้แก่ ตำแหน่งที่ตั้ง (หรือเจ้าของเครือข่าย) การเข้าถึง (หรือคนอื่นๆ ที่เชื่อมต่อกับเครือข่ายนั้น) และกิจกรรม (หรือสิ่งที่คุณกำลังทำบนเครือข่าย)

ใครเป็นเจ้าของเครือข่าย Wi-Fi ที่บ้านของคุณ แล้วที่โรงเรียนล่ะ ที่ร้านกาแฟล่ะ

1. พ่อแม่/ผู้ดูแลของคุณเป็นเจ้าของเครือข่าย Wi-Fi ที่บ้าน

ผู้ดูแลและ/หรือเขตนั้นเป็นเจ้าของเครือข่ายที่โรงเรียน
และเจ้าของร้านกาแฟเป็นเจ้าของเครือข่ายที่ร้านกาแฟ

คุณรู้จักคนเหล่านี้เป็นการส่วนตัวหรือไม่ คุณเชื่อถือบุคคลเหล่านี้หรือไม่

1. ให้ผู้เข้าร่วมสนทนากันว่าพวกเขาอาจเชื่อถือคนเหล่านี้ต่างกันไปอย่างไร

บอกนักเรียนของคุณ

คุณควรรู้จักและเชื่อถือบุคคลที่เป็นเจ้าของเครือข่าย Wi-Fi ในบางครั้ง
คุณสามารถตัดสินได้ว่าเจ้าของเครือข่ายใช้งาน SSID ของเครือข่ายหรือไม่

Service Set Identifier (SSID) คือชื่อของเครือข่าย Wi-Fi
และเป็นชื่อที่คุณเห็นเมื่อพยายามเชื่อมต่อ Wi-Fi มักมีการนำ SSID
ไปใช้เพื่อสื่อสารว่าใครเป็นเจ้าของเครือข่ายรวมถึงรายละเอียดอื่นๆ เกี่ยวกับเครือข่าย
ถึงกระนั้น คุณก็ควรระมัดระวังเนื่องจากแทบทุกคน (ที่รู้วิธี) สามารถสร้าง SSID ได้
ตัวอย่างเช่น ผู้ที่รู้วิธีสร้างสามารถสร้าง SSID ที่เหมือนกับ SSID
ที่คุณใช้ที่โรงเรียนทุกประการขึ้นมาได้ นี่คือตัวอย่างของการปลอมเป็นเครือข่ายที่รู้จักและเชื่อถือได้ซึ่งน่าจะทำไปเพื่อเก็บชื่อผู้ใช้และรหัสผ่าน

การทราบว่าใครเป็นเจ้าของเครือข่ายช่วยให้คุณตัดสินได้ว่าเครือข่ายนั้นปลอดภัยหรือไม่
หากเครือข่ายนั้นเป็นของบุคคลหรือองค์กรที่คุณเชื่อถือ
คุณก็มีแนวโน้มที่จะเชื่อมต่อได้อย่างสบายใจ อย่างไรก็ตาม
หากเครือข่ายดังกล่าวเป็นเครือข่ายที่ไม่รู้จัก คุณก็ไม่ควรเชื่อมต่อ
เนื่องจากคุณไม่รู้ว่าใครเป็นเจ้าของเราเตอร์ที่คุณเชื่อมต่ออยู่
เนื่องจากปริมาณการใช้งานที่เกิดขึ้นบนเครือข่ายทั้งหมดจะต้องผ่านเราเตอร์
จึงอาจเป็นไปได้ที่เจ้าของเราเตอร์จะติดตามหรือบันทึกทราฟฟิกบนเว็บของคุณอยู่

เมื่อคุณเชื่อมต่อ Wi-Fi อุปกรณ์ของคุณจะเชื่อมต่อกับเครือข่ายในเครื่องของอุปกรณ์
และเครือข่ายนั้นจะทำการเชื่อมต่อกับอินเทอร์เน็ตที่มีขอบเขตกว้างกว่า
เนื่องจากอุปกรณ์ของคุณแลกเปลี่ยนข้อมูลกับเครือข่ายนี้ การที่คุณสามารถเชื่อถืออุปกรณ์อื่นๆ
ที่คุณเชื่อมต่อด้วยได้จึงเป็นสิ่งสำคัญ
ซึ่งอุปกรณ์ที่คุณเชื่อมต่อด้วยนี้ก็คืออุปกรณ์ทั้งหมดบนเครือข่าย
เช่นเดียวกับงานกลุ่มที่คุณทำที่โรงเรียน คงจะดีกว่าถ้าคุณสามารถเชื่อใจคนอื่นๆ
ที่คุณทำงานด้วยได้!

การนำรหัสผ่านมาใช้กับเครือข่ายอาจช่วยจำกัดผู้ที่เชื่อมต่อกับเครือข่ายได้
ซึ่งจะช่วยให้คุณทราบได้ดีกว่าว่ามีใครบ้างที่กำลังใช้งานเครือข่าย ไม่ว่าจะเป็นคนในครอบครัว
เพื่อนๆ หรือลูกค้าคนอื่นๆ ในร้านกาแฟ
ซึ่งดีกว่าการที่เครือข่ายนั้นเปิดให้ทุกคนใช้งานได้แบบไม่มีข้อจำกัด
ซึ่งคุณแทบจะไม่ทราบเลยว่ามีใครใช้งานเครือข่ายอยู่บ้าง

ไม่ว่าคุณจะตัดสินใจเข้าร่วมเครือข่ายที่อาจดูน่าสงสัยหรือไม่
การแลกเปลี่ยนที่คุณเต็มใจในแง่ของความปลอดภัยทางออนไลน์ก็เป็นสิ่งที่ต้องพูดถึง
คุณอาจลองพิจารณาว่า “ฉันควรชั่งน้ำหนักระหว่างโอกาสที่ข้อมูลในบัญชีผู้ใช้ของฉันจะรั่วไห

ลกับความสะดวกสบายที่ได้จากการเข้าร่วมเครือข่ายที่มีให้ใช้งานอย่างไร”

ถามนักเรียนของคุณ

คุณควรอ่านข่าว/บล็อกออนไลน์โดยใช้เครือข่าย Wi-Fi ที่บ้านหรือไม่ แล้วที่โรงเรียนล่ะ ที่ร้านกาแฟล่ะ

1. อธิบายว่าเนื้อหาในหน้าเว็บส่วนใหญ่แล้วไม่ใช่ข้อมูลที่ละเอียดอ่อน คุณอาจทำสิ่งนี้บนเครือข่ายใดก็ได้

คุณควรส่งหมายเลขบัตรเครดิตผ่านเครือข่าย Wi-Fi ที่บ้านหรือไม่ แล้วที่โรงเรียนล่ะ ที่ร้านกาแฟล่ะ เหตุใดคุณจึงไม่แชร์

1. ให้ผู้เข้าร่วมสนทนากันเกี่ยวกับเหตุผลที่ทำให้การส่งหมายเลขบัตรเครดิตผ่าน Wi-Fi ที่บ้านของตนปลอดภัยที่สุด และเหตุผลที่ทำให้การส่งผ่าน Wi-Fi ของร้านกาแฟไม่ปลอดภัย นอกจากนี้ ให้หารือเกี่ยวกับเหตุผลที่ทำให้ไม่ควรใช้เครือข่ายของโรงเรียนในการส่งข้อมูลนี้แม้เครือข่ายของโรงเรียนจะค่อนข้างเชื่อถือได้ก็ตาม เนื่องจากข้อมูลนี้มีความละเอียดอ่อนมาก

คุณควรตรวจสอบอีเมลส่วนตัวโดยใช้เครือข่าย Wi-Fi ที่บ้านหรือไม่ แล้วที่โรงเรียนล่ะ ที่ร้านกาแฟล่ะ

1. หารือกันว่าเหตุใดการตรวจสอบอีเมลส่วนตัวโดยใช้เครือข่ายที่บ้านจึงน่าจะปลอดภัยที่สุด ทั้งนี้ขึ้นอยู่กับเนื้อหาของบัญชีผู้ใช้อีเมลด้วย ตัวอย่างเช่น บางคนอาจมีบัญชีผู้ใช้อีเมลหลายบัญชีสำหรับวัตถุประสงค์ต่างๆ (เช่น บัญชีหนึ่งเอาไว้รับอีเมลทางการตลาด/อีเมลส่งเสริมการขาย อีกบัญชีหนึ่งมีไว้ส่งอีเมลติดต่อกับเพื่อนและครอบครัว)

บอกนักเรียนของคุณ

คุณควรส่ง/ดูข้อมูลที่ละเอียดอ่อนรวมถึงรหัสผ่านและข้อมูลธนาคารบนเครือข่ายที่เป็นส่วนตัวและปลอดภัย โดยใช้เว็บไซต์ที่ใช้ SSL/TLS แทนที่จะใช้เครือข่ายสาธารณะที่ใช้ร่วมกัน อาจเกิดอันตรายกับข้อมูลส่วนตัวนี้หากคุณส่งหรือเข้าถึงข้อมูลขณะอยู่บนเครือข่ายร่วมซึ่งมีผู้ที่คุณไม่รู้จักหรือเชื่อใจไม่ได้ใช้งานอยู่

นิยามของคำว่าข้อมูลที่ละเอียดอ่อนอาจจะไม่ชัดเจนเนื่องจากความเป็นส่วนตัวนั้นเป็นการตัดสินใจส่วนตัวที่คุณจะต้องตัดสินด้วยตัวเอง
การพิจารณาแต่ละสถานการณ์เพื่อตัดสินว่าคุณควรเชื่อมต่อกับเครือข่ายหรือไม่เป็นสิ่งสำคัญ ลองถามตัวเองก่อนตัดสินใจว่าจะเชื่อมต่อหรือไม่เชื่อมต่อว่าคุณเชื่อใจเจ้าของเครือข่ายและคนอื่นๆ ที่เชื่อมต่อกับเครือข่ายหรือไม่ กิจกรรมใดที่คุณทำทางออนไลน์ และข้อมูลใดที่คุณแชร์

เครือข่ายที่ปลอดภัยและไม่ปลอดภัย

ส่วนที่หนึ่ง

ปฏิสัมพันธ์ในชั้นเรียน

โปรดทราบว่า: ส่วนหนึ่งของเนื้อหาในกิจกรรมนี้ครอบคลุมอยู่แล้วใน “กิจกรรมที่ 2: การเลือกเครือข่าย Wi-Fi”
คุณสามารถตัดสินใจได้ว่าจะเรียนรู้เนื้อหานี้อีกครั้งหรือข้ามเนื้อหานี้ไป

บอกนักเรียนของคุณ

ตามที่ได้พูดถึงไปก่อนหน้านี้ เครือข่าย Wi-Fi
ที่ไม่ปลอดภัยคือเครือข่ายที่ไม่จำเป็นต้องใช้รหัสผ่านในการเข้าสู่ระบบ
การใช้เครือข่ายที่ไม่ปลอดภัยทำให้ข้อมูลที่คุณส่งและรับผ่านเครือข่ายตกอยู่ในอันตราย

เครือข่าย Wi-Fi ที่ปลอดภัยคือเครือข่ายที่จำเป็นต้องใช้รหัสผ่านและเปิดใช้งานการเข้ารหัส
ผู้กำหนดค่าเครือข่ายคือผู้ที่เลือกว่าจะเปิดการเข้ารหัสหรือไม่ การเข้ารหัสจะรวมข้อมูลต่างๆ
ที่คุณส่งและรับผ่านเครือข่ายเข้าด้วยกัน จึงทำให้แฮ็กเกอร์ที่ใช้เครือข่าย Wi-Fi
เดียวกันดูข้อมูลที่คุณส่งหรือรับได้ยากขึ้นมาก

การที่เครือข่ายนั้นเป็นเครือข่ายที่ปลอดภัยไม่ได้หมายความว่าข้อมูลของคุณจะปลอดภัย
แน่นอนว่าการรับส่งข้อมูลผ่านเครือข่ายที่ปลอดภัยย่อมปลอดภัยกว่า
แต่แฮ็กเกอร์ที่ตั้งใจขโมยข้อมูลจริงๆ ก็อาจหาวิธีเข้าถึงข้อมูลของคุณจนได้

โปรโตคอลการเข้ารหัสสำหรับเครือข่าย Wi-Fi ที่ใช้กันทั่วไปมีอยู่สามประเภท ได้แก่ Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) หรือ WPA2 WEP และ WPA
นั้นล้าสมัยแล้วและคุณควรถือว่าเครือข่ายที่ใช้โปรโตคอลทั้งสองเป็นเครือข่ายที่ไม่ปลอดภัย
นอกจากนี้ WPA2 ยังได้รับการพิสูจน์แล้วว่าถูกแฮ็กได้ง่าย

เพื่อให้แน่ใจว่าข้อมูลของคุณได้รับการปกป้องอย่างเต็มที่
ให้ตรวจสอบว่าเว็บไซต์ที่คุณใช้เข้ารหัสโดยใช้ SSL/TLS หรือไม่

ถามนักเรียนของคุณ

มีใครยกตัวอย่างเครือข่ายที่ปกป้องด้วยรหัสผ่านที่เคยใช้ได้บ้าง

1. ตัวอย่างเช่น Wi-Fi ที่บ้าน, Wi-Fi ของโรงเรียน และเครือข่าย Wi-Fi ในสถานที่สาธารณะบางที่ เช่น ร้านกาแฟ

มีใครยกตัวอย่างเครือข่ายที่ไม่ปลอดภัยที่เคยใช้ได้บ้าง

แล้วตัวอย่างของเครือข่ายที่ปลอดภัยล่ะ

บอกนักเรียนของคุณ

คุณสามารถตรวจสอบว่าเครือข่าย Wi-Fi ได้รับการเข้ารหัสหรือไม่โดยการตรวจสอบการตั้งค่าเ
ครือข่ายหรือเครือข่ายไร้สายบนอุปกรณ์ของคุณ

ส่วนที่สอง

ปฏิสัมพันธ์ในชั้นเรียน

ก่อนเข้าสู่การเรียนรู้นี้
ให้ทำการค้นหาบนอินเทอร์เน็ตเพื่อดูวิธีตรวจสอบประเภทการเข้ารหัสของเครือข่าย Wi-Fi
สำหรับระบบปฏิบัติการประเภทต่างๆ จากนั้น ให้สาธิตวิธีหาประเภทการเข้ารหัสที่เครือข่ายใช้
ตัวอย่างเช่น สำหรับระบบปฏิบัติการ MacOS ให้คลิกที่ “การกำหนดลักษณะของระบบ” ->
“เครือข่าย -> “เลือก Wi-Fi” -> เลือกชื่อเครือข่ายที่เหมาะสม ในแท็บ Wi-Fi
จะมีรายชื่อเครือข่ายที่รู้จักและคอลัมน์ที่ระบุประเภทการเข้ารหัสที่ใช้

บอกนักเรียนของคุณ

ใช่ว่าการเชื่อมต่อทั้งหมดจะเท่าเทียมกัน
เครือข่ายที่ไม่ปลอดภัยจะอนุญาตให้ทุกคนเชื่อมต่อเครือข่ายได้
และคุณจะไม่ทราบชัดว่าใครเป็นผู้ควบคุมเครือข่าย
การเข้าร่วมเครือข่ายที่ไม่ปลอดภัยจะทำให้คุณถูกขโมยข้อมูลได้ง่าย
เนื่องจากใครก็ตามที่อยู่บนเครือข่ายอาจดูข้อมูลที่คุณส่งและรับ เช่น ทราฟฟิกบนเว็บ
(หน้าเว็บต่างๆ, รหัสผ่าน ฯลฯ) ได้หากคุณไม่ใช้การเชื่อมต่อ SSL/TLS

ปฏิสัมพันธ์ในชั้นเรียน

คุณอาจพิจารณาการพูดคุยเกี่ยวกับการใช้เครือข่าย VPN
เพื่อเพิ่มการรักษาความปลอดภัยอีกชั้นหนึ่งเมื่อใช้งาน Wi-Fi
ทั้งนี้ขึ้นอยู่กับความรู้ทางเทคนิคของผู้เข้าร่วม โปรดอ้างอิงจากลิงก์ VPN ในส่วน “แหล่งข้อมูล”
หากต้องการข้อมูลเพิ่มเติม

การตระหนักถึงความปลอดภัยในการเชื่อมต่อ

ชื่อส่วน

ปฏิสัมพันธ์ในชั้นเรียน

แบ่งผู้เข้าร่วมออกเป็นกลุ่ม กลุ่มละ 2-3 คน
แจกเอกสารประกอบเกี่ยวกับความปลอดภัยในการเชื่อมต่อ:
แจกใบงานสำหรับผู้เข้าร่วมและมอบหมายสถานการณ์ให้กับแต่ละกลุ่ม
ให้เวลาผู้เข้าร่วมหารือกันเกี่ยวกับสถานการณ์ที่ได้รับมอบหมาย 5 นาที
จากนั้นจึงให้แต่ละกลุ่มแชร์คำตอบ คำตอบคือตัวอักษรสีเขียวที่อยู่บนใบงาน

งาน

ส่วนที่หนึ่ง

งาน

ขอให้ผู้เข้าร่วม:

1. เขียนไทม์ไลน์ของวันธรรมดาๆ หนึ่งวันและเขียนชื่อเครือข่าย Wi-Fi ที่ตนเชื่อมต่อ

2. จากเครือข่ายที่แสดงในไทม์ไลน์
   ให้ผู้เข้าร่วมเลือกเครือข่ายมาสองเครือข่ายแล้วเขียนย่อหน้าสั้นๆ สำหรับแต่ละเครือข่าย
   โดยอธิบายถึงคนอื่นที่เชื่อมต่อกับเครือข่ายนั้น เครือข่ายนั้นปลอดภัยแค่ไหน

3. นอกจากนี้
   ให้ผู้เข้าร่วมอธิบายโอกาสและความเสี่ยงที่อาจเกิดขึ้นจากการเชื่อมต่อเครือข่ายทั้งสอง