เคล็ดลับสำหรับ การใช้ Wi-Fi สาธารณะอย่างปลอดภัย

คนร้ายสามารถฉวยโอกาสกับคุณทางออนไลน์ได้ อ่านบทความด้านล่างสำหรับเคล็ดลับบางประการในการพิจารณาเมื่อคุณต้องใช้ Wi-Fi สาธารณะ

ในการตอบสนองต่อการระบาดของไวรัสโคโรน่าและการปิดตัวของธุรกิจต่างๆ และห้องสมุด หลายคนในพวกเราใช้เวลามากยิ่งขึ้นออนไลน์ จากผลลัพธ์ เราอาจจะจำเป็นต้องใช้ Wi-Fi สาธารณะเพื่อเชื่อมต่ออินเตอร์เน็ท หากคุณพบว่าตนเองต้องการใช้ Wi-Fi สาธารณะ โปรดพิจารณาถึงคำแนะนำดังต่อไปนี้ จากหัวหน้าเจ้าหน้าที่ในความเป็นส่วนตัว เพื่อให้การช่วยเหลือในการปกป้องข้อมูลของคุณ:

1. ยืนยันว่าคุณได้มีเครื่อข่ายที่ถูกต้อง

ตรวจสอบให้มั่นใจว่าคุณเชื่อมต่อกับเครือข่ายที่ถูกต้อง คนร้ายอาจสร้างเครือข่ายที่ดูไม่เป็นอันตรายตามชื่อของพวกเขา แต่ในความเป็นจริงก็คือให้คุณเชื่อมต่อกับเครือข่ายการตั้งค่าเพื่อดูการท่องอินเทอร์เน็ตของคุณ นั่นหมายความว่า หากคุณป้อนข้อมูลการรับรองการเข้าสู่ระบบ หรือรหัสผ่านลงในเว็บไซต์ แฮ็กเกอร์จะสามารถขโมยข้อมูลของคุณได้ เพื่อป้องกันสิ่งนี้ ขอให้คุณได้ให้อ่านชื่อเครือข่ายอย่างระมัดระวังและหากเป็นไปได้ให้ถามพนักงานหรือตรวจสอบเครื่องหมายของธุรกิจเพื่อให้แน่ใจว่าเครือข่ายนั้นถูกต้องตามกฎหมาย

เครือข่ายที่รู้จักกันดีเช่น เครือข่ายกาแฟที่คุ้นเคยนั้น คุณอาจจะไม่ค่อยสงสัยเนื่องจาก บริษัท กำลังดำเนินการเครือข่ายเป็นบริการกับธุรกิจของพวกเขา เครือข่ายที่รู้จักมักปลอดภัยกว่าเครือข่าย Wi-Fi ฟรีแบบสุ่มที่อาจปรากฏในโทรศัพท์ของคุณในที่สาธารณะ

2. ปิดการเชื่อมต่ออัตโนมัติ

อุปกรณ์จำนวนมาก (สมาร์ทโฟน แล็ปท็อปและแท็บเล็ต) มีการตั้งค่าการเชื่อมต่อโดยอัตโนมัติ การตั้งค่านี้จะช่วยให้อุปกรณ์ของคุณเชื่อมต่อกับเครือข่ายใกล้เคียงได้สะดวกยิ่ง ถือว่าไม่มีปัญหากับเครือข่ายที่เชื่อถือได้ แต่สามารถเชื่อมต่ออุปกรณ์ของคุณกับเครือข่ายที่อาจไม่ปลอดภัยได้เช่นเดียวกัน คุณสามารถปิดการใช้งานคุณสมบัตินี้ โดยการผ่านคุณสมบัติการตั้งค่าบนอุปกรณ์ของคุณ ให้ปิดการตั้งค่าเหล่านี้เสมอ โดยเฉพาะเมื่อคุณต้องเดินทางไปยังสถานที่ที่ไม่คุ้นเคย เพื่อเป็นการป้องกันไว้ล่วงหน้าคุณสามารถตรวจสอบ “ให้ลืมเครือข่าย” หลังจากใช้ Wi-Fi สาธารณะ

คุณควรตรวจสอบ Bluetooth ของคุณในที่สาธารณะ การเชื่อมต่อ Bluetooth ช่วยให้อุปกรณ์ต่าง ๆ สามารถสื่อสารซึ่งกันและกันและแฮกเกอร์สามารถค้นหาสัญญาณ Bluetooth แบบเปิดเพื่อเข้าถึงอุปกรณ์ของคุณ ปิดใช้งานฟังก์ชั่นนี้ในโทรศัพท์และอุปกรณ์อื่น ๆ เมื่อคุณอยู่ในพื้นที่ที่ไม่คุ้นเคยเสมอ

3. การการแชร์ไฟล์

ตรวจสอบให้แน่ใจว่า คุณได้ปิดตัวเลือกการแชร์ไฟล์ในขณะที่ใช้ Wi-Fi สาธารณะแล้ว คุณสามารถปิดการแชร์ไฟล์ได้ จากการตั้งค่าระบบหรือแผงควบคุม ซึ่งขึ้นอยู่กับระบบปฏิบัติการของคุณเอง AirDrop เป็นตัวอย่างของคุณสมบัติการแชร์ไฟล์ที่คุณต้องการที่จะปิด ระบบปฏิบัติการบางระบบเช่น Windows / PC จะปิดการแชร์ไฟล์ให้กับคุณโดยเลือกตัวเลือก “สาธารณะ” เมื่อเชื่อมต่อกับเครือข่ายสาธารณะใหม่เป็นครั้งแรก

ขั้นตอนในการปิดการแชร์ไฟล์

บน PC:

1. ไปที่ศูนย์เครือข่ายและการแบ่งปัน
2. แล้ว ให้เปลี่ยนการตั้งค่าการแชร์แบบเลือกเอง
3. ปิดการแชรไฟล์และเครื่องพิมพ์

สำหรับ Macs:

1. ไปที่ การตั้งค่าที่ต้องการ
2. เลือกการแชร์
3. ไม่เลือกทุกอย่าง
4. ต่อไป ให้ไปที่ ค้นหา คลิกบน AirDrop และเลือก ยินยอมให้ฉันได้ถูกค้นพบโดย: ไม่มีใคร

สำหรับ iOS แค่หา AirDrop ในศูนย์ควบคุมและปิดมันเสีย

4. ใช้ VPN

พิจารณาติดตั้ง VPN (เครือข่ายส่วนตัวเสมือน) บนอุปกรณ์ของคุณ VPN เป็นทางเลือกที่ปลอดภัยที่สุดสำหรับความเป็นส่วนตัวแบบดิจิทัลในการใช้ Wi-Fi สาธารณะ มันทำการเข้ารหัสข้อมูลของคุณในขณะที่ส่งผ่านไปยังและจากอุปกรณ์ของคุณและทำหน้าที่เป็น “อุโมงค์” ป้องกันเพื่อให้ข้อมูลของคุณไม่สามารถมองเห็นได้เมื่อมันผ่านเครือข่าย

5. คำเตือนจาก FBI ในเรื่องเกี่ยวกับเว็บไซต์ที่เข้ารหัส - HTTPS

FBI ได้เตือนถึง เว็ปไซต์ที่มีที่อยู่ที่เริ่มต้นด้วย “https” สถานะของ “https” และไอคอนที่เป็นรูปล็อค เป็นการระบุว่าปริมาณการใช้งานเว็บนั้นได้รับการเข้ารหัสและผู้เยี่ยมชมสามารถแชร์ข้อมูลได้อย่างปลอดภัย อย่างไรก็ตามตอนนี้อาชญากรไซเบอร์กำลังทำธุรกรรมกับสาธารณะ ด้วยการชักจูงผู้คนไปยังเว็บไซต์ที่เป็นอันตรายซึ่งรวม https และดูว่าปลอดภัยเมื่อพวกเขาไม่อยู่

คำแนะนำของ FBI:

- อย่าเพียงเชื่อแค่ดูชื่ออีเมล: ให้สงสัยถึงเจตนาของเนื้อหาอีเมลนั้นด้วย
- หากคุณได้รับอีเมลที่น่าสงสัยพร้อมลิงก์จากผู้ติดต่อที่รู้จัก ขอให้คุณได้ทำการยืนยันว่าข้อความนั้นถูกต้องตามกฎหมายโดยการโทรหรือส่งอีเมลถึงผู้ติดต่อ อย่าตอบกลับไปยังอีเมลที่น่าสงสัยโดยตรง
- ตรวจสอบการสะกดที่ผิดหรือโดเมนที่ไม่ถูกต้องภายในลิงก์นั้น (เช่น หากที่อยู่ที่ควรลงท้ายด้วย “.gov” แต่กลับมาลงท้ายด้วย “.com” แทน)

- อย่าเชื่อถือเว็บไซต์เพียงเพราะมีไอคอนเป็นรูปตัวล็อคหรือ “https” ในแถบที่อยู่ของเบราว์เซอร์

6. ไม่แนะนำให้คุณเข้าถึงข้อมูลที่ละเอียดอ่อน

แม้ว่า หากคุณมี VPN มันก็ยังไม่เป็นการแนะนำให้ทำการ เข้าถึงข้อมูลบัญชีธนาคารของคุณ หรือ ข้อมูลส่วนตัวที่มีความละเอียดอ่อนใดๆ เช่น หมายเลขประกันสังคม บนเครื่อข่ายที่ไม่ปลอดภัยในสาธารณะ แม้แต่เครือข่ายสาธารณะที่มีความปลอดภัยก็มีความเสี่ยง แม้แต่เครือข่ายสาธารณะที่มีความปลอดภัยก็มีความเสี่ยงอยู่ดี สำหรับธุรกรรมทางการเงินการใช้ฟังก์ชั่นฮอตสปอตของสมาร์ทโฟนอาจดีกว่า

7. ปลอดภัย กับ ไม่ปลอดภัย

โดยทั่วไปมีเครือข่าย Wi-Fi สาธารณะสองประเภท: ปลอดภัยและไม่ปลอดภัย

หากเป็นไปได้ ขอให้เชื่อมต่อกับเครือข่ายสาธารณะที่ปลอดภัยเท่านั้น ไม่ว่าจะเวลาใดก็ตาม เครือข่ายที่ไม่ปลอดภัยสามารถเชื่อมต่อได้โดยไม่ต้องมีคุณสมบัติด้านความปลอดภัยเช่นรหัสผ่านหรือเข้าสู่ระบบ เครือข่ายที่ปลอดภัยมักจะกำหนดให้ผู้ใช้ต้องยอมรับข้อกำหนดและเงื่อนไขลงทะเบียนบัญชีหรือพิมพ์รหัสผ่านก่อนที่จะเชื่อมต่อกับเครือข่ายต่างๆ

8. เปิดใช้งานไฟร์วอลล์ของคุณอยู่เสมอ

หากคุณใช้แล็ปท็อปให้เปิดใช้งานไฟร์วอลล์ของคุณในขณะที่ใช้ Wi-Fi สาธารณะเสมอ ไฟร์วอลล์ทำหน้าที่เป็นเกราะกำแพงป้องกันอุปกรณ์ของคุณจากการคุกคามของมัลแวร์ ผู้ใช้อาจปิดการใช้งานไฟร์วอลล์ Windows เนื่องจากป๊อปอัปและการแจ้งเตือนแล้วให้ทำการลืมมัน หากคุณต้องการรีสตาร์ทบน PC ให้ไปที่แผงควบคุม “ระบบและความปลอดภัย” และเลือก “ไฟร์วอลล์ Windows” หากคุณเป็นผู้ใช้ Mac ให้ไปที่ “การตั้งค่าระบบ” จากนั้น “ความปลอดภัยและความเป็นส่วนตัว” จากนั้นไปที่แท็บ “ไฟร์วอลล์” เพื่อเปิดใช้งานคุณสมบัตินั้น

9. ใช้ซอฟต์แวร์ป้องกันไวรัส

ตรวจสอบให้แน่ใจว่าติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชันรุ่นล่าสุดบนแล็ปท็อปของคุณเสมอ โปรแกรมป้องกันไวรัสนี้ จะทำให้สามารถช่วยปกป้องคุณในขณะที่ใช้ Wi-Fi สาธารณะโดยการตรวจจับมัลแวร์ที่อาจเข้าสู่ระบบของคุณในขณะที่ใช้เครือข่ายที่ใช้ร่วมกันได้ การแจ้งเตือนจะเตือนคุณว่า ได้มีการโหลดไวรัสที่รู้จักบนอุปกรณ์ของคุณหรือหากมีกิจกรรมที่น่าสงสัยโจมตีหรือหากมัลแวร์เข้าสู่ระบบของคุณ

10. ใช้การรับรองความถูกต้องด้วยปัจจัยสองอย่างหรือหลายปัจจัย

ใช้การรับรองความถูกต้องแบบหลายปัจจัย (MFA) เมื่อเข้าสู่เว็บไซต์ด้วยข้อมูลส่วนบุคคลของคุณเสมอ นั้นหมายความว่าคุณมีรหัสยืนยันตัวที่สอง (ส่งข้อความไปยังโทรศัพท์ของคุณหรือจัดทำโดยแอพหรือคีย์ทางกายภาพ) ซึ่งจะช่วยปกป้องคุณต่อไปอีก ดังนั้นแม้ว่าแฮ็กเกอร์จะได้รับชื่อผู้ใช้และรหัสผ่านของคุณแล้ว แต่พวกเขาก็ไม่สามารถเข้าถึงบัญชีของคุณได้โดยไม่ต้องมีรหัสการตรวจสอบสิทธิ์

11. ติดตามอุปกรณ์ส่วนตัวของคุณ

อย่า ทิ้งแล็พท๊อป แท็บเลท หรือ สมาร์ทโฟนของคุณ โดยไม่ได้มาดูแลในสถานที่สาธารณะ หรือ ในยานพาหนะ แม้ว่าคุณมีความระมัดระวังในเครือข่าย Wi-Fi แต่นั่นจะไม่หยุด คนที่จะนำทรัพย์สินของคุณหรือแอบดูข้อมูลของคุณได้ ระวังระไวต่อสิ่งรอบตัวและใส่ใจคนรอบข้าง

12. เคล็ดลับในเรื่องความปลอดภัยออนไลน์อื่น ๆ

นี่คือเคล็ดลับบางประการสำหรับการใช้งานออนไลน์อย่างปลอดภัยโดยเฉพาะ ที่เมื่อคุณใช้การเชื่อมต่อ Wi-Fi สาธารณะ:

- ใช้รหัสผ่านที่เดายาก
- เข้ารหัสอุปกรณ์ของคุณ
- ระวังอีเมลฟิชชิง
- ระวังสิ่งที่คุณประกาศลงบนโซเชียลมีเดีย รายละเอียดส่วนบุคคลมากเกินไป อันเป็นสิ่งที่แฮกเกอร์สามารถเดารหัสผ่านได้
- ลบข้อมูลเก่าที่คุณไม่ต้องการอีกต่อไป
- หากเครือข่ายขอให้คุณติดตั้งซอฟต์แวร์เพิ่มเติมหรือส่วนขยายเบราว์เซอร์ใด ๆ ขออย่าได้ทำการเชื่อมต่อ
- ตรวจสอบว่ามีการติดตั้งแพตช์และการอัพเดทซอฟต์แวร์ล่าสุดในอุปกรณ์ของคุณเพื่อป้องกันปัญหาที่ท่านทราบอยู่แล้ว