ท่องเที่ยว เดินทาง อย่างปลอด(ภัย) ในโลกไซเบอร์

ดร.ปราณิสา อิศรเสนา
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น

สมัยก่อนเวลาท่องเที่ยวเดินทาง สิ่งแรกที่คนเราจะนึกถึงคงจะเป็นเรื่องความปลอดภัยของยานพาหนะจากอุบัติเหตุ ความกังวลเรื่องสุขภาพจากโรคระบาด ไข้หวัดนก การจี้ปล้นต่างๆ เป็นต้น แต่ปัจจุบันนี้ อีกเรื่องหนึ่งที่คงละเลยไม่ได้ ได้แก่ความปลอดภัยจากการโจมตีทางไซเบอร์ ผ่านอุปกรณ์พกพาของพวกเรานั่นเอง

เมื่อโทรศัพท์เคลื่อนที่ กลายเป็นอุปกรณ์ที่เราป้อนข้อมูลส่วนตัว ทำธุรกรรมต่างๆ มากมาย เป็นทุกอย่างในชีวิตก็ว่าได้ ซึ่งบางครั้งเราก็ต้องเดินทางไปเที่ยวหรือทำงานนอกสถานที่บ้าง แล้วเราจะแน่ใจได้อย่างไรว่า เราจะยังปลอดภัยในโลกไซเบอร์เช่นเดียวกับที่เคยเป็นในพื้นที่ของเรา

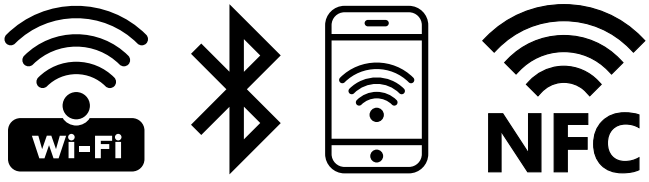
หากจะวางกรอบแนวคิดด้านความปลอดภัย เราจะต้องชั่งน้ำหนักอยู่เสมอระหว่างความปลอดภัย การใช้งานง่าย และประโยชน์ใช้สอย ตัวอย่างใกล้ตัว เช่น รหัสผ่านเข้าระบบ ซึ่งช่วยสนับสนุนด้านความปลอดภัย แต่หากพาสเวิร์ดยาวมากๆ หรือหมดอายุเร็วไป ผู้ใช้ก็จะรู้สึกเบื่อหน่ายเพราะขาดคุณสมบัติข้อใช้งานง่าย ในทางกลับกัน แต่ถ้าพาสเวิร์ดง่ายเกินไป สั้นเกินไป ความปลอดภัยก็จะน้อยลง เพราะคนร้ายคาดเดาได้ง่าย

นอกจากนี้ ก็เช่น คุณเป็นอีกคนหนึ่งหรือไม่ที่คลิกฟังก์ชั่นจำพาสเวิร์ดไว้ถาวรในเครื่อง เพื่อล็อกอินเข้าเว็บไซต์ หรือเช็คอีเมล์ได้ทันที เพราะขี้เกียจจำ เวลาใช้พีซีร่วมกับคนอื่นในจุดบริการอินเทอร์เน็ตสาธารณะ เช่น โรงแรม พอใช้เสร็จ คุณก็แค่ปิดเบราเซอร์แล้วเดินจากไป โดยไม่ได้สั่ง Log out จากโปรแกรมจริงๆ ทำให้ผู้ใช้พีซีต่อจากคุณ เข้าใช้ระบบเหมือนเป็นตัวคุณได้ทันที หากใช่แปลว่า คุณควรตระหนักในเรื่องความปลอดภัยทางไซเบอร์มากกว่านี้ค่ะ

อีกประเด็นที่ส่งผลกับกับประโยชน์ใช้สอยของอุปกรณ์พกพาอยู่เสมอได้แก่ แบตเตอรี่ และการจัดการพลังงาน พลังงานจะหมดเร็วขึ้นมากมื่อคุณเปิดฟังก์ชันที่ช่วยเพิ่ม security เช่น การใช้ vpn การใช้ mobile firewall ซึ่งเป็นประโยชน์มากก็จริงแต่ช่วงที่โดนโจมตีแบตเตอรี่จะลดเร็วมาก การเข้ารหัสก็ใช้พลังงานไม่น้อย ดังนั้น คุณจึงควรเตรียม แบตเตอรี่สำรองหรือพาวเวอร์แบงค์ไปด้วยระหว่างเดินทางด้วย

ไวไฟ (Wi-fi) อำนวยความสะดวกให้คุณใช่ไหม คุณใช้ไวไฟฟรีที่ร้านอาหารหรือเปล่า คุณเคยแชร์ hotspot เชื่อมต่อ บลูทูธ หรือใช้ near field communication (NFC) บ้างไหม คุณแน่ใจได้อย่างไรว่า access point ที่คุณเชื่อมต่ออยู่เป็นอุปกรณ์ของผู้ให้บริการจริงหรือเป็น hotspot ปลอม

คำแนะนำที่อาจดูโหดร้ายสักหน่อยก็คือทางที่ดีอย่าใช้งานฟรีไวไฟ เพื่อส่งข้อมูลสำคัญๆ หรือ Log in ใดๆ เพราะต่อให้เป็นอุปกรณ์สาธารณะจริง ก็มีโอกาสถูกดักข้อมูลตลอดเวลา อย่างน้อยใช้สัญญาณ อินเทอร์เน็ตมือถือโดยไม่เปิดเป็น hotspot จะปลอดภัยกว่า



Threat ของอุปกรณ์ไร้สายไม่จำเป็นต้องอยู่ในระยะใกล้ตัวคุณ ระยะของสัญญาณ ตัวรับที่มีประสิทธิภาพสามารถจับสัญญาณบลูทูธได้ไกลเป็น 100 เมตร การเข้ารหัสไวไฟก็สำคัญ หลายท่านทราบว่า WPA2 ดีกว่า WPA/TKIP ที่สามารถ crack ได้ใน 7 นาที แต่แม้แต่ WPA2 ก็ยังไม่ปลอดภัยหากใช้คีย์สั้นเกินไป

ที่พักบางแห่งมีช่องเสียบสายแลนให้ เรารู้ได้อย่างไรว่าไม่มีอุปกรณ์ดักสัญญาณ tab สายต่ออยู่กับช่องเสียบสัญญาณนั้น แน่นอนว่าเรายอมอยากได้ speed มากกว่า เพราะเทียบกับไวไฟแล้ว

เสียบสายแลนดูจะเร็วกว่า แต่โปรดจำไว้เสมอว่าข้อมูลที่ไม่ได้เข้ารหัสก็จะยังสุ่มเสี่ยงโดนดักจับอยู่ดี หากเป็นไปได้โปรดใช้ vpn หรือเข้ารหัสข้อมูลสำคัญๆ เสมอ หากมีสายแลนให้เสียบ สายเมาส์ คีย์บอร์ดให้ลองไล่สายดูว่ามาจากไหนมีอุปกรณ์ กล่องใดที่ไม่น่าไว้วางใจคั่นอยู่หรือไม่ แม้แต่อุปกรณ์ usb charger ที่ไม่ใช่ของเราก็อันตรายได้ !

Juice Jacking หมายถึง การส่งมัลแวร์ผ่านอุปกรณ์ชาร์จไฟ วิธีป้องกันคือ ต้องตั้งค่าอุปกรณ์ของเราไม่ให้ sync ข้อมูลกับ USB โดยอัตโนมัติหรือหากไม่สะดวกตั้งค่า ให้ใช้อุปกรณ์ป้องกัน sync คั่นระหว่างช่องเสียบ และสายสัญญาณของเรา เช่น syncstop เป็นต้น

อุปกรณ์ป้องกัน Sync

VPN ช่วยเรื่องความปลอดภัยก็จริง แต่จะทำให้ส่งข้อมูลได้ช้ามาก จนถึงขั้นทนไม่ได้ทีเดียว ฟรี vpn ทำให้เกิดการ delay เพิ่มขึ้นได้ถึง 500% หาก internet ไม่เร็วพอไม่แนะนำให้ใช้ vpn ตลอดเวลา ให้ใช้เฉพาะเวลาส่งข้อมูลสำคัญก็จะดีกว่า

อุปกรณ์ Backup เช่น Hard Drive สำรอง หากมีข้อมูลที่สำคัญ ควรเข้ารหัสไฟล์เอาไว้ หากคุณนำโน้ตบุคบริษัทไปใช้ ให้ระวังการขโมย สูญหาย และควรเข้ารหัสไฟล์สำคัญในเครื่องโน้ตบุคเช่นกัน ล็อคกุญแจไว้ และผูกกับสายนิรภัยก็ช่วยได้ค่ะ

GPS เราได้ check in บอกคนร้ายหรือไม่ว่าเราอยู่ไหนไปไหน จำเป็นหรือไม่ที่คนต้องรู้ความเคลื่อนไหวของเราตลอดเวลา GPS ทำให้แบตเตอรี่หมดเร็วอีกด้วยค่ะ

ระแวงไว้ก่อนเพื่อความปลอดภัยของเรากันนะคะ TPA news