ความปลอดภัยไซเบอร์งาน FIFA World Cup 2018 น่าห่วง พบจุดเชื่อมต่อ Wi-Fi กว่า 20% ไม่ปลอดภัย

รายงานวิจัยของแคสเปอร์สกี้ แลป ชี้ว่าจุดบริการเน็ตเวิร์ก Wi-Fi จำนวน 7,176 จุด ตามเมืองแข่งขัน FIFA World Cup 2018 จากประมาณ 32,000 จุด ไม่ใช้การเข้ารหัสข้อมูลสื่อสาร แฟนฟุตบอลทั้งหลายตามเมืองเหล่านั้นมีความเสี่ยง ควรมีมาตรการวิธีการป้องกันข้อมูลสำคัญส่วนตัวด้วยตนเอง โดยเฉพาะ เมื่อใดก็ตามที่ใช้การเชื่อมต่อ Wi-Fi ตามเมืองต่างๆ ที่เป็นเจ้าภาพแข่งขัน FIFA World Cup

งานระดับโลกเช่นนี้มักเป็นช่วงเวลาที่ผู้คนมากมายทั่วโลกต่างพากันต่อเชื่อมเน็ตเวิร์กกันอย่างหนาแน่นเพื่ออัพโหลดโพสต์ ติดต่อเพื่อนฝูง คนรัก แชร์ความตื่นเต้นบันเทิงกัน ทำให้เน็ตเวิร์กเหล่านี้ถูกใช้เป็นช่องทางในการโอนย้ายถ่ายเทเงิน รวมทั้งข้อมูลอันมีค่าผ่านอินเทอร์เน็ตได้ด้วย และข้อมูลเหล่านี้เองคือหมายที่มิจฉาชีพ หรือเธิร์ดปาร์ตี้ ไม่จำเป็นว่าจะต้องเป็นอาชญากรผู้ร้ายไซเบอร์เท่านั้น ใช้เป็นช่องทางเข้าแทรกแซงเพื่อดึงเอาข้อมูลมาใช้เพื่อประโยชน์ของตัวเอง

การวิจัยของแคสเปอร์สกี้ แลป นั้นอยู่บนพื้นฐานการวิเคราะห์ Wi-Fi สาธารณะตามจุดต่างๆ ที่ติดตั้งอยู่ใน 11 หัวเมืองที่มีการแข่งขัน FIFA World Cup 2018 ได้แก่ เมือง Saransk, Samara, Nizhny Novgorod, Kazan, Volgograd, Moscow, Ekaterinburg, Sochi, Rostov, Kaliningrad, และ Saint Petersburg ผลการวิจัยพบว่าไม่ใช่ทุกจุดสัญญานต่อเชื่อมไร้สายที่จะใช้วิธีการเข้ารหัสและอัลกอริธึ่มสำหรับตรวจสอบความถูกต้อง ซึ่งเป็นรูปแบบวิธีการที่สำคัญต่อความปลอดภัยของเน็ตเวิร์ก Wi-Fi หมายความว่าแฮกเกอร์เพียงแต่หาทางมาอยู่ใกล้ๆ แอคเซสพอยต์เพื่อเข้าแทรกทราฟฟิกบนเน็ตเวิร์ก ก็สามารถที่จะโจรกรรมข้อมูลมีค่าจากยูสเซอร์ที่ไม่ได้เตรียมการป้องกันตัวไว้ได้แล้ว

ทั้งนี้ มีเมืองจำนวนสามเมืองที่มีอัตราความเสี่ยงของเน็ตเวิร์ก Wi-Fi สูงที่สุด ได้แก่ เมือง Saint Petersburg (37%), เมือง Kaliningrad (35%) และ เมือง Rostov (32%) ในทางตรงข้าม จุดที่ปลอดภัยที่สุดกลับเป็นเมืองเล็กๆ เช่น เมือง Saransk (เพียง 10% มีเป็นระบบเปิด) และ เมือง Samara (17% มีเป็นระบบเปิด) เน็ตเวิร์ก Wi-Fi สาธารณะจำนวนเกือบสองในสามในสถานที่เหล่านี้ใช้ Wi-Fi Protected Access (WPA/WPA2) protocol family สำหรับเข้ารหัสทราฟฟิก ซึ่งเป็นโปรโตคอลที่ได้รับการยอมรับว่าเป็นหนึ่งในโปรโตคอลที่ปลอดภัยที่สุดสำหรับการใช้ Wi-Fi

อย่างไรก็ตาม ก็ต้องพึงระลึกไว้เสมอว่า แม้แต่เน็ตเวิร์ก WPA/WPA2 ที่ว่ากันว่าเสถียรก็ต้องเผชิญกับการโจมตีใน

ลักษณะ brute-force (โจมตีคนที่ใช้พาสเวิร์ดง่ายๆ) และ dictionary attacks (สุ่มพาสเวิร์ดจากคำในพจนานุกรม) รวมทั้ง key reinstallation attacks (แฮกเกอร์ที่อยู่ในบริเวณครอบคลุมสัญญาณเดียวกันกับอุปกรณ์ของคุณ สามารถถอดรหัสและขโมยข้อมูล ไปจนถึงควบคุมทราฟิกข้อมูลของคุณได้ดังใจ) นั่นย่อมหมายถึงความไม่ปลอดภัย

เดนิส เลเกโซ นักวิจัยความปลอดภัยอาวุโส แคสเปอร์สกี้ แลป กล่าวว่า “เมื่อไม่มีการเข้ารหัสข้อมูลที่สื่อสาร ผนวกกับความเป็นที่นิยมในความสนใจของหมู่มวลสาธารณชนทั่วโลก อย่าง FIFA World Cup นี้ ทำให้เน็ตเวิร์กการสื่อสารไร้สาย Wi-Fi เป็นเป้าหมายของบรรดาผู้ร้ายอาชญากรไซเบอร์ที่มีความปราถนาจะล้วงเข้ามาลักข้อมูลส่วนตัวต่างๆ ของยูสเซอร์ ถึงแม้ว่าแอคเซสพอยต์กว่าสองในสามในหัวเมืองที่จัดแข่ง FIFA World Cup จะใช้การเข้ารหัสโดยใช้ Wi-Fi Protected Access (WPA/WPA2) protocol family ที่มีความปลอดภัยที่สุดก็ตาม แอคเซสพอยต์เหล่านี้ก็ถือว่ายังไม่ปลอดภัยเพียงพอ ถ้าหากไม่ได้มีวิธีการป้องกันพาสเวิร์ดให้พ้นจากผู้ร้าย งานวิจัยของเราชี้ว่าความมั่นคงปลอดภัยทางไซเบอร์นั้นมีความเกี่ยวโยงกับโครงสร้างโดยรวมทั้งหมด มิใช่เพียงแค่ส่วนใดส่วนหนึ่ง การแข่งขัน FIFA World Cup 2018 เป็นตัวยืนยันว่างานยิ่งใหญ่ระดับโลกเช่นนี้โดยตัวของมันเองแล้วมีความปลอดภัย แต่ตามเมืองต่างๆ ที่ให้บริการ Wi-Fi Hotspot นั้นเป็นอีกเรื่องหนึ่ง และไม่จำเป็นว่าจะมีความปลอดภัยในระดับเดียวกันไปด้วย”

หากท่านเดินทางไปชมการแข่งขัน FIFA World Cup 2018 ตามเมืองต่างๆ ในครั้งนี้ และอาจต้องใช้ Wi-Fi เน็ตเวิร์กสาธารณะ ควรปฏิบัติตามกฎง่ายๆ ในการป้องกันข้อมูลอันมีค่าส่วนตัว ขณะร่วมลุ้นร่วมเชียร์ทีมโปรดในเมืองนั้นๆ ดังนี้

• เมื่อใดก็ตามที่เป็นไปได้ ให้เชื่อมต่อโดยใช้ Virtual Private Network (VPN) ซึ่งข้อมูลที่เข้ารหัสของคุณจะสื่อสารผ่านเส้นทางที่ได้รับการป้องกัน หมายความว่าผู้ร้ายไซเบอร์จะไม่สามารถอ่านข้อมูลของคุณได้ ถึงแม้ว่าจะไปแอบขโมยแอคเซสของคุณมาได้ก็ตาม เช่น โซลูชั่น สำหรับ VPN อย่าง Kaspersky Secure Connection สามารถสวิตช์ออนได้อัตโนมัติเมื่อใดก็ตามที่การเชื่อมต่อการต่อเชื่อมไม่ปลอดภัย เป็นต้น

• อย่าไว้วางใจเน็ตเวิร์กที่ไม่ต้องใช้พาสเวิร์ดเพื่อเข้าใช้งาน หรือพาสเวิร์ดที่เดาง่าย หรือหาพบได้ง่าย

• แม้ว่าเน็ตเวิร์กบางอันจะใช้พาสเวิร์ดที่แข็งแกร่ง ก็ยังต้องระมัดระวังอยู่ดี ผู้ร้ายไซเบอร์สามารถหาพาสเวิร์ดเข้าเน็ตเวิร์กตามร้านกาแฟได้ง่ายๆ จากนั้นก็เพียงแต่สร้างการเชื่อมต่อหลอกๆ ที่ตั้งให้ใช้พาสเวิร์ดเดียวกัน เพียงเท่านี้ก็สามารถขโมยข้อมูลส่วนตัวของคุณไปได้ง่ายๆ แล้ว ควรไว้วางใจเฉพาะเน็ตเวิร์กที่มีชื่อและพาสเวิร์ดที่ได้รับมาโดยตรงจากพนักงานเจ้าหน้าที่ของสถานที่นั้นๆ เท่านั้น

• เพื่อให้การป้องกันเป็นไปอย่างแข็งแกร่งสูงสุด ให้ปิดการเชื่อมต่อ Wi-Fi ทุกครั้งที่คุณไม่ได้ใช้งานแล้ว ซึ่งประหยัดแบตเตอรี่ไปในตัว และขอแนะนำเพิ่มเติมว่า ควรที่จะยกเลิกคำสั่งให้เชื่อมต่อเน็ตเวิร์ก Wi-Fi แบบอัตโนมัติไปเสียด้วยจะดีกว่า

• ถ้าหากคุณไม่มั่นใจถึง 100% ว่าเน็ตเวิร์กไร้สายที่คุณใช้งานมีความปลอดภัยเพียงพอ แต่ยังจำเป็นต้องใช้งานต่อเข้าอินเทอร์เน็ต คุณก็ควรพยายามจำกัดกิจกรรมบนเน็ตให้เป็นเพียงแบบพื้นฐานทั่วไปเท่านั้น เช่น ใช้เพื่อค้นหาข้อมูล คุณไม่ควรทำกิจกรรมออนไลน์ใดๆ ที่ต้องล็อกอินใส่พาสเวิร์ด เช่น โซเชียลเน็ตเวิร์ก หรืออีเมล และแน่นอนว่าอย่าได้ทำธุรกรรมการเงินออนไลน์ หรือใส่รายละเอียดเกี่ยวกับบัญชีธนาคารเลย หลีกเลี่ยงความเป็นไปได้ หรือการเปิดโอกาสให้ข้อมลส่วนตัว ข้อมูลสำคัญ หรือพาสเวิร์ดถูกขโมยแล้วนำไปใช้เพื่อประโยชน์ในทางมิจฉาชีพโดยเด็ดขาด

• หลีกเลี่ยงการตกเป็นเป้าของเหล่าอาชญากรมิจฉาชีพไซเบอร์ คุณควรเปิดอ็อพชั่น “always use a secure connection” (HTTPS) ในการตั้งค่าในเครื่องสื่อสารที่คุณใช้งาน ซึ่งเป็นอ็อพชั่นซึ่งแนะนำให้เปิดใช้งานเมื่อใดก็ตามที่เข้าเว็บไซต์ใดๆ ก็ตามที่คุณคิดว่าอาจจะมีความปลอดภัยไม่เพียงพอเท่าที่ควร

ท่านสามารถอ่านข้อมูลเพิ่มเติมเกี่ยวกับสถานการณ์ Wi-Fi การเชื่อมต่อในการแข่งขัน FIFA World Cup ตามเมืองต่างๆ ได้ที่ https://securelist.com/fifa-public-wi-fi-guide/85919/

###