

แพ็คกระเป๋าเที่ยวให้สนุกต้องไม่ประมาท แคนเปอร์ สก็ย่าเคล็ดไม่ลับเพื่อความปลอดภัยไซเบอร์ตลอด ทริป



วันหยุดเทศกาลคือช่วงเวลาที่นำครอบครัว เพื่อน และคนที่รักมาเจอกัน บางคนก็ใช้เวลาอยู่ด้วยกันง่ายๆ ที่บ้าน บ้างก็แพ็คกระเป๋าชวนกันไปสถานที่ท่องเที่ยวยอดฮิตเพื่อพักผ่อนเติมพลัง ยิ่งวันหยุดยาวใกล้จะมาถึงแล้ว ผู้ใช้งานอินเทอร์เน็ตน่าจะเริ่มคิดถึงการทำให้วันหยุดให้ปลอดภัยจากผู้ร้ายไซเบอร์ที่ไม่เคยหยุดพัก คุณอาจคิดว่า ภัยคุกคามไซเบอร์นั้นไกลตัว แต่ในความจริงแล้วภัยร้ายนั้นใกล้ตัวคุณมากกว่าที่คาดคิด

ในปี 2014 นักวิจัยของแคนเปอร์สก็เปิดเผยข้อมูลกลุ่มปฏิบัติการ Darkhotels ที่โจมตีโรงแรมหรูในทวีปเอเชีย โดยใช้วิธีการเข้าควบคุมเครื่องคอมพิวเตอร์ผ่านเครือข่าย Wi-Fi ของโรงแรม พบเหยื่อเป็นลูกค้าประวัติดีมีฐานะดีจำนวนมาก ล่าสุดในปี 2019 นี้เอง แคนเปอร์สก็เปิดโปงแคมเปญการโจมตีชื่อ RevengeHotels มีเป้าหมายเป็นธุรกิจการโรงแรมและการท่องเที่ยว เพื่อขโมยข้อมูลบัตรเครดิตของลูกค้า พบเหยื่อเป็นโรงแรมมากกว่า 20 แห่งในทวีปละตินอเมริกา ยุโรป และเอเชีย ซึ่งรวมประเทศไทยด้วย

เห็นได้ชัดว่า สถานที่ท่องเที่ยวใดที่ถูกใจนักท่องเที่ยวจำนวนมาก ก็ย่อมถูกใจผู้ร้ายไซเบอร์เช่นกัน จังหวัดท่องเที่ยวยอดฮิตของประเทศไทยคือ กรุงเทพฯ เชียงใหม่ ภูเก็ต และพัทยา โดยอุตสาหกรรมการท่องเที่ยวของ

ประเทศไทยนั้นได้รับการคาดการณ์ไว้ให้เป็นตัวขับเคลื่อนสำคัญทางเศรษฐกิจและผลิตภัณฑ์มวลรวมในประเทศ (GDP) ทั้งนี้สภาอุตสาหกรรมท่องเที่ยวแห่งประเทศไทย (สทท.) คาดการณ์ว่าในไตรมาสที่ 4 ปีนี้ซึ่งเป็นช่วงฤดูกาลท่องเที่ยวของปี จะมีนักท่องเที่ยวต่างชาติเดินทางมาประเทศไทยราว 10.41 ล้านคน สูงกว่าช่วงเดียวกันในปี 2018 ถึง 7.21% และคาดว่าจะมีรายได้จากการท่องเที่ยว 536,834 ล้านบาท

ในส่วนของนักท่องเที่ยวไทย ศูนย์วิจัยกสิกรไทยประเมินว่าการเดินทางของนักท่องเที่ยวไทยไปต่างประเทศในปีนี้จะยังขยายตัวอย่างต่อเนื่อง และคาดว่าจะมีคนไทยไปท่องเที่ยวต่างประเทศจำนวน 10.55 – 10.75 ล้านคน เติบโตขึ้น 5.4% – 7.4% จากปี 2018 ซึ่งเป็นตัวเลขสูงที่สุดในรอบ 6 ปี

อย่างไรก็ดี การใช้เวลาอยู่ที่บ้านในช่วงวันหยุดเทศกาลก็เชื่อว่าจะปลอดภัยจากภัยคุกคามไซเบอร์หากผู้ใช้มีพฤติกรรมที่ไม่ระแວดระวัง เพราะนอกเหนือจากแคมเปญร้ายที่หมายโจมตีนักท่องเที่ยวแล้ว อาชญากรไซเบอร์ยังสร้างกลโกงหลอกลวงมากมายดักรอเหยื่อ ไม่ว่าจะเป็นฟิชซิ่ง แแบ็งกิ้งโทรจัน และบ็อตเน็ตการเงินที่โจมตีเว็บไซต์ และแอปพลิเคชันออนไลน์ช้อปปิ้ง เพื่อขโมยข้อมูลลูกค้า ชื่อล็อกอิน พาสเวิร์ด หมายเลขบัตรเครดิต และหมายเลขโทรศัพท์ เป็นต้น

โยว เชียง เทียง ผู้จัดการทั่วไป บริษัท แคสเปอร์สกี ประจำภูมิภาคเอเชียตะวันออกเฉียงใต้ กล่าวว่า “แน่นอนว่าช่วงวันหยุดยาวเป็นช่วงที่ดีที่สุดของปีที่เราจะใช้เวลาร่วมกับญาติสนิทมิตรสหายเพื่อเดินทางท่องเที่ยวและพักผ่อน เราจึงควรนอนวันดีๆ เช่นนั้นไว้โดยการเพิ่มมาตรการระแວดระวังภัยไซเบอร์ไว้ในแผน ช่วงเทศกาลเป็นช่วงที่มีการช้อปปิ้งออนไลน์และการโพสต์โซเชียลมีเดียในปริมาณมาก อีกทั้งมีผู้ใช้งานจำนวนมากที่พกโทรศัพท์มือถือและแล็ปท็อปของบริษัทขณะเดินทาง จึงเป็นช่วงเวลาที่เหมาะสมที่อาชญากรไซเบอร์หมายตารอโอกาสนี้เพื่อซุ่มโจมตีเช่นกัน จึงขอแนะนำให้ผู้ใช้ทุกคนมีอุปนิสัยการใช้งานออนไลน์ขั้นพื้นฐานที่ดี เพื่อหลีกเลี่ยงให้พ้นภัยคุกคาม”

คำแนะนำสำหรับนักช้อปปิ้งออนไลน์

ทำการซื้อขายผ่านตลาดออนไลน์ที่เป็นทางการเท่านั้น และหากกดลิงก์มาจากที่อื่น ให้สังเกตดูเว็บแอดเดรสด้วย หากแตกต่างจากร้านค้าออนไลน์ทางการ นักช้อปควรพิจารณาเลือกข้อเสนออื่นๆ จากเว็บทางการแทน

อย่าคลิกลิงก์ที่คุณไม่คุ้นเคยที่ส่งมาทางอีเมลหรือโซเชียลมีเดีย แม้จะมาจากคนที่คุณรู้จักก็ตามที่ เว้นเสียแต่ว่าคุณกำลังรอข้อความเหล่านั้นอยู่แล้ว

ตรวจสอบให้แน่ใจว่าอีเมลแอดเดรสของผู้ส่งข้อความมาถึงคุณนั้น ถ้าไม่ใช่เว็บไซต์โดเมนทางการของแบรนด์นั้นๆ ก็อย่าได้คลิกลิงก์เข้าไปโดยเด็ดขาด

เลือกบริการการชำระเงินที่มีขั้นตอนการตรวจสอบและการอนุมัติ

ใช้โซลูชันเพื่อความปลอดภัยที่มีเทคโนโลยีแอนตี้ฟิชซิ่ง เช่น Kaspersky Security Cloud และ Kaspersky Total Security ซึ่งจะช่วยแจ้งเตือนเมื่อผู้ใช้กำลังจะเข้าเว็บฟิชซิ่ง

ไม่ใช่พาสเวิร์ดเดียวกันหลายเว็บไซต์หลายเซอวีริส เพราะถ้าหากหลุดไปอยู่ในมือผู้ประสงค์ร้าย แอคเค๊าท์ทั้งหมด

ทุกรายการจะตกอยู่ในความเสี่ยง สามารถเลือกใช้โซลูชันจัดการพาสเวิร์ด เช่น Kaspersky Password Manager เพื่อสร้างพาสเวิร์ดที่แยกยากและมีตัวช่วยจำ

คำแนะนำสำหรับนักท่องเที่ยว

จองตั๋วเครื่องบินและที่พักจากเว็บไซต์ทางการที่เชื่อถือได้เท่านั้น แนะนำให้ผู้ใช้พิมพ์ชื่อเว็บไซต์ในช่อง address บนเบราว์เซอร์ด้วยตัวเองแทนการกดลิงก์จากที่อื่น

หากได้รับอีเมลหรือโซเชียลมีเดียแจ้งว่าได้รับของรางวัลจากบริษัทท่องเที่ยวหรือสายการบิน ให้ตรวจสอบที่เว็บไซต์อย่างเป็นทางการของบริษัทนั้นๆ ว่าจริงหรือไม่ และต้องตรวจสอบลิงก์ก่อนกดทุกครั้ง

ใช้บัตรเครดิตเสมือนจริง (virtual payment card) ในการจองตั๋ว จองที่พัก หรือทำธุรกรรมผ่านตัวแทนท่องเที่ยว เพราะบัตรจะใช้งานได้เพียงครั้งเดียวเท่านั้น และจะหมดอายุไม่สามารถใช้งานได้อีก

เมื่อชำระเงินค่าจองหรือเช็คเอาท์ที่โรงแรมที่พัก ให้ใช้ virtual wallet เช่น Apple Pay หรือ Google Pay หรือบัตรเครดิตสำรองที่มีการจำกัดวงเงิน

อย่าวางสัมภาระให้ห่างจากตัวหรือไม่มีผู้ดูแล นอกจากนี้ ควรตั้งพาสเวิร์ดและล็อกโมบายดีไวซ์ต่างๆ ที่พกขณะเดินทาง

ติดตั้งแอปป้องกันการโจรกรรมบนโมบายดีไวซ์ หรือทดลองใช้ฟีเจอร์ป้องกันการโจรกรรมที่ติดตั้งมาบนเครื่องให้คุ้นเคย

ใช้โซลูชันเพื่อความปลอดภัยที่ป้องกันสแปมและฟิชชิ่งได้ เช่น Kaspersky Security Cloud

ไม่ใช้ Wi-Fi สาธารณะ และไม่ใช้ Wi-Fi ในห้องพักรวม นอกเสียจากว่าได้ทำการเข้ารหัสและใส่พาสเวิร์ดแล้ว หรือใช้ virtual private network (VPN) แทน

###