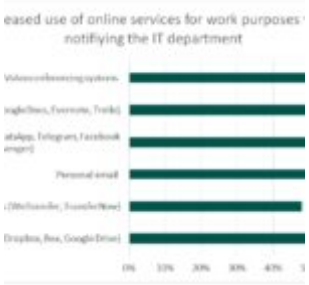
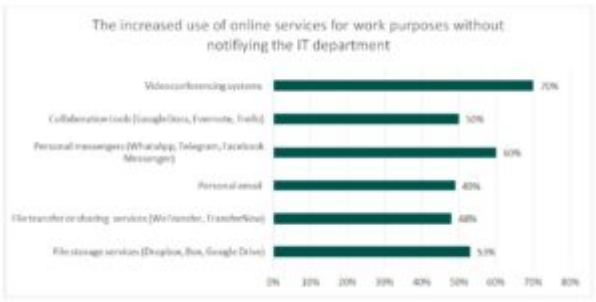


รายงานล่าสุดของแคสเปอร์สกี้สะท้อนเสียงพนักงาน WFH 73% ไม่ได้รับคำแนะนำการทำงานจากบ้านให้ปลอดจากภัยไซเบอร์



จากรายงานล่าสุดของแคสเปอร์สกี้ เรื่อง “วิธีที่ COVID-19 เปลี่ยนวิธีการทำงานของคน” (How COVID-19 changed the way people work) พนักงานจำนวนสามในสี่ (73%) ที่ทำงานจากที่บ้านยังไม่ได้รับคำแนะนำหรือการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ที่ออกแบบมาเพื่อป้องกันตนเองจากความเสี่ยง แม้ว่าการควบคุมความปลอดภัยของไอทีในองค์กรและข้อมูลจากระยะไกลจะทำได้ยากขึ้น แต่ภัยคุกคามก็ยังคงอยู่ ตัวอย่างเช่นพนักงานหนึ่งในสี่ (27%) กล่าวว่าพวกเขาได้รับอีเมลฟิชชิ่งที่เกี่ยวข้องกับ COVID-19 เพื่อหลีกเลี่ยงความเสี่ยงดังกล่าวเป็นสิ่งสำคัญที่องค์กรต่างๆต้องให้ความรู้แก่พนักงานเกี่ยวกับความปลอดภัยทางไซเบอร์

ในขณะที่พนักงานใช้เวลาทำงานที่บ้านอย่างกะทันหัน เป็นเรื่องสำคัญที่ธุรกิจต่างๆ ต้องมั่นใจว่าพนักงานสามารถทำงานได้ตามปกติ การรักษาความปลอดภัยให้กับพนักงานกลายเป็นงานที่ท้าทาย เนื่องจากต้องใช้ทรัพยากรจำนวนมากเพื่อให้สามารถเข้าถึงบริการด้านความปลอดภัยได้อย่างสม่ำเสมอ พนักงานจำเป็นต้องทำงานให้ดี ดังนั้นการสร้างมาตรการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพจึงเป็นเรื่องสำคัญ เนื่องจากการทำงานระยะไกลอาจนำความเสี่ยงใหม่ ๆ เช่น การโจมตีทางสแปมและฟิชชิ่งที่เพิ่มขึ้น การเชื่อมต่อกับจุด WiFi ที่ถูกบุกรุก หรือการใช้ระบบไอทีเงาโดยไม่ได้รับอนุญาต

อย่างไรก็ตาม จากการสำรวจแรงงาน 6,000 คนทั่วโลกแสดงให้เห็นว่านายจ้างอาจไม่อธิบายให้พนักงานฟังถึงวิธีการหลีกเลี่ยงการตกเป็นเหยื่อของความเสี่ยงเหล่านี้ ผู้ตอบแบบสอบถามอย่างน้อย 73% กล่าวว่าพวกเขาไม่ได้รับการฝึกอบรมการตระหนักรู้ความปลอดภัยทางไซเบอร์เมื่อพวกเขาเริ่มทำงานจากระยะไกล นอกจากนี้ พนักงานมากกว่าหนึ่งในสี่ (27%) ที่ทำการสำรวจระบุว่าได้รับฟิชชิ่งอีเมลในหัวข้อของ COVID-19 การดาวน์โหลดเนื้อหาที่เป็นอันตรายจากอีเมลดังกล่าวโดยไม่ตั้งใจสามารถนำไปสู่อุปกรณ์ที่ติดไวรัสและข้อมูลธุรกิจถูกโจมตี พนักงานหลายคนได้เพิ่มการใช้บริการออนไลน์สำหรับงานที่ไม่ได้รับการอนุมัติจากแผนกไอทีของตนหรือที่รู้จักกันในชื่อระบบไอทีเงา (Shadow IT) เช่น การประชุมทางวิดีโอ (70%) ระบบส่งข้อความ (60%) หรือบริการจัดเก็บไฟล์ (53%)

นายอันเดรย์ แดนเควิช ผู้จัดการฝ่ายการตลาดผลิตภัณฑ์อาวุโส แคสเปอร์สกี้ กล่าวว่า “เป็นการยากที่จะรักษา ‘ธุรกิจตามปกติ’ เมื่อทุกสิ่งจำเป็นต้องเปลี่ยนแปลงอย่างมาก ในขณะที่พนักงานพยายามทำงานให้สอดคล้องกับความเป็นจริงใหม่ของการทำงานจากที่บ้าน ทีมไอทีและความปลอดภัยบนโลกไซเบอร์อยู่ภายใต้แรงกดดัน เพื่อให้พวกเขาทำงานได้อย่างปลอดภัย เหตุการณ์ทางไซเบอร์สามารถเพิ่มความยากลำบากให้กับความท้าทายนี้ได้ดังนั้นจึงเป็นเรื่องสำคัญที่จะต้องระมัดระวังและให้แน่ใจว่าการทำงานจากระยะไกลยังคงปลอดภัยในการทำงาน”

แคสเปอร์สกี้ขอแนะนำมาตรการต่อไปนี้เพื่อช่วยให้ธุรกิจเปิดใช้งานการทำงานระยะไกลที่ปลอดภัยสำหรับพนักงาน:
• ตรวจสอบให้แน่ใจว่าพนักงานของคุณรู้ว่าต้องติดต่อใครหากพวกเขาประสบปัญหาด้านไอทีหรือความปลอดภัย ให้ความสนใจเป็นพิเศษกับพนักงานที่ต้องทำงานจากอุปกรณ์ส่วนบุคคล – ให้นโยบายและคำแนะนำด้านความปลอดภัยแก่พวกเขาโดยเฉพาะ
• กำหนดเวลาการฝึกอบรมความตระหนักด้านความปลอดภัยขั้นพื้นฐานสำหรับพนักงานของคุณ ซึ่งสามารถทำได้ทางออนไลน์ และควรครอบคลุมแนวทางปฏิบัติที่จำเป็นเช่นการจัดการบัญชีและรหัสผ่านความปลอดภัยของอีเมล ความปลอดภัยของอุปกรณ์ปลายทางและการท่องเว็บ แคสเปอร์สกี้ร่วมกับ Area9 Lyceum ได้จัดทำหลักสูตรฟรีเพื่อช่วยให้พนักงานทำงานอย่างปลอดภัยจากที่บ้าน
• ใช้มาตรการป้องกันข้อมูลที่สำคัญเพื่อปกป้องข้อมูลและอุปกรณ์ขององค์กร รวมถึงการเปิดการป้องกันด้วยรหัสผ่านการเข้ารหัสอุปกรณ์ที่ใช้ในการทำงานและมั่นใจได้ว่ามีการสำรองข้อมูล
• ตรวจสอบให้แน่ใจว่าอุปกรณ์ ซอฟต์แวร์ แอปพลิเคชั่น และบริการได้รับการอัพเดตด้วยแพตช์ล่าสุด
• ติดตั้งซอฟต์แวร์ป้องกันที่พิสูจน์แล้ว เช่น Kaspersky Endpoint Security Cloud ในอุปกรณ์ปลายทางทั้งหมด รวมถึงอุปกรณ์มือถือ นอกจากนี้ยังช่วยให้มั่นใจได้ว่ามีการใช้บริการออนไลน์ที่ได้รับการอนุมัติเท่านั้นเพื่อวัตถุประสงค์ในการทำงานลดความเสี่ยงของระบบไอทีเงา

หากต้องการอ่านรายงานแคสเปอร์สกี้ฉบับสมบูรณ์ และเรียนรู้เพิ่มเติมเกี่ยวกับวิธีการแพร่ระบาดของโรคที่มีอิทธิพลต่อการทำงาน กรุณาเยี่ยมชมหน้านี้ https://www.kaspersky.com/blog/report-covid-wfh/35244/