3 อันดับภัยไซเบอร์ใกล้ตัวที่คนไทยถูกหลอกมากที่สุด

หากพูดถึงภัยไซเบอร์ในปัจจุบัน เชื่อว่าหลายคนเคยได้ยินข่าวการโจมตีสถาบันการเงิน ภาคธุรกิจต่าง ๆ หรือหน่วยงานภาครัฐมาบ้างแล้ว แต่ในความเป็นจริงนั้น ภัยไซเบอร์อยู่ใกล้ตัวเรามากกว่าที่คิด คอลัมน์ Financial Wisdom ฉบับนี้ จะพาไปทำความรู้จักภัยไซเบอร์ใกล้ตัวแต่ละประเภทที่ควรรู้ รวมถึงแนะนำวิธีรับมือและป้องกันตนเองจากภัยที่อาจเกิดขึ้น

ภัยประเภทที่ 1 : มิจฉาชีพบน Social Media

ในยุคแห่ง Social Media นั้น เราคงปฏิเสธไม่ได้ว่า เราใช้ชีวิตและทำกิจกรรมต่าง ๆ บนโลกออนไลน์มากขึ้นเมื่อเทียบกับสมัยก่อน ซึ่งมิจฉาชีพเองก็เริ่มใช้ช่องทางดังกล่าวเพื่อแสวงหาผลประโยชน์เช่นเดียวกัน โดยอาศัยข้อมูลจากแชทหรือโพสต์ต่าง ๆ เป็นตัวช่วยในการสวมรอยหรือปลอมแปลงข้อมูลเพื่อหลอกลวงประชาชน ยกตัวอย่างเช่น การส่งข้อความแชทเพื่อหลอกให้โอนเงิน หรือการปลอมแปลงสลิปโอนเงินในการสั่งซื้อสินค้าออนไลน์ ซึ่งถ้าหากเราไม่ระวังอาจทำให้สูญเสียเงิน หรือเสียผลประโยชน์ทางธุรกิจได้

วิธีรับมือและป้องกัน :

1. อย่าหลงเชื่อข้อความผ่านแชทเพื่อขอให้โอนเงินหรือขอข้อมูลใด ๆ หากผู้ส่งข้อความเป็นเพื่อน ควรติดต่อเพื่อนโดยตรงผ่านช่องทางอื่นเพื่อยืนยันตัวตนและจุดประสงค์ก่อน
2. ควรตรวจสอบสลิปโอนเงินจากผู้โอนให้มั่นใจก่อนยืนยันการโอนเงินทุกครั้ง

ภัยประเภทที่ 2 : อีเมลหลอกลวง (Phishing)

ทุกวันนี้ เราทุกคนมีอีเมลเพื่อใช้ในชีวิตประจำวันและสมัครบริการต่าง ๆ บนโลกออนไลน์ จึงไม่ถือเป็นเรื่องแปลกที่เหล่ามิจฉาชีพจะนิยมใช้ช่องทางนี้ในการแสวงหาผลประโยชน์หรือสร้างความเดือดร้อนให้กับประชาชน ซึ่งหนึ่งในกรณีที่พบเห็นบ่อย คือ การส่งอีเมลโดยแอบอ้างเป็นธนาคารพาณิชย์เพื่อหลอกให้ทำธุรกรรม หรือกรอกข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต นอกจากนี้ มิจฉาชีพอาจฝังมัลแวร์ (โปรแกรมมุ่งร้าย) ไว้ในเอกสารแนบของอีเมล ซึ่งหากเปิดไฟล์ดังกล่าว จะทำให้เครื่องคอมพิวเตอร์ของผู้รับเกิดความเสียหายได้ เช่น ไฟล์ต่าง ๆ ถูกยึดเพื่อเรียกค่าไถ่ หรือระบบคอมพิวเตอร์ถูกทำลายจนไม่สามารถใช้งานได้

วิธีรับมือและป้องกัน :

หากได้รับอีเมลต้องสงสัยให้ "คิด" ก่อน "คลิก" ควรตรวจสอบผู้ส่ง เนื้อหา และลิงก์ภายในอีเมลโดยละเอียดก่อนตอบกลับหรือให้ข้อมูลใด ๆ ทุกครั้ง

ภัยประเภทที่ 3 : การขโมยข้อมูลส่วนบุคคล (Data Theft)

สำหรับผู้อ่านที่ติดตามข่าวด้าน Cybersecurity ในช่วงนี้ จะเห็นได้ว่ามีข่าวเว็บไซต์และบริการหลายแห่งถูกแฮกข้อมูล หรือทำข้อมูลรั่วไหลออกมาบ่อยครั้ง ซึ่งรวมถึงเว็บไซต์และบริการสาธารณะที่ประชาชนส่วนใหญ่ใช้อยู่ด้วย โดยข้อมูลที่รั่วไหลมักเป็นข้อมูลสำคัญ เช่น ชื่อบัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลบัตรเครดิต และมิจฉาชีพสามารถใช้ข้อมูลดังกล่าวเข้าถึงบัญชีผู้ใช้งานของเรา หรือกระทำการใดโดยมิชอบในนามของเราได้ เช่น โอนเงินโดยทุจริต

วิธีรับมือและป้องกัน :

1. ไม่ให้ข้อมูลสำคัญกับเว็บไซต์หรือบริการใด ๆหากไม่จำเป็น
2. หมั่นติดตามข่าวสารด้าน Cybersecurity อย่างสม่ำเสมอ หากพบว่ามีข่าวเว็บไซต์หรือบริการที่ท่านใช้งานอยู่ถูกขโมยข้อมูลไป ควรรีบเปลี่ยนรหัสผ่านหรือดำเนินการต่าง ๆ เพื่อป้องกันหรือลดความเสียหายที่อาจเกิดขึ้น เช่น อายัดบัตรเครดิตทันที

จะเห็นได้ว่าภัยไซเบอร์นั้นมีหลากหลายรูปแบบ และอาจส่งผลกระทบต่อตัวเรา ครอบครัว และองค์กรได้โดยไม่ทันตั้งตัว ดังนั้น เราจึงต้องตระหนักรู้และเท่าทันภัยไซเบอร์ตลอดเวลาโดยติดตามข่าวสารอย่างสม่ำเสมอ นอกจากนี้ การอัปเดตอุปกรณ์ต่าง ๆ ให้เป็นเวอร์ชันล่าสุดเพื่ออุดช่องโหว่ด้านความปลอดภัย ก็เป็นสิ่งที่สำคัญเช่นเดียวกัน