“สื่อไซเบอร์วัคซีน” สร้างภูมิคุ้มกันรู้ทันมิจฉาชีพออนไลน์

หากพูดถึงภัยไซเบอร์จาก “มิจฉาชีพออนไลน์” ในปัจจุบัน เชื่อว่าหลายคนเคยได้ยินข่าวการโจมตีสถาบันการเงิน ภาคธุรกิจต่าง ๆ หรือหน่วยงานภาครัฐมาบ้างแล้ว แต่ในความเป็นจริงนั้น ภัยไซเบอร์อยู่ใกล้ตัวเรามากกว่าที่คิด ซึ่งภัยไซเบอร์ใกล้ตัวแต่ละประเภทที่ควรรู้ และวิธีรับมือเพื่อป้องกันตนเองจากภัยที่อาจเกิดขึ้น

ปัจจุบันภัยบนโลกออนไลน์ เป็นอาชญากรรมทางเทคโนโลยีได้มีการพัฒนารูปแบบ และใช้กลโกงที่หลากหลาย ส่งผลกระทบต่อประชาชนและความมั่นคงของประเทศ มีผู้เดือดร้อนและมูลค่าความเสียหายจำนวนมาก ซึ่งที่ผ่านมา ตำรวจได้ดำเนินการทั้งมาตรการป้องกันปราบปราม และประชาสัมพันธ์เผยแพร่ผ่านสื่อต่าง ๆ ทั้งผ่านสื่อดิจิทัลและสื่อสิ่งพิมพ์ แต่ก็ยังคงมีประชาชนหลงเชื่อและตกเป็นเหยื่อ จนต้องสูญเสียเงินเป็นจำนวนมาก

ดังนั้น การเผยแพร่ข้อมูลความรู้ เตือนภัยบนโลกออนไลน์ ถือเป็นไซเบอร์วัคซีนภูมิคุ้มกันให้ประชาชนได้รู้เท่าทันไม่ตกเป็นเหยื่อมิจฉาชีพ โดยคาดหวังจะกระจายไซเบอร์วัคซีนไปยังประชาชนในทุกจังหวัดผ่านช่องทางร้านค้าปลีกร้านค้าส่งของเครือซีพี ได้แก่ ร้าน 7-11 ห้างแม็คโคร และโลตัส เป็นต้น รวมถึงสื่อสารผ่านสถานีข่าว TNN16 และสื่อต่าง ๆ ของกลุ่มโทรคมนาคมและการสื่อสารของเครือฯ

อินเทอร์เน็ตทำให้ชีวิตประจำวันของเราสะดวกสบายมากขึ้น การติดต่อสื่อสารเป็นไปได้โดยง่าย เพื่อนฝูง ญาติพี่น้อง หรือคนไม่รู้จักก็สามารถติดต่อสื่อสารกันได้อย่างรวดเร็ว แต่ความสะดวกสบายนี้ก็มีอันตรายแฝงมาด้วย โดยเป็นเครื่องมือที่ช่วยทำให้มิจฉาชีพที่อยู่ไกลจากเหยื่อสามารถเข้ามาใกล้ชิดหลอกลวงเงินไปจากเหยื่อได้โดยง่ายหากไม่ระมัดระวัง เราลองมาทำความรู้จักกับกลโกงออนไลน์ที่พบบ่อย ๆ กัน

มิจฉาชีพบน Social Media

มิจฉาชีพจะหลอกให้เหยื่อโอนเงินผ่านบริการโอนเงินที่มิจฉาชีพสามารถรับเงินได้โดยไม่ต้องมีเอกสารแสดงตน เพราะยากต่อการติดตาม

หน่วยงานราชการ หรือองค์กรระหว่างประเทศต่าง ๆ ที่ยกตัวอย่างมีหน้าที่ชัดเจน และส่วนใหญ่จะไม่ติดต่อกับประชาชนโดยตรง อย่างไรก็ตาม หากหน่วยราชการใดมีกิจต้องติดต่อกับประชาชน การแจ้งให้ประชาชนดำเนินการใด ๆ จะมีเอกสารหลักฐานเป็นลายลักษณ์อักษร หากมีผู้แอบอ้างว่าเป็นเจ้าหน้าที่เหล่านั้น โดยเฉพาะอย่างยิ่งกรณีต้องมีการโอนเงินหรือชำระเงิน ควรตรวจสอบไปยังหน่วยงานนั้นโดยตรงก่อน โดยไม่ใช้อีเมลหรือหมายเลขโทรศัพท์ที่ได้รับแจ้งมา

วิธีรับมือและป้องกัน อย่าหลงเชื่อข้อความผ่านแชทเพื่อขอให้โอนเงินหรือขอข้อมูลใด ๆ หาก ผู้ส่งข้อความเป็นเพื่อน ควรติดต่อเพื่อนโดยตรงผ่านช่องทางอื่นเพื่อยืนยัน ตัวตนและจุดประสงค์ก่อน ควรตรวจสอบสลิปโอนเงิน และชื่อผู้รับให้มั่นใจก่อนยืนยันการโอนเงินทุกครั้ง

อีเมลหลอกลวง

มิจฉาชีพจะอ้างเป็นผู้ให้บริการบัญชีอีเมลแต่ชื่อบัญชีอีเมล (email address) ที่แสดง จะไม่ใช่ชื่อบัญชีอีเมลของผู้ให้บริการอีเมลจริง นอกจากนั้น ข้อความในอีเมลที่มิจฉาชีพส่งให้เหยื่อคนที่ 2 มักเป็นภาษาอังกฤษหรือเป็นภาษาไทยที่ไม่คุ้นเคย เช่น ใช้สรรพนามต่างจากที่เคยใช้สนทนากันหากได้รับอีเมลต้องสงสัยให้ “คิด” ก่อน “คลิก” ควรตรวจสอบผู้ส่ง เนื้อหาและลิงก์ภายในอีเมลโดยละเอียดก่อนตอบกลับหรือให้ข้อมูลใด ๆ ทุกครั้ง

การขโมยข้อมูลส่วนบุคคล

วิธีรับมือและป้องกันไม่ให้ข้อมูลสำคัญกับเว็บไซต์หรือบริการใด ๆ หากไม่จำเป็น หมั่นติดตามข่าวสารด้าน Cybersecurity อย่างสม่ำเสมอ หากพบว่ามีข่าวเว็บไซต์หรือบริการที่ท่านใช้งานอยู่ถูกขโมยข้อมูลไป ควรรีบเปลี่ยนรหัสผ่านหรือดำเนินการต่าง ๆ เพื่อป้องกันหรือลดความเสียหายที่อาจเกิดขึ้น เช่น อายัดบัตรเครดิตทันที

ขอเลขที่บัญชีเงินฝากเป็นที่พักเงิน

มิจฉาชีพจะประกาศรับสมัครงานผ่านอินเทอร์เน็ต หลอกเหยื่อว่าเป็นบริษัทต่างประเทศที่ขายสินค้าในประเทศไทยเป็นจำนวนมาก จึงขอให้เหยื่อทำหน้าที่เป็นผู้รวบรวมเงินให้ โดยอาจจ่ายค่าจ้างเป็นสัดส่วนกับเงินที่ได้รับ เช่น ร้อยละ 25 ของเงินค่าสินค้า

เมื่อมีเงินโอนเข้าบัญชีของเหยื่อ บริษัทจะแจ้งเหยื่อให้หักค่าจ้างไว้ แล้วโอนเงินที่เหลือทั้งหมดให้แก่บริษัทแม่ในต่างประเทศทันที ผ่านบริการโอนเงินที่ไม่ต้องใช้เอกสารแสดงตน โดยที่เหยื่อไม่รู้เลยว่า เงินที่โอนเข้ามาในบัญชีเหยื่อนั้นเป็นเงินผิดกฎหมายที่มิจฉาชีพหลอกให้คนอื่นโอนมาให้ กว่าเหยื่อจะรู้ตัวก็อาจเป็นตอนที่พนักงานธนาคารติดต่อเพื่ออายัดบัญชีของเหยื่อหรือถูกตำรวจจับแล้ว

โฆษณาปล่อยเงินกู้นอกระบบ

มิจฉาชีพแอบอ้างเป็นผู้ให้บริการเงินกู้แล้วโฆษณาผ่านเว็บไซต์ต่าง ๆ หรือส่งอีเมลหาเหยื่อโดยตรงว่าให้บริการเงินกู้นอกระบบ ดอกเบี้ยต่ำ อนุมัติเงินเร็ว ไม่ต้องซื้อสินค้า ไม่ตรวจสอบเครดิตบูโร เมื่อเหยื่อติดต่อไปและขอกู้เงิน ผู้ให้กู้จะอ้างว่าจะส่งสัญญาให้กับผู้ขอกู้เพื่อลงลายมือชื่อ พร้อมทั้งขอให้เหยื่อโอนเงินชำระค่าทำสัญญา ค่าเอกสาร ค่ามัดจำ หรือดอกเบี้ยภายในเวลาที่กำหนด เช่น ก่อน 18.00 น. เพื่อผู้ให้กู้จะโอนเงินกู้ให้ก่อนเวลา 20.00 น. โดยสามารถยกเลิกและขอเงินโอนล่วงหน้าดังกล่าวคืนได้

เหยื่อส่วนมากมักจะรีบร้อน และกลัวว่าจะไม่ได้เงินกู้ จึงรีบโอนเงินให้กับผู้ให้กู้ในเวลาที่กำหนด แต่เมื่อติดต่อกลับผู้ให้กู้เพื่อขอรับเงินกู้ กลับไม่สามารถติดต่อผู้ให้กู้ได้อีกเลย และสูญเงินไปโดยไม่มีโอกาสได้เงินคืน

วิธีป้องกันเปิดเผยข้อมูลในโซเชียลเน็ตเวิร์กเท่าที่จำเป็น เพื่อป้องกันไม่ให้มิจฉาชีพนำข้อมูลไปแอบอ้างใช้ทำธุรกรรมควรเปลี่ยนรหัสผ่าน (password) ในการเข้าใช้บัญชีอีเมลหรือบัญชีโซเชียลเน็ตเวิร์กเป็นประจำ เมื่อได้รับการติดต่อแจ้งให้โอนเงินให้ควรตรวจสอบข้อเท็จจริงก่อนโอนเงิน เช่น ติดต่อหน่วยงานที่ถูกอ้างถึงโดยตรง อาทิ กรมศุลกากร โทร. 1164 ธนาคารแห่งประเทศไทย โทร. 1213 หรือสำนักงานตัวแทนในประเทศไทยของหน่วยงานต่างชาติ

ไม่โลภต่อเงินที่ไม่มีที่มา หรือผลตอบแทนที่สูงเกินจริง ควรพิจารณาให้รอบคอบถึงความเป็นไปได้ในความเป็นจริงตรวจหาไวรัสในเครื่องคอมพิวเตอร์เป็นประจำ เพื่อป้องกันการขโมยข้อมูลการใช้งาน และติดตามข่าวสารกลโกงอย่างสม่ำเสมอ

จะเห็นได้ว่าภัยไซเบอร์จาก “มิจฉาชีพออนไลน์” นั้นมีหลากหลายรูปแบบ และอาจส่งผลกระทบต่อตัวเราครอบครัว และองค์กรได้โดยไม่ทันตั้งตัว ดังนั้น เราจึงต้องตระหนักรู้และเท่าทันภัยไซเบอร์ตลอดเวลาโดยติดตามข่าวสารอย่างสม่ำเสมอ นอกจากนี้ การอัปเดตอุปกรณ์ต่าง ๆ ให้เป็นเวอร์ชันล่าสุดเพื่ออุดช่องโหว่ด้านความปลอดภัย ก็เป็นสิ่งที่สำคัญเช่นเดียวกัน