บทความ

ภัยไซเบอร์ใกล้ตัววัยเริ่มทำงาน: รู้ทันกลโกง สังเกตให้เป็น ป้องกันได้

ในยุคที่การทำธุรกรรมทางการเงินและการสื่อสารเกิดขึ้นผ่านช่องทางดิจิทัลเป็นหลัก กลุ่มวัยเริ่มทำงาน ซึ่งมีอายุระหว่าง ๒๒ – ๒๙ ปี ถือหนึ่งในกลุ่มเสี่ยงที่มีความเสี่ยงสูงต่อการตกเป็นเหยื่อของมิจฉาชีพออนไลน์ เนื่องจากกลุ่มนี้มีทั้งรายได้ประจำ บัญชีธนาคาร และความคุ้นเคยกับเทคโนโลยีที่ทำให้เชื่อมั่นในการทำธุรกรรมออนไลน์มากจนเกินไป จากข้อมูลของสำนักงานตำรวจแห่งชาติและสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พบว่ามูลค่าความเสียหายจากภัยไซเบอร์ในประเทศไทยเพิ่มสูงขึ้นอย่างต่อเนื่องทุกปี บทความนี้จึงมุ่งนำเสนอความรู้เชิงปฏิบัติเพื่อให้ผู้อ่านสามารถรับมือกับภัยได้อย่างยั่งยืนและมีประสิทธิภาพ

๑. รูปแบบการหลอกลวงที่วัยเริ่มทำงานมักตกเป็นเหยื่อ มิจฉาชีพออนไลน์มีการพัฒนารูปแบบการหลอกลวงอย่างต่อเนื่องเพื่อให้สอดคล้องกับพฤติกรรมของกลุ่มเป้าหมาย รูปแบบที่พบบ่อยในกลุ่มวัยเริ่มทำงาน มีดังต่อไปนี้

๑.๑ การหลอกลวงผ่านงานออนไลน์รายได้ดี

มิจฉาชีพจะใช้โฆษณาชักชวนให้ทำงานออนไลน์ที่มีลักษณะเรียบง่าย เช่น การกดไลก์โพสต์ การรีวิวสินค้าหรือการกดซื้อสินค้าเพื่อรับค่าตอบแทน โดยอ้างว่าสามารถทำได้จากที่บ้าน และมีรายได้ ๕๐๐ - ๒,๐๐๐ บาทต่อวัน กระบวนการหลอกลวงมักดำเนินการดังนี้ เริ่มต้นให้เหยื่อทำงานและได้รับเงินในระยะแรก เพื่อสร้างความน่าเชื่อถือ หลังจากนั้นมักจะให้เหยื่อโอนเงินค้ำประกันหรือทำออเดอร์และรอเงินคืน โดยอ้างว่าจะโอนคืนในภายหลัง ท้ายสุดเมื่อเหยื่อโอนเงินก้อนใหญ่มิจฉาชีพจะหายตัวไปโดยไม่สามารถติดต่อได้

๑.๒ การโจมตีแบบฟิชชิ่ง

ฟิชชิ่งเป็นการส่งอีเมลหรือข้อความแจ้งเตือนปลอมที่แอบอ้างเป็นหน่วยงานที่น่าเชื่อถือ เช่น ธนาคารหรือบริษัทขนส่งพัสดุ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัวหรือรหัสผ่าน นอกจากนี้มิจฉาชีพยังสร้างเว็บไซต์ปลอมที่ใช้ในการหลอกลวงมักออกแบบให้มีหน้าตาคล้ายกับเว็บจริง จึงจำเป็นที่จะต้องตรวจสอบลิงก์ URL อย่างละเอียดทุกครั้ง รูปแบบที่พบบ่อย ได้แก่ อีเมลแจ้งเตือนว่าบัญชีธนาคารจะถูกระงับ พร้อมลิงก์ให้ยืนยันตัวตน ข้อความแจ้งเตือนมีเนื้อหาว่ามีพัสดุรอรับ ให้กดลิ้งก์เพื่อชำระค่าธรรมเนียมหรือค่าปรับ และอีเมลที่อ้างว่ามีเงินคืนภาษีมักจะให้กรอกข้อมูลบัญชีธนาคารเพื่อรับเงิน

๑.๓ การแอบอ้างเป็นบุคคลที่รู้จัก

มิจฉาชีพจะเจาะเข้าบัญชี LINE หรือ Facebook ของบุคคลที่เหยื่อรู้จัก จากนั้นส่งข้อความขอยืมเงินโดยอ้างเหตุฉุกเฉิน วัยเริ่มทำงานมักตกเป็นเหยื่อของรูปแบบนี้เนื่องจากความไว้วางใจที่มีต่อบุคคลที่รู้จักและไม่ต้องการเสียน้ำใจด้วยการให้ยืมเงินโดยขาดการไตร่ตรองและพิจารณาอย่างรอบคอบ

๑.๔ การหลอกลวงด้านการลงทุน

มิจฉาชีพมักจะชักชวนให้ลงทุนในสินทรัพย์ดิจิทัล หุ้น หรือสินทรัพย์อื่นๆ โดยสัญญาว่าจะได้รับผลตอบแทนสูงผิดปกติ เช่น ๒๐ – ๓๐% ต่อเดือน กลโกงประเภทนี้มีความซับซ้อนสูงขึ้น โดยสร้างแอปพลิเคชัน หรือเว็บไซต์ปลอมที่มีหน้าแดชบอร์ดแสดงผลกำไรที่สมจริง เพื่อสร้างความน่าเชื่อถือในระยะแรกก่อนที่เหยื่อจะโอนเงินก้อนใหญ่

๑.๕ การหลอกลวงทางอารมณ์

มิจฉาชีพมักจะสร้างโปรไฟล์ปลอมของบุคคลที่มีรูปลักษณ์ดีในแพลตฟอร์มสังคมออนไลน์หรือในแอปพลิเคชันหาคู่ จากนั้นสร้างความสัมพันธ์อย่างค่อยเป็นค่อยไป เป็นระยะเวลาประมาณ ๑ - ๓ เดือน ก่อนจะขอให้โอนเงินด้วยเหตุผลต่างๆ หรือชักชวนให้ลงทุนร่วมกัน กลุ่มวัยเริ่มทำงานที่ต้องการสร้างความสัมพันธ์ใหม่มักตกเป็นเป้าหมายของกลโกงประเภทนี้

/๒. ข้อสังเกต...

๒. ข้อสังเกตและสัญญาณเตือนภัย

การรู้จักสังเกตสัญญาณเตือนเป็นหลักสำคัญในการป้องกันตนเองจากภัยไซเบอร์ข้อสังเกตที่ควรระวังมีดังต่อไปนี้

๒.๑ การสร้างความเร่งด่วน

มิจฉาชีพมักใช้กลยุทธ์กดดันให้เหยื่อตัดสินใจอย่างรวดเร็ว โดยใช้ภาษาที่แสดงความเร่งด่วน เช่น ด่วนมาก หมดเวลาภายใน ๒๔ ชั่วโมง หรือโอกาสสุดท้าย วัตถุประสงค์หลักคือการป้องกันไม่ให้เหยื่อมีเวลาคิดพิจารณาอย่างรอบคอบ

๒.๒ ผลตอบแทนที่สูงผิดปกติ

ข้อเสนอใดก็ตามที่สัญญาผลตอบแทนสูงกว่าความเป็นจริงอย่างมีนัยสำคัญ ควรได้รับการพิจารณาอย่างระมัดระวัง โดยอัตราดอกเบี้ยของธนาคารพาณิชย์อยู่ที่ประมาณ ๑ – ๒% ต่อปี และกองทุนรวมส่วนใหญ่มักให้ผลตอบแทนเฉลี่ย ๑๐ – ๑๕% ต่อปี ดังนั้นข้อเสนอที่อ้างผลตอบแทน ๒๐% ขึ้นไปต่อเดือนจึงเป็นสัญญาณเตือนที่ชัดเจนว่ามีความเป็นไปได้ว่าอาจเป็นมิจฉาชีพ

๒.๓ ลิงก์และที่อยู่เว็บไซต์ที่ผิดปกติ

เว็บไซต์ปลอมมักใช้ชื่อโดเมนที่คล้ายกับเว็บจริงแต่มีความแตกต่างเล็กน้อย ตัวอย่างเช่น เว็บไซต์จริงของกรมคือ www.dla.go.th ในทางกลับกันเว็บไซต์ปลอมที่อาจพบเห็นจะมีลักษณะดังนี้ www.dla.go.th-secure.com โดยมีการใส่คำว่า -secure เพิ่มเติมทำให้น่าเชื่อถือมากยิ่งขึ้น ดังนั้น ผู้ใช้งานควรตรวจสอบลิงก์ URL อย่างละเอียดทุกครั้งก่อนกรอกข้อมูล

๒.๔ การขอข้อมูลที่เป็นความลับ

สถาบันการเงินและหน่วยงานภาครัฐที่ถูกกฎหมายจะไม่มีการขอรหัสผ่าน หมายเลข PIN รหัส OTP หรือข้อมูลส่วนตัวที่ละเอียดอ่อนผ่านทางโทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือข้อความแจ้งเตือน การร้องขอข้อมูลเหล่านี้ผ่านช่องทางดังกล่าวถือเป็นข้อความจากมิจฉาชีพที่ชัดเจน

๒.๕ โปรไฟล์ออนไลน์ที่ผิดสังเกต

บัญชีออนไลน์ที่มีรูปโปรไฟล์สวยงามเกินจริง มีจำนวนเพื่อนหรือผู้ติดตามน้อยมีประวัติการโพสต์น้อย หรือเพิ่งสร้างบัญชีใหม่ ควรได้รับการตรวจสอบเพิ่มเติมและพิจารณาอย่างรอบคอบว่าเป็นมิจฉาชีพหรือไม่

๓. แนวทางการป้องกันตนเองจากภัยไซเบอร์

การป้องกันภัยไซเบอร์อย่างมีประสิทธิภาพ ต้องอาศัยทั้งความรู้ความเข้าใจและการปฏิบัติอย่างสม่ำเสมอ แนวทางที่แนะนำมีดังต่อไปนี้

๓.๑ เปิดใช้งานการยืนยันตัวตนสองขั้นตอน

การยืนยันตัวตนสองขั้นตอนเป็นมาตรการรักษาความปลอดภัย ที่กำหนดให้ผู้ใช้ต้องยืนยันตัวตนด้วยวิธีสองวิธีที่แตกต่างกัน เช่น รหัสผ่านร่วมกับรหัส OTP จาก Application บนโทรศัพท์มือถือ แม้มิจฉาชีพจะทราบรหัสผ่าน แต่ไม่สามารถเข้าถึงบัญชีได้หากไม่มีโทรศัพท์ของเจ้าของบัญชี

๓.๒ การจัดการรหัสผ่านอย่างปลอดภัย

การจัดการรหัสผ่านที่ดีเป็นพื้นฐานสำคัญของความปลอดภัยทางไซเบอร์ โดยมีหลักการดังต่อไปนี้ ใช้รหัสผ่านที่มีความยาวอย่างน้อย ๑๒ ตัวอักษร ประกอบด้วยตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ ไม่ใช้รหัสผ่านเดิมซ้ำกันในหลายแพลตฟอร์ม และไม่ใช้ข้อมูลส่วนตัวที่คาดเดาได้ง่าย เช่น วันเกิด ชื่อ หรือหมายเลขโทรศัพท์

/๓.๓ การตรวจสอบ...

๓.๓ การตรวจสอบก่อนคลิกลิงก์

ก่อนกดลิงก์ที่ได้รับทางไปรษณีย์อิเล็กทรอนิกส์ ข้อความแจ้งเตือน หรือแพลตฟอร์มโซเชียลมีเดีย ควรตั้งคำถามดังต่อไปนี้

(๑) ตรวจสอบว่าเราได้สมัครใช้บริการหรือสั่งซื้อสินค้าที่เกี่ยวข้องกับข้อความนี้หรือไม่ และลิงก์ URL ปลายทางตรงกับลิงก์ของหน่วยงานจริงหรือไม่

(๒) กรณีตรวจสอบตามข้อ (๑) แล้วยังไม่ชัดเจนให้เปิดเว็บเบราว์เซอร์ และพิมพ์ที่อยู่เว็บไซต์โดยตรงแทนการกดลิงก์

๓.๔ การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ

การอัปเดตซอฟต์แวร์เป็นการปิดช่องโหว่ด้านความปลอดภัยที่อาจถูกมิจฉาชีพนำไปใช้โจมตีระบบ แนะนำให้ตั้งค่าการอัปเดตอัตโนมัติสำหรับระบบปฏิบัติการ แอปพลิเคชันธนาคาร และซอฟต์แวร์ที่ใช้งานประจำ

๓.๕ การตรวจสอบธุรกรรมทางการเงินก่อนดำเนินการ

เมื่อได้รับคำขอให้โอนเงินหรือดำเนินธุรกรรมทางการเงิน ไม่ว่าจะเป็นบุคคลที่รู้จักหรือหน่วยงานใดก็ตาม ควรดำเนินการตามขั้นตอนดังต่อไปนี้

(๑) ติดต่อผู้ส่งข้อความโดยตรงผ่านหมายเลขโทรศัพท์ที่ทราบอยู่แล้ว ไม่ใช่หมายเลขที่ระบุในข้อความ

(๒) ในกรณีที่เป็นธุรกรรมกับสถาบันการเงิน ให้ติดต่อสอบถามโดยตรงผ่านหมายเลขที่ระบุไว้ด้านหลังบัตรเดบิตหรือเครดิต และสำหรับธุรกรรมที่มีมูลค่าสูง ควรพิจารณาดำเนินการที่สาขาธนาคารโดยตรง

๓.๖ ความระมัดระวังในการใช้เครือข่ายสาธารณะ

เครือข่าย Wi-Fi สาธารณะมีความเสี่ยงสูงต่อการถูกดักจับข้อมูล ควรหลีกเลี่ยงการทำธุรกรรมทางการเงินหรือการกรอกข้อมูลส่วนตัวที่ละเอียดอ่อนบนเครือข่ายดังกล่าว หากจำเป็นต้องใช้เครือข่ายสาธารณะ ควรเปลี่ยนไปใช้เครือข่ายโทรศัพท์มือถือแทน

โดยสรุป ภัยไซเบอร์เป็นปัญหาที่มีความซับซ้อนและพัฒนาอย่างต่อเนื่อง การป้องกันตนเองอย่างมีประสิทธิภาพต้องอาศัยความรู้ความเข้าใจเกี่ยวกับรูปแบบการหลอกลวง ความสามารถในการสังเกตสัญญาณเตือน และการปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างสม่ำเสมอ วัยเริ่มทำงานควรตระหนักว่า การหยุดคิดวิเคราะห์ก่อนดำเนินการทางดิจิทัล โดยเฉพาะอย่างยิ่งในกรณีที่เกี่ยวข้องกับการเงิน เป็นกลยุทธ์ที่มีประสิทธิภาพสูงสุดในการป้องกันภัยไซเบอร์ การรู้เท่าทันมิจฉาชีพเป็นทักษะที่ทุกคนสามารถพัฒนาได้ และการแบ่งปันความรู้ดังกล่าวให้แก่คนรอบข้าง จะช่วยลดความเสียหายที่เกิดจากภัยไซเบอร์ในสังคมโดยรวมได้อย่างยั่งยืน คาถาป้องกันมิจฉาชีพยุคดิจิทัลที่ดีที่สุดคือ **“ไม่เชื่อ – ไม่รีบ – ไม่โอน” การไม่เชื่อ** คือการพิจารณาอย่างถี่ถ้วนก่อนกระทำการสิ่งใดสิ่งหนึ่ง แม้จะอ้างตัวเป็นเจ้าหน้าที่รัฐขู่ว่ามีพัวพันคดี หรือแจ้งว่าได้รับสิทธิพิเศษ **การไม่รีบ** มักมาพร้อมความกลัวและความโลภ ให้เวลาในการตรวจสอบข้อเท็จจริง อย่ากดลิงก์หรือโอนเงินในทันที **การไม่โอน** คือการตรวจสอบชื่อบัญชีปลายทางทุกครั้ง และปฏิเสธการโอนเงินให้บัญชีบุคคลธรรมดาในการซื้อสินค้าหรือติดต่อราชการ การตรวจสอบให้มั่นใจคือการโทรกลับไปสอบถามหน่วยงานต้นสังกัดด้วยเบอร์ทางการ หรือติดต่อสถานีตำรวจใกล้บ้าน เพื่อสร้างภูมิคุ้มกันภัยหลอกลวงทางออนไลน์อย่างยั่งยืนและมีประสิทธิภาพ

บรรณานุกรม

กรมส่งเสริมการปกครองท้องถิ่น. (2569). รู้ทันกลโกงมิจฉาชีพ ป้องกันภัยไซเบอร์ เริ่มต้นที่ตัวเรา: รูปแบบมิจฉาชีพที่พบบ่อยตามช่วงวัย พร้อมแนวทางการป้องกันภัย. เผยแพร่โดยเทศบาลตำบลหลุบ. สืบค้นจาก https://www.lub.go.th/news-6-5-2569-1/

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.). (2566). ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.). สำนักงานตำรวจแห่งชาติ. สืบค้นจาก https://thaipoliceonline.com

ไทยพีบีเอส. (2567, 29 กรกฎาคม). เผยสถิติอาชญากรรมไซเบอร์ ผู้เสียหายส่วนใหญ่เป็นหญิงวัยทำงาน. สืบค้นจาก https://www.thaipbs.or.th/news/content/342472

ธนาคารแห่งประเทศไทย. (2566). อัตราดอกเบี้ยเงินฝากและเงินให้สินเชื่อของธนาคารพาณิชย์. สืบค้นจาก https://www.bot.or.th/th/statistics/interest-rate.html

สำนักงานตำรวจแห่งชาติ. (2566, 9 กรกฎาคม). หลอกลงทุนระบาดหนัก! ตร. เตือนต้องมีสติ "ไม่เชื่อ ไม่รีบ ไม่โอน". อินโฟเควสท์. สืบค้นจาก https://www.infoquest.co.th/2023/316436

สำนักงานปลัดกระทรวงกลาโหม. (2568, 26 ธันวาคม). 5 กลโกงมิจฉาชีพยอดฮิต และวิธีป้องกัน. กรมประชาสัมพันธ์. สืบค้นจาhttps://www.prd.go.th/th/content/category/detail/id/39/iid/459323

เดลินิวส์. (2568, 31 พฤษภาคม). อย่าโอนก่อนเด็ดขาด! ระวัง 6 กลโกงยอดฮิตจากมิจฉาชีพออนไลน์. สืบค้นจาก https://www.dailynews.co.th/news/4765954/