TB-CERT
Thailand Banking Sector CERT

ANNUAL REPORT 2023

รายงานประจำปี 2566
ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
สมาคมธนาคารไทย

TB-CERT

Thailand Banking Sector CERT

รายงานประจำปี
Annual Report 2023

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
Thailand Banking Sector CERT: TB-CERT

จัดทำโดย

ดร.กิตติ โฆษะวิสุทธิ์

ธาวินี วงศ์วิศว์

ปรมินทร์ ช่วงมณี

ชญานิน แก้วหาญ

ณิชากร ตั้งบวรพิเชฐ

จัดการออกแบบ

นภัสสร แก้วบุญสม

ที่ปรึกษา

ดร.กิตติ โฆษะวิสุทธิ์

บรรณาธิการ

ธาวินี วงศ์วิศว์

ศูนย์ประสานงานด้านความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
สมาคมธนาคารไทย

5/13 หมู่ 3 ถนนแจ้งวัฒนะ ตำบลคลองเกลือ อำเภอปากเกร็ด จังหวัดนนทบุรี 11120
โทร 0 2558 7500 E-mail: contact@tb-cert.or.th

เผยแพร่เมื่อ

มีนาคม 2024
TLP:CLEAR

TB-CERT

Thailand Banking Sector CERT

รายงานประจำปี TB-CERT 2023

สารบัญ

เกี่ยวกับ TB-CERT

เกี่ยวกับ TB-CERT

ความเป็นมา

Thailand Banking Sector Computer Emergency Response Team หรือ TB-CERT จัดตั้งขึ้นโดยความเห็นชอบของผู้บริหารระดับสูงของธนาคารพาณิชย์ในประเทศไทย เพื่อสนับสนุนให้สมาชิกกลุ่มซึ่งเป็นพนักงานของธนาคารได้มีการแลกเปลี่ยนข้อมูลและประสบการณ์เพื่อประโยชน์โดยรวมของสถาบันการเงินในประเทศไทย โดยเฉพาะเพื่อการนำไปใช้ในการป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจจะมีผลกระทบกับการบริการ ทรัพยากร หรือบุคลากรขององค์กร โดยจะไม่เสนอความเห็นต่อผลิตภัณฑ์ทางการเงิน (Product) หรือให้ข้อมูลเชิงลบต่อหน่วยงานหรือบุคคลที่สาม อันจะทำให้เกิดความเสื่อมเสียและเป็นอุปสรรคต่อกิจกรรมการแลกเปลี่ยนความคิดเห็นหรือความสัมพันธ์อันดีของสมาชิกในกลุ่ม

ค่านิยมหลัก

TB-CERT เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลในด้านความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์รวมของบุคลากรที่มีความชำนาญด้านไซเบอร์ และเป็นแหล่งให้ความรู้และสร้างความตระหนักในการระวังภัยที่อาจเกิดขึ้นได้ทุกเมื่อ ไม่ว่าจะเกิดกับบุคลากร ลูกค้า หรือธุรกิจของธนาคาร รวมถึงเป็นศูนย์กลางในการติดต่อสื่อสารกับองค์กรที่เกี่ยวข้องทั้งในและต่างประเทศ เพื่อให้สามารถรับรู้ข่าวสารและช่วยเหลือในการแก้ปัญหาภัยไซเบอร์ที่เกิดขึ้นกับสมาชิก ทั้งนี้เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์และพร้อมรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ

การดำเนินงาน

การดำเนินงานของ TB-CERT จะครอบคลุม 4 ด้านที่สำคัญคือ

1. **เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูล** ทั้งภัยคุกคามด้านไซเบอร์และแนวทางการแก้ไข
2. **สร้างมาตรฐานกลางด้านความมั่นคงปลอดภัย** ของการใช้เทคโนโลยีใหม่
3. **กำหนดกระบวนการในการรับมือภัยไซเบอร์ภาคการธนาคาร** และจัดให้มีการซ้อมรับมือร่วมกันอย่างสม่ำเสมอ
4. **ส่งเสริมการพัฒนาบุคลากรด้าน Cybersecurity** โดยครอบคลุมทั้งการสร้างบุคลากรใหม่เข้าสู่ภาคการเงิน และพัฒนาบุคลากรของสถาบันการเงินให้มีความรู้ความเข้าใจ และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

คำนิยม

คำนิยม

โดย

ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ในยุคดิจิทัลที่ธุรกรรมทางการเงินเกิดขึ้นได้ในพริบตาและข้อมูลต่าง ๆ สามารถถ่ายเทหากันได้ภายในเวลาไม่กี่วินาที ความมั่นคงปลอดภัยทางไซเบอร์ในภาคการเงินการธนาคารจึงเป็นแกนหลักที่รวบรวมความไว้วางใจ ความมั่นคง และความยั่งยืนของระบบการเงินไว้ด้วยกัน อย่างไรก็ตาม เป็นเรื่องที่หลีกเลี่ยงไม่ได้ที่ภาคการเงินการธนาคารจะตกเป็นเป้าหมายสำคัญของการโจมตีทางไซเบอร์ซึ่งเป็นเรื่องที่เกิดขึ้นทั่วโลก และการที่จะต่อสู้กับภัยคุกคามเหล่านี้จำเป็นจะต้องมีความร่วมมือระหว่างสถาบันการเงิน หน่วยงานภาครัฐ และผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ ในการแบ่งปันข้อมูลและความเชี่ยวชาญร่วมกันเพื่อให้เท่าทันและสามารถป้องกันภัยจากผู้ที่ประสงค์ร้าย

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ยังยืนสำหรับภาคการเงินการธนาคารจึงเป็นสิ่งที่จำเป็น เนื่องด้วยเป็นสิ่งที่เกี่ยวเนื่องกับการปกป้องความมั่นคงของเศรษฐกิจ การปกป้องสินทรัพย์ที่ได้มาอย่างยากลำบากของบุคคลรวมทั้งผู้ประกอบธุรกิจเพื่อสร้างความมั่นใจให้กับระบบการเงินของเรา เราจึงจำเป็นต้องปรับตัว สร้างสรรค์นวัตกรรม และทำงานร่วมกัน เพื่อที่จะสร้างความมั่นคงแข็งแกร่งและอยู่ในสถานะก้าวนำหน้าผู้ไม่หวังดีที่คอยจะใช้ประโยชน์จากช่องโหว่อยู่เสมอ ดังนั้น เมื่อเราก้าวสู่ยุคดิจิทัลมากยิ่งขึ้น ความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืนจะเป็นกุญแจสำคัญในการเสริมสร้างความเชื่อมโยงระหว่างความแข็งแกร่งของระบบการเงินและการรับประกันความปลอดภัยทางเศรษฐกิจ ทั้งสำหรับเราในปัจจุบันและรุ่นลูกหลานในอนาคต

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ให้ความสำคัญสูงสุดกับการแก้ไขปัญหากลโกงออนไลน์และภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งการแก้ปัญหาในลักษณะเชิงรุก โดยสร้างความร่วมมืออย่างแข็งขันทั้งกับภาคธนาคารและโทรคมนาคมในการจัดการกับความท้าทายที่เกิดจากการหลอกลวงออนไลน์ เราได้ริเริ่มและต่อยอดมาตรการ รวมทั้งกลยุทธ์ในการต่อสู้กับกลโกงออนไลน์ ไม่ว่าจะเป็นการป้องกัน สกัดกั้น และปราบปราม และด้วยพระราชกำหนดมาตรการป้องกันอาชญากรรมทางเทคโนโลยีฉบับใหม่ที่มีผลบังคับใช้เมื่อเดือนมีนาคม 2566 ที่ผ่านมา มีส่วนช่วยเหลือแก่ผู้ตกเป็นเหยื่อ ธนาคาร และเจ้าหน้าที่ในการดำเนินการมากขึ้นเพื่อระงับเหตุได้อย่างทันท่วงที ทำให้ภาคธนาคารและเจ้าหน้าที่รัฐดำเนินขั้นตอนต่าง ๆ เพื่อระงับเหตุร่วมกันได้อย่างสะดวกรวดเร็ว มีแนวโน้มที่จะป้องกันภัยจากการหลอกลวงออนไลน์ได้มากขึ้น ประกอบกับการเผยแพร่และสร้างความตระหนักรู้ของทุกภาคส่วนไปยังประชาชน ทำให้ทุกคนมีภูมิคุ้มกันที่แข็งแกร่งขึ้นในการต่อสู้กับภัยออนไลน์ และตลอดระยะเวลาที่ผ่านมา ศูนย์ประสานงานด้านความมั่งคงปลอดภัยไซเบอร์ภาคการธนาคาร หรือ TB-CERT ภายใต้สมาคมธนาคารไทย ซึ่งเป็นแหล่งรวบรวมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ ก็เป็นหนึ่งในกลไกสำคัญที่ร่วมป้องกัน ประสานงาน และหาแนวทางปฏิบัติที่ดีที่สุดเพื่อก้าวไปสู่ความมั่นคงปลอดภัยทางไซเบอร์ที่ยั่งยืนในประเทศไทย ตลอดจนส่งเสริมความร่วมมือและแนวทางปฏิบัติที่ดีระหว่างภาครัฐและเอกชนต่อไป

คำนิยม

โดย

คุณผยง ศรีวณิช

กรรมการผู้จัดการใหญ่ ธนาคารกรุงไทย
และประธานสมาคมธนาคารไทย

ด้วยความก้าวหน้าทางเทคโนโลยีที่นำสมัย ประกอบกับอาชญากรนั้นมีการพัฒนารูปแบบการก่ออาชญากรรมอย่างต่อเนื่องโดยอาศัยประโยชน์จากเทคโนโลยีและนำมาใช้ในการกระทำผิด ก่อให้เกิดประเด็นความมั่นคงปลอดภัยทางไซเบอร์ซึ่งถือเป็นเรื่องที่สำคัญและเร่งด่วน ส่งผลให้การรักษาความมั่นคงปลอดภัยให้กับธนาคารถือเป็นสิ่งสำคัญ และนั่นเป็นเหตุผลที่ศูนย์ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคาร หรือ TB-CERT ได้จัดตั้งขึ้นภายใต้สมาคมธนาคารไทย ซึ่งได้รับการสนับสนุนการดำเนินงานจากทุกภาคส่วน ไม่ว่าจะเป็นธนาคารแห่งประเทศไทย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวมถึงสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้การดำเนินงานเป็นไปตามภารกิจและเป้าหมายของ TB-CERT

ปัจจุบันการโจมตีทางไซเบอร์และการฉ้อโกงออนไลน์ ได้เข้าใกล้ตัวเราและเพิ่มมากขึ้นอย่างเห็นได้ชัด ทั้งในแง่ของความถี่และผลกระทบที่เกิดขึ้น แม้ว่าความก้าวหน้าทางเทคโนโลยีเช่น Generative AI ที่ได้นำมาซึ่งความสะดวกสบายและศักยภาพในการดำรงชีวิต แต่ในขณะเดียวกันก็ก่อให้เกิดความเสี่ยงจากผู้อาชญากรทางไซเบอร์ที่สร้างความเดือดร้อนแก่ผู้ใช้งานโดยใช้กลโกงที่ซับซ้อน รุนแรง ซึ่งภัยคุกคามเหล่านี้ส่งผลกระทบอย่างกว้างขวางในระดับชาติ โดยเฉพาะอย่างยิ่งผลกระทบต่อบุคคลซึ่งเป็นลูกค้าของธนาคารและธุรกิจอื่น ๆ ดังนั้น หลายภาคส่วนจึงมีส่วนเกี่ยวข้องในการรับมือกับขั้นตอนต่าง ๆ ของการฉ้อโกงออนไลน์เหล่านี้ และทุกฝ่ายจำเป็นต้องร่วมมือกันทำหน้าที่เพื่อรับผิดชอบในการปกป้องประชาชนและสังคม ไม่ว่าจะเป็นภาครัฐ เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจกรรมโทรคมนาคมแห่งชาติ สำนักงานตำรวจแห่งชาติ และภาคธนาคาร เพื่อรับมือกับกระบวนการของกลโกงที่ซับซ้อนขึ้น ส่งผลให้กระบวนการตอบสนองและตรวจจับ รวมถึงการบังคับใช้กฎหมายที่ต้องมีความซับซ้อนและแข็งแกร่งมากยิ่งขึ้น

ด้วยความตระหนักถึงความท้าทายเหล่านี้ ภาคการธนาคาร ภาคโทรคมนาคม และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ จึงได้ร่วมกันเสริมความแข็งแกร่งโดยการพัฒนาด้านเทคโนโลยีและสร้างนวัตกรรมใหม่ ๆ อย่างต่อเนื่อง ทั้งนี้เพื่อให้เกิดการทำงานที่สอดประสานดียิ่งขึ้นให้และรวดเร็วในการตอบสนอง อีกทั้งยังเป็นการยกระดับความรู้ทางด้านเทคโนโลยีและนวัตกรรมในการตรวจจับและป้องกันภัยออนไลน์ด้วยระบบสำหรับตรวจจับธุรกรรมที่น่าสงสัย และช่วยให้การสื่อสารระหว่างภาคส่วนต่าง ๆ รวดเร็วยิ่งขึ้น ทำให้เราสามารถหยุดอาชญากรรมที่อาจเกิดขึ้นก่อนที่จะบานปลายและสามารถควบคุมความเสียหายไว้ได้ ซึ่งสมาคมธนาคารไทยเองอยู่ระหว่างการพัฒนาระบบ Central Fraud Registry โดยแพลตฟอร์มนี้จะช่วยให้สามารถติดตามและแชร์ข้อมูลกิจกรรมที่เข้าข่ายว่าเป็นการทุจริต เป็นการนำเทคโนโลยีมาช่วยตรวจจับและป้องกันความเสียหายก่อนที่จะเกิดขึ้น นอกจากนี้ การที่ภาครัฐได้แก่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ให้ความสำคัญกับประเด็นดังกล่าวและมีบทบาทสำคัญในกระบวนการบังคับใช้กฎหมายโดยพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้ให้อำนาจแก่ธนาคารในการแบ่งปันข้อมูลที่สำคัญเพื่อป้องกันการหลอกลวงออนไลน์ และยังช่วยให้สามารถติดตามเส้นทางการเงินที่ผิดกฎหมายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ตลอด 7 ปีที่ผ่านมาของ TB-CERT ได้เป็นที่ประจักษ์ในหลายด้าน ไม่ว่าจะเป็นการสร้างหรือแลกเปลี่ยนข้อมูลทางเทคนิคระหว่างธนาคารสมาชิก การสร้างความร่วมมือระหว่างภาคการธนาคาร ภาครัฐ และภาคอุตสาหกรรมอื่น ๆ การสร้างความตระหนักรู้ด้านภัยไซเบอร์ให้กับบุคลากรของธนาคารและภาคประชาชน เพื่อรับรองความปลอดภัยทางไซเบอร์ที่ยั่งยืนภายใต้เศรษฐกิจดิจิทัลของเรา ซึ่งเป็นภารกิจที่สมาคมธนาคารไทยให้ความสำคัญ โดยเฉพาะอย่างยิ่งการร่วมมือกันของทุกภาคส่วน จะนำไปสู่ความปลอดภัยทางไซเบอร์ที่ยั่งยืนร่วมกัน และสมาคมธนาคารไทยจะทำหน้าที่สนับสนุนการดำเนินงานของ TB-CERT ในการสร้างสังคมดิจิทัลที่มีความมั่นปลอดภัยทางไซเบอร์อย่างยั่งยืน เพื่อประโยชน์ต่อลูกค้าของธนาคาร ประชาชน และประเทศชาติของเรา

วิสัยทัศน์สำหรับภูมิทัศน์ใหม่ ภาคการเงินประเทศไทย เพื่อเศรษฐกิจดิจิทัล และการเติบโตอย่างยั่งยืน

โดย

คุณเดช ฐิติวณิช
ผู้ช่วยผู้ว่าการ สายระบบข้อสนเทศ
ธนาคารแห่งประเทศไทย

วิสัยทัศน์สำหรับภูมิทัศน์ใหม่ภาคการเงินประเทศไทยเพื่อเศรษฐกิจดิจิทัลและการเติบโตอย่างยั่งยืน มีหลายประเด็นที่กล่าวถึงความยั่งยืน ไม่ว่าจะเป็นด้านสิ่งแวดล้อม การพัฒนาระบบการชำระเงินและการใช้เทคโนโลยีและข้อมูลในการสร้างสรรค์นวัตกรรม ซึ่งจะช่วยเพิ่มประสิทธิภาพและการเข้าถึงบริการทางการเงิน มี 3 หลักการสำคัญ ได้แก่

1) การเปิดกว้างในการแข่งขัน (Open Competition) รวมถึงการขยายขอบเขตธุรกิจและความยืดหยุ่นในการดำเนินธุรกิจของธนาคารและสถาบันการเงินอื่นๆ ภายใต้การกำกับของ ธปท. โดยการประเมินความเสี่ยงและในสภาวะการแข่งขันที่เท่าเทียม เช่น การออกใบอนุญาตในการดำเนินธุรกิจธนาคารพาณิชย์ไร้สาขา (Virtual Banking) เป็นต้น

2) การเปิดกว้างให้ผู้ให้บริการกลุ่มต่าง ๆ เข้าถึงโครงสร้างพื้นฐานทางการเงินอย่างเหมาะสมและเป็นธรรม (Open Infrastructure) ซึ่งโครงสร้างพื้นฐานนี้จะส่งเสริมการเปลี่ยนแปลงไปสู่ความเป็นเศรษฐกิจดิจิทัลมากยิ่งขึ้น เช่น การพัฒนา PromptBiz และ

3) การเปิดกว้างให้มีการใช้ประโยชน์จากข้อมูล (Open Data) ซึ่งจะสนับสนุนให้เกิดการพัฒนาและส่งเสริมให้เข้าถึงบริการทางการเงินที่ดีขึ้น

การที่เราได้ใช้ประโยชน์จากเทคโนโลยีและข้อมูล ก็ได้เปิดโอกาสให้ผู้ไม่หวังดีหาทางโจมตีหรือหลอกลวง (social engineering) มากขึ้น ความมั่นคงปลอดภัยทางไซเบอร์ที่ยั่งยืนจึงเป็นสิ่งที่สำคัญอย่างมาก สถาบันการเงินและองค์กรต่าง ๆ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ที่แข็งแกร่งเพื่อปกป้อง ตรวจจับ ตอบสนอง และกู้คืนจากเหตุการณ์ที่เกิดขึ้นอย่างรวดเร็ว นอกจากนี้ หลายครั้งที่เราโดนโจมตีมักจะเกิดขึ้นจากจุดอ่อนของมนุษย์ จึงเป็นสิ่งสำคัญที่จะต้องเพิ่มพูนความรู้และสร้างความตระหนักรู้ให้กับทุกคน เพราะบุคคล กระบวนการ และเทคโนโลยี (People, Process, and Technology) เป็นเสาหลักที่สำคัญของความมั่นคงทางไซเบอร์ ซึ่งภาคการเงินจำเป็นต้องสร้างสมดุลระหว่างการส่งเสริมนวัตกรรมและการจัดการความเสี่ยงด้านไซเบอร์ เพื่อให้ภาคการเงินสามารถปรับตัวกับความท้าทายใหม่ ๆ ในขณะที่ยังคงมีประสิทธิภาพในการป้องกัน และสามารถเดินหน้าสู่เศรษฐกิจดิจิทัลที่ยั่งยืน โดยธนาคารแห่งประเทศไทยมีความยินดีที่จะร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์กับทุกองค์กรและบุคลากรที่เกี่ยวข้อง เพื่อสร้างความเชื่อมั่นให้กับระบบการเงินต่อไป

สารจากกรรมการ

ดร.กิตติ โฆษะวิสุทธิ์
ประธานกรรมการ TB-CERT
Senior Vice President and Chief Information Security Officer
ธนาคารกรุงเทพ จำกัด (มหาชน)

" Let us embrace security mindfulness as a daily practice and strive to create a safer online environment for ourselves and those around us. "

คุณชัชวัฒน์ อัศวรักวงศ์
รองประธานกรรมการ TB-CERT
Managing Director and Chief Information Security Officer,
Kasikorn Business Technology Group

" ในยุคดิจิทัลนี้ เราปฏิเสธไม่ได้ว่าข้อมูลข่าวสาร การรับรู้และการเท่าทันต่อสถานการณ์ (Situation Awareness) เป็นสิ่งสำคัญมาก การมีข้อมูลและการรับรู้สถานการณ์ได้อย่างรวดเร็วจะทำให้เราสามารถนำไปใช้ในการป้องกัน ปรับตัว รวมถึงการวางแผนในการรับมือต่อเหตุการณ์ต่าง ๆ ได้แบบเชิงรุก อย่างไรก็ตาม จะเห็นได้ว่าการเผยแพร่ข้อมูลที่ไม่ถูกต้อง และข้อมูลบิดเบือน (Misinformation & Disinformation) มีอยู่มากมายในปัจจุบัน โดยเฉพาะทางช่องทางสื่อสังคมออนไลน์ต่าง ๆ (Social Media) ซึ่งไม่ก่อประโยชน์ และยังสร้างความเสียหาย ทำให้ประชาชนเกิดความแตกตื่นในวงกว้าง ดังนั้นเราจึงจำเป็นต้องใช้สติ และวิจารณญาณในการรับรู้ และแชร์ข้อมูลข่าวสาร ทำความเข้าใจ และตรวจสอบข้อเท็จจริงของข้อมูลจากผู้เชี่ยวชาญหรือแหล่งข้อมูลที่น่าเชื่อถือ พวกเรามาร่วมมือกัน แลกเปลี่ยนข้อมูลที่มีประโยชน์ ลดละเลิกการแชร์ข้อมูลที่ไม่ถูกต้อง เพียงแค่นี้เราก็จะมีส่วนร่วมในการทำให้สังคมในยุคดิจิทัลของพวกเราที่เต็มไปด้วยข้อมูลมหาศาล น่าอยู่ขึ้นอีกหลายเท่าแล้วครับ "

คุณภคพงศ์ จุลวงศาศิลป์
กรรมการ TB-CERT
Head of Cyber Security Department, ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)

“ In the past year, TB-CERT has navigated significant cybersecurity challenges, including a surge in mobile banking cybercrime, ransomware attacks on major banks partner, cloud-related risks, critical vulnerabilities, persistent phishing attempts, DDoS attacks, and incidents related to ATM services. Addressing these threats requires collective efforts and a commitment to modern and comprehensive cybersecurity strategies. As we move forward, continuous investment in technology, risk management, and system upgrades is crucial to ensuring the stability and security of Thailand's financial sector. The Committee appreciates the dedication of all stakeholders involved in safeguarding the nation's financial infrastructure. ”

คุณวชิราวัชร์ มหาทัพกฤษ
กรรมการ TB-CERT
Executive Vice President, Cyber Security ธนาคารออมสิน

“ การรวมกลุ่มของเหล่าสมาชิก TB-CERT ซึ่งประกอบด้วยผู้เชี่ยวชาญด้าน Cybersecurity จากทุกธนาคารในประเทศไทย และองค์กรที่เกี่ยวข้องกับระบบชำระเงิน ได้สร้างความเป็นเพื่อน เป็นมิตร มีกิจกรรมที่ทำให้สมาชิกได้ใกล้ชิดสนิทสนมกัน ปลดพันธนาการ การเป็นคู่แข่งทางธุรกิจ มีแต่ความเป็นมิตร ที่จะช่วยเหลือเกื้อกูลกัน การให้ความรู้ใหม่ ๆ แก่เพื่อน มิได้ทำให้เพื่อนเก่งกว่า แต่ทำให้ "เรา" แข็งแกร่งไปด้วยกัน การแลกเปลี่ยน incident ที่เกิดขึ้น ไม่ได้ทำให้เกิดความเสียหน้า หรืออ่อนแอ แต่เป็น Hero สำหรับเพื่อน ๆ ที่จะได้นำความรู้ไปปกป้องตัวเอง ปกป้องลูกค้า และปกป้องประชาชน เพื่อเพิ่มความเข้มแข็งด้าน Cybersecurity ของประเทศต่อไป ”

คุณเชิดศักดิ์ นานา
กรรมการ TB-CERT
Senior Vice President, IT Security, ธนาคารกรุงไทย จำกัด (มหาชน)

“ ในปี 2566 ที่ผ่านมานั้น ธุรกิจภาคธนาคารได้ผ่านเรื่องราวมากมาย และที่สำคัญที่สุดคือเรื่องภัยคุกคามของแก๊งคอลเซ็นเตอร์และการถูกดูดเงินจากบัญชีผ่านระบบโมบายแบงก์กิ้ง ซึ่งภาคธนาคารได้ให้ความสำคัญและทุ่มเทสมองสติปัญญาในการดูแลควบคุมและแก้ปัญหาที่เกิดขึ้นมาโดยตลอด ไม่ว่าจะเป็นการให้ความรู้ภาคประชาชนซึ่งเป็นลูกค้าให้มีความตระหนักรู้เท่าทันกลโกงของมิจฉาชีพที่มาหลากหลายรูปแบบเพื่อที่จะไม่ตกเป็นเหยื่อและสูญเสียทรัพย์สินเงินทองตามที่ปรากฏตลอดจนการพัฒนาเทคโนโลยีใหม่ ๆ เพื่อรับมือภัยคุกคามดังกล่าว

อย่างไรก็ดีความร่วมมือจากภาคส่วนต่าง ๆ เป็นสิ่งจำเป็นไม่ว่าจะเป็นภาคราชการหรือภาคประชาชนที่เป็นผู้มีส่วนได้ส่วนเสียโดยตรงถือเป็นสิ่งที่สำคัญยิ่ง เพื่อให้การให้บริการของธนาคารมีความมั่นคงปลอดภัยและสนับสนุนเศรษฐกิจของประเทศไทยในอนาคต ”

คุณกริช กาดนอก
กรรมการ TB-CERT
Head of IT Security ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)

“ ภัยคุกคามทางไซเบอร์ ได้เพิ่มความเสี่ยงของอาชญากรรมทางการเงิน (Financial Crime and Fraud) นอกเหนือไปจากการรับมือกับภัยคุกคามทางไซเบอร์แล้ว เราต้องก้าวข้ามขอบเขตการทำงานเพื่อต่อต้านอาญชกรรมทางการเงิน (Financial Crime and Fraud) ร่วมกัน ”

คุณอดิศักดิ์ วงศ์จันลา
กรรมการ TB-CERT
Cybersecurity Advisory specialist
ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

“ ในโลกปัจจุบันมีการเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะการเปลี่ยนแปลงทางดิจิทัลที่เปิดประตูให้กับโอกาสและความท้าทายในรูปแบบของภัยทางไซเบอร์ที่เพิ่มขึ้น ซับซ้อนขึ้น รุนแรงขึ้น ซึ่งเราอยู่ในยุคที่มีการใช้บริการต่างๆ ร่วมถึงบริการด้านการเงิน เชื่อมต่ออินเทอร์เน็ตกลายเป็นสิ่งสำคัญและอยู่ในชีวิตประจำวันสำหรับทุกคน ซึ่งความสะดวกสบายนี้ มีความเสี่ยงที่เพิ่มขึ้นอย่างมากต่อความปลอดภัยทางการเงิน ข้อมูลส่วนบุคคลและองค์กร

ดังนั้นเราต้องมีความพร้อมที่จะสามารถรับมือกับภัยคุกคามทางไซเบอร์ในทุก ๆ ด้าน ด้านแรก ในฐานะผู้ให้บริการต้องเรียนรู้และตามให้ทัน เราไม่สามารถหยุดพัฒนาได้เพราะเทคนิคใหม่ ๆ ของภัยคุกคามเกิดขึ้นตลอดเวลา ที่สำคัญเราต้องพัฒนาไปจนถึงระดับวางมาตรการป้องกันไว้ล่วงหน้า เพื่อก้าวนำหน้าภัยคุกคามในปัจจุบันให้ได้

ด้านที่สอง เราต้องมีความเข้มงวดในการตรวจสอบความปลอดภัยทางไซเบอร์กับ third party ของเรา ซึ่งเป็นจุดเสี่ยงจุดหนึ่งที่เราไม่อาจจะมองข้ามได้ เพื่อให้ third party เหล่านั้นสามารถรักษาความปลอดภัยระบบและข้อมูลของเราได้อย่างมั่นคง

ด้านที่สาม เราต้องมองออกนอกกรอบในฐานะผู้ให้บริการ ต้องมองไปถึงความปลอดภัยของผู้ใช้บริการหรือประชาชนด้วย ปัจจุบันกรณีการฉ้อโกงทางไซเบอร์มีเป็นจำนวนมาก การประชาสัมพันธ์สื่อสาร ในทุกภาคส่วน จะเป็นวัคซีนช่วยให้ประชาชนเข้าใจถึงภัยทางไซเบอร์ซึ่งเป็นส่วนสำคัญในการสร้างสังคมดิจิทัลที่มีความปลอดภัยและยั่งยืน เพื่อให้ทุกคนสามารถใช้เทคโนโลยีได้อย่างมั่นคงและมั่นใจ ”

"Ready to confront cyber threats?"

คุณประกลกฤษ แสงชูวงศ์
กรรมการ TB-CERT
Team Head of Information Security Detection and Response
ธนาคารทหารไทยธนชาต จำกัด (มหาชน)

“ เหตุการณ์ตั้งแต่ปี 2566 เป็นต้นไป แนวโน้มภัยคุกคามด้านไซเบอร์จะสูงขึ้น และมีความซับซ้อนในการตรวจจับ หรือแก้ไขปัญหา ตลอดจนผลกระทบด้านความเสียหายต่อภาคเศรษฐกิจและสังคม ชื่อเสียง การเสียโอกาสทางด้านธุรกิจ การฟ้องร้อง จะสูงขึ้นตามมา ทั้งนี้สาเหตุหลัก ๆ คือมีการมุ่งเป้าการโจมตีจากกลุ่มองค์กรอาชญากรรมไซเบอร์ ที่ทำงานเป็นระบบ แบบแผนมากขึ้น ทำให้ต่อจากนี้ ในภาคการธนาคารที่ได้ดำเนินแนวทางการบริหารจัดการไซเบอร์ก็ต้องมุ่งเน้นแนวทางเตรียมความพร้อมให้สามารถรับมือต่อต้านภัยคุกคามไซเบอร์ได้ทุกรูปแบบที่จะเกิดขึ้น ให้มากขึ้นจากเดิมที่มีอยู่ให้รัดกุมยิ่งขึ้น ประกอบกับต้องเสริมศักยภาพในการสามารถกู้คืนระบบ หรือข้อมูล ให้พร้อมต่อการบริการลูกค้าและประชาชนให้รวดเร็วที่สุด ตลอดจนการดูแลลูกค้า หากเกิดการรั่วไหลของข้อมูลที่อาจจะเกิดจากผู้ให้บริการรายอื่น ที่อาจส่งผลกระทบต่อธุรกิจของสถาบันการเงินได้ ให้มากขึ้นจากเดิมขึ้นไปอีก

ทั้งนี้ ปัจจัยที่จะทำให้องค์กรประสบความสำเร็จที่ละเลยไม่ได้ คือ ทำให้ผู้บริหารระดับสูงและพนักงานมีความเข้าใจและตระหนักรู้ในภัยคุกคามไซเบอร์มากขึ้น เช่น เพื่อตัดสินใจในการลงทุนให้เหมาะสมตามความเสี่ยงขององค์กร หรือให้ความร่วมมือในการปรับกลยุทธ์ ตลอดจนแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์แก่องค์กรอย่างมีประสิทธิภาพและประสิทธิผลสูงสุด

สิ่งสำคัญอีกสิ่งที่จะลืมไม่ได้ คือ การพัฒนาทักษะความสามารถ และการสร้างโอกาสให้ผู้สนใจเข้ามาเป็นบุคลากรด้านไซเบอร์มากขึ้น เพื่อให้รองรับกับการเปลี่ยนแปลงในโลกยุคดิจิทัล โดย ณ ปัจจุบันวิชาชีพด้านไซเบอร์ มีความต้องการสูงมาก และถือเป็นวิชาชีพที่สำคัญไม่แพ้อาชีพด้านเทคโนโลยีอื่น ๆ เช่น ปัญญาประดิษฐ์ (AI/ML), นักวิเคราะห์ข้อมูล Data Analytic ฯลฯ เลยทีเดียว

ทั้งหมดนี้ ถือเป็นภารกิจที่สำคัญของ TB-CERT ต่อไป ”

คุณยศ กิมสวัสดิ์
กรรมการ TB-CERT
ประธานสำนักงานระบบการชำระเงิน สมาคมธนาคารไทย

“ การรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ในยุคดิจิทัลที่มีความผสมผสานกันระหว่าง Digital Fraud กับ Cybercrime มีความท้าทายหลายอย่าง แต่สิ่งหนึ่งที่จะช่วยให้การรับมือกับเหตุการณ์เหล่านี้ได้อย่างมีประสิทธิภาพอย่างแท้จริง คือการสร้างความร่วมมือและการทำงานร่วมกันทั้งภายในและภายนอกองค์กร ”

บทวิเคราะห์ภัยคุกคาม และองค์รวมในการพัฒนาความมั่นคงปลอดภัย ของ Mobile Application ในประเทศไทย

บทวิเคราะห์ภัยคุกคามและองค์รวมในการพัฒนาความมั่นคงปลอดภัยของ Mobile Application ในประเทศไทย

โดย ดร.ภิตติ โฆษะวิสุทธิ์
ประธานกรรมการ TB-CERT

ในปี 2566 มีเหตุการณ์การโจมตี Mobile Application เกิดขึ้นหลายเหตุการณ์ โดยมิจฉาชีพมีการพัฒนาเทคนิคใหม่ ๆ เพื่อหลบหลีกมาตรการการป้องกันที่ทางธนาคารได้พัฒนาเสริมเพิ่มเติม หนึ่งในปัจจัยที่ส่งเสริมให้มิจฉาชีพสามารถที่จะพัฒนาเทคนิคใหม่ ๆ ให้สามารถหลบหลีกมาตรการป้องกันได้นั้นคือสภาพแวดล้อมในการใช้งาน Mobile Application ซึ่งประกอบไปด้วย 4 องค์ประกอบ ได้แก่ องค์ประกอบที่ 1. ระบบเปิดกับระบบปิด องค์ประกอบที่ 2. เทคโนโลยีกับสังคมโซเชียล องค์ประกอบที่ 3. ความเป็นจริงกับความคิดเห็น องค์ประกอบที่ 4. การโจมตีและการป้องกัน ทั้ง 4 องค์ประกอบนี้ ส่งผลโดยตรงต่อความเสี่ยงและแนวทางการพัฒนาให้ระบบนิเวศน์ของการใช้ Mobile Application มีความปลอดภัย

บทวิเคราะห์นี้จะแสดงองค์ประกอบที่สำคัญในการที่จะพัฒนาองค์รวมของการพัฒนาความมั่นคงปลอดภัยของ Mobile Application ในประเทศไทย

องค์ประกอบที่ 1. ระบบเปิดกับระบบปิด

ระบบปฏิบัติการของโทรศัพท์มือถือมีส่วนสำคัญและถือเป็นพื้นฐานของสภาพแวดล้อมในการใช้งาน Mobile Application ปัจจุบันระบบปฏิบัติการหลัก ๆ จะมี 2 ระบบ คือ ระบบเปิดซึ่งเป็นระบบปฏิบัติการที่มีบริษัทผู้ผลิตโทรศัพท์มือถือหลายรายนำไปใช้ และอาจจะมีการปรับเปลี่ยนเพิ่มเติมเพื่อเป็นการสร้างจุดขาย รวมถึงการมี Store เป็นของตัวเองเพื่อใช้ในการกระจายซอฟต์แวร์ของตนเอง โดยกระบวนการควบคุม การตรวจสอบกลั่นกรองซอฟต์แวร์ให้มีความถูกต้อง มีคุณภาพ และ มีความมั่นคงปลอดภัยนั้น อาจจะแตกต่างกัน เนื่องจากการที่มีผู้ผลิตโทรศัพท์มือถือหลายรายนำไปใช้ทำให้ในภาพรวมของระบบปฏิบัติการที่มีสภาพเป็นระบบเปิดนั้น มีการบริหารจัดการและควบคุมเรื่องความมั่นคงปลอดภัยที่แตกต่างกันในแต่ละราย จึงอาจจะมีความเสี่ยงที่จะถูกนำไปใช้สร้างความเสียหายให้กับผู้ใช้งานได้ ในขณะที่ในอีกระบบจะเป็นระบบปิดซึ่งเป็นการพัฒนาระบบปฏิบัติการที่มีบริษัทผู้ผลิตรายเดียว มีการพัฒนาระบบปฏิบัติการ และกระบวนการควบคุมการตรวจสอบกลั่นกรองซอฟต์แวร์ที่ควบคุมโดยบริษัทเดียว ในมุมมองของระบบนิเวศน์การใช้งานและการควบคุมในตลาดที่มีปริมาณผู้ใช้งานจำนวนมากทั่วโลก การพัฒนาซอฟต์แวร์จะทำได้เร็วและหลากหลายใน

ระบบเปิด แต่ควรจะต้องมีการสร้างกลไกในด้านของการควบคุมคุณภาพและความมั่นคงปลอดภัยภาพรวมที่ดีควบคู่กันไปด้วย จึงจะไม่ถูกนำไปใช้เป็นช่องทางในการสร้างความเสียหายให้กับผู้ใช้งานต่อไป

องค์ประกอบที่ 2. เทคโนโลยีกับสังคมโซเชียล

ความก้าวหน้าทางเทคโนโลยีในปัจจุบันเป็นไปอย่างรวดเร็ว ซึ่งผู้ใช้งานจะต้องติดตามข้อมูลข่าวสารและต้องพยายามทำความเข้าใจทั้งประโยชน์และโทษของเทคโนโลยีดังกล่าวตลอดเวลา ในขณะเดียวกันปัจจุบันสังคมโซเชียลเป็นแหล่งที่ทุกคนสามารถเข้าถึงได้และก็ยังสามารถเป็นผู้ให้ข้อมูลได้อีกด้วย แต่ด้วยสังคมโซเชียลเป็นสังคมเปิดมิได้มีการยืนยันตัวตนอย่างเข้มข้น และที่สำคัญสังคมโซเชียลยังมีอัลกอริทึมในการเลือกสิ่งที่ผู้ใช้งานสนใจมาแสดงเท่านั้น โดยมิได้มีการนำเสนอข้อมูลในอีกด้านหนึ่ง จึงจะมีแนวโน้มที่จะตอกย้ำความเข้าใจหรือความสนใจของผู้ได้รับข้อมูลจากสังคมโซเชียลในประเด็นนั้น ๆ หรือที่เรียกว่า Confirmation Bias ดังนั้นผู้ใช้งานจึงจะต้องมีความเข้าใจเทคโนโลยีหรือเครื่องมือที่ใช้งานอยู่เพื่อที่สามารถใช้งานเทคโนโลยีได้อย่างมีประสิทธิผลภายใต้ข้อจำกัดหรือลักษณะเฉพาะของเทคโนโลยีนั้น ๆ

องค์ประกอบที่ 3. ความเป็นจริงกับความคิดเห็น

ข้อมูลเป็นสิ่งสำคัญเพื่อให้เกิดความเข้าใจ เกิดความรู้ในเรื่องต่าง ๆ ในขณะที่บางครั้งตัวอักษรหรือภาพวิดีโอบนโลกอินเทอร์เน็ตนั้นอาจจะเป็นความคิดเห็นจากความเข้าใจหรือมุมมองของผู้ที่ต้องการสื่อความให้ผู้อื่นรับทราบ การตรวจสอบหรือแยกแยะว่าเป็นข้อมูลที่แสดงถึงความเป็นจริงหรือข้อมูลที่แสดงถึงความคิดเห็น จึงมีส่วนสำคัญที่จะต้องมีการประเมินความถูกต้องและตรวจสอบจากหลายแหล่งข้อมูลก่อนที่จะนำมาใช้งาน ในช่วงเวลานี้ที่มีการพัฒนาเทคโนโลยีปัญญาประดิษฐ์มาใช้งาน โดยเฉพาะอย่างยิ่ง Generative AI ข้อมูลที่ถูกสร้างขึ้นโดย Generative AI นั้นยังมีข้อจำกัดอีกมาก โดยเฉพาะความสามารถในการตรวจสอบที่มาของคำตอบ มิฉะนั้นผลลัพธ์ดังกล่าวจะกลายเป็นความคิดเห็นที่ถูกสร้างจาก AI ได้ ซึ่งผู้ใช้งานจะต้องมีความเข้าใจว่าผลลัพธ์จาก Generative AI อาจจะมีความคลาดเคลื่อนหรือเกินความเป็นจริง (Hallucination) จึงจำเป็นต้องมีการตรวจเช็คและสอบข้อมูลนั้นก่อนที่จะนำไปใช้งาน

องค์ประกอบที่ 4. การโจมตีและการป้องกัน

เทคนิคการโจมตีมักจะเริ่มจากการทดสอบมาตรการการป้องกันเพื่อรวบรวมข้อมูลสำหรับหาวิธีการหลบหลีกมาตรการการป้องกัน ทั้งนี้ในการพัฒนา Mobile Application ของผู้พัฒนาแต่ละยี่ห้อต้องคำนึงถึงความมั่นคงปลอดภัยเพื่อป้องกันการโจมตี Application ของตนเอง สำหรับธนาคารได้มีการพัฒนามาตรการต่าง ๆ ในการป้องกันการโจมตีในรูปแบบต่าง ๆ ซึ่งสามารถสรุปมาตรการด้านความมั่นคงปลอดภัยได้ดังนี้

รูปแบบการโจมตี	มาตรการด้านความมั่นคงปลอดภัย
เปิดสิทธิ์ให้เข้าถึงระบบปฏิบัติการ (Rooted/Jailbroken)	ตรวจจับ Rooted/Jailbroken และระงับการใช้งาน สนับสนุนให้มีการ Update OS ให้เป็นปัจจุบันเสมอ
เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application Permission)	กำหนดการตรวจสอบยืนยันตัวตนที่ได้มาตรฐาน
เข้าถึง Source Code และข้อมูลที่สำคัญได้	ทำการ Obfuscation หรือเข้ารหัสข้อมูลในส่วนที่สำคัญ
การดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลหรือสวมรอยการเข้าใช้งานระหว่างการรับส่ง (Man in the Middle Attack)	ทำการเข้ารหัสข้อมูลก่อนส่งผ่านเครือข่ายสาธารณะ
โจมตีเจาะระบบแอปพลิเคชัน	ดำเนินการตรวจสอบแอปพลิเคชันก่อนออกให้ใช้บริการ
Social Engineering	จัดให้มีการเสริมสร้างความรู้ ความเข้าใจการใช้บริการเทคโนโลยีทางการเงินให้แก่ประชาชน ทั้งความรู้เกี่ยวกับภัยคุกคามใหม่ ๆ และวิธีการปฏิบัติตนให้ปลอดภัยในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ในเชิงรุก และต่อเนื่อง
แก้ไขปรับแต่งแอปพลิเคชัน	ป้องกันการแก้ไขหรือดัดแปลงแอปพลิเคชัน
เดาหรือสุ่มค่า PIN	กำหนดให้ตั้งค่า PIN ที่ซับซ้อนเพื่อให้ยากต่อการคาดเดา และ Lock การเข้าใช้หากผิดหลายครั้ง
โจมตีด้วยเทคนิค DDoS Attack เพื่อทำให้ระบบทำงานไม่ได้	มีระบบการป้องกัน DDoS Attack เพื่อยกระดับการป้องกันข้อมูลรั่วไหลระหว่าง รับ/ส่ง หรือป้องกันระบบถูกโจมตีจนไม่สามารถให้บริการได้
ทำหน้าจอซ้อนทับเพื่อไม่ให้เห็นขั้นตอนการโอนเงินของมิจฉาชีพ (Overlay)	ตรวจจับและป้องกันการถูกซ้อนทับหน้าจอ
ควบคุมเครื่องเหยื่อ	- ใช้ Accessibility service ในการควบคุมเครื่องโทรศัพท์ มือถือเหยื่อ - ให้การ Copy หน้าจอ (Mirroring) และควบคุมการใช้เครื่องโทรศัพท์ มือถือเหยื่อ
หลอกให้ดาวน์โหลดโปรแกรมมัลแวร์ที่เตรียมไว้	ตรวจจับและป้องกันการดาวน์โหลดโปรแกรมจากแหล่งอื่นที่ไม่ใช่ Official Store (Sideloading)

โดยสรุปธนาคารมีการวิเคราะห์สถานการณ์และเทคนิคการโจมตีที่ซับซ้อน หลากหลายของมิจฉาชีพในปัจจุบันเพื่อช่วยให้การพัฒนายกระดับความมั่นคงปลอดภัยของแอปพลิเคชันมือย่างต่อเนื่อง ประกอบกับมีการวิเคราะห์องค์ประกอบที่สำคัญที่ส่งผลโดยตรงต่อความเสี่ยงและแนวทางการพัฒนาให้ระบบนิเวศน์ของการใช้ Mobile Application ให้มีความปลอดภัย หากผู้ใช้งานในโลกออนไลน์และผู้พัฒนาระบบ Mobile Application ใด ๆ มีความเข้าใจถึงความเสี่ยงที่อาจจะส่งผลกระทบต่อตนเองและผู้อื่นได้จากการโจมตีของมิจฉาชีพ จะช่วยยกระดับให้สังคมมีความมั่นคงปลอดภัยได้และจะทำให้นำไปสู่การพัฒนาความมั่นคงปลอดภัยของ Mobile Application ในภาพรวมของประเทศไทยได้อย่างเข้มแข็งและยั่งยืน

กิตติ โฆษะวิสุทธิ์

บทนำ

บทนำ

TB-CERT มุ่งมั่นในการสร้างความเข้มแข็งด้านความมั่นคงปลอดภัยไซเบอร์ให้กับภาคการธนาคาร ชุมชน และ ประชาชน เพื่อให้ธุรกิจ สังคม และประเทศไทย ก้าวสู่การใช้ดิจิทัลในชีวิตประจำวันได้อย่างปลอดภัย ในปี 2566 ที่ผ่านมา ภาคการธนาคารพบกับความท้าทายมากมายในเรื่องของความมั่นคงปลอดภัยไซเบอร์ที่ทุกวันนี้มีความซับซ้อน และมีการปรับเปลี่ยนเทคนิควิธีการโจมตีได้อย่างรวดเร็วผสมผสานกับเทคนิคการหลอกลวงทางออน์ไลน์ที่เปลี่ยนไปตามแต่ละช่วงเวลา

รูปแบบของภัยคุกคามนอกจากจะมีการพัฒนาเทคนิคเชิงลึกแล้ว การหลอกลวงทางออน์ไลน์ด้วยข้อมูลที่หาได้จากแหล่งต่าง ๆ ในโลกไซเบอร์ ทำให้ประสิทธิผลของการโจมตีมีแนวโน้มที่สูงขึ้น เครื่องมือสำคัญที่ใช้ในการโจมตีอีกส่วนหนึ่งคือการบิดเบือนข้อมูลหรือการสร้างข้อมูลเท็จ (Disinformation) และนำมาใช้ในการโน้มน้าวให้เหยื่อเป้าหมายเชื่อและดำเนินการตามขั้นตอนที่เตรียมไว้ การพัฒนาทักษะทางเทคนิคอย่างต่อเนื่องเป็นสิ่งที่ยังคงสำคัญเพื่อที่จะสามารถวิเคราะห์แยกแยะสัญญาณความผิดปกติที่ซ้อนเร้นอยู่ได้อย่างมีประสิทธิภาพ การสร้างความรู้ความเข้าใจ ความตระหนักให้รู้เท่าทันกลลวงของมิจฉาชีพในสถานการณ์ที่เป็นปัจจุบันในขณะนั้น จะเป็นการเสริมสร้างภูมิคุ้มกันต่อภัยไซเบอร์ในภาพรวมได้ดี

ก้าวต่อไปสู่ความท้าทายที่จะมาถึง คงหนีไม่พ้นความเร็วในการนำเอาเทคโนโลยีมาใช้ในการโจมตีของฝั่งมิจฉาชีพ และความเร็วในการนำเอาเทคโนโลยีมาใช้ในการป้องกันของฝั่งผู้ให้บริการ โดยเฉพาะเทคโนโลยีด้านปัญญาประดิษฐ์ ในขณะที่ธุรกิจจำเป็นต้องเดินหน้าต่อไปนั้น การพัฒนาด้านความมั่นคงปลอดภัยจำเป็นต้องเน้นการตอบโจทย์ในระยะยาวของธุรกิจซึ่งถือเป็นการพัฒนาบทใหม่ของความมั่นคงปลอดภัยไซเบอร์สู่ความยั่งยืน (Sustainable Cybersecurity)

กิจกรรมในปี 2023

ในปีที่ผ่านมา TB-CERT ได้มีการจัดกิจกรรมรวมถึงดำเนินงานต่าง ๆ แบ่งออกเป็น 5 ด้านตามภารกิจของ TB-CERT ดังนี้

Standardize: งานด้านกำหนดมาตรฐานด้าน Cybersecurity

People Development: งานด้านการพัฒนาบุคลากร

Collaboration: งานด้านการสร้างความร่วมมือกับหน่วยงานต่าง ๆ ทั้งภายในและภายนอกภาคการธนาคาร

Awareness: การสร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity

Services: การให้บริการ แจ้งเตือน และคำแนะนำแก่สมาชิก

กิจกรรมและผลงานสำคัญในปี 2023

1

งานกำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคธนาคาร

1. แบบสอบถามการตระหนักรู้ต่อภัยทุจริตบน Mobile Banking Application (Awareness Test)
2. การประเมินความพร้อมด้าน Cyber Resilience สำหรับผู้ให้บริการภายนอก (IT Outsourcing) ที่ธนาคารส่วนใหญ่ใช้บริการ (3rd Party Concentration Risk)

2

งานด้านการพัฒนาบุคลากร

1. งานสัมมนาประจำปี TB-CERT Cybersecurity Annual Conference 2023
2. งานด้านการสร้างความตระหนักรู้ด้านภัยไซเบอร์ Cybersecurity Proficiency Development Program (Webinar, Workshop, E-Learning) ให้กับหน่วยงานสมาชิก
3. การซ้อมรับมือภัยไซเบอร์ภาคการธนาคาร (Banking Cyber Drill)
4. การแข่งขันทักษะทางไซเบอร์ภาคการธนาคาร (Cyber Combat)

3

งานด้านการสร้างความร่วมมือ

1. งานและกิจกรรมภายใต้ความร่วมมือ
   - ร่วมเป็นวิทยากร
   - ร่วมให้สัมภาษณ์และแถลงข่าว
   - ร่วมแสดงบูธให้ความรู้ด้าน Cybersecurity
2. การสร้างความร่วมมือกับหน่วยงาน ภายใต้ MOU CERT Readiness ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย
3. การสร้างความร่วมมือภายในสมาชิก
4. การสร้างความร่วมมือกับต่างประเทศ

4

การสร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity

1. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับสถาบันธนาคารไทย (TBAC)
2. การจัดทำ Infographic เพื่อให้ความรู้ภาคประชาชน
3. การสร้างความตระหนักรู้ด้านภัยไซเบอร์ผ่านสื่อ Facebook

5

การให้บริการแก่สมาชิก

1. การแจ้งเตือนข้อมูลข่าวสาร และประสานแจ้งเหตุ
2. การศึกษาและวิเคราะห์ข้อมูลเพื่อให้คำแนะนำ หาทางป้องกันให้กับสมาชิกในภาพรวม และ/หรือออกมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

งานกำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคธนาคาร

แบบสอบถามการตระหนักรู้ต่อภัยทุจริตบน Mobile Banking Application (Awareness Test)

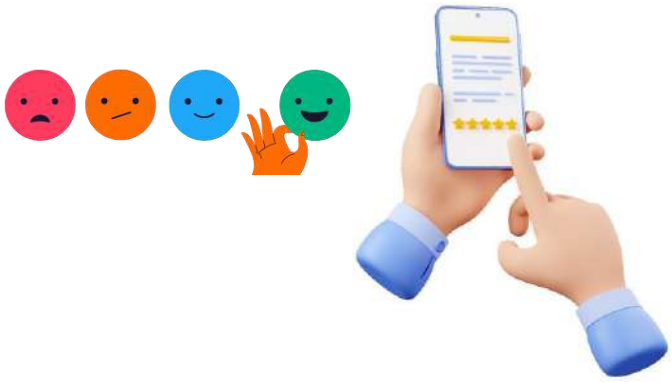
จากภัยทางการเงินรูปแบบใหม่ ๆ ที่เกิดขึ้นในหลายช่องทาง ทำให้ธนาคารแห่งประเทศไทยประกาศแนวทางการดำเนินการตามมาตรการแก้ไขปัญหาภัยทุจริตออนไลน์ เพื่อป้องกันความเสี่ยงและปิดช่องโหว่ภัยทุจริตที่มิจฉาชีพใช้เข้าถึงประชาชน ซึ่งหนึ่งในแนวทางการแก้ปัญหาดังกล่าว TB-CERT จึงได้กำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคธนาคาร โดยสร้างแบบสอบถามการตระหนักรู้ต่อภัยทุจริตบน Mobile Banking Application ที่ให้ผู้ใช้งานประเมินเป็นระยะ เพื่อปลูกฝังความเข้าใจความปลอดภัยในการใช้โทรศัพท์มือถือขั้นพื้นฐาน ลดโอกาสที่จะตกเป็นเหยื่อของการโจมตี และมีความกระตือรือร้นให้มากที่สุดเกี่ยวกับภัยคุกคามที่มาในรูปแบบต่าง ๆ ทั้งนี้ ในการออกแบบแต่ละคำถาม ต้องคำนึงถึงประโยชน์ของผู้ประเมินเป็นหลัก อีกทั้งต้องใช้ภาษาที่เข้าใจง่ายไม่ซับซ้อนจนเกินไป และไม่ส่งผลกระทบต่อประสบการณ์การใช้งานแอปพลิเคชัน โดยแบบสอบถามแบ่งออกเป็น 3 หัวข้อหลัก ได้แก่

1. **ความปลอดภัยของรหัสผ่าน** โดยอ้างอิงจาก NIST Password Guidelines ซึ่งแสดงให้เห็นว่าในการรักษาความปลอดภัยของรหัสผ่านนั้น นอกจากต้องคำนึงถึงคุณภาพของรหัสผ่านที่ตั้งแล้ว ยังรวมถึงอุปนิสัยของผู้ใช้งานในการเลือกใช้ จัดเก็บ และอัปเดตรหัสผ่านอีกด้วย เช่น
    - รหัสผ่านของคุณมีความเรียบง่าย และใช้ข้อมูลส่วนตัว เช่น 1234 หรือ วันเดือนปีเกิด หรือเบอร์โทรศัพท์ ใช่หรือไม่
    - ระหว่างที่คุณกดรหัสผ่าน ไม่จำเป็นต้องระวังคนแอบดูรหัสผ่านที่คุณกำลังกด ใช่หรือไม่
2. **การใช้งานโทรศัพท์มือถือให้ปลอดภัย** ในบางครั้งการใช้งานโทรศัพท์มือถือโดยไม่ระมัดระวังอาจเป็นการเปิดช่องโหว่ให้มิจฉาชีพสามารถเข้าถึงข้อมูลบนเครื่องหรือเข้าควบคุมอุปกรณ์ และนำไปสู่การสูญเสียทรัพย์สินได้เช่นกัน ดังนั้น ผู้ใช้งานจึงควรคำนึงถึงวิธีการใช้งานโทรศัพท์มือถือให้ปลอดภัย เช่น
    - ก่อนการติดตั้งแอปพลิเคชัน คุณได้อ่านการขอสิทธิ์เข้าถึงข้อมูลและความเป็นส่วนตัวอย่างละเอียด ใช่หรือไม่
    - คุณเชื่อมต่อ Wi-Fi สาธารณะ หรือ Wi-Fi ที่คุณไม่รู้จักเป็นประจำ ใช่หรือไม่

3. **วิธีการสังเกตและระวังตัวเบื้องต้น** ในยุคที่ภัยทางการเงินเกิดขึ้นมากและมักจะพัฒนาวิธีการใหม่ ๆ เพื่อหลอกเหยื่อให้เสียหาย การติดตามข่าวสาร อัปเดตความรู้เรื่องกลอุบายรวมถึงลักษณะการหลอกลวงจึงเป็นสิ่งสำคัญ เพื่อที่จะสร้างเกราะป้องกันให้กับตนเอง เช่น

   - เมื่อได้ URL ทางอีเมลหรือ SMS ให้คลิกโดยไม่ลังเล ใช่หรือไม่
   - เมื่อได้รับโทรศัพท์จากคนไม่รู้จัก หรือไม่คาดว่าจะได้รับโทรศัพท์นั้น คุณสามารถทำตามคำบอกได้ทุกอย่าง ใช่หรือไม่

การตอบแบบสอบถามเหล่านี้บน Mobile Banking Application ถือเป็นหนึ่งในมาตรการที่จะช่วยสร้างความตระหนัก เตือนสติให้ประชาชนฉุกคิดก่อนจะทำธุรกรรมทางการเงินใด ๆ อย่างไรก็ตาม มิจฉาชีพเองก็มีการพัฒนาวิธีการหลอกลวงอยู่ตลอด ดังนั้นประชาชนจะต้องติดตามข่าวสารจากแหล่งข่าวที่เชื่อถือได้ เพื่อให้รู้เท่าทันภัยทางการเงิน ตั้งสติไม่ตื่นตระหนกกับสถานการณ์ และหมั่นหาความรู้เรื่องการใช้เทคโนโลยีต่าง ๆ ให้ปลอดภัยอยู่เสมอ



การประเมินความพร้อมด้าน Cyber Resilience สำหรับผู้ให้บริการภายนอก (IT Outsourcing) ที่ธนาคารส่วนใหญ่ใช้บริการ (3rd Party Concentration Risk)

ปัจจุบันองค์กรหลายแห่งมีการปรับเปลี่ยนวิถีการทำงานภายในองค์กรเพื่อให้ตอบรับกับการเปลี่ยนแปลงของโลกในยุคที่เทคโนโลยีมีการก้าวหน้าล้ำสมัยอย่างก้าวกระโดด เพื่อให้ธุรกิจดำเนินการได้อย่างรวดเร็ว การใช้บริการจากหน่วยงานภายนอก หรือที่เรียกว่า การ Outsource จึงเข้ามาตอบโจทย์การดำเนินธุรกิจที่ต้องให้ทันต่อการบริการต่าง ๆ ธนาคารเองก็เช่นกัน ด้วยสถานการณ์ที่สำคัญเร่งด่วน ต้องรีบออกบริการให้กับลูกค้าในยุคสมัยนี้ จำเป็นต้องใช้บริการจากหน่วยงานภายนอกในบางเรื่องเช่นการจ้างบริษัทให้ช่วยพัฒนาโปรแกรม เพื่อที่จะเพิ่มจำนวนบุคลากรในการพัฒนาระบบงานที่ต้องใช้เทคโนโลยีใหม่ได้ในเวลาอันสั้น ซึ่งจะทำให้สามารถสามารถดำเนินการให้ทันต่อความต้องการของลูกค้า หรือการใช้ Infrastructure จากผู้ให้บริการภายนอกเพื่อการ Scale หรือประสิทธิภาพของการรับ load งานที่ดีขึ้น เป็นต้น

แต่ทำไม? เราจึงต้องทำการประเมินความพร้อมเรื่อง Cyber Resilience กับผู้ให้บริการภายนอกที่ธนาคารส่วนใหญ่ใช้บริการ ซึ่งคำว่า Cyber Resilience นั้นเราใช้ในความหมายที่กล่าวถึง ความสามารถในการเตรียมความพร้อม และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติขององค์กร ซึ่งการที่องค์กรมี Cyber Resilience ที่ดีนั้น แปลว่าองค์กรมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ได้ดี แต่เนื่องจากการที่ธนาคารมีการใช้บริการจากผู้ให้บริการภายนอกที่กระจุกตัวอยู่ในรายสำคัญ ๆ (Significant IT Outsourcing) อาจก่อให้เกิดความเสี่ยงด้านการกระจุกตัวของ IT Outsourcing (Concentration risk) เช่น เมื่อหลายปีก่อนมีเหตุการณ์ที่ข้อมูลสำคัญของธนาคารรั่วไหลจากผู้ที่ให้บริการ IT Outsourcing เอง ภาคการธนาคารจึงจำเป็นต้องช่วยกันใส่ใจกับเรื่องความมั่นคงปลอดภัยไซเบอร์ของบริษัทที่ใช้บริการอยู่ อีกทั้งจะต้องกำหนดแนวทางการประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ที่สอดคล้องกับมาตรฐานที่ใช้ในภาคการเงินการธนาคาร และนำมาใช้กับบริษัท IT Outsourcing เพื่อที่จะได้มีแนวทางการประเมินความพร้อมและความเสี่ยงที่อาจจะเกิดกับบริษัท IT Outsourcing รวมถึงวางแนวการจัดการความเสี่ยงดังกล่าวรวมกัน โดยแบบของการประเมินนั้นถูกพัฒนามาจากแบบการประเมินความพร้อมด้าน Cyber Resilience ที่ธนาคารแห่งประเทศไทยใช้ประเมินความพร้อมด้าน Cyber Resilience ของธนาคารพาณิชย์ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย (CRAF – Cyber Resilience Assessment Framework)

กรอบของการประเมินแบ่งออกเป็น 3 ส่วน ส่วนที่ 1 เกี่ยวกับข้อมูลของบริษัทผู้ให้บริการ ส่วนที่ 2 เกี่ยวกับ ข้อมูลความเสี่ยงตั้งต้น (Inherent risk) ส่วนที่ 3 ข้อมูลเกี่ยวกับมาตรการควบคุมในแต่ละโดเมน

ส่วนที่ 1 เกี่ยวกับข้อมูลของบริษัทผู้ให้บริการ

ประกอบด้วย ชื่อบริษัท ชื่อ ตำแหน่ง ผู้ทำแบบประเมิน และส่วนสำคัญคือ ชื่อ ตำแหน่งผู้รับรองการประเมิน โดยส่วนนนี้จำเป็นต้องเป็นผู้ที่มีหน้าที่รับผิดชอบโดยตรงเท่านั้น ได้แก่

1) Head of IT Security หรือ Chief Information Security Officer (CISO) และ
2) ผู้บริหารตำแหน่งสูงสุดที่รับผิดชอบบริหารจัดการการให้บริการในประเทศไทย เช่น Managing Director หรือ Country Manager เป็นต้น

ส่วนที่ 2 เกี่ยวกับข้อมูลความเสี่ยงตั้งต้น (Inherent risk)

เป็นส่วนที่ให้บริษัทพิจารณาระดับความเสี่ยงที่เกิดจากเหตุการณ์ที่ถูกโจมตีทางไซเบอร์ตามแบบต่าง ๆ เช่น เหตุการณ์การโจมตีประเภท Social Engineering โดยให้หลักการพิจารณาความเสี่ยงจากการให้นับจำนวนครั้งที่เกิด โดยนับทั้งที่มีความเสียหายและไม่มีความเสียหายที่เกิดกับพนักงานภายในและลูกค้าของบริษัทที่พบในรอบ 12 เดือนที่ผ่านมา โดยนับจาก IT / Security Incident Report ได้ เป็นต้น โดยจะนำมากำหนดระดับความเสี่ยง สูง กลาง ต่ำ จากจำนวนเหตุการณ์ที่เกิดขึ้น

ประเภทของเหตุการณ์ที่ใช้เป็นกรอบในการประเมิน

1. เหตุการณ์ Social Engineering
2. เหตุการณ์ Phishing Website / Mobile Application
3. เหตุการณ์ SQL Injection, XSS, CSRF
4. เหตุการณ์ DDoS
5. เหตุการณ์ Malware
6. เหตุการณ์ Data Breach

ส่วนที่ 3 ข้อมูลเกี่ยวกับมาตรการควบคุมในแต่ละโดเมน

แบ่งออกเป็น 5 โดเมนได้แก่

โดเมนที่ 1: Governance การกำกับดูแล

บริษัทจะต้องมีการกำหนดและบทบาทหน้าที่ของคณะกรรมการบริษัท และผู้บริหารระดับสูง ไว้เป็นลายลักษณ์อักษร และ กำหนดกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Strategy) โดยคำนึงถึงนโยบายด้าน Cyber Resilience ระเบียบวิธีปฏิบัติ และเทคโนโลยี การบริหารจัดการความเสี่ยงด้านไซเบอร์ การบริหารจัดการบุคลากรและการฝึกอบรม

โดเมนที่ 2: Identification การระบุและบริหารจัดการทรัพย์สิน

บริษัทควรจะต้องมีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เช่น มีการทำทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ครอบคลุมอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ระบบงาน และข้อมูล ที่สามารถเชื่อมโยงกับเหตุการณ์การคุกคามทางไซเบอร์ ซึ่งจะนำมาใช้บริหารจัดการ และระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ รวมถึงจะต้องมีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อข้อมูลลูกค้าเป็นประจำ ระบุขั้นตอนปฏิบัติ และระบบการจัดเก็บข้อมูลลูกค้า รวมถึงการจัดลำดับชั้นความลับของข้อมูล เป็นต้น

โดเมนที่ 3: Protection การป้องกัน

การป้องกันเพื่อไม่ให้เกิด Cyber Attack กับองค์กร ซึ่งบริษัทจำเป็นต้องมีการดำเนินการเพื่อป้องกันโครงสร้างพื้นฐาน เช่น เครือข่ายเน็ตเวิร์ค ภายใต้ scope ของการให้บริการ โดยจะต้องมีมาตรการควบคุมการเข้าใช้งานอุปกรณ์นั้น ๆ มีการตรวจสอบการตั้งค่าของอุปกรณ์ให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยอยู่เป็นประจำ รวมถึงการควบคุมการเข้าใช้งานอุปกรณ์เหล่านั้นด้วย โดยบริษัทจะต้องมีการพิสูจน์ตัวตนทั้งระดับ Physical และ Logical เพื่อใช้ควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System) ระบบงาน (Application) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร Communication) และบริษัทต้องกำหนดนโยบายการตั้งรหัสผ่าน (Password Policy) ที่ครอบคลุมการกำหนดระดับความซับซ้อนของรหัสผ่าน จำนวนครั้งสูงสุดของการใส่รหัสผ่านผิด และเงื่อนไขการตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม เป็นต้น ทั้งนี้การกำหนดสิทธิ์การเข้าถึงระบบงานและข้อมูลลับให้พนักงานตามขอบเขตหน้าที่ความรับผิดชอบของแต่ละคนให้เป็นไปตามความจำเป็น (Least Privilege) และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี (Segregation of Duty) จะช่วยให้การป้องกันภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้ด้วย

การรักษาความมั่นคงปลอดภัยของข้อมูลก็เป็นส่วนควบคุมที่บริษัทจำเป็นต้องพิจารณาให้ความสำคัญและปฏิบัติตามเช่นกัน เช่น การรักษาความปลอดภัยของข้อมูลในอุปกรณ์ที่ใช้ปฏิบัติงานไม่ให้เกิดการรั่วไหล บริษัทต้องมีมาตรการดูแลจัดการป้องกันข้อมูลรั่วไหล หรือมีซอฟต์แวร์ที่ช่วยควบคุมการส่งข้อมูลออกนอกองค์กรไปสู่สาธารณะ หรือองค์กรอื่น ๆ หรือมีมาตรการและแนวทางในการจัดการทำลายข้อมูลที่ถูกบันทึกไว้ใน Hard disk ตามมาตรฐานสากล รวมถึงบริษัทต้องมีมาตรการในการตรวจสอบและปรับปรุง Patch ของระบบปฏิบัติการ (Operation System) และระบบงาน (Application) บนอุปกรณ์พกพาที่เชื่อมต่อกับระบบเครือข่ายภายในให้เป็นปัจจุบันอยู่เสมอ

หากบริษัทมีบริการเกี่ยวกับการเขียนโปรแกรม บริษัทควรจะมีกระบวนการพัฒนาโปรแกรมให้มีความมั่นคงปลอดภัย และกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (Secure Coding) และสอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าวด้วย โดยจะต้องมีการทดสอบเจาะระบบอย่างสม่ำเสมอ และทำ Source code review เป็นต้น

โดเมนที่ 4: Detection การตรวจจับ

บริษัทควรมีการตรวจสอบช่องโหว่ ประเมินผลกระทบของช่องโหว่ ติดตั้ง Anti Malware ที่อุปกรณ์ที่ใช้ให้บริการ บริษัทต้องมีการจำลองการโจมตีทางไซเบอร์ (Red teaming) โดยใช้สถานการณ์เสมือนจริงเพื่อใช้ประเมินระบบความมั่นคงปลอดภัยขององค์กร โดยจะต้องสามารถใช้ทดสอบกระบวนการป้องกัน การตรวจจับ การรับมือ และการกู้คืน โดยสถานการณ์จำลองควรที่จะนำเอาข้อมูลการรายงานเหตุการณ์จากการถูกโจมตีหรือภัยคุกคามทางไซเบอร์ จาก Cyber Threat Intelligence มาใช้ในการออกแบบสถานการณ์จำลองให้อยู่ในรูปแบบเสมือนจริง (Simulation Cyber Attack) และมีการทดสอบเจาะระบบโดยไม่มีการแจ้งเตือนหน่วยงานเฝ้าระวังการรักษาความมั่นคงปลอดภัยล่วงหน้า (Silent Mode) เพื่อให้มั่นใจได้ว่าบริษัทสามารถรับมือเมื่อมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นจริง ซึ่งบริษัทสามารถอ้างอิงตามแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง การทดสอบเจาะระบบแบบ Intelligence-led Penetration Testing (iPentest) ได้

นอกจากนี้บริษัทต้องจัดให้มีการจัดเก็บบันทึกเหตุการณ์ (Log)

- บันทึกการเข้าถึง (Access Log)
- บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ
- บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log)
- บันทึกด้านการรักษาความปลอดภัย (Security Event Log)

โดยบันทึกดังกล่าวต้องถูกจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด ด้วยวิธีการที่ปลอดภัย เพื่อให้สามารถสืบหาสาเหตุเมื่อเกิดเหตุการณ์ได้

การตรวจจับกิจกรรมที่ผิดปกติ (Anomalies Activity Detection) การบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management)

การแลกเปลี่ยนองค์ความรู้ภัยคุกคามทางไซเบอร์ภายในองค์กรให้เกิดความตระหนักรู้เกี่ยวกับภัยเหล่านี้เพื่อให้เกิดการสื่อสารที่ถูกต้องและเข้าใจสถานกาณ์ได้รวดเร็วขึ้น

โดเมนที่ 5: Response and Recovery

การเตรียมการเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Response Planning) จะช่วยเพิ่มประสิทธิภาพในการรับมือกับเหตุการณ์ภัยทางไซเบอร์ได้ บริษัทจึงควรมีแผน มาตรฐาน และระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ซึ่งรวมถึงการเก็บพยานหลักฐานทาง Digital (Digital Forensics) ไว้อย่างชัดเจน และจัดทำแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) และคู่มือการตอบสนอง (Playbook) สำหรับภัยไซเบอร์สำคัญที่บริษัทมีโอกาสเผชิญ โดยการจัดทำแผนนั้นจะต้องมีการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบเพื่อให้สามารถใช้อ้างอิงในการรับมือภัยคุกคาม ตอบสนองต่อเหตุการณ์ และกู้คืนระบบและข้อมูลได้อย่างรวดเร็วและทันการณ์ ทั้งนี้จำเป็นต้องมีกระบวนการทบทวนแผนฉุกเฉินเตรียมไว้โดยคำนึงถึงเหตุการณ์ความเสียหายครอบคลุมสถานการณ์จำลองต่าง ๆ ที่อาจเกิดขึ้น รวมถึงเหตุการณ์จากภัยไซเบอร์ที่อาจส่งผลกระทบรุนแรงอย่างน้อยครอบคลุมเหตุการณ์ บริษัทควรมีการกำหนดตัวชี้วัดและประเมินประสิทธิภาพการทำงานของหน่วยงาน CSIRT เช่น SLAs, KPI, และ Performance มีการบริหารจัดการเหตุการณ์ผิดปกติและแนวทางการจำกัดความเสียหาย รวมถึงสรุปเหตุการณ์ผิดปกติ ภัยคุกคาม หรือเหตุละเมิด (Violations) ทางไซเบอร์ที่เกิดขึ้นกับบริษัท เสนอคณะกรรมการบริษัท หรือคณะกรรมการที่เกี่ยวข้องรับทราบการส่งต่อและการรายงานข้อมูลเหตุการณ์ (Escalation and Reporting)

งานด้านการพัฒนาบุคลากร

การพัฒนาองค์กรสู่ความมั่นคงปลอดภัย

ปฏิเสธไม่ได้ว่าธุรกิจในปัจจุบันถูกขับเคลื่อนด้วยเทคโนโลยีซึ่งนอกจากการที่จะเลือกเฟ้นเทคโนโลยีที่ทันสมัย สามารถตอบโจทย์ธุรกิจได้แล้ว การเตรียมความพร้อมขององค์กรไม่ว่าจะเป็นโครงสร้างองค์กร กระบวนการปฏิบัติงานระหว่างผู้ที่เกี่ยวข้องกับเทคโนโลยีนั้น ๆ การพัฒนาหรือปรับเปลี่ยนทักษะที่จำเป็นของบุคลากร เป็นอีกส่วนที่จะทำให้เกิดการผสมผสานหลอมรวมเทคโนโลยีเหล่านั้นให้เข้ากับกระบวนการปฏิบัติงานเพื่อที่จะสามารถนำเทคโนโลยีมาใช้ในการผลักดันธุรกิจได้อย่างมีประสิทธิผล นอกจากการบริหารจัดการเทคโนโลยี กระบวนการทำงาน และการพัฒนาทักษะความสามารถของบุคลากรที่จะต้องมีความสอดคล้องแล้วนั้น การพัฒนาด้านความมั่นคงปลอดภัยให้กับองค์กรจะเป็นองค์ประกอบสำคัญอีกส่วนหนึ่งที่จะต้องมีการพัฒนาไปพร้อม ๆ กันเพื่อสร้างความเชื่อมั่นในการให้บริการ บทความนี้จะวิเคราะห์ถึงการพัฒนาด้านความมั่นคงปลอดภัยขององค์กรในแต่ละช่วงเวลาที่ผ่านมาซึ่งจะมีการยกระดับไปตามแต่ละช่วงเวลาดังนี้

การเสริมความมั่นคงปลอดภัยขององค์กรในช่วงที่จุดประสงค์ของการโจมตีมุ่งไปที่การทำให้เป้าหมายใช้การไม่ได้ เช่น มัลแวร์ที่ทำให้เกิด Blue Screen หรือที่เรียกว่า The Blue Screen of Death หรือ Distributed Denial of Service นั้น องค์กรจะมุ่งเน้นไปที่การป้องกัน (Protect) เพื่อไม่ให้เกิดผลกระทบต่อบริการหรือการให้บริการเป็นหลักซึ่งวิธีการป้องกันต่าง ๆ นั้นจะอยู่ในรูปแบบของ signature หรือ กระบวนการตอบสนองที่มีการเตรียมการไว้ ในช่วงเวลาต่อมาแม้ว่าจะมีกลไกและมาตรการเพื่อการป้องกันอย่างเข้มแข็งก็ตาม แต่มิจฉาชีพก็พยายามที่จะหลบหลีกแนวป้องกันดังกล่าวโดยการพัฒนาเทคนิคการโจมตีใหม่ ๆ ทำให้การป้องกันแบบเดิมซึ่งก็คือ signature base ไม่สามารถตรวจจับความผิดปกติได้ องค์กรจึงจำเป็นต้องใช้เทคโนโลยีด้านการตรวจจับและพัฒนาทักษะการตรวจจับ (Detect) ให้เท่าทันมิจฉาชีพเพื่อที่จะสามารถตรวจจับสัญญาณของความผิดปกติที่มักจะเกิดขึ้นในช่วงแรกของการพยายามเจาะระบบให้ถึงเป้าหมาย ด้วยเทคนิคผสมผสานเทคนิครูปแบบใหม่กับเทคนิครูปแบบเดิม ซึ่งเมื่อตรวจจับสัญญาณของความผิดปกติในบางช่วงบางตอนได้แล้ว จะต้องวิเคราะห์ความเป็นไปได้ของความสำเร็จของการโจมตี และมีการเตรียมแผนการตอบสนอง (Respond) และกู้คืน

ระบบในส่วนที่ได้รับผลกระทบ (Recover) เราทราบกันดีว่ากรอบการทำงานเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กรนี้คือ NIST Cybersecurity Framework ซึ่งเป็นกรอบการทำงานที่จะสร้างให้องค์กรมีความพร้อมรับมือกับภัยคุกคามทางไซเบอร์ (Cyber resilience) โดยหัวใจในการสร้างให้องค์กรมีความสามารถในการพร้อมรับมือต่อรูปแบบภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา ไม่สามารถคาดเดากระบวนท่าได้และอาจจะเกิดขึ้นกับองค์กรท่านเป็นองค์กรแรกนั้นคือ การประสานความร่วมมือของหน่วยงานต่าง ๆ ในองค์กรแบบมีความเข้าใจในสถานการณ์ เข้าใจผลกระทบและกำหนดทิศทาง รวมถึงกลยุทธ์ในการแก้ไขสถานการณ์ โดยข้อมูลข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence) เป็นองค์ประกอบที่สำคัญในการประเมินผลกระทบที่อาจจะตามมา ฉะนั้นองค์กรจะต้องมีการจัดโครงสร้างองค์กร เตรียมเครื่องมืออุปกรณ์สำรอง จัดเตรียมกระบวนการประสานงานเพื่อพร้อมรับมือภัยคุกคามทางไซเบอร์ และตระเตรียมศักยภาพขององค์กรต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

การพัฒนาองค์กรให้มีความมั่งคงปลอดภัยจากจุดนี้ไป แม้ว่าองค์กรจะมีความพร้อมในการพร้อมรับมือกับภัยคุกคามทางไซเบอร์ (Cyber resilience) แล้ว ความพร้อมหรือความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์นั้นจะต้องพัฒนาต่อไปเพื่อที่จะสามารถสนับสนุนเป้าหมายทางธุรกิจในระยะยาว เช่น ความสามารถในการสร้างความเชื่อมั่นให้กับผู้ใช้งานต่อการจัดการเหตุการณ์ต่าง ๆ ทางไซเบอร์ได้อย่างมีประสิทธิผล การวิเคราะห์และกลั่นกรองข้อมูลที่ใช้ในการประเมินสถานการณ์และผลกระทบที่อาจจะเกิดขึ้น ซึ่งอาจจะออกมาในรูปแบบของแผนรองรับต่าง ๆ ที่แสดงถึงกลยุทธ์ในการตอบสนองต่อเหตุการณ์ ในแผนรับรองหรือกลยุทธ์ในการตอบสนองต่อเหตุการณ์จะต้องมีแนวทางที่ชัดเจนในการช่วยเหลือผู้ใช้บริการให้มีผลกระทบน้อยที่สุด เป็นต้น นี่ก็คือการยกระดับองค์กรให้มีความมั่นคงปลอดภัยและสร้างความยั่งยืนให้กับองค์กร และเป็นมุมมองของธีมงาน Annual Conference ของ TB-CERT ในปี 2023 ที่ผ่านมาในชื่อธีมว่า “Sustainable Cybersecurity”

งานสัมมนาประจำปี TB-CERT Cybersecurity Annual Conference 2023

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT (TB-CERT) สมาคมธนาคารไทย จัดงานสัมมนาประจำปีด้านความมั่นคงปลอดภัยไซเบอร์ TB-CERT Cybersecurity Annual Conference 2023 ภายใต้หัวข้อหลัก “Sustainable Cybersecurity” เมื่อวันที่ 22 กันยายน 2566 ณ โรงแรม The Athenee Hotel, a Luxury Collection Hotel, Bangkok” เพื่อเผยแพร่ความรู้และสร้างความตระหนักถึงการเตรียมพร้อมและยกระดับด้านความมั่นคงปลอดภัยไซเบอร์ให้กับสมาชิกและบุคลากรในอุตสาหกรรมภาคการเงินการธนาคาร การลงทุน ประกันภัย รวมทั้งภาคอุตสาหกรรมอื่น ๆ ที่เกี่ยวข้อง โดยได้รับเกียรติจาก 1) คุณผยง ศรีวณิช กรรมการผู้จัดการใหญ่ ธนาคารกรุงไทย จำกัด (มหาชน) และประธานสมาคมธนาคารไทย กล่าว Welcome Address 2) ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กล่าว Opening Speech และ 3) คุณเดช ฐิติวณิช ผู้ช่วยผู้ว่าการสายระบบข้อสนเทศ ธนาคารแห่งประเทศไทย กล่าว Special Event Keynote และวิทยากรจากหน่วยงานผู้สนับสนุน ไม่ว่าจะเป็น Keynote Speaker โดยบริษัท Gartner รวมทั้งการออกบูธแสดงเทคโนโลยีและโซลูชันจากองค์กรชั้นนำทั่วโลกผู้สนับสนุนการจัดงานถึง 17 บูธ มีผู้เข้าร่วมงานจากภาคธนาคาร และหน่วยงานอื่น ๆ รวมกว่า 500 ท่าน นอกจากนี้ ยังมีการจัดแข่งขัน TB-CERT Cyber Combat ประจำปี เพื่อฝึกทักษะในการปฏิบัติการเชิงรุกและเชิงรับของบุคลากรในภาคการธนาคารและหน่วยงานพันธมิตรอีกด้วย ซึ่งได้รับการสนับสนุนระบบการฝึกดังกล่าวจากบริษัท Cyberbit

สำหรับหัวข้อ Sustainable Cybersecurity ในปีนี้ ถูกคิดขึ้นมาเพื่อให้องค์กรตระหนักในด้านการสร้างความยั่งยืนด้านความมั่นคงปลอดภัยไซเบอร์ เนื่องด้วยความก้าวหน้าทางเทคโนโลยีที่ทำให้เกิดการเปลี่ยนแปลงในการดำเนินการทางธุรกิจ พฤติกรรมของผู้ใช้บริการ สภาพกิจกรรมทางสังคม รวมทั้งการพัฒนาบุคลากรให้มีทักษะเหมาะสมกับยุคดิจิทัล ด้วยการเปลี่ยนแปลงและความซับซ้อนนี้ก่อให้เกิดความท้าทายจากการถูกโจมตีโดยอาศัยเทคโนโลยีด้วยเช่นกัน นอกจากองค์กรจะต้องสร้างศักยภาพให้มีความสามารถในการกู้คืนธุรกิจให้สามารถกลับมาให้บริการได้อย่างรวดเร็ว (Organizational Resiliency) แล้ว องค์กรจะต้องพิจารณากรอบแนวคิดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เดิม และพัฒนาเพิ่มเติมเพื่อให้เกิดความยั่งยืน ซึ่งไม่เพียงเพื่อเพิ่มความสามารถในการรับมือกับภัยคุกคามที่เปลี่ยนแปลงอย่างไม่เคยเกิดขึ้น แต่จากกรอบแนวคิดนี้จะต้องช่วยสนับสนุนเป้าหมายองค์กรในระยะยาวโดยไม่ลดทอนความสามารถในการดำเนินการให้บรรลุเป้าหมายธุรกิจในอนาคตอีกด้วย ดังนั้น ความยั่งยืนด้านไซเบอร์จึง

เป็นหัวข้อสำคัญในการแลกเปลี่ยนมุมมองต่อแนวทางการพัฒนา ปัญหา และอุปสรรค หรือแนวทางการสนับสนุนจากส่วนต่าง ๆ เพื่อให้เกิดความยั่งยืนด้านความ มั่นคงปลอดภัยไซเบอร์ของสังคมเศรษฐกิจดิจิทัล

คุณผยง ศรีวณิช กรรมการผู้จัดการ ธนาคารกรุงไทย และประธานสมาคมธนาคารไทย ได้กล่าวถึงความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการป้องกันภัยไซเบอร์ อาทิ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งความร่วมมือในการป้องกันภัยทุจริตออนไลน์ อาทิ การใช้เทคโนโลยี AI ในการตรวจจับรูปแบบการฉ้อโกงออนไลน์ ซึ่งหน่วยงานภาครัฐก็ได้ให้ความสำคัญกับประเด็นเร่งด่วนดังกล่าว โดยมีบทบาทสำคัญในการเสนอและบังคับใช้กฎหมายที่ช่วยอำนวยความสะดวกในการดำเนินงานของภาคการธนาคาร และสำหรับการจัดงานสัมมนาในครั้งนี้จะเป็นโอกาสในการแลกเปลี่ยนมุมมอง การเสริมสร้างความร่วมมือภายในและนอกสายงานด้านการเงินการธนาคาร รวมทั้งการเพิ่มความตระหนักในความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ ที่จะนำไปสู่ความปลอดภัยไซเบอร์ที่ยั่งยืนได้

ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กล่าวว่า ความมั่นคงปลอดภัยทางไซเบอร์ที่ยั่งยืนไม่ใช่ทางเลือกแต่เป็นเรื่องที่จำเป็น เนื่องจากเป็นประเด็นที่มีความเกี่ยวข้องทางเศรษฐกิจและสังคมอย่างหลีกเลี่ยงไม่ได้ ตราบใดที่สังคมยังต้องเปลี่ยนแปลงไปสู่ดิจิทัลที่เติบโตขึ้นเรื่อย ๆ ความมั่นคงปลอดภัยไซเบอร์เป็นรากฐานที่สำคัญอย่างหนึ่งของระบบการเงินที่แข็งแกร่งทั้งในปัจจุบันและอนาคต กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เป็นหน่วยงานหลักในการขับเคลื่อนด้านดิจิทัลของประเทศซึ่งได้ดำเนินการในหลายประเด็น อาทิ G-Cloud High Society, G-Cloud Data Protection และยังดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ในลักษณะเชิงรุกอีกด้วย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ให้ความสำคัญกับแก้ไขปัญหาภัยทุจริตออนไลน์และความเสี่ยงจากการโจมตีทางไซเบอร์ เนื่องจากปัญหาเหล่านี้มีผลกระทบต่อประชาชนในวงกว้างและส่งผลต่อความสูญเสียทางเศรษฐกิจ โดยเฉพาะอย่างยิ่งผลกระทบต่อภาคการเงินการธนาคารที่มักตกเป็นเป้าหมายและถูกใช้เป็นเครื่องมือในการหลอกลวงประชาชนและการทำธุรกรรมที่ผิดกฎหมาย โดยกระทรวงฯ ได้มีความร่วมมือกับธนาคารและหน่วยงานโทรคมนาคมอย่างเต็มที่เพื่อแก้ไขปัญหาที่เกิดขึ้น เราได้กำหนดมาตรการและกลยุทธ์ซึ่งเน้นในสามมิติหลักคือ การป้องกัน การระงับ และการยับยั้ง (Prevention, Interception, and Suppression) ซึ่งปัจจุบันทางธนาคารและหน่วยงานที่เกี่ยวข้องสามารถมีแนวทางที่สะดวกรวดเร็วมากขึ้นในการจัดการกับการฉ้อโกงออนไลน์จากการบังคับใช้พระราชกฤษฎีกาเรื่องการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ และหวังเป็นอย่างยิ่งว่า การสัมมนาในวันนี้ จะเป็นการหารือและแลกเปลี่ยนความรู้ด้านความมั่นคงปลอดภัย

ไซเบอร์ที่สำคัญ อันจะนำไปสู่ความร่วมมือประสานงานระหว่างภาครัฐและเอกชน ที่จะสร้างนโยบายและแนวปฏิบัติที่ดีที่สุดเพื่อการก้าวไปสู่ความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืนสำหรับประเทศไทย

คุณเดช ฐิติวณิช ผู้ช่วยผู้ว่าการ สายระบบข้อสนเทศ ธนาคารแห่งประเทศไทย ได้กล่าวในช่วง Special Event Keynote ถึงวิสัยทัศน์สำหรับภูมิทัศน์ใหม่ภาคการเงินประเทศไทยเพื่อเศรษฐกิจดิจิทัลและการเติบโตอย่างยั่งยืน ซึ่งในรายงานดังกล่าวมีหลายประเด็นที่กล่าวถึงความยั่งยืน ไม่ว่าจะเป็นด้านสิ่งแวดล้อม การพัฒนาระบบการชำระเงิน และอีกหนึ่งประเด็นสำคัญคือเรื่องของการใช้เทคโนโลยีและข้อมูลในการสร้างสรรค์นวัตกรรม ซึ่งนวัตกรรมจะช่วยเพิ่มประสิทธิภาพและการเข้าถึงบริการทางการเงินได้ผ่าน 3 หลักการ ได้แก่ 1) การเปิดกว้างในการแข่งขัน (Open Competition) รวมถึงการขยายขอบเขตธุรกิจและความยืดหยุ่นในการดำเนินการธุรกิจของธนาคารและสถาบันการเงินนอกธนาคาร และผู้ที่เข้าสู่ตลาดใหม่ ภายใต้การควบคุมโดยการประเมินความเสี่ยงและในสภาวะการแข่งขันเท่าเทียมและไม่สร้างการครอบครองตลาดที่ไม่เป็นธรรม 2) การเปิดกว้างให้ผู้ให้บริการกลุ่มต่าง ๆ เข้าถึงโครงสร้างพื้นฐานทางการเงินอย่างเหมาะสมและเป็นธรรม (Open Infrastructure) ซึ่งโครงสร้างพื้นฐานนี้จะส่งเสริมกระบวนการเปลี่ยนแปลงไปสู่ความเป็นเศรษฐกิจดิจิทัลมากยิ่งขึ้น เช่น การพัฒนา PromptBiz และ 3) การเปิดกว้างให้มีการใช้ประโยชน์จากข้อมูล (Open Data) ซึ่งจะสนับสนุนให้เกิดการพัฒนาบริการทางการเงินที่ดีขึ้น

การที่เราได้ใช้ประโยชน์จากเทคโนโลยี ในอีกด้านได้เปิดโอกาสให้ผู้ไม่หวังดีหาทางโจมตีหรือหลอกลวงทางดิจิทัลมากขึ้น ความมั่นคงปลอดภัยทางไซเบอร์ที่ยั่งยืนจึงเป็นสิ่งที่สำคัญอย่างมาก สถาบันการเงินและองค์กรต่าง ๆ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ที่แข็งแกร่งเพื่อปกป้อง ตรวจจับ ตอบสนอง และกู้คืนจากเหตุการณ์ที่เกิดขึ้นอย่างรวดเร็ว นอกจากนี้ หลายครั้งที่เราโดนโจมตีจากจุดอ่อนของมนุษย์ จึงเป็นสิ่งสำคัญที่จะต้องเพิ่มพูนความรู้และสร้างความตระหนักรู้ให้กับทุกคน เพราะบุคคล กระบวนการ และเทคโนโลยี (People, Process, and Technology) เป็นเสาหลักที่สำคัญของความมั่นคงทางไซเบอร์ ซึ่งภาคการเงินจำเป็นต้องสร้างสมดุลระหว่างการส่งเสริมนวัตกรรมและการจัดการความเสี่ยงด้านไซเบอร์ เพื่อให้ภาคการเงินสามารถปรับตัวกับความท้าทายใหม่ ๆ ในขณะที่ยังคงมีประสิทธิภาพในการป้องกัน และสามารถเดินหน้าสู่เศรษฐกิจดิจิทัลที่ยั่งยืน โดยธนาคารแห่งประเทศไทยมีความยินดีที่จะร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับทุกองค์กรและบุคลากรที่เกี่ยวข้อง เพื่อสร้างความเชื่อมั่นให้กับระบบการเงินต่อไป

สำหรับการจัดงานในครั้งนี้ TB-CERT ขอขอบคุณแขกผู้มีเกียรติทุกท่านทั้งในและต่างประเทศ และบริษัท Partner ต่าง ๆ ที่สละเวลามาร่วมงานและแสดงนิทรรศการเทคโนโลยีและนำเสนอโซลูชันที่น่าสนใจมากมาย ได้แก่ บริษัท Cisco และ NTT, บริษัท Imperva, บริษัท Akamai Technologies, บริษัท Trellix บริษัท Forcepoint, บริษัท Kaspersky, บริษัท Mandiant, บริษัท Yip In Tsoi และ Zscaler, บริษัท Check Point, บริษัท CrowdStrike, บริษัท Datadog, บริษัท Dell Technologies ร่วมกับ Microsoft และ Intel, บริษัท Fortinet, บริษัท SecIron, บริษัท SentinelOne, บริษัท Splunk และบริษัท Trend Micro ซึ่งช่วยให้งานสัมมนา TB-CERT Cybersecurity Annual Conference 2023 ในปีนี้เสร็จสิ้นสมบูรณ์ไปด้วยดีตามวัตถุประสงค์ของงาน หวังเป็นอย่างยิ่งว่าทุก ๆ ท่านจะได้เพิ่มพูนความรู้และอัปเดตเทคโนโลยีใหม่ ๆ จากงานครั้งนี้ไปไม่มากก็น้อย รวมถึงได้แลกเปลี่ยนข้อมูลข่าวสารและสร้างความสัมพันธ์ที่ดีทั้งภายในและภายนอกหน่วยงาน

ประมวลภาพการจัดงาน TB-CERT Cybersecurity Annual Conference 2023

Welcome Address

Khun Payong Srivanich

CEO, Krung Thai Bank

Chairman of The Thai Bankers' Association

Opening Remarks

Professor Wisit Wisitsora-at

Permanent Secretary,
Ministry of Digital Economy and Society

Special Event Keynote

Khun Dej Titivanich

Assistant Governor, Information Technology Group,
Bank of Thailand

Keynote Speaker

"Top Trend Towards Sustainable Cybersecurity"

Mr. Jonathan Krause

Vice President & Executive Partner (SE Asia),
Gartner Executive Programs,
Gartner Advisory (Singapore) Pte. Ltd.

Panel Discussion

"The Road to Sustainability in Cybersecurity, Obstacles, Challenges, and Expectation"

Moderator:

Dr. Wit Sittivaekin, Program Host, The Standard Wealth

Panelist:

1. Khun Chatchawat Asawarakwong
   Vice Chairman of TB-CERT
   CISO of KASIKORN Business-Technology Group [KBTG]
2. Khun Chaolvalit Rattanakornkrisri
   Director, Cloud Solution, Microsoft Thailand
3. Khun Vilaiporn Taweelappontong
   Consulting Leader, PwC Thailand Financial Services
   Strategy and Operations Leader, PwC Southeast Asia Consulting

Recap & Closing

Dr. Kitti Kosavisutte

Chairman of TB-CERT
CISO of Bangkok Bank

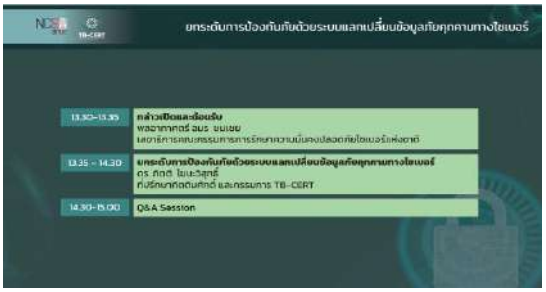
งานด้านการสร้างความตระหนักรู้ด้านภัยไซเบอร์
Cybersecurity Proficiency Development Program
(Webinar & Workshop)

Webinar workshop: การวิเคราะห์ภัยคุกคามทางไซเบอร์ให้กับธนาคารสมาชิก

วันที่ 12-13 มกราคม 2566 TB-CERT ได้จัดการสัมมนาออนไลน์ ด้านการวิเคราะห์ภัยคุกคามทางไซเบอร์ให้กับธนาคารสมาชิก ในหัวข้อต่าง ๆ ดังนี้ 1) การใช้งานระบบ MISP 2) การวิเคราะห์ภัยคุกคามและมัลแวร์ 3) การนำข้อมูลภัยคุกคามมาสร้าง Indicator of Compromise (IOC) 4) อบรมการแชร์ข้อมูลตาม TLP และการนำไปใช้งาน

Webinar: ยกระดับการป้องกันภัยด้วยระบบแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

TB-CERT ร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดงานสัมมนาออนไลน์ในหัวข้อ “ยกระดับการป้องกันภัยด้วยระบบแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์” ในวันที่ 17 มีนาคม 2566



Webinar workshop หัวข้อ “รู้มั้ยแกะ C2 ง่ายนิดเดียว”

TB-CERT จัดงานสัมมนาออนไลน์ในหัวข้อ “รู้มั้ยแกะ C2 ง่ายนิดเดียว” ในวันที่ 7 เมษายน 2566 โดยคุณสัญจร กีรติรังสรรค์ วิทยากร ได้แชร์ความรู้เกี่ยวกับแอปดูดเงินแต่ละประเภท ได้เรียนรู้และรู้จักการทำงานของแอปดูดเงินในเบื้องต้น การวิเคราะห์ไฟล์ APK การหา C2 จาก APK

งานสัมมนา หัวข้อ “Future of Cyber Threat Intelligence”

TB-CERT ร่วมกับ Financial Services Information Sharing and Analysis Center (FS-ISAC) จัดงานสัมมนาในหัวข้อ Future of Cyber Threat Intelligence: Emerging trends, AI and how they impact the future of cybersecurity เมื่อวันที่ 25 เมษายน 2566

งานสัมมนา Future of Thailand's Financial Services Executive Forum

TB-CERT ร่วมกับ บริษัท Amazon Web Services (AWS) ในการจัดงานสัมมนา Future of Thailand's Financial Services Executive Forum เพื่อรับฟังแนวโน้มการบริการทางการเงินรวมถึงความมั่นคงปลอดภัยไซเบอร์ และความร่วมมือจาก AWS ในการสนับสนุนนวัตกรรมที่เกี่ยวข้องกับบริการทางการเงินและระบบคลาวด์ของผู้ให้บริการทางการเงินดังกล่าว เมื่อวันที่ 17 พฤษภาคม 2566

Webinar “Android accessibility service”

TB-CERT ได้จัด online session เพื่ออัปเดตความรู้ทางเทคนิคเกี่ยวกับ Android accessibility service เมื่อวันที่ 18 สิงหาคม 2566

การซ้อมรับมือภัยไซเบอร์ภาคการธนาคาร (Banking Cyber Drill)

การซ้อมรับมือภัยไซเบอร์ภาคการธนาคารในปีนี้ จัดขึ้นเมื่อวันที่ 15 พฤศจิกายน 2566 ในรูปแบบ Hybrid Exercise มีผู้แทนหน่วยงานสมาชิก TB-CERT ตามบทบาทต่าง ๆ ที่เกี่ยวข้องเข้าร่วมรวมกว่า 500 คน TB-CERT ได้ใช้รูปแบบการซักซ้อมให้เสมือนจริง โดยเฉพาะในส่วนของทีมเทคนิค (SOC) ที่ได้มีการจำลองระบบการบริการสำคัญของธนาคารให้ทีมเทคนิคได้ลงมือปฏิบัติค้นหาร่องรอยการโจมตี ซึ่งเป็นหนึ่งในทักษะด้านไซเบอร์ที่ทีม SOC ควรมี และได้ใช้แพลตฟอร์ม Rattanakosin ซึ่งเป็นแพลตฟอร์มสำหรับการซักซ้อมรับมือภัยไซเบอร์โดยสามารถใช้ในการสื่อสารความเห็น การแลกเปลี่ยนข้อมูล โดยสามารถรองรับจำนวนผู้เข้าร่วมการซักซ้อมแบบ Online ได้จำนวนมาก ผู้ที่เข้าร่วมซักซ้อมการเผชิญเหตุสามารถให้ความเห็นมีส่วนร่วมในการตัดสินใจ ในบทบาทของตนเอง เมื่อทีมเทคนิค (SOC) ได้วิเคราะห์ข้อมูลจากระบบจำลองจะแจ้งข้อมูลเหล่านั้นและให้ข้อมูลสถานการณ์ที่พบให้กับผู้ที่เข้าร่วมซักซ้อมในแต่ละบทบาท จึงเป็นการซักซ้อมแบบผสมผสานระหว่างทีมเทคนิคที่ลงมือปฏิบัติเหมือนเป็นการเผชิญเหตุร่วมกับทีมอื่น ๆ ที่เกี่ยวข้องในสถานการณ์ได้อย่างครบถ้วน

หัวข้อการซักซ้อม

"Disinformation and Fraudulent in Banking Service"
เกิดเหตุการณ์โจมตีช่องโหว่ที่ส่งผลกระทบกับระบบงานสำคัญที่มีการเก็บข้อมูลลูกค้า
อีกทั้งยังเกิดเหตุการณ์ขู่เรียกค่าไถ่จากกรณีข้อมูลลูกค้ารั่วไหล
ส่งผลต่อความเชื่อมั่นของประชาชนต่อสถาบันการเงิน

วัตถุประสงค์

1. **เพื่อยกระดับการประเมินผลกระทบต่อเหตุการณ์โจมตีทางไซเบอร์ที่เกิดขึ้น**
2. **เพื่อยกระดับทักษะในการวิเคราะห์การโจมตีทางไซเบอร์ การตอบสนองต่อการแจ้งเตือนภัยคุกคามที่ได้รับจาก Threat Intelligence รวมถึงการประเมินแนวทางแก้ไขและป้องกันเหตุในอนาคต ในระดับผู้ปฏิบัติงานด้วยระบบจำลอง**
3. เพื่อซักซ้อมขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติจากการโจมตีทางไซเบอร์ และกระบวนการประสานงานระหว่างผู้เกี่ยวข้อง ทั้งภายในหน่วยงานสมาชิก TB-CERT และหน่วยงานภายนอก
4. เพื่อยกระดับการซ้อมรับมือภัยไซเบอร์ให้ผู้บริหารได้มีปฏิสัมพันธ์กับผู้ปฏิบัติงาน โดยจำลองสถานการณ์การซ้อมให้มีการร่วมกันตัดสินใจในการแก้ไขสถานการณ์โดยเฉพาะในสภาวะวิกฤต (crisis)

5. เพื่อพัฒนากระบวนการรับมือภัยโจมตีทางไซเบอร์ให้มีประสิทธิภาพและสื่อสารต่อสาธารณะได้อย่างเหมาะสมกับภาคการธนาคาร
6. เพื่อพัฒนากระบวนการประสานงานของหน่วยงาน CII และ TB-CERT ในฐานะเป็น Sectorial CERT ไปยัง Regulator, NCSA ตาม พ.ร.บ. ไซเบอร์ และ สคส. ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

จากสถานการณ์จำลองที่ใช้ในการซักซ้อมในปีนี้ถูกออกแบบให้มีประเด็นเหตุการณ์ที่หลากหลาย โดยเกิดขึ้นในช่วงเวลา 1 วันของการซักซ้อม ไม่ว่าจะเป็นเหตุการณ์การถูกโจมตีจากช่องโหว่ของ Library ที่มีการใช้งานอย่างแพร่หลายในหลายองค์กรทั่วโลก ซึ่งองค์กรของผู้เข้าร่วมซักซ้อมอาจจะมีแนวโน้มที่จะมีช่องโหว่นั้นด้วย การประเมินสถานการณ์ในช่วงต้นที่ข้อมูลยังไม่เพียงพอ และยังไม่ได้รับการยืนยันแน่ชัด จึงเป็นส่วนหนึ่งของสถานการณ์จำลองที่ให้ทีมเทคนิคได้คิดวิเคราะห์ บันทึก สอบทานและเพิ่มเติมเข้าไปในคู่มือ Cyber Incident Response Plan ว่าจะต้องมีการตรวจสอบและยืนยันความถูกต้องของข้อมูล รวมถึงแหล่งข้อมูลที่น่าเชื่อถือต่าง ๆ ร่วมด้วย โดยหน่วยงานที่ระบุว่าเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของภาคการธนาคาร ยังจำเป็นต้องปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อให้เกิดการเตรียมการสำหรับการปฏิบัติตามกฎหมาย นอกจากนี้สถานการณ์จำลองยังเกี่ยวข้องกับข้อมูลรั่วไหล ซึ่งหน่วยงานที่มีข้อมูล PII สำคัญเก็บไว้จำเป็นต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อีกด้วย

จากการซักซ้อมครั้งนี้ แสดงถึงความพร้อมของหน่วยงานในภาคการธนาคารในการตอบสนองต่อเหตุการณ์การโจมตี รวมถึงการควบคุมเหตุการณ์เพื่อมิให้มีการลุกลามบานปลาย (Containment) ให้เป็นไปอย่างมีประสิทธิภาพ แต่เนื่องจากช่วงแรกของเหตุการณ์จะยังมีความไม่ชัดเจนในสถานการณ์ที่เกิดขึ้น เนื่องจากข้อมูลยังมีเพียงบางส่วนและจะอยู่ในระหว่างที่ทีมงานที่เกี่ยวข้อง โดยเฉพาะทีมงานด้านเทคนิคจะยังคงวิเคราะห์สถานการณ์และยังไม่สามารถสรุปสาเหตุหรือลักษณะของการโจมตีได้ การประเมินผลกระทบจะยังอยู่บนข้อจำกัด ส่วนในช่วงท้ายมีเหตุการณ์ที่พบข้อมูลรั่วไหลและมีข้อมูลที่บิดเบือนความจริงร่วมด้วย (Disinformation) ในสถานการณ์จริงอาจจะมีการส่งต่อแพร่กระจายสร้างผลกระทบในวงกว้าง ขั้นตอนของการประเมินสถานการณ์และการประเมินผลกระทบจึงมีบทบาทสำคัญจริง ๆ เพื่อให้ได้ข้อสรุปแนวทางในการสื่อความของระดับภาคการธนาคาร ผู้ที่เข้าร่วมซักซ้อมจะต้องพิจารณาประเด็นความเสี่ยงและผลกระทบในด้านต่าง ๆ ไม่ว่าจะเป็นด้านลูกค้า ด้านความเสียหาย ด้านชื่อเสียง และด้านกฎหมาย ให้รอบด้าน เพื่อการฝึกกำหนดกลยุทธ์และแนวทางการจัดการเหตุได้อย่างทันท่วงทีเช่นเดียวกันกับขั้นตอนการปฏิบัติงานตามสถานการณ์จริงที่เกิดขึ้น

การแข่งขันทักษะทางไซเบอร์ภาคการธนาคาร (Cyber Combat)

การแข่งขันทักษะทางไซเบอร์ภาคการธนาคารในปีนี้ TB-CERT ได้ใช้รูปแบบการแข่งขันที่ใช้ระบบจำลองการโจมตีองค์กรเสมือนจริง (Enterprise Attack Simulation) โดยเริ่มจากรอบคัดเลือก เพื่อคัดทีมจำนวน 16 ทีมที่ผ่านเข้าสู่รอบการแข่งขัน โดยในรอบการแข่งขันนั้นจะแบ่งออกเป็น 2 รอบ ซึ่งจะเก็บคะแนนทั้ง 2 รอบมารวมกันเพื่อหาทีมผู้ชนะ โดยได้มีการประเมินทักษะความสามารถของทีมผู้เข้าร่วมแข่งขัน ที่ออกแบบและประเมินโดยอ้างอิงตามกรอบ NICE Framework ซึ่งเป็นมาตรฐานสากลที่นิยมใช้กันอย่างแพร่หลายที่พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST 800-181 Rev1) เพื่อใช้ในการประเมิน การวางแผน และการพัฒนาบุคลากร ซึ่งเป็นข้อมูลอ้างอิงสำหรับการกำหนดบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับงานด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการแสดงข้อมูลความสัมพันธ์ระหว่างองค์ความรู้ (Knowledge) ทักษะ(Skills) และความสามารถ (Abilities) ด้านต่าง ๆ ที่จำเป็นกับบทบาทหน้าที่ในสายงานความมั่นคงปลอดภัยไซเบอร์

โจทย์การโจมตีองค์กรเสมือนจริง (Enterprise Attack Simulation) แบ่งออกเป็นการโจมตีในด้านต่าง ๆ ดังนี้

โจทย์ที่ 1 เป็นการโจมตีแบบ Cross Site Scripting (XSS) และหลอกเหยื่อในองค์กรให้ติดตั้งโปรแกรมดักจับข้อมูล หรือ Keylogger จากนั้นจะทำการขยายผลการโจมตีไปยัง Domain controller และทำการขโมยข้อมูลขององค์กรออกไป

โจทย์ที่ 2 เป็นการโจมตีโดยใช้สื่อ Removable Media และได้ทำการขยายผลการโจมตีโดยใช้มัลแวร์ประเภท Worm เพื่อแพร่กระจายไปยังระบบอื่นๆ ในองค์กร

โจทย์ที่ 3 เป็นการโจมตีโดยใช้ Phishing ที่สามารถหลบหลีกการตรวจจับโดยใช้เทคนิคที่เรียกว่า Steganography หรือการอำพรางข้อมูลเพื่อหลบหลีกการตรวจจับ จากนั้นได้ติดตั้งโปรแกรม Trojan เพื่อขโมยข้อมูลออกจากองค์กรไปภายนอก

จากการแข่งขันทักษะทางไซเบอร์ดังกล่าว ได้ดำเนินการสำเร็จลุล่วงตามวัตถุประสงค์ โดยผู้เข้าแข่งขันจากธนาคารสมาชิกและหน่วยงานพันธมิตรของ TB-CERT จะได้ความรู้ ความเข้าใจ และการปฏิบัติการรับมือต่อภัยทางไซเบอร์ เป็นสร้างความคุ้นเคยกับลักษณะการโจมตีด้วยสถานการณ์จำลองเหตุการณ์ทางไซเบอร์เพื่อเตรียมความพร้อมในการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ทุกเวลา สมาชิกในทีมจะได้รับการฝึกฝนและพัฒนาทักษะความปลอดภัยทางไซเบอร์ รวมทั้งการสร้างเครือข่ายด้านความปลอดภัยทางไซเบอร์ในภาคการธนาคารของประเทศไทย และหน่วยงานพันธมิตรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อื่น ๆ

งานด้านการสร้างความร่วมมือ

งานและกิจกรรมภายใต้ความร่วมมือ

สร้างความร่วมมือกับ CERT และหน่วยงานต่าง ๆ ในประเทศไทย

สร้างความร่วมมือกับหน่วยงานภายใต้ MOU CERT Readiness ภาคการเงิน

สร้างความร่วมมือกับต่างประเทศ

สร้างความร่วมมือภายใน TB-CERT

- ออกบูธแสดงนิทรรศการด้านความมั่นคงปลอดภัยไซเบอร์ ภายในงาน Thailand National Cyber Week 2023 วันที่ 17-18 กุมภาพันธ์ 2566 ณ มิตรทาวน์ฮอลล์ สามย่านมิตรทาวน์ จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อเผยแพร่ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สร้างความตระหนักและระมัดระวัง เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์และพร้อมรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ
- ริเริ่มก่อตั้งกลุ่ม Thailand CERTs Community (THCC) ให้กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีหน่วยงาน Sectorial CERT ในประเทศไทยที่ทั้งเริ่มก่อตั้งและได้ก่อตั้งขึ้นแล้วเข้าร่วม วัตถุประสงค์เพื่อสร้างเครือข่ายความร่วมมือให้ครอบคลุม โดยได้จัดประชุมสัมมนาเชิงวิชาการเมื่อวันที่ 10-12 มิถุนายน 2566 มีหน่วยงาน CERT ต่าง ๆ เข้าร่วม ได้แก่ Thai-CERT, TB-CERT, TTC-CERT, MOT-CERT, NIA-CERT, Gov-CERT, Energy-CERT, TCM-CERT, TI-CERT, Health-CERT, MOD-CERT, CCIB, และ RTN
- กรรมการ TB-CERT และประธานสำนักงานระบบการชำระเงิน สมาคมธนาคารไทย คุณยศ กิมสวัสดิ์ ให้สัมภาษณ์ในรายการ กรุงเทพธุรกิจ BIZ INSIGHT เมื่อวันที่ 2 พฤษภาคม 2566 ในประเด็นเกี่ยวกับแอปดูดเงิน มาตรการของสมาคมธนาคารไทยในการปิดช่องทางจากมิจฉาชีพที่จะเข้าถึงประชาชน มาตรการในการตอบสนองและรับมือของสถาบันการเงิน รวมทั้งการยกระดับความปลอดภัยของ Mobil Banking Application
- ต้อนรับและหารือกับคณะอาจารย์จากมหาวิทยาลัยขอนแก่น เมื่อวันที่ 23 พฤษภาคม 2566 นำโดย อ.ดร.กิตติ์ เธียรธโนปจัย ผู้ช่วยอธิการบดีฝ่ายดิจิทัล มหาวิทยาลัยขอนแก่น เข้าหารือและศึกษาดูงาน TB-CERT โดยได้มีการนำเสนอประโยชน์ของการใช้ข่าวกรองภัยคุกคามไซเบอร์
- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ ร่วมเป็นวิทยากรในงานสัมมนา Smart Cybersecurity Summit Thailand เมื่อวันที่ 24 พฤษภาคม 2566 ณ ศูนย์ประชุมแห่งชาติสิริกิติ์ ในหัวข้อ Implementing & Managing Cybersecurity in Intelligences Information and How We Battle with the Scam in Banking Sector
- กรรมการ TB-CERT คุณชัชวัฒน์ อัศวรักวงศ์ ร่วมแถลงข่าวจับกุมแก๊งคอลเซ็นเตอร์ โดยกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (ตำรวจไซเบอร์) เมื่อวันที่ 25 พฤษภาคม 2566 โดยเป็นการทลายแก๊ง call center ที่ส่ง SMS ปลอม ด้วยวิธี False base station attack ที่ไม่ผ่านเสาสัญญาณค่ายมือถือ TB-CERT ขอย้ำเตือนประชาชนและให้ข้อมูลความรู้เท่าทันภัยคุกคามเหล่านี้ ผู้แทนองค์กรต่าง ๆ ที่ร่วมแถลงข่าว ได้แก่ 1. กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 2. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

3. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ 4. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 5. สำนักงานตำรวจแห่งชาติ 6. ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร และ 7. ผู้แทนเครือข่าย AIS และ TRUE

- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ ให้ความรู้แก่ประชาชนโดยร่วมเป็นวิทยากรในงาน Privacy & Security Summit 2023 เมื่อวันที่ 30 พฤษภาคม 2566 จัดโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสมาคมผู้ใช้ดิจิทัลไทย ณ โรงแรมเดอะเบอร์เคลีย์ ประตูน้ำ ซึ่ง TB-CERT ได้นำเสนอในหัวข้อ Drive a Culture of Privacy & Security Consciousness in Your Organization เพื่อให้องค์กรสร้างวัฒนธรรมความตระหนักให้กับพนักงานในการมีทัศนคติที่ถูกต้องต่อการปกป้องข้อมูลและระบบขององค์กร ตลอดจนปกป้องข้อมูลของตนเอง
- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ ร่วมเป็นวิทยากรในงานประชุมวิชาการ การดำเนินกิจกรรมบนระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (WUNCA) ครั้งที่ 43 จัดโดยกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ระหว่างวันที่ 10-12 กรกฎาคม 2566 ณ โรงแรมอวานี ขอนแก่น โฮเทลแอนด์คอนเวนชั่นเซ็นเตอร์ ซึ่งได้นำเสนอในหัวข้อ Cyber Security
- กรรมการ TB-CERT และประธานสำนักงานระบบการชำระเงิน คุณยศ กิมสวัสดิ์ ร่วมเป็นวิทยากรในการเสวนาให้กับผู้สื่อข่าวเศรษฐกิจอาวุโส หัวข้อ “ความปลอดภัยของข้อมูลในโลกการเงิน ภัยการเงิน การหลอกลวงทางไซเบอร์ การทำคดีด้านการเงินเจ้าหน้าที่ตำรวจ” ร่วมกับผู้แทนจากชมรมตรวจสอบทุจริต ธนาคารแห่งประเทศไทย และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี เมื่อวันที่ 15 กรกฎาคม 2566 ณ มหาวิทยาลัยหอการค้าไทย
- สมาชิก TB-CERT คุณสัญจร กีรติรังสรรค์ ได้เป็นผู้ร่วมแถลงข่าว ให้ข้อมูลเกี่ยวกับแอปดูดเงินและแสดงวิธีการของมิจฉาชีพหรือแก๊งคอลเซ็นเตอร์ที่เข้ามาหลอกลวงเหยื่อให้ติดตั้งแอปพลิเคชันปลอม รวมทั้งข้อสังเกต ข้อควรระวัง ในงานแถลงข่าวของสำนักงานตำรวจแห่งชาติ เตือนภัยออนไลน์ “ระวัง!!! แอปดูดเงิน คล้ายเว็บไซต์ กฟน. หลอกคืนเงินคำนวณค่า FT ผิด แถมมีข้อความ Google Play ตบตา” เมื่อวันที่ 19 กรกฎาคม 2566 ณ สำนักงานตำรวจแห่งชาติ
- กรรมการ TB-CERT คุณชัชวัฒน์ อัศวรักวงศ์ ให้สัมภาษณ์และพูดคุยในรายการทันโลกเศรษฐกิจ สถานีวิทยุโทรทัศน์กองทัพบกช่อง 5 ในหัวข้อ “TB-CERT สร้างภูมิคุ้มกันก่อนตกเป็นเหยื่อโจรไซเบอร์” ดำเนินรายการโดย คุณภาณุพงศ์ กรรณาธิกรณ์ เมื่อวันที่ 20 กรกฎาคม 2566

- กรรมการ TB-CERT คุณประกลกฤษ แสงชูวงศ์ ให้สัมภาษณ์ทางรายการ Police Talk ทางช่อง Police TV สถานีโทรทัศน์สำนักงานตำรวจแห่งชาติ ในประเด็น "มิจฉาชีพหลอกติดตั้งแอปดูดเงิน" เมื่อวันที่ 20 สิงหาคม 2566
- กรรมการ TB-CERT คุณวชิรวัชร์ มหาทัพกฤษ ร่วมเสวนาวิชาการ มุมมองรอบด้าน 360 องศา กับ PDPA : ประสบการณ์และกรณีศึกษา ในงาน (NECTEC Annual Conference & Exhibitions 2023 : NECTEC ACE 2023) ภายใต้แนวคิด “ฐานรากเทคโนโลยีก้าวไกล พัฒนาไทยก้าวหน้า : Data for Thai Data for All” จัดโดย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ร่วมกับพันธมิตร ณ โรงแรมอีสติน แกรนด์ พญาไท กรุงเทพมหานคร เมื่อวันที่ 12 กันยายน 2566
- กรรมการ TB-CERT คุณชัชวัฒน์ อัศวรักวงศ์ ร่วมเป็นวิทยากรในงานสัมมนาเพื่อขับเคลื่อนประชาคมไซเบอร์แห่งชาติ ในช่วงเสวนาหัวข้อ “การขับเคลื่อนให้เกิดการบูรณาการความร่วมมือในการปราบปรามอาชญากรรมทางเทคโนโลยี” จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ณ โรงแรมอัศวิน แกรนด์ คอนเวนชั่น เมื่อวันที่ 25 กันยายน 2566
- กรรมการ TB-CERT คุณภคพงศ์ จุลวงศาศิลป์ ร่วมบรรยายในหัวข้อ แนวโน้มภัยคุกคามและกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคารปี 2024 ภายในงานสัมมนา TechTalkThai Virtual Summit เมื่อวันที่ 5 ตุลาคม 2566 โดยได้อัปเดตแนวโน้มภัยคุกคามและความเสี่ยงด้านไซเบอร์ล่าสุดที่ภาคการธนาคารต้องเผชิญในปี 2024 รวมถึงแนะนำกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งการพัฒนาบุคลากร การนำเทคโนโลยีอย่าง AI มาประยุกต์ใช้ และการปรับปรุงกระบวนการตามมาตรฐานและกรอบการทำงานต่าง ๆ ให้ทันสมัย
- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ ร่วมเป็นวิทยากรเสวนาในงาน the Future of BFSI Cybersecurity เมื่อวันที่ 20 ตุลาคม 2566 ณ โรงแรม The Okura Prestige กรุงเทพ ในหัวข้อ Generative AI and Its Implications for the BFSI Industry: A Discussion on the Potential Risks and Vulnerabilities Introduced by Generative AI and the Necessity for Robust Security Measures
- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ ให้สัมภาษณ์ในรายการเรื่องดังหลังข่าว ช่อง NBT เมื่อวันที่ 7 พฤศจิกายน 2566 ในประเด็นของภัยไซเบอร์ภาคการธนาคาร vs มิจฉาชีพ เพื่อไขข้อข้องใจและคลายความกังวลของประชาชนในเรื่องของการรักษาความปลอดภัยของระบบธนาคาร และบทบาทของ TB-CERT ในการเฝ้าระวัง แลกเปลี่ยนข้อมูล รวมถึงวิเคราะห์กรณีต่าง ๆ ที่เกิดขึ้นเพื่อหาช่องทางปรับปรุงระบบความปลอดภัยของธนาคารอยู่เสมอ

- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ ร่วมเป็นวิทยากรเสวนาในงาน “Myanmar CIO/ CXO/ CISO Summit 2023 | Bangkok | Thailand” เมื่อวันที่ 14 พฤศจิกายน 2566 ณ โรงแรม Eastin Grand Hotel Sathorn โดยมีผู้เข้าร่วมงานจาก 16 ธนาคารเมียนมาร์
- กรรมการ TB-CERT คุณชัชวัฒน์ อัศวรักวงศ์ ให้สัมภาษณ์ในรายการทันโลกเศรษฐกิจ สถานีวิทยุโทรทัศน์กองทัพบกช่อง 5 ในหัวข้อ “สแกนใบหน้าลดเสี่ยงก่อนโอนเงินปลอดภัยจริงหรือ” ออกอากาศเมื่อวันที่ 16 พฤศจิกายน 2566 เพื่อให้ความรู้และอธิบายข้อเท็จจริงเกี่ยวกับกรณีที่มิจฉาชีพมีการทำโปรแกรมเพื่อหลีกเลี่ยงการสแกนใบหน้าในการโอนเงิน รวมทั้งสร้างความตระหนักให้กับประชาชนในเรื่องของการป้องกันตนเองจากแอปดูดเงิน
- กรรมการ TB-CERT ดร.กิตติ โฆษะวิสุทธิ์ เป็นวิทยากรในงาน Cyber Defense Initiative Conference (CDIC 2023) เมื่อวันที่ 30 พฤศจิกายน 2566 ณ Grand Hall, BITEC Bangna ในหัวข้อ เสริมแกร่งด้านภัยไซเบอร์ด้วยมาตรฐานกลางด้านความมั่นคงปลอดภัยกับการใช้เทคโนโลยีใหม่สำหรับบริการทางการเงิน
- กรรมการ TB-CERT คุณชัชวัฒน์ อัศวรักวงศ์ ร่วมเป็นวิทยากรในช่วงเสวนาหัวข้อ มุมมองของหน่วยงานกำกับดูแล บทบาทและกรณีศึกษาสำหรับองค์กรในการปฏิบัติตามข้อกำหนดกฎหมายและกฎเกณฑ์ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคล .. กฎหมายลำดับรองและประกาศที่เกี่ยวข้อง การใช้บังคับ ข้อกังวลและความคาดหวัง สำหรับองค์กรภายใต้กำกับในการปฏิบัติตามข้อกำหนด ภายในงาน Cyber Defense Initiative Conference (CDIC 2023) เมื่อวันที่ 30 พฤศจิกายน 2566 ณ Grand Hall, BITEC Bangna
- สร้างความร่วมมือกับ Google ระดับ Global เรื่องการทำ Play Integrity API เพื่อตรวจสอบ Genuine App ของธนาคาร และ Take Down แอปฯ อันตรายที่อยู่ใน Official Store
- สร้างความร่วมมือกับ 3 หน่วยงานกำกับดูแลภาคการธนาคาร การลงทุน และประกันภัย ในการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์
- สร้างความร่วมมือระหว่างสมาชิก TB-CERT และสมาชิก TB-CERT กับฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ธนาคารแห่งประเทศไทย ผ่านการจัดประชุมสมาชิกประจำปีและกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการ

การสร้างความร่วมมือกับหน่วยงาน ภายใต้บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย

ในปีที่ผ่านมา TB-CERT ได้ร่วมมือกับ 3 หน่วยงานกำกับดูแลภาคการเงิน ได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) ในการจัดกิจกรรมเพื่อส่งเสริมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากร 3 กลุ่มผ่านโครงการต่าง ๆ ดังนี้

- จัดโครงการ Financial Sector Cybersecurity Talent เป็นการจัดอบรมสัมมนาในหลักสูตร “ISO 27002 Intensive and Cybersecurity Training” เมื่อวันที่ 24-25 กรกฎาคม 2566 ณ โรงแรมเซ็นทาราแกรนด์ เซ็นทรัลลาดพร้าว โดยมีผู้เข้าร่วมโครงการ ได้แก่ บุคลากรที่เริ่มต้นทำงานในด้าน Cybersecurity หรือผู้ที่สนใจในหลักสูตรดังกล่าว จากภาคการธนาคาร การลงทุน และประกันภัย รวม 120 คน
- จัดโครงการ Financial Sector Cybersecurity New Gen เมื่อวันที่ 24 ตุลาคม 2566 ณ โรงแรม S31 โดยมีวัตถุประสงค์เพื่อส่งเสริมและสื่อสารให้คนรุ่นใหม่ได้ตระหนักถึงความสำคัญของ Cybersecurity ในภาคการเงิน รวมถึงสร้างทัศนคติที่ดีต่อวิชาชีพ และสร้างเครือข่ายของกลุ่มนักศึกษาที่พร้อมจะเข้าสู่วิชาชีพในด้านดังกล่าว โดยเป็นการจัดศึกษาดูงานในหน่วยงานด้าน Cybersecurity และการบรรยายจากวิทยากรด้าน Cybersecurity และด้านทรัพยากรบุคคล มีนิสิต นักศึกษา ชั้นปีที่ 3-4 ลงทะเบียนเข้าร่วมงานกว่า 90 คน
- จัดโครงการ Board Awareness โดยจัดงานสัมมนา Cyber Resilience Leadership: Mission for Embracing the Future of AI & Cybersecurity มีวัตถุประสงค์เพื่อให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับคณะกรรมการขององค์กรภาคการเงิน เมื่อวันที่ 2 พฤศจิกายน 2566 ณ โรงแรมสวิสโซเทล กรุงเทพ รัชดา ในลักษณะของการจัดบรรยายและ workshop มีคณะกรรมการจากหน่วยงานภาคการเงิน ได้แก่ หน่วยงานภายใต้การกำกับดูแลของ ธปท. สำนักงาน ก.ล.ต. และสำนักงาน คปภ. เข้าร่วมงานกว่า 200 คน

การสร้างความร่วมมือภายใน TB-CERT ผ่านการประชุมสมาชิกประจำปีและกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการ

เมื่อวันที่ 26-28 มกราคม 2567 TB-CERT ได้จัดการประชุมสมาชิกประจำปีและกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการ มีวัตถุประสงค์เพื่อประชุมสมาชิกประจำปี และวางแผนงานของ TB-CERT อีกทั้งเป็นการเสริมสร้างความสัมพันธ์ระหว่างสมาชิก TB-CERT อีกด้วย

การจัดกิจกรรมในครั้งนี้ประกอบด้วย Team Collaboration เป็นการฝึกทักษะการสื่อสาร การทำงานเป็นทีม การแก้ไขปัญหา ให้ผู้ร่วมกิจกรรมมีความเข้าใจและใส่ใจกับความรู้สึกและความต้องการของผู้อื่น นำไปสู่การแบ่งปันความรู้ ประสบการณ์ และการเรียนรู้ในการทำงานร่วมกัน รวมไปถึง Soft skill training: 7 Habits ซึ่งเป็นทักษะในการสร้างอุปนิสัยของผู้ที่มีประสิทธิผลสูง ไม่ว่าจะเป็นประสิทธิผลส่วนบุคคล ระดับทีมงาน หรือองค์กร ซึ่งจะช่วยพัฒนาไปสู่ความสำเร็จในการสร้างสมดุลของชีวิตส่วนตัวและการงาน

นอกจากนี้ ในด้านความมั่นคงปลอดภัยไซเบอร์ ได้มีการประชุมร่วมกับฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ธนาคารแห่งประเทศไทย การร่วมกันคิดเชิงออกแบบเพื่อนำไปสู่กระบวนการแชร์ข้อมูลของกลุ่มที่ดีขึ้น รวมไปถึงการแลกเปลี่ยนข้อมูล Red sharing เพื่อการขับเคลื่อนงานด้านความมั่นคงปลอดภัยสารสนเทศภาคการธนาคารให้มีความแข็งแกร่ง และสามารถรับมือกับภัยคุกคามทางไซเบอร์อย่างทันท่วงที นำไปสู่การเตรียมความพร้อมในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

งานด้านการสร้างความตระหนักรู้ภัยคุกคามทางไซเบอร์

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับสถาบันธนาคารไทย (Thai Banking Academy: TBAC)

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับสถาบันธนาคารไทย (Thai Banking Academy หรือ TBAC) มีวัตถุประสงค์ของการจัดทำเนื้อหาในปีนี้เพื่อให้พนักงานธนาคารมีความรู้พื้นฐานด้าน Security เฉพาะเรื่องๆ ที่คัดสรรมา ถือเป็นจุดเริ่มต้นของการสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ รวมถึงทำให้ได้ความรู้ใหม่ ๆ สร้างแนวความคิดใหม่ เพื่อต่อยอดความรู้เดิมที่มีอยู่ โดยจะเน้นเป็นคลิปวิดีโอสั้น ๆ กระชับได้ใจความ ซึ่งเรียกว่า Micro learning เป็นการเรียนรู้ในระยะเวลาสั้น ๆ เน้นเนื้อหาที่กระชับและตรงประเด็น เพื่อช่วยพัฒนาความรู้และทักษะในเรื่องหนึ่ง ๆ โดยเฉพาะ ทำให้ผู้เรียนสามารถนำไปปรับใช้ในชีวิตหรือการทำงานจริงได้ ซึ่งแต่ละเรื่องอาจจะมีหลาย EP พร้อมกับมี Quiz ให้ผู้เรียนได้ฝึกทดสอบความเข้าใจของตนเอง ตัวอย่างของเนื้อหาที่นำมาให้เรียนรู้ ได้แก่

1. **แฉกลโกงแอปดูดเงิน** มี 4 EP เกี่ยวกับ แอปดูดเงินและเจาะลึกกลโกงที่มิจฉาชีพใช้ รวมถึงข้อแนะนำในการป้องกัน
   - EP 1: แฉกลโกงแอปดูดเงิน
   - EP 2: เจาะลึกกลโกงแอปดูดเงิน
   - EP 3: โทรศัพท์ของเรามีแอปดูดเงิน แอบติดตั้งอยู่หรือไม่?
   - EP 4: พฤติกรรมเพื่อป้องกันมิจฉาชีพ
   - Quiz
2. **Multi-Factor Authentication** มี 2 EP เกี่ยวกับ การยืนตันตัวตนด้วยหลายปัจจัยคืออะไรและนำไปใช้อย่างไร
   - EP 1: มารู้จัก MFA หรือ Multifactor Authentication คืออะไร
   - EP 2: เราควรปฏิบัติตัวอย่างไร เพื่อให้การใช้ MFA ปลอดภัยและมีประสิทธิภาพ
   - Quiz
3. **Mobile Operating System** มี 2 EP เกี่ยวกับ ระบบปฏิบัติการ OS ของมือถือคืออะไร และทำอย่างไรมือถือเราจะปลอดภัย
   - EP 1: Mobile Operating System คืออะไร และเหตุผลที่ควรอัปเดตอย่างสม่ำเสมอ
   - EP 2: คำแนะนำเกี่ยวกับเวอร์ชันขั้นต่ำของระบบปฏิบัติการในการใช้กับ Mobile Banking Application ให้มีความปลอดภัยมากยิ่งขึ้น
   - Quiz

รูปที่ 1 แสดงตัวอย่างเนื้อหาการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับสถาบันธนาคารไทย

ซึ่งเนื้อหาดังกล่าวจะช่วยให้พนักงานของธนาคาร โดยเฉพาะพนักงานที่สาขามีความรู้ขั้นพื้นฐาน เพื่ออย่างน้อยสามารถช่วยให้คำแนะนำกับลูกค้าได้อย่างเข้าใจ รวมถึงเป็นการปฏิบัติที่ดีต่อตนเองและองค์กรในโลกยุคดิจิทัล

การจัดทำ Infographic เพื่อให้ความรู้ภาคประชาชน

ในปีที่ผ่านมา TB-CERT ได้จัดทำ Infographic เพื่อเตือนและให้ความรู้กับประชาชนโดยสื่อสารผ่าน social media ทาง Facebook Page: TB-CERT และเว็บไซต์สมาคมธนาคารไทย ตั้งแต่เดือนมกราคม-ธันวาคม รวม 59 เรื่อง โดย 59 เรื่องนี้สื่อให้เห็นว่าภัยทุจริตทางการเงินและภัยไซเบอร์นั้นเกิดขึ้นมากมาย

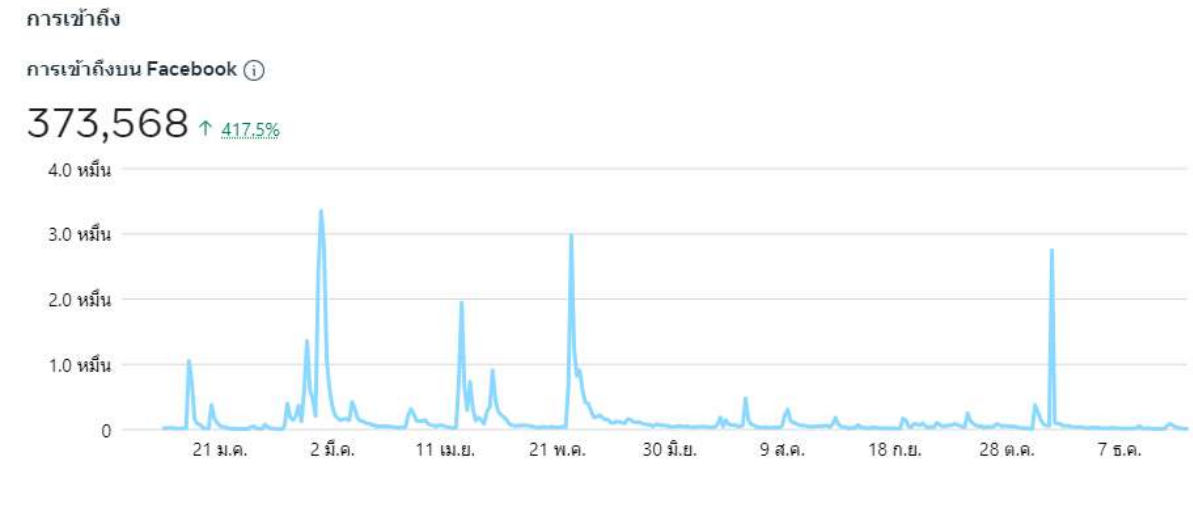
ลำดับ	วันที่เผยแพร่	หัวข้อ
1	10 มกราคม 2566	ระวังภัยจากเว็บไซต์หลอกลวง (Web Phishing)
2	18 มกราคม 2566	มารู้จัก O.MG CABLE กันเถอะ 1/2
3	18 มกราคม 2566	มารู้จัก O.MG CABLE กันเถอะ 2/2
4	2 กุมภาพันธ์ 2566	ไม่ว่าจะช่องทางไหน ๆ FB Messenger, LINE, SMS, WhatsApp โจรมักจะส่ง link มาให้กด
5	6 กุมภาพันธ์ 2566	App Permission 1/4
6	6 กุมภาพันธ์ 2566	App Permission 2/4
7	6 กุมภาพันธ์ 2566	App Permission 3/4
8	6 กุมภาพันธ์ 2566	App Permission 4/4
9	14 กุมภาพันธ์ 2566	แอปฯ แฝงบนมือถือ Android ตรวจจับง่าย ๆ และปลอดภัยด้วย Google Play Protect
10	14 กุมภาพันธ์ 2566	วิธีการเปิดใช้งาน Google Play Protect
11	3 มีนาคม 2566	กลยุทธ์หรือยุทธวิธีที่มิจฉาชีพใช้ประกอบการชักจูง
12	29 มีนาคม 2566	เช็คก่อนเชื่อ ไม่หลงเป็นเหยื่อกลโกง
13	17 เมษายน 2566	2 แอปฯ อันตรายบน Play Store 1/2
14	17 เมษายน 2566	3 แอปฯ อันตรายบน Play Store 2/2
15	20 เมษายน 2566	ระวัง !! มิจฉาชีพส่ง SMS ชวนให้ตกใจ พร้อมลิงก์ให้แอดLINE ปลอม
16	27 เมษายน 2566	รู้หรือไม่ คนร้ายสามารถปลอมแปลงชื่อผู้ส่ง SMS เป็นชื่อธนาคารหรือองค์กรต่างๆได้เหมือนกัน
17	25 พฤษภาคม 2566	แจ้งเตือนภัย!! หลอกติดตั้งแอปพลิเคชันเลียนแบบ DLT SMART QUEUE
18	29 พฤษภาคม 2566	เตือนภัย !! มิจฉาชีพปลอมเว็บไซต์ DLT SMART QUEUE กรมการขนส่งทางบก 1/2

ลำดับ	วันที่เผยแพร่	หัวข้อ
19	29 พฤษภาคม 2566	เตือนภัย !! มิจฉาชีพปลอมเว็บไซต์ DLT SMART QUEUE กรมการขนส่งทางบก 2/2
20	10 สิงหาคม 2566	ติดตั้งแอปฯ มือถือแบบปลอดภัย ต้องไม่ดาวน์โหลดนอก Official Store 1/2
21	10 สิงหาคม 2566	ติดตั้งแอปฯ มือถือแบบปลอดภัย ต้องไม่ดาวน์โหลดนอก Official Store 2/2
22	10 สิงหาคม 2566	สายเรียกเข้าของมิจ(ฉาชีพ) อ้างเป็นเจ้าหน้าที่
23	25 สิงหาคม 2566	ระวัง!! แอปฯ แอบอ้างลงทะเบียนเงินดิจิทัล 10,000 บาท
24	28 สิงหาคม 2566	เตือนภัย SMS ยอดค้างชำระ M-Flow ให้ Add Line กรมการขนส่งทางบกปลอม
25	5 กันยายน 2566	เอ๊ะสักนิดก่อนคิดจะสแกน
26	1 ตุลาคม 2566	[#31Days31Tips] Sharing is caring แชร์ข่าวสารเรื่องภัยออนไลน์
27	2 ตุลาคม 2566	[#31Days31Tips] 3 Spot Check จุดสังเกตข้อมูลให้ปลอดภัยห่างไกลมิจฉาชีพ
28	3 ตุลาคม 2566	[#31Days31Tips] ธนาคารเลิกส่งลิงก์ให้ทาง SMS และ อีเมลแล้ว
29	4 ตุลาคม 2566	[#31Days31Tips] ก่อนคลิกลิงก์ เช็กดีหรือยัง
30	5 ตุลาคม 2566	[#31Days31Tips] อย่าเพิ่งกดลิงก์ ตรวจสอบกับหน่วยงานโดยตรงก่อนดีกว่า
31	6 ตุลาคม 2566	[#31Days31Tips] ธนาคารไม่ขอข้อมูลส่วนตัวผ่านโซเชียลมีเดีย
32	7 ตุลาคม 2566	[#31Days31Tips] วิธีสังเกตบัญชีแชทปลอม
33	8 ตุลาคม 2566	[#31Days31Tips] ควรเช็กอะไรบ้าง ถ้าไม่อยากเจอแอปฯ ไวรัส 1/3
34	9 ตุลาคม 2566	[#31Days31Tips] ควรเช็กอะไรบ้าง ถ้าไม่อยากเจอแอปฯ ไวรัส 2/3
35	10 ตุลาคม 2566	[#31Days31Tips] ไม่ใช่ Wi-Fi สาธารณะทำธุรกรรมทางการเงิน
36	11 ตุลาคม 2566	[#31Days31Tips] ตรวจสอบบัญชีผู้ใช้ปลอดภัยด้วย Security Checkup
37	12 ตุลาคม 2556	[#31Days31Tips] ควรเช็กอะไรบ้าง ถ้าไม่อยากเจอแอปฯ ไวรัส 3/3
38	13 ตุลาคม 2556	[#31Days31Tips] อัปเดตแอปฯ Mobile Banking อย่างสม่ำเสมอ
39	14 ตุลาคม2556	[#31Days31Tips] อย่ามองข้ามการแจ้งเตือนให้อัปเดตระบบของโทรศัพท์มือถือ
40	15 ตุลาคม 2566	[#31Days31Tips] ไม่ตอบข้อความจากคนแปลกหน้า และอย่าเชื่อทันทีเมื่อมีคนแอบอ้างเป็นเจ้าหน้าที่หน่วยงานรัฐ

ลำดับ	วันที่เผยแพร่	หัวข้อ
41	16 ตุลาคม 2566	[#31Days31Tips] วิธีตั้งรหัสผ่านให้รัดกุม
42	17 ตุลาคม 2566	[#31Days31Tips] เปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอน
43	18 ตุลาคม 2566	[#31Days31Tips] เอ๊ะสักนิด ก่อนสแกน QR Code
44	19 ตุลาคม 2566	[#31Days31Tips] เช็กลิสต์ต้องทำก่อนจะเชื่อหรือส่งต่อข้อมูลออนไลน์
45	20 ตุลาคม 2566	[#31Days31Tips] เอ๊ะสักนิด ก่อนสแกนหน้าทุกครั้ง
46	21 ตุลาคม 2566	[#31Days31Tips] ท่องโลกออนไลน์แบบไร้ตัวตนกับ Incognito Mode
47	22 ตุลาคม 2566	[#31Days31Tips] วิธีสังเกตโปรไฟล์ปลอม
48	23 ตุลาคม 2566	[#31Days31Tips] ตรวจสอบประวัติกิจกรรมแปลกๆ บน Social Media
49	24 ตุลาคม 2566	[#31Days31Tips] ไม่ขายบัญชีธนาคาร หรือซิมโทรศัพท์ของตัวเองให้กับบุคคลอื่น
50	25 ตุลาคม 2566	[#31Days31Tips] เก็บข้อมูลส่วนตัวให้มิด ไม่เปิดเผย
51	26 ตุลาคม 2566	[#31Days31Tips] หยุด! อย่าจ่าย! หน่วยงานจริงจะไม่เร่งให้ชำระเงินทันที
52	27 ตุลาคม 2566	[#31Days31Tips] โดนมิจฉาชีพหลอก ควรทำอะไรต่อ
53	28 ตุลาคม 2566	[#31Days31Tips] ระวังมิจฉาชีพมา อย่าแชร์ข้อมูลส่วนตัวบนโลกออนไลน์มากเกินไป
54	29 ตุลาคม 2566	[#31Days31Tips] ตั้งสติรู้ทันกลลวงมิจฉาชีพ
55	30 ตุลาคม 2566	[#31Days31Tips] อบรมเด็กๆ ด้วยหลักสูตร Be Internet Awesome สร้างภูมิคุ้มกันในการท่องโลกออนไลน์
56	31 ตุลาคม 2566	[#31Days31Tips] 2 Steps ต้องทำทันที เมื่อตกเป็นเหยื่อ
57	7 พฤศจิกายน 2566	เตือนภัย มิจฉาชีพมุ่งเป้าหลอกกลุ่มผู้เกษียณอายุให้ติดตั้งแอปฯ ปลอมรับเงินบำนาญ อ้างเป็นกรมบัญชีกลาง 1/2
58	7 พฤศจิกายน 2566	เตือนภัย มิจฉาชีพมุ่งเป้าหลอกกลุ่มผู้เกษียณอายุให้ติดตั้งแอปฯ ปลอมรับเงินบำนาญ อ้างเป็นกรมบัญชีกลาง 2/2
59	8 พฤศจิกายน 2566	มุกใหม่ระบาด ให้ติดตั้งแอปฯ ผ่าน TestFlight

การสร้างความตระหนักรู้ด้านภัยไซเบอร์ผ่านสื่อ Facebook

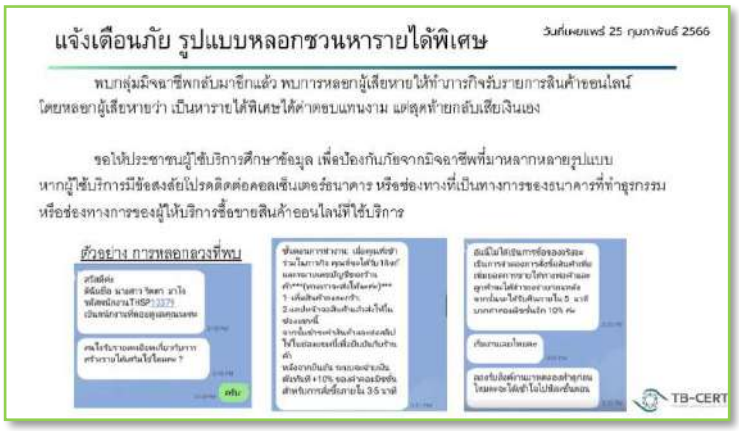
ในสังคมยุคปัจจุบัน ปฏิเสธไม่ได้ว่า “สื่อสังคมออนไลน์” หรือ Social Media ได้เข้ามามีบทบาทอิทธิพลต่อพฤติกรรมการใช้ชีวิตประจำวันของเราเป็นอย่างมาก อีกทั้งยังเป็นจุดเปลี่ยนของโลกแห่งการสื่อสารไปสู่รูปแบบใหม่ ๆ ที่รวดเร็ว ทำให้หลาย ๆ องค์กรหรือหน่วยงานรวมถึง TB-CERT เอง เล็งเห็นถึงความสำคัญ จึงได้นำสื่อสังคมออนไลน์มาปรับประยุกต์ใช้ในด้านการประชาสัมพันธ์และสื่อสารไปยังประชาชน เพื่อให้ตระหนักรู้เท่าทันภัยทางการเงินและไม่ตกเป็นเหยื่อของมิจฉาชีพ กลยุทธ์การประชาสัมพันธ์ผ่านสื่อสังคมออนไลน์ด้วยการใช้ Facebook ของ TB-CERT[1] ตลอดปี 2566 มีวัตถุประสงค์ที่ต้องการให้สมาชิกเพจหรือผู้เข้าชม ได้รับความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับภัยทางการเงิน และสามารถนำความรู้ไปปรับใช้ได้ในชีวิตประจำวัน โดยได้เริ่มดำเนินการมาตั้งแต่ 29 ตุลาคม พ.ศ. 2560 จนถึงปัจจุบัน ในการนี้ มีผู้ปฏิบัติงานเป็นแอดมินเพจ ซึ่งดูแล จัดทำเนื้อหา แก้ไข ควบคุมและวิเคราะห์ข้อมูลขององค์กรเพื่อเผยแพร่สื่อประชาสัมพันธ์ รวมถึงสร้างการมีส่วนร่วมและการมีปฏิสัมพันธ์ระหว่างกันกับสมาชิกเพจหรือผู้เข้าชม โดยเผยแพร่เนื้อหาด้วยรูปแบบของข้อความ ภาพ เสียง วิดีโอ สื่อผสมอื่นๆ เช่น Infographic Banner หรือการถ่ายทอดออกอากาศสด เป็นต้น ซึ่งปัจจุบัน Facebook page “TB-CERT” มียอดการเข้าถึงในปี 2566 จำนวน 373,568 ครั้ง ดังรูปที่ 2



รูปที่ 2 แสดงตัวเลขภาพรวมการเข้าถึงของ TB-CERT Facebook page

[1] Facebook ของ TB-CERT สามารถเข้าถึงได้ที่ https://www.facebook.com/TBCERT.Official

จากยอดจำนวนผู้เข้าถึงข้อมูล (Reach)[2] ทั้งหมด พบว่า ปัจจัยที่ส่งผลต่อจำนวนผู้เข้าถึงส่วนหนึ่งมาจากการจัดทำเนื้อหาที่น่าสนใจและเป็นประโยชน์ ขณะเดียวกันต้องเผยแพร่ข่าวสารนั้นออกไปด้วยความรวดเร็ว ทันต่อเหตุการณ์เพื่อตอบสนองต่อการรับรู้ข่าวสารของผู้เข้าชม/สมาชิกเพจ ณ เวลานั้นได้อย่างทันท่วงที เพราะการที่จะทำให้ผู้เข้าชมเลือกหรือตัดสินใจเข้ามาติดตามข้อมูลข่าวสารขององค์กรนั้น เป็นสิ่งสำคัญที่สุด ยิ่งยอดตัวเลขของผู้เข้าถึงข้อมูลขององค์กรมีมากเท่าไร ก็ยิ่งแสดงให้เห็นถึงการให้ความสนใจของประชาชนและการประสบความสำเร็จในการสื่อสารถึงประชาชนมากขึ้นเท่านั้น ยกตัวอย่างเช่น ในช่วงปลายเดือนกุมภาพันธ์ TB-CERT ได้โพสต์เกี่ยวกับการแจ้งเตือนภัยมิจฉาชีพในรูปแบบหลอกชวนหารายได้พิเศษ มียอดการเข้าถึงรวมสูงสุด 1.2 แสนบัญชี ดังรูปที่ 3

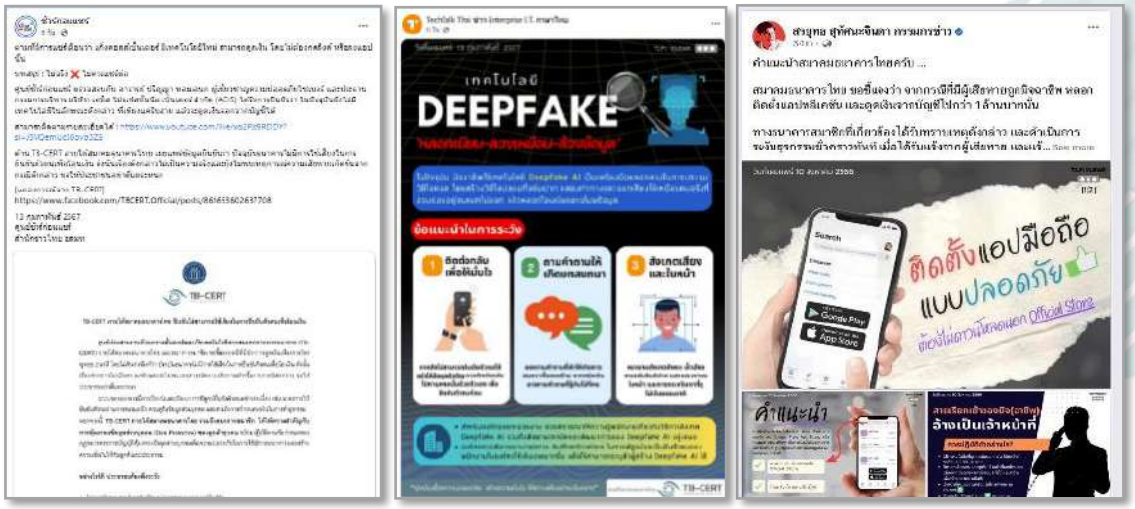


รูปที่ 3 แสดงเนื้อหาการแจ้งเตือนภัยมิจฉาชีพบน TB-CERT Facebook page

อีกปัจจัยหนึ่งที่สามารถกระตุ้นจำนวนผู้เข้าถึงได้ คือ การแชร์โพสต์ผ่านเพจของสื่อสำนักข่าว เพจของบุคคลที่มีชื่อเสียง หรือเพจของผู้เชี่ยวชาญด้าน Cybersecurity เนื่องจากเพจของกลุ่มเหล่านี้มีผู้ติดตามเพจ (Page followers)[3] เป็นจำนวนมาก และประชาชนมักเห็นว่าข้อมูลที่โพสต์ผ่านเพจเหล่านี้มีความน่าเชื่อถือ ดังนั้นเพื่อเป็นการการกระจายข่าวสารที่ถูกต้องไปถึงประชาชนในวงกว้าง การประสานขอความร่วมมือกับเพจต่าง ๆ ในการแชร์ข่าวสารจึงเป็นอีกหนึ่งวิธีที่ TB-CERT ได้ดำเนินการ ดังรูปที่ 4

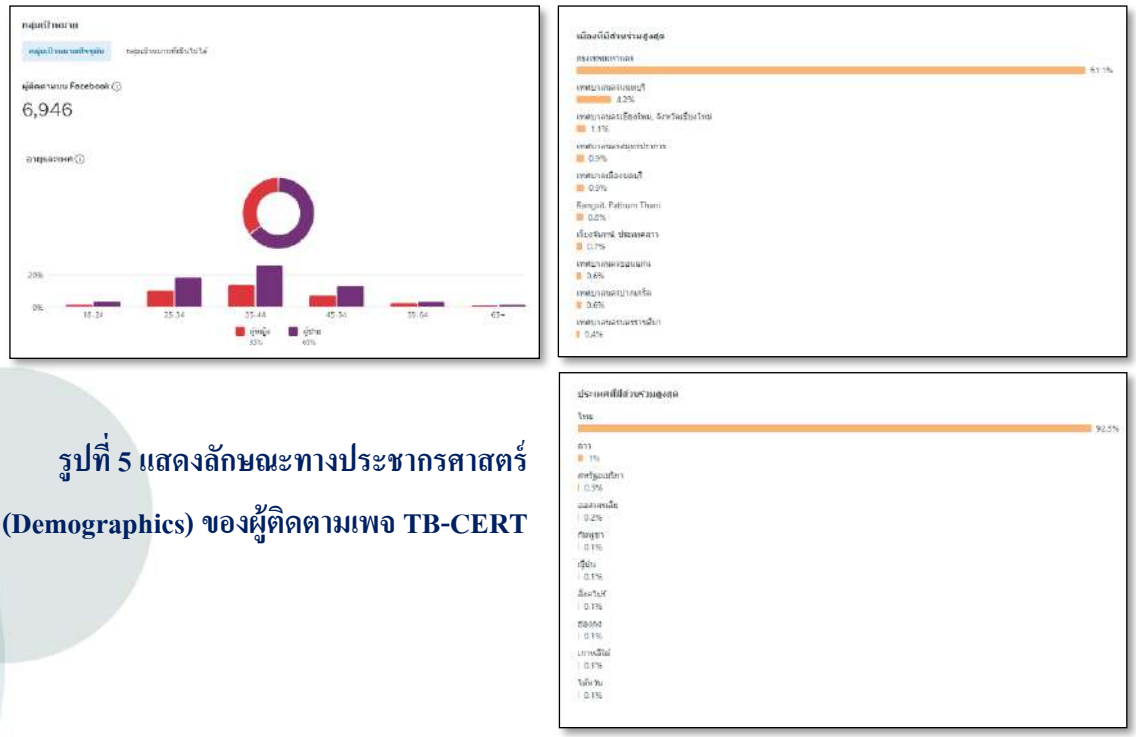
[2] ยอดจำนวนผู้เข้าถึงข้อมูล (Reach) คือ จำนวนบัญชีผู้ใช้งานบน Facebook ที่เห็นเนื้อหาหรือโพสต์จากเพจ ในฟีดข่าวของพวกเขา โดยอาจเป็นผลจากการเผยแพร่โพสต์โดยตรง การแชร์ การแสดงความคิดเห็น หรือการกดถูกใจ

[3] ผู้ติดตามเพจ (Page followers) คือ จำนวนบัญชีผู้ใช้งานบน Facebook ที่ได้กดปุ่ม "ติดตาม" (Follow) เพจ เพื่อรับการอัปเดตเกี่ยวกับเนื้อหาหรือโพสต์จากเพจนั้น ๆ ในฟีดข่าว



รูปที่ 4 แสดงตัวอย่างโพสต์ที่มีการแชร์โดยเพจสำนักข่าว

นอกจากปัจจัยด้านเนื้อหาแล้ว การศึกษาลักษณะทางประชากรศาสตร์ (Demographics) ของผู้ติดตามเพจ ซึ่งประกอบไปด้วย ข้อมูลเพศ ข้อมูลอายุ และข้อมูลตำแหน่งที่ตั้งทางภูมิศาสตร์ ก็เป็นส่วนสำคัญในการวิเคราะห์ความสนใจและแนวคิดของผู้ใช้งาน เพื่อนำมาใช้ประโยชน์ในการออกแบบเนื้อหาต่อไป โดยจากจำนวนผู้ติดตามเพจของ TB-CERT ทั้งหมด 6,946 คน จัดแบ่งเป็นช่วงอายุตั้งแต่ 18-24 ปี (4%), 25-34 ปี (29%), 35-44 ปี (40%), 45-54 ปี (20%), 55-64 ปี (5%) และ 65 ปีขึ้นไป (2%) จากจำนวนนี้ คิดเป็นเพศชาย 65% และเพศหญิง 35% ส่วนใหญ่อาศัยอยู่ในกรุงเทพมหานคร (61%) ดังรูปที่ 5



รูปที่ 5 แสดงลักษณะทางประชากรศาสตร์ (Demographics) ของผู้ติดตามเพจ TB-CERT

นอกจากนี้ ตลอดเดือนตุลาคม ปี 2566 TB-CERT ได้มีการสร้างความร่วมมือร่วมกับธนาคารแห่งประเทศไทย และ Google Thailand ในการจัดแคมเปญ #31Days31Tips ที่นำเสนอเนื้อหาความรู้ด้านดิจิทัลและเคล็ดลับความปลอดภัยบนโลกออนไลน์ในรูปแบบต่าง ๆ เพื่อเพิ่มการมีส่วนร่วมและการแบ่งปันความรู้ความเข้าใจ ที่จะช่วยให้คนไทยมีภูมิคุ้มกันทางไซเบอร์และใช้เทคโนโลยีออนไลน์ได้อย่างปลอดภัย โดยเนื้อหาประกอบด้วย 4 หมวดหมู่ ได้แก่ **1) การรักษาความปลอดภัยของบัญชีออนไลน์ 2) การป้องกันตัวเองจากสแกม 3) การตรวจเช็คข่าวปลอมหรือข้อมูลที่ไม่ถูกต้อง** และ **4) การปกป้องความเป็นส่วนตัวบนโลกออนไลน์** เพื่อเสริมทักษะดิจิทัลให้คนไทยรู้เท่าทันกลลวงออนไลน์อย่างรอบด้าน ดังตัวอย่างในรูปที่ 6

รูปที่ 6 แสดงเนื้อหาจากแคมเปญ #31Days31Tips ร่วมกับธปท. และ Google Thailand

จากการสังเกตและวิเคราะห์ข้อมูลเชิงลึกของ TB-CERT Facebook page ตลอดปี 2566 พบว่าส่วนสำคัญอีกส่วนหนึ่งที่จะเพิ่มประสิทธิภาพและยอดของสมาชิกเพจหรือผู้เข้าชมเพจองค์กรได้ ประกอบด้วย

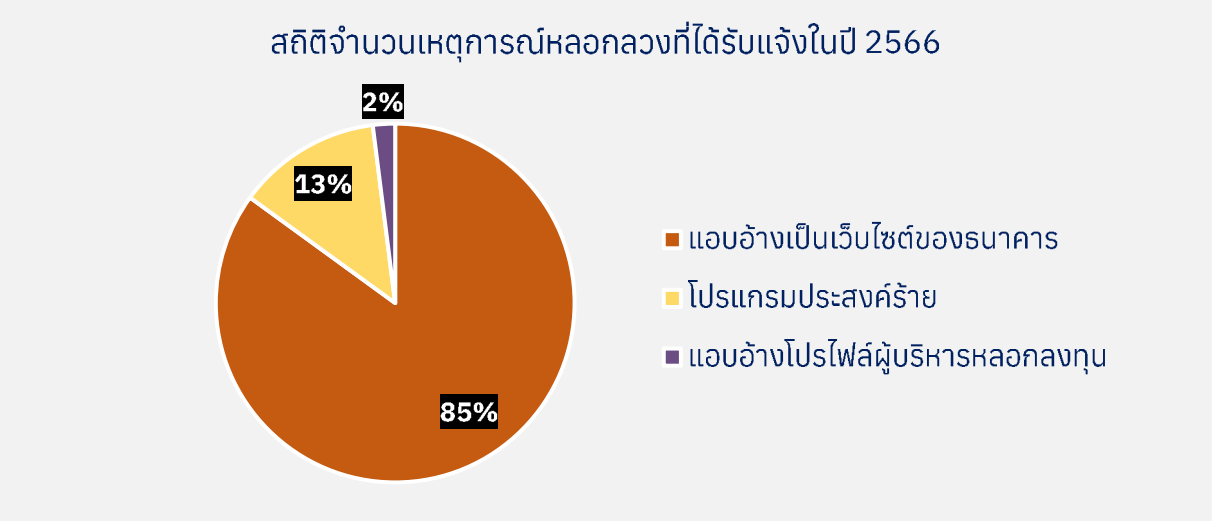
1. การออกแบบเนื้อหาข่าวควรทำให้โดดเด่น ใช้ข้อความสั้น กระชับได้ใจความ มีสีสันสะดุดตา เลือกภาพประกอบคมชัด สื่อความหมายได้ดี
2. ใช้วิธีผสมผสานรูปแบบการนำเสนอในหลาย ๆ ลักษณะ ตามความเหมาะสมของเนื้อหา เช่น รูปภาพ วิดีโอสั้น ๆ การถ่ายทอดออกอากาศสด
3. การตอบกลับข้อความสมาชิกเพจ ควรตอบกลับให้รวดเร็วและครอบคลุม (โดยปกติควรตอบ 95% ของจำนวนข้อความทั้งหมด และควรตอบภายใน 5 นาที) สถานะบนหน้าเพจจะแสดงเป็น “ปกติตอบกลับโดยทันที” เพื่อแสดงถึงความกระตือรือร้นในการสื่อสารกับประชาชน
4. การสร้างเพจให้เป็นโปรไฟล์ธุรกิจและประสานความร่วมมือเพจที่มียอดผู้ติดตามจำนวนมากในการแชร์ข่าวสารเพื่อสร้างความน่าเชื่อถือให้กับองค์กร

สิ่งที่ TB-CERT รวบรวมและสรุปเป็นองค์ความรู้นั้น นับว่าเป็นเพียงกลยุทธ์หนึ่งในหลาย ๆ วิธีที่มีส่วนช่วยเสริมให้งานด้านการประชาสัมพันธ์ขององค์กรประสบความสำเร็จ เพื่อสร้างภาพลักษณ์ที่ดีให้เป็นที่ประจักษ์และเกิดการยอมรับแก่สาธารณชนทั่วไป ยังมีเทคนิค วิธีการ รวมถึงรายละเอียดอีกมากมายที่แอดมินเพจและผู้เกี่ยวข้องจำเป็นต้องเรียนรู้ ศึกษา ทำความเข้าใจ และนำไปปรับประยุกต์ใช้ให้เกิดศักยภาพและประสิทธิภาพต่อองค์กรต่อไป

สถิติการรับมือภัยไซเบอร์ และแนวโน้มภัยไซเบอร์ในปี 2024 ของภาคการเงินการธนาคาร

สรุปสถิติการรับมือภัยไซเบอร์

ในปี 2566 ทีมงาน TB-CERT มีการรับแจ้งเหตุและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident response) โดยที่ผ่านมา ได้มีการประสานความร่วมมือไปยังหน่วยงานพันธมิตรทั้งในประเทศและต่างประเทศ ในการระงับและปิดกั้นการเข้าถึงเว็บไซต์ปลอมและเว็บไซต์อันตรายที่ได้รับแจ้งจากหน่วยงานสมาชิก เพื่อลดโอกาสที่มิจฉาชีพใช้หลอกลวงประชาชนให้รวดเร็วและยับยั้งความเสียหายที่เกิดขึ้น

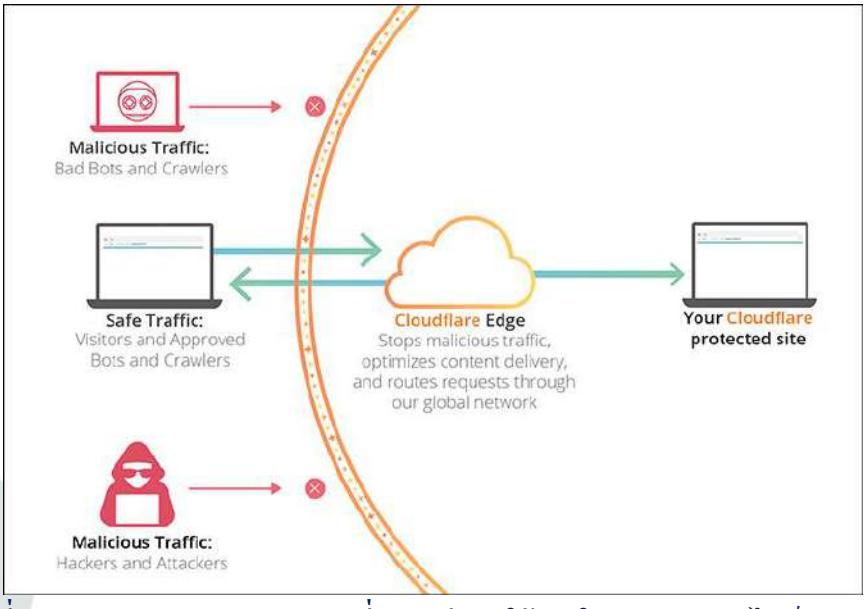


รูปที่ 7 แสดงสถิติจำนวนเหตุการณ์หลอกลวงที่ได้รับแจ้งในปี 2566

จากสถิติจำนวนเหตุการณ์ที่ได้รับแจ้ง ดังรูปที่ 7 พบว่า 85% ของการหลอกลวงมาในรูปแบบของการปลอมแปลงและแอบอ้างเป็นเว็บไซต์ของธนาคารและปล่อยกู้สินเชื่อ โดยมีการสร้างหน้าเว็บไซต์ที่ใช้ตราสัญลักษณ์ของหน่วยงานจริง และมีการขอข้อมูลส่วนตัว เช่น เลขบัตรประชาชน เบอร์โทรศัพท์ เป็นต้น นอกจากนี้ 13% ของการหลอกลวงมาในรูปแบบของโปรแกรมประสงค์ร้าย โดยการสร้างแอปพลิเคชันที่ใช้ตราสัญลักษณ์เลียนแบบหน่วยงานจริง เพื่อหลอกให้ประชาชนติดตั้งแอปพลิเคชันปลอมดังกล่าวเพื่อใช้ในการดักจับข้อมูลบนอุปกรณ์ โดยเฉพาะอย่างยิ่งการดักจับ PIN ในการเข้าใช้งาน Mobile Banking Application หรือการควบคุมอุปกรณ์จากระยะไกล ที่ทำให้ผู้ไม่ประสงค์ดีสามารถโอนเงินจากบัญชีผู้ใช้งานได้โดยไม่รู้ตัว และท้ายที่สุด 2% ของการหลอกลวงมาในรูปแบบของการแอบอ้างโปรไฟล์ผู้บริหารของหน่วยงานเพื่อสร้างความน่าเชื่อถือในการหลอกลงทุน การหลอกลวงในลักษณะนี้มักจะพบบนสื่อโซเชียลมีเดียที่มีการซื้อบริการโฆษณา โดยเป็นการสร้างเพจที่แอบอ้างชื่อ และรูปภาพของผู้บริหารของธนาคาร และโพสต์ข้อความที่มีเนื้อหาเกี่ยวกับการชักชวนร่วมลงทุนที่จะได้รับผลตอบแทนดี

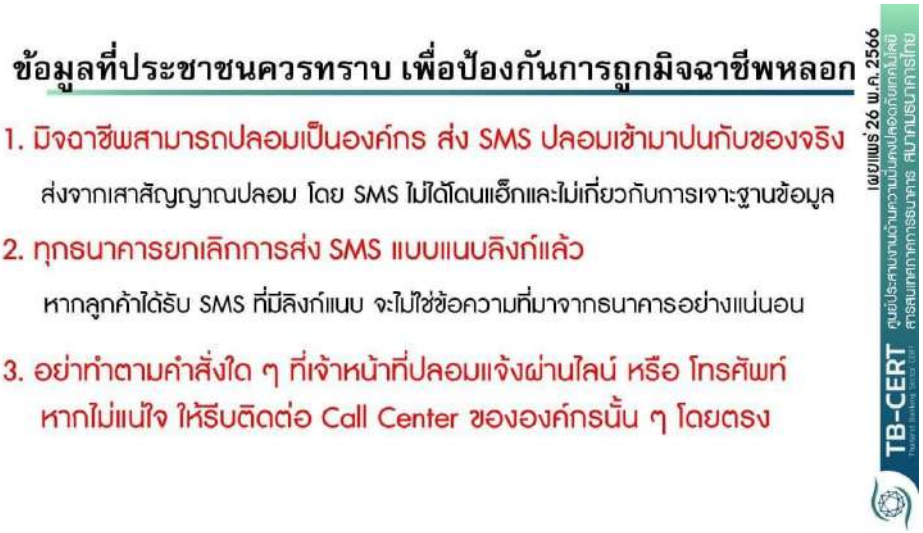
สิ่งที่สังเกตได้เพิ่มเติมคือ 75% ของเว็บไซต์ปลอมเหล่านี้ใช้ภาษาไทย ชี้ให้เห็นว่าผู้ไม่ประสงค์ดีได้ศึกษาการใช้ภาษาไทย และอุปนิสัยของประชาชนชาวไทย เพื่อให้การหลอกลวงแนบเนียนมากยิ่งขึ้น นอกจากภาษาไทยแล้ว พบว่าอีก 15% ของเว็บไซต์ปลอมใช้ภาษาเวียดนาม และเป็นการแอบอ้างกลุ่มธนาคารที่มีการขยายสาขาไปยังประเทศเวียดนามจริง จึงอาจตีความได้ว่ากลุ่มผู้ไม่ประสงค์ดีขยายขอบเขตของการโจมตีไปยังธนาคารในต่างประเทศ และเลือกใช้ภาษาท้องถิ่นของประเทศนั้น ๆ เพื่อหลอกลวงประชาชน

เมื่อวิเคราะห์การจดทะเบียนเว็บไซต์ปลอม ผลลัพธ์แสดงให้เห็นว่ามีการจดทะเบียนจากผู้ให้บริการในประเทศสหรัฐอเมริกา (50%), ประเทศจีน (20%), ประเทศรัสเซีย (17%), ประเทศไอซ์แลนด์ (5%), ประเทศสเปน (3%), ประเทศโปรตุเกส (3%) และประเทศเวียดนาม (2%) ในจำนวนนี้มีการใช้บริการจดทะเบียนโดเมนผ่านหลากหลายบริษัท เช่น GoDaddy, NameCheap, NameSilo เป็นต้น และใช้วิธีการจดทะเบียนซ่อนตัวภายใต้ผู้ให้บริการที่น่าเชื่อถืออย่าง Cloudflare โดยพบมากถึง 80% ของเว็บไซต์ปลอมทั้งหมด ซึ่งปกติแล้วระบบของ Cloudflare ได้ถูกออกแบบมาเพื่อเป็นตัวกลางระหว่างให้การเชื่อมต่อระหว่างผู้ใช้งานและเว็บไซต์ดังรูปที่ 8 แต่ผู้ไม่ประสงค์ดีกลับนำไปใช้ในทางที่ผิดโดยนำมาใช้ในการซ่อนเว็บไซต์อันตรายอยู่หลัง Cloudflare ซึ่งทีมงาน TB-CERT ได้วางแผนสร้างความร่วมมือกับบริษัท Cloudflare เพื่อรับมือกับกลุ่มผู้ไม่ประสงค์ดีในการดำเนินการระงับและปิดกั้นเว็บไซต์ปลอมต่อไป



รูปที่ 8 การทำงานของ Cloudflare ที่มิจฉาชีพมาใช้งานในการซ่อนเว็บไซต์อันตราย

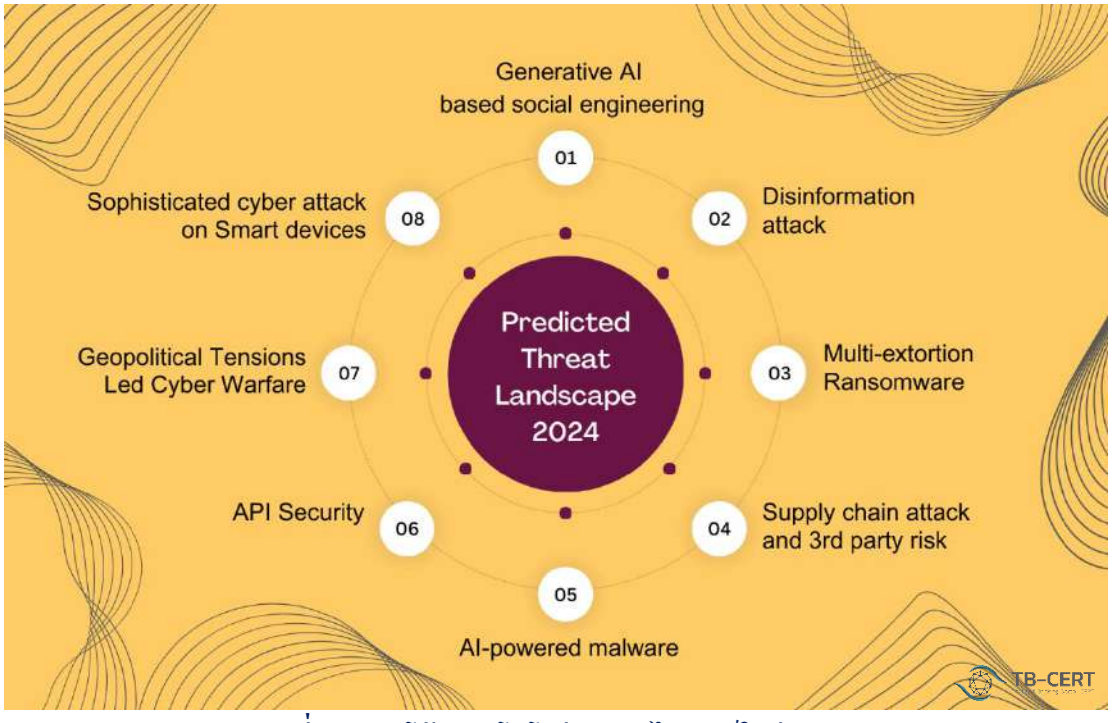
นอกจากเว็บไซต์ปลอมที่แอบอ้างหน่วยงานจริงแล้ว ยังมีเหตุการณ์ที่ผู้ไม่ประสงค์ดีส่งลิงก์ผ่านช่องทาง SMS เพื่อให้ประชาชนคลิกและนำไปสู่การหลอกลวงในรูปแบบอื่น ๆ ต่อไป ซึ่งทีมงาน TB-CERT พบว่า หากเทียบกับจำนวนสถิติตัวเลขของ SMS ปลอมในปี 2022 กับจำนวนเหตุการณ์ของ SMS ปลอมในปี 2023 นั้น จะเห็นถึงการลดลงอย่างมีนัยสำคัญ ซึ่งอาจบ่งชี้ได้ว่ามาตรการที่ธนาคารแห่งประเทศไทยขอความร่วมมือธนาคารต่าง ๆ ในการยกเลิกบริการแนบลิงก์ทาง SMS อีเมล และช่องทางโซเชียลมีเดียต่าง ๆ นั้น เป็นส่วนสำคัญในการช่วยไม่ให้ประชาชนตกเป็นเหยื่อของมิจฉาชีพ รวมถึงการให้ความร่วมมือเป็นอย่างดีของผู้ให้บริการเครือข่ายโทรศัพท์มือถือในการช่วยเหลือระงับเบอร์โทรศัพท์อันตรายอีกด้วย



รูปที่ 9 การแจ้งมาตรการเสริมในการป้องกันการถูกมิจฉาชีพหลอก

แนวโน้มเทคโนโลยีและภัยไซเบอร์ในปี 2024 ของภาคการเงินการธนาคาร

จากการรวบรวมข้อมูลเหตุการณ์ภัยไซเบอร์ที่เกิดขึ้นในปีที่ผ่านมาประกอบกับการวิเคราะห์สถานการณ์และแนวโน้มจากรายงานหลายแหล่ง TB-CERT จึงได้คาดการณ์แนวโน้มรูปแบบการโจมตีทางไซเบอร์ สำหรับปี 2024 ดังนี้



รูปที่ 10 แนวโน้มเทคโนโลยีและภัยไซเบอร์ในปี 2024

1. ภัยจากการนำปัญญาประดิษฐ์แบบ Generative AI มาใช้ในการโจมตีและการฉ้อโกงทางดิจิทัล (Digital fraud) เพิ่มมากขึ้น

ในปีที่ผ่านมาได้เกิดกระแสการปรับตัวใช้งานเทคโนโลยี Generative AI กันอย่างกว้างขวาง กล่าวคือ การนำเอา AI หรือปัญญาประดิษฐ์ มาใช้ออกแบบสร้างเนื้อหาใหม่ๆ เช่น ช่วยในการเขียนโค้ดโปรแกรม ชุดคำสั่ง สร้างรูปภาพ สร้างเสียง สร้างวิดีโอ หรือตอบโต้กับมนุษย์ได้เสมือนการตอบโต้จริงๆ แบบ Real-Time ซึ่งเป็นด้านที่เป็นประโยชน์กับมนุษย์ในทางสร้างสรรค์ แต่ในทางกลับกันยังมีมิจฉาชีพที่นำ Generative AI มาใช้สร้างข้อมูลในการหลอกลวงที่มีความซับซ้อนและเจาะจงเป้าหมายได้ง่ายมากขึ้น โดยจะเห็นได้จากหลาย

รายงานการวิเคราะห์และคาดการณ์แนวโน้ม [4] [5] [6] ได้มีการพิจารณาถึงผลลัพธ์ด้านลบของเทคโนโลยีปัญญาประดิษฐ์ว่าจะมีความรุนแรงเพิ่มมากขึ้น หากยังขาดการควบคุมและใช้งานอย่างมีจริยธรรม

2. การโจมตีโดยใช้การสร้างข้อมูลบิดเบือน (Disinformation Attack)

การโจมตีโดยในรูปแบบ Disinformation Attack เป็นการสร้างข้อมูลที่เป็นเท็จหรือข้อมูลที่ถูกบิดเบือน เพื่อหลอกลวง สร้างความสับสน หรือเปลี่ยนแปลงความเห็นของเจ้าของข้อมูล โดยมีเจตนาในการที่จะทำให้ผู้รับข้อมูลมีความเข้าใจไปในแนวทางต้องการ ซึ่งจะมุ่งเป้าการโจมตีไปในด้านต่าง ๆ เช่นด้านการเงิน การเมือง เศรษฐกิจ หรือสังคม และอาจส่งผลกระทบต่อความมั่นคงความปลอดภัย หรือความเชื่อมั่นของภาคประชาชนได้ การตรวจสอบข้อมูลที่ถูกบิดเบือน (Disinformation) ไม่ใช่เรื่องที่ง่าย เนื่องจากมีเทคโนโลยีที่มีความสามารถในการผลิตข้อมูลที่ถูกบิดเบือนด้วยวิธีการที่ซับซ้อนมากขึ้น โดยจะเห็นได้จากรายงาน Global Risks Report 2024 [4] ได้มีการคาดการณ์ว่าข้อมูลบิดเบือน (Disinformation) จะถูกนำมาใช้เป็นเครื่องมือในการโจมตีและสร้างผลกระทบเป็นอันดับ 1 ในอีก 2 ปีข้างหน้า ข้อมูลที่ถูกบิดเบือน (Disinformation) ยังอยู่กับเราต่อไป จึงเป็นเรื่องที่ทุกภาคส่วนควรต้องเร่งให้ความสำคัญอย่างยิ่ง เพื่อเตรียมความพร้อมและสร้างความตระหนักรู้ให้กับภาคประชาชนในการตรวจสอบข้อมูลข่าวสารที่ได้รับมา ให้ไม่หลงเชื่อและตื่นตระหนกต่อข้อมูลดังกล่าว

3. การโจมตีโดยใช้วิธีการเรียกค่าไถ่แบบหลายชั้น (Multi-extortion Ransomware)

การโจมตีโดยใช้วิธิการเรียกค่าไถ่แบบหลายชั้น หรือ Multi-extortion Ransomware จะเป็นเทคนิคการโจมตีที่ไม่เพียงแค่เข้ารหัสข้อมูลของเหยื่อเท่านั้น แต่ยังทำการขู่ที่จะเผยแพร่ข้อมูลที่ขโมยไปด้วย ไม่ว่าจะเป็นช่องทางอินเทอร์เน็ตหรือขายให้กับผู้อื่น เช่น คู่แข่งทางการค้า หรือใช้ข้อมูลดังกล่าวไปข่มขู่ลูกค้าของธุรกิจได้ หากเหยื่อไม่จ่ายค่าไถ่ในเวลาที่กำหนด เพื่อที่จะเร่งรัดให้เหยื่อจ่ายเงิน จากรายงาน [7] [8] ข้อมูลของกลุ่ม Ransomware พบว่ามีขีดความสามารถเพิ่มมากขึ้นรวดเร็วอย่างมีนัยสำคัญ โดยพบการแชร์เทคนิคและ

[4] Global Risks Report 2024, World Economic Forum

[5] Gartner Top 10 Strategic Technology Trends 2024

[6] Proactive risk management in Generative AI, Deloitte

[7] Cyble: Threat Landscape Report 2023-2024

[8] Symantec: The 2024 Ransomware Threat Landscape

เครื่องมือในการโจมตีเหยื่อระหว่างกลุ่ม โดยมีการแตกเป็นกลุ่มใหม่ ๆ เพิ่มมากขึ้น และมีเทคนิคการเรียกค่าไถ่แบบหลายชั้นที่มีแนวโน้มซับซ้อนมากขึ้น จึงเป็นสิ่งที่องค์การควรต้องจัดทำแผนการรับมือและซักซ้อมแผนดังกล่าวให้พร้อมต่อเหตุการณ์ นอกจากนั้นทุกหน่วยงานจะต้องมีการสอบทานมาตรการในการป้องกันมัลแวร์พิจารณากระบวนการปิดช่องโหว่ให้มีประสิทธิภาพรวมถึงแนวทางการจัดการความเสี่ยงอีกด้วย

4. ภัยจาก 3rd party ที่มีมาตรการการรักษาความปลอดภัยไม่ดีเพียงพอ

ความเสี่ยงจาก 3rd party ยังเป็นเรื่องที่ท้าทายในการบริหารจัดการต่อทุกภาคธุรกิจรวมถึงภาคการธนาคารด้วย ปัจจุบันการทำงานร่วมกันกับ 3rd party ซึ่งอาจจะหมายถึงผู้ให้บริการภายนอก (Outsourcing service provider) ผู้จัดหาหรือขายสินค้า (Supplier, Vendor) พันธมิตรทางธุรกิจ (Business partner) และการร่วมทำธุรกิจ (Joint venture) เพื่อต่อยอดในการทำธุรกิจและสนับสนุนการทำงานให้มีประสิทธิภาพมากยิ่งขึ้นได้รับความนิยมและมีแนวโน้มว่าจะมีเพิ่มมากขึ้น ในช่วงที่ผ่านมา พบว่าสาเหตุที่หน่วยงานต่าง ๆ ถูกโจมตีทางด้านไซเบอร์ ส่วนหนึ่งมีต้นเหตุเกิดจากการที่ 3rd party ที่หน่วยงานที่ถูกโจมตีใช้บริการ ไม่มีการรักษาความปลอดภัยทางไซเบอร์ที่ดีพอ จึงเป็นจุดอ่อนและช่องทางให้ Threat Actor สามารถใช้เป็นช่องทางในการโจมตีหน่วยงานต่าง ๆ ได้ อีกทั้งเมื่อเหตุการณ์การโจมตีทางไซเบอร์หรือข้อมูลรั่วไหลเกิดขึ้นที่ 3rd party ก็จะส่งผลกระทบต่อหน่วยงานผู้ใช้บริการเองโดยตรงด้วยเช่นกัน จึงเป็นเหตุที่จะมองข้ามผลกระทบจากภัยคุกคามที่เกิดกับจาก 3rd party นี้ไปไม่ได้

5. การนำปัญญาประดิษฐ์มาสร้างมัลแวร์ที่ซับซ้อนมากขึ้น (AI-powered Malware)

จากการเติบโตของปัญญาประดิษฐ์ (AI) ในช่วงปีที่ผ่านมาอย่างรวดเร็ว มีการนำเอาเทคโนโลยีปัญญาประดิษฐ์ (AI) ไปใช้ในทางที่ผิด เช่น การนำเอาเทคโนโลยีปัญญาประดิษฐ์ (AI) มาสร้างมัลแวร์ที่มีความซับซ้อนและมีขีดความสามารถให้การหลบหลีกและตรวจจับเพิ่มมากขึ้น ส่งผลให้เกิดผลกระทบทางลบต่อการนำปัญญาประดิษฐ์ (AI) ไปใช้ เนื่องด้วยปัญญาประดิษฐ์ (AI) มีอัลกอริทึม (Algorithm) ที่สามารถเรียนรู้จากข้อมูลที่หลากหลายตามวัตถุประสงค์ของการพัฒนาและจะนำไปใช้ ปัญญาประดิษฐ์ (AI) ยังสามารถที่จะเรียนรู้ข้อมูลจากเทคนิคต่าง ๆ ที่มัลแวร์ (Malware) ถูกพัฒนาขึ้นมาจำนวนมหาศาลที่มีบนโลกใบนี้ได้ จึงมีความสามารถที่นำข้อมูลดังกล่าวมาใช้สร้างมัลแวร์ (Malware) ที่ความสามารถฉลาดและซับซ้อนในการซ่อนและปิดจุดอ่อนตัวเอง อีกทั้งปัญญาประดิษฐ์ (AI) ยังเรียนรู้เทคนิคการตรวจจับได้ จึงสามารถที่จะพัฒนาตัวเองให้หลบหลีกการตรวจจับได้เช่นกัน จากการวิเคราะห์ข้อมูลรายงานมัลแวร์ในปี 2023 ของผู้ให้

บริการ Sandbox [9] โดยหากพิจารณาตาม MITRE ATT&CK แล้ว เทคนิคที่ถูกนำมาใช้มากที่สุด 2 อันดับแรก ก็คือ T1036.005 Masquerading: Match Legitimate Name or Location และ T1518.001 Software Discovery: Security Software Discovery พบว่าเป็นมัลแวร์ที่ใช้เทคนิคการปลอมแปลงตัวเองและหลบหลีกการตรวจจับจากอุปกรณ์ป้องกันขององค์กร จากข้อมูลดังกล่าวประกอบการรายงานข้อกังวลผลกระทบด้านลบเกี่ยวกับการนำปัญญาประดิษฐ์ (AI) มาใช้ในทางที่ผิด จึงเป็นเรื่องที่ควรต้องพิจารณาแนวทางการรับมือที่เหมาะสมต่อไป

6. แนวโน้มการโจมตี API ที่ไม่มีความปลอดภัย

จากการเติบโตของเทคโนโลยี Application Programming Interface หรือเรียกว่า API เข้ามามีบทบาทสำคัญในการเป็นช่องทางในการเชื่อมต่อบริการของธนาคารกับหน่วยงานภายนอกอื่นหรือจะเป็นการเชื่อมต่อระหว่างระบบภายในธนาคารอีกด้วย โดยตัวอย่างของข้อมูลที่มีการรับส่งผ่าน API เช่น ข้อมูลส่วนบุคคล ข้อมูลการเงิน หรือข้อมูลทางธุรกิจ ดังนั้นการพัฒนา API ที่ไม่ปลอดภัยอาจทำให้เกิดความเสี่ยงต่อการโจมตีทางไซเบอร์ได้ โดยในปีที่ผ่านมาหลายองค์กรได้เล็งเห็นความสำคัญเร่งปรับตัวและพัฒนาเสริมความปลอดภัยให้กับ API ขององค์กร ในปีที่ผ่านมา TB-CERT และธนาคารแห่งประเทศไทยได้ร่วมกันพัฒนาแนวปฏิบัติการใช้เทคโนโลยี Application Programming Interface (API) ในการให้บริการทางการเงิน เพื่อให้เป็นกรอบในการ Implement เทคโนโลยี API ให้มีความปลอดภัย

7. Geopolitical Tensions Led Cyber Warfare

ในปีที่ผ่านมาได้พบสงครามไซเบอร์ (Cyber warfare) ที่เกิดขึ้นจากความขัดแย้งในหลายพื้นที่และมีผลกระทบขยายตัวออกไปในหลายประเทศที่สนับสนุนฝ่ายต่าง ๆ อย่างที่เห็นได้ชัดในสงครามรัสเซียและยูเครน แต่สิ่งที่พบการเพิ่มขึ้นแบบมีนัยสำคัญและกระทบโดยตรงกับประเทศไทยก็คือ การพบกลุ่ม Hacktivism เกิดขึ้นใหม่จำนวนมากอย่างมีนัยสำคัญในหลายประเทศ รวมถึงประเทศเพื่อนบ้านของประเทศไทย ซึ่งกลุ่ม Hacktivism นี้จะเป็นกลุ่มของแฮคเกอร์ที่มีการแสดงออกทางความเชื่อ การเมือง โดยการโจมตีฝ่ายตรงข้ามที่ไม่เห็นด้วยหรือมีความเชื่อต่างกัน และในปีที่ผ่านมา ได้พบว่า มีอย่างน้อย 2 เหตุการณ์สำคัญเกิดขึ้นจากการดำเนินการของ Hacktivism คือ

[9] Malware Trends Overview Report: 2023, ANY.RUN

เหตุการณ์ที่ 1 โดยกลุ่ม Anonymous Cambodia กลุ่ม NDT SEC กลุ่ม K0LzSec และกลุ่ม CYBER SKELETON ได้ประกาศปฏิบัติการภายใต้ชื่อว่า OpThailand โดยมีเป้าหมายในการโจมตีเว็บไซต์ของหน่วยงานสำคัญต่าง ๆ ในประเทศไทยด้วยเทคนิค Distributed Denial of Service (DDoS) เพื่อทำให้หน่วยงานดังกล่าวไม่สามารถให้บริการหรือเข้าเว็บไซต์ของหน่วยงานต่าง ๆ ดังกล่าวไม่สามารถให้บริการได้

เหตุการณ์ที่ 2 เกิดขึ้นเนื่องจากความขัดแย้งและสงครามระหว่างอิสราเอล-ฮามาส โดยกลุ่ม AnonGhost และกลุ่ม 4-EXPLOITATION ประกาศโจมตี หน่วยงานรัฐ สถาบันการเงินและหน่วยงานต่างๆ ในประเทศไทย เนื่องจาก Hacktivism 2 กลุ่มนี้เข้าใจว่าประเทศไทยสนับสนุนฝ่ายตรงข้ามกับฝ่ายที่ตนเองสนับสนุน ซึ่งหลายหน่วยงานในประเทศไทยได้รับผลกระทบทั้งทางตรงและทางอ้อม ถึงแม้ว่าในภาคการเงินธนาคารและสถาบันการเงินของประเทศไทยจะไม่ได้รับความเสียหายจากการโจมตี แต่กลุ่มดังกล่าวได้มีการแอบอ้างว่าปฏิบัติการการโจมตีไปหน่วยงานต่าง ๆ รวมถึงธนาคารบางแห่งสำเร็จ ซึ่งก่อให้เกิดการเข้าใจผิดและกระทบต่อชื่อเสียงของหน่วยงานที่ถูกกล่าวถึงเช่นกัน

ซึ่งทาง TB-CERT คาดการณ์ว่าในปี 2024 และอนาคตอันใกล้ เราจะได้เห็นกลุ่ม Hacktivism ที่มีเพิ่มมากขึ้น อันเนื่องมาจากความขัดแย้งในด้านต่าง ๆ ในระดับระหว่างประเทศยังคงมีต่อเนื่องและมีแนวโน้มมากขึ้น และจากการติดตามความเคลื่อนไหวของ Hacktivism กลุ่มสำคัญ ๆ จะพบว่า Hacktivism บางกลุ่มที่มีความสามารถสูงจะให้บริการการโจมตีในลักษณะของ as a service ให้กับกลุ่ม Hacktivism กลุ่มอื่น ๆ ด้วย ซึ่งจะทำให้การโจมตีทางไซเบอร์มีมากขึ้นตามไปด้วย จึงเป็นเรื่องที่ทุกหน่วยต้องให้ความสำคัญในการยกระดับความพร้อมในการรับมือต่อภัยคุกคามทางด้านไซเบอร์ ติดตามและเฝ้าระวัง รวมถึงการซักซ้อมการรับมือต่อภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ

8. ภัยจากการโจมตีอุปกรณ์ Smart Device ที่มีความซับซ้อนมากขึ้น

ในช่วงเวลา 2-3 ปีที่ผ่านมา พฤติกรรมการใช้ชีวิต การทำงาน หรือดำเนินธุรกิจได้ทำธุรกรรมต่าง ๆ ผ่านอุปกรณ์ Smart Device มากขึ้น จึงเป็นเป้าหมายให้กลุ่มมิจฉาชีพมุ่งเป้าโจมตีที่อุปกรณ์ Smart device ของเหยื่อโดยตรง เนื่องจากมีโอกาสความสำเร็จมากกว่าที่จะมุ่งโจมตีที่ระบบ โดยในช่วงแรกที่พบจะเป็นการหลอกเหยื่อให้คลิกลิงก์และติดตั้งแอปพลิเคชันปลอมหรือเพื่อควบคุมเครื่องของของเหยื่อจากระยะไกล แต่ในช่วงที่ผ่านมามิจฉาชีพได้ใช้เทคนิคการหลอกที่ความซับซ้อนเยอะมากขึ้น เช่น การใช้ประโยชน์จาก

ข้อมูลเหยื่อที่รั่วไหล การปลอมแปลงเป็นเจ้าหน้าที่รัฐ หลอกให้เหยื่อกรอก Pin ที่ใช้อยู่ประจำ หรือการหลอกให้เหยื่อแสกนหน้าให้มิจฉาชีพผ่านแอปพลิเคชันปลอม ซึ่งเทคนิคดังกล่าว TB-CERT ได้ร่วมกันวิเคราะห์และได้ออกมาตรการเพื่อยกระดับการป้องกันอย่างต่อเนื่อง ซึ่งจากทีผ่านมาเราได้เห็นมิจฉาชีพได้พยายามหาจุดอ่อนจากการใช้ Smart Device ที่มีฟังก์ชันอำนวยความสะดวกสบายให้กับผู้ใช้งานไม่ว่าจะเป็นบริการ Accessibility Service, Screen Mirroring หรือ Video Call ผ่านแอปพลิเคชันแชท เป็นต้น

อ้างอิง

- Global Risks Report 2024, World Economic Forum
- Gartner Top 10 Strategic Technology Trends 2024
- Proactive risk management in Generative AI, Deloitte
- Cyble: Threat Landscape Report 2023-2024
- Symantec: The 2024 Ransomware Threat Landscape
- Malware Trends Overview Report: 2023, ANY.RUN
- CompTIA State of Cybersecurity 2024
- Global Cybersecurity Outlook 2024, World Economic Forum

บทสรุปและเป้าหมายในปี 2567

บทสรุป และ เป้าหมาย ในปี 2567

ในปี 2566 การแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะปัญหาที่เกี่ยวกับแอปพลิเคชันปลอมหรือที่รู้จักกันดีว่าเป็นแอปดูดเงินนั้น ได้รับความร่วมมือเป็นอย่างดีจากทุกหน่วยงานสมาชิกของภาคการธนาคาร ธนาคารแห่งประเทศไทย บริษัทผู้ให้บริการเครือข่ายโทรศัพท์มือถือ หน่วยงาน Sectorial CERT รวมทั้งหน่วยงานภาครัฐต่าง ๆ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) เป็นต้น แม้ว่าจะเกิดความเสียหายเป็นจำนวนมาก แต่เมื่อศึกษาแนวโน้มแล้วพบว่า ความเสียหายจากแอปดูดเงินในช่วงปลายปีมีปริมาณลดลงอย่างมีนัยสำคัญ

อย่างไรก็ตาม การพัฒนาทักษะความรู้เชิงเทคนิค การสร้างความรู้ความเข้าใจ ความตระหนัก ให้รู้เท่าทันกลลวงของมิจฉาชีพในสถานการณ์ที่เป็นปัจจุบันในขณะนั้น ที่สำคัญคือทักษะการตรวจสอบความน่าเชื่อถือของข้อมูล (Information Validation) จะเป็นทักษะที่มีความสำคัญในการคัดกรองข้อมูลที่ถูกบิดเบือน (Disinformation) เป็นการเสริมสร้างภูมิคุ้มกันต่อภัยไซเบอร์ในภาพรวมของประชาชนในยุคดิจิทัล และจะเป็นส่วนหนึ่งในการยกระดับความน่าเชื่อถือของประเทศไทยในเวทีสากล

ในปี 2567 นี้ การยกระดับการวิเคราะห์ข้อมูล การทำงานร่วมกันระหว่างหน่วยงานทั้งภายในและภายนอกภาคการธนาคาร การสร้างความเชื่อมโยงกระบวนการจัดการทุจริตและการจัดการด้านความมั่นคงปลอดภัยยังคงมีความจำเป็นอย่างยิ่ง เพื่อที่จะทำให้สามารถวิเคราะห์สถานการณ์ได้ดีขึ้น ทำให้การประเมินความเสี่ยงในการทำธุรกิจทำได้มีประสิทธิภาพมากขึ้น โดยจะสามารถนำไปใช้ในการป้องกันความเสี่ยงโดยตรง ซึ่งจะเป็นการลดต้นทุนของธุรกิจได้อีกด้วย

ภาคผนวก

การแจ้งเตือน Incident Alert

ในการให้บริการแก่ธนาคารสมาชิก TB-CERT ได้มีการแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์ (Incident alert) โดยสรุปรายการเหตุการณ์ Alert ระหว่างวันที่ 1 มกราคม - 31 ธันวาคม 2566 มีจำนวน 10 เหตุการณ์ ดังนี้

ลำดับ	วันที่แจ้ง	หัวข้อ
1	20 มกราคม 2566	แจ้งผลวิเคราะห์รายงาน Android malware ที่ธนาคารในไทยทำร่วมกับบริษัท Trend Micro
2	16 มีนาคม 2566	แจ้งเตือนพบการประกาศขายข้อมูลคนไทย 55 ล้านรายชื่อ จากแฮกเกอร์ 9Near
3	17 มีนาคม 2566	แจ้งเตือนช่องโหว่ของ Microsoft Outlook ที่ตกเป็นเป้าของกลุ่มแฮกเอกร์จากรัสเซีย
4	9 พฤษภาคม 2566	แจ้งเตือนพบการใช้ SMS Sender name ชื่อเหมือนธนาคาร
5	12 มิถุนายน 2566	แจ้งเตือนพบช่องโหว่อุปกรณ์ Fortigate
6	4 กรกฎาคม 2566	แจ้งเตือนยกระดับการเฝ้าระวังโจมตีด้วย DDoS จากกลุ่มแฮกเกอร์ประเทศกัมพูชา
7	20 สิงหาคม 2566	แจ้งเตือนพบช่องโหว่ Zero-day ของอุปกรณ์ Citrix
8	14 สิงหาคม 2566	แจ้งเตือนยกระดับการเฝ้าระวังโจมตี จากกลุ่มแฮกเกอร์ประเทศกัมพูชา (สถานการณ์ต่อเนื่อง)
9	26 ตุลาคม 2566	แจ้งเตือน พบกลุ่ม Hacktivist จากประเทศเพื่อนบนโจมตีหน่วยงานในประเทศไทย
10	9 พฤศจิกายน 2566	แจ้งเตือน ตรวจสอบความปลอดภัยตู้ ATM เนื่องจากพบอุปกรณ์ต่อพ่วงแปลกปลอม

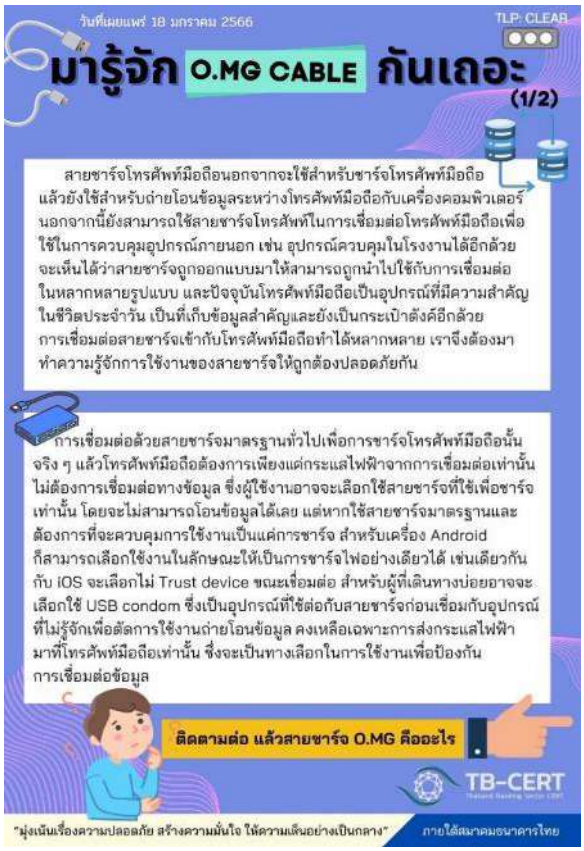
Technical Recommendation

ในรอบปีที่ผ่านมา TB-CERT ได้มีการแชร์ข้อมูลข่าวจากกลุ่ม Threat Intelligence ต่าง ๆ กลุ่มสมาชิก TB-CERT รวมทั้งการวิเคราะห์ข้อมูลข่าวกรองไซเบอร์จากระบบ MISP เพื่อสรุปข้อมูลภัยคุกคามไซเบอร์ และข้อมูล Technical recommendation ให้หน่วยงานสมาชิกใช้ในการยกระดับการเฝ้าระวัง ดังนี้

ลำดับ	วันที่เผยแพร่	หัวข้อ
1	9 มกราคม 2566	Fin7 Unveiled: A deep dive into notorious cybercrime gang
2	9 มกราคม 2566	TIS Group: Thai banking external attack
3	6 กุมภาพันธ์ 2566	TB-CERT Member Generated IoC • Android malware in Thailand (Fake dating apps) • Android malware in Thailand (Fake government and corporate apps)
4	6 กุมภาพันธ์ 2566	GodFather Android Malware
5	7 มีนาคม 2566	Supply Chain Attacks via New Malicious Python Packages in PyPi
6	7 มีนาคม 2566	WinorDLL64: a backdoor from Lazarus
7	3 เมษายน 2566	1.Blind Eagle Deploys Fake UUE Files
8	3 เมษายน 2566	Ongoing campaign, Chinese cyber espionage group SharpPanda
9	8 พฤษภาคม 2566	FIN7 Hackers Exploit Veeam Backup
10	8 พฤษภาคม 2566	Lazarus Subgroup Targeting Apple Devices with New RustBucket macOS Malware
11	6 มิถุนายน 2566	ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations
12	6 มิถุนายน 2566	Kimsuky Group Using Meterpreter to Attack Web Servers
13	3 กรกฎาคม 2566	MOVEit Transfer Critical Vulnerability (CVE-2023-34362)
14	3 กรกฎาคม 2566	Anatsa banking trojan
15	7 สิงหาคม 2566	Ivanti / MobileIron CVE-2023-35078 exploit active scanning
16	7 สิงหาคม 2566	Tomcat Under Attack: Exploring Mirai Malware and Beyond
17	4 กันยายน 2566	FIN8 group exploits the CVE-2023-3519 RCE in attacks on Citrix NetScaler systems in massive attacks.
18	4 กันยายน 2566	Chinese Cyber Actors Continue to Globally Exploit Barracuda ESG Zero-Day

ลำดับ	วันที่เผยแพร่	หัวข้อ
19	2 ตุลาคม 2566	US and Japan warn of Chinese hackers backdooring Cisco routers
20	2 ตุลาคม 2566	APT groups targeting Thailand Government
21	6 พฤศจิกายน 2566	Israel-Hamas Conflict
22	6 พฤศจิกายน 2566	Exploit for Cisco IOS XE Zero-day Vulnerability (CVE-2023-20198)
23	4 ธันวาคม 2566	Citrix NetScaler Vulnerability series (CVE-2023-3519, CVE-2023-4966, CVE-2023-4967)

Public Awareness




วันที่เผยแพร่ 6 กุมภาพันธ์ 2566
TLP: CLEAR
ทำไมเวลาเราลงแอปพลิเคชันใหม่ๆ ต้องให้เรากดอนุญาต ให้มีการเข้าถึง กล้อง ไมค์ หรือ รายชื่อผู้ติดต่อ ด้วยนะ ?
โดยปกติแล้ว การขอสิทธิ์เข้าถึงนี้ ก็เพื่อประโยชน์ด้านฟีเจอร์ของแอปพลิเคชัน เช่น
กล้องและไมค์
ปฏิทิน
รายชื่อผู้ติดต่อ
App Permission
แต่หากไม่ระวัง การให้ Permission อาจทำให้มีการเข้าถึงและละเมิดความเป็นส่วนตัวได้
App Permission
แล้วเราควรอนุญาตอะไรบ้าง ?
ตรวจสอบการตั้งค่าอย่างไร ?
ไปดูกัน!
(1/4)
TB-CERT


วันที่เผยแพร่ 6 กุมภาพันธ์ 2566
TLP: CLEAR
พิจารณาอย่างไร ก่อนให้ Permission ?
ควรพิจารณาถึงความเหมาะสมกับประเภทของแอปพลิเคชัน ความจำเป็นของการทำงาน และนึกถึงความปลอดภัยของข้อมูลส่วนตัวอยู่เสมอ เช่น หากแอปพลิเคชันถ่ายรูป แต่กลับมีการขอเข้าถึง SMS หรือลงโปรแกรม ซึ่งถือว่าไม่เหมาะสม เราก็ไม่ควรกดอนุญาต App Permission
ตัวอย่างการขอ Permission ที่ควรสังเกตและระมัดระวัง
เข้าถึงสิทธิ์การถ่ายรูป
เข้าถึงข้อมูลการใช้งาน SMS
เข้าถึงข้อมูลการใช้งาน Accessibility หรือการส่งงานโดยไม่ผ่านสื่อหน้าจอของผู้ใช้
เข้าถึงข้อมูลการใช้หน่วยความจำภายนอก (External storage)
เข้าถึงสิทธิ์การลบ (ปรแกรมบนอุปกรณ์มือถือได้)
เข้าถึงสิทธิ์การแก้ไขเปลี่ยนแปลงการตั้งค่าของอุปกรณ์มือถือได้
ไปดูวิธีการตรวจสอบและการตั้งค่ากัน
App Permission
(2/4)
TB-CERT


วันที่เผยแพร่ 6 กุมภาพันธ์ 2566
TLP: CLEAR
วิธีการตรวจสอบ App Permission
ก่อนติดตั้งแอป
Android
รูปที่ 1
1. เมื่อเจอแอปที่ต้องการติดตั้งใน Play Store > ให้ไปที่ เกี่ยวกับแอปนี้ (About this app)
2. ไปที่ สิทธิ์ของแอป (App Permissions)
3. ตรวจสอบสิทธิ์ในการเข้าถึงของแอป
iOS
รูปที่ 2
1. เมื่อเจอแอปที่ต้องการติดตั้งใน App Store > ให้ไปที่ ความเป็นส่วนตัวของแอป (App Privacy)
2. ไปที่ See Details เพื่อตรวจสอบสิทธิ์ในการเข้าถึง
เฮ๊ะ !!!
ทำไมแอปต้องขอเข้าถึงข้อมูลการใช้งานเล็กน้อย
(3/4)
TB-CERT


วันที่เผยแพร่ 6 กุมภาพันธ์ 2566
TLP: CLEAR
วิธีตรวจสอบ App Permission
หลังติดตั้งแอป
รูปที่ 3
1. ไปที่การตั้งค่า (Settings) > แอป (Apps)
2. เลือก App ที่ต้องการจัดการ
3. ปิดการอนุญาตที่ไม่จำเป็น โดยแตะปุ่มสีเขียวให้เป็นสีเทา
รูปที่ 4
1. ไปที่การตั้งค่า (Settings) > แอป (Apps)
2. เลือก App ที่ต้องการจัดการ > การอนุญาต (Permissions)
3. ปิดการอนุญาตที่ไม่จำเป็น โดยแตะปุ่มสีเขียวให้เป็นสีเทา
คำแนะนำ
• ก่อนติดตั้งแอปพลิเคชัน ควรตรวจสอบ App Permission ตามวิธีดังรูปที่ 1 และ 2 หากแอปมีการขอสิทธิ์เข้าถึงเกินจำเป็น ไม่ควรติดตั้งแอปดังกล่าวเพื่อลดความเสี่ยง
• หากติดตั้งแอปพลิเคชันไปแล้ว สามารถเปลี่ยนแปลง App Permission ตามวิธีดังรูปที่ 3 และ 4
• ดาวน์โหลดและติดตั้งแอปพลิเคชันจาก Play Store หรือ App Store เท่านั้น
(4/4)
TB-CERT


วันที่เผยแพร่ 14 กุมภาพันธ์ 2566
TLP: CLEAR
แอปอันตราย
แอบแฝงบนมือถือ Android ตรวจจับ
ง่าย ๆ และปลอดภัย ด้วย Google Play Protect
หลังจากที่มีการรายงานว่าพบแอปพลิเคชันที่สามารถขโมยเงินของ
ผู้ใช้งาน อ่านข้อความ และสอดแนมการทำงานต่าง ๆ ภายในเครื่องได้
วันนี้เราจึงมาแนะนำวิธีการตรวจสอบมือถือ Android ว่า
"มีแอปพลิเคชันที่เป็นอันตรายอยู่
ในมือถือของคุณหรือไม่"
ด้วย Google Play Protect ซึ่งเป็นระบบป้องกันมัลแวร์
ที่มาพร้อมกับ Android ทำหน้าที่ตรวจจับแอปพลิเคชัน
ที่ผู้ใช้งานดาวน์โหลด ว่ามีอันตรายหรือไม่ ถ้าหากพบ
ความผิดปกติก็จะหยุดการทำงานของแอปพลิเคชันนั้น
(1/2)
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย
TB-CERT


วันที่เผยแพร่ 14 กุมภาพันธ์ 2566
TLP: CLEAR
วิธีการเปิดใช้งาน Google Play Protect
1. เข้าไปที่ Google Play Store
2. เลือกไอคอนโปรไฟล์ที่ด้านขวาบน และเลือก Play Protect
3. เลือก scan เพื่อตรวจหามัลแวร์ในแอปพลิเคชันต่าง ๆ
4. ระบบจะค้นหาแอปพลิเคชันที่เป็นอันตราย** หากเจอให้ Uninstall
ปลอดภัย
พบแอปอันตราย
กด Uninstall
เพื่อลบการติดตั้ง
(2/2)
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย
TB-CERT


วันที่เผยแพร่ 3 มีนาคม 2566
TLP: CLEAR
กลยุทธ์หรือยุทธวิธี
ที่มิจฉาชีพใช้ประกอบการชักจูง
Urgency
Misdirection
Sympathy
Authority
เหตุจูงใจหลัก ๆ ที่ทำให้หลงกล
รัก
หลอกให้รักและเชื่อใจ
โลภ
หลอกล่อด้วยของแถม ของฟรี
เงินคืน หรือ ลงทุนได้ผลตอบแทนดี
กลัว
หลอกให้กลัวว่าจะต้องถูกดำเนินคดี
ถูกปรับ เคยหลบเลี่ยงภาษี
ถ้าไม่ทำก็คลาดความผิดตามที่ถูกกล่าวอ้าง
หลง
หลอกให้หลง จบง่ายในกาม
เช่น ให้ดู live สด 18+
TB-CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้สมาคมธนาคารไทย


วันที่เผยแพร่ 29 มีนาคม 2566
TLP: CLEAR
'เช็คก่อนเชื่อ ไม่หลงเป็นเหยื่อกลโกง'
ธนาคารได้ออกมาตรการยกเลิกส่งลิงก์ผ่านทางSMS เพื่อเป็นการป้องกันมิจฉาชีพ แต่มิจฉาชีพเองก็ได้เปลี่ยนกลวิธีโดยใช้การส่งไลน์ไอดีหรือสแกนคิวอาร์โค้ดเพื่อให้ประชาชนเพิ่มเพื่อน และคุยหลอกล่อ ล้วงข้อมูลด้วยวิธีต่าง ๆ ไม่ว่าจะเป็น การส่งลิงก์ให้กด หรือคิวอาร์โค้ดให้สแกนเพื่อเข้าสู่เว็บหรือแอปฯ อันตราย
วิธีสังเกตและข้อควรระวัง
• ไม่เพิ่มเพื่อนหรือเปิดช่องทางการติดต่อจากคนที่ไม่รู้จัก
หากมีการขอให้แอดไลน์ ให้สงสัยไว้ก่อนว่าเป็นมิจฉาชีพ
• สังเกตบทสนทนา และไม่ให้ข้อมูลส่วนตัวเด็ดขาด
หากมีการขอความช่วยเหลือหรือมีการขอข้อมูลสำคัญหรือให้ติดตั้งแอปฯ หรือมีการให้ข้อมูลพยายามสร้างความน่าเชื่อถือ ควรรวบรวมข้อมูลและแจ้งธนาคารให้ทราบ
• สังเกต Line Official จะมีโล่สีเขียวและน้ำเงิน
หากไม่ใช่ ให้สันนิษฐานไว้ก่อนว่าเป็นของปลอม
เตือนภัย!
มิจฉาชีพเริ่มเปลี่ยนจาก
ส่งลิงก์เป็นให้แอดไลน์ไอดี
หรือ QR Code
พี่แอดไลน์แล้ว
ทักผมมาทางนี้
ได้เลยครับ
"มุ่งเน้นเรื่องความปลอดภัย สร้างความเชื่อมั่น ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย
TB-CERT


วันที่เผยแพร่ 17 เมษายน 2566
TLP: CLEAR
2 แอปฯ อันตรายบน Play Store
(1/2)
"ดูดเงิน สอดแนม อ่านข้อความ"
ลบทิ้งด่วน !!
Google Play
aaorntoteq
Accessibility Service Go
Accessibility Service
พบ 2 แอปฯ บน Google Play Store ที่มีการขออนุญาตเข้าถึง Accessibility Service เพื่อบังหน้าจอ รวบรวมข้อมูลการสัมผัสหน้าจอ ซึ่งอาจนำไปสู่การขโมยข้อมูลส่วนตัวและการเข้าถึงบัญชีธนาคาร
ข้อแนะนำ
หากได้รับลิงก์จากคนไม่รู้จัก แล้วมีการให้ดาวน์โหลดแอปฯ ให้สงสัยไว้ก่อนว่าเป็นลิงก์อันตรายจากมิจฉาชีพ ควรหลีกเลี่ยงการดาวน์โหลดและติดตั้ง
"มุ่งเน้นเรื่องความปลอดภัย สร้างความเชื่อมั่น ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย
TB-CERT


วันที่เผยแพร่ 17 เมษายน 2566
TLP: CLEAR
วิธีตรวจสอบมือถือ Android
ถูกติดตั้งแอปฯ ดูดเงินหรือไม่
(2/2)
ไปที่เมนูการตั้งค่า > แอปพลิเคชัน > จุดสามจุด (ขวาบน) > การเข้าถึงพิเศษ
หากตรวจสอบแล้วพบการติดตั้งแอปฯ เหล่านี้ ให้รีบ ถอนการติดตั้ง
วิธีลบแอปฯ บนมือถือ Android
Manage apps & device
aaorntoteq
Rate this app
"มุ่งเน้นเรื่องความปลอดภัย สร้างความเชื่อมั่น ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย
TB-CERT


วันที่เผยแพร่ 20 เมษายน 2566
TLP: CLEAR
ระวัง
มิจฉาชีพส่ง SMS ชวนให้ตกใจ พร้อมลิงก์ให้แอด LINE ปลอม
LINE ปลอม
ABANK
มีผู้เข้าสู่ระบบธนาคารของคุณจากอุปกรณ์อื่น หากไม่ได้ดำเนินการด้วยตนเอง โปรดติดต่อทันที ABANK.ta-line.cc
ABANK
Add
Block
Report
แอคเคาท์ธนาคารของจริงต้องมี ★ ★ เท่านั้น
ธนาคารไม่มีนโยบายแนบลิงก์ผ่าน SMS
คำแนะนำ
ช่องทาง LINE ของธนาคารของจริง
มีสัญลักษณ์ ★ ★ หน้าชื่อ
แอด LINE โดยการพิมพ์ชื่อธนาคารเองเท่านั้น
ตั้งสติให้มั่น ไม่กดลิงก์ โทรติดต่อธนาคารโดยตรง
TB-CERT


รู้หรือไม่
คนร้ายสามารถปลอมแปลงชื่อผู้ส่ง SMS เป็นชื่อธนาคารหรือองค์กรต่าง ๆ ได้เหมือนกับของจริง!!!!
ปัจจุบันมิจฉาชีพมีการส่ง SMS โดยให้เหยื่อหลงเชื่อคิดว่าเป็นข้อความจากธนาคารนั้นจริง โดยไม่ผ่านเครือข่ายของผู้ให้บริการวิธีการนี้เรียกว่า
FALSE BASE STATION (FBS) ATTACK
ข้อแนะนำ
หากท่านได้รับ SMS ใด ๆ จากธนาคาร แล้วมีการแนบลิงก์มา ให้ สงสัยไว้ได้เลยว่าเป็นมิจฉาชีพ
ตัวอย่าง
TB-CERT
ชื่อธนาคารผู้ส่งจริง
ข้อความ
มิจฉาชีพ
มีผู้เข้าสู่ระบบธนาคารของคุณจากอุปกรณ์อื่น หากไม่ได้ดำเนินการด้วยตนเอง โปรดต่อติดต่อทันที
ABANK.ta-line.cc
ลิงก์
"ธนาคารได้ยกเลิกการส่งลิงก์ใด ๆ ผ่าน SMS ตามนโยบายธนาคารแห่งประเทศไทย"


วันที่เผยแพร่ 25 พฤษภาคม 2566
TLP: CLEAR
แจ้งเตือนภัย!!
หลอกติดตั้งแอปพลิเคชันเลียนแบบ DLT SMART QUEUE
พบกลุ่มมิจฉาชีพกลับมาอีกแล้ว โดยการหลอกผู้เสียหายให้ติดตั้งแอปพลิเคชันหลอกลวง มีลักษณะเลียนแบบแอปพลิเคชัน DLT Smart Queue กรมการขนส่งทางบก
ขอแจ้งให้ประชาชนผู้ใช้บริการรับทราบและติดตาม เพื่อป้องกันภัยจากมิจฉาชีพ
คำแนะนำ
1. ไม่คลิกลิงก์ ดาวน์โหลดแอปพลิเคชันจากนอก Official store
2. ต้องพิมพ์ชื่อค้นหาแอปพลิเคชันด้วยตนเองใน Official store หากต้องการดาวน์โหลดและติดตั้ง
3. อย่าหลงเชื่อข้อมูลมิจฉาชีพ แม้ข้อมูลนั้นจะถูกต้อง ให้ติดต่อกลับไปหน่วยงานนั้นโดยตรง
Google Play
DLT Smart Queue
ตัวอย่าง แอปพลิเคชันหลอกลวงที่พบ
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
TB-CERT ภายใต้สมาคมธนาคารไทย


วันที่เผยแพร่ 29 พฤษภาคม 2566
TLP: CLEAR
(1/2)
เตือนภัย !
มิจฉาชีพปลอมเว็บไซต์ DLT SMART QUEUE
กรมการขนส่งทางบก
https://gecc.dlt.go.th/dlt-Smartqueue
https://dlt-license.com/login
ปลอม
เมื่อทำการกดปุ่มลงทะเบียน/เข้าสู่ระบบ/หรือลืมรหัสผ่าน จะขึ้นให้ Add ปลอม
TB-CERT


วันที่เผยแพร่ 29 พฤษภาคม 2566
TLP: CLEAR
(2/2)
เตือนภัย !
มิจฉาชีพปลอมเว็บไซต์ DLT SMART QUEUE
กรมการขนส่งทางบก
จากนั้น ให้ ADD ปลอม
โล่สีเทา คือบัญชีที่ยังไม่ผ่านการรับรอง
กรมการขนส่งทางบก
E-license Thailand
สังเกต LINE หน่วยงานจริง จะมีโล่ดาวสีเขียวและสีน้ำเงิน
TB-CERT


วันที่เผยแพร่ 10 สิงหาคม 2566
TLP: CLEAR
(1/2)
ติดตั้งแอปมือถือ
แบบปลอดภัย
ต้องไม่ควานไปโหลดนอก Official Store
Search
Google Play
App Store
TB-CERT


วันที่เผยแพร่ 10 สิงหาคม 2566
TLP: CLEAR
(2/2)
คำแนะนำ
การติดตั้งแอปพลิเคชันที่มาจาก Store ที่ได้รับการยอมรับ เช่น Google Play, App Store, หรือ Huawei AppGallery เป็นการป้องกันอันตรายจากมิจฉาชีพขั้นพื้นฐานที่ทุกคนควรทราบและปฏิบัติตาม โดยมีคำแนะนำดังนี้
พิมพ์ชื่อแอปด้วยตัวเองใน Official Store
ไม่กดลิงก์จากคนที่ไม่รู้จัก
ไม่สแกนใบหน้า ลายนิ้วมือ หรือใส่รหัส PIN ตามคำบอกของบุคคลอื่น
TB-CERT


วันที่เผยแพร่ 10 สิงหาคม 2566
TLP: CLEAR
สายเรียกเข้าของมิจ(ฉาชีพ)
อ้างเป็นเจ้าหน้าที่
ควรปฏิบัติตัวอย่างไร?
ไม่ทำตามในสิ่งที่บุคคลนั้นบอก เช่น ให้กดลิงก์ ติดตั้งแอป ใส่รหัส PIN
ติดต่อหน่วยงานและคุยกับเจ้าหน้าที่เองโดยตรง เนื่องจากมิจฉาชีพอาจใช้ข้อมูลที่รั่วไหลมาอ้างเพื่อสร้างความน่าเชื่อถือ
เจ้าหน้าที่หน่วยงานจริงจะไม่โทรศัพท์ผ่านช่องทาง
สังเกตสัญลักษณ์โล่ของ หน่วยงาน
บัญชีที่ยังไม่ยืนยันตัวตน หรือบัญชีที่ไม่มีโล่ —> ควรระวัง!!
บัญชีที่ยืนยันตัวตนและตรวจสอบแล้ว
บัญชีทางการขององค์กรหรือหน่วยงาน
TB-CERT


วันที่เผยแพร่ 25 สิงหาคม 2566
TLP: CLEAR
!!ระวัง!!
แอปฯ แอบอ้าง
'ลงทะเบียนเงินดิจิทัล'
10,000 บาท
ไม่ติดตั้งแอปฯ
ไม่กดลิงก์
ไม่แอดไลน์
ปลอม!!
TB-CERT


TB-CERT
เตือนภัย มาอีกแล้ว
เมื่อได้รับ SMS ยอดค้างชำระ m-flow และหากคลิ๊กลิ้งก์จะให้ Add LINE ของ
กรมการขนส่งทางบกปลอม
แล้วรู้ได้ไงว่าปลอม? จุดสังเกตคือ !!!!!!!!!!
โล่สีเขียว หรือ ปลอมแน่นอนจ้า
โล่สีกรม ของ LINE หากไม่มีอยู่ด้านหน้าชื่อของหน่วยงานสันนิษฐานไว้เลยว่า
Step 1
Step 2
Step 3
หากคุณหยุดที่ step 2
ไม่ไปคุยต่อใน LINE ปลอม
คุณคือผู้รอดจาก มิจฉาชีพ
หลอกดูดเงินแน่นอน!!
TLP: WHITE
เผยแพร่วันที่ 28/8/2566

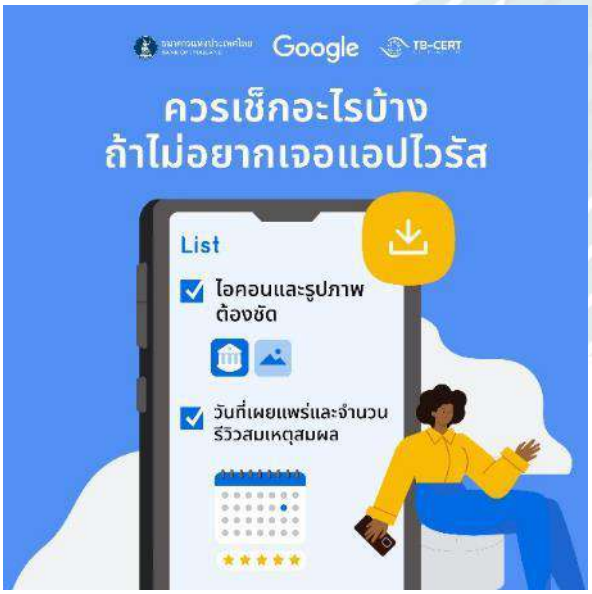

Google
TB-CERT
รู้หรือไม่?!
ธนาคารเลิกส่งลิงก์ให้ทาง
SMS และ อีเมล แล้ว
พฤ. 5 ต.ค.
หากได้รับ ให้คิดเลยว่า
มาจากมิจฉาชีพ
แน่นอน!


Google
TB-CERT
รู้หรือไม่?!
ธนาคารไม่ขอข้อมูลส่วนตัว
ผ่านโซเชียลมีเดีย
สวัสดีค่ะ ติดต่อจากธนาคารนะคะ
รบกวนขอข้อมูลเพื่อตรวจสอบบัญชีค่ะ
http://bonkofthai.com/etd87
หากได้รับลิงก์ให้คิดเลยว่า
มาจากมิจฉาชีพแน่นอน!


Google
TB-CERT
อย่าเพิ่งกดลิงก์!
ตรวจสอบกับหน่วยงานโดยตรง
ก่อนดีกว่า!
พฤ. 5 ต.ค.
ธนาคาร
สวัสดีค่ะ เจ้าหน้าที่ฝ่ายข้อมูลธนาคาร
ขอให้ท่านรีบอัปเดตสถานะข้อมูลให้เป็น
ปัจจุบัน สามารถคลิกลิงก์เพื่อดำเนินการ
ได้เลยค่ะ
http://bonkofthailand.com/ufi24


Google
TB-CERT
เซฟไว้เลย! วิธีสังเกต
บัญชีแชทปลอม
1.ใช้ชื่อและรูปโปรไฟล์เหมือน
ของจริง หรือหน่วยงานจริง
2.ไม่มีเครื่องหมาย "โล่สีเขียว
หรือ โล่สีน้ำเงิน"
3. ส่งข้อความมาหาก่อน
เพราะหน่วยงานรัฐจะไม่ติดต่อ
มาส่วนตัว
USER NAME


Google
TB-CERT
ควรเช็กอะไรบ้าง
ถ้าไม่อยากเจอแอปไวรัส
List
อ่านรีวิวและ
การให้คะแนน


Google
TB-CERT
ควรเช็กอะไรบ้าง
ถ้าไม่อยากเจอแอปไวรัส
List
ไอคอนและรูปภาพ
ต้องชัด
วันที่เผยแพร่และจำนวน
รีวิวสมเหตุสมผล


Google
TB-CERT
ควรเช็กอะไรบ้าง
ถ้าไม่อยากเจอแอปไวรัส
List
สิทธิ์การเข้าถึงข้อมูล
รุกล้ำความเป็นส่วนตัว
เกินไปหรือไม่
เช็กข้อมูลนักพัฒนาแอป
ว่าน่าเชื่อถือหรือไม่


Google
TB-CERT
ไม่ตอบ!
ข้อความจากคนแปลกหน้า
unknown
อย่าเชื่อทันที!
เมื่อมีคนแอบอ้างเป็น
หน่วยงานรัฐ


Google
TB-CERT
ทำธุรกรรมการเงิน
อย่างปลอดภัยง่ายนิดเดียว
ไม่ใช้ Wi-fi สาธารณะ หรือ Free Wi-fi
และที่ชาร์จสาธารณะในการทำธุรกรรมการเงินโดยเด็ดขาด
FREE
Wi Fi


Google
TB-CERT
ทำธุรกรรมการเงิน
อย่างปลอดภัยง่ายนิดเดียว
หมั่นอัปเดตแอป Mobile Banking เสมอ
เพื่อความปลอดภัยในการใช้งาน
UPDATE


Google
TB-CERT
รหัสผ่าน ต้องรัดกุม
JhK7#98Ks
ความยาวอย่างน้อย 8 ตัวอักษร
ใช้ทั้งตัวอักษรพิมพ์ใหญ่และเล็ก
ผสมตัวเลขและสัญลักษณ์เข้าด้วยกัน
ไม่ใช้ข้อมูลส่วนตัว เช่น วันเกิด
และไม่ใช้รหัสผ่านที่ซ้ำกัน!


Google
TB-CERT
เช็กลิสต์ต้องทำ
ก่อนจะเชื่อหรือส่งต่อข้อมูลออนไลน์
เช็กแหล่งที่มาของข้อมูล
อย่างละเอียดผ่าน Google
เช็กว่าทำไมแหล่งที่มาจึง
แชร์ข้อมูลดังกล่าว
เช็กว่าแหล่งที่มาน่าเชื่อถือ
และมีความรู้เกี่ยวกับ
หัวข้อนั้น ๆ หรือไม่


Google
TB-CERT
เอ๊ะซักนิด
ก่อนสแกน QR Code
1
สแกนเพื่อจ่ายเงิน ให้ทำผ่าน
แอปธนาคาร และเช็ก
ชื่อปลายทางและจำนวนเงิน
ให้ถูกต้อง
2
สแกนเพื่อดูข้อมูล เมื่อสแกนแล้ว
ต้องสังเกต URL ว่าเป็นเว็บไซต์
ของหน่วยงานนั้นจริง ถ้าไม่แน่ใจ
อย่าคลิกต่อ


Google
TB-CERT
เอ๊ะซักนิด
ก่อนสแกนหน้าทุกครั้ง
เพื่อป้องกันมิจฉาชีพเข้าถึงข้อมูลส่วนตัว
รู้จักแอปนี้หรือไม่
แอปเชื่อถือได้หรือไม่
ทำไมจึงต้องให้
สแกนหน้า


Google
TB-CERT
ไม่ขายบัญชีธนาคาร หรือซิมโทรศัพท์
ของตัวเอง ให้กับบุคคลอื่น
Bank
รู้หรือไม่!
เปิด – ขาย –
ให้เช่า – ให้ยืม:
จัดหา –
โฆษณา:
จำคุก 3 ปี หรือ
ปรับ 300,000 บาท หรือ
ทั้งจำทั้งปรับ
จำคุก 2-5 ปี หรือ
ปรับ 200,000-500,000 บาท หรือ
ทั้งจำทั้งปรับ


Google
TB-CERT
เลขบัตร
ประชาชน
เลขบัตร
เครดิต
Bank
เบอร์บัญชี
ธนาคาร
วัน เดือน
ปีเกิด
เก็บให้มิด ข้อมูลส่วนตัวเหล่านี้
ไม่ควรเปิดเผย!


Google
TB-CERT
เซฟไว้เลย! วิธีสังเกต
โปรไฟล์ปลอม
1. ไม่มี Verified Badge
2. ชื่อโปรไฟล์สะกดผิดหรือ ต่างจากโปรไฟล์จริงเล็กน้อย
3. โปรไฟล์เพิ่งสร้างมาไม่นาน
4. มียอดติดตามและ ยอดไลก์น้อย
12
300


Google
TB-CERT
ตั้งสติรู้ทันกลลวงมิจฉาชีพ!
กลโกงมักมาพร้อมความรู้สึกเร่งด่วน
เพื่อให้คุณไม่ได้ทันระวังตัว
ให้ใช้เวลาตรวจสอบข้อมูล
จนกว่าจะสบายใจได้เลย


Google
TB-CERT
โดนมิจฉาชีพหลอก!
ควรรีบทำอะไรต่อ
หากเผลอคลิกลิงก์ หรือไม่แน่ใจว่าโดนหลอก
ให้รีบเปลี่ยนรหัสผ่านแอปต่าง ๆ ทันที


Google
TB-CERT
ระวังมิจฉาชีพมา!
อย่าแชร์ข้อมูลส่วนตัว
บนโลกออนไลน์มากเกินไป
เลขหนังสือ เดินทาง
โลเคชั่น
วันเดือน ปีเกิด
ตั๋วเครื่องบิน
ข้อมูล ส่วนตัวอื่น ๆ


Google
TB-CERT
2 STEPS
ต้องทำทันที เมื่อตกเป็นเหยื่อ!
1. โทรหาธนาคารต้นทาง เพื่อระงับการทำธุรกรรม 72 ชั่วโมง
2. แจ้งความเพื่อยืดเวลา ระงับต่อเป็น 7 วัน


วันที่เผยแพร่ 7 พฤศจิกายน 2566
TLP: CLEAR
1/2
เตือนภัย! มิจฉาชีพมุ่งเป้าหลอก
'กลุ่มผู้เกษียณอายุ' ติดตั้งแอปปลอมรับเงินบำนาญ อ้างกรมบัญชีกลาง
TestFlight
OPEN
What's New
TB-CERT เตือนภัยออนไลน์ ให้ติดตั้งแอป 'TestFlight' ซึ่งเป็นแอปจริงบน Official Store แล้วหลอกซ้อนให้ติดตั้งแอปปลอม 'Digital Pension' รับเงินบำนาญดิจิทัล อ้างเป็นของกรมบัญชีกลาง
เทคนิคที่แก๊งมิจฉาชีพใช้หลอก
แอปพลิเคชัน 'TestFlight' เป็นแอปจริงบน Official Store ที่นักพัฒนาแอปมักจะใช้ในการทดสอบและพัฒนาแอปพลิเคชันใหม่ ๆ มิจฉาชีพอาศัยช่องทางนี้ในการส่งลิงก์ให้ติดตั้งแอป จากนั้นจะหลอกให้เหยื่อลงแอปปลอมที่เป็นอันตราย ซึ่งอ้างว่าเป็นแอป 'Digital Pension' เพื่อรับเงินบำนาญในรูปแบบดิจิทัล จากกรมบัญชีกลาง
"โดยมิจฉาชีพมีข้อมูลส่วนบุคคลที่น่าเชื่อถือ ทำให้เหยื่อตายใจ"
ข้อควรระวัง
Apps
Digital Pension
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
TB-CERT


วันที่เผยแพร่ 7 พฤศจิกายน 2566
TLP: CLEAR
2/2
เจาะลึกขั้นตอนการหลอกลวง
1 ส่งลิงก์ทางอีเมล หรือ LINE เพื่อติดตั้งแอป TestFlight ลงบนโทรศัพท์มือถือ ซึ่งเป็นแอปจริงบน Official Store
2 หลอกให้กรอก code ตามที่บอก หรือส่งลิงก์ ให้ติดตั้งแอปปลอมที่มีลักษณะหน้าตาเหมือนแอปจริงที่อยู่บน TestFlight
3 เมื่อหลอกเหยื่อให้ติดตั้งแอปปลอมแล้ว ก็ทำการโอนเงินออกจากบัญชี
ประชาชนทั่วไปที่ไม่เกี่ยวข้องกับการพัฒนาและทดสอบแอป
ไม่ควรติดตั้งแอป TestFlight
STEP 1
TestFlight
STEP 2
Digital Pension
STEP 3
ท่องไว้ให้ขึ้นใจ
ไม่ทำตามคำบอกจากใครทางโทรศัพท์ ที่ให้มีการติดตั้งหรืออัปเดตแอปต่าง ๆ
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
TB-CERT


วันที่เผยแพร่ 8 พฤศจิกายน 2566
TLP: CLEAR
มุกใหม่ระบาด
อย่าหลงกด เด็ดขาด !!!
Step 1
Got TestFlight
Step 2
Join the Beta
Digital Pensions
Terms of Service
What to Test
App Information
TB-CERT ขอย้ำเตือนทุกท่าน
หากต้องการติดตั้งแอปฯ ของหน่วยงานใด ๆ ให้พิมพ์ค้นหาชื่อแอปฯ เองบน Official Store เท่านั้น ห้ามกดผ่านลิงก์หรือทำตามคำบอกของบุคคลทางโทรศัพท์เด็ดขาด
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
TB-CERT

รายนามคณะกรรมการ TB-CERT ปี 2023

ประธานกรรมการ	**ดร. กิตติ โฆษะวิสุทธิ์** Senior Vice President and Chief Information Security Officer ธนาคารกรุงเทพ
รองประธานกรรมการ และกรรมการ ด้านการสื่อสาร	**คุณชัชวัฒน์ อัศวรักวงศ์** Managing Director and Chief Information Security Officer ธนาคารกสิกรไทย
กรรมการ ด้านการสื่อสาร	**คุณเชิดศักดิ์ นานา** Senior Vice President, IT Security ธนาคารกรุงไทย
กรรมการ ด้านเทคนิค	**คุณภคพงศ์ จุลวงศาศิลป์** Head of Cyber Security Department ธนาคารกรุงศรีอยุธยา
กรรมการ ด้านเทคนิค	**คุณอดิศักดิ์ วงศ์จันลา** Cyber Security Advisory Specialist, Digital Technology Security ธนาคารไทยพาณิชย์
กรรมการ ด้านวิชาการ	**คุณประกลกฤษ แสงชูวงศ์** Team Head of Information, Security Detection and Response ธนาคารทหารไทยธนชาต
กรรมการ ด้านวิชาการ	**คุณกริช กาดนอก** Head of IT Security ธนาคารเกียรตินาคินภัทร
กรรมการ ด้านการสร้างความร่วมมือ	**คุณวชิราวัชร์ มหาทัพกฤษ** Executive Vice President, Cyber Security ธนาคารออมสิน
กรรมการ ด้านการสร้างความร่วมมือ	**คุณสมภพ สุรัตนกวีกุล** Director, IT Security Office, Information Technology Department ธนาคารแห่งประเทศไทย
กรรมการ และหัวหน้าคณะเลขานุการ	**คุณยศ กิมสวัสดิ์** Head of Payment System Office สมาคมธนาคารไทย
คณะเลขานุการ	**คุณปรมินทร์ ช่วงมณี** CERT Manager
	คุณธาวินี วงศ์วิศว์ CERT Relations Manager

หน่วยงานสมาชิก TB-CERT ปี 2023

ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร Bank of Agriculture and Agricultural Cooperatives	ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน) Kiatnakin Phatra Bank Plc.
บริษัท บริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน) Bangkok Commercial Asset Management Public Company Limited	ธนาคารกรุงไทย จำกัด (มหาชน) Krung Thai Bank Public Company Limited
ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) Bank of Ayudhya Public Company Limited	ธนาคารแลนด์ แอนด์ เฮ้าส์ จำกัด (มหาชน) Land and Houses Bank Public Company Limited
ธนาคารกรุงเทพ จำกัด (มหาชน) Bangkok Bank Public Company Limited	ธนาคารมิซูโฮ จำกัด สาขากรุงเทพฯ Mizuho Bank Bangkok Branch
ธนาคารแห่งประเทศไทย Bank of Thailand	บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด National Credit Bureau Company Limited
ธนาคารแห่งประเทศจีน (ไทย) จำกัด Bank of China	บริษัท เนชั่นแนลดิจิทัลไอดี จำกัด National Digital ID Company Limited
ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน) CIMB Thai Bank Public Company Limited	บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด National ITMX Company Limited
ธนาคารซิตี้แบงก์ Citibank N.A.	บริษัท ศูนย์ประมวลผล จำกัด Processing Center Company Limited
สถาบันคุ้มครองเงินฝาก Deposit Protection Agency (DPA)	ธนาคาร ไทยพาณิชย์ จำกัด (มหาชน) The Siam Commercial Bank Public Company Limited
ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย Export-Import Bank of Thailand	ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด (มหาชน) Standard Chartered Bank (Thai) Public Company Limited
ธนาคารอาคารสงเคราะห์ Government Housing Bank	ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย Small And Medium Enterprise Development Bank of Thailand
ธนาคารออมสิน Government Savings Bank	ธนาคารไทยเครดิต จำกัด (มหาชน) The Thai Credit Bank Public Company Limited
ธนาคารอิสลามแห่งประเทศไทย Islamic Bank of Thailand	ธนาคารทิสโก้ จำกัด (มหาชน) TISCO Bank Public Company Limited
ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน) Industrial and Commercial Bank of China (Thai) Public Company Limited (ICBC Thai)	ธนาคารทหารไทยธนชาต จำกัด (มหาชน) TMB Thanachart Bank Public Company Limited
ธนาคารกสิกรไทย จำกัด (มหาชน) KASIKORNBANK Public Company Limited	ธนาคารยูโอบี จำกัด (มหาชน) United Overseas Bank (Thai) Public Company Limited

TB-CERT

Thailand Banking Sector CERT

The Thai Bankers' Association

4th Fl., 5/13 Moo 3,
Chaengwattana Rd., Pakkret, Nonthaburi 11120
Phone : 025587500 Website : www.tba.or.th
Youtube : TB-CERT The Thai Bankers' Association
Facebook : TB-CERT