ANNUAL REPORT 2022

Your cyber behavior indicates your cyber risk.

TB-CERT
Thailand Banking Sector CERT

TB-CERT

Thailand Banking Sector CERT

รายงานประจำปี
Annual Report 2022

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
Thailand Banking Sector CERT: TB-CERT

จัดทำโดย

ชัชวัฒน์ อัศวรักวงศ์
ธาวินี วงศ์วิศว์
ปรมินทร์ ช่วงมณี
ชญานิน แก้วหาญ

ที่ปรึกษา

กิตติ โฆษะวิสุทธิ์

บรรณาธิการ

ธาวินี วงศ์วิศว์

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

เผยแพร่เมื่อ

เมษายน 2023
TLP:CLEAR

TB-CERT

Thailand Banking Sector CERT

รายงานประจำปี TB-CERT 2022

Content

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
พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เมื่อหลายปีที่ผ่านมา ผมได้รู้จักและชื่นชม TB-CERT มาก่อน โดยเฉพาะการแลกเปลี่ยนความรู้และข้อมูลกับหน่วยงานต่าง ๆ เราจะได้รู้กว้างขึ้นเพราะบางครั้งการที่เราอยู่ในที่แคบของเรา อาจจะมองข้ามสิ่งดี ๆ ไปก็ได้ พอผมได้มาทำงานที่ สกมช. ผมได้รู้จัก TB-CERT มากขึ้น การคุยแลกเปลี่ยนความรู้กันกับ TB-CERT ทำให้ผมเห็นมุมมองในอีกมุมที่มากขึ้นและได้เรียนรู้สิ่งใหม่จากการแลกเปลี่ยนความรู้ประสบการณ์กัน ผมเห็นว่า TB-CERT ทำงานร่วมกันแบบเพื่อนและมีจุดประสงค์เพื่อให้เกิดประโยชน์ในองค์รวมร่วมกันมากกว่าจะทำงานคนเดียว TB-CERT เป็นแบบอย่างให้กับอีกหลาย ๆ หน่วยงานที่จะต้องจัดตั้ง Sectoral CERT หรือที่อื่น ๆ ให้เข้าใจการทำงานข้ามหน่วยงานแบบเข้าอกเข้าใจอีกฝ่าย การรับมือกับการโจมตีทางไซเบอร์นั้นจำเป็นต้องร่วมด้วยช่วยกันป้องกันภัยที่แฝงมากับทางโลกออนไลน์ที่ทุกวันนี้มีเพิ่มมากขึ้นอย่างเห็นได้ชัด การที่ TB-CERT ได้มีส่วนช่วยผลักดันทำให้เกิดการร่วมกลุ่มผู้เชี่ยวชาญด้านไซเบอร์จากหลากหลายอุตสาหกรรม ไม่ว่าจะเป็น อุตสาหกรรมการเงิน พลังงาน หน่วยงานของรัฐ จะช่วยให้ประเทศสามารถรับมือกับผู้ร้ายได้อย่างมีประสิทธิภาพ เพราะเราแชร์ข้อมูลทางเทคนิคที่มีเฉพาะในอุตสาหกรรมที่บางครั้งอาจจะมีบางจุดเล็ก ๆ น้อย ๆ ที่มีความแตกต่างกัน ก็ทำให้เพื่อน ๆ ได้ความรู้ในส่วนที่ตนเองไม่มีไปด้วย

ผมติดตามอ่าน Annual Report ประจำปีของ TB-CERT ซึ่งในแต่ละปีก็ให้ความรู้เยอะมาก ไม่ว่าจะเป็นกิจกรรมการให้ความรู้ด้านไซเบอร์ การจัดทำแนวปฏิบัติกลางร่วมกันในสมาชิก ผมชื่นชมกับผลงานของ TB-CERT ที่ต้องยอมรับว่าคนน้อยแต่สามารถสร้างสรรค์ผลงานให้เป็นที่ประจักษ์ได้อย่างโดดเด่น ในปัจจุบันนี้หากให้ผมถามคนในวงการด้านนี้ ไม่มีใครไม่รู้จัก TB-CERT ซึ่งผมขอแสดงความยินดีกับ TB-CERT มาก ๆ ที่เป็นส่วนหนึ่งของการสร้างสรรค์ผลงานและประโยชน์ให้กับประเทศและประชาชนโดยเฉพาะกลุ่มอุตสาหกรรมการเงินที่รวมตัวกันได้อย่างเหนียวแน่นและช่วยกันพัฒนาบุคลากรด้านไซเบอร์ให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างยอดเยี่ยม

คำนิยม โดย
ดร. เศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการธนาคารแห่งประเทศไทย

ในโลกการเงินและนวัตกรรมที่กำลังก้าวสู่ยุคดิจิทัล มีการนำเทคโนโลยีและข้อมูลมาใช้กับการพัฒนาบริการและนวัตกรรมทางการเงินใหม่ ๆ รวมทั้งการเชื่อมโยงกับระบบภายนอกมากขึ้น เพื่อตอบโจทย์ทางด้านธุรกิจและผู้ใช้บริการได้ดียิ่งขึ้น และลดช่องว่างในการเข้าถึงบริการทางการเงินของประชาชน

การเปลี่ยนผ่านไปสู่โลกการเงินดิจิทัล มาพร้อมกับความเสี่ยงหลายด้านที่เพิ่มขึ้น โดยเฉพาะความเสี่ยงด้านไซเบอร์ ซึ่งเป็นความเสี่ยงสำคัญที่ภาคการเงินต้องเตรียมความพร้อมรับมือให้เท่าทัน โดยในช่วงที่ผ่านมาแนวโน้มภัยคุกคามไซเบอร์ทั้งในประเทศไทยและทั่วโลกได้ปรับเปลี่ยนอย่างรวดเร็ว ทั้งรูปแบบวิธีการและความซับซ้อน ไม่ว่าจะเป็นภัยคุกคามที่มุ่งเป้าโจมตีสถาบันการเงินโดยตรง โจมตีผู้ให้บริการภายนอก (3rd Party) ของสถาบันการเงิน หรือโจมตีผู้ใช้บริการทางการเงินผ่านการทุจริตหลอกลวงออนไลน์รูปแบบต่าง ๆ

ที่ผ่านมา TB-CERT มีบทบาทสำคัญอย่างยิ่งในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ โดยบูรณาการความร่วมมือกับหน่วยงานต่าง ๆ ทั้งหน่วยงานควบคุมหรือกำกับดูแล (Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และหน่วยงานภาครัฐที่เกี่ยวข้อง รวมทั้งช่วยให้ความรู้ในการใช้บริการทางการเงินให้กับประชาชน เพื่อเสริมสร้างภูมิคุ้มกันให้ใช้บริการการเงินดิจิทัลได้อย่างมั่นใจและปลอดภัย บทบาทดังกล่าวยังคงต้องดำเนินต่อไปอย่างเข้มข้นมากขึ้นตามภัยความเสี่ยงที่เปลี่ยนแปลง

ในนามของธนาคารแห่งประเทศไทย ผมขอขอบคุณและแสดงความชื่นชม คณะทำงาน TB-CERT และผู้เกี่ยวข้องทุกท่าน ที่ร่วมแรงร่วมใจกันสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับภาคการเงินตลอดระยะเวลาที่ผ่านมา รวมทั้งขอเป็นกำลังใจให้ทุกท่าน ที่มุ่งมั่น ทุ่มเท ช่วยกันสร้างความเข้มแข็งให้องค์กรและประเทศ เพื่อการเติบโตที่ยั่งยืนของภาคการเงินไทยต่อไป

คำนิยม โดย
คุณผยง ศรีวณิช
กรรมการผู้จัดการใหญ่ ธนาคารกรุงไทย และประธานสมาคมธนาคารไทย

ในปัจจุบัน ด้วยความก้าวหน้าทางเทคโนโลยีได้ส่งผลให้เราใช้ชีวิตได้อย่างสะดวกสบายขึ้น จากการทำธุรกรรมออนไลน์ ลดการใช้เงินสด การดำเนินการออนไลน์ต่าง ๆ ซึ่งประเทศไทยได้มีการปรับตัวเข้าสู่ยุคเศรษฐกิจดิจิทัลดังจะเห็นได้จากจำนวนผู้ใช้บริการทางการเงินผ่านทางช่องทางดิจิทัลทั้งภาคธุรกิจและภาคประชาชน ซึ่งช่วยให้เกิดความสะดวกสบายและลดต้นทุนในการทำธุรกรรม รวมถึงเกิดผู้ให้บริการทางการเงินดิจิทัลใหม่ ๆ อันจะเป็นประโยชน์ต่อผู้ใช้บริการที่มีทางเลือกหลากหลายมากขึ้น โดยธนาคารเองก็มีการปรับตัวอยู่เสมอในการนำเทคโนโลยีใหม่ ๆ มาอำนวยความสะดวกด้านการเงินดิจิทัลให้กับประชาชนอย่างแพร่หลาย ทำให้ประชาชนสามารถเข้าถึงบริการต่าง ๆ ของธนาคาร รวมถึงสวัสดิการและสิทธิประโยชน์ได้ง่ายขึ้น ขณะเดียวกัน ผู้ไม่หวังดีก็อาศัยความก้าวหน้าทางเทคโนโลยีในการก่ออาชญากรรมทางไซเบอร์ ที่มีปริมาณเพิ่มขึ้นอย่างรวดเร็วและซับซ้อนจากประโยชน์ของความก้าวหน้าของเทคโนโลยีและการสื่อสารด้วยเช่นกัน ในปีที่ผ่านมาพบเหตุการณ์หลอกลวงประชาชนให้หลงเชื่อและโอนเงินให้กับมิจฉาชีพและส่งต่อให้กับกลุ่มเครือข่าย ก่อให้เกิดความเสียหายแก่ประชาชนและลูกค้าธนาคารเป็นวงกว้างและทวีความรุนแรง ซึ่งทุกภาคส่วนรวมทั้งประชาชนทุกคนต้องเตรียมความพร้อม เพื่อป้องกันและรับมือกับภัยคุกคามทางเทคโนโลยีหรือความเสี่ยงในยุคเศรษฐกิจดิจิทัล

ตลอดระยะเวลากว่า 6 ปีที่ผ่านมา ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector Computer Emergency Response Team) หรือ TB-CERT ซึ่งถูกจัดตั้งขึ้นโดยความร่วมมือระหว่างธนาคาร เพื่อสร้างเครือข่ายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของธนาคาร เป็นศูนย์กลางในการแลกเปลี่ยน วิเคราะห์ข้อมูล และเป็นที่ปรึกษาที่เชื่อถือได้ให้กับธนาคารสมาชิกและผู้ใช้บริการจากธนาคาร รวมถึงสนับสนุนในการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ และการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับภาคประชาชน ในปีที่ผ่านมา TB-CERT ยังคงดำเนินบทบาทสำคัญในการทำงานเชิงรุก สร้างความร่วมมือกับธนาคารสมาชิกและหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชน ไม่ว่าจะเป็นการแชร์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างหน่วยงานสมาชิก การสร้างความร่วมมือร่วมกับหน่วยงานกำกับดูแลภาคการเงิน ภาคโทรคมนาคม ไปจนถึงหน่วยงานสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ในการร่วมกันผนึกกำลังป้องกันและแก้ไขปัญหาด้านการหลอกลวงโดยอาศัย

เทคโนโลยี (Digital Fraud) และอาชญากรรมทางไซเบอร์ (Cyber Crime) โดยยกระดับความร่วมมือและกระบวนการดำเนินการต่าง ๆ เพื่อป้องกันและยับยั้งเหตุให้ได้ทันท่วงที ทั้งในแง่ของกระบวนการดำเนินงานของธนาคารให้รัดกุมและสามารถตรวจสอบติดตามเพื่อป้องกันการเกิดเหตุ รวมทั้งความร่วมมือกับหน่วยงานกำกับดูแลที่เกี่ยวข้องเพื่อปรับปรุงกฎเกณฑ์ให้รัดกุมและตรวจสอบไม่ให้มิจฉาชีพอาศัยช่องทางเข้ามาก่ออาชญากรรมทางเทคโนโลยี ความร่วมมือกับหน่วยงานสืบสวนสอบสอนเพื่อให้ประชาชนสามารถเข้าถึงการแจ้งเบาะแสและร้องเรียนได้อย่างสะดวกรวดเร็วยิ่งขึ้นผ่านระบบออนไลน์ ไม่เพียงเท่านั้น ยังดำเนินสร้างความตระหนักรู้ให้ประชาชนอย่างต่อเนื่องผ่านสื่อต่าง ๆ ของหน่วยงาน เพื่อให้ประชาชนรู้เท่าทันและไม่ตกเป็นเหยื่อของภัยดังกล่าว

นอกจากการสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับภาคประชาชนแล้ว ภาคธนาคารมีการพัฒนาระบบ Mobile Banking ของธนาคารให้มีความปลอดภัยมากยิ่งขึ้นด้วยการเพิ่มส่วนของการยืนยันตัวตนแบบ Multifactor Authentication ยกตัวอย่างเช่นนอกจากผู้ใช้บริการ Mobile Banking จะต้องใส่รหัส 6 ตัวแล้วยังให้มีการใช้ Biometrics เป็นการพิสูจน์ยืนยันตัวตนอีกชั้นหนึ่งในการทำธุรกรรมด้วย นอกจากนี้ ยังได้รับการสนับสนุนจากภาครัฐที่มีการออกพระราชกำหนด (พ.ร.ก.) มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งจะกำหนดให้ธนาคารสามารถแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีต้องสงสัยและระงับธุรกรรมทางอิเล็กทรอนิกส์ที่อาจเป็นการทุจริตหรือบัญชีม้าโดยไม่ขัดกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อช่วยให้การระงับการทำธุรกรรมทางอิเล็กทรอนิกส์ข้ามธนาคารนั้นเป็นไปได้อย่างรวดเร็ว เพื่อลดความเสียหายที่จะเกิดขึ้นกับประชาชน และในภาคการธนาคารเอง สมาคมธนาคารไทยได้มีการหารือร่วมกับส่วนงานที่เกี่ยวข้องในการจัดตั้ง “ศูนย์ตรวจเช็กธุรกรรมที่มีความเสี่ยงทุจริต” หรือ Central Fraud Registry ที่จะเป็นระบบกลางในการแลกเปลี่ยนข้อมูลและ เชื่อมโยงข้อมูลการทุจริตต่าง ๆ ให้สามารถตรวจสอบข้อมูลต้องสงสัยระหว่างธนาคารด้วยกันได้อย่างรวดเร็วมากยิ่งขึ้น นอกจากนี้ทางสมาคมธนาคารไทยได้มีการประสานความร่วมมือไปยังผู้ให้บริการโทรศัพท์เคลื่อนที่ผ่านทาง สำนักงาน กสทช. เพื่อประสานความร่วมมือในการแชร์ข้อมูลอาทิเช่น การตรวจสอบจำนวนซิมการ์ดที่บัญชีม้าเหล่านี้ถือครองอยู่ เพื่อนำมาร่วมในกระบวนการตรวจสอบและป้องกันด้วย และในอนาคตก็จะนำเทคโนโลยี AI มาช่วยในการเฝ้าระวังตรวจจับพฤติกรรมต้องสัยสัยได้อย่างแม่นยำยิ่งขึ้นด้วย

การปรับตัวให้ทันต่อการเปลี่ยนแปลงและเท่าทันต่อเทคโนโลยีรวมถึงภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์เป็นสิ่งที่สถาบันการเงินให้ความสำคัญและดำเนินการอย่างต่อเนื่องเสมอมา ไม่ว่าจะเป็นการพัฒนาระบบป้องกันที่รัดกุมเข้มแข็ง การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที การพัฒนาบุคลากรให้ทันต่อเทคโนโลยี การสร้างความตระหนักรู้ให้กับประชาชน รวมถึงการสร้างความร่วมมือของทุกภาคส่วนที่เกี่ยวข้องเพื่อป้องกันความเสียหายต่อข้อมูลส่วนบุคคลและสินทรัพย์ของประชาชน รวมทั้งต่อสถาบันการเงินซึ่งเป็นโครงสร้างพื้นฐานที่สำคัญของประเทศ อย่างไรก็ดีการพิจารณาปรับปรุงกฎหมายหรือกฎระเบียบต่าง ๆ เพื่อให้การรับมือต่อเหตุที่เกิดขึ้นเป็นไปได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น เป็นสิ่งจำเป็นที่ต้องอาศัยความร่วมมือทั้งภาครัฐและเอกชนที่เกี่ยวข้องมาร่วมกันคิดวิเคราะห์และหาทางออกร่วมกัน โดยที่สมาคมธนาคารไทยมีการเตรียมความพร้อมร่วมกับธนาคารสมาชิกและหน่วยงานที่เกี่ยวข้องเพื่อผลักดันให้เกิดระบบติดตามความเสี่ยงในการทำธุรกรรมซึ่งต้องอาศัยความร่วมมือทางด้านเทคโนโลยีในการเตรียมระบบรวมถึงเร่งรัดให้กฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีมีผลบังคับใช้ซึ่งจะช่วยหยุดยั้งหรือระงับเหตุภัยการหลอกหลวงได้โดยอาศัยเทคโนโลยีให้เกิดความรวดเร็วยิ่งขึ้น ทั้งนี้เพื่อประโยชน์แก่พี่น้องประชาชนและประเทศชาติของเรา

สารจากกรรมการ

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

“ การทำงานร่วมกันอย่างใกล้ชิดของสมาชิก TB-CERT ในปีที่ผ่านมา ตอกย้ำว่าการรับมือต่อภัยคุกคามทางด้านไซเบอร์ และภัยจาก Digital Fraud ต่าง ๆ นั้น เราต้องร่วมมือเป็นหนึ่งเดียวกัน การแชร์และการแลกเปลี่ยนเทคนิคกันจะทำให้พวกเราได้เรียนรู้ และสามารถก้าวข้ามปัญหาไปด้วยกัน "Together we can" ”

คุณสมภพ สุรัตนกวีกุล
รองประธานกรรมการ TB-CERT
Director, IT Security Office, Information Technology Department ธนาคารแห่งประเทศไทย

“ ปีนี้เป็นปีที่ทุกคนคาดหวังว่า เศรษฐกิจไทยจะดีขึ้นหลังเหตุโควิด แต่สำหรับสถานการณ์ทางไซเบอร์ในไทยแล้ว ยังคงมีแนวโน้มที่รุนแรงขึ้นทั้งระดับองค์กรและระดับประชาชน คนร้ายยังคงพัฒนากลยุทธ์ของตนอย่างต่อเนื่อง ขณะที่แต่ละองค์กรต้องพัฒนามาตรการรักษาความปลอดภัยไปให้ทัน ความร่วมมือในกลุ่มธนาคารมีความสำคัญมาก เราต้องทำงานร่วมกันเพื่อสร้างระบบการเงินที่ปลอดภัยและยืดหยุ่น ปกป้ององค์การและลูกค้าของเราจากอันตรายที่อาจเกิดขึ้น เราต้องระมัดระวังในการต่อสู้กับอาชญากรรมทางไซเบอร์และมุ่งมั่นที่จะปกป้องอุตสาหกรรมการเงินของเราโดยรวม ”

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

" การมุ่งมั่นที่จะเพิ่มภูมิคุ้มกันด้านความมั่นคงปลอดภัยให้ดีขึ้นอย่างต่อเนื่องนั้นก็เพื่อที่จะสร้างความเป็นอยู่ที่ดีขึ้นของสังคมในยุคดิจิทัล แต่เมื่อมีสังคมและความเป็นอยู่ที่ดีแล้วก็อย่าละเลยการคงอยู่ของมัน "

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

" การวิเคราะห์ข้อมูลจากข่าวการโจมตีทางไซเบอร์ไม่ว่าจะเป็นในระดับ strategic หรือ technical จะทำให้เราเข้าใจรูปแบบการโจมตี เทคนิควิธีการ ป้องกันที่มิจฉาชีพใช้ในการโจมตี แนวทางป้องกันภัย และหากมีข้อมูลมากเพียงพอและแลกเปลี่ยนข้อมูลกับหน่วยงานสมาชิกจะช่วยให้ภาคการธนาคารสามารถรับมือกับเหล่ามิจฉาชีพได้อย่างมีประสิทธิภาพ ลดการสูญเสียในวงกว้าง และเพิ่มการป้องกันได้ถูกทาง "

คุณวชิราวัชร์ มหาทัพกฤษ
กรรมการ TB-CERT
Inspector general, Chief Information Security Officer, ธนาคารออมสิน

" ในห้วงหลายปีที่ผ่านมา ทุกธนาคารให้ความสำคัญยิ่งต่อการแบ่งปันข้อมูลด้านความปลอดภัยไซเบอร์ (Cybersecurity) ซึ่งกันและกันในภาคการธนาคารและในช่วง 1-2 ปีนี้ การแบ่งปันก็พัฒนาไปสู่การแลกเปลี่ยนและให้ความร่วมมือระหว่างภาคอุตสาหกรรมที่ต่างกัน เช่น ภาคการประกันภัย ภาคการลงทุนในตลาดหุ้น และภาคการให้บริการโทรคมมาคม เป็นต้น ซึ่งเป็นนิมิตหมายอันดีที่จะทำให้ทุกภาคอุตสาหกรรมมีความเข้มแข็ง อันจะส่งผลดีต่อภาพรวมในการรักษาปลอดภัยไซเบอร์ของประเทศไทย

แต่ในปัจจุบัน มิจฉาชีพมุ่งโจมตีไปยังอุปกรณ์ส่วนบุคคล (End point) ของประชาชนทั่วไป (Cybercrime) โดยเฉพาะโทรศัพท์แบบสมาร์ทโฟน เป้าหมายหลักคือ การโอนเงิน/ดูดเงินจากแอป Mobile banking รวมถึงการลักลอบขโมยข้อมูลส่วนบุคคลจากอุปกรณ์ฯ ทำให้ธนาคารต้องพัฒนาแอป Mobile banking ให้สามารถป้องกันกลโกงในรูปแบบต่าง ๆ แต่ก็ถือว่า ยังเป็นการแก้ไขปัญหาที่ปลายเหตุ เพราะมิจฉาชีพก็มีการปรับเปลี่ยนวิธีการไปเรื่อย ๆ เพื่อหลบเลี่ยงการตรวจจับและป้องกันที่มีอยู่

การแก้ไขปัญหาที่ต้นเหตุ จึงควรเป็นสิ่งที่สำคัญสูงสุด หลายท่านคงมีคำถามว่า ทำอย่างไร? จริง ๆ แล้วเป็นสิ่งที่เราทำมาตลอดในองค์กร นั่นคือการสร้างความตระหนักรู้ (Awareness) แก่เจ้าหน้าที่ของธนาคาร ถึงตรงนี้ทุกท่านคงคิดว่าแค่หมื่นคนยังยากเลย แล้วทั้งประเทศจะทำได้อย่างไร ใช่ครับ แม้การสร้างความตระหนักรู้แก่ลูกค้าและประชาชนทั่วประเทศจะเป็นการยาก หากแต่ถ้าทุกองค์กรในประเทศให้ความสำคัญต่อการสร้างภูมิคุ้มกันทางไซเบอร์ให้กับประชาชน ให้การสื่อสารไปยังทุกช่องทาง โซเชียลมีเดีย ทีวี วิทยุ วารสาร ฯลฯ รวมทั้งสถาบันการศึกษาในทุกระดับอันเป็นองค์กรที่สร้างพื้นฐานความรู้ ทำการสอดแทรกหรือมีวิชาที่สร้างความตระหนักรู้ด้านมิจฉาชีพทางไซเบอร์ เข้าไปในชั่วโมงเรียนหรือกิจกรรมก็จะทำให้ภูมิคุ้มกันทางไซเบอร์เกิดขึ้นตั้งแต่ยังเยาว์และมีโอกาสถ่ายทอดไปยังผู้ใหญ่ซึ่งเป็นผู้ปกครองอีกด้วย

การสร้างภูมิคุ้มกันทางไซเบอร์ที่กล่าวมา คงมิใช่ภาคการธนาคารแค่อุตสาหกรรมเดียวที่จะทำได้สำเร็จ แต่ต้องเป็น "วาระแห่งชาติ" ที่ทุกภาคส่วนทุกอุตสาหกรรม ทุกภาครัฐ ทุกสถาบันการศึกษา และทุกสื่อสารมวลชน ให้ความร่วมมือกันในการสร้างภูมิคุ้มกันทางไซเบอร์ให้กับประชาชน "

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

“ ภารกิจหลักที่มีความสำคัญมาเป็นอันดับ 1 ในช่วงเวลานี้ คงไม่พ้นเรื่องของการรับมือกับภัยจากมิจฉาชีพที่ทำการหลอกลวงประชาชนในรูปแบบของการหลอกให้ลงแอปพลิเคชันปลอมที่สามารถควบคุมเครื่องของลูกค้าและสร้างความสูญเสียดังที่เป็นข่าว ซึ่งในเรื่องนี้ทาง TB-CERT ได้มีการประสานงานร่วมกันทั้งในภาคธนาคาร ธนาคารแห่งประเทศไทย กระทรวง DE และหน่วยงานอื่น ๆ เพื่อร่วมกันวางแผนในการรับมือและป้องกันในทุกมิติ ซึ่งที่ผ่านมาก็ได้ผลดีเป็นที่น่าพอใจ แต่มิจฉาชีพเองก็มีการพัฒนาวิธีการหลอกลวงใหม่ ๆ อยู่เสมอ ด้วยเหตุนี้ความร่วมมือของภาคส่วนต่าง ๆ ที่นอกเหนือจากที่ได้กล่าวมาจึงมีความจำเป็นอย่างยิ่ง อีกทั้งการเร่งให้ความรู้แก่ภาคประชาชน ซึ่งเป็นผู้ได้รับผลกระทบโดยตรง ได้รับรู้ข่าวสารให้เกิดความรู้ความเข้าใจ และไม่ตกเป็นเหยื่อเหมือนในที่ผ่านมา TB-CERT จะยังคงมุ่งมั่นพัฒนาและสนันสนุนแนวทางของสมาคมธนาคารไทยเพื่อประโยชน์แก่ประชาชนและประเทศชาติต่อไป ”

คุณพาวิต ศักดิ์สูง
กรรมการ TB-CERT
Head of Digital Technology Security, ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

“ ในช่วงเวลาที่ผ่านมาข่าวสารด้านโจรกรรมไซเบอร์ ผ่านระบบ Mobile Banking ได้ปรากฏในสื่อออนไลน์และสื่อทั่วไปอย่างต่อเนื่อง การโจรกรรมนี้เป็นการใช้วิธีหลอกลวงประชาชนผ่านสื่อสังคมออนไลน์ให้ติดตั้งแอปพลิเคชันโจรกรรมบนเครื่องมือถือเหยื่อเพื่อเข้าควบคุมเครื่องมือถือในการทำธุรกรรม

TB-CERT ได้ติดตามข่าวสารและประสานงานหน่วยงานที่เกี่ยวข้องเพื่อเผยแพร่ข้อมูลข่าวสารและประสานงานเรื่องการยกระดับมาตรการป้องกันภัยทางไซเบอร์อย่างต่อเนื่องโดยถือเป็นภารกิจที่สำคัญในปีที่ผ่านมา ปี 2566 และปีถัด ๆ ไป ”

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

" สถานการณ์โควิด-19 ผ่านพ้นไป แต่สถานการณ์ภัยคุกคามไซเบอร์ไม่ได้ลดหย่อนลงเลย เหตุการณ์ต่าง ๆ เช่น แอปดูดเงิน หรือการหลอกลวงต่าง ๆ สร้างความเสียหายไม่เพียงแต่อุตสาหกรรมธนาคาร แต่ปัจจุบันเกิดเป็นผลกระทบระดับชาติไปแล้ว ซึ่งมีผลต่อเศรษฐกิจของประเทศ เนื่องจากมีผู้เสียหายจำนวนมาก ซึ่งการช่วยป้องกันอย่างหนึ่งที่ภาคการธนาคารจะร่วมมือกันเพื่อลดผลกระทบ คือ การแบ่งปันความรู้ โดยมีข้อมูลเท่าที่จำเป็นในการป้องกันภัยคุกคามที่เกิดขึ้น ตลอดจนแนวทางใหม่ ๆ ในด้านการจัดการรักษาความปลอดภัยไซเบอร์ เพื่อยกระดับขีดความสามารถการต่อยอดให้ภาคการธนาคารมีความเข้มแข็งต่อไป "

คุณยศ กิมสวัสดิ์
กรรมการ TB-CERT
ประธานสำนักงานระบบการชำระเงิน สมาคมธนาคารไทย

" การรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ในยุคดิจิทัลที่มีความผสมผสานกันระหว่าง Digital Fraud กับ Cybercrime มีความท้าทายหลายอย่าง แต่สิ่งหนึ่งที่จะช่วยให้การรับมือกับเหตุการณ์เหล่านี้ได้อย่างมีประสิทธิภาพอย่างแท้จริง คือการสร้างความร่วมมือและการทำงานร่วมกันทั้งภายในและภายนอกองค์กร "

บทความประจำปี

หยุดภัยจาก Social Engineering ด้วยสติและความร่วมมือจากหน่วยงานต่างๆ

หยุดภัยจาก Social Engineering ด้วยสติและความร่วมมือจากหน่วยงานต่าง ๆ

โดย คุณชัชวัฒน์ อัศวรักวงศ์
ประธานกรรมการ TB-CERT

ในปี 2022 ที่ผ่านมา เรายังคงได้ยินข่าวการโจมตีทางไซเบอร์ที่สำคัญ ทั้งในและต่างประเทศอย่างต่อเนื่อง โดยรูปแบบของภัยคุกคามทางไซเบอร์หลัก ๆ ที่เกิดขึ้นในประเทศไทย ยังคงเป็นเรื่องของการโจมตีโดยมัลแวร์ (Malware) โดยเฉพาะแรนซัมแวร์ (Ransomware) หรือที่รู้จักกันว่ามัลแวร์เรียกค่าไถ่ การละเมิดข้อมูลและขู่กรรโชก (Data Breach & Extortion) การโจมตีประเภท DoS (Denial of Services) DDoS (Distributed Denial of Services) และรวมถึงการใช้ bot ในการโจมตีเพื่อทำให้การให้การบริการของระบบเป้าหมายหยุดชะงัก ซึ่งภัยดังกล่าวเกิดขึ้นกับหลายอุตสาหกรรม ทั้งภาครัฐ และเอกชน ก่อให้เกิดความเสียหายต่อองค์กร ทั้งด้านสถานะการเงิน การหยุดชะงักในการดำเนินกิจการ การให้บริการ การเสียชื่อเสียง และลดทอนความน่าเชื่อถือขององค์กรต่อผู้บริโภคและประชาชน การพัฒนาความสามารถในการบริหารจัดการและรับมือต่อภัยคุกคามทางไซเบอร์ ทั้งเรื่องการจัดการเทคโนโลยี การเตรียมความพร้อมเรื่องกระบวนการและการสร้างทักษะที่จำเป็นให้กับบุคลากรรวมถึงการสร้างวัฒนธรรมทางไซเบอร์ให้กับองค์กรจึงเป็นสิ่งสำคัญที่องค์กรและหน่วยงานต่าง ๆ ต้องดำเนินการอย่างต่อเนื่อง

นอกจากภัยคุกคามทางไซเบอร์ที่ยังคงเกิดขึ้นอย่างต่อเนื่องดังกล่าวแล้ว ในปีที่ผ่านมายังมีเหตุการณ์ด้าน Digital Fraud ที่มิจฉาชีพใช้วิธีการ Social Engineering ในการหลอกลวงประชาชนเป็นจำนวนมาก เช่น จากแก๊ง Call Center SMS ปลอม Line Account ปลอม หลอกให้ลงทุน ซื้อของออนไลน์ และรวมถึงการหลอกให้ประชาชนติดตั้งแอปฯ ดูดเงิน ซึ่งสร้างความเสียหายให้กับประชาชนเป็นวงกว้าง ส่งผลกระทบต่อความเชื่อมั่นต่อสถาบันการเงิน และเศรษฐกิจของประเทศ ซึ่งแนวโน้มการก่ออาชญากรรมทางด้านไซเบอร์โดยใช้วิธีการ Social Engineering โจมตีไปที่ประชาชนมีแนวโน้มสูงขึ้น ซึ่งหากหน่วยงานที่เกี่ยวข้องไม่ร่วมมือกันจัดการ ปัญหานี้จะยังคงอยู่และสร้างความเสียหายให้กับประเทศไปอีกยาวนาน

การรับมือและป้องกันภัยจากกลุ่มมิจฉาชีพที่ดีที่สุด เริ่มต้นได้ที่ตัวเราเองเป็นอันดับแรก เมื่อมิจฉาชีพใช้วิธีการ Social Engineering ในการหลอกลวง โดยใช้จุดอ่อนของมนุษย์ซึ่งมนุษย์ถือว่าเป็นจุดอ่อนที่สุดสำหรับการโจมตีทางด้านไซเบอร์ เนื่องจากมนุษย์ทุกคนมีอารมณ์ เช่น มีความโลภ มีความกลัว มีความลุ่มหลง ดังนั้นหากพวกเรามีสติ คอยติดตามข่าวสาร และไม่หลงกลกับความโลภ ความกลัว ความลุ่มหลง หากไม่แน่ใจให้ติดต่อหน่วยงานต้นสังกัดที่ถูกแอบอ้าง และไม่เปิดเผยข้อมูลส่วนตัวโดยเฉพาะรหัสผ่าน ข้อมูลส่วนบุคคลหรือเอกสารสำคัญ ให้กับบุคคลแปลกหน้าโดยเด็ดขาด โอกาสที่เราจะรอดปลอดภัยจากภัยจากมิจฉาชีพก็จะสูงตามไปด้วย

นอกจากนี้ความร่วมมือจากหน่วยงานที่เกี่ยวข้องก็สำคัญมาก การที่เราจะช่วยกันจัดการและป้องกันภัยจากมิจฉาชีพที่ต้นเหตุได้อย่างมีประสิทธิภาพ เช่น การคัดกรองหรือระงับเบอร์โทรศัพท์ ที่แก๊ง Call Center ใช้โทรหลอกประชาชน การลงทะเบียน คัดกรอง และระงับชื่อผู้ส่ง SMS (SMS sender) ได้อย่างรวดเร็ว ก็สามารถช่วยลดโอกาสที่มิจฉาชีพจะใช้ช่องทางเหล่านี้สำหรับติดต่อและหลอกประชาชนได้ การปิดกั้นการเข้าถึงเว็บไซต์ปลอม หรือเว็บไซต์อันตรายอย่างรวดเร็วและทันการณ์ก็เป็นอีกหนึ่งกลไลสำคัญที่จะช่วยตัดตอนกระบวนการที่มิจฉาชีพใช้หลอกหลวงประชาชนได้อย่างมีประสิทธิภาพเช่นกัน

ที่ผ่านมา TB-CERT ตระหนักถึงความเดือนร้อนจากภัยคุกคามด้าน Digital Fraud ในรูปแบบต่าง ๆ ของมิจฉาชีพ โดยเฉพาะกรณีแอปฯ ดูดเงินที่มิจฉาชีพใช้เป็นช่องทางในการแอบโอนเงินของประชาชนผ่าน Mobile Banking ออกไป จึงมีการประสานงานขอความร่วมมือไปยัง Operators และ กสทช. เพื่อร่วมมือกันจัดการต้นน้ำ คือเพิ่มความเข้มข้นในการจัดการชื่อผู้ส่ง SMS ปลอม (Fake SMS sender) การประสานงานไปยังกระทรวงดิจิทัลและเศรษฐกิจเพื่อสังคมเพื่อดำเนินการระงับการเข้าถึงเว็บไซต์ปลอมและเว็บไซต์อันตรายให้ทันท่วงที และมีการหารือกันในกลุ่มสมาชิก TB-CERT เพื่อหาแนวทางการป้องกันและรับมือกับภัยจากกลุ่มมิจฉาชีพแอปฯ ดูดเงินร่วมกันอย่างเข้มข้นมาโดยตลอด และจะยังดำเนินการทำงานร่วมกันกับหน่วยงานต่างๆ อย่างใกล้ชิดเพื่อดำเนินมาตรการป้องกันไม่ให้ประชาชนได้รับความเสียหายจากมิจฉาชีพดังกล่าวต่อไป

หากพวกเราทุกคนร่วมมือกัน เริ่มจากตัวเราในการระมัดระวัง มี “สติ” อยู่เสมอ เท่าทันการใช้งานเทคโนโลยี โดยเฉพาะอย่างยิ่งการใช้งาน Social media ต่างๆ ประกอบกับการทำงานร่วมกันเป็นหนึ่งเดียวของหน่วยงานที่เกี่ยวข้อง เราจะสามารถลดโอกาสที่จะตกเป็นเหยื่อของมิจฉาชีพได้อย่างมีนัยสำคัญ สุดท้ายนี้ขอให้พึงระลึกอยู่เสมอว่า “มีสติก่อนคลิก ใช้สติก่อนแชร์ ไม่แน่ใจให้เช็คต้นทาง”

บทนำ

บทนำ

บทบาทที่สำคัญของTB-CERT ในการทำงานร่วมกันกับหน่วยงานสมาชิกเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ และอีกหลากหลายความท้าทายที่เกิดขึ้นในยุคดิจิทัลที่ภัยทางไซเบอร์เกิดขึ้นเพิ่มมากขึ้นทุก ๆ วัน และทวีความรุนแรงส่งผลกระทบต่อลูกค้าของธนาคารและประชาชนทั้งประเทศเป็นวงกว้าง การรักษาความเชื่อมั่นของประชาชนต่อการใช้บริการของธนาคารในภาพรวมก็เป็นหนึ่งในบทบาทที่ TB-CERT ให้ความสำคัญเช่นกัน ทั้งนี้ TB-CERT ยังเล็งเห็นว่าการดำเนินการเพื่อรับมือต่อเหตุการณ์ที่เกิดขึ้นนั้นไม่สามารถทำได้เพียงแค่ TB-CERT องค์กรเดียว หากแต่เราต้องได้รับความร่วมมือกับหน่วยงานสมาชิกและหน่วยงานภายนอกอื่น ๆ ร่วมด้วยเพื่อช่วยกันรับมือกับความท้าทายที่เกิดขึ้น ดังนั้นในการดำเนินงานตามภารกิจ 5 แกนหลักของ TB-CERT จะช่วยสนับสนุนและส่งเสริมการเตรียมความพร้อมเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ได้ ซึ่งภารกิจ 5 แกนหลักได้แก่ 1. พัฒนาบุคลากรด้าน Cybersecurity ของภาคการธนาคาร เพื่อให้เกิดทักษะความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านกิจกรรมต่าง ๆ ในรูปแบบการสื่อสารทุกช่องทาง ไม่ว่าจะเป็นการอบรมให้ความรู้กับสมาชิกทั้งภาคทฤษฎีและภาคปฏิบัติ หรือ การจัดสัมมนาเชิงวิชาการ การฝึกซ้อมรับมือต่อภัยคุกคามทางไซเบอร์หรือที่เราเรียกว่า Cyber Drill การฝึกซ้อมการตั้งรับและโจมตีทางไซเบอร์หรือที่เราเรียกว่า Cyber Combat เหล่านี้เป็นกิจกรรมการเพิ่มทักษะและความรู้ให้กับสมาชิกให้มีความพร้อมในการรับมือกับเหตุการณ์ทางไซเบอร์อยู่เสมอและทันต่อเหตุการณ์ในปัจจุบัน ซึ่งบุคลากรที่มีความเชี่ยวชาญในด้านนี้ยังคงขาดแคลนทั่วโลก การต่อยอดบุคลากรที่มีอยู่จึงเป็นส่วนที่ TB-CERT เล็งเห็นเป็นสำคัญ 2. กำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคการธนาคาร เพื่อให้มีแนวทางในการปฏิบัติในทิศทางเดียวกันและยกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมของภาคการธนาคาร ทั้งนี้การกำหนดมาตรฐานหรือแนวทางการปฏิบัติ เราได้ทำงานอย่างใกล้ชิดกับหน่วยงานกำกับดูแลซึ่งก็คือธนาคารแห่งประเทศไทยเพื่อที่ว่าการกำหนดมาตรฐานหรือแนวปฏิบัติเหล่านี้สามารถนำมาใช้งานได้จริงในทางปฏิบัติ 3. สร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity สำหรับภาคการธนาคาร ซึ่งเป็นอีกส่วนหนึ่งที่จะยกระดับความมั่นคงปลอดภัยทางไซเบอร์ให้กับประชาชน รู้เท่าทันภัยและสามารถป้องกันตนเองได้ในเบื้องต้น ซึ่งในยุคดิจิทัลนี้ที่เทคโนโลยีล้ำหน้าไปมาก ประชาชนจะต้องรู้เท่าทันกับภัยคุกคามที่มีแนวโน้มสูงขึ้น และหากประชาชนรู้ไม่เท่าทันภัยหลอกลวงในยุคดิจิทัล ประชาชนจะกลายเป็นจุดอ่อนให้เหล่ามิจฉาชีพมุ่งโจมตีได้ 4. วิจัยและพัฒนาด้าน Cybersecurity ให้กับภาคการธนาคาร ซึ่งจะเป็นส่วนที่ทำให้ TB-CERT มีข้อมูลและความรู้เพื่อช่วยในการวิเคราะห์สถานการณ์ เหตุการณ์แนวโน้มที่อาจจะเกิดขึ้น 5. การให้บริการแก่ธนาคารสมาชิกในการตอบสนองต่อภัยคุกคามทางไซเบอร์ให้ทันท่วงที ภารกิจเหล่านี้จะยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของภาคการธนาคารได้ในภาพรวมอย่างยั่งยืน

นอกจากภารกิจที่ TB-CERT ได้ดำเนินการเพื่อยกระดับและเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์แล้วนั้น การสร้างและขยายเครือข่ายความร่วมมือกับทุกภาคส่วนก็เป็นส่วนสำคัญยิ่งที่ TB-CERT ในฐานะศูนย์ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคารจะต้องดำเนินการควบคู่กันไปด้วย เพราะการแจ้งเหตุหรือการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ทั้งเพื่อการป้องกันและรับมือต่อเหตุการณ์นั้น จำเป็นต้องติดต่อประสานงานไปยังภาคส่วนอื่น ๆ ที่เกี่ยงข้องในเหตุการณ์และไม่เกี่ยวข้องในเหตุการณ์ ให้รับทราบถึงสถานการณ์ที่อาจจะเกิดขึ้นหรือเกิดขึ้นแล้ว ให้เตรียมพร้อมในการรับมือให้ทันต่อเหตุการณ์ และนำข้อมูลไปใช้ในการป้องกันและเฝ้าระวังก่อนที่เหตุการณ์จะเกิดขึ้น

กิจกรรมในปี 2022

กิจกรรมและผลงานสำคัญในปี 2022

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

Standardize: การกำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคธนาคาร

People Development: การพัฒนาบุคลากรด้าน Cybersecurity ของภาคธนาคาร อาทิ การจัดอบรม การซักซ้อมรับมือภัยไซเบอร์

Awareness: การสร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity แก่สมาชิก ผู้บริหารของหน่วยงานสมาชิก ลูกค้า และสื่อมวลชน

Research & Development: การบริหารจัดการและสร้างองค์ความรู้ด้าน Cybersecurity

Services: Alert & Warning, Incident Handling Recommendation, Incident Response Coordination

Q1

- Banking Cyber Drill
- Webinar: Financial Services in driving sustainable outcomes
- Public Awareness
- Technical Recommendation & Alerts
- Cyber Brain E-Learning

กิจกรรมและผลงานสำคัญในปี 2022

Q2

- Webinar: Stop Ransomware Dead in its Tracks
- Roundtable Seminar: Implementing a People-First Cybersecurity Strategy
- Workshop: Optimization Cloud Governance on AWS
- Public Awareness
- Technical Recommendation & Alerts
- Cyber Brain E-Learning

Q3

- Webinar: FS-ISAC Knowledge Sharing (Bangkok Chapter)
- Workshop: Cyber Range Cloud Security
- Webinar: Post Quantum – Are we ready?
- Roundtable Seminar: The Effectiveness with Threat Intelligence
- Cybersecurity Annual Conference: Next Chapter – building trust and collaboration
- Cyber Combat
- Public Awareness
- Technical Recommendation & Alerts
- Cyber Brain E-Learning

Q4

- Seminar: Cyber Resilience Leadership 2022
- Project: Cyber staff and new gen in financial sector
- TB-CERT Annual meeting
- Recommendation for Mobile Operating System of Mobile Banking Application
- Public Awareness
- Technical Recommendation & Alerts
- Cyber Brain E-Learning
- Cybersecurity lessons for TBAC

งานกำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคธนาคาร

API Security Standard

เนื่องด้วยเทคโนโลยี Application Programming Interface หรือเรียกว่า API เข้ามามีบทบาทสำคัญในการให้บริการทางการเงินในปัจจุบันมากยิ่งขึ้น และเป็นเทคโนโลยีหนึ่งที่ช่วยให้การเชื่อมต่อระหว่างระบบเพื่อแลกเปลี่ยนข้อมูลและบริการระหว่างผู้ให้บริการทางการเงินมีประสิทธิภาพมากขึ้น ส่งเสริมการใช้ทรัพยากรที่จำเป็นร่วมกัน ลดเวลาและต้นทุนในการพัฒนาระบบ รวมทั้งสนับสนุนการพัฒนาบริการที่หลากหลายเพื่อตอบสนองความต้องการแก่ผู้ใช้บริการทางการเงินได้ดีขึ้น

อย่างไรก็ตาม นอกจากประโยชน์ที่ได้รับจากการใช้เทคโนโลยี API ในการให้บริการทางการเงินแล้ว การนำ API มาใช้ในการให้บริการทางการเงินอาจก่อให้เกิดความเสี่ยงต่าง ๆ ด้วยเช่นกัน ซึ่งอาจกระทบต่อการดำเนินงานหรือการให้บริการของผู้ให้บริการทางการเงิน โดยเฉพาะอย่างยิ่งในความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงมีความจำเป็นอย่างยิ่งที่การใช้เทคโนโลยี API ในการให้บริการทางการเงินจะต้องดำเนินการพัฒนาและให้บริการภายใต้กรอบการควบคุมดูแลและการบริหารจัดการที่ดี สอดคล้องตามมาตรฐานสากล เพื่อให้ลดผลกระทบที่อาจเกิดจากความเสี่ยงในด้านต่าง ๆ ที่อาจเกิดขึ้น

ธนาคารแห่งประเทศไทย (ธปท.) และศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) จึงได้ร่วมกันจัดทำแนวปฏิบัติการใช้เทคโนโลยี Application Programming Interface (API) ในการให้บริการทางการเงินขึ้น โดยมีวัตถุประสงค์ที่สำคัญได้แก่

(1) กำหนดมาตรฐานในการนำเทคโนโลยี API มาใช้ในการให้บริการทางการเงิน เพื่อเป็นมาตรฐานขั้นต่ำให้ผู้ให้บริการ API มีการประยุกต์ใช้มาตรฐานข้อมูลที่ได้รับการยอมรับ ส่งเสริมใช้งานระหว่างกันได้ (Interoperability) มีการรักษาความมั่นปลอดภัยด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยของข้อมูล และความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานสากลและกฎเกณฑ์เกี่ยวข้อง รวมทั้งมีการบริหารจัดการ API บริหารจัดการความสัมพันธ์ระหว่างผู้ให้บริการและผู้ใช้บริการ API และความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสม

(2) สร้างสภาพแวดล้อมที่สนับสนุนการต่อยอดนวัตกรรมทางการเงิน ซึ่งจะช่วยลดระยะเวลาและอุปสรรคของนักพัฒนาที่นำ API ไปประยุกต์ใช้ โดยจัดให้มีช่องทางสนับสนุนและเปิดเผยข้อมูลที่จำเป็นแก่ผู้ใช้บริการ API

(3) คุ้มครองผู้ใช้บริการทางการเงินในด้านต่าง ๆ เช่น มีการคุ้มครองข้อมูลส่วนบุคคล มีกระบวนการจัดการปัญหาและการเยียวยาชดเชยความเสียหายที่อาจเกิดขึ้นกับผู้ใช้บริการ มีการให้ความรู้ความเข้าใจ และให้ประสบการณ์การใช้งานที่ดี

ซึ่งขอบเขตของแนวปฏิบัติฉบับนี้ครอบคลุมผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของ ธปท. ได้แก่ สถาบันการเงิน ผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินที่อยู่ภายใต้การกำกับของ ธปท. และผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน ที่มีการประยุกต์ใช้เทคโนโลยี API ในการให้บริการทางการเงิน

โดยแนวปฏิบัติฉบับนี้ได้กำหนดหลักการพึงปฏิบัติให้ผู้ให้บริการทางการเงินปฏิบัติตามไว้ 6 หลักการ ประกอบด้วย

(1) กลไกการบริหารจัดการและกำกับดูแล API (Governance) เพื่อให้มีการบริหารจัดการและกำกับดูแลการใช้เทคโนโลยี API อย่างเหมาะสมตามระดับความเสี่ยงของลักษณะของข้อมูลหรือบริการตลอดทั้งวงจรชีวิตของการให้บริการหรือใช้บริการ API โดยคำนึงถึงปัจจัยต่าง ๆ ที่เกี่ยวข้อง ภายใต้กรอบการบริหารความเสี่ยงที่ดี และส่งเสริมความเปิดกว้าง การใช้งานระหว่างกันได้ รวมทั้งการพัฒนาต่อยอดในอนาคต

(2) แนวทางการบริหารจัดการวงจรชีวิต API (API Lifecycle Management) เพื่อให้มีการบริหารจัดการวงจรชีวิต API (API lifecycle) ตั้งแต่สร้าง พัฒนา เผยแพร่ จัดการ ติดตามการใช้งาน และเลิกใช้งานอย่างเหมาะสม เพื่อสามารถให้บริการได้อย่างต่อเนื่อง และช่วยลดความเสี่ยงจากการถูกโจมตีผ่านช่องทาง API

(3) มาตรฐานด้านความมั่นคงปลอดภัย API (API Security Standard) เพื่อให้มีการบริหารจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการรักษาความมั่นคงปลอดภัยของระบบและข้อมูลตามมาตรฐานสากลและหลักเกณฑ์ที่เกี่ยวข้องอย่างเหมาะสมตามระดับความเสี่ยงของประเภท API และข้อมูล โดยแบ่งแนวทางควบคุมความมั่นคงปลอดภัยไว้เป็น 7 ด้าน ได้แก่

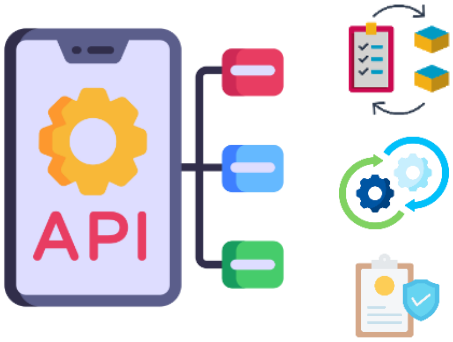
1. กระบวนการยืนยันตัวตน (Authentication)
2. กระบวนการตรวจสอบสิทธิ์การใช้งาน (Authorization)
3. การรักษาความลับของข้อมูลและการตรวจสอบความถูกต้องของข้อมูล (Data Confidentiality and Integrity)
4. การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร (Secure Communication)
5. การพัฒนาโปรแกรมและการกำหนดค่าที่ปลอดภัย (Secure Coding and Configuration)
6. การจัดเก็บข้อมูลบันทึกเหตุการณ์ และการเฝ้าระวัง (Audit Log and Monitoring)
7. ความเพียงพอของทรัพยากร (Resource Sufficiency)

(4) ความสัมพันธ์ระหว่างผู้ให้บริการ API และผู้ใช้บริการ API (Contractual Relationship) เพื่อให้มีการบริหารจัดการความสัมพันธ์และข้อสัญญาระหว่างกันอย่างเหมาะสมตามความสัมพันธ์ทางธุรกิจภายใต้ข้อสัญญาที่มีอยู่ระหว่างกัน กฎหมาย และหลักเกณฑ์การกำกับดูแลที่เกี่ยวข้องสอดคล้องกับระดับความเสี่ยง รวมทั้งมีการกำหนดบทบาทหน้าที่ความรับผิดชอบระหว่างกันที่ชัดเจน และมีการทบทวนมาตรฐานความมั่นคงปลอดภัยระหว่างกันอย่างสม่ำเสมอ

(5) การเปิดเผยข้อมูลการให้บริการ API (API Service Information Disclosure) เพื่อให้มีการเปิดเผยข้อมูลพื้นฐานที่จำเป็นต่อการใช้งาน API อย่างเพียงพอต่อการตัดสินใจเลือกใช้งาน หรือนำ API ไปใช้งานได้อย่างมีประสิทธิภาพ มีช่องทางในการทดสอบให้แก่ผู้ใช้งาน และส่งเสริมให้ผู้ใช้บริการมีสภาวะแวดล้อมที่เอื้ออำนวยให้สามารถนำ API ไปใช้พัฒนานวัตกรรมได้อย่างรวดเร็วยิ่งขึ้น

(6) การคุ้มครองผู้ใช้บริการทางการเงิน (Customer Protection) เพื่อให้ผู้ใช้บริการทางการเงินได้รับการคุ้มครองตามกฎหมายและตามสิทธิต่าง ๆ ที่ตนมี ได้รับข้อมูลที่เพียงพอ มีช่องทางในการแจ้งปัญหาและข้อร้องเรียน ได้รับการดูแล และการเยียวยาอย่างเหมาะสมเมื่อได้รับความเสียหายจากการใช้บริการ

g



ข้อเสนอแนะมาตรฐานด้านความมั่นคงปลอดภัย ระบบปฏิบัติการโทรศัพท์มือถือ สำหรับโมบายแอปพลิเคชัน ของภาคการธนาคาร

การให้บริการการโอนเงินและการชำระเงินแบบออนไลน์ผ่านแอปพลิเคชันบนโทรศัพท์มือถือ ได้รับความนิยมในการใช้งานเพิ่มสูงขึ้นอย่างต่อเนื่องในยุคปัจจุบัน เพื่อตอบโจทย์ไลฟ์สไตล์การจับจ่ายใช้สอยที่ทันสมัย และการตอบสนองตามนโยบายสังคมไร้เงินสด ทำให้จำนวนผู้ใช้งานแอปพลิเคชันต่าง ๆ ที่เกี่ยวกับการโอนเงินและการชำระเงินผ่านโทรศัพท์มือถือเพิ่มมากขึ้น อีกทั้งในอนาคตแอปพลิเคชันของธนาคารและผู้ให้บริการอื่นบนโทรศัพท์มือถือจะยิ่งมีฟังก์ชั่นเพิ่มขึ้น เพื่ออำนวยความสะดวกและตอบโจทย์ความต้องการความรวดเร็วในการทำธุรกรรมการเงินต่าง ๆ ให้กับผู้ใช้งาน ทำให้โทรศัพท์มือถือเป็นอีกหนึ่งเป้าหมายสำคัญที่มิจฉาชีพออนไลน์พยายามเข้าถึง เพื่อที่จะขโมยข้อมูลส่วนบุคคลที่สำคัญ รวมถึงลักลอบขโมยเงินจากบัญชีธนาคารของผู้ใช้งาน

ในภาคการธนาคารได้เล็งเห็นถึงความสำคัญในการดูแลความปลอดภัยของระบบหลักที่ให้บริการโมบายแบงก์กิ้ง และมีมาตรการด้านความปลอดภัยเพื่อป้องกันภัยคุกคามทางไซเบอร์ระดับองค์กรเพื่อความมั่นคงปลอดภัยในส่วนของระบบหลักมาอย่างต่อเนื่อง อย่างไรก็ตาม เพื่อความปลอดภัยต่อข้อมูลและทรัพย์สินของผู้ใช้งานโมบายแบงก์กิ้ง การกำหนดมาตรฐานด้านความปลอดภัยสำหรับโทรศัพท์มือถือที่จะอนุญาตให้ผู้ใช้บริการสามารถติดตั้งและใช้งานแอปพลิเคชันโมบายแบงก์กิ้งได้ จึงถือเป็นพื้นฐานสำคัญที่ช่วยลดความเสี่ยงด้านความปลอดภัยที่อาจเกิดจากมิจฉาชีพออนไลน์และภัยคุกคามทางไซเบอร์ จากการใช้งานแอปพลิเคชันโมบายแบงก์กิ้ง โดยแนวทางการพิจารณาดำหนดมาตรฐานความปลอดภัยดังกล่าว อ้างอิงจากการพัฒนาแอปพลิเคชัน OWASP Mobile Application Security Verification Standard (MASVS) และการทดสอบความปลอดภัย OWASP Mobile Security Testing Guide (MSTG) ทั้งนี้ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) และธนาคารสมาชิก ได้ร่วมกันพิจารณากำหนดเกณฑ์การประเมินเวอร์ชั่นของระบบปฏิบัติการขั้นต่ำ และออกเอกสารชื่อว่า “ข้อเสนอแนะมาตรฐานด้านความมั่นคงปลอดภัยระบบปฏิบัติการโทรศัพท์มือถือสำหรับโมบายแอปพลิเคชันของภาคการธนาคาร” หรือชื่อภาษาอังกฤษว่า “Recommendation for Mobile Operating System of Mobile Banking Application” โดยมีวัตถุประสงค์เพื่อแสดงให้เห็นถึงความเสี่ยงด้านความปลอดภัยของระบบปฏิบัติการ ในกรณีที่ใช้งานแอปพลิเคชันโมบายแบงก์กิ้งบนระบบปฏิบัติการที่ล้าสมัย หรือไม่มีการสนับสนุนจากเจ้าของผลิตภัณฑ์ เพื่อให้เกิดความเข้าใจและมีแนวทางป้องกันเบื้องต้น ในระหว่างการวางแผน Upgrade ระบบปฏิบัติการให้ทันสมัยในเวลาที่เหมาะสม

เกณฑ์การประเมินเวอร์ชันของระบบปฏิบัติการขั้นต่ำที่ธนาคารอนุญาตให้ใช้งานแอปพลิเคชันโมบายแบงก์กิ้ง

เกณฑ์การประเมินเวอร์ชันฯ จะพิจารณาจากปัจจัยที่ใช้ป้องกันภัยคุกคามทางไซเบอร์ที่มีผลต่อการใช้งานแอปพลิเคชันโมบายแบงก์กิ้งอย่างปลอดภัย ซึ่งประกอบด้วย

(1) ความปลอดภัยในการรับ-ส่งข้อมูล เป็นการพิจารณาความปลอดภัยด้านการรับ-ส่งข้อมูลระหว่างโทรศัพท์มือถือของผู้ใช้บริการ และแอปพลิเคชันโมบายแบงก์กิ้งของธนาคารผู้ให้บริการ ซึ่งอาจมีความเสี่ยงที่ข้อมูลสำคัญจะถูกดักจับ หรือถูกเปลี่ยนแปลงแก้ไขข้อมูลระหว่างการรับ-ส่งข้อมูลได้ ดังนั้น อุปกรณ์โทรศัพท์มือถือที่ใช้งานจะต้องรองรับโพรโทคอลที่ได้มาตรฐานความปลอดภัยเพียงพอ ได้แก่

1.1) รองรับการใช้งานโพรโทคอลที่มีมาตรฐานความปลอดภัย ได้แก่ TLS 1.2 ขึ้นไป

1.2) ไม่สนับสนุนการใช้งานโพรโทคอลที่ไม่ปลอดภัย ได้แก่ SSLv3

1.3) ไม่สนับสนุนการใช้งานอัลกอริทึมที่ไม่ปลอดภัย ได้แก่ SHA-1, RC4

(2) ความปลอดภัยในการจัดเก็บข้อมูลบนเครื่องโทรศัพท์มือถือ เป็นการพิจารณาความปลอดภัยด้านการจัดเก็บข้อมูลบนอุปกรณ์โทรศัพท์มือถือที่ประกอบด้วยข้อมูลสำคัญ ข้อมูลส่วนตัว และข้อมูลที่มีความละเอียดอ่อน ดังนั้น ความปลอดภัยในการจัดเก็บข้อมูลและการบริหารจัดการข้อมูลบนโทรศัพท์มือถือจึงเป็นสิ่งสำคัญ การพิจารณาการใช้งานเทคโนโลยีการเข้ารหัสข้อมูลบนอุปกรณ์โทรศัพท์มือถือต้องมีความปลอดภัยอย่างเหมาะสมและสอดคล้องกับสถานการณ์ภัยคุกคามที่อาจจะเกิดขึ้นในปัจจุบัน ดังนั้น โทรศัพท์มือถือที่ใช้งานจะต้องรองรับเทคโนโลยีการรักษาความปลอดภัยของข้อมูล ได้แก่ เทคโนโลยีที่เป็นมาตรฐานการเข้ารหัสข้อมูล และเทคโนโลยีที่เป็นมาตรฐานการจัดเก็บข้อมูล

2.1) เทคโนโลยีที่เป็นมาตรฐานการเข้ารหัสข้อมูล รองรับการเข้ารหัสของข้อมูลสำคัญรูปแบบต่าง ๆ เช่น การเข้ารหัสแบบไฟล์ (File encryption) และการเข้ารหัสตามโครงสร้างไฟล์ (Metadata encryption) เพื่อป้องกันข้อมูลสำคัญจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต และจากแอปพลิเคชันอื่นที่ไม่ได้รับอนุญาต

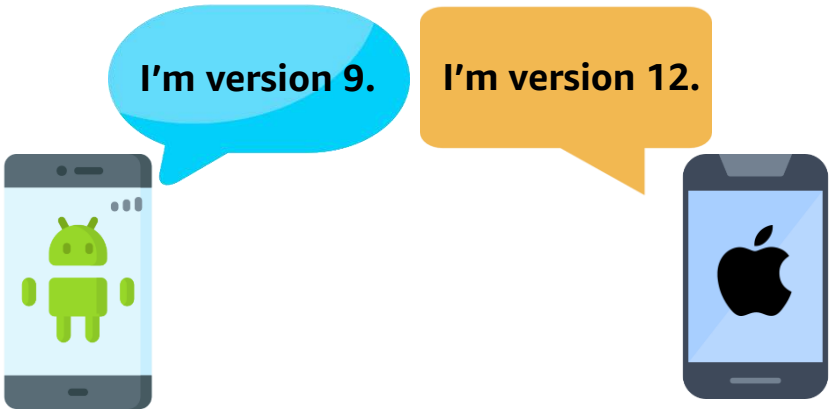
2.2) โมดูลที่ใช้เข้ารหัสข้อมูล รองรับมาตรฐานความปลอดภัยสากล ได้แก่ FIPS 140-2 ขึ้นไป

2.3) เทคโนโลยีที่เป็นมาตรฐานการจัดเก็บข้อมูล ข้อมูลสำคัญเหล่านี้ควรต้องเก็บอยู่ในพื้นที่บันทึกข้อมูลที่ปลอดภัย (Secure storage device) รวมถึงการกำหนดพื้นที่พิเศษเพื่อสร้างความปลอดภัยของข้อมูลขณะประมวลผล ตัวอย่างเช่น Secure enclave, StrongBox keymaster และ Trusted Execution Environment (TEE) เพื่อจำกัดสิทธิ์การอ่านและการเข้าถึงข้อมูลจากแอปพลิเคชันที่ไม่ได้รับอนุญาต นอกจากนี้ยังช่วยป้องกันการเข้าถึงข้อมูลจากมัลแวร์ในกรณีที่เครื่องอาจถูก Compromised ได้

(3) ความปลอดภัยของระบบปฏิบัติการ โดยพิจารณาจากความรุนแรงของช่องโหว่ที่เกิดขึ้น และการดูแลแก้ไขช่องโหว่นั้น ๆ หากระบบปฏิบัติการเวอร์ชันใดที่ล้าสมัย หรือไม่มีการสนับสนุนจากเจ้าของผลิตภัณฑ์ และมีช่องโหว่ระดับรุนแรง (Critical) ที่อาจส่งผลทำให้เกิดการทำงานข้ามสิทธิ์ (Bypass authorization) หรือทำให้แอปพลิเคชันโมบายอื่นสามารถประมวลผลข้าม Sandbox ได้ จึงไม่ควรให้อนุญาตให้ติดตั้งและใช้งานแอปพลิเคชันโมบายแบงก์กิ้งบนระบบปฏิบัติการเวอร์ชันดังกล่าวได้

(4) ความปลอดภัยของเทคโนโลยีที่ใช้ในการพัฒนาแอปพลิเคชัน โดยพิจารณาจากเทคโนโลยี ไลบรารี หรือคอมโพเนนต์ที่ใช้พัฒนาแอปพลิเคชันโมบายแบงก์กิ้งอาจมีช่องโหว่ เช่น การใช้งานคอมโพเนนต์ในการพัฒนาแอปพลิเคชัน หากเทคโนโลยี ไลบรารี หรือคอมโพเนนต์ที่นำมาใช้พัฒนาแอปพลิเคชันมีช่องโหว่ระดับรุนแรงที่ไม่สามารถแก้ไขได้ ก็จะส่งผลทำให้ผู้ใช้งานแอปพลิเคชันดังกล่าว มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ได้ จึงไม่ควรอนุญาตให้ติดตั้งและใช้งานแอปพลิเคชันโมบายแบงก์กิ้งบนระบบปฏิบัติการเวอร์ชันที่ใช้งานไลบรารี หรือคอมโพเนนต์ที่มีช่องโหว่ระดับรุนแรง

จากการศึกษาปัจจัยทั้ง 4 ปัจจัยข้างต้นนั้น TB-CERT จึงได้เสนอข้อแนะนำเวอร์ชันขั้นต่ำของระบบปฏิบัติการสำหรับโทรศัพท์มือถือ ที่จะสามารถติดตั้งและใช้งานแอปพลิเคชันโมบายแบงก์กิ้ง โดยสำหรับแพลตฟอร์ม iOS คือ iOS เวอร์ชัน 12 และแพลตฟอร์ม Android คือ Android เวอร์ชัน 9 และได้ประกาศขอความสนับสนุนให้ธนาคารสมาชิกและภาคการธนาคารพิจารณา เพื่อปรับเวอร์ชันขั้นต่ำของระบบปฏิบัติการสำหรับโทรศัพท์มือถือตามข้อเสนอแนะดังกล่าว

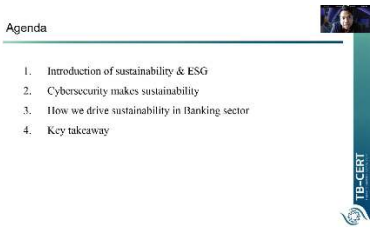


งานด้านการพัฒนาบุคลากร

งานด้านการสร้างความตระหนักรู้ด้านไซเบอร์ให้กับสมาชิก Cybersecurity Professional Development Program

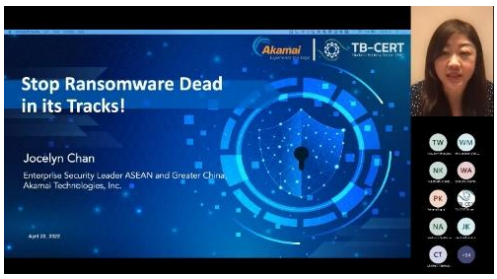
1. งานสัมมนาออนไลน์ หัวข้อ “Financial Services in driving sustainable outcomes”

TB-CERT ร่วมกับบริษัท SAP Thailand จัดงานสัมมนาออนไลน์ในหัวข้อ “Financial Services in driving sustainable outcomes” ในวันที่ 25 มีนาคม 2022 เวลา 10.00-11.15 น. ด้วยแนวคิดการดำเนินธุรกิจขององค์กรอย่างยั่งยืน ESG (Environment, Social, Governance) เป็นประเด็นสากลที่หลายองค์กรทั่วโลกให้ความสำคัญ รวมทั้งบทบาทขององค์กรภาคการเงินการธนาคารที่จะขับเคลื่อนองค์กร ไม่ว่าจะเป็นการลงทุน การบริหารจัดการ ยิ่งไปกว่านั้น ประเด็นความมั่นคงปลอดภัยทางไซเบอร์ยังเป็นส่วนหนึ่งของความยั่งยืนด้านสังคมและธรรมาภิบาล ซึ่งในงานสัมมนาได้เรียนรู้และรับทราบถึงแนวทางที่จะองค์กรภาคการเงินการธนาคารจะสามารถพัฒนาและปรับตัวไปสู่การเป็นองค์กรแห่งความยั่งยืนต่อไป



2. งานสัมมนาออนไลน์ หัวข้อ “Stop Ransomware Dead in its Tracks”

TB-CERT ร่วมกับบริษัท Akamai Technologies จัดงานสัมมนาออนไลน์ในหัวข้อ “Stop Ransomware Dead in its Tracks” ในวันที่ 22 เมษายน 2022 เวลา 10.00-11.30 น. มีผู้เข้าร่วมงาน 82 คน



3. Roundtable Seminar หัวข้อ “Implementing a People-First Cybersecurity Strategy”

TB-CERT ร่วมกับบริษัท Proofpoint จัดงาน Roundtable Seminar หัวข้อ “Implementing a People-First Cybersecurity Strategy” ในวันที่ 27 พฤษภาคม 2022 เวลา 10.30-13.30 น. ณ โรงแรม The Okura Prestige โดยในงานสัมมนาได้กล่าวถึง

- How to build a business case and executive narrative
- Use DMARC as stop phishing emails from getting through
- Build an outcome-driven approach to cybersecurity

---

4. Webinar FS-ISAC Knowledge Sharing (Bangkok Chapter)

TB-CERT ร่วมกับ Financial Services Information Sharing and Analysis Center (FS-ISAC) จัด Webinar เพื่อแชร์ความรู้เกี่ยวกับ FS-ISAC Threat Intelligence และ Investigation Technique and Tactic on DLP Incident เมื่อวันที่ 15 กรกฎาคม 2022 มีผู้เข้าร่วมงาน 35 คน

---

5. Webinar “Post Quantum: Are We Ready?”

TB-CERT ร่วมกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และบริษัทควอนตัมเทคโนโลยีฟาวเดชั่น (ประเทศไทย) หรือ QTFT จัดงานสัมมนาออนไลน์หัวข้อ “Post Quantum: Are We Ready?” เพื่อเตรียมพร้อมรับมือและสร้างความตระหนักรู้เกี่ยวกับสถานการณ์เมื่อทฤษฎี Quantum ถือกำเนิดขึ้นซึ่งเป็นเทคโนโลยีใหม่ที่หน่วยงานและองค์กรควรเตรียมพร้อมรับมือต่อสถานการณ์ที่คาดว่าจะเกิดขึ้นในอนาคตอันใกล้ เมื่อวันที่ 27 กรกฎาคม 2022 มีผู้เข้าร่วมงาน 90 คน


---

6. งานสัมมนาหัวข้อ “The Effectiveness with Threat Intelligence”

TB-CERT ร่วมกับบริษัท Kaspersky จัดงานสัมมนาหัวข้อ “The Effectiveness with Threat Intelligence” เมื่อวันที่ 16 สิงหาคม 2022 ณ โรงแรม Rosewood Bangkok เพื่อเผยแพร่ข้อมูลจาก Global Research and Analysis Team (GReAT) ด้านบทวิเคราะห์เกี่ยวกับ Threat Landscape ในปี 2022 โดยเฉพาะในภูมิภาคเอเชียแปซิฟิค มีผู้เข้าร่วมงานจำนวน 40 คน


โครงการ Cybersecurity Development Program (Workshop)
จัดอบรมเชิงปฏิบัติการให้กับธนาคารสมาชิกด้านความมั่นคงปลอดภัยไซเบอร์

ในปี 2022 จากกระแสการปรับตัวการใช้เทคโนโลยีคลาวด์อย่างต่อเนื่อง เพื่อตอบสนองต่อการดำเนินธุรกิจในปัจจุบัน จึงเป็นเรื่องสำคัญอย่างยิ่งในการขับเคลื่อนองค์กรเข้าสู่เทคโนโลยีคลาวด์อย่างมีความมั่นคงปลอดภัย ดังนั้น ทาง TB-CERT จึงได้จัดอบรมหลักสูตรเพื่อสร้างความเข้าใจทั้งในภาคทฤษฎีและภาคปฏิบัติให้กับหน่วยงานสมาชิก TB-CERT โดยมุ่งเน้นการออกแบบและใช้งานบริการของคลาวด์ (Cloud services) ตามกรอบความมั่นคงปลอดภัย NIST Cybersecurity Framework (CSF) และสร้างความเข้าใจหลักการความรับผิดชอบร่วม (Shared Responsibility Model) ระหว่างผู้ใช้บริการและผู้ให้บริการเทคโนโลยีคลาวด์ ในการร่วมกันรักษาความมั่นคงปลอดภัยให้กับองค์กร อีกทั้งผู้เข้ารับการอบรมได้รับการฝึกทักษะภาคปฏิบัติ (Hands-on) ในการแก้ไขปัญหาตามโจทย์ในด้านความปลอดภัยของระบบคลาวด์ เพื่อสร้างความเข้าใจในการนำความรู้ไปปรับใช้ในองค์กรและภาคการธนาคารได้อย่างเหมาะสม

เรื่องที่ 1 “Optimization Cloud Governance on AWS”

TB-CERT ร่วมกับบริษัท Amazon Web Services (AWS) Thailand จัดการอบรมเชิงปฏิบัติการเพื่อเสริมสร้างความรู้การบริหารจัดการการใช้งานเทคโนโลยีบนคลาวด์ เมื่อวันที่ 29-20 มิถุนายน และ 4 กรกฎาคม 2022 มีผู้เข้าร่วมอบรม 73 คน

เรื่องที่ 2 “Cyber range cloud security”

TB-CERT ร่วมกับบริษัท Palo Alto Networks จัดการอบรมเชิงปฏิบัติการเพื่อเสริมสร้างความรู้ความเข้าใจเรื่อง Cyber Range Cloud Security เมื่อวันที่ 22 และ 25 กรกฎาคม 2022 ผู้เข้าร่วมอบรม 30 คน

งานด้านการพัฒนาศักยภาพในการรับมือภัยไซเบอร์ Cyber Combat

โครงการ Practical Cybersecurity Competition ในรูปแบบ Cyber Combat Virtual Tournament เพื่อสร้างความร่วมมือกับหน่วยงานภายนอกภาคการธนาคารทั่วประเทศและฝึกทักษะการค้นหาหลักฐานทางด้านดิจิทัลเมื่อเกิดเหตุการณ์ถูกโจมตีด้านไซเบอร์ แบ่งการฝึกออกเป็น 2 ส่วน คือ ส่วนอบรมฝึกฝนทักษะให้เรียนรู้เกี่ยวกับการรับมือและการโจมตีด้วยวิธีการต่าง ๆ ซึ่งทักษะส่วนใหญ่จะมุ่งเน้นการค้นหาข้อมูลและเทคนิคที่แตกต่างกันออกไป การอบรมทักษะ 2 วันคือวันที่ 7 และ 9 กันยายน 2022 ส่วนการฝึกในส่วนที่ 2 คือส่วนของการแข่งขัน ซึ่งถือเป็นตัววัดระดับความรู้ที่ได้เรียนมาด้วย การแข่งขันแบ่งออกเป็น 2 รอบ โดยรอบคัดเลือกจัดขึ้นในวันที่ 8 กันยายน จากจำนวนทีม 42 ทีม ทีมละ 4 คน และคัดเหลือเพียง 20 ทีมเท่านั้นที่จะเข้าแข่งขันรอบ Final การแข่งขันรอบ Final นี้จะมีรูปแบบการแข่งขันที่เสมือนกับการปฏิบัติงานจริงมากขึ้นจากปีก่อน ๆ ในรูปแบบ Attack & Defense ที่ภายในทีมจะได้ประสานงาน หารือกันภายใน ให้ระบบของทีมตนยังคง Available อยู่ ไม่ล่ม และไม่ถูกแฮ็ก และจะต้องทำคะแนนจากการเจาะระบบของอีกทีมเมื่อพบช่องโหว่

การแข่งขันรอบนี้จัดขึ้นเป็นระยะเวลา 2 วันคือ วันที่ 21-22 กันยายน 2022 ที่โรงแรม The Athenee Hotel, a Luxury Collection Hotel, Bangkok โดยผู้ชนะ 3 อันดับแรกได้แก่ ทีมจากหน่วยงาน ตลาดหลักทรัพย์แห่งประเทศไทย ธนาคารกรุงเทพ และธนาคารกสิกรไทย ตามลำดับ

สรุปทักษะสำคัญ 6 เรื่องที่ผู้เข้าแข่งขันได้ฝึกและนำมาปรับใช้คือ

1. **Exploit development** คือ ทักษะการเจาะช่องโหว่หรือจุดอ่อนของระบบ เพื่อทำการเข้าควบคุมการทำงานในระบบนั้น ๆ
2. **Web exploitation** คือ ทักษะการเจาะช่องโหว่ของเว็บแอปพลิเคชัน เพื่อเข้าถึงฐานข้อมูลหรือดักอ่านข้อมูลบนหน้าเว็บ
3. **Reverse engineering** คือ ทักษะการวิเคราะห์คำสั่งคอมพิวเตอร์ที่ใช้ในการทำงาน โดยสืบย้อนกลับไปค้นหาความหมายของคำสั่งว่ามีการทำงานเชื่อมโยงกันอย่างไร เพื่อแก้ไขจุดผิดพลาดและพัฒนาชุดคำสั่งต่อไป
4. **Digital Forensic** คือ ทักษะการรวบรวมหลักฐาน ตรวจพิสูจน์ และเก็บรักษาข้อมูลหลักฐานทางดิจิทัลที่เป็นร่องรอยหลงเหลือของผู้โจมตีระบบ
5. **Cryptography** คือ ทักษะการปกปิดข้อมูลโดยการเข้ารหัส และการถอดรหัสเพื่ออ่านข้อมูล
6. **Threat Defense** คือ ทักษะการตั้งค่าความปลอดภัยของระบบ เพื่อป้องกันการโจมตีทางไซเบอร์

ภาพการจัดงาน TB-CERT Cyber Combat2022

งานด้านการพัฒนาศักยภาพในการรับมือภัยไซเบอร์ Cyber Drill

การซักซ้อมรับมือภัยไซเบอร์เป็นกิจกรรมที่สำคัญในการเตรียมความพร้อมและความเข้าใจในการตอบสนองต่อสภาวการณ์การถูกโจมตีทางไซเบอร์ เพื่อให้โจทย์ที่ใช้ในการซักซ้อมสะท้อนถึงมุมมองความเสี่ยงต่อภาคการธนาคารจริง ๆ ซึ่งในปีที่ผ่านมา TB-CERT ได้มีการออกแบบสอบถามถึงมุมมองต่อภัยคุกคามทางไซเบอร์ที่สำคัญจากผู้บริหารระดับสูงของธนาคารสมาชิกซึ่งให้ความสำคัญต่อภัยคุกคามในด้านต่าง ๆ ดังนี้ 1. ภัยคุกคามต่อบริการ Mobile Banking 2. ภัยคุกคามประเภท 3rd Party Attack และ 3. ภัยคุกคามประเภท Ransomware และ Phishing Attack สำหรับการซักซ้อมในปีที่ผ่าน ๆ มามีข้อจำกัดที่จำนวนคนที่สามารถเข้าร่วมซักซ้อมได้ในสถานที่เดียวกันทำให้กระบวนการด้านการจัดการเหตุ ประสานงาน และตัดสินใจนั้นอาจจะไม่เสมือนจริงเท่าที่ควร จึงได้มีการพัฒนา Platform สำหรับซักซ้อมเพื่อให้สามารถเข้าร่วมการซักซ้อมได้แบบ Online โดยผู้ที่มีส่วนร่วมในการเผชิญเหตุสามารถเข้าร่วมให้ความเห็น ร่วมตัดสินใจได้ด้วยตนเองซึ่งถือเป็นมิติการซักซ้อม Banking Cyber Drill แบบ New Normal

ภัยคุกคามทางไซเบอร์ที่มีผลกระทบในระดับของภาคการธนาคารนั้น นอกจากผลกระทบในวงกว้างแล้ว การควบคุมสถานการณ์เป็นสิ่งที่สำคัญที่ต้องมีความร่วมมือการสื่อความในจังหวะเวลาและเนื้อหาที่เหมาะสม ซึ่งหมายถึงการมีการเตรียมกลยุทธ์ในการสื่อความในรูปแบบต่าง ๆ ล่วงหน้า จึงเป็นวัตถุประสงค์หลักของการซักซ้อมที่ต้องการจะพัฒนาความพร้อมการสื่อความในภาพรวมของภาคการธนาคาร

สถานการณ์จำลองที่ใช้ในการซักซ้อมถูกออกแบบให้มีประเด็นเหตุการณ์ที่หลากหลายโดยเกิดขึ้นในช่วงเวลา 1 วันของการซักซ้อมไม่ว่าจะเป็นเหตุการณ์การถูกโจมตีที่ 3rd party หรือผู้ให้บริการภายนอกผ่านเทคโนโลยี API แล้ว ยังจำเป็นต้องปฏิบัติตาม พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เพื่อให้เกิดการเตรียมการสำหรับการปฏิบัติตามกฎหมายทั้งสองฉบับ โดยมีผู้แทนจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เข้าร่วมซักซ้อมด้วย จากการซักซ้อมครั้งนี้แสดงถึงความพร้อมของหน่วยงานในภาคการธนาคารในการตอบสนองต่อเหตุการณ์การโจมตี รวมถึงการควบคุมเหตุการณ์เพื่อมิให้มีการลุกลามบานปลาย (Containment) เป็นไปอย่างมีประสิทธิภาพ แต่เนื่องจากเหตุการณ์ที่มีผลกระทบในวงกว้างจริง ๆ นั้น แนวทางในการสื่อความจะมีความแตกต่างขึ้นกับกลยุทธ์ของแต่ละหน่วยงาน โดยจะพิจารณาจากประเด็นความเสี่ยงและผลกระทบในด้านต่าง ๆ ไม่ว่าจะเป็นด้านลูกค้า ด้านความเสียหาย ด้านชื่อเสียง ด้านกฎหมาย รวมถึงความชัดเจนของสถานการณ์ในขณะนั้น ๆ อีกด้วย

หัวข้อการซักซ้อม

จากการรวบรวมข้อมูลความเห็นผู้บริหารระดับสูงของธนาคารสมาชิกพบว่า ภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อบริการต่าง ๆ รวมถึงมีผลกระทบต่อประชาชนอย่างมีนัยสำคัญ อันประกอบด้วย 1. ภัยคุกคามต่อบริการ Mobile Banking 2. ภัยคุกคามประเภท 3rd Party Attack และ 3. ภัยคุกคามประเภท Ransomware และ Phishing Attack มาใช้ในการออกแบบเรื่องราวสถานการณ์จำลองให้สมจริงและมีการเพิ่มเรื่องราวเพื่อให้มีการเตรียมความพร้อมสำหรับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จึงสรุปหัวข้อการซักซ้อมได้คือ

"เกิดเหตุการณ์การโจมตีช่องโหว่ของ API ที่หลายธนาคารใช้เชื่อมต่อกับหน่วยงานภายนอก ส่งผลกระทบต่อบริการของภาคการธนาคารในวงกว้าง อีกทั้งยังเกิดเหตุการณ์ขู่เรียกค่าไถ่จากกรณีข้อมูลลูกค้ารั่วไหล ส่งผลต่อความเชื่อมั่นของประชาชนต่อสถาบันการเงิน"

วัตถุประสงค์

1. เพื่อยกระดับการซ้อมรับมือภัยไซเบอร์ให้ผู้บริหารได้มีปฏิสัมพันธ์กับผู้ปฏิบัติงาน โดยจำลองสถานการณ์การซ้อมให้มีการร่วมกันตัดสินใจในการแก้ไขสถานการณ์
2. เพื่อประเมินทักษะในการวิเคราะห์การโจมตีทางไซเบอร์ รวมถึงการประเมินแนวทางแก้ไขและป้องกันเหตุในอนาคต ในระดับผู้ปฏิบัติงาน
3. เพื่อซักซ้อมการตอบสนองต่อเหตุการณ์การแจ้งเตือนภัยคุกคามที่ได้รับจากระบบ Threat Intelligence
4. เพื่อซักซ้อมขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติจากการโจมตีทางไซเบอร์ที่เกิดขึ้น และกระบวนการประสานงานระหว่างผู้เกี่ยวข้อง ทั้งภายในหน่วยงานสมาชิก TB-CERT และหน่วยงานภายนอก
5. เพื่อพัฒนากระบวนการรับมือภัยโจมตีทางไซเบอร์ให้มีประสิทธิภาพและ**กลยุทธ์การสื่อสารต่อสาธารณะได้อย่างเหมาะสมกับสถานการณ์ (Media Handling)**
6. เพื่อพัฒนากระบวนการประสานงานของหน่วยงาน CII และ TB-CERT ในฐานะเป็น Sectorial CERT ไปยัง Regulator และ NCSA ตาม พ.ร.บ. ไซเบอร์

การซ้อมรับมือกับภัยคุกคามทางไซเบอร์ในปี 2022 นี้เราเล็งเห็นถึงความสำคัญของกลไกการจัดการด้านการสื่อความซึ่งเป็นหนึ่งในหัวใจหลักของการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ ดังนั้นการฝึกการสื่อสารทั้งภายในและภายนอกในการฝึกซ้อมครั้งนี้จึงเป็นหัวใจหลักของแผนการฝึกซ้อมเพื่อเพิ่มความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์ขององค์กร

การสื่อสารภายในและภายนอก

กลไกการจัดการด้านการสื่อสารเป็นการสื่อประเด็นสำคัญของเหตุการณ์ที่กำลังเกิดขึ้นให้กับผู้ที่เกี่ยวข้องทั้งภายในและภายนอก โดยจะต้องคำนึงถึงการสื่อสารข้อความถึงผู้รับสารตามความเหมาะสม ในจังหวะที่ถูกต้อง ผู้ให้ข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายในการสื่อความโดยมีเนื้อความในการสื่อต้องครบถ้วนและไม่ก่อให้เกิดผลเสียกับองค์กร

สำหรับแนวทางปฏิบัติการจัดการด้านการสื่อสาร (Media Handling) ต่อสื่อสาธารณะจึงมีไว้ เพื่อให้ผู้บริหารและสมาชิกได้รับทราบแนวทางการวิธีจัดการและให้ข้อมูลแก่สื่อ เช่น การให้สัมภาษณ์ การแถลงข่าว การให้ข้อมูลผ่านสื่อสังคมออนไลน์ รวมทั้งการสร้างความเข้าใจกับผู้มีอิทธิพลต่อความคิดเห็นของสาธารณชน (influencers) เพื่อเสริมสร้างความน่าเชื่อถือต่ออุตสาหกรรมทางการเงินของประเทศไทย

Media Handling มีความสำคัญต่อองค์กรอย่างยิ่ง การเข้าใจพลังและตระหนักถึงอิทธิพลของสื่อ และหรือ influencers จะทำให้องค์กรมีโอกาสที่ตอบสนองต่อสื่อได้อย่างมีประสิทธิภาพ ใช้ช่องทางการสื่อสารที่เหมาะสมรวมถึงตระหนักเกี่ยวกับปัญหาขององค์กรอย่างแท้จริง ดังนั้นองค์กรจะต้องมีการจัดการด้านการสื่อสาร (Media Handling) เพื่อใช้เป็นแนวทางในการตอบสนองต่อสื่อเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยทางด้านไซเบอร์ที่สถานการณ์มีระดับความรุนแรงต่าง ๆ

การเตรียมการจัดการด้านการสื่อสารจะแสดงให้เห็นถึงกระบวนการการเตรียมการการสื่อความ ทั้งภายในและภายนอก คณะทำงาน ช่องทางการสื่อสาร รวมถึงหลักปฏิบัติเพื่อให้การสื่อความมีประสิทธิภาพสูงสุด รวมถึงการวางแผนการตอบสนองต่อสื่อสังคมด้วยเพื่อลดผลกระทบด้านลบ หรืออคติที่จะเกิดขึ้นกับองค์กร และขยายไปถึงการสร้างความน่าเชื่อถือขององค์กรต่อบุคคลภายนอก การสื่อความนั้นจะสอดคล้องกับเกณฑ์การพิจารณาระดับความรุนแรงของเหตุการณ์ที่องค์กรประเมิน ซึ่งองค์กรอาจจะแบ่งความรุนแรงของสถานการณ์ออกเป็นระดับสูง กลาง และต่ำ แล้วแต่เกณฑ์การพิจารณาผลกระทบขององค์กรนั้น ๆ โดย Media Handling จะมุ่งเน้นการสื่อสารสำหรับเหตุการณ์ที่ก่อให้เกิดผลกระทบกับความน่าเชื่อถือขององค์กร กระทบกับลูกค้าขององค์กร และกระทบกับทรัพย์สินขององค์กร โดยในที่นี้การซักซ้อมรับมือต่อภัยคุกคามทางไซเบอร์ภาคการธนาคารของ TB-CERT จึงเน้นการจัดการเรื่องต่อสื่อเมื่อเกิดเหตุการณ์ระดับความรุนแรงกระทบต่อภาพลักษณ์ขององค์กรและต่อลูกค้า

จากระดับความรุนแรงที่เกิดขึ้นกับองค์กร จะนำมากำหนดขั้นตอนในการสื่อความและการติดต่อแจ้งเหตุการณ์กับสื่อมวลชน โดยข้อความสื่อความมุ่งเน้นในเรื่องการรักษาภาพลักษณ์ความน่าเชื่อถือขององค์กร และยังรวมถึงความสำคัญของการไม่เปิดเผยข้อมูลที่ละเอียดอ่อนเกินจำเป็น เช่น รายละเอียดด้านเทคนิคของมาตรการตอบโต้ที่อาจทำให้องค์กรถูกโจมตีได้

กลยุทธ์วางแผนการสื่อสาร

หลักสำคัญในการพิจารณาก่อนที่จะดำเนินการสื่อความ มี 2 หัวข้อดังนี้

1. พิจารณาระดับความรุนแรงของสถานการณ์ที่กำลังเกิดขึ้นกับองค์กรว่ามีความรุนแรงระดับใด เช่น ภายในองค์กรไม่สามารถปฏิบัติงานได้เลย หรือ สามารถปฏิบัติงานได้แต่เป็นไปด้วยความล่าช้า
2. พิจารณาผู้ที่ได้รับผลกระทบ
   - ลูกค้า โดยพิจารณาอย่างชัดเจน เช่น ลูกค้าทั่วไป ลูกค้า SME
   - พนักงาน ต้องแบ่งแยกให้ชัดเจน ว่าเป็นพนักงานในส่วนที่ต้องให้บริการกับลูกค้า หรือพนักงานที่เป็นส่วนสนับสนุนองค์กร เช่น ฝ่าย IT ฝ่ายทรัพยากรบุคคล อื่นๆ เป็นต้น

เมื่อพิจารณา 2 หัวข้อที่ผ่านมา ให้นำการพิจารณานี้มาเป็นปัจจัยในการเลือกกลยุทธ์ในการสื่อสาร โดยแบ่งกลยุทธ์ในการสื่อสารดังนี้

1. กลยุทธ์ชี้แจงให้เหตุผล

เป็นการอธิบายเหตุผลและสาเหตุของปัญหา ซึ่งกลยุทธ์นี้ควรใช้เมื่อเหตุการณ์ความรุนแรงเกิดขึ้นในช่วงแรก และเป็นการอธิบายสั้น ๆ เพื่อป้องกันการเกิดข่าวลือและรักษาภาพลักษณ์ความน่าเชื่อถือขององค์กร

2. กลยุทธ์แบบตอบโต้กลับ

เป็นวิธีที่ใช้ตอบโต้ผู้ที่กระทำผิด การใช้กลยุทธ์นี้ต้องทราบรายละเอียดอย่างชัดเจนว่าผู้ที่กระทำผิดเป็นใคร สร้างความเสียหายส่วนใดกับองค์กรบ้าง รวมถึงการฟ้องร้องคดีตามกฎหมาย

3. กลยุทธ์การขออภัย/ขอโทษ

หากเหตุการณ์ที่เกิดขึ้นสืบเนื่องมาจากความบกพร่อง หรือความผิดพลาดขององค์กร จนทำให้ลูกค้าขององค์กรได้รับความเดือดร้อนในวงกว้าง ผู้บริหารควรพิจารณาการสื่อสารโดยการยอมรับความผิดพลาด พร้อมทั้งมาตรการดูแลผู้ที่ได้รับความเดือดร้อน การสื่อสารในกรณีนี้ต้องคำนึงถึงพันธกิจขององค์กร ที่มีต่อลูกค้า ต่อคู่ค้า และต่อสังคมด้วย เพื่อสร้างความเชื่อมั่นในระยะยาว

4. กลยุทธ์แบบปฏิเสธ

กลยุทธ์นี้ใช้กับสื่อมวลชนหรือบุคคลภายนอก ในบางครั้งองค์กรควรเลือกการปฏิเสธ การให้สัมภาษณ์หากพิจารณาแล้วว่าเหตุการณ์ที่เกิดขึ้นไม่ได้ส่งผลกระทบต่อสังคม หรือประชาชนในวงกว้าง และประเมินแล้วเหตุการณ์ที่เกิดขึ้นสามารถแก้ไขได้ หรือยังไม่มีข้อมูลสนับสนุนเพียงพอต่อการสื่อความกับสื่อสาธารณะ ซึ่งหากไม่มีข้อมูลเพียงพอการที่เลือกจะให้สัมภาษณ์อาจจะไม่เป็นผลดีต่อภาพลักษณ์องค์กรหรือหากให้ข้อมูลที่ผิดพลาดอาจจะทำให้เหตุการณ์รุนแรงขยายวงกว้างไปมากกว่าเดิมได้

5. กลยุทธ์การตลาดเอาใจลูกค้า

ในกรณีเหตุการณ์ที่เกิดขึ้น สร้างความเสียหายให้กับลูกค้าโดยได้รับผลกระทบในการทำธุรกรรมทางการเงิน เกิดความเสียหายต่อธุรกิจ หรือทรัพย์สิน องค์กรได้พิจารณาการชดเชยความเสียหายให้ลูกค้า ซึ่งสิ่งเหล่านี้จำเป็นอย่างยิ่งที่จะต้องสื่อสารให้ลูกค้าและประชาชนทราบ เพราะเป็นการแสดงความรับผิดชอบอย่างเป็นรูปธรรม

นอกจากกลยุทธ์ในการสื่อความที่ต้องมีการกำหนดและเตรียมการไว้แล้วนั้น องค์กรจำเป็นต้องมีการกำหนดผู้ให้ข่าวกับสื่อมวลชน (Spokesperson) และรูปแบบและช่องทางการสื่อสารที่เหมาะสมที่ต้องการสื่อความ ไม่ว่าจะเป็นการให้สัมภาษณ์หรือการแถลงข่าว ผ่านการ Phone in การเขียนข่าวลงโซเชียลมีเดีย การโต้ตอบกับสื่อผ่านช่องทางโทรทัศน์ เป็นต้น รวมถึงการเตรียมการร่างข้อความที่เป็นข้อความพื้นฐานไว้ (pre-message) ในแต่ละกรณีเพื่อให้การตอบสนองและการรับมือทันเวลาต่อเหตุการณ์ที่เกิดขึ้น

งานบริการด้านคำแนะนำและแจ้งเตือนภัยไซเบอร์ให้กับสมาชิก

เอกสาร Technical recommendation (TR Document)

เอกสาร Technical recommendation (TR Document) เป็นเอกสารที่เกี่ยวกับคำแนะนำด้านเทคนิคในการรับมือกับเหตุการณ์โจมตีทางไซเบอร์ โดยได้มีการสรุปรายงานในที่ประชุมสมาชิกทั้งหมด 30 เรื่อง ดังนี้

ลำดับ	หัวข้อ
1	Vulnerability exploited to distribute StealthLoader malware
2	Log4shell report: Attacks tracked by state-sponsored groups
3	New Khonsari ransomware and Orcus RAT
4	Lazarus report: the two TigerDownloader and TigerRAT families discovered
5	AsyncRAT signaling take advantage of new distribution techniques
6	Lazarus reporting: Used Windows Update client and GitHub
7	LockBit report: released a version of the ransomware for Linux systems and VMware ESXi servers
8	Log4Shell exploitation series
9	Russian and Ukrainian cyberwarfare
10	New Destructive Malware Used In Cyber Attacks on Ukraine
11	IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine
12	Russian and Ukrainian cyberwarfare (Continue)
13	Caketap rootkit by UNC2891 targets banks
14	Malware Campaigns are targeting African Banking Sector (RemcosRAT)
15	North Korean State-Sponsored APT Targets Blockchain Companies
16	Hackers exploiting Spring4Shell vulnerability to deploy Mirai Botnet Malware
17	Exploitation of F5 BIG-IP iControl REST (CVE-2022-1388)
18	Grandoreiro Banking Malware resurfaces for tax season
19	Lazarus hackers attack VMware servers using Log4Shell exploits
20	CVE 2017-11882 attack alert from CSIRT-NBU (Computer Security Incident Response Team of the National bank of Ukraine)
21	CVE-2022-30190 (Follina) Microsoft Support Diagnostic Tool (MSDT) in Windows vulnerability
22	Black Basta ransomware operators expand their attack arsenal with QakBot Trojan and PrintNightmare exploit
23	Pegasus spyware operator (zero-click exploits)
24	LockBit 3.0 attack on a service industry organization in Mexico
25	LockBit 3.0 ransomware attack
26	Cisco hacked by Yanluowang ransomware gang
27	Critical vulnerability for Microsoft Exchange in active exploitation (Zero-day)
28	LockBit 3.0 Ransomware Distributed via Word Documents
29	OPERA1ER APT
30	Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7

Cybersecurity Alerts to members

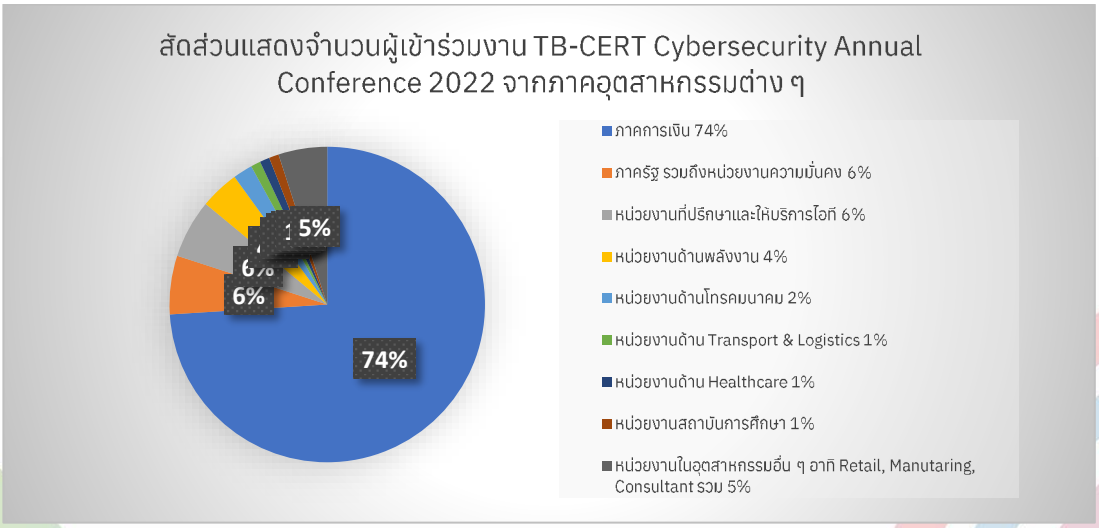
แจ้งเตือนให้สมาชิกรับทราบข่าวสารอย่างรวดเร็วเพื่อนำไปวิเคราะห์และเตรียมป้องกันภัยไซเบอร์ได้อย่างทันท่วงทีทั้งหมด 5 หัวข้อ ดังนี้

ลำดับ	หัวข้อ
1	การแจ้งเตือนภัยคุกคามทางไซเบอร์ (Hive Ransomware)
2	แจ้งเตือนพบความพยายามโจมตีผ่านทางช่องโหว่ระบบ VMware Digital Work Space (CVE-2022-22954)
3	ข้อมูล IoC ที่มีการ Exploit F5 BIG-IP (CVE-2022-1388)
4	ข้อมูล IoC ช่องโหว่ Follina ของผลิตภัณฑ์ Microsoft (CVE-2022-30190)
5	ข้อมูล IoC ของปฏิบัติการ Pegasus operator (zero-click exploits)

งานด้านการสร้างความตระหนักรู้ด้านไซเบอร์ให้กับภาคประชาชน

งานสัมมนาประจำปี
TB-CERT Cybersecurity Annual Conference 2022

เมื่อวันที่ 22 กันยายน 2022 TB-CERT ได้จัดงานสัมมนาประจำปี TB-CERT Cybersecurity Annual Conference 2022 ภายใต้หัวข้อหลัก “Next Chapter of Building trust and collaboration” ณ โรงแรม The Athenee Hotel, a Luxury Collection Hotel, Bangkok โดยมีวัตถุประสงค์หลักเพื่อเสริมสร้างความรู้ความเข้าใจในเรื่องการเตรียมพร้อมรับมือและตอบสนองต่อภัยไซเบอร์ที่เกิดขึ้นได้อย่างยืดหยุ่นและมั่นคง พร้อมกันนี้ยังช่วยพัฒนาทักษะบุคลากรของธนาคารสมาชิกให้มีทักษะในเชิงเทคนิคอีกด้วย สำหรับหัวข้อหลัก “Next Chapter of Building trust and collaboration” มีนัยสำคัญที่ต้องการสื่อความในงานนี้คือ แม้ว่าสถานการณ์การแพร่ระบาดโควิดจะบรรเทาลงบ้างแล้ว แต่ได้ก่อให้เกิดการเปลี่ยนแปลงด้านสภาพแวดล้อมการทำงาน สภาพความเสี่ยง ความมั่นคงปลอดภัยทางไซเบอร์ ทักษะความรู้ที่จำเป็นต่อการดำรงชีวิตและการทำงาน การปรับตัวต่อการเปลี่ยนแปลงดังกล่าวถือว่าเป็นบทพิสูจน์ใหม่ของมนุษย์ในการที่จะก้าวข้ามการเปลี่ยนแปลงครั้งสำคัญนี้ ซึ่งความร่วมมือของภาคส่วนต่าง ๆ และความเชื่อมั่นต่อกันในการสร้างความร่วมมือจะเป็นสิ่งสำคัญในการดำเนินงานและก้าวผ่านอุปสรรคหรือความท้าทายที่เกิดขึ้น กลุ่มเป้าหมายหลักของงานสัมมนาในครั้งนี้ ได้แก่ 1. หน่วยงานสมาชิก TB-CERT 2. หน่วยงานภายใต้สมาคมธนาคารไทย สมาคมธนาคารนานาชาติ และสมาคมสถาบันการเงินของรัฐ 3. หน่วยงานภายใต้บันทึกข้อตกลงความร่วมมือด้านไซเบอร์ภาคการเงิน การลงทุน และการประกันภัย ได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) และ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. 4. กลุ่มอุตสาหกรรมอื่น ๆ ในประเทศไทย เช่น หน่วยงานความมั่นคง อุตสาหกรรมด้านพลังงาน อุตสาหกรรมด้านการคมนาคม องค์กรจากต่างประเทศ และ อื่น ๆ ซึ่งมีผู้เข้าร่วมงานทั้งหมด 418 คน แบ่งเป็นผู้เข้าร่วมงานจากภาคอุตสาหกรรมต่าง ๆ ดังนี้



นอกจากนี้ ภายในงานยังได้รับเกียรติกล่าวเปิดงานจากคุณสิริธิดา พนมวัน ณ อยุธยา ผู้ช่วยผู้ว่าการสายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย ซึ่งมีผู้แทนสมาคมธนาคารไทย ได้แก่ คุณชาติศิริ โสภณพนิช ที่ปรึกษาสมาคมธนาคารไทย และกรรมการผู้จัดการใหญ่ ธนาคารกรุงเทพ กล่าว Welcome Note ภายใต้หัวข้อ “Next Chapter of Building trust and collaboration” มีเนื้อหาดังนี้

Welcome Note
Mr. Chartsiri Sophonpanich, President Bangkok Bank,
Advisor to The Thai Bankers' Association
“TB-CERT Cybersecurity Annual Conference 2022”
The Next Chapter of Building Trust and Collaboration
Venue: The Athenee Hotel, a Luxury Collection Hotel, Bangkok
Date: September 22, 2022 Time: 9:00-9:10am

Bank of Thailand Assistant Governor, Khun Siritida Panomwon Na Ayudhya,

Distinguished guests,

Ladies and gentlemen,

Good morning

It is my great honor to welcome participants from many countries, representatives from Thailand's critical information infrastructure organizations, defense, telecommunications, energy, and all banking members to this TB-CERT Cybersecurity Annual Conference 2022.

First, may I thank the guests of honor, partners, and the speakers for taking part in this event. I would also like to thank all of you for participating. I hope that you are looking forward to learning from each other and gaining new insights into the critical issues we will discuss as much as I am.

This is the 5th year that we are holding our major annual conference. While the Covid pandemic has started to ease; working environments, risk conditions and the cybersecurity space, along with the knowledge and skills needed to drive future innovation, continue to evolve.

Adapting to such changes presents us with a new challenge, one which requires us all to reflect on how we can more effectively collaborate with each other and build trust with stakeholders throughout this great transformation. As we come together today under the theme of **'The Next Chapter of Building Trust and Collaboration'** I would like to mention three key areas for us to focus on.

First, Thailand and the rest of the world is undergoing a rapid digital transformation driven by the adoption of technologies that deliver convenient services to customers while increasing business efficiency. However, this transformation has seen a corresponding rise in digital fraud and cybercrime, the combatting of which requires us to remain vigilant and implement clear workflows for mitigating such issues.

Second, it is key that we do not see cyber threats as an IT issue. Responsibility for managing these threats lies with multiple departments and teams. On the macro level, we must work together through cross-industry organizations including those focused on Thailand's critical information infrastructure.

Third, our combined success depends on us all working hard to develop, strengthen and enhance competency and skills of our cybersecurity teams so they can adapt to the ever-changing spectrum of cyber threats.

This conference is one of the largest cybersecurity conferences organized by the financial sector. We are privileged to have experts from leading organizations share their experiences with us throughout the event. We also have a cyber combat session to serve and enhance our skills and provide network opportunities for our cyber security people. This time we have expanded the cooperation to include the defense, energy, and telecommunications sectors. I do hope that this conference will also help increase public awareness of cyber security and enable us to collaborate more closely on this very important subject.

I'd like to take this opportunity to express my gratitude to the Bank of Thailand, the Thai Bankers' Association and MITRE and offer special thanks to all other sponsoring and supporting organizations. Your consistent support is the foundation for the success of this conference.

Thank you.

ประมวลภาพการจัดงาน TB-CERT Cybersecurity Annual Conference 2022

1. Welcome Speech

Khun Chartsiri Sophonpanich, Advisor, Thai Bankers' Association and President, Bangkok Bank

2. Opening Remarks

Khun Siritida Panomwon Na Ayudhya, Assistant Governor, Payment Systems Policy and Financial Technology Group, Bank of Thailand

3. Keynote: Taking MITRE's ATT&CK to the Next Level

Khun Barbara A Grewe, Director of International Strategy and Policy, MITRE

4. Panel Discussion: Privacy, Security, and Unfairness in adopting emerging technologies

Moderator: Khun Pipoauh Poomkaewkra, News Anchor Nation TV22

Panelist:

1.Khun Barbara A Grewe, Director of International Strategy and Policy, MITRE

2.Khun Chatchawat Asawarakwong, Chairman, Thailand Banking Sector CERT

3.Khun Kritiyanee Buranatrevedhya, Partner, Baker&McKenzie Limited Attorneys at Law, Bangkok

5. Closing

Dr. Kitti Kosavisutte, Honorary Advisor and Committee, TB-CERT

งาน BOT Digital Finance Conference 2022

TB-CERT ได้เข้าร่วมแสดงบูธเพื่อเผยแพร่ข้อมูลและสร้างความตระหนักด้านภัยไซเบอร์ให้กับภาคประชาชนภายในงาน BOT Digital Finance Conference 2022 จัดโดยธนาคารแห่งประเทศไทย ระหว่างวันที่ 27-29 ตุลาคม 2022 ณ ศูนย์การเรียนรู้ ธนาคารแห่งประเทศไทย โดยได้จัดแสดงงานที่มีเนื้อหาในการสร้างความตระหนักด้านการรักษาข้อมูลส่วนบุคคลของประชาชน

งานวิทยากรเผยแพร่ความรู้ในงานสัมมนา และสื่อต่าง ๆ

1. ร่วมเป็นวิทยากรหัวข้อ “การยกระดับมาตรฐาน CII ตาม พ.ร.บ.ไซเบอร์”

เมื่อวันที่ 13 มกราคม 2022 ดร.กิตติ โฆษะวิสุทธิ์ ที่ปรึกษากิตติมศักดิ์และกรรมการ TB-CERT ร่วมเป็นวิทยากรบรรยายในหัวข้อ “การยกระดับมาตรฐาน CII ตาม พ.ร.บ.ไซเบอร์” ในงานสัมมนาออนไลน์ Cybersecurity Knowledge Sharing ครั้งที่ 13 จัดโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้ความรู้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและผู้ที่สนใจเกี่ยวกับบทบาทและความสำคัญของหน่วยงาน CII ต่อภัยไซเบอร์

2. ร่วมเสวนาในหัวข้อ “เปิดมุมมองความปลอดภัยไซเบอร์ 2022”

วันที่ 30 มีนาคม 2022 คุณชัชวัฒน์ อัศวรักวงศ์ ประธานกรรมการ TB-CERT ร่วมเสวนาในงานสัมมนา “ไทยกับความปลอดภัยไซเบอร์ 2022” โดยมติชนออนไลน์ ในการเสวนาหัวข้อ “เปิดมุมมองความปลอดภัยไซเบอร์ 2022” ร่วมกับวิทยากรผู้เชี่ยวชาญทั้งภาครัฐและเอกชน

3. ร่วมบรรยายในงานสัมมนาออนไลน์หัวข้อ “บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของการทำ Digital Transformation ภาคธนาคาร”

วันที่ 28 เมษายน 2022 คุณประกลกฤษ แสงชูวงศ์ กรรมการด้านวิชาการ TB-CERT ร่วมเป็นวิทยากรบรรยายในหัวข้อ “การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของการทำ Digital Transformation ภาคการธนาคาร” ภายในงาน TTT Virtual Summit: Enterprise Cybersecurity 2022 โดย TechTalkThai โดยได้กล่าวถึงแนวทางการประเมินความเสี่ยงและการวางแผนการรับมือกับความเสี่ยงในด้านต่าง ๆ ทั้งการพัฒนาแอปพลิเคชัน การปรับไปใช้ระบบคลาวด์ การคุ้มครองข้อมูลส่วนบุคคล และการป้องกันภัยคุกคามไซเบอร์ รวมไปถึงแนวทางปฏิบัติ กรอบการทำงาน และมาตรฐานที่ควรนำมาประยุกต์ใช้เพื่อให้ภาคธนาคารสามารถทำ Digital Transformation ได้อย่างมั่นคงปลอดภัย

---

4. ร่วมเสวนาในหัวข้อ: Digital Fraud & Cyber Crime ในงาน Privacy Security Summit

วันที่ 25 พฤษภาคม 2022 คุณชัชวัฒน์ อัศวรักวงศ์ ประธานกรรมการ TB-CERT ร่วมเสวนาในหัวข้อ “Digital Fraud & Cyber Crime” ภายในงาน Privacy Security Summit ที่ทางสมาคมผู้ใช้ดิจิทัลไทย (DUGA) เป็นผู้จัดงานขึ้น โดยเสวนาร่วมกับคุณวรุณ กาญจนภู รองเลขาธิการสมาคมธนาคารไทย โดยมีคุณยศ กิมสวัสดิ์ ประธานสำนักงานระบบการชำระเงินสมาคมธนาคารไทยเป็นผู้ดำเนินรายการ ซึ่งได้เล่าเรื่องราว และตัวอย่างเหตุการณ์ภัยที่ได้ประสบพบเจอแก่ผู้เข้าร่วมรับฟังรวมถึงสร้างความเข้าใจเกี่ยวกับการทุจริต ฉ้อโกง ทางโลกดิจิทัลและอาชญากรรมทางไซเบอร์

---

5. ร่วมเสวนาในการจัดกิจกรรม Capacity Building NCSA และ CERT CII Cyber Training

วันที่ 6 มิถุนายน 2022 คุณสมบูรณ์ หิรัญภัทรศิลป์ ผู้แทนคณะกรรมการ TB-CERT ร่วมเป็นวิทยากรเสวนาในการจัดกิจกรรม Capacity Building NCSA และ CERT CII Cyber Training โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ร่วมกับสถานทูตออสเตรเลียในการจัดกิจกรรมดังกล่าว เพื่อส่งเสริมให้เกิดการเรียนรู้แนวทางหรือเทคนิควิธีการต่าง ๆ ทั้งภาคทฤษฎี และภาคปฏิบัติ เช่น การรับมือและการจัดการกับภัยคุกคาม การโจมตี ทักษะด้านเทคโนโลยี ด้านสถาปัตยกรรมและการออกแบบระบบด้านการจัดการความเสี่ยง เป็นต้น

6. ร่วมบรรยายในหัวข้อ “แนวโน้มภัยคุกคามไซเบอร์และการป้องกันสำหรับภาคธนาคาร”

เมื่อวันที่ 28 พฤศจิกายน 2022 คุณภคพงศ์ จุลวงศาศิลป์ กรรมการ TB-CERT ร่วมเป็นวิทยากรบรรยายในหัวข้อ “แนวโน้มภัยคุกคามไซเบอร์และการป้องกันสำหรับภาคธนาคาร” ภายในงานสัมมนา “NCSA Virtual Summit #1” จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ร่วมกับ TechTalkThai เพื่ออัปเดตแนวโน้มภัยคุกคามและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ล่าสุดสำหรับหน่วยงาน CII และองค์กรธุรกิจ รวมถึงบทเรียนต่าง ๆ จากการที่ PDPA บังคับใช้มาแล้วกว่า 6 เดือน โดยได้กล่าวถึงแนวโน้มภัยคุกคามไซเบอร์ภาคการธนาคารที่เกิดขึ้นในช่วงปี 2022 โดยเฉพาะเรื่องแก๊ง Call Center ที่กำลังเป็นประเด็นร้อนในปัจจุบัน พร้อมแชร์กลยุทธ์การป้องกันและรับมือทั้งในส่วนที่ดำเนินโดยภาคการธนาคารเอง และคำแนะนำในการป้องกันตัวเองสำหรับประชาชนทั่วไป รวมถึงสรุปกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ที่ TB-CERT ได้ดำเนินการในช่วงปีที่ผ่านมา

งานเอกสารเผยแพร่เพื่อสร้างความตระหนักรู้ให้กับภาคประชาชน (Public Awareness)

จัดทำเอกสารเพื่อสร้างความตระหนักรู้ให้กับภาคประชาชนได้เข้าใจภัยคุกคามทางด้านไซเบอร์ในรูปแบบต่าง ๆ เป็นประจำซึ่งได้เผยแพร่ผ่าน TB-CERT Facebook (https://www.facebook.com/TBCERT.Official) และเว็บไซต์สมาคมธนาคารไทย (https://www.tba.or.th/pso-tb-cert/tb-cert/) โดยในปี 2022 ได้จัดทำทั้งสิ้นจำนวน 15 เรื่อง ดังนี้

ลำดับ	เรื่อง	วันที่เผยแพร่
1	เตือนภัยแก๊งคอลเซ็นเตอร์โทรหลอกลวงให้โอนเงิน	24 Jan 2022
2	คนไทยรวมพลัง รับมือแก๊งคอลเซ็นเตอร์หลอกลวง	29 Jan 2022
3	6 สิ่งที่ต้องทำ เมื่อข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ	21 Feb 2022
4	Fake News รับมืออย่างไร	7 Mar 2022
5	รู้ยัง มุกใหม่ ของแก๊งคอลเซ็นเตอร์	26 Apr 2022
6	หลักการกลโกงครั้งใหม่ (ภาค 1) มิจฉาชีพเห็นช่องทางนี้ในการหลอกลวงได้อย่างไร มาดูกัน	23 May 2022
7	หลักการกลโกงครั้งใหม่ (ภาค 2) ของเหล่าแก๊งคอลเซ็นเตอร์กับมือถือ Android	25 May 2022
8	เอ๊ะ! สักนิดก่อนคิดจะสแกน หลักการคิดง่ายๆ เพื่อให้คุณเอ๊ะ! ก่อนตกเป็นเหยื่อมิจฉาชีพ	14 Jun 2022
9	QR Code ปลอม หรือ Fake QR Code คืออะไร	7 Jul 2022
10	เช็คง่าย ๆ ว่า Slip ที่เราได้มานั้น จริงหรือปลอม	1 Aug 2022
11	รู้ทันและรับมือ Pegasus Spyware	3 Aug 2022
12	รู้ไว้ปลอดภัยห่างไกลแก๊งมิจฉาชีพ-1	27 Sep 2022
13	รู้ไว้ปลอดภัยห่างไกลแก๊งมิจฉาชีพ-2	27 Sep 2022
14	3 ส. เตือนใจ ระวังภัย SMS Phishing	8 Dec 2022
15	ภัยรูปแบบใหม่ของมิจฉาชีพที่ส่ง SMS ด้วยชื่อคล้ายหรือชื่อเดียวกับองค์กรฯ	24 Dec 2022

งานด้านการสร้างความร่วมมือ

การสร้างความร่วมมือกับ CERT ในประเทศไทย

สืบเนื่องจาก พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ 2562 เขียนบัญญัติไว้ว่าจะต้องมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไว้ในมาตรา 50 เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ TB-CERT ซึ่งถูกกำหนดโดยธนาคารแห่งประเทศไทยให้เป็นศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับภาคการธนาคาร ได้หารือกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือ สกมช. จัดให้มีการประชุมหารือและสร้างเครือข่ายผู้ประสานงานในการรับมือกับภัยคุกคามทางไซเบอร์ โดยจัดให้มีการพบปะและประชุมกันทุก ๆ เดือน เพื่อสร้างความสัมพันธ์และแลกเปลี่ยนความรู้ทางเทคนิคกันกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ที่จัดตั้งขึ้นจากภาคอุตสาหกรรมอื่น ๆ เช่น ภาคตลาดทุน ภาคประกันภัย ภาคโทรคมนาคม ภาครัฐ เป็นต้น การสร้างความรู้จักกันและสานสัมพันธ์เช่นนี้จะช่วยให้เมื่อเกิดภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อเป็นวงกว้างนอกอุตสาหกรรมของภาคการธนาคาร สามารถรับมือกับเหตุการณ์ที่เกิดขึ้นได้รวดเร็วยิ่งขึ้น เกิดการช่วยเหลือซึ่งกันและกัน และการสร้างความร่วมมืออันดีนี้จะส่งผลให้เกิดการรับมือกับมิจฉาชีพได้อย่างเป็นรูปธรรมและยั่งยืนให้กับประเทศไทย



การสร้างความร่วมมือกับหน่วยงาน
ภายใต้บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย

TB-CERT ภายใต้สมาคมธนาคารไทย ได้มีการลงนามบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย เมื่อวันที่ 22 กันยายน 2016 ร่วมกับ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ร่วมกันจัดกิจกรรมภายใต้แผนการดำเนินงานตามข้อตกลงและขอบเขตของความร่วมมือเพื่อส่งเสริมและสนับสนุนระหว่างกันในด้านการรับมือภัยคุกคามทางไซเบอร์ ดังนี้

1. การจัดงานสัมมนาด้านความมั่นคงปลอดภัยไซเบอร์สำหรับคณะกรรมการขององค์กรภาคการเงิน (Cyber Resilience Leadership 2022)

เมื่อวันที่ 30 พฤศจิกายน 2022 สมาคมธนาคารไทย ร่วมกับ ธปท. สำนักงาน ก.ล.ต. และสำนักงาน คปภ. จัดงานสัมมนาด้านความมั่นคงปลอดภัยไซเบอร์ให้กับคณะกรรมการขององค์กรภาคการเงิน (Cyber Resilience Leadership 2022) หรือ Board Awareness โดยมีวัตถุประสงค์เพื่อสนับสนุนให้คณะกรรมการขององค์กรภาคการเงิน มีความรู้และตระหนักรู้ภัยคุกคามไซเบอร์ รวมทั้งเพิ่มโอกาสในการแลกเปลี่ยนมุมมองภัยคุกคามไซเบอร์ระหว่างองค์กร และสามารถนำไปปรับใช้ในการกำกับดูแลการบริหารจัดการความเสี่ยงของแต่ละองค์กร มีผู้เข้าร่วมงานได้แก่ คณะกรรมการและผู้บริหารระดับสูงจากภาคการธนาคาร ตลาดทุน และการประกันภัย จำนวน 300 คน จากการจัดอบรมจำนวน 2 ครั้ง ครั้งละ 0.5 วัน (รอบเช้าและรอบบ่าย)

กล่าวเปิดงานภาคเช้า โดยคุณรื่นวดี สุวรรณมงคล
เลขาธิการ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

กล่าวเปิดงานภาคบ่าย โดยคุณสิริธิดา พนมวัน ณ อยุธยา
ผู้ช่วยผู้ว่าการ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
ธนาคารแห่งประเทศไทย

2. การจัดโครงการ Cybersecurity for New Gen in Financial Sector

สมาคมธนาคารไทย ร่วมกับ ธปท. สำนักงาน ก.ล.ต. และสำนักงาน คปภ. ดำเนินการตามแผนงานโครงการ Cybersecurity for New Gen in Financial Sector ซึ่งมีวัตถุประสงค์เพื่อสื่อสารและผลักดันให้คนรุ่นใหม่เห็นความสำคัญของงานด้าน Cybersecurity ในภาคการเงิน รวมถึงให้ความรู้ใหม่ ๆ ผ่านช่องทางออนไลน์ โดยมีกลุ่มเป้าหมายคือ นิสิต นักศึกษา ที่กำลังจะเรียนจบระดับอุดมศึกษา ให้รู้จักภาคการเงินว่ามีงานแบบใดบ้าง ต้องมีความรู้ ทักษะใดบ้างในด้าน IT Security และ Cybersecurity เป็นการนำเสนอสายงานด้าน IT และ Cybersecurity ในหน่วยงานของภาคการเงิน ตั้งแต่ 1st, 2nd , 3rd Line ผ่านการจัดทำวิดีโอคลิปโดย Influencer (beartai) ในหัวข้อ “เปิดโลกงานด้าน IT และ Cyber Security ที่ภาคการเงินอยากได้ตัว” เผยแพร่เมื่อวันที่ 15 ธันวาคม 2022 ซึ่งมีผู้สนใจรับชมคลิปมากกว่า 100,000 ครั้ง ทั้งจากแพลตฟอร์ม Facebook และ YouTube และทำให้มีผู้เข้าถึงและติดตามข่าวสารจาก Facebook page ของโครงการ (Fincybersec Thailand) มากขึ้น

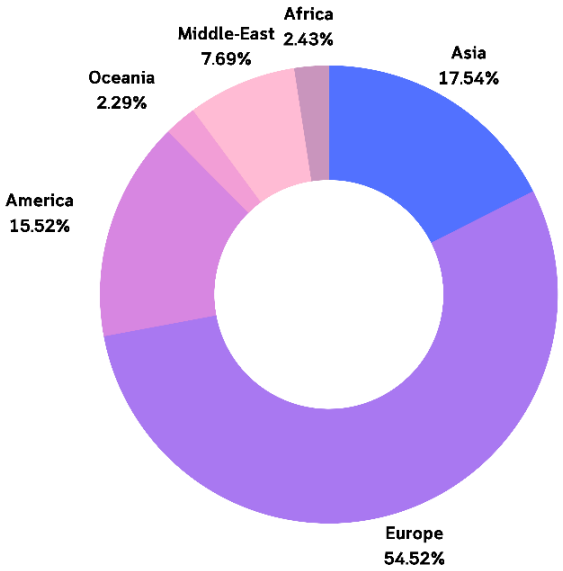
Reference: https://www.facebook.com/beartai/videos/1363752954453126/

https://www.youtube.com/watch?v=hiHY2mtIzC0

ภาพรวมและสถิติภัยคุกคามทางไซเบอร์ในปี 2022

ภาพรวมและสถิติภัยคุกคามทางไซเบอร์ในปี 2022

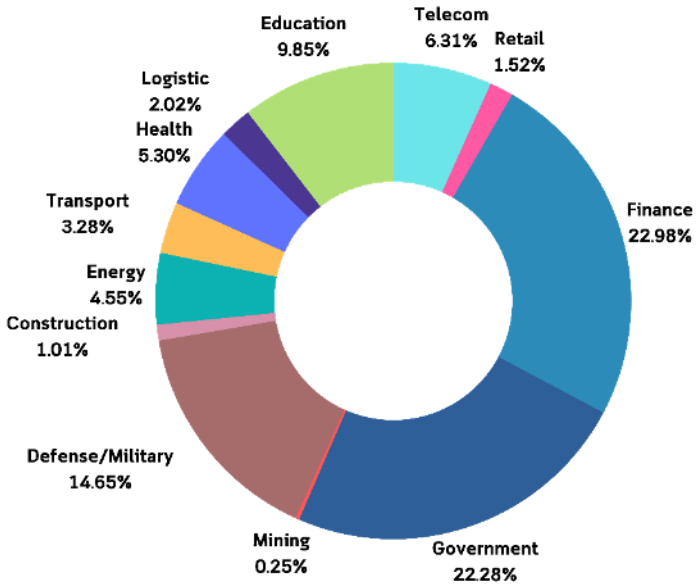
ในปี 2022 ทีมงาน TB-CERT ได้รวบรวมสถิติภัยคุกคามทางไซเบอร์ จากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence หรือ CTI) ของ TB-CERT จากข้อมูลพบว่าภูมิภาคยุโรปเป็นภูมิภาคของโลกที่ถูกโจมตีในปี 2022 มากเป็นอันดับ 1 คิดเป็นสัดส่วน 54.52% รองลงมาเป็นภูมิภาคเอเชีย เป็นสัดส่วน 17.54% และภูมิภาคอเมริกาเป็นสัดส่วน 15.52% ตามลำดับ ดังรูปที่ 1 จากตัวเลขสถิติดังกล่าวมีความสอดคล้องกับสถานการณ์สงครามระหว่างรัสเซีย-ยูเครน ที่เกิดโจมตีทางไซเบอร์หลายประเทศในภูมิภาคยุโรป



รูปที่ 1 แสดงอัตราส่วนจำนวนภัยคุกคามทางไซเบอร์ตามภูมิภาคโลกที่ถูกโจมตีในปี 2022

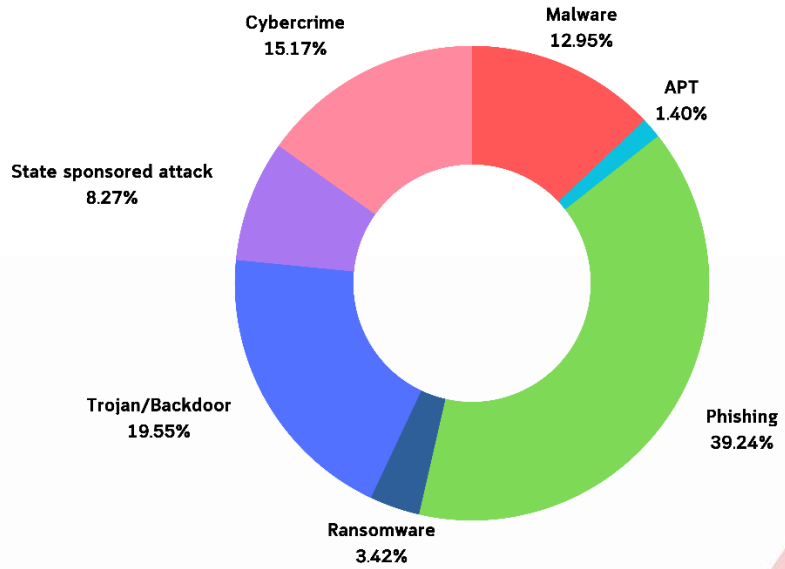
จากสถิติภัยคุกคามทางไซเบอร์แบ่งตามประเภทอุตสาหกรรมในปี 2022 พบว่าภาครัฐหรือหน่วยงานของรัฐเป็นเป้าหมายอันดับ 1 คิดเป็นสัดส่วน 28.28% ซึ่งภาครัฐเองก็ยังเป็นเป้าหมายสำคัญที่กลุ่มคนร้ายมุ่งโจมตีเป็นอันดับแรก โดยปัจจัยสำคัญคือเรื่องความขัดแย้งระหว่างประเทศและมีความเกี่ยวข้องกับความขัดแย้งระหว่างรัสเซีย-ยูเครน รวมถึงการโจมตีที่ได้รับการสนับสนุนจากรัฐของประเทศคู่ขัดแย้ง (State-sponsored attack) โดยพบว่าการโจมตีที่ได้รับการสนับสนุนจากรัฐนั้นส่วนใหญ่จะเป็นการโจมตีรูปแบบ DDoS และ Malware เพื่อทำลายบริการและข้อมูลที่สำคัญของที่ฝ่าย [1] ส่วนในภาคการเงินนั้นพบเหตุการณ์การโจมตีมากเป็นอันดับ 2 คิดเป็นสัดส่วน 22.98% ซึ่งจากการวิเคราะห์ข้อมูลพบว่าจะเป็นการโจมตีในรูปแบบการหลอกฟิชชิง (Phishing) เป็นหลัก โดยมีแรงจูงใจในเรื่องการเงินที่กลุ่มผู้โจมตีคาดหวังว่าจะได้รับจากการโจมตีในภาคอุตสาหกรรมการเงินนั่นเอง ดังรูปที่ 2

[1] Cyber Peace Institute: cyberpeaceinstitute.org



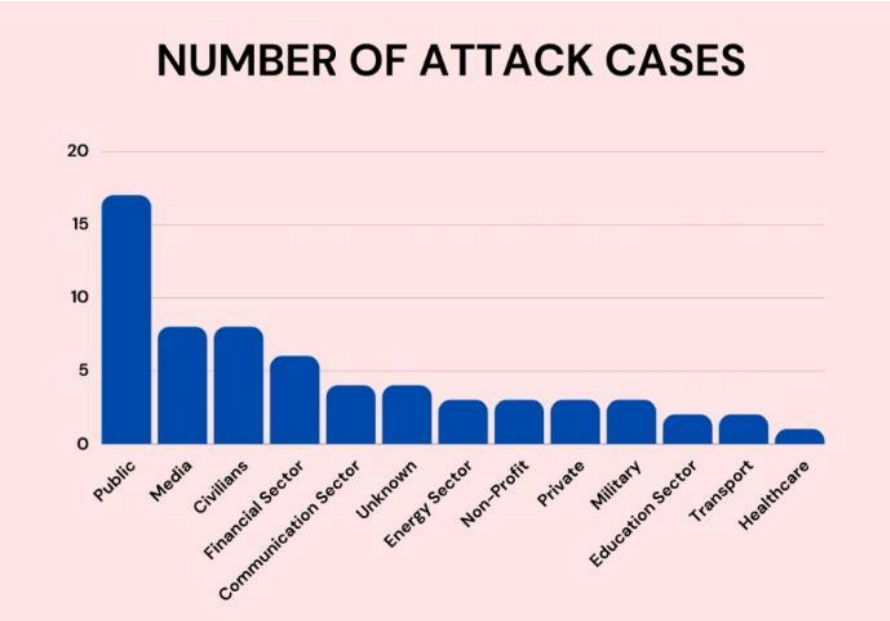
รูปที่ 2 แสดงอัตราส่วนจำนวนภัยคุกคามทางไซเบอร์แบ่งตามภาคอุตสาหกรรมทั่วโลกที่ถูกโจมตีในปี 2022

สถิติแบ่งตามประเภทของการโจมตีอันดับ 1 คือ ฟิชชิง (Phishing) ที่สัดส่วน 38.80% และลำดับถัดมาคือ Trojan/Backdoor ที่สัดส่วน 19.33% และ Cybercrime ที่สัดส่วน 15.00% ตามลำดับ ดังรูปที่ 3 ซึ่งประเภทการโจมตีสูงสุดที่พบคือ Phishing ที่มุ่งเน้นการโจมตีที่ระดับตัวบุคคลเป็นหลัก โดยเป็นการหลอกคนภายในองค์กรให้กรอกรหัสผ่าน หรือหลอกติดตั้งโปรแกรมประสงค์ร้ายที่สอดคล้องกับสถิติที่พบประเภทการโจมตี Trojan/Backdoor ที่เป็นอันดับ 2 โดยการโจมตีทั้ง 2 ประเภทนี้ก็เพื่อขยายผลการโจมตีไปยังระบบสำคัญขององค์กรต่อไป



รูปที่ 3 แสดงอัตราส่วนจำนวนภัยคุกคามทางไซเบอร์แบ่งตามประเภทของการโจมตีในปี 2022

สำหรับสถานการณ์ความขัดแย้งระหว่างรัสเซีย-ยูเครน จากการรวบรวมข้อมูลรูปแบบการใช้การโจมตีทางไซเบอร์ในช่วงสถานการณ์ดังกล่าว ซึ่งน่าจะเป็นประโยชน์สำหรับการเตรียมความพร้อมในการรับมือหรือเพื่อเป็นข้อมูลประกอบสำหรับนำไปเป็นส่วนหนึ่งของข้อมูลข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence) ในช่วงต้นของความขัดแย้งนั้นการโจมตีจะมุ่งเน้นไปที่ public sector และบริการด้านพลเรือน (civilians) ของทั้งสองฝ่าย เพื่อที่จะพยายามขัดขวางการให้บริการของภาครัฐรวมถึงการลดความน่าเชื่อถือของรัฐของฝ่ายตรงข้าม และสร้างผลกระทบต่อความเป็นอยู่ของพลเรือน แต่ที่น่าสังเกตคือมีการตั้งเป้าหมายไปที่ Media หรือหน่วยงานสื่อในช่วงเดือนมีนาคม หลังจากเหตุการณ์ความขัดแย้งได้ผ่านไปเดือนเศษ ซึ่งในช่วงดังกล่าวจะมีปฏิบัติการทางการข่าว (Information Operation) สูงขึ้นอย่างเห็นได้ชัด จะมีการปล่อยข่าวโจมตีกันจากทั้งสองฝ่าย สำหรับเป้าหมายการโจมตีที่พบในลำดับถัดไปคือ ด้านการเงินและภาคการโทรคมนาคม ซึ่งจะสอดคล้องกับการข่าวที่ออกในช่วงนั้น (รูปที่ 4)



รูปที่ 4 แสดงจำนวนเคสการโจมตีในแต่ละ sector ในช่วงเดือน มค.-เมย. 2022 ในสถานการณ์ความขัดแย้งรัสเซีย-ยูเครน

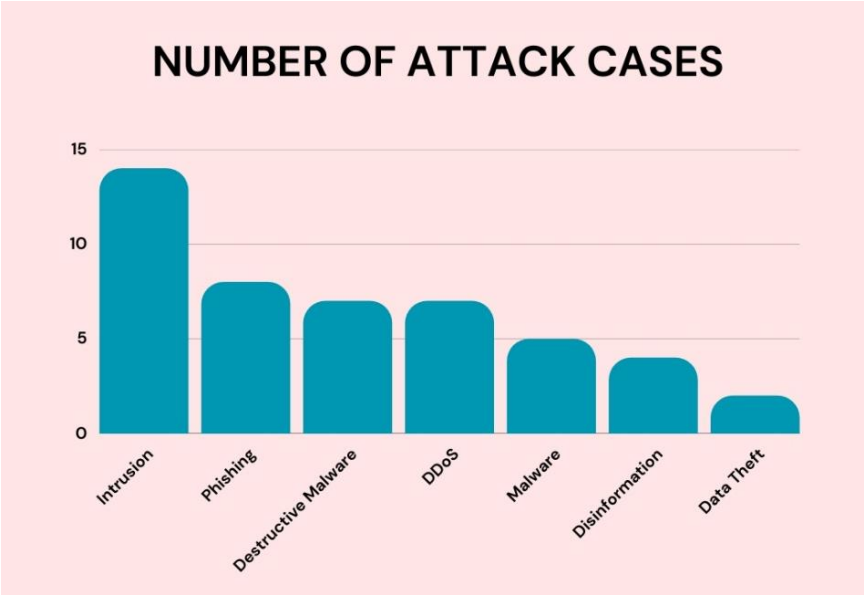
จากสถานการณ์ความขัดแย้งดังกล่าวหากวิเคราะห์สถิติของเทคนิคที่ใช้ในการโจมตี (รูปที่ 5) แล้ว ความพยายามในการเจาะระบบมีจำนวนมากซึ่งเป็นขั้นตอนเบื้องต้นเพื่อใช้ค้นหาช่องโหว่เพื่อที่จะดำเนินการในขั้นตอนการโจมตีถัดไป โดยทาง CISA-Cybersecurity & Infrastructure Security Agency, US ได้มีการรวบรวมช่องโหว่ที่ควรจะเฝ้าระวังเป็นพิเศษในช่วงเวลาดังนี้

Vulnerability Used in the Situation and Recommend Mitigation

1. CVE-2018-13379 FortiGate VPNs
2. CVE-2019-1653 Cisco router
3. CVE-2019-2725 Oracle WebLogic Server
4. CVE-2019-7609 Kibana

5. CVE-2019-9670 Zimbra software
6. CVE-2019-10149 Exim Simple Mail Transfer Protocol
7. CVE-2019-11510 Pulse Secure
8. CVE-2019-19781 Citrix
9. CVE-2020-0688 Microsoft Exchange
10. CVE-2020-4006 VMWare (note: this was a zero-day at time.)
11. CVE-2020-5902 F5 Big-IP
12. CVE-2020-14882 Oracle WebLogic
13. CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

ส่วนการใช้ Phishing จะพบได้ค่อนข้างเยอะ รวมถึงการใช้ malware ประเภทต่าง ๆ ในการโจมตีฝ่ายตรงข้ามซึ่งจะเป็นขั้นตอนต่อเนื่องกัน และที่น่าสังเกตและสัมพันธ์กับ Information Operation หรือการโจมตีด้านการข่าว นั่นคือการใช้ข้อมูลที่บิดเบือนความจริงในช่วงเวลาเดียวกันด้วย (disinformation)



รูปที่ 5 แสดงสถิติการโจมตีแบ่งตามเทคนิคที่ใช้ในการโจมตีในช่วงสถานการณ์ความขัดแย้ง

บทวิเคราะห์ภัยคุกคามทางไซเบอร์

วิวัฒนาการของภัยไซเบอร์ต่อ Mobile Banking Application

การใช้บริการทางการเงินมีแนวโน้มที่จะเพิ่มสูงขึ้นอย่างรวดเร็ว นอกจากแรงผลักดันจากสถานการณ์การระบาดของโควิดแล้ว โครงสร้างพื้นฐานของประเทศยังเอื้ออำนวยที่จะให้ทางเลือกกับผู้บริโภคในการจ่ายโอนด้วยโทรศัพท์มือถือได้โดยเว้นระยะห่างทางสังคมที่มาเสริมกันในจังหวะที่สอดรับกันพอดี นั่นทำให้ความนิยมในการใช้งาน Internet Banking ซึ่งเป็นการทำงานบน Browser เปลี่ยนมาเป็น Mobile Banking ซึ่งเป็นแอปพลิเคชันบริการทางการเงินบนโทรศัพท์มือถือกันมากขึ้น

ภาพรวมของระบบนิเวศ (Ecosystem) ของการให้บริการทางการเงินในยุคดิจิทัลนั้นจะประกอบไปด้วย

1. **ผู้ให้บริการทางการเงิน** ซึ่งประกอบด้วยธนาคารหรือหน่วยงานที่ไม่ใช่ธนาคารแต่ให้บริการทางการเงิน เช่น ให้บริการเงินกู้ ให้บริการกระเป๋าเงินอิเล็กทรอนิกส์ ผ่านแอปพลิเคชันบริการทางการเงิน (Mobile Banking Application)
2. **ผู้ให้บริการเครือข่าย** ซึ่งจะเป็นผู้ประกอบการที่ให้บริการอินเทอร์เน็ต (Internet Service Provider) หรือให้บริการเครือข่ายโทรศัพท์มือถือ (Mobile Operator) เพื่อที่จะให้ผู้ใช้งานสามารถทำธุรกรรมด้วย Mobile Banking Application บนโทรศัพท์มือถือและเชื่อมต่อมาที่บริการทางการเงินได้ในรูปแบบต่าง ๆ
3. **หน่วยงานกำกับดูแล** ซึ่งจะคอยกำกับดูแลเพื่อให้บริการทางการเงิน หรือบริการเครือข่าย เป็นไปอย่างมีคุณภาพและมีความมั่นคงปลอดภัย

ด้านความมั่นคงปลอดภัยของ Mobile Banking Application นั้น ในขั้นตอนกระบวนการพัฒนา Mobile Banking Application ธนาคารจะมีการประเมินความเสี่ยงต่าง ๆ ของ Mobile Banking Application โดยอ้างอิงมาตรฐานสากลต่าง ๆ เช่น OWASP Top 10 Mobile Risk 2016 ซึ่งมีรายละเอียดดังนี้

1. **Improper Platform Usage** คือ การที่ไม่ได้นำเอาแนวทางการพัฒนาด้านความมั่นคงปลอดภัยของแต่ละ platform มาใช้อย่างถูกต้อง ไม่ว่าจะเป็น Android, iOS หรือ Windows
2. **Insecure Data Storage** คือการจัดเก็บข้อมูลที่ไม่ปลอดภัยซึ่งจะทำให้มิจฉาชีพสามารถเข้าถึงข้อมูลส่วนบุคคลได้
3. **Insecure Communication** คือการส่งข้อมูลผ่านเครือข่ายสาธารณะที่ไม่ปลอดภัย ซึ่งจะทำให้มิจฉาชีพสามารถดักหรือขโมยข้อมูลสำคัญได้ในระหว่างที่มีการส่งข้อมูลข้ามเครือข่าย
4. **Insecure Authentication** คือการพิสูจน์ยืนยันตัวตนที่ไม่ปลอดภัยซึ่งจะทำให้มิจฉาชีพสามารถปลอมตัวหรือ bypass การพิสูจน์ยืนยันตัวตน หรือ แม้กระทั้งสามารถดักข้อมูลในกระบวนการพิสูจน์ยืนยันตัวตนเพื่อนำไปใช้ในการเข้าใช้ระบบแทนได้

5. **Insufficient Cryptography** คือความไม่เพียงพอของการเข้ารหัสซึ่งจะเกิดจากการ implement ไม่เป็นไปตามกระบวนการมาตรฐาน หรือ ใช้ algorithm ที่ไม่ปลอดภัย
6. **Insecure Authorization** คือการมอบสิทธิที่ไม่ปลอดภัยโดยเฉพาะสิทธิการใช้งานของผู้ดูแลระบบ ซึ่งจะทำให้มิจฉาชีพใช้สิทธิที่ไม่ได้รับอนุญาตหรือจะสามารถ bypass การควบคุมอื่น ๆ ได้
7. **Client Code Quality** คือโค้ดของซอฟต์แวร์ที่ไม่ได้คุณภาพ ซึ่งอาจจะมาจากการใช้โค้ดของ 3rd party หรือที่ไม่เข้าใจการพัฒนาโค้ดที่มีความปลอดภัยเช่นมี buffer overflow, memory leak เป็นต้น
8. **Code Tampering** คือความสามารถในการปรับเปลี่ยนโค้ดต้นฉบับเพื่อแทรกการทำงานอื่นหรือปรับเปลี่ยนการทำงาน API และ repackage ใหม่เพื่อเอาขึ้น store
9. **Reverse Engineering** คือวิธีการของมิจฉาชีพในการวิเคราะห์การทำงานของแอปพลิเคชัน เพื่อที่จะถอดรหัสโครงสร้างการควบคุมของแอปพลิเคชัน และนำไปวิเคราะห์แนวทางในการโจมตีเป้าหมายให้มีประสิทธิภาพ
10. **Extraneous Functionality** คือการคงเหลือฟังก์ชันที่ใช้สำหรับการพัฒนาไว้ในซอฟต์แวร์ใช้งานจริง ซึ่งฟังก์ชันเหล่านั้นอาจจะถูกค้นพบและมีช่องโหว่ที่จะถูกใช้โจมตีได้

นอกจากนั้น Mobile Banking Application ยังมีการตรวจจับ rooted/jailbreak และจะระงับการใช้งาน เนื่องจากจะเป็นอันตรายสำหรับผู้ใช้งานหากเครื่องมีการ rooted/jailbreak จะทำให้ความปลอดภัยของเครื่องในระดับพื้นฐานของระบบปฏิบัติการถูก bypass ได้ นอกจากนั้น TB-CERT ยังมีการสื่อความเป็นระยะ ให้ผู้ใช้งานมีการ upgrade OS และ Mobile Banking Application อยู่เป็นประจำ

จากการเฝ้าระวังการโจมตีทางไซเบอร์ยังไม่มีรายงานพบว่ามีการเจาะระบบสำเร็จ แต่อย่างไรก็ตาม TB-CERT ได้ศึกษาติดตามรูปแบบการหลอกลวงตลอดเวลาโดยพบว่ารูปแบบการหลอกลวงที่พบในตั้งแต่ช่วงของการใช้งาน Internet Banking จนถึงปัจจุบันจะมีขั้นตอนสำคัญดังนี้

1. **ขั้นตอนหลอกลวง ล่อเหยื่อ** ด้วยสภาพการติดต่อสื่อสารในปัจจุบันที่มีหลากหลายช่องทาง มิจฉาชีพมีการเตรียมเรื่องราวที่จะใช้ในการหลอกหรือชวนเชื่อ และจะพยายามติดต่อสื่อสารไปในหลาย ๆ ช่องทางไม่ว่าจะเป็นการโทรศัพท์ซึ่งจะเป็นกรณีที่เรียกกันว่าแก๊งคอลเซ็นเตอร์ หรือจะใช้ช่องทาง SMS ในการส่งข้อความ SMS ที่เชิญชวนให้กดลิงก์ หรือจะเป็นการติดต่อผ่านช่องทางโซเชียลมีเดีย แต่ทั้งนี้ทั้งนั้นการหลอกลวงที่จะได้ผลจะต้องมีการพูดคุยโต้ตอบเพื่อให้เหยื่อหลงเชื่อได้ง่าย พบว่าเมื่อเริ่มพูดคุยกับเหยื่อได้แล้วมักจะชวนให้เพิ่มชื่อใน Line ซึ่งเป็นช่องทางที่คนไทยส่วนใหญ่มีใช้กัน เพื่อที่จะได้พูดคุยโต้ตอบส่งข้อมูลเพื่อทำให้มีความน่าเชื่อถือและเชื่อได้ว่าเป็นของจริง โดยเทคนิคการหลอกเหยื่อนั้น มิจฉาชีพมักจะมีการเปลี่ยนเนื้อหาที่ใช้ เพื่อเกาะกระแสความสนใจและทำให้สังเกตแยกแยะได้ยากขึ้น ซึ่งจะเห็นได้จากข้อความที่ใช้จะเกี่ยวข้องกับภาษีในช่วงฤดูการยื่นภาษีบุคคลธรรมดา เป็นต้น

2. **ขั้นตอนหลอกให้ติดตั้งโปรแกรม** ขั้นตอนนี้เป็นขั้นตอนหลังจากที่เหยื่อเริ่มเชื่อว่าเป็นหน่วยงานจริงที่ติดต่อมา ก็จะหลอกขอข้อมูลเพิ่มเติมและหลอกให้เหยื่อติดตั้ง Mobile Application ปลอม ซึ่งเป็น

เครื่องมือที่มิจฉาชีพเตรียมเอาไว้สำหรับการดำเนินการในขั้นตอนถัดไป ในขั้นตอนการติดตั้งโปรแกรม มิจฉาชีพจะพยายามให้เหยื่อดำเนินการอนุญาตการติดตั้งโปรแกรม รวมถึงอนุญาต Permission ต่าง ๆ ตามที่มิจฉาชีพต้องการ โดยจะพยายามที่จะเบี่ยงเบนความสนใจด้วยการอธิบายว่าเป็นข้อมูลสำคัญ หรือเร่งรัดให้เหยื่อไม่ทันคิดและทำตามที่บอก เช่น การขอรหัสในการควบคุมจากระยะไกล (Remote Control) เพื่อใช้ในการ Remote เข้าควบคุมเครื่องโดยอ้างว่าเป็นรหัสที่จะใช้ในการช่วยดำเนินการแก้ปัญหาให้ เป็นต้น ทั้งนี้ หากโทรศัพท์ไม่ได้ Jail break หรือ Root การจะเข้าครอบครองเครื่องด้วยการ Remote Control หรือ ลงโปรแกรมมักจะต้องให้เหยื่อทำตามคำขอหลายขั้นตอนแต่มักจะใช้กลยุทธ์เพื่อให้เหยื่อทำตาม ซึ่งจะกล่าวในรายละเอียดต่อไป

3. **ขั้นตอนควบคุมการใช้งานด้วยเครื่องมือที่ถูกหลอกให้ติดตั้งในขั้นตอนที่ 2** ซึ่งเมื่อการติดตั้งโปรแกรมเสร็จสิ้นสมบูรณ์แล้ว มิจฉาชีพก็จะดำเนินการตามสิ่งที่ได้เตรียมการไว้ซึ่งจะทำให้เกิดการโอนเงินขโมยข้อมูลส่วนบุคคล จากเครื่องโทรศัพท์ออกไปได้ ถึงจุดนี้มิจฉาชีพได้ข้อมูลและเครื่องมือพร้อมที่จะดำเนินการ และจะเลือกลงมือตามที่ได้ออกแบบไว้ และมีการเตรียมบัญชีม้าสำหรับโอนเงินเป็นทอด ๆ เพื่อหลบหลีกการติดตาม

รูปที่ 6 แสดงขั้นตอนทั่วไปของมิจฉาชีพที่ใช้เพื่อโจมตีเหยื่อ

จากขั้นตอนของมิจฉาชีพโดยเฉพาะในขั้นตอนที่ 1 นั้น เนื่องจากปัจจุบันช่องทางการติดต่อสื่อสารมีการใช้เครื่องมือมากมายหลากหลายเช่น โทรศัพท์, SMS, Email, Social Media ต่าง ๆ เป็นต้น จึงทำให้มิจฉาชีพสามารถใช้วิธีที่หลากหลายในการหลอกลวงได้เช่นกัน สำหรับการที่จะป้องกันหรือลดความเสี่ยงจากมิจฉาชีพดังกล่าวจะต้องมีความร่วมมือกับหน่วยงานที่ให้บริการในช่องทางต่าง ๆ เหล่านั้น ไม่ว่าจะเป็นผู้ให้บริการเครือข่ายโทรศัพท์มือถือ ผู้ให้บริการสื่อโซเชียลต่าง ๆ ในการเฝ้าระวัง หรือจัดการยุติการใช้งานสื่อโซเชียลที่พบว่าถูกใช้ในการหลอกลวงโดยเร็ว นอกจากนั้นหน่วยงานกำกับดูแลของผู้ให้บริการต่าง ๆ ไม่

ว่าจะเป็นธนาคาร ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ ผู้ให้บริการสื่อโซเชียลต่าง ๆ จะต้องหามาตรการในการควบคุมและกำกับดูแลกลไกในการจัดการลดความเสี่ยงภัยทางไซเบอร์เหล่านั้น ที่สำคัญอีกส่วนหนึ่งคือการสร้างความเข้าใจในการใช้งานเทคโนโลยีอย่างปลอดภัยของทุก ๆ ภาคส่วน เพื่อยกระดับให้สังคมมีภูมิคุ้มกันต่อภัยไซเบอร์

ด้วยขั้นตอนของมิจฉาชีพดังกล่าว การวิวัฒนาการของภัยไซเบอร์ต่อบริการทางการเงินจนถึงปัจจุบันจะสรุปได้เป็นสามยุคคือ

1. ยุคแรก เป็นยุคที่มุ่งเน้นในการขโมยข้อมูลของเหยื่อเพื่อเข้าใช้บริการแทนเหยื่อ ซึ่งเป็นช่วงที่ Internet Banking กำลังเป็นที่นิยมและการใช้งาน Internet Banking จะใช้งานผ่าน Browser ซึ่งมิจฉาชีพจะใช้เทคนิค Phishing ในการหลอกให้เหยื่อคลิกและกรอกข้อมูลบน Phishing Website ที่เตรียมไว้เพื่อขโมยตัวตนในโลกดิจิทัล เช่น Username, Password และรหัส OTP เพื่อใช้ในการเข้าใช้บริการแทนเหยื่อและดำเนินการโอนเงินต่อไป

2. ยุคที่สอง เป็นยุคที่มีการใช้ Mobile Banking เพิ่มมากขึ้น การขโมยตัวตนไปเพื่อปลอมแปลงตัวตนของเหยื่อทำได้ยากขึ้น มิจฉาชีพจึงปรับเปลี่ยนวิธีมา**หลอกเพื่อให้เหยื่อติดตั้งแอปพลิเคชัน ที่ใช้ในการรีโมทเพื่อควบคุมเครื่องเหยื่อจากทางไกล** เช่น Team Viewer, Anydesk, RealVNC แม้ว่าแอปพลิเคชันต่าง ๆ เหล่านั้นจะถูกใช้ในการ support หรือใช้แก้ปัญหาการใช้งานจากทางไกล โดยผู้ใช้งานจะต้องให้รหัสที่อยู่บนแอปพลิเคชันรีโมทดังกล่าวก่อน เพื่อที่จะเป็นการอนุญาตให้สามารถรีโมทเข้ามาที่เครื่องได้ แต่ผู้ใช้งานอาจจะถูกหลอกให้ส่งรหัสดังกล่าวไปให้มิจฉาชีพ

3. ยุคที่สาม การใช้งานแอปพลิเคชันรีโมทในยุคที่สองจะมีข้อจำกัดที่มิจฉาชีพจะต้องอยู่พูดคุยกับเหยื่อในช่วงเวลาเดียวกัน มิจฉาชีพจึงได้ปรับเปลี่ยนมา**ใช้ Accessibility Service** ซึ่งจะ**ทำให้สามารถครอบครองเครื่องและดักจับข้อมูล**ได้ทั้งหมด และดำเนินการโอนเงินในจังหวะใดก็ได้ แม้ว่าจะต้องเตรียมขั้นตอนการชักชวนหลอกลวงให้เหยื่อทำตามประกอบกับขั้นตอนจะมีมากขึ้นก็ตามยุทธวิธีหลอกให้เกิดความหลงเพื่อที่จะทำให้เหยื่อไหวตัวได้ช้า

หากจะสรุปกลยุทธ์หรือยุทธวิธีที่มิจฉาชีพเลือกใช้กับเหยื่อเพื่อให้เหยื่อทำตามแนวทางที่มิจฉาชีพได้เตรียมการไว้ สามารถสรุปได้ 4 กลยุทธ์ด้วยกันคือ

1. **Urgency** เป็นการสร้างสถานการณ์ที่เร่งรีบน่าตกใจ ทำให้เหยื่อกลัวและไม่ได้มีเวลาตรึกตรอง จึงใช้ช่วงเวลานั้นบอกให้เหยื่อทำตามที่ต้องการ
2. **Misdirection** เป็นการโน้มน้าวจูงเหยื่อไปในทิศทางสถานการณ์ที่ออกแบบไว้เพื่อเบี่ยงเบนขั้นตอนที่เหยื่อคุ้นเคย เช่นสถานการณ์ให้คำปรึกษาทางการเงินและโน้มน้าวไปกรอกข้อมูลหรือคุยต่อใน Line เป็นต้น

3. **Sympathy** เป็นการสร้างความเห็นอกเห็นใจในสถานการณ์ที่กำลังลำบากและให้ช่วยโอนข้อมูลหรือขอให้แสดงข้อมูลส่วนบุคคล
4. **Authority** เป็นการแอบอ้างหน่วยงานที่มีอำนาจเช่น ตำรวจ สรรพากร เพื่อให้ดำเนินการตามที่ได้ออกแบบ ไม่ว่าจะเป็นการขอข้อมูลส่วนบุคคลหรือลงโปรแกรมในเครื่องโทรศัพท์มือถือ

กลยุทธ์ดังกล่าวจะใช้ได้ผล จะต้องมีการออกแบบสถานการณ์ให้เกิดเหตุจูงใจที่จะชักชวนให้เหยื่อเกิดความรัก โลภ กลัว หรือ หลง เพื่อให้เหยื่อหลงกลได้ง่ายขึ้น ตามรายละเอียดในรูปที่ 7

รูปที่ 7 แสดงเหตุจูงใจที่ทำให้หลงกลก่อนจะใช้กลยุทธ์ที่มิจฉาชีพใช้ประกอบในการสร้างสถานการณ์

จากเทคนิคการหลอกลวงที่มิจฉาชีพใช้ จึงได้มีการวิเคราะห์แนวทางในการสร้างพฤติกรรมพื้นฐานที่จะสามารถนำไปปฏิบัติได้ง่าย และสามารถสรุปเป็น 8 พฤติกรรมปลอดภัยดังนี้

1. **อุปกรณ์ปลอดภัย** อุปกรณ์ที่ใช้งานอยู่จะต้องมีความปลอดภัยเป็นพื้นฐาน ซึ่งนอกจากจะต้อง update อยู่เป็นประจำแล้ว ไม่ควรจะ Jailbreak หรือ Root และควรตั้งล็อคหน้าจอ
2. **รหัสปลอดภัย** ควรตั้งรหัสไม่ให้ง่ายเกินไป และไม่ควรเปิดเผยให้ผู้อื่น หากต้องมีการ key-in รหัสผ่านหรือก่อนที่จะให้รหัสผ่านแก่ใครหรือกับระบบใด ควรต้องถามตัวเองก่อนว่าทำไมต้องให้รหัสนั้น
3. **ตัวตนปลอดภัย** ปัจจุบันการมีตัวตนในยุคดิจิทัลคงจะหลีกเลี่ยงไม่ได้ที่จะมีข้อมูลความเป็นตัวตน รวมถึงกิจกรรมต่าง ๆ ในโลกดิจิทัล (Digital Footprint) แต่อย่างไรก็ตามข้อมูลส่วนตัวสำคัญจริง ๆ ไม่ควรจะเปิดเผยเกินความจำเป็น จะต้องเลือกใช้กับหน่วยงานที่มั่นใจ และตรวจสอบก่อนให้ข้อมูลเพื่อสร้างตัวตนที่ปลอดภัยในโลกดิจิทัล

4. **เชื่อมต่อปลอดภัย** การเชื่อมต่อ WiFi สาธารณะ รวมถึงระหว่างการเชื่อมต่อเพื่อทำรายการควรระวังการถูกแอบดูข้อมูล
5. **แอปพลิเคชันปลอดภัย** การติดตั้งแอปพลิเคชันจะต้องพิมพ์ชื่อแอปพลิเคชันเองบน Official Store โดยไม่คลิกลิงก์เพื่อดาวน์โหลด และเมื่อมีการถาม Permission ควรจะอ่านให้ละเอียดก่อนว่า Permission ที่ขอนั้นสอดคล้องกับประเภทของแอปพลิเคชันหรือไม่
6. **ติดตามข้อมูลข่าวสาร** ควรติดตามข่าวสารเทคนิคการหลอกลวงประเภทต่าง ๆ จากแหล่งที่น่าเชื่อถือ เช่น TB-CERT เพื่อเข้าใจและเตรียมระวังภัยรูปแบบต่าง ๆ
7. **สื่อสารปลอดภัย** การพูดคุยหรือให้ข้อมูลกับบุคคลที่ไม่รู้จักทางออนไลน์ ควรจะตรวจสอบคู่สนทนาให้ดีก่อนโดยไม่แสดงข้อมูลตัวตนก่อนหากถูกถาม เพื่อไม่ให้คล้อยตามสวมรอยตามข้อมูลที่ให้ไปจนคิดว่าเป็นจริงตามนั้น
8. **รอบคอบ** มีความระมัดระวัง มีสติรอบคอบไม่เร่งรีบในจังหวะที่ทำธุรกรรมสำคัญ เพื่อลดความผิดพลาดโดยไม่ทันระวังจากการชักจูงหลอกลวง

รูปที่ 8 แสดง 8 พฤติกรรมปลอดภัยลดความเสี่ยง

ทั้งนี้แม้ว่าจะมีพฤติกรรมภาพรวมเพื่อที่จะมีความมั่นคงปลอดภัยบนโลกไซเบอร์นั้น ควรจะตั้งรหัสผ่านที่ไม่เกี่ยวข้องกับข้อมูลตัวตนที่อยู่ในโลกไซเบอร์ หากสังเกตความผิดปกติเมื่อมีการสื่อสารสนทนากับผู้ที่ไม่รู้จักให้เก็บหลักฐานการสนทนา พิจารณาว่าได้ให้ข้อมูลสำคัญอะไรไปแล้วบ้าง และรีบปรึกษาธนาคารเพื่อตรวจสอบความผิดปกติในบัญชีและขอคำแนะนำ ที่สำคัญคือการติดตั้งแอปพลิเคชัน ซึ่งไม่จำเป็นต้องเป็นแอปพลิเคชันของธนาคารเท่านั้น แอปพลิเคชันอื่น ๆ ที่ต้องการใช้งาน ควรจะต้องพิมพ์ชื่อแอปพลิเคชันบนร้านค้าที่ได้รับความน่าเชื่อถือ (Official Store) ด้วยตนเอง ตัวอย่างเช่น App Store, Google

Play Store หรืออื่น ๆ ผู้ใช้งานมือถือจะต้องไม่กดติดตั้งจากลิงก์ที่ถูกส่งมาจากช่องทางการสื่อสารต่าง ๆ ทั้งนี้ การติดตั้งแม้ว่าจะเป็นแอปพลิเคชันที่มาจากร้านค้าที่ได้รับความน่าเชื่อถือ (Official Store) โดยหากมีการขอ Permission ให้เช็ค Permission ที่ขอว่าเหมาะสมกับฟังก์ชันของแอปพลิเคชันนั้นหรือไม่

อย่างไรก็ตาม มัลแวร์ยังมีการพัฒนาอย่างต่อเนื่อง การติดตามพัฒนาการ รวมถึงแลกเปลี่ยนข้อมูลทางเทคนิคเพื่อวิเคราะห์แนวทางการป้องกันเป็นบทบาทหลักของ TB-CERT ที่จะช่วยยกระดับด้านความมั่นคงปลอดภัยของบริการทางการเงินและยังมุ่งมั่นและเป็นส่วนหนึ่งในการสร้างภูมิคุ้มกันทางไซเบอร์ให้กับสังคมไทย

หมายเหตุ วิธีการเช็ค permission สามารถดูได้จาก TB-CERT awareness (https://www.tba.or.th/pso-tb-cert/tb-cert/public-awareness/)

แนวโน้มเทคโนโลยี และภัยไซเบอร์ในปี 2023 ของภาคการเงินการธนาคาร

แนวโน้มเทคโนโลยีและภัยไซเบอร์ในปี 2023 ของภาคการเงินการธนาคาร

จากการรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นในปีที่ผ่านมาประกอบกับการวิเคราะห์สถานการณ์และแนวโน้มจากรายงานที่เกี่ยวข้อง ทาง TB-CERT จึงได้คาดการณ์แนวโน้มรูปแบบการโจมตีทางไซเบอร์สำหรับปี 2023 ดังนี้

1. การโจมตีทางไซเบอร์เพื่อการฉ้อโกงทางดิจิทัล (Digital Fraud) เพิ่มมากขึ้น

การหลวงลวงโดยใช้ช่องทางดิจิทัลมีแนวโน้มจะเพิ่มมากขึ้น โดยการใช้ช่องทางดิจิทัลเป็นเครื่องมือหลักในการหลอกลวงเพื่อสามารถเข้าถึงเหยื่อได้จำนวนมากต่อการปฏิบัติการโจมตีแต่ละครั้ง ประกอบกับประเทศไทยมีการใช้งานช่องทางดิจิทัลมากเป็นอันดับต้น ๆ ของโลก โดยจะเห็นได้จากรายงาน DIGITAL 2023 Global Overview Report [2] ที่รวบรวมของมูลการใช้งานผู้ใช้งานอินเทอร์เน็ตช่องอายุระหว่าง 16 - 64 ปี จากทั่วโลก พบว่าประเทศไทยมีใช้งานอินเทอร์เน็ตต่อวันเป็นอันดับ 9 ของโลกโดยมีการใช้งานโดยเฉลี่ยที่ 8 ชั่วโมง 6 นาทีต่อวัน และใช้งานผ่านอุปกรณ์ Smart phone เป็นอันดับ 2 โลก ซึ่งเป็นเป้าหมายขนาดใหญ่ของคนร้ายและคุ้มค่าต่อการลงทุนของคนร้าย โดยจากกระแสข่าวเหตุการณ์แอปดูดเงินในปีที่ผ่านมาของประเทศไทย จะเห็นได้ว่ามิจฉาชีพมุ่งโจมตีกลุ่มเป้าหมายผู้ใช้งาน Smart phone โดยการหลอกติดตั้งแอปพลิเคชันปลอมหรือเพื่อควบคุมเครื่องของเหยื่อจากระยะไกล ซึ่งการโจมตีรูปแบบนี้จะสอดคล้องสถิติภัยคุกคามทางไซเบอร์ จากระบบข่าวกรองภัยคุกคามทางไซเบอร์ของ TB-CERT โดยรูปแบบการโจมตี 2 อันดับแรก คือ 1. ฟิชชิง (Phishing) 2. Trojan/Backdoor ซึ่งการโจมตีทั้ง 2 แบบนี้จะเป็นต้นทางของการทำ Digital Fraud เพื่อหลอกลวงเหยื่อลำดับต่อไป ซึ่งจากสถิติและสถานการณ์ ทาง TB-CERT คาดการณ์ได้ว่าในปี 2023 สถานการณ์ที่เกี่ยวกับ Digital Fraud ทั่วโลกรวมถึงประเทศไทยจะยังเพิ่มขึ้นอย่างต่อเนื่อง ดังนั้นการใช้งานเทคโนโลยีดิจิทัลต่าง ๆ ต้องมาพร้อมความตระหนักรู้การใช้งานและการป้องกันภัย อีกทั้งยังเป็นความท้าทายต่อผู้ให้บริการธุรกิจเองจะต้องรับผิดชอบต่อสังคมและลูกค้า ในการสร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy) อย่างถูกต้องและปลอดภัยต่อผู้ใช้บริการอย่างทั่วถึง

2. การโจมตีข้ามอุตสาหกรรม (Cross sector impact) แนวโน้มเพิ่มขึ้น

จากการโจมตีข้ามอุตสาหกรรมเพิ่มขึ้นในปีที่ผ่านมาและยังมีแนวโน้มขยายไปหลากหลายอุตสาหกรรม โดยจะเห็นได้จากมิจฉาชีพที่มุ่งโจมตีทางการเงินของประชาชนนั้นจะไม่ได้โจมตีระบบของธนาคารโดยตรง เนื่องจากระบบของธนาคารมีการป้องกันที่เข็มแข็งยากต่อการโจมตีโดยตรงให้สำเร็จได้ จึงได้ใช้วิธีอ้อมโดยผ่านช่องทางของภาคอุตสาหกรรมอื่น ตัวอย่างเช่น กรณีหลอกประชาชนให้รับตั๋วเครื่องบินฟรี จะเป็นเส้นทางการหลอกโดยเริ่มต้นจากส่งข้อความสั้น (SMS) ปลอม หลอกให้คลิกลิงก์เพื่อ

[2] DIGITAL 2023 Global Overview Report: https://datareportal.com/

ชักชวนพูดคุยผ่านแอปพลิเคชันแชท และให้ดาวน์โหลดแอปพลิเคชันปลอมผ่านหน้าเว็บไซต์ที่สายการบินที่ถูกปลอมแปลง จนท้ายที่สุดประชนชนหลงเชื่อติดตั้งและถูกควบคุมเครื่องและโอนเงินสำเร็จ จากตัวอย่างเส้นทางการหลอกลวงจะเห็นได้ชัดว่า ต้องผ่านหลายภาคอุตสาหกรรมตั้งแต่ภาคโทรคมนาคม ภาคบริการ ภาคธนาคาร รามถึงภาครัฐที่เป็นผู้บังคับใช้กฎหมาย ซึ่งเป็นเรื่องที่ท้าทายระดับประเทศในการรับมือภัยการโจมตีของกลุ่มอาชญากรที่ปรับเปลี่ยนไป จากสถานการณ์ประเทศไทยในปัจจุบันซึ่งสอดคล้องกับรายงาน The Global State of Mobile Phishing [3] ที่ได้รวบรวมสถิติทั่วโลกในการโจมตีด้วยฟิชชิง (Phishing) ผ่านทางโทรศัพท์มือถือ ซึ่งพบว่ามีสัญญาณการโจมตีเพิ่มขึ้นแบบมีนัยสำคัญตั้งแต่ปี 2021 หลายภูมิภาคทั่วโลก โดยจะพบใน 3 รูปแบบสำคัญดังนี้ รูปแบบที่ 1 เรียกว่า SMS phishing (smishing) รูปแบบที่ 2 Voice phishing (vishing) รูปแบบที่ 3 QR code phishing (quishing) ซึ่งจะทำการปลอมแปลงเป็นบริการต่าง ๆ ที่คนในประเทศนั้นนิยมใช้งานและมุ่งโจมตีเป้าหมายที่ระดับบุคคล โดยทาง TB-CERT คาดการณ์ว่าในปี 2023 การโจมตีข้ามอุตสาหกรรม (Cross sector impact) จะเพิ่มขึ้น การรับมือภัยคุกคามจึงจำเป็นอย่างยิ่งที่ต้องมีการรับมือแบบบูรณาการหลายหน่วยงานร่วมมือกันหลายฝ่ายข้ามอุตสาหกรรม และต้องปรับเปลี่ยนให้เท่าทันต่อการโจมตีที่เปลี่ยนแปลงอย่างรวดเร็วให้ทันท่วงที

3. การนำ AI และ Machine Learning มาใช้ในการโจมตีมากขึ้น

การใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) และ Machine Learning ในปีที่ผ่านมีการปรับเปลี่ยนครั้งสำคัญ ตัวอย่างเช่น ChatGPT เป็นแชทบอทปัญญาประดิษฐ์ที่เข้ามามีบทบาทต่อการเปลี่ยนแปลงหลายอุตสาหกรรมรวมถึงรูปแบบวิธีการทำงาน เช่น การเขียนโปรแกรม การเขียนบทความหรือบทภาพยนตร์ จะเห็นได้ว่าเทคโนโลยีปัญญาประดิษฐ์สามารถเข้ามาทำงานแทนมนุษย์ได้ดีในบางสถานการณ์ซึ่งจะเป็นประโยชน์การการดำเนินธุรกิจ แต่ในทางกลับกันเริ่มเห็นสัญญาณว่ากลุ่มมิจฉาชีพมีการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้แพร่หลายมากขึ้น ตัวอย่างเช่น ใช้ปัญญาประดิษฐ์ในการช่วยให้เขียนข้อความหลอกฟิชชิง (Phishing) ในภาษาอื่น ๆ ได้หลายประเทศ หรือช่วยในการเขียนโปรแกรมแกรมโจมตีระบบเป้าหมาย โดยการใช้เทคโนโลยีปัญญาประดิษฐ์อาจจะส่งผลให้รูปแบบการโจมตีมีรูปแบบความหลากหลายมากขึ้น ยากต่อการตรวจจับในวิธีการและรูปแบบเดิม ๆ ซึ่งทาง TB-CERT คาดการณ์ว่าในปี 2023 กลุ่มมิจฉาชีพจะมีการเทคโนโลยีปัญญาประดิษฐ์มาเป็นเครื่องมือในการโจมตีมากขึ้น ซึ่งเป็นความท้าทายต่อภาคการเงินการธนาคารเองเช่นกันในการเตรียมพร้อมป้องกันและรับมือ

[3] The Global State of Mobile Phishing: www.lookout.com

บทสรุป

บทสรุป

โลกเปลี่ยนแปลงเข้าสู่ยุคที่ภัยคุกคามทางไซเบอร์มีผลกระทบต่อประชาชนและทำให้เกิดความเสียหายมากมายจนกลายเป็นอาชญากรรมทางไซเบอร์ที่ทุกภาคส่วนให้ความสนใจในการช่วยเหลือประชาชนให้พ้นจากภัยเหล่านี้ แต่นั่นก็เป็นเรื่องที่ท้าทายมาก ซึ่งความท้าทายเหล่านี้มีหลากหลายมิติที่เราทุกคนต้องช่วยกันแก้ไข ไม่ว่าจะเป็นในมุมของกฎหมายที่บางครั้งก็อาจจะล้าสมัยไปเมื่อเทียบกับยุคดิจิทัลที่เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วและมีความล้ำสมัยไปมาก การพัฒนาของกฎหมายจะต้องปรับเปลี่ยนให้ทันกับภัยคุกคามเหล่านี้ ทั้งในส่วนของการรับมือ การป้องกัน และการตรวจจับ ในด้านของประชาชนเองที่จำเป็นต้องมีความตระหนักรู้ในการใช้งานเทคโนโลยีอย่างปลอดภัยและมีสติ อีกด้านหนึ่งเนื่องจากมิจฉาชีพได้มีการพัฒนาวิธีการหลอกลวงอยู่ตลอด แม้ว่าทีมไซเบอร์จะพยายามหาทางป้องกันแต่มิจฉาชีพก็ปรับเปลี่ยนกลยุทธ์และวิธีการโจมตีใหม่ ๆ ได้ตลอด ดังนั้นประชาชนจะต้องตระหนักรู้การใช้เทคโนโลยีต่าง ๆ อย่างไรให้ปลอดภัยและติดตามข่าวสารเพื่อให้รู้เท่าทันภัยหลอกลองของมิจฉาชีพอยู่เสมอ

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคารเล็งเห็นและติดตามความท้าทายในการรับมือกับภัยคุกคามทางไซเบอร์ในหลากหลายรูปแบบในยุคดิจิทัลนี้มาตลอดระยะเวลาหลายปี การพัฒนาบุคลากรของภาคการธนาคาร ไม่ว่าจะเป็นโครงการ Cyber Brain, Cyber Combat ที่ให้สมาชิกได้เข้ามาเรียนรู้ฝึกทักษะทางด้านไซเบอร์ทั้งทฤษฎีและปฏิบัติการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ในภาคการธนาคาร (Banking Cyber Drill) การสร้างความตระหนักรู้กับประชาชนและให้ความรู้กับพนักงานของหน่วยงานด้วยความร่วมมือกับสถาบันธนาคารไทย (Thai Banking Academy หรือ TBAC) ผ่านโครงการในการพัฒนาความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้พนักงานของหน่วยงานได้ศึกษารูปแบบภัยคุกคามใหม่ ๆ รวมทั้งการจัด Annual Conference ที่ให้พนักงานได้อัปเดตเทคโนโลยีใหม่และภัยคุกคามทางไซเบอร์ ยังคงเป็นเรื่องที่เราให้ความสำคัญอย่างต่อเนื่อง

ที่สำคัญอีกส่วนหนึ่งคือการสร้างความร่วมมือกับหน่วยงานภายนอกที่เป็นส่วนหนึ่งในระบบนิเวศน์ภาพรวมของการรับมือกับภัยคุกคามทางไซเบอร์ไม่ว่าจะเป็น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) หน่วยงานผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ ธนาคารแห่งประเทศไทย (ธปท.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และหน่วยงานพันธมิตรต่าง ๆ เพื่อให้สามารถรับมือกับภัยในปัจจุบันได้อย่างทันท่วงทีและช่วยลดผลกระทบในวงกว้าง ความร่วมมือที่เป็นเอกภาพของประเทศไทยอย่างเหนียวแน่นจะช่วยให้ความท้าทายที่พวกเราเผชิญอยู่ลดน้อยลงอย่างมีนัยสำคัญ และสร้างความยั่งยืนให้กับภาพรวมได้

เป้าหมายของ TB-CERT ในปี 2023

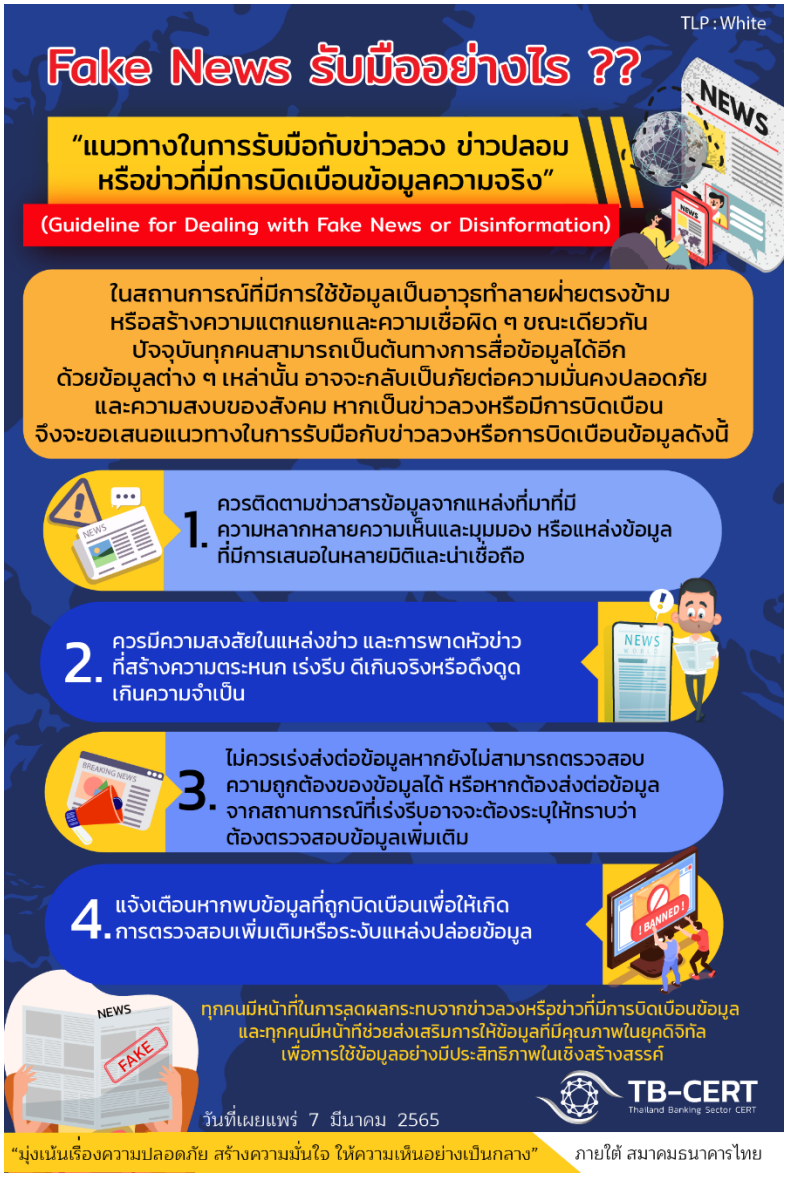
เป้าหมายของ TB-CERT ในปี 2023

ตลอดระยะเวลา 1 ปี 2022 ที่ผ่านมา TB-CERT เฝ้าติดตามเหตุการณ์สำคัญ ๆ ที่เกิดขึ้นทั่วโลกและเหตุการณ์ที่ได้รับจากการแชร์ของธนาคารสมาชิก จึงเห็นภัยคุกคามทางไซเบอร์ที่ได้ทวีความรุนแรงและซับซ้อนขึ้น ไม่ว่าจะเป็นการโจมตีทางไซเบอร์ที่หน่วยงานภายนอก (3rd party attack) ส่งผลกระทบต่อองค์กร หรือการทำทุจริตฉ้อโกง หลอกลวงต่าง ๆ ทางโลกออนไลน์ที่ในปัจจุบันมีความเกี่ยวโยงกับการโจมตีทางไซเบอร์ ซึ่งมิจฉาชีพใช้วิธีเทคนิคแบบผสมผสานระหว่างการหลอกลวงทางออนไลน์กับการใช้เทคนิคทางด้านไซเบอร์มาเป็นเครื่องมือในการหลอกลวงทำทุจริตนั้น ๆ ทำให้การทำทุจริตสัมฤทธิ์ผลอย่างแพร่หลายและรวดเร็ว ตัวอย่างเช่น การส่งลิงก์อันตรายผ่านช่องทางข้อความสั้นหรือ SMS รวมถึงสร้าง Line Account ปลอม เพื่อใช้เป็นช่องทางหลอกให้ประชาชนหลงเชื่อทำการดาวน์โหลดแอปฯ ปลอม เกิดความสูญเสียเป็นวงกว้าง ซึ่งคาดว่าจะมีแนวโน้มสูงมากยิ่งขึ้นในปี 2023 ดังนั้นเป้าหมายการดำเนินงานของ TB-CERT จึงเน้น 5 ส่วนสำคัญที่จะช่วยให้การรับมือต่อเหตุการณ์ที่เกิดขึ้นนั้นเป็นไปอย่างทันท่วงที ดังนี้

1. **กระตุ้นให้เกิดการแชร์ข้อมูลระหว่างธนาคารสมาชิกให้มากขึ้น** ผ่านกลไกการแลกเปลี่ยนข้อมูลในวาระของการประชุมสมาชิกประจำเดือน เพื่อนำข้อมูลการเชร์เหล่านี้มาใช้เป็นแนวทางให้สมาชิกนำไปปฏิบัติต่อได้หรือพัฒนาต่อยอดจากสิ่งที่มี
2. **การเพิ่มพูนประสิทธิภาพของการนำข้อมูลที่ได้รับจากการแชร์จากสมาชิกให้เกิดประโยชน์สูงสุด** โดยทำการวิเคราะห์และสร้างเสริมข้อมูลภัยไซเบอร์เชิงลึก (enrichment) เพื่อช่วยทำให้การบริหารจัดการด้านภัยคุกคามทางไซเบอร์นั้นมีความยั่งยืนเพิ่มมากขึ้น
3. **มุ่งเน้นการทำงานให้เกิดภาพของความร่วมมือกันในระดับภาคอุตสาหกรรมการธนาคาร** ซึ่งการร่วมมือในระดับนี้จะช่วยให้การรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพในภาพรวมของภาคอุตสาหกรรมการเงิน
4. **สร้างและสนับสนุนวัฒนธรรมการทำงานร่วมกันระหว่างทีม IT security กับทีม Fraud ให้มากขึ้น** เพื่อช่วยให้การรับมือต่อภัยคุกคามทางไซเบอร์และการทำทุจริตออนไลน์มีความคล่องตัว รวดเร็ว ตอบสนองต่อเหตุการณ์ได้ทันท่วงที
5. **พัฒนาบุคลากรให้มีทักษะและความรู้ด้านไซเบอร์ที่จำเป็นต้องมีในปัจจุบัน** เพื่อให้เท่าทันต่อภัยคุกคามทางไซเบอร์ใหม่ ๆ ได้

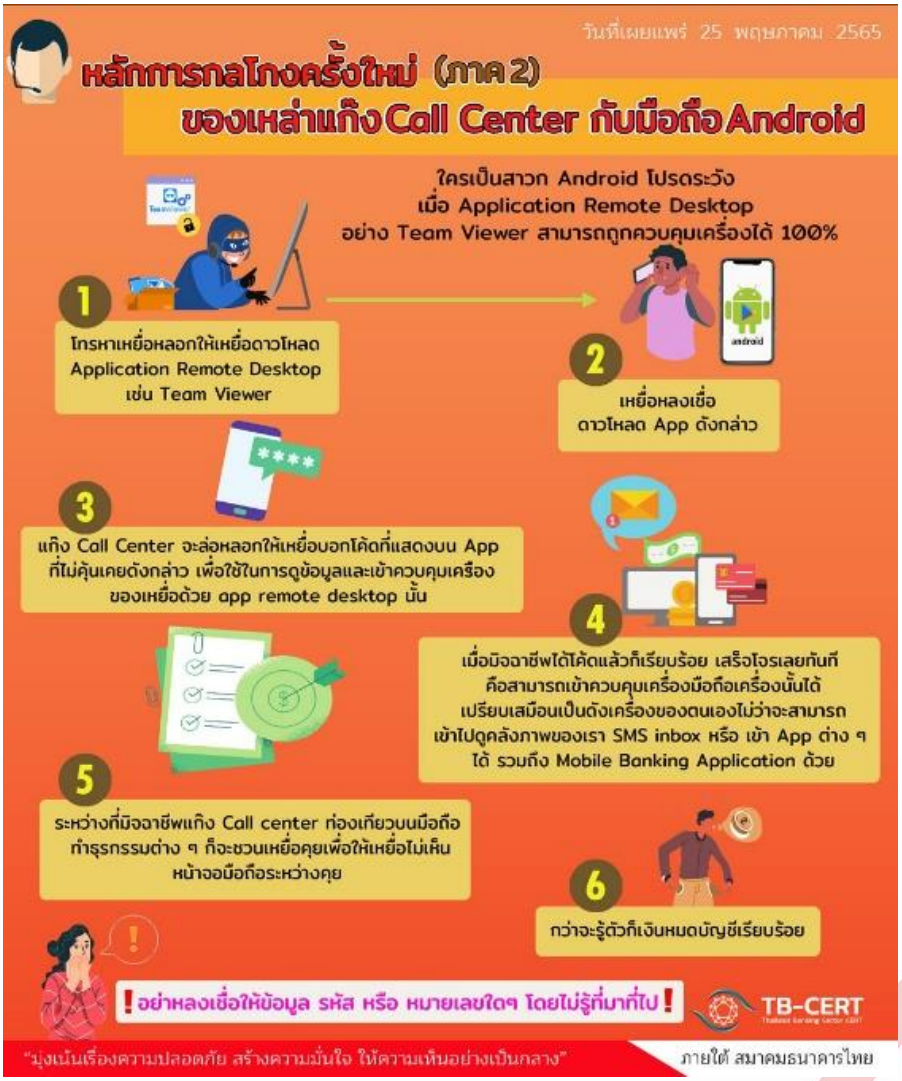
ภาคผนวก

Public Awareness


TLP : White
Fake News รับมืออย่างไร ??
"แนวทางในการรับมือกับข่าวลวง ข่าวปลอม
หรือข่าวที่มีการบิดเบือนข้อมูลความจริง"
(Guideline for Dealing with Fake News or Disinformation)
NEWS
ในสถานการณ์ที่มีการใช้ข้อมูลเป็นอาวุธทำลายฝ่ายตรงข้าม
หรือสร้างความแตกแยกและความเชื่อผิด ๆ ขณะเดียวกัน
ปัจจุบันทุกคนสามารถเป็นต้นทางการสื่อข้อมูลได้อีก
ด้วยข้อมูลต่าง ๆ เหล่านั้น อาจจะกลับเป็นภัยต่อความมั่นคงปลอดภัย
และความสงบของสังคม หากเป็นข่าวลวงหรือมีการบิดเบือน
จึงจะขอเสนอแนวทางในการรับมือกับข่าวลวงหรือการบิดเบือนข้อมูลดังนี้
1. ควรติดตามข่าวสารข้อมูลจากแหล่งที่มาที่มี
ความหลากหลายความเห็นและมุมมอง หรือแหล่งข้อมูล
ที่มีการเสนอในหลายมิติและน่าเชื่อถือ
2. ควรมีความสงสัยในแหล่งข่าว และการพาดหัวข่าว
ที่สร้างความตระหนก เร่งรีบ ดีเกินจริงหรือดึงดูด
เกินความจำเป็น
3. ไม่ควรเร่งส่งต่อข้อมูลหากยังไม่สามารถตรวจสอบ
ความถูกต้องของข้อมูลได้ หรือหากต้องส่งต่อข้อมูล
จากสถานการณ์ที่เร่งรีบอาจจะต้องระบุให้ทราบว่า
ต้องตรวจสอบข้อมูลเพิ่มเติม
4. แจ้งเตือนหากพบข้อมูลที่ถูกบิดเบือนเพื่อให้เกิด
การตรวจสอบเพิ่มเติมหรือระงับแหล่งปล่อยข้อมูล
BANNED
NEWS
FAKE
ทุกคนมีหน้าที่ในการลดผลกระทบจากข่าวลวงหรือข่าวที่มีการบิดเบือนข้อมูล
และทุกคนมีหน้าที่ช่วยส่งเสริมการให้ข้อมูลที่มีคุณภาพในยุคดิจิทัล
เพื่อการใช้ข้อมูลอย่างมีประสิทธิภาพในเชิงสร้างสรรค์
TB-CERT Thailand Banking Sector CERT
วันที่เผยแพร่ 7 มีนาคม 2565
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย


TeamViewer
วันที่เผยแพร่ 26 เมษายน 2565
รู้ยัง ?
มุกใหม่ ของแก๊งคอลเซ็นเตอร์
อย่าหลงเชื่อแก๊งคอลเซ็นเตอร์ให้ติดตั้งโปรแกรมต่าง ๆ เช่น Team Viewer,
AnyDesk หรือ Remote Desktop อื่น ๆ เพื่อเข้ามาควบคุมการใช้งาน
บนเครื่องมือถือของเรา
เตือนสติอยู่ตลอดเวลา ว่าอย่าเชื่ออะไร ง่าย ๆ ให้รู้จักเอ๊ะ?
สงสัยว่าเป็นมิจฉาชีพไว้ก่อน ไม่ว่าจะมุกใหม่มุกเก่าก็ทำอะไรเราไม่ได้
1. ไม่หลงเชื่อกับคนที่เราไม่รู้จัก
หากชวนคุย วางสายทันทีไม่ต้องไปคุยด้วย
2. มีเจ้าหน้าที่โทรมาจากไหนก็ตอบเขาไปเลย
ว่าเราจะโทรกลับไปเบอร์กลางเอง
3. อย่าโหลด App แปลก ๆ ที่เราไม่รู้ที่มาที่ไป
TB-CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย


หลักการกลโกงครั้งใหม่ (ภาค 1)
วันที่เผยแพร่ 23 พฤษภาคม 2565
มิจฉาชีพเห็นช่องทางนี้ในการหลอกลวงครั้งนี้ได้อย่างไร มาดูกัน
1 โทรหาเหยื่อหลอกให้เหยื่อดาวโหลด Application Remote Desktop เช่น Team Viewer
2 เหยื่อหลงเชื่อดาวโหลด app ดังกล่าว
แก๊ง call center
เหยื่อ
3 แก๊ง Call Center จะล่อหลอกให้เหยื่อบอกโค้ดที่แสดงบน app ที่ไม่คุ้นเคยดังกล่าว เพื่อใช้ในการดูข้อมูลและเข้าควบคุมเครื่องของเหยื่อด้วย app remote desktop นั้น
4 แก๊ง Call center ชวนเหยื่อคุยเพื่อให้เหยื่อไม่เห็นหน้าจอมือถือในระหว่างที่คุย
5 แก๊ง Call center ทำการติดตั้ง mobile app และเปิดใช้ app ด้วยข้อมูล SMS OTP จากเครื่องที่เหยื่อใช้อยู
6 เมื่อติดตั้ง App ได้ คราวนี้ก็โอนเงินออกได้อย่างสบายใจ
! อย่าหลงเชื่อให้ข้อมูล รหัส หรือ หมายเลขใดๆ โดยไม่รู้ที่มาที่ไป !
TB-CERT Thailand Banking Sector CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย


วันที่เผยแพร่ 25 พฤษภาคม 2565
หลักการกลโกงครั้งใหม่ (ภาค 2)
ของเหล่าแก๊ง Call Center กับมือถือ Android
ใครเป็นสาวก Android โปรดระวัง
เมื่อ Application Remote Desktop
อย่าง Team Viewer สามารถถูกควบคุมเครื่องได้ 100%
1 โทรหาเหยื่อหลอกให้เหยื่อดาวโหลด Application Remote Desktop เช่น Team Viewer
2 เหยื่อหลงเชื่อ ดาวโหลด App ดังกล่าว
3 แก๊ง Call Center จะล่อหลอกให้เหยื่อบอกโค้ดที่แสดงบน App ที่ไม่คุ้นเคยดังกล่าว เพื่อใช้ในการดูข้อมูลและเข้าควบคุมเครื่องของเหยื่อด้วย app remote desktop นั้น
4 เมื่อมิจฉาชีพได้โค้ดแล้วก็เรียบร้อย เสร็จโจรเลยทันที คือสามารถเข้าควบคุมเครื่องมือถือเครื่องนั้นได้ เปรียบเสมือนเป็นดังเครื่องของตนเองไม่ว่าจะสามารถเข้าไปดูคลังภาพของเรา SMS inbox หรือ เข้า App ต่าง ๆ ได้ รวมถึง Mobile Banking Application ด้วย
5 ระหว่างที่มิจฉาชีพแก๊ง Call center ท่องเที่ยวบนมือถือทำธุรกรรมต่าง ๆ ก็จะชวนเหยื่อคุยเพื่อให้เหยื่อไม่เห็นหน้าจอมือถือระหว่างคุย
6 กว่าจะรู้ตัวก็เงินหมดบัญชีเรียบร้อย
! อย่าหลงเชื่อให้ข้อมูล รหัส หรือ หมายเลขใดๆ โดยไม่รู้ที่มาที่ไป !
TB-CERT Thailand Banking Sector CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย


เอ๊ะสักนิดก่อนคิดจะสแกน QR CODE
หลักการคิดง่ายๆเพื่อให้คุณ เอ๊ะ ?
ก่อนตกเป็นเหยื่อมิจฉาชีพ
คนสแกน QR Code คือคน จ่ายตัง
คนรับตัง ต้องโชว์ QR Code
สแกน=จ่ายเงิน, โชว์=รับเงิน
เอ๊ะ? เรากำลังทำอะไรอยู่ ฉุดคิดสักนิดก่อนทำธุรกรรมทุกครั้ง
วันที่เผยแพร่ 14 มิถุนายน 2565
TB-CERT Thailand Banking Sector CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย


วันที่เผยแพร่ 7 กรกฎาคม 2565
QR Code ปลอม หรือ Fake QR Code คืออะไร
และทำอย่างไรเราจะปลอดภัยจากมิจฉาชีพที่ใช้ QR Code ปลอมมาหลอกเรา
QR Code คืออะไร ? QR Code ย่อมาจาก Quick Response Code คือ สัญลักษณ์ที่ใช้แทนข้อมูลต่างๆ ซึ่งได้รับการพัฒนามาจากบาร์โค้ด 2 มิติให้สามารถอ่านข้อมูลได้เร็ว แม่นยำขจัดข้อผิดพลาดจากความผิดรูปของภาพโค้ดได้ดี และยังสามารถใช้แทนข้อมูลจำนวนมากได้ในโค้ดเดียว ในปัจจุบันสามารถใช้สมาร์ทโฟนในการอ่าน QR Code ได้จึงทำให้การใช้ QR Code มีการใช้กันแพร่หลายมากขึ้นเพราะมีความสะดวกรวดเร็ว โดยผู้ใช้ไม่จำเป็นต้องพิมพ์ข้อมูลจำนวนมากหรือพิมพ์ URL เพื่อเข้าถึง Website ต่างๆ นอกจากนี้ยังมีการนำ QR Code ไปใช้ในการเข้าถึงเมนูร้านอาหารบนโทรศัพท์มือถือ ยืนยันการจองในงานสัมมนาต่างๆ สแกนบอร์ดดิ้งพาส แบบสอบถามสุขภาพที่สนามบิน หรือ เพื่อธุรกรรมการเงิน และอื่นๆ อีกมากมาย
จะเห็นว่าทุกเทคโนโลยีใหม่ ๆ ที่เข้ามาสู่การใช้ในชีวิตประจำวันเรามากขึ้น มักจะหนีไม่พ้นภัยคุกคามจากเหล่ามิจฉาชีพที่พยายามหาช่องโหว่ของการใช้เทคโนโลยีใหม่ ๆ เหล่านี้ในการเข้าถึงข้อมูลของเราและหรือก่ออาชญากรรมฉ้อโกงต่างๆ การทำ QR Code ขึ้นมาในปัจจุบันก็ไม่ยากเพราะมี Website ในการ Generate QR Code โดยมิจฉาชีพจะใช้ QR Code ที่สร้างขึ้นเองนั้นหลอกให้คนสแกนเพื่อที่จะพาเราไปสู่ Website ที่มิจฉาชีพเตรียมไว้เพื่อหลอกเอาข้อมูลต่างๆ ของเราได้
กลโกงโดยการสร้าง QR Code ปลอมมาหลอกลวงจึงมีมากขึ้นเรื่อยๆ ซึ่งเป็นเหตุผลว่าการทำความเข้าใจเทคโนโลยีและแนวทางในการป้องกันจึงเป็นเรื่องสำคัญ พื้นฐานของการป้องกันการหลอกลวงด้วย QR Code คืออย่าสแกน QR Code ที่เราไม่เชื่อถือ
แนวทางการป้องกันที่เราควรพึงวิเคราะห์มีดังนี้
1. หากเราได้รับข้อความที่น่าสงสัยที่แนบ QR Code ที่คาดว่าน่าจะส่งมาจากองค์กรขนาดใหญ่ เช่น ธนาคาร ไปรษณีย์ กรมการกงสุล กรมศุลกากร หรือ อื่นๆ ให้สังเกต URL ที่แสดงก่อนกดเลือกที่จะเข้าถึง Website นั้น หรือหากไม่แน่ใจให้ติดต่อธนาคารหรือหน่วยงานนั้นโดยตรงเสมอเพื่อดูว่าข้อความนั้นมาจากที่เหล่านั้นจริงหรือไม่
2. พึงระลึกไว้เสมอว่า QR Code จะใช้ในการจ่ายเงินให้เจ้าของ QR Code ไม่ใช่เพื่อรับเงิน หากมีคนขอให้เราสแกนรหัสเพื่อรับเงิน นี่อาจเป็นการหลอกลวง เราจะถูกหักเงินแทนการรับเงิน หรือแย่กว่านั้น อาจจะเป็นการให้ข้อมูลเพิ่มเติมเพื่อให้พวกมิจฉาชีพเข้าถึงบัญชีธนาคารของเราก็ได้
3. สังเกต URL ที่แสดงขณะ scan QR Code ว่าเป็น Website ที่น่าสงสัยหรือติดตั้งซอฟต์แวร์ตรวจสอบ Website บนอุปกรณ์คอมพิวเตอร์หรือมือถือ ตัวอย่างซอฟต์แวร์อ้างอิง https://vpnoverview.com/antivirus/best-antivirus/ ด้วยวิธีนี้หากมีการสแกน QR Code ที่เป็นอันตราย อย่างน้อยเราก็อาจจะได้รับการปกป้องจากการหลอกลวงด้วย Website ปลอมที่แฝงมากับ QR Code ได้
4. หากพบ QR Code ที่ดูไม่น่าเชื่อถือ แต่เราต้องการข้อมูลเพิ่มเติมเกี่ยวกับบริการหรือผลิตภัณฑ์ที่นำเสนอให้ลองค้นหาข้อมูลด้วยตนเองก่อนและตรวจสอบตัวเองให้แน่ใจว่าเราไม่ได้ให้ข้อมูลติดต่อใด ๆ จากการสแกน QR Code นั้น
ติดตามข่าวสารการแจ้งเตือนการหลอกลวงเป็นประจำ เพื่อติดตามวิธีการหลอกลวงใหม่ๆ จากแหล่งที่น่าเชื่อถือ และมีสติทุกครั้งในการทำธุรกรรมต่างๆ เราก็จะไม่ตกเป็นเหยื่อของเหล่ามิจฉาชีพ
TB-CERT Thailand Banking Sector CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย


ดูอย่างไร สลิป (Slip) จริงหรือปลอม
เผยแพร่วันที่ 1/8/2565
ด้วยยุคดิจิทัลที่ทุกคนล้วนหันมาใช้เทคโนโลยีที่ทันสมัย สะดวกสบาย ในการใช้ชีวิต หนึ่งในเทคโนโลยีที่ทันสมัยนี้ได้แก่ การใช้ Mobile Banking Application ในการสแกนจ่าย โอน เงิน และทุกครั้งที่ความสะดวกสบายมักจะมาพร้อมกับภัยทางดิจิทัลในรูปแบบต่าง ๆ และหนึ่งในนั้นคือการทำ Slip ปลอม เพื่อหลอกให้ผู้รับคิดว่าได้รับการโอนเรียบร้อยแล้ว
โอนเงินสำเร็จ
27 ก.ค. 65 23:39 น.
A
น.ส. กอไก่ ธ. ธนาคาร A Xxx-x-x3562-x
น.ส. ขอไข่ ธ. Promptpay Xxx-xxx-2487
เลขที่รายการ: 012345678910IAPP02444
จำนวน: 10,000.00 บาท
ค่าธรรมเนียม: 0.00
Verified by A
**ภาพ Slip จำลองเพื่อการอธิบายเท่านั้น
เช็คง่าย ๆ ว่า Slip ที่เราได้มานั้น จริงหรือปลอม
1
ให้สังเกตว่า Slip ของธนาคาร จะต้องมี QR Code อยู่ท้าย Slip ด้วย
2
ให้ใช้ ฟังก์ชัน Scan ของ Mobile App ของ ธนาคาร ที่ท่านมีอยู่ Scan QR code ที่อยู่ใน Slip นั้น หากเป็นของจริง จะแสดงรายละเอียดการโอนนั้น ตามภาพ
ตรวจสอบสำเร็จ
จาก น.ส. กอไก่ ธ. ธนาคาร A Xxx-x-x3562-x
ไปที่ Promptpay Xxx-xxx-2487
จำนวนเงิน 10,000.00 บาท
ไม่ยากเลยใช่มั้ยคะ ลองทดสอบสแกน QR code ของผู้ที่โอนมาดูกันได้เลย !!!!!
TB-CERT
ภายใต้สมาคมธนาคารไทย
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"


TLP: WHITE
รู้ทันและรับมือ Pegasus spyware
Pegasus spyware สปายแวร์ที่ถูกพัฒนาขึ้นโดยบริษัท NSO Group ซึ่งจะเป็นมัลแวร์เชิงพาณิชย์ (Commercial malware) ที่มีความสามารถในการดักจับข้อมูล และติดตามพฤติกรรม โดยพบครั้งแรกปี 2016 และต่อมาได้พัฒนาความสามารถให้สามารถโจมตีช่องโหว่ของอุปกรณ์ด้วยเทคนิคแบบไม่ต้องคลิก (Zero-click exploits) ได้ ซึ่งโดยปกติแล้วการโจมตีทั่วไปจะหลอกให้คลิกหรือติดตั้งแอปพลิเคชันในช่วงเริ่มต้น ดังนั้น ความสามารถของ Pegasus spyware จึงสร้างความตื่นตระหนกในวงกว้าง
ทาง TB-CERT ขอแนะนำแนวทางการรับมือ ดังนี้
1. อัปเดตระบบปฏิบัติการเป็นเวอร์ชันล่าสุดที่รองรับ เพื่อแก้ไขช่องโหว่ของการโจมตี Zero-click exploits
2. หลีกเลี่ยงการใช้เครื่องที่ Jailbreak iOS หรือ Root Android
3. ปิดฟังก์ชันการใช้งาน iMessage หรือ ลบแอปพลิชัน เช่น WhatsApp, Signal, Telegram เป็นต้น หากไม่ได้ใช้งาน เพราะเป็นช่องทางที่จะถูกใช้ในการโจมตีช่องโหว่ของอุปกรณ์มือถือได้
4. ระงับการใช้อุปกรณ์ และแอปพลิเคชันสำคัญเมื่อสงสัยว่าเครื่องติดสปายแวร์
5. หากสงสัยว่าอุปกรณ์มือถือหรือแอปพลิเคชันธนาคารที่ท่านใช้อยู่ ได้รับอันตรายจากสปายแวร์ ให้ติดต่อธนาคารที่ใช้บริการทันที เพื่อตรวจสอบธุรกรรมต้องสงสัย
ทั้งนี้ควรหลีกเลี่ยงการติดตั้งแอปพลิเคชันใดๆ จากลิงค์ SMS , Website ที่น่าสงสัย และแก็งคอลเซ็นเตอร์ รวมถึงควรติดตามข้อมูลเกี่ยวกับแอปพลิเคชันที่เป็นอันตราย และติดตามข่าวสารด้านความมั่นคงปลอดภัยสม่ำเสมอ
วันที่เผยแพร่ 3 สิงหาคม 2565 เวอร์ชัน 1.1
TB-CERT Thailand Banking Sector CERT
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
ภายใต้ สมาคมธนาคารไทย

รู้ไว้ปลอดภัยห่างไกลแก๊งมิจฉาชีพ (1/2)

จากกรณีที่ประชาชนถูกแก๊งมิจฉาชีพหลอกให้ติดตั้ง App อันตราย โดยการส่ง link URL ปลอมเป็นเว็บไซต์ขององค์กรมีชื่อเสียง มาให้ Click เพื่อติดตั้ง App เราจะมีวิธีการป้องกันก่อนตกเป็นเหยื่อแก๊งมิจฉาชีพเหล่านี้ได้อย่างไร และเมื่อรู้ตัวว่าตกเป็นเหยื่อแล้วเราจะมีวิธีการรับมืออย่างไร รวมถึงเราจะมีวิธีตรวจสอบมือถือเราอย่างไรว่าปลอดภัยจาก App อันตรายที่เราอาจจะโหลดมาติดตั้งโดยไม่รู้ตัว

7 ข้อป้องกันภัยจากแก๊งมิจฉาชีพปลอมแปลง App อันตราย

1 อ่านและสังเกต Permission หรือสิทธิ์ของ App บน Android ทุกครั้งก่อนกดยอมรับ (Accept) เพื่อติดตั้ง App นั้นโดยสังเกตดังนี้

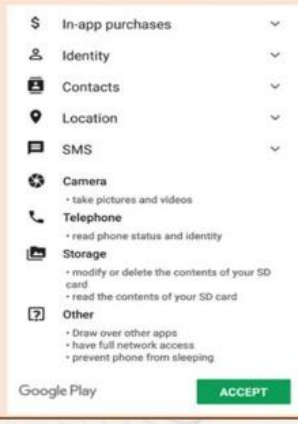
- มีการขอสิทธิ์ (Permission) ใช้งาน ที่มากเกินประเภทของ App หรือไม่ ตัวอย่างเช่น การติดตั้ง App ประเภทถ่ายรูป แต่กลับมีการขอสิทธิ์ ในการส่งหรืออ่านข้อความ SMS (Send/View SMS) ซึ่งมีโอกาสที่จะเป็น App อันตรายและไม่ควรกดยอมรับเพื่อติดตั้ง App นั้น

ตัวอย่าง สิทธิ์ของ App (Permission) ที่ผู้ใช้งานควรมั่นสังเกต เช่น

1. การขอส่งหรืออ่านข้อความ SMS (Send/View SMS)
2. การขอบันทึกหน้าจอ (Take picture and record video)
3. การขอแสดงทับบนหน้าจอของ App อื่น (Display over other apps)

จุดสังเกตก่อนติดตั้ง App
โดยตรวจสอบก่อนกดยอมรับ (Accept)

ก่อนติดตั้งควรกดปุ่ม เพื่อขยายอ่านรายละเอียดการขอสิทธิ์ (Permission) ใช้งานของ App



จุดสังเกตหลังติดตั้ง App
กรณียอมรับ (Accept) การติดตั้งไปแล้ว
สามารถตรวจเช็คได้จากการตั้งค่า (Setting) และไปที่ App permissions เพื่อตรวจสอบการขอสิทธิ์ (Permission) ใช้งานของ App

หมายเหตุ กรณี Android เวอร์ชันที่ต่างกัน อาจจะมีการแสดงเมนูที่ต่างกันบ้างเล็กน้อย

2 ไม่ติดตั้ง App ใด ๆ ที่ไม่ได้อยู่ใน play store หรือ ที่มีคนส่ง link ให้ติดตั้ง

3 ปิดการใช้งานการติดตั้ง App ที่ไม่รู้จัก (Turn off "Install unknown apps") โดยตรวจเช็คได้จากการตั้งค่า (Setting) ตามตัวอย่างข้างล่าง

4 ไม่เปิดเผยข้อมูลส่วนตัว Pin code หรือ รหัสผ่านใด ๆ ที่ใช้ในการทำธุรกรรม แม้ว่าจะไม่เกี่ยวข้องกับ Mobile Banking ก็ตาม

5 ติดตั้งโปรแกรมป้องกันมัลแวร์

6 ตระหนักอยู่เสมอว่าบุคคลในโลกสื่อโซเชียล ต่าง ๆ อาจเป็นมิจฉาชีพ

7 ไม่ใช้รหัสผ่านสำหรับการปลดล็อกหน้าจอเป็นค่าเดียวกันกับรหัสผ่านสำหรับเข้าใช้ App ของธนาคาร รวมทั้ง App อื่น ๆ ด้วย

วันที่เผยแพร่ 27 กันยายน 2565

"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง" ภายใต้ สมาคมธนาคารไทย TB-CERT

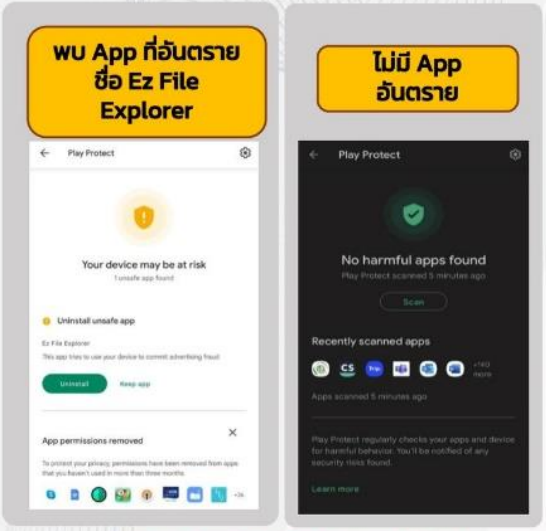
(2/2)

รู้ไว้ปลอดภัยห่างไกลแก๊งมิจฉาชีพ

2 ข้อควรหมั่นตรวจสอบ

1. หมั่นตรวจสอบอีเมลหรือ SMS แจ้งเตือนการเข้าใช้งานบัญชีหรือเมื่อมีการเคลื่อนไหวทางบัญชี

2. ควรเปิดการใช้งาน Google play Protect เพื่อตรวจสอบการติดตั้ง App ที่อันตราย โดยการเข้าไปที่ เปิดแอป Google Play Store จากนั้นเลือกไอคอนโปรไฟล์ที่ด้านขวาบน และเลือก Play Protect จากนั้น เลือกการตั้งค่า Setting และเปิดการสแกนแอปด้วย Play Protect จากนั้น ระบบจะค้นหา App ที่เป็นอันตราย หากเจอให้ Uninstall



ภาพตัวอย่างจากหน้าจอมือถือประเภท Android

3 ข้อควรรู้เมื่อตกเป็นเหยื่อแก๊งมิจฉาชีพหลอกให้ติดตั้ง App อันตราย

1. ให้นำซิมออกจากเครื่อง และตัดการเชื่อมต่อ WI-FI หรือหากใช้ WI-FI ของที่อยู่อาศัย ให้ปิด WI-FI หรือ router เป็นการชั่วคราวเพื่อหยุดการเชื่อมต่อทางไกล หากจอค้างทำให้ไม่สามารถตัดการเชื่อมต่อ WI-FI ได้ ให้ทำการปิดเครื่องโดยกดปุ่ม Power ค้างและกดปุ่ม volume down แช่ไว้ 10 วินาที ซึ่งการปิดเครื่องอาจจะมีผลต่อหลักฐานสำหรับการพิสูจน์หลักฐานทางดิจิทัล

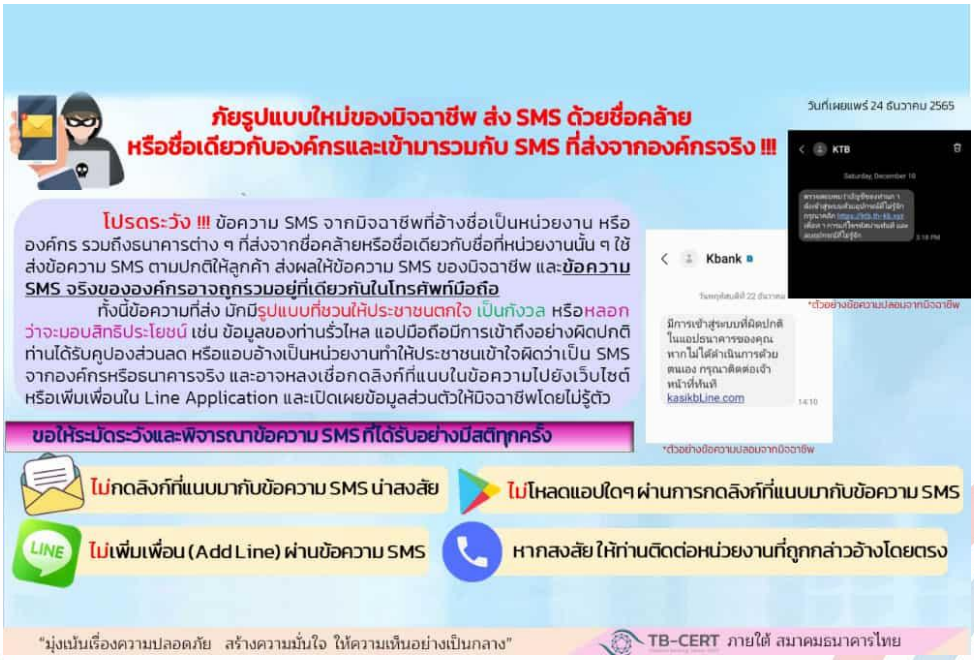
2. โทรแจ้งธนาคารขอระงับบัญชี ขอคำแนะนำเบื้องต้นและแจ้งความกับตำรวจ

3. พิจารณาทำการพิสูจน์หลักฐานทางดิจิทัล (Mobile Device Forensics) เพื่อวิเคราะห์การทำงานของ App อันตราย

วันที่เผยแพร่ 27 กันยายน 2565

"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง" ภายใต้ สมาคมธนาคารไทย TB-CERT


3 ส. เตือนใจ
ระวังภัย SMS Phishing
TLP: WHITE
วันที่เผยแพร่ 8 ธันวาคม 2565
สงสัย: ดูชื่อผู้ส่ง
สังเกต: เนื้อหาข้อความ
ส่งข่าว: แจ้ง call center หรือช่องทางติดต่อธนาคาร
BankInfo
Today 4:38 AM
บัญชีของคุณถูกระงับ โปรดยืนยันข้อมูล https://bankinfo.internet.com
XXX อย่าคลิก !!!
Subject
Text Message
จากข่าวที่ปรากฏเมื่อช่วงปลายปีที่แล้ว เกี่ยวกับภัย SMS Phishing ที่แพร่หลาย ซึ่งเหตุการณ์ดังกล่าวยังคงเกิดขึ้นต่อเนื่อง และหลายท่านคงได้เห็นมีการส่งต่อเพื่อเตือนภัยกันอีกมากในช่วงนี้
TB-CERT ขอแนะนำ
คาถา 3 ส.
เพื่อให้ทุกคนร่วมกันระวังภัย ดังนี้
สงสัย
สังเกต
ส่งข่าว
สงสัย
ชื่อผู้ส่งที่ไม่ใช่ชื่อธนาคาร หรือที่ใช้ชื่อคล้ายธนาคาร
สังเกต
เนื้อหาข้อความเชิญชวน เกินจริง และมีลิงก์แนบ
ส่งข่าว
ให้ธนาคารที่ถูกปลอมแปลง ทราบ เพื่อยับยั้งความเสียหาย
TB-CERT
มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง
Version 1.0


ภัยรูปแบบใหม่ของมิจฉาชีพ ส่ง SMS ด้วยชื่อคล้าย หรือชื่อเดียวกับองค์กรและเข้ามารวมกับ SMS ที่ส่งจากองค์กรจริง !!!
วันที่เผยแพร่ 24 ธันวาคม 2565
KTB
Kbank
*ตัวอย่างข้อความปลอมจากมิจฉาชีพ
ไปรดระวัง !!! ข้อความ SMS จากมิจฉาชีพที่อ้างชื่อเป็นหน่วยงาน หรือองค์กร รวมถึงธนาคารต่าง ๆ ที่ส่งจากชื่อคล้ายหรือชื่อเดียวกับชื่อที่หน่วยงานนั้น ๆ ใช้ส่งข้อความ SMS ตามปกติให้ลูกค้า ส่งผลให้ข้อความ SMS ของมิจฉาชีพ และข้อความ SMS จริงขององค์กรอาจถูกรวมอยู่ที่เดียวกันในโทรศัพท์มือถือ
ทั้งนี้ข้อความที่ส่ง มักมีรูปแบบที่ชวนให้ประชาชนตกใจ เป็นกังวล หรือหลอกว่าจะมอบสิทธิประโยชน์ เช่น ข้อมูลของท่านรั่วไหล แอปมือถือมีการเข้าถึงอย่างผิดปกติ ท่านได้รับคูปองส่วนลด หรือแอบอ้างเป็นหน่วยงานทำให้ประชาชนเข้าใจผิดว่าเป็น SMS จากองค์กรหรือธนาคารจริง และอาจหลงเชื่อกดลิงก์ที่แนบในข้อความไปยังเว็บไซต์ หรือเพิ่มเพื่อนใน Line Application และเปิดเผยข้อมูลส่วนตัวให้มิจฉาชีพโดยไม่รู้ตัว
ขอให้ระมัดระวังและพิจารณาข้อความ SMS ที่ได้รับอย่างมีสติทุกครั้ง
ไม่กดลิงก์ที่แนบมากับข้อความ SMS น่าสงสัย
ไม่โหลดแอปใดๆ ผ่านการกดลิงก์ที่แนบมากับข้อความ SMS
ไม่เพิ่มเพื่อน (Add Line) ผ่านข้อความ SMS
หากสงสัยให้ท่านติดต่อหน่วยงานที่ถูกกล่าวอ้างโดยตรง
"มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง"
TB-CERT ภายใต้ สมาคมธนาคารไทย

ภาพกิจกรรมการสร้าง Trust และ Collaboration ระหว่างสมาชิก








รายนามคณะกรรมการ TB-CERT วาระปี 2021-2023

ประธานกรรมการ	**คุณชัชวัฒน์ อัศวรักวงศ์** Managing Director and Chief Information Security Officer ธนาคารกสิกรไทย
รองประธานกรรมการ	**คุณสมภพ สุรัตนกวีกุล** Director, IT Security Office, Information Technology Department ธนาคารแห่งประเทศไทย
ที่ปรึกษากิตติมศักดิ์และกรรมการด้านสื่อสาร	**ดร. กิตติ โฆษะวิสุทธิ์** Senior Vice President, Head of Security Management ธนาคารกรุงเทพ
กรรมการด้านสื่อสาร	**คุณเชิดศักดิ์ นานา** Senior Vice President, IT Security ธนาคารกรุงไทย
กรรมการด้านวิชาการ	**คุณพาวิต ศักดิ์สูง** Head of Digital Technology Security ธนาคารไทยพาณิชย์
กรรมการด้านวิชาการ	**คุณประกลกฤษ แสงชูวงศ์** Team Head of Information, Security Detection and Response ธนาคารทหารไทยธนชาต
กรรมการด้านเทคนิค	**คุณภคพงศ์ จุลวงศาศิลป์** Head of Cyber Security Department ธนาคารกรุงศรีอยุธยา
กรรมการด้านเทคนิค	**คุณวชิราวัชร์ มหาทัพกฤษ** Inspector general, Chief Information Security Officer ธนาคารออมสิน
กรรมการ	**คุณยศ กิมสวัสดิ์** Head of Payment System Office สมาคมธนาคารไทย
คณะเลขานุการ	**คุณปรมินทร์ ช่วงมณี** CERT Manager
	คุณธาวินี วงศ์วิศว์ CERT Relations Manager

หน่วยงานสมาชิก TB-CERT

	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร Bank of Agriculture and Agricultural Cooperatives		ธนาคารกรุงไทย จำกัด (มหาชน) Krung Thai Bank Public Company Limited
	บริษัท บริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน) Bangkok Commercial Asset Management Public Company Limited		ธนาคารแลนด์ แอนด์ เฮ้าส์ จำกัด (มหาชน) Land and Houses Bank Public Company Limited
	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) Bank of Ayudhya Public Company Limited		ธนาคารมิซูโฮ จำกัด สาขากรุงเทพฯ Mizuho Bank Bangkok Branch
	ธนาคารกรุงเทพ จำกัด (มหาชน) Bangkok Bank Public Company Limited		บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด National Credit Bureau Company Limited
	ธนาคารแห่งประเทศไทย Bank of Thailand		บริษัท เนชั่นแนลดิจิทัลไอดี จำกัด National Digital ID Company Limited
	ธนาคารแห่งประเทศจีน (ไทย) จำกัด Bank of China		บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด National ITMX Company Limited
	ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน) CIMB Thai Bank Public Company Limited		บริษัท ศูนย์ประมวลผล จำกัด Processing Center Company Limited
	ธนาคารซิตี้แบงก์ Citibank N.A.		ธนาคารไทยพาณิชย์ 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 เพื่อรายย่อย จำกัด (มหาชน) The Thai Credit Retail 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
	ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน) Kiatnakin Phatra Bank Plc.		

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