Volume 10/2566
19 กรกฎาคม 2566

Cyber Attack โจรที่ติดตามตัวไปทุกที่ กับ Cyber Security ที่ทุกคนต้องรู้

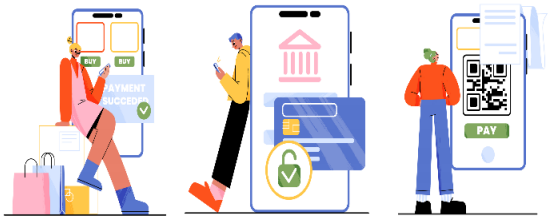
จัดทำโดย
นางสาวสุมิตรา ตั้งสมวรพงษ์
ฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

สรุปประเด็นสำคัญ:

- **ณ ช่วงต้นปี 2566 ประเทศไทยมีผู้ใช้อินเทอร์เน็ตสูงถึง 61.21 ล้านคน หรือ 85.3% ของประชากรทั้งหมดในประเทศ สูงกว่าค่าเฉลี่ยโลกที่อยู่ที่ 64.4%** และคนไทยใช้เวลาในระบบอินเทอร์เฉลี่ยคนละ 7 ชั่วโมง 4 นาทีต่อวัน ซึ่งถือว่าคนไทยใช้เวลาบนโลกอินเทอร์เน็ต สูงสุดติด 10 อันดับแรกของโลก และ**มีพฤติกรรมการทำธุรกรรมทางอินเทอร์เน็ตผ่านมือมากยิ่งขึ้น หรือสามารถเข้าถึงโลกอินเทอร์ได้อย่างรวดเร็วเพียงปลายนิ้วสัมผัส ขณะที่ภัยคุกคามทางไซเบอร์รุนแรงขึ้น เสมือนเปิดประตูหน้าหาข้อมูลและโอกาส แต่หากขาดความระมัดระวังก็เสมือนเปิดประตูหลังต้อนรับโจร**
- ขณะที่**มูลค่าความเสียหายจากภัยคุกคามทางไซเบอร์ทั่วโลกมีมูลค่าเพิ่มมากขึ้นอย่างต่อเนื่อง** โดยมีการคาดการณ์ว่า ในปี 2566 มูลค่าความเสียหายจะสูงถึง 8 ล้านล้านดอลลาร์สหรัฐ และจะเพิ่มขึ้นเป็น 10.5 ล้านล้านดอลลาร์สรัฐ ในปี 2568 ซึ่ง**หน่วยงานทั่วโลกตระหนักถึงความสำคัญเร่งด่วนในการจัดการปัญหาด้านภัยคุกคามทางไซเบอร์** สอดคล้องกับจากการสำรวจของ World Economic Forum ปีล่าสุดที่เปิดเผยว่า **95% ของผู้นำองค์กรยอมรับว่าความปลอดภัยด้านไซเบอร์มีความสำคัญ ควรนำไปพิจารณาเป็นส่วนหนึ่งของแผนกลยุทธ์ในการจัดการความเสี่ยงระดับองค์กร**
- **ในประเทศไทยภัยคุกคามของอาชญากรรมทางไซเบอร์เพิ่มมากขึ้น เมื่อพิจารณาจากการรับแจ้งความออนไลน์เกี่ยวกับภัยคุกคามของอาชญากรรมทางไซเบอร์ในช่วง 1 ปีที่เปิดให้บริการ** พบว่า มีจำนวนคดี 218,210 คดี รวม**มูลค่าความเสียหาย 31,579 ล้านบาท หรือ 85 ล้านบาทต่อวัน ซึ่งส่วนใหญ่เป็นความเสียหายในระดับบุคคล**ในคดีเกี่ยวกับการหลอกลวงผ่านแก๊งค์คอลเซ็นเตอร์ คดีเกี่ยวกับการซื้อขายสินค้าหรือบริการผ่านทางออนไลน์แต่ไม่ได้รับสินค้า การปล่อยกู้นอกระบบผ่านแอพพลิเคชั่น การหลอกลงทุนแบบแชร์ลูกโซ่ เป็นต้น
- **ในส่วนความเสียหายในระดับองค์กรหรือหน่วยงานตามการรายงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)** เปิดเผยว่า ภัยคุกคามทางไซเบอร์ ในช่วงวันที่ 1 ตุลาคม 2564 ถึง 30 กันยายน 2565 มีเหตุการณ์เกิดขึ้น 551 เหตุการณ์ โดย **2 ใน 3 เป็นการโจมตีโดยการแฮ๊กเว็บไซต์** (Hacked website) ของหน่วยงานราชการและหน่วยงานสำคัญ เป้าหมายส่วนใหญ่เป็นหน่วยงานการศึกษา หน่วยงานสาธารณสุข และนอกจากนี้ยังมีการ**คุกคามอื่น ๆ ที่บริษัทเอกชนได้รับผลกระทบ อาทิ การขัดขวางการเข้าถึงข้อมูลหรือระบบงาน การรั่วไหลของข้อมูล เป็นต้น ซึ่งบางกรณีใช้เวลานานในการแก้ไขปัญหา ซึ่งอาจส่งผลกระทบเป็นวงกว้าง**
- **ทุกภาคส่วนควรตระหนักถึงภัยคุกคามและร่วมมือกันป้องกัน ร่วมสร้างความปลอดภัยทางไซเบอร์ (Cyber Security) โดยตระหนักถึงภัย ระวังตัว ไม่ชัวร์ ไม่ Click ไม่แชร์ และทุกคนควรตระหนักถึงข้อเท็จจริงที่ว่า "ไม่มีการลงทุนใดให้ผลตอบแทนเกินจริงหรือการลงทุนที่มีการรับประกันผลตอบแทน" ดังนั้น อย่าหลงเชื่อ ต้องตรวจสอบข้อมูลไปยังหน่วยงานที่เกี่ยวข้องโดยตรง ให้ตั้งสติ อย่ารีบร้อนเร่งลงทุนตามการเร่งให้ลงทุนหรือเร่งให้ทำธุรกรรม ก็จะช่วยลดโอกาสในการถูกคุกคามทางไซเบอร์ได้**

เทคโนโลยีก้าวไกลตามไปทุกที่ ประชาชนไทยเข้าถึงโลกอินเทอร์เน็ตได้อย่างรวดเร็วเพียงปลายนิ้วสัมผัส ขณะที่ภัยคุกคามทางไซเบอร์รุนแรงขึ้น เสมือนเปิดประตูหน้าหาข้อมูลและโอกาส แต่หากขาดความระมัดระวังก็เสมือนเปิดประตูหลังต้อนรับโจร

ปัจจุบัน “อินเทอร์เน็ต” กลายเป็นปัจจัยที่ 5 ในการดำเนินชีวิตของเรา โดยเฉพาะอย่างยิ่งในช่วงที่มีการแพร่ระบาดรุนแรงของเชื้อโคโรน่าไวรัส 2019 (COVID-19) ที่ประชาชนปรับเปลี่ยนรูปแบบการดำเนินชีวิต โดยทำกิจกรรมออนไลน์ผ่านอินเทอร์เน็ตเพิ่มขึ้น



ทั้งการติดต่อสื่อสารผ่านอินเทอร์เน็ต (on-line communication) การทำงานทางไกล (remote station) การประชุม / การสัมมนาออนไลน์ (e-meeting and virtual seminar) การเรียนออนไลน์ (online study) การรับตรวจวินิจฉัยและรับคำปรึกษาจากแพทย์ผู้เชี่ยวชาญโดยตรงเกี่ยวกับอาการป่วยเบื้องต้นที่ไม่รุนแรงผ่านระบบออนไลน์ (telemedicine / e-Health) การซื้อขายหรือทำธุรกรรมผ่านช่องทางการตลาดออนไลน์ (Shopping on e-marketplace) ซึ่งจากรายงาน Digital 2023 ที่จัดทำโดย CrowdStrike Holdings, Inc.[1] เปิดเผยว่า **จากข้อมูล ณ ต้นปี 2566 มีผู้ใช้งานอินเทอร์เน็ตในประเทศไทยรวมสูงถึง 61.21 ล้านคน หรือคิดเป็น 85.3% ของประชากรทั้งหมดของประเทศ สูงกว่าค่าเฉลี่ยโลกที่มีการเข้าถึง 64.4%**

และผลการศึกษาจาก “รายงานผลการสำรวจพฤติกรรมของผู้ใช้อินเทอร์เน็ต ปี 2565” ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศษฐกิจและสังคม ประจำปี 2565 (Thailand Internet User Behavior 2022)[2] เปิดเผยว่า

- **คนไทยใช้เวลาในการเข้าถึงอินเทอร์เน็ตเฉลี่ยคนละ 7 ชั่วโมง 4 นาทีต่อวัน โดยเฉพาะในวันหยุดคนไทยใช้เวลาถึง 7 ชั่วโมง 27 นาที ซึ่งถือว่าคนไทยใช้เวลาบนโลกอินเทอร์เน็ตสูงสุดติด 10 อันดับแรกของโลก**[3]
- กิจกรรมออนไลน์ที่มีแนวโน้มเติบโตอย่างต่อเนื่อง ได้แก่ การติดต่อสื่อสาร การดูหนัง/ฟังเพลง การซื้อขายของ การทำธุรกรรม ทางการเงิน และการอ่านข่าว โพสต์บทความ หนังสือ
- **3 อุปกรณ์หลัก (devices) ที่นิยมใช้ในการเข้าถึงอินเทอร์เน็ต ได้แก่ โทรศัพท์เคลื่อนที่ (97.07%) รองลงมา** คือ แท็บเล็ต (Tablets) (19.35%) และแล็ปท็อป / โน้ตบุ๊ก (Laptop / Notebook computer) (18.42%)

ปัจจัยสนับสนุนสำคัญในการใช้อินเทอร์เน็ตเพิ่มมากขึ้น นอกจากพฤติกรรมการใช้ชีวิตที่เปลี่ยนแปลงไปแล้ว ปฏิเสธไม่ได้ว่าความครอบคลุมของสัญญาณอินเทอร์เน็ตก็มีความสำคัญ ซึ่งจากข้อมูลเปิดเผยโดยบริษัท ไทยคม จำกัด (มหาชน) ยังชี้ให้เห็นว่า **ปัจจุบันสัญญาณโทรศัพท์มือถือครอบคลุมมากกว่า 90% ของพื้นที่ประเทศไทย** และในพื้นที่ที่สัญญาณมือถือเข้ายังไม่ถึงประชาชนก็ยังสามารถต่อเชื่อมสัญญาณอินเทอร์เน็ตผ่านดาวเทียมได้

ดังนั้น อาจกล่าวได้ว่า **ประชาชนไทยมีความสะดวกสามารถทำธุรกรรมในเกือบทุกที่และตลอดเวลา ขณะเดียวกันการเข้าถึงอินเทอร์เน็ตได้สะดวกรวดเร็ว เราก็คอยสอดส่องระมัดระวังอาชญากรรมทางไซเบอร์ (Cyber Crime / Cyber Attack) เพื่อป้องกันไม่ให้เข้ามาสร้างความเสียหายให้เราในฐานะผู้ใช้อินเทอร์เน็ต**

---

[1] เป็นบริษัทในสหรัฐอเมริกาและจดทะเบียนซื้อขายในตลาด NASDAQ ให้บริการด้านเทคโนโลยีความปลอดภัยทางไซเบอร์ บริการคลาวด์เวิร์กโหลด และการรักษาความปลอดภัยเอนด์พอยต์ ข่าวกรองภัยคุกคาม และบริการตอบโต้การโจมตีทางไซเบอร์

[2] ดำเนินการสำรวจข้อมูลผ่านแบบสอบถามออนไลน์ จากกลุ่มตัวอย่างจำนวน 46,348 ราย ทั่วประเทศ ในช่วงเดือนเมษายน - กรกฎาคม 2565

[3] ข้อมูลจัดทำโดย Meltwater, and We Are Social โดยพิจารณาจากการใช้อินเทอร์เน็ตทั่วโลกของผู้ใช้อินเทอร์เน็ต อายุระหว่าง 16 - 64 ปี

หน่วยงานทั่วโลกตระหนักถึงความสำคัญเร่งด่วนในการจัดการปัญหาภัยคุกคามทางไซเบอร์ หลังการคุกคามทางไซเบอร์มีแนวโน้มรุนแรงขึ้น โดยคาดว่า ในปี 2568 มูลค่าความเสียหายทั่วโลกจากอาชญากรรมทางไซเบอร์จะพุ่งสูงถึง 10.5 ล้านล้านดอลลาร์สรัฐ

Cybercrime หรือ อาชญากรรมทางไซเบอร์ คือ เป็นอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ผ่านระบบอินเทอร์เน็ตและช่องทางออนไลน์ต่างๆ ซึ่งสร้างความเสียหายทางการเงินและชื่อเสียงทั้งในระดับบุคคล ครอบครัว องค์กร และระดับประเทศ โดยกองทุนการเงินระหว่างประเทศ (International Monetary Fund: IMF) ได้เผยแพร่รายงาน “The Global Cyber Threat” ในปี 2564[4] ได้ให้ความเห็นว่า **“การคุกคามทางไซเบอร์เป็นปัญหาระดับโลก โดยเฉพาะภัยคุกคามทางไซเบอร์ต่อระบบการเงินที่เพิ่มขึ้น และต้องอาศัยประชาคมโลกร่วมมือป้องกัน”** ซึ่งสอดคล้องกับการดำเนินโครงการของ**ธนาคารโลก (World Bank) ได้มีการจัดตั้งกองทุนชื่อ Cybersecurity Multi-Donor Trust Fund[5] ภายใต้โครงการ Digital Development Partnership Umbrella หรือ DDP เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับการคุกคามด้านไซเบอร์** และการให้ความช่วยเหลือทางด้านเทคนิคให้แก่ประเทศกำลังพัฒนา ในการสร้างหรือช่วยเพิ่มศักยภาพด้านความปลอดภัยในโลกไซเบอร์และสามารถใช้เทคโนโลยีได้อย่างมั่นคงปลอดภัย (Cyber Resilience)

Cybersecurity
MULTI-DONOR TRUST FUND

ทำความเข้าใจเกี่ยวกับอาชญากรรมทางไซเบอร์จากสำนักงานสอบสวนกลาง สหรัฐอเมริกา

จากเว็บไซต์ของสำนักงานสอบสวนกลาง (Federal Bureau of Investigation: FBI) ซึ่งเป็นหน่วยงานด้านข่าวกรองและความมั่นคงภายในของประเทศสหรัฐอเมริกา[6] ได้อธิบายเกี่ยวกับอาชญากรรมทางไซเบอร์ไว้เบื้องต้น ดังนี้

- **การหลอกลวงโดยการส่งอีเมล์ด้านธุรกิจ (Business email compromise: BEC)** อาศัยข้อเท็จจริงที่ปัจจุบันมีการใช้อีเมล์ในการติดต่อทั้งในเรื่องส่วนตัวและธุรกิจ และเป็นหนึ่งในอาชญากรรมออนไลน์ที่สร้างความเสียหายทางการเงินมากที่สุด

- **การโจรกรรมข้อมูลส่วนบุคคล (Identity theft)** เป็นอาชญากรรมที่เก่าแก่และยังคงมีอยู่ อาศัยความประมาทจากผู้ใช้งานอินเทอร์เน็ตและระบบอินเทอร์เน็ตที่มีป้องกันไม่ดี เพื่อเข้าถึงข้อมูลส่วนตัว อาทิ เลขที่บัตรประชาชน หมายเลขโทรศัพท์ เลขที่บัตรเครดิต อีเมล์ เป็นต้น และนำก่อคดีสร้างความเสียหายแก่เจ้าของข้อมูลโดยเจ้าของข้อมูลมิได้รับทราบหรือยินยอม เช่น การนำไปขอสินเชื่อ / ซื้อขายผ่านบัตรเครดิต

- **โปรแกรมการจับข้อมูลเป็นประกันเพื่อเรียกค่าไถ่ (Ransomwares)** เป็นการเขียนโปรแกรม (software and malwares) เพื่อกีดกันไม่ให้เจ้าของข้อมูลหรือระบบงานสามารถเข้าถึงข้อมูล ระบบงาน หรือเครือข่ายของตนเองได้ และต้องการให้เจ้าของข้อมูลหรือระบบงานจ่ายค่าไถ่เพื่อให้สามารถกลับมาเข้าถึงข้อมูลหรือเครือข่ายของตนได้อีกครั้ง

[4] https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

[5] https://www.worldbank.org/en/programs/cybersecurity-trust-fund

[6] https://www.fbi.gov/investigate/cyber

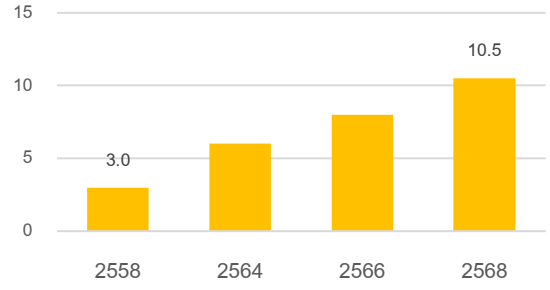
- **การหลอกลวงให้ผู้ใช้อินเทอร์เน็ตเปิดเผยข้อมูลละเอียดอ่อนโดยการส่งข้อความผ่านทางอีเมลหรือข้อความสั้นผ่านข้อความในโทรศัพท์มือถือ (Spoofing and phishing)** อาศัยความไว้วางใจที่ผู้ใช้งานอินเทอร์เน็ตมีต่อหน่วยงานที่ให้ความไว้วางใจ หลอกลวงให้กรอกข้อมูลสำคัญ อาทิ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน โดยนักต้มตุ๋นสามารถนำไปใช้ก่ออาชญากรรมทางการเงินต่อไป

มูลค่าความเสียหายจากอาชญากรรมไซเบอร์ทั่วโลกพุ่ง คาดว่าในปี 2566 มูลค่าความเสียหายฯ จะสูงถึง 8 ล้านล้านดอลลาร์สหรัฐ และจะเพิ่มขึ้นเป็น 10.5 ล้านล้านดอลลาร์สรัฐ ในปี 2568

จากรายงาน “2022 Official Cybercrime Report” ที่จัดทำโดยบริษัท Cybersecurity Ventures[7] ได้คาดการณ์ว่ามูลค่าความเสียหายจากอาชญากรรมทางไซเบอร์ทั่วโลก[8] จะเพิ่มขึ้นจาก 3 ล้านล้านดอลลาร์สหรัฐในปี 2558 เป็น 10.5 ล้านล้านดอลลาร์สหรัฐในปี 2568 (ภาพที่ 1) และ**ประเมินว่า ในปี 2566 แต่ละวันทั่วโลกจะเกิดความเสียหายจากอาชญากรรมทางไซเบอร์รวมกันมีมูลค่าสูงถึง 21.9 พันล้านดอลลาร์สรัฐ หรือ ประมาณ 771.5 พันล้านบาทต่อวัน** โดยเฉพาะความเสียหายจาก Ransomware ที่ Cybersecurity Ventures ประเมินว่าจะเพิ่มขึ้นอย่างรวดเร็ว โดยคาดว่าในปี 2574 จะมีมูลค่าความเสียหายจะสูงถึง 265 พันล้านดอลลาร์สหรัฐ (ภาพที่ 2)

ภาพที่ 1 มูลค่าความเสียหายที่เกิดขึ้นทั่วโลก จากอาชญากรรมทางไซเบอร์

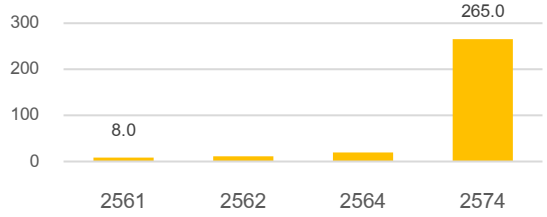
หน่วย: ล้านล้านดอลลาร์สหรัฐ



ที่มา: 2022 Official Cybercrime Report by Cybersecurity Venture

ภาพที่ 2 มูลค่าความเสียหายที่เกิดขึ้นทั่วโลก จาก Ransomwares

หน่วย: พันล้านดอลลาร์สหรัฐ



ที่มา: 2022 Official Cybercrime Report by Cybersecurity Venture

จากความร้ายแรงของการคุกคามด้านไซเบอร์ หน่วยงานต่างๆ ให้ความสำคัญเพิ่มมากขึ้น ซึ่ง จากรายงาน Global Cybersecurity Outlook 2023 ของ World Economic Forum ที่เผยแพร่เมื่อเดือนมกราคม 2566[9] ได้เปิดเผยว่า **95% ของผู้นำองค์กรยอมรับว่าความปลอดภัยด้านไซเบอร์มีความสำคัญควรนำไปพิจารณาเป็นส่วนหนึ่งของแผนกลยุทธ์ในการจัดการความเสี่ยงระดับองค์กร** (organization’s enterprise risk-management strategic) และพิจารณาเพิ่มการกำกับดูแลด้านความมั่นคงทางไซเบอร์ (cyber-resilience governance) เข้าไปในแผนธุรกิจขององค์กรด้วย

[7] บริษัทวิจัยและสื่อสิ่งพิมพ์ชั้นนำระดับโลกที่เผยแพร่ข้อมูลเศรษฐกิจดิจิทัลโลกและข้อมูลสถิติที่สำคัญเกี่ยวกับความปลอดภัยด้านไซเบอร์

[8] ประเมินจากความเสียหายจากข้อมูลเสียหาย (damage and destruction of data) การโจรกรรมเงิน (stolen money) การสูญเสียประสิทธิผล (lost productivity) การละเมิดทรัพย์สินทางปัญญา (theft of intellectual property) การขโมยข้อมูลส่วนบุคคลและข้อมูลทางการเงิน (theft of personal and financial data) การยักยอก (embezzlement) การฉ้อโกง (fraud) การหยุดชะงักของการดำเนินธุรกิจตามปกติหลังการโจมตี (post-attack disruption to the normal course of business) การกู้คืนและการลบข้อมูลที่ถูกแฮ็กข้อมูลและระบบ (restoration and deletion of hacked data and systems) และความเสียหายต่อชื่อเสียง (reputational harm)

[9] https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

นอกจากนี้ จากรายงาน “Industries boost cyber defenses against growing number of attack” ที่จัดทำโดยบริษัทมูดีส์ อินเวสเตอส์เซอร์วิส (Moody’s)[10] ให้ข้อมูลเพิ่มเติมว่า **ธุรกิจที่มีความเสี่ยงในการตกเป็นเหยื่อของการคุกคามทางไซเบอร์ ได้แก่ กลุ่มสาธารณูปโภคขั้นพื้นฐาน เช่น หน่วยงานให้บริการไฟฟ้า ประปา โรงพยาบาล ผู้ให้บริการเครือข่ายและเทคโนโลยีการสื่อสาร หน่วยงานของรัฐ เป็นต้น**

ในประเทศไทยมีภัยคุกคามของอาชญากรรมทางไซเบอร์เพิ่มขึ้น ซึ่งจากสถิติการรับแจ้งความผ่านระบบออนไลน์ พบว่า ในช่วง 1 ปี มีมูลค่าความเสียหายสูงถึง 85 ล้านบาทต่อวัน ส่วนใหญ่เป็นความเสียหายระดับบุคคล ขณะที่ความเสียหายระดับองค์กร / หน่วยงานส่วนใหญ่เป็นการแฮ็กเว็บไซต์ โดยเป้าหมายการโจมตี คือ หน่วยงานภาครัฐ หน่วยงานสาธารณสุข ซึ่งอาจส่งผลกระทบเป็นวงกว้าง ดังนั้น ทุกภาคส่วนควรตระหนักถึงภัยคุกคามและร่วมมือกันป้องกัน

ในประเทศไทยมีภัยคุกคามของอาชญากรรมทางไซเบอร์มีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง จากสถิติการรับแจ้งความผ่านระบบการรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ ในช่วงเดือนมีนาคม - ธันวาคม 2565 หรือในช่วง 10 เดือนแรกที่เปิดระบบให้บริการประชาชน พบว่า มีผู้เข้ามาแจ้งความ 163,091 คดี มีมูลค่าความเสียหายรวมกว่า 27,305 ล้านบาท หรือมีมูลค่าการเสียหายสูงถึง 91 ล้านบาทต่อวัน[11] โดยกว่า 50% ของมูลค่าความเสียหาย หรือประมาณ 15,800 ล้านบาท เป็นการหลอกลวงผ่านแก๊งค์คอลเซ็นเตอร์หลอกลวงผ่านทางออนไลน์ด้วยวิธีการต่าง ๆ ตามมาด้วยคดีเกี่ยวกับการซื้อขายสินค้าหรือบริการผ่านทางออนไลน์แต่ไม่ได้รับสินค้า การปล่อยกู้นอกระบบผ่านแอพพลิเคชั่น การหลอกลงทุนแบบแชร์ลูกโซ่ เป็นต้น ซึ่งมีมูลค่าความเสียหายรวมประมาณ 1,230 ล้านบาท และอันดับที่ 3 คือ แฮ็กระบบคอมพิวเตอร์ การเรียกค่าไถ่ทางคอมพิวเตอร์ การคุกคามทางเพศ หลอกให้ไปทำงานต่างประเทศ และ**ความเสียหายจากอาชญากรรมทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้นเรื่อย ๆ โดยในช่วง 1 ปีนับจากเปิดระบบรับให้บริการ พบว่า จำนวนคดีสูงถึง 218,210 คดี มีมูลค่าความเสียหายรวม 31,579 ล้านบาท หรือมีมูลค่าการเสียหายสูงถึง 85 ล้านบาทต่อวัน**

เมื่อพิจารณา**ความเสียหายจากคดีที่แจ้งความผ่านระบบออนไลน์ พบว่า ส่วนใหญ่เป็นความเสียหายในระดับบุคคล ทั้งนี้อาจเนื่องจากกรณีความเสียหายโดยตรงต่อหน่วยงานหรือองค์กร หน่วยงานจะประสานงานขอความช่วยเหลือโดยตรงจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)** ภายใต้สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งจากจากรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ที่จัดทำโดย ศปช. เปิดเผย**สถิติภัยคุกคามทางไซเบอร์ ในช่วงวันที่ 1 ตุลาคม 2564 ถึง 30 กันยายน 2565 พบว่า มีเหตุการณ์เกิดขึ้น 551 เหตุการณ์**[12] (ตารางที่ 1) พบว่า

- **2 ใน 3 เป็นการโจมตีโดยการแฮ็กเว็บไซต์ (Hacked website) ของหน่วยงานราชการและหน่วยงานสำคัญ เป้าหมายส่วนใหญ่เป็นหน่วยงานการศึกษา หน่วยงานสาธารณสุข** ซึ่งมีเว็บไซต์และระบบงานต่าง ๆ ที่ให้บริการอยู่เป็นจำนวนมาก และหน่วยงานต่าง ๆ ที่มีระบบไอทีเป็นเอกเทศ ยากต่อการดูแลจากหน่วยงานกลาง ขาดความสม่ำเสมอในการตรวจสอบความปลอดภัย ทำให้ง่ายต่อการโจมตี

[10] https://www.moodys.com/web/en/us/about/insights/data-stories/cyber-risks-are-rising.html

[11] ข่าวทำเนียบรัฐบาล; https://www.thaigov.go.th/news/contents/details/63924

[12] รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ห้วงวันที่ 1 ตุลาคม 2564 ถึง 30 กันยายน 2565 ที่นำเสนอต่อที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 1/2566 เมื่อวันที่ 5 มกราคม 2566

- เหตุการณ์ที่พบมากที่สุด คือ การแฮ็กเว็บไซต์เพื่อแฝงหน้าเว็บไซต์พนันออนไลน์ (gambling website) ในเว็บไซต์ของหน่วยงาน เพื่อให้ผู้เข้าใช้งานเว็บไซต์สามารถเข้าถึงเว็บไซต์พนันออนไลน์เพิ่มขึ้น
- ตามมาด้วย การโจมตีโดยการเปลี่ยนแปลงหน้าเว็บไซต์ (website defacement) ของหน่วยงาน เพื่อทดสอบความสามารถของแฮ็กเกอร์หรือเป็นผลจากการเคลื่อนไหวของการเมืองของกลุ่มต่างๆ และ
- การสร้างหน้าเว็บไซต์เพื่อ Phishing อยู่บนเว็บไซต์ของหน่วยงานรัฐ และการฝังมัลแวร์อันตรายบนหน้าเว็บไซต์หน่วยงานเพื่อหลอกให้ผู้เข้าถึงเว็บไซต์ดาวน์โหลดไปติดตั้งในเครื่อง อาทิ การใช้ชื่อโดเมนคล้ายกับหน่วยงานจริงและสร้างหน้าเว็บไซต์คล้ายเว็บไซต์จริง เพื่อหลอกลวงให้ผู้ใช้งานกรอกข้อมูลส่วนตัว

ตารางที่ 1 จำนวนภัยคุกคามทางไซเบอร์ จำแนกตามประเภทภัยคุกคาม

ประเภทภัยคุกคาม	จำนวน	%
Hack Website	**367**	**66.6**
- Gambling website	186	33.8
- Website Defacement	125	22.7
- Website Phinishing	38	6.9
- Website Malware	18	3.3
จุดอ่อนช่องโหว่ (Vulnerability)	**63**	**11.4**
ข้อมูลรั่วไหล (Data Breach)	**48**	**8.7**
Ransomware	**21**	**3.8**
มัลแวร์ขโมยข้อมูลการเงิน (Emotet: Banking trojan)	**9**	**1.6**
การโจมตีเครื่องคอมพิวเตอร์อยู่ภายใต้การควบคุมและมีการติดต่อไปยังเซิร์ฟเวอร์ (Command and Control Server)	**6**	**1.1**
อื่นๆ	**37**	**6.7**
รวม	**551**	**100.0**

ที่มา: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)

- **รองลงมา คือ จุดอ่อนช่องโหว่ของระบบ (Vulnerability)** ซึ่งเหตุการณ์กว่าครึ่งหนึ่งเกิดกับหน่วยงานภาครัฐ
- **ข้อมูลรั่วไหล (Data Breach)** เกิดขึ้นกับหน่วยงานรัฐและเอกชนใกล้เคียงกัน
- **การโจมตีด้วย Ramsomware มีข้อสังเกตว่า เกิดขึ้นกับหน่วยงานสำคัญของภาครัฐและภาคเอกชนที่มีทุนจดทะเบียนสูง และกระจายตัวอยู่ในหลายอุตสาหกรรม** โดยการโจมตีนี้จะส่งผลให้หน่วยงานเจ้าของระบบไม่สามารถใช้ระบบงาน และ/หรือไม่สามารถใช้ระบบงานสำรองได้ ซึ่งการโจมตีแบบ Ramsomware ต้องใช้เวลานานและจำเป็นต้องอาศัยผู้เชี่ยวชาญภายนอกร่วมแก้ไขปัญหา

ภาพที่ 3 ตัวอย่างการคุกคามทางไซเบอร์ในประเทศไทย

ที่มา: เว็บไซต์ของหน่วยงานต่างๆ รวบรวมโดย SET Research

ความปลอดภัยทางไซเบอร์ (Cyber Security): ตระหนักถึงภัย ระวังตัว ไม่ชัวร์ไม่ Click ไม่แชร์

จากความสะดวกรวดเร็วในการเข้าถึงโลกอินเทอร์เน็ต พฤติกรรมการใช้อินเทอร์เน็ต และความรุนแรงของภัยคุกคามทางไซเบอร์ ทุกภาคส่วนควรมีการรณรงค์ให้ทุกคนตระหนักถึงความรุนแรงของภัยคุกคาม และร่วมกันป้องกันและร่วมสร้างความปลอดภัย เพื่อ ลดโอกาสการถูกคุกคามทางไซเบอร์ ซึ่งสรุปแนวทางการดำเนินการเพื่อความปลอดภัยทางไซเบอร์ เป็น ABCD-S เพื่อง่ายต่อการจดจำและนำไปใช้ (ภาพที่ 4) ดังนี้

ภาพที่ 4 สรุปแนวทางดำเนินการเพื่อความปลอดภัยทางไซเบอร์ แบบ ABCD-S

A-Access Control	ระมัดระวังการเข้าถึงอุปกรณ์ของเรา เหมือนเฝ้าระวังประตูไม่มีใครปลอมแปลงเข้ามา
B-Back Up	ระมัดระวังรักษาข้อมูลสำคัญ เหมือนเฝ้าระวังทรัพย์ที่เรามี
C-Cautions	ตระหนักถึงความเสี่ยงในการใช้งาน เหมือนเตรียมตัวระวังไม่เปิดโอกาสให้โจร
D-Devices	สอดส่องอุปกรณ์ให้ใช้งานได้อย่างปลอดภัย เหมือนเตรียมเครื่องมือทำมาหากินที่ปลอดภัย
S-Scan/Setting	สร้างเครื่องมือป้องกันและสอดส่องผู้แอบแฝง เหมือนตำรวจกวดขันคอยจับโจร

Access Control

ป้องกันผู้อื่นเข้าถึงอุปกรณ์ / ข้อมูล

- กำหนด password ในการเข้าใช้งาน / เข้าถึงข้อมูล ให้ยากต่อการคาดเดา และเปลี่ยนเป็นประจำ
- ตั้งค่าการยืนยันตัวตนแบบหลายปัจจัยในทุกอุปกรณ์และทุกบัญชี (Multi-factor Authentication) เช่น ยืนยันโดยลายนิ้วมือและตั้งค่า password
- ปิดระบบใช้งานหรือปิดล็อกหน้าจออุปกรณ์ (Log-off) ทุกครั้ง ที่ไม่ได้ใช้งานหน้าจอ

Back-up

สำรองข้อมูล

- ดำเนินการสม่ำเสมอ
- สำรองแบบ offline backup เช่น การสำรองใน External Harddisk เพื่อลดความเสียหายจากโจมตีโดย ransomware

Cautions

ระมัดระวัง

- การเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะ และอย่าทำธุรกรรมที่ละเอียดอ่อนใดๆ เมื่ออยู่บนเครือข่ายสาธารณะ
- การเปิดเผยข้อมูลส่วนตัวในระบบออนไลน์หรือในบัญชีโซเชียลมีเดีย / การใช้งาน file sharing ควรจำกัดสิทธิ์ในการเข้าถึงข้อมูล
- การลงโปรแกรมหรือ Application หากยังไม่มีการตรวจสอบแหล่งที่มาที่น่าเชื่อถือและมีความชัดเจน

Device

ดูแลทุกอุปกรณ์ให้พร้อมต้านภัยคุกคาม

- ติดตั้ง / Update ระบบปฏิบัติงานที่น่าเชื่อถือ และโปรแกรมป้องกันไวรัสหรือมัลแวร์ และกำหนดรอบในการตรวจสอบการคุกคามภายในเครื่อง
- ล็อกการต่อเชื่อมอุปกรณ์ที่ยังไม่ได้มีการตรวจสอบไวรัส / มัลแวร์ เช่น การปิดการเชื่อมต่อ USB เป็นต้น

Scan / Setting

หมั่นตรวจสอบการคุกคาม

- ตรวจสอบไวรัสในไฟล์ข้อมูล / อีเมล์ ก่อนเปิดทุกครั้ง
- ตรวจสอบ URL ให้ถูกต้อง ก่อนเข้าเยี่ยมชมเว็บไซต์

ที่มา: รวบรวมโดยฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

นอกจากการเตรียมตัว ตระหนักถึงภัย ระวังตัวตามที่กล่าวมาแล้วข้างต้นแล้ว จากการแจ้งความออนไลน์ที่มีคดีเรื่องการหลอกลวงผ่านระบบออนไลน์ที่มีจำนวนมาก **ทุกคนควรตระหนักถึงข้อเท็จจริงที่ว่า “ไม่มีการลงทุนใดให้ผลตอบแทนเกินจริงหรือการลงทุนที่มีการรับประกันผลตอบแทน” ดังนั้น อย่าหลงเชื่อ ต้องตรวจสอบข้อมูลไปยังหน่วยงานที่เกี่ยวข้องโดยตรง ให้ตั้งสติ อย่ารีบร้อนเร่งลงทุนตามการเร่งให้ลงทุนหรือเร่งให้ทำธุรกรรม ก็จะช่วยลดโอกาสในการถูกคุกคามทางไซเบอร์ได้**