

ความปลอดภัยทางไซเบอร์ (Cybersecurity)



นางสาวสายชล แซ่ลี้

ผู้อำนวยการสำนักประสานงาน (สทช.)
รักษาการผู้อำนวยการสำนักปฏิบัติการ

ตำแหน่งปัจจุบัน • ผู้อำนวยการสำนักประสานงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประสบการณ์ทำงาน • รักษาการผู้อำนวยการสำนักปฏิบัติการ

- ผู้อำนวยการกลุ่มงานส่งเสริมและสนับสนุนความร่วมมือทางวิชาการ ศูนย์พัฒนานโยบายดิจิทัลเพื่อเศรษฐกิจและสังคม สดช.
- ผู้อำนวยการกลุ่ม กองโครงสร้างพื้นฐานด้านมาตรฐานเทคโนโลยีดิจิทัล สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)
- ผู้อำนวยการกลุ่มงานมาตรฐาน สำนักธุรกรรมทางอิเล็กทรอนิกส์ สป.กก.
- รองผู้อำนวยการสำนักงานเตรียมการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สป.กก.)
- ผู้อำนวยการกลุ่มงานบริหารจัดการโครงสร้างพื้นฐาน สำนักส่งเสริมและพัฒนารัฐบาลอิเล็กทรอนิกส์ สป.กก.

การศึกษา

- 2544-2547 วท.ม.เทคโนโลยีสารสนเทศและการจัดการ มหาวิทยาลัยเชียงใหม่
- 2541-2543 ศศ.บ.การจัดการทั่วไป (คอมพิวเตอร์ธุรกิจ) สถาบันราชภัฏลำปาง
- 2538-2540 ปวส.คอมพิวเตอร์ธุรกิจ วิทยาลัยอาชีวศึกษาลำปาง

ผลงานสำคัญหรือทักษะหรือความสามารถพิเศษ

- 2559 โครงการเข้าใช้อินเทอร์เน็ตสาธารณะสู่ชุมชน
- 2560 โครงการยกระดับโครงสร้างพื้นฐานโทรคมนาคมเพื่อขับเคลื่อนเศรษฐกิจของประเทศ
กิจกรรมที่ ๑ การขยายโครงข่ายอินเทอร์เน็ตความเร็วสูงให้ครอบคลุมทั่วประเทศ เพื่อสนับสนุนการพัฒนาเศรษฐกิจภายในประเทศ (เน็ตประชารัฐ)
กิจกรรมที่ ๒ การเพิ่มประสิทธิภาพโครงข่ายอินเทอร์เน็ตระหว่างประเทศสู่การเป็น ASEAN Digital Hub
- 2565 โครงการเร่งรัดพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1
- 2566 คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

CERTIFICATES



นางสาวสายชล แซ่ลี้
ผู้อำนวยการสำนักประสานงาน (สภมช.)



วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหาร
จัดการความมั่นคงปลอดภัยไซเบอร์
ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนอง
ต่อภัยคุกคามไซเบอร์ทุกมิติ

พันธกิจ MISSIONS

เสนอแนะนโยบาย แผน ยุทธศาสตร์
และปรับปรุงกฎหมายว่าด้วยการรักษา
ความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง
กำหนดแนวทาง มาตรฐาน มาตรการ
ที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์
ทั้งในปัจจุบันและอนาคต

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์
ประมวลผล แจ้งเตือน และปฏิบัติการ
เพื่อป้องกัน รับมือ และลดความเสี่ยง
จากภัยคุกคามทางไซเบอร์

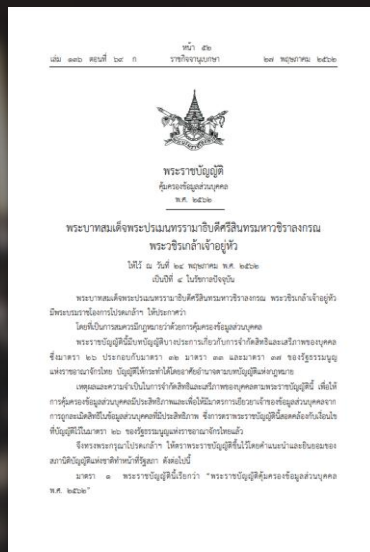
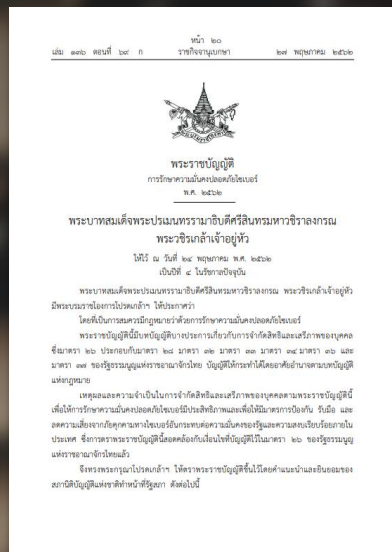
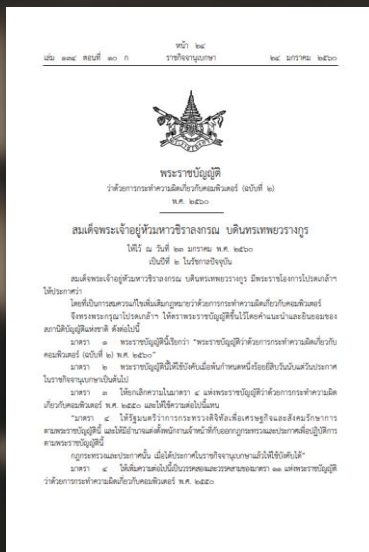
เป็นศูนย์กลางในการประสานความร่วมมือ
รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือ
หน่วยงานภาครัฐและเอกชนทั้งในประเทศ
และต่างประเทศเพื่อการรักษาความมั่นคง
ปลอดภัยไซเบอร์

เผยแพร่ความรู้ความเข้าใจ และสนับสนุน
การพัฒนาบุคลากรด้านการรักษา
ความมั่นคงปลอดภัยไซเบอร์



ประเทศไทยได้ออกกฎหมายและกำหนดหน่วยงานสำคัญหลายฉบับเพื่อเน้นการรักษาความมั่นคงทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

SECURE & TRUSTED ENVIRONMENT



- มาตรการคุ้มครองข้อมูลส่วนบุคคล
- สิทธิเจ้าของข้อมูล
- โกล่เกลี่ย ระงับข้อพิพาท



Incident Response
- Critical Information
Infrastructure
Protection

หมายเหตุ : ระดับวิกฤต
เป็นอำนาจหน้าที่ สำนักงาน
สภามันคงแห่งชาติ
(สมช.)

กำหนดความผิดและบทลงโทษ

- ความผิดที่ก่อข้อมูลคอมพิวเตอร์
และระบบคอมพิวเตอร์โดยตรง

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ๒๕๖๐

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

กฎหมายฉบับนี้ครอบคลุมการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การเข้าถึงและการเผยแพร่ข้อมูลเท็จ เป็นกฎหมายพื้นฐานสำหรับการดำเนินคดีกับผู้กระทำความผิดทางไซเบอร์

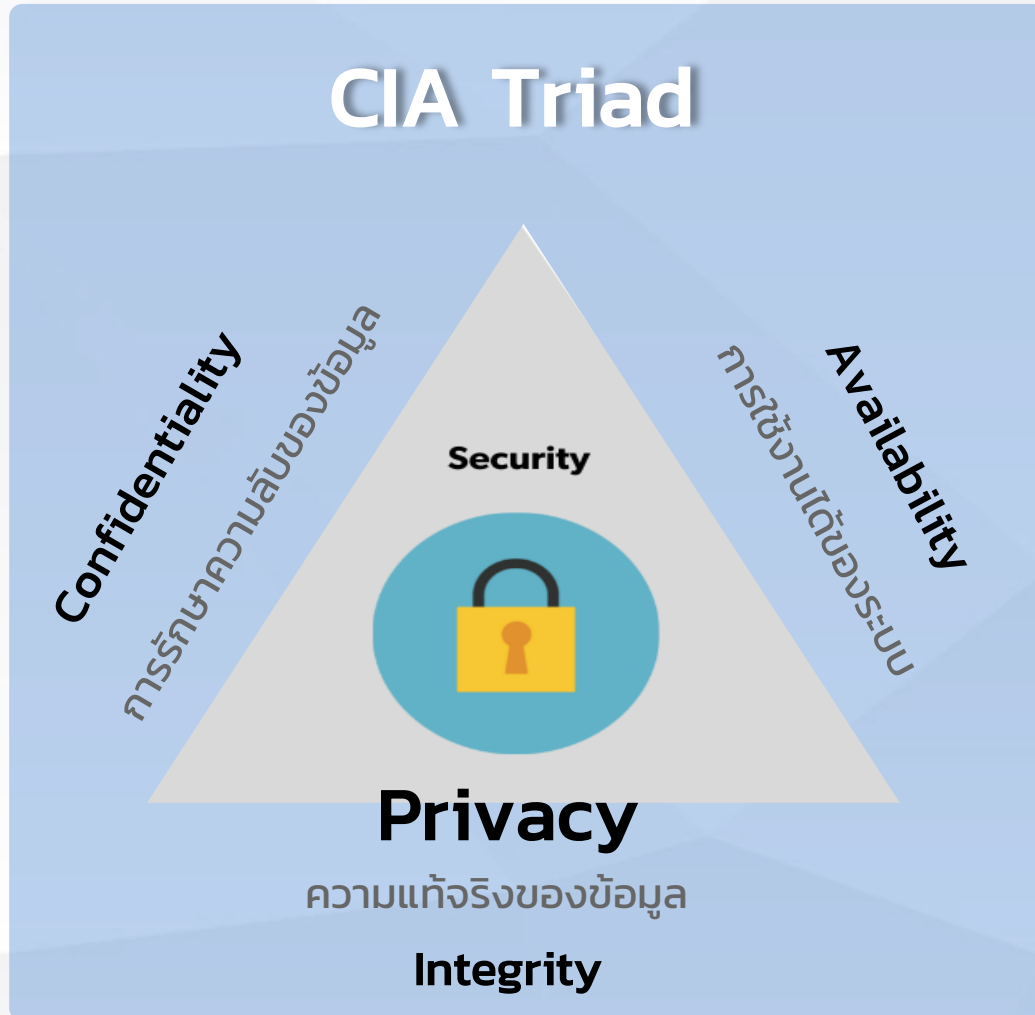
กฎหมายที่มีเป้าหมายเพื่อความมั่นคงแห่งชาติในโลกไซเบอร์ กฎหมายฉบับนี้บังคับให้องค์กรในภาคส่วนสำคัญ (เช่น การเงิน พลังงาน คมนาคม และสุขภาพ) ต้องดำเนินการมาตรการป้องกันโครงสร้างพื้นฐานสารสนเทศที่สำคัญ (Critical Information Infrastructure - CII) และให้สิทธิแก่รัฐบาลในการตรวจสอบและจัดการเหตุการณ์ทางไซเบอร์

มีเป้าหมายในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยกำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ และจัดเก็บข้อมูล พร้อมทั้งให้สิทธิกับเจ้าของข้อมูลในการควบคุมข้อมูลส่วนตัวและกำหนดบทลงโทษกรณีละเมิด



สร้างความตระหนัก และเสริมทักษะจำเป็นด้าน
ความมั่นคงปลอดภัยทางไซเบอร์

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น **ความลับสูงสุด** ผู้ที่สามารถเข้าถึงได้ คือ **ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น**
- เบอร์โทรของพนักงานในบริษัท จัดเป็น **ข้อมูลภายในเท่านั้น** ผู้ที่สามารถเข้าถึงได้ คือ **พนักงานบริษัททุกคน**

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มี ความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

การรักษาความปลอดภัยทางไซเบอร์คืออะไร



Cyber Security คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยจุดประสงค์ คือ เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม

ทั้งนี้หลายองค์กร ต่างให้ความสำคัญเรื่องระบบรักษาความปลอดภัยของข้อมูลไม่แพ้กัน เพราะหากลูกค้าหรือผู้ใช้บริการโดนโจรกรรมข้อมูลทางอิเล็กทรอนิกส์ไป อาจทำให้องค์กรเสียชื่อเสียงได้ เพราะฉะนั้น Cyber Security จึงมีความสำคัญ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง



สถานการณ์ภัยคุกคามไซเบอร์ระดับโลก

Ransomware เป็นการโจมตีที่มีสัดส่วนสูงสุด 23% ตามด้วย Data Theft และ Server Access ซึ่งมีสัดส่วน 13% และ 10% ตามลำดับ



1. Ransomware

ไฟล์ถูกเข้ารหัสทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ได้ โดยผู้ใช้งานจะต้องจ่ายเงินตามข้อความ “เรียกค่าไถ่” เพื่อปลดล็อกข้อมูลคืนมา



2. Data Theft

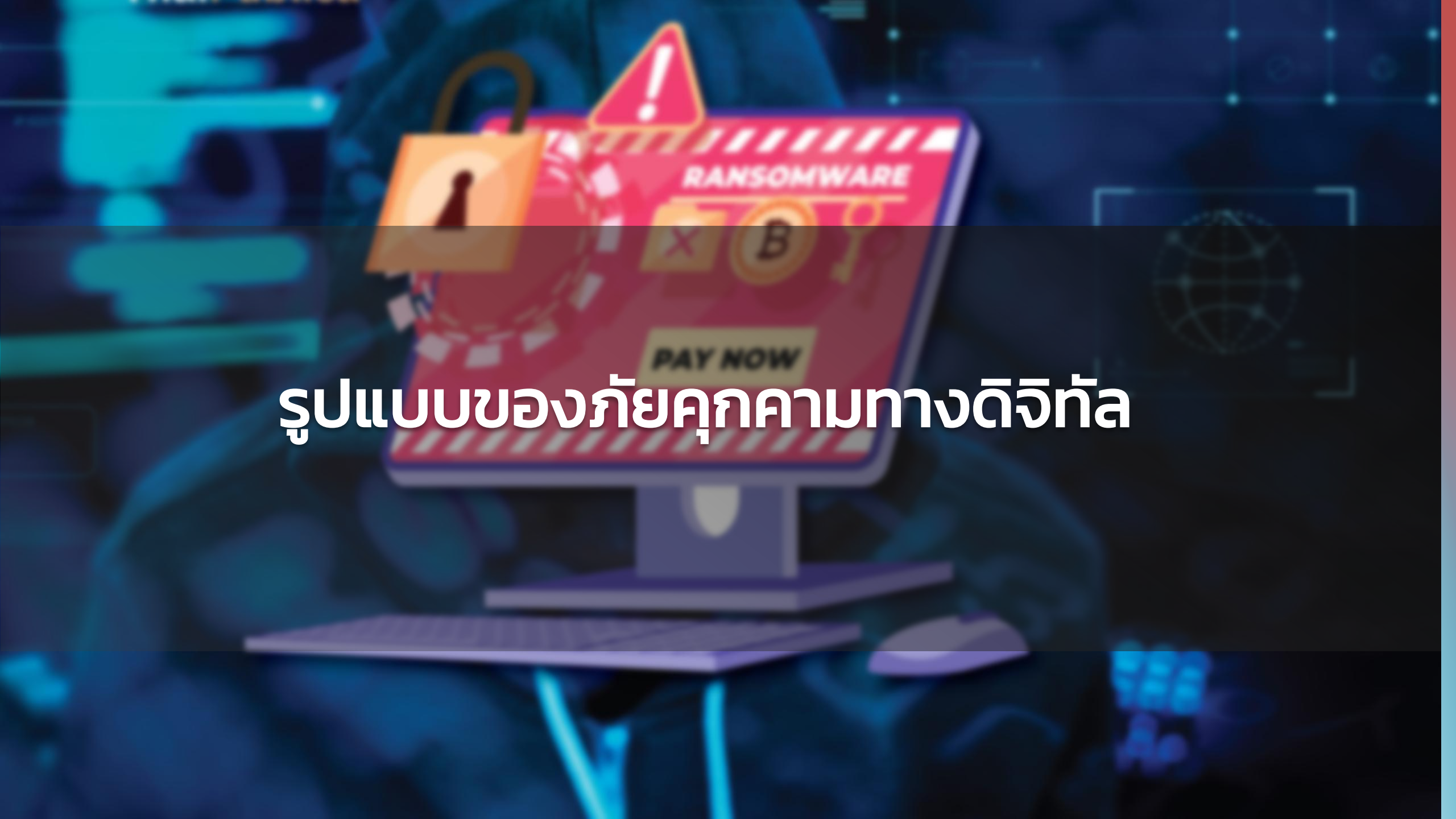
ส่วนใหญ่เกิดจากบุคคลภายในองค์กร ด้วยมองว่าข้อมูลเป็นสิทธิ์ของตน เนื่องจากเป็นผู้จัดทำขึ้น หรือจงใจจะเปิดการเข้าถึงข้อมูลเพื่อเปิดเผยการประพฤติมิชอบของนายจ้างจากมุมมองของสังคม



3. Server Access

การเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งอาจมีจุดประสงค์ในการขโมยข้อมูล แก้ไขปรับเปลี่ยน หรือทำให้หยุดชะงัก ไม่สามารถให้บริการแก่ผู้ใช้งานได้

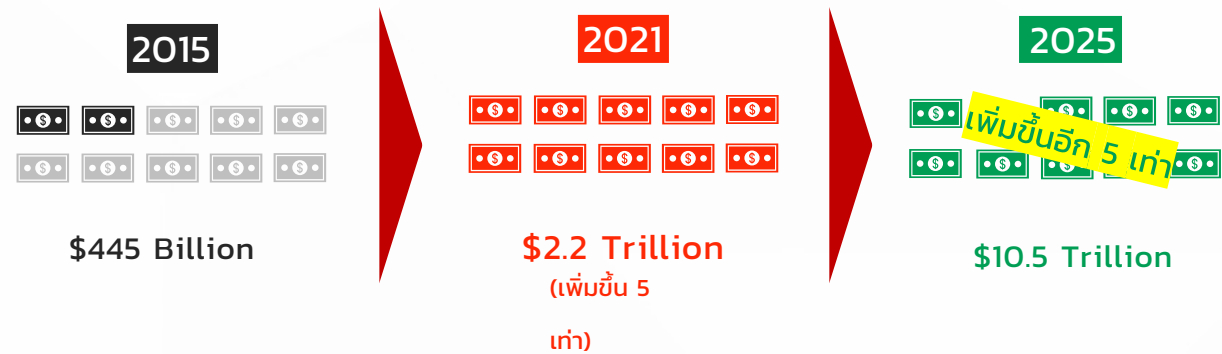
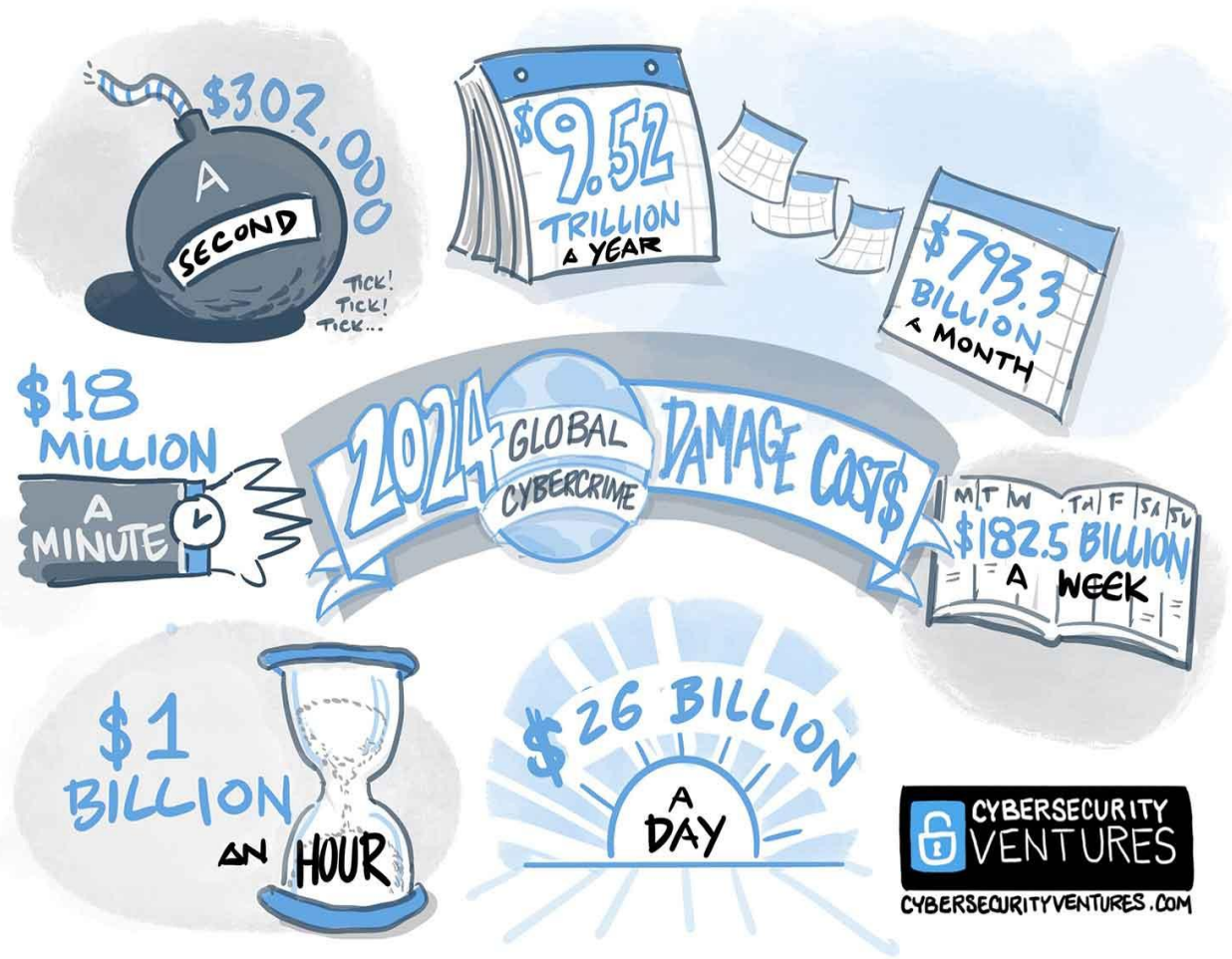


An illustration of a computer monitor displaying a ransomware interface. The screen is red with a yellow padlock icon on the left, a yellow warning triangle with an exclamation mark at the top center, and the word "RANSOMWARE" in white capital letters. Below this, there is a Bitcoin icon and a yellow button with the text "PAY NOW". The background is dark blue with glowing blue lines and a globe icon on the right.

รูปแบบของภัยคุกคามทางดิจิทัล

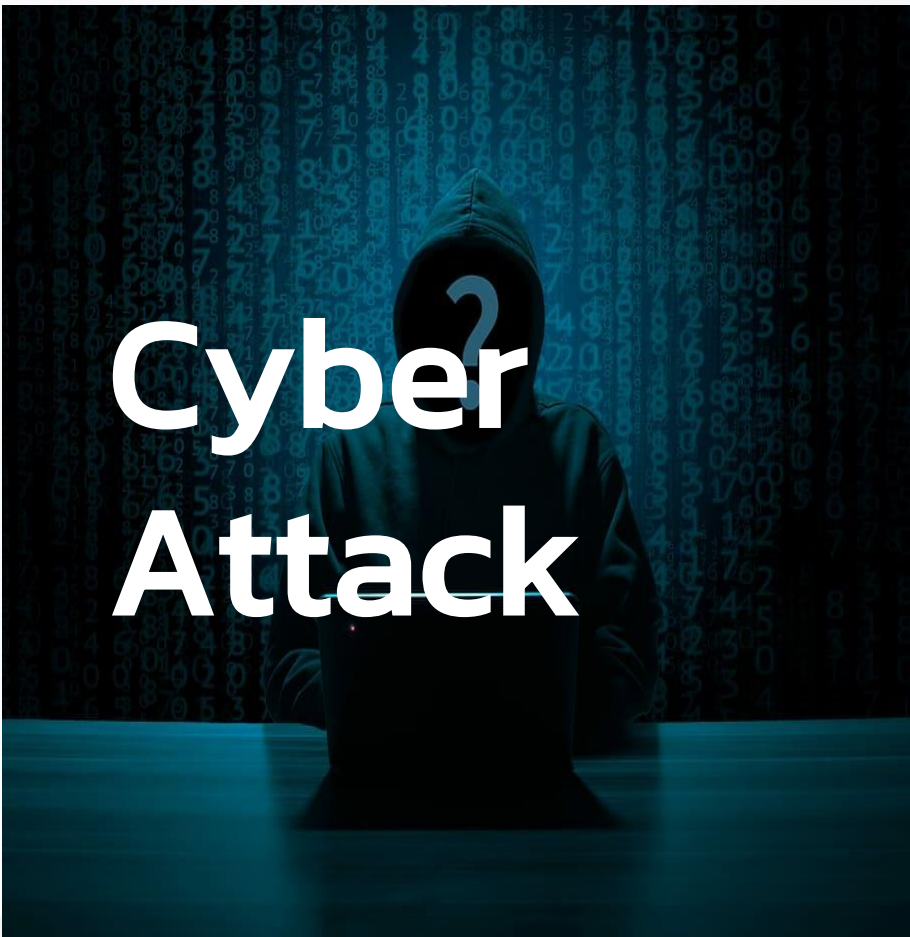
มูลค่าความเสียหายจากอาชญากรรมไซเบอร์ทั่วโลก

การแยกย่อยของต้นทุนความเสียหายจากอาชญากรรมทางไซเบอร์ทั่วโลกที่ Cybersecurity Ventures คาดการณ์ไว้ในปี 2024:



- 9.5 ล้านล้านเหรียญสหรัฐต่อปี
- 793 พันล้านเหรียญสหรัฐต่อเดือน
- 182.5 พันล้านเหรียญสหรัฐต่อสัปดาห์
- 26 พันล้านเหรียญสหรัฐต่อวัน
- 1 พันล้านเหรียญสหรัฐต่อชั่วโมง
- 18 ล้านเหรียญสหรัฐต่อนาที
- 302,000 เหรียญสหรัฐต่อวินาที

เป้าหมาย ของ Cyberattackers



Cyber Attack

- **บุคคล** : ผู้โจมตีอาจกำหนดเป้าหมายเป็นรายบุคคลเพื่อผลประโยชน์ส่วนตัว เช่น โดยการขโมยข้อมูลรับรองการเข้าสู่ระบบหรือเรียกค่าไถ่ข้อมูลส่วนบุคคล
- **ข้อมูลส่วนบุคคล** : ผู้โจมตีอาจพยายามขโมยข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น ข้อมูลรับรองการเข้าสู่ระบบ ข้อมูลทางการเงิน และหมายเลขประกันสังคม เพื่อขายในตลาดมืดหรือใช้เพื่อขโมยข้อมูลประจำตัว
- **ทรัพย์สินทางปัญญา** : ผู้โจมตีอาจพยายามขโมยข้อมูลที่เป็นกรรมสิทธิ์ เช่น ความลับทางการค้าและเทคโนโลยีที่เป็นกรรมสิทธิ์ เพื่อให้ได้เปรียบในการแข่งขันหรือขายข้อมูลให้กับบุคคลอื่น
- **โครงสร้างพื้นฐานที่สำคัญ** : การโจมตีทางไซเบอร์บนโครงสร้างพื้นฐานที่สำคัญ เช่น โครงข่ายไฟฟ้า โรงบำบัดน้ำ และระบบขนส่ง สามารถส่งผลกระทบร้ายแรงและทำให้การทำงานของบริการที่จำเป็นหยุดชะงักได้
- **หน่วยงานรัฐบาลและองค์กรทางการเมือง** : ผู้โจมตีอาจกำหนดเป้าหมายหน่วยงานรัฐบาลและองค์กรทางการเมืองเพื่อขโมยข้อมูลที่ละเอียดอ่อนหรือขัดขวางการดำเนินงานของหน่วยงาน
- **ธุรกิจ** : การโจมตีทางไซเบอร์ต่อธุรกิจอาจทำให้สูญเสียข้อมูลที่ละเอียดอ่อน สูญเสียทางการเงิน และทำลายชื่อเสียงของบริษัท

ภาพรวมของ Cybersecurity ในปัจจุบัน

ภัยคุกคามทางไซเบอร์มีความซับซ้อนและหลากหลายมากขึ้น

- รูปแบบการโจมตีพัฒนาอย่างต่อเนื่อง เช่น Ransomware-as-a-Service (RaaS), AI-driven phishing, และ Supply Chain Attacks
- กลุ่มแฮกเกอร์มักทำงานแบบองค์กร มีเป้าหมายชัดเจน และวางแผนระยะยาว

เป้าหมายหลักของการโจมตีเปลี่ยนไป

- จากองค์กรขนาดใหญ่ → สู่ธุรกิจขนาดกลางและเล็ก (SMEs)
- จากข้อมูลส่วนตัว → สู่การเจาะระบบโครงสร้างพื้นฐานสำคัญ เช่น พลังงาน, ระบบสาธารณสุข, การเงิน

การเปลี่ยนแปลงของสภาพแวดล้อมการทำงาน

- การทำงานแบบ Hybrid หรือ Remote Work ทำให้ขอบเขตการรักษาความปลอดภัยยากขึ้น
- อุปกรณ์ส่วนตัวของพนักงานกลายเป็นจุดอ่อนใหม่ (BYOD: Bring Your Own Device)

การใช้ AI และ Automation ในการรักษาความปลอดภัย

- ระบบ AI เริ่มมีบทบาทในการตรวจจับพฤติกรรมผิดปกติ
- แต่ในขณะเดียวกัน แฮกเกอร์ก็ใช้ AI ในการโจมตี เช่น Deepfake, Phishing ด้วยข้อความสมจริง

Cyber Crime Statistics 2025

The latest key cyber crime statistics, facts, and data from the industry's leading resources



500%

How much the median ransomware payment skyrocketed by in 2024.



\$55B

The amount that's been stolen via domestic and international business email compromise scams between October 2013 and December 2023.



32% of phishing impersonation attacks in Q4 2024 used Microsoft's brand and reputation to their gain.



\$12T

Cyber crime costs are expected to top this amount by 2025.



\$1.5B

How much North Korean nation-state hacker group TraderTraitor stole from Bybit's cryptocurrency exchange.



\$600 is the average price of passport data on the dark web.



50% of BEC emails were crafted using generative AI technologies.



55% of brand impersonation attacks stemmed from companies' own brands.

Cyber Security Statistics Data Sources:
Computer Crime Research Center (Jan 2024)
Check Point Research's Q4 2024 Brand Phishing Trends
FBI Alert Numbers F022625-PSA & F091124-PSA
NordPM's Dark Web Case Study
Perception Point's 2024 Cybersecurity Trends & Insights
Sophos State of Ransomware 2024 Report

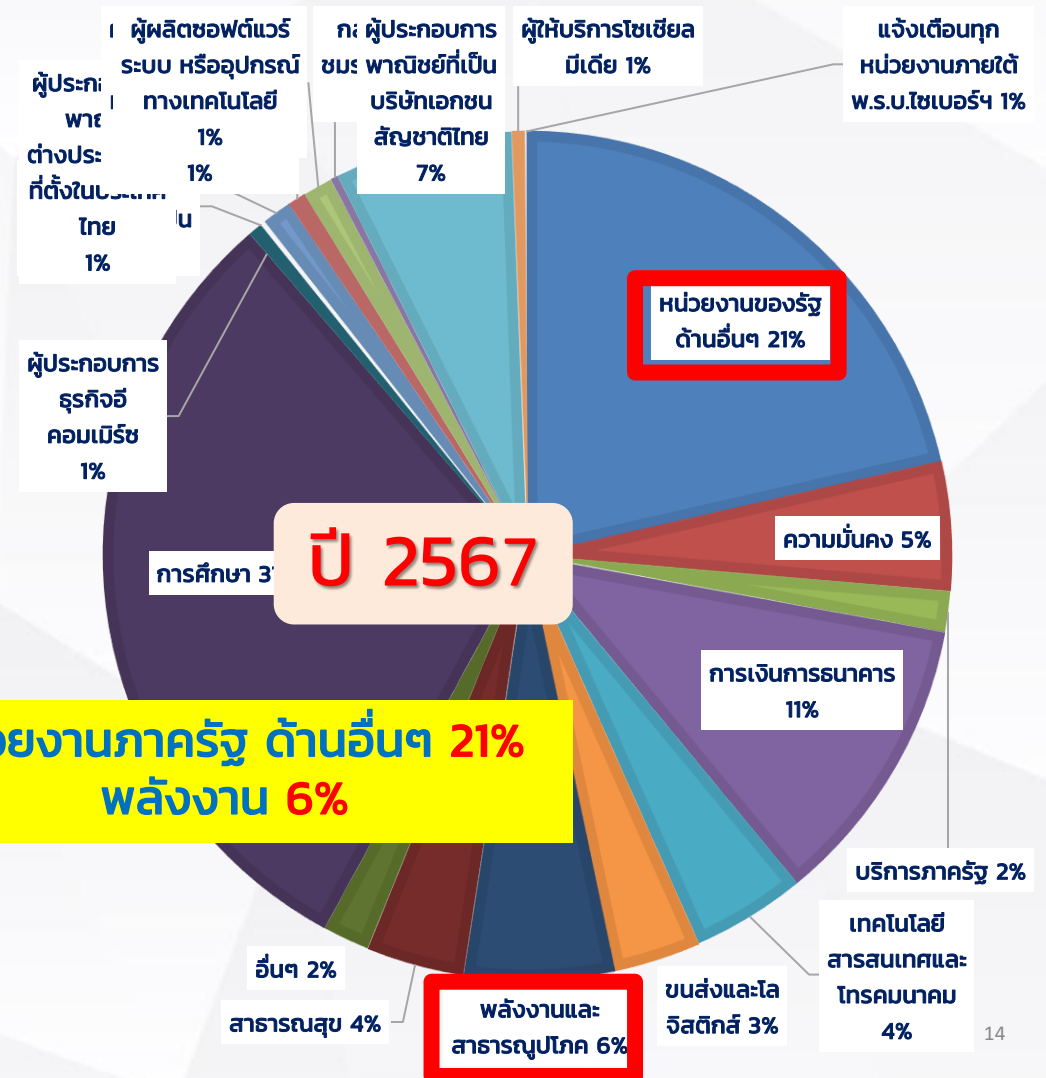
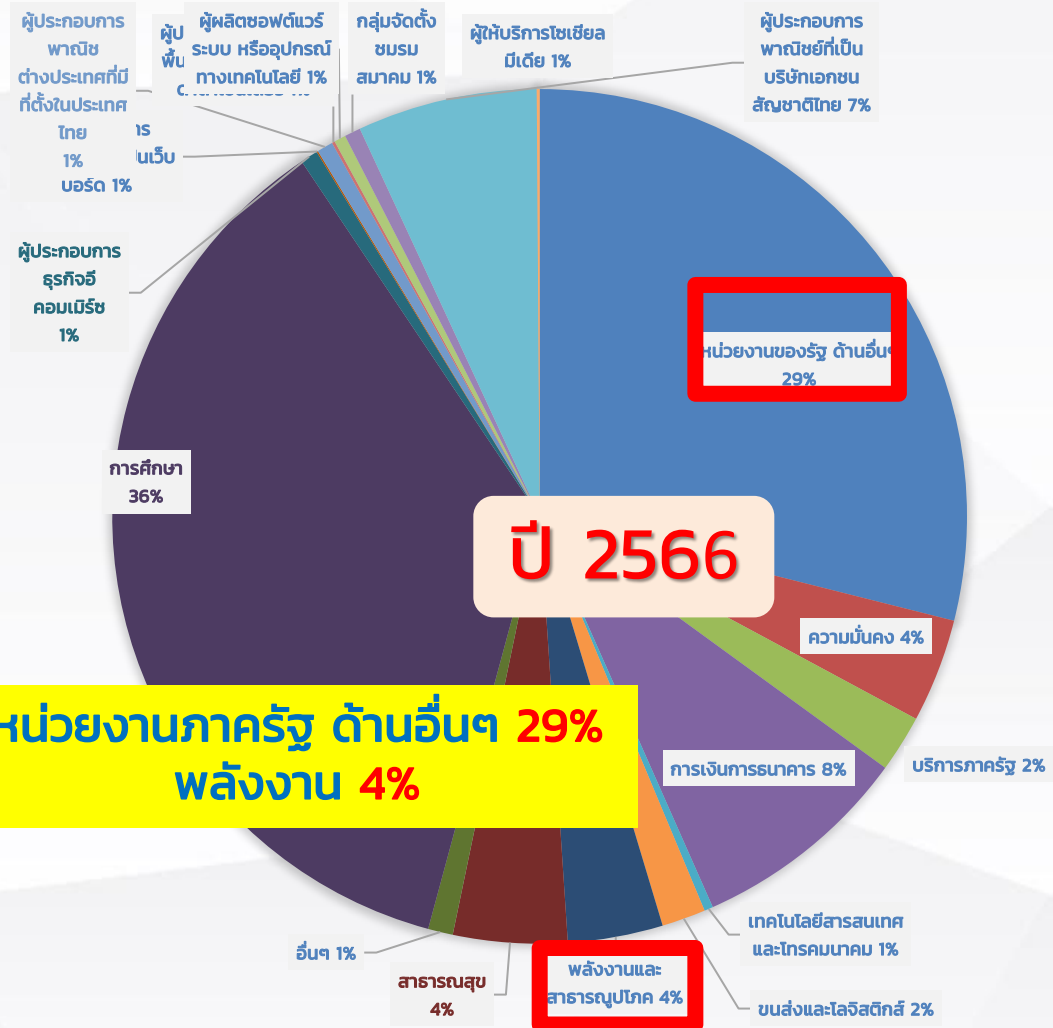
สถิติภัยคุกคามทางไซเบอร์

ประเภทภัยคุกคาม	ปีงบประมาณ 2565 (เหตุการณ์)	ปีงบประมาณ 2566 (เหตุการณ์)	ปีงบประมาณ 2567 (เหตุการณ์)	ห้วง ตุลาคม 2567 - พฤษภาคม 2568 (เหตุการณ์)
Intrusion Attempts	414	473	684	579
Fraud	54	221	181	418
Availability	2	5	1	62
Malicious Code	48	35	18	80
Intrusions	4	139	0	21
Information Content Security	0	53	7	272
Other	29	0	0	0
รวมทั้งสิ้น	551	1,808	1,827	1,432



ผลการดำเนินงานที่สำคัญภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล

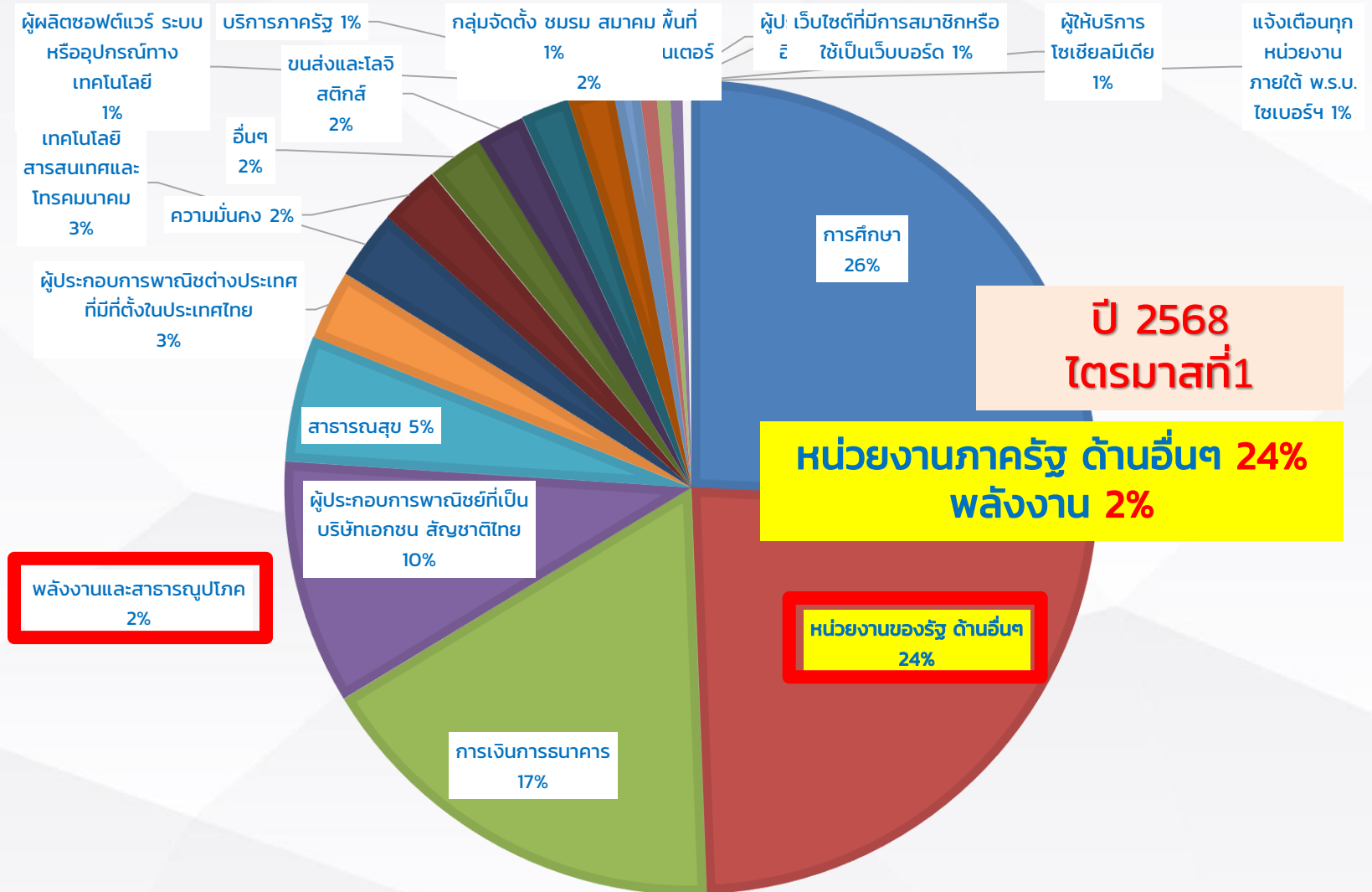
สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์



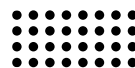
ผลการดำเนินงานที่สำคัญภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล

รวมทั้งสิ้น **1,656** เหตุการณ์

การศึกษา	427
หน่วยงานของรัฐ ด้านอื่นๆ	391
การเงินการธนาคาร	280
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	161
สาธารณสุข	83
ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	46
เทคโนโลยีสารสนเทศและโทรคมนาคม	46
ความมั่นคง	40
อื่นๆ	37
ขนส่งและโลจิสติกส์	32
พลังงานและสาธารณูปโภค	32
ผู้ประกอบการให้เข้าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	30
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	17
บริการภาครัฐ	11
กลุ่มจัดตั้ง ชมรม สมาคม พื้นที่	9
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	8
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	3
ผู้ให้บริการโซเชียลมีเดีย	2
แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ	1



ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์



First Name	Last Name	Account Name	Mobile	Email	Last Modified Date	Created Date	Contact ID	Account ID	Customer Created Date
นภสร	คำสิงห์	นภสร คำสิงห์เรือง	81-86 am	am@il.com	03/25 03/00	00	vY5Z 0C	lUx	03/20
ศิริภา	ศิริพร	ศิริพร นทร	81-86 sirip	sirip@om.com	03/25 03/00	00	vYY7 0C	lxV	03/20
ธนพร(นาง)	สงวน	ธนพร สงวน	61-97 poc	poc@mail.com	03/25 03/00	00	o0m 0C	mQA	03/20
ปริญญ์	สรวดี	ปริญญ์ สรวดี	88-24 mo	mo@msd	15/23 03/00	00	tKF 0C	msd	03/20
สุวิมล	ธนิช	สุวิมล ธนิชลาภ	65-54 kw	kw@com	19/25 03/00	00	vkm 0C	nLA	03/20
นำวัน	ณัฐ	นำวัน ณัฐ	61-91 na	na@aill.com	01/25 03/00	00	rOM 0C	nk	03/20
อุบลรัตน์	ธนิช	อุบลรัตน์ พรสุด	86-84 djd	djd@m	07/25 03/00	00	r4 0C	oS	03/20
บัณฑิต	ทอง	บัณฑิต ทองดี	92-04 par	par@il.com	07/25 03/00	00	jJ 0C	y7	03/20
ประสิทธิ์	ละออง	ประสิทธิ์ ละออง	90-22 boc	boc@aill.com	03/24 03/00	00	ma 0C	pBY	03/20
มาลี	บุรุษ	มาลี บุรุษ	85-92 e l	el@gmail.com	04/25 03/00	00	Eg 0C	pe4	03/20
เพ็ญศรี	เจียร	เพ็ญศรี เจียร	61-45 ch	ch@ail.com	03/25 03/00	00	wh8 0C	qW	03/20
สุกัญญา	รัตน	สุกัญญา รัตน	81-15 ihw	iww@om.com	20/25 03/00	00	wK 0C	qZ8	03/20
สิริพงษ์	ใจ	สิริพงษ์ ใจ	98-57 kar	kaw@om.com	07/25 03/00	00	woO 0C	rB	03/20
ศิริชัย	มิตร	ศิริชัย มิตร	80-05 nar	nar@igmail.c	03/25 03/00	00	53 0C	rUR	03/20
วรรณภา	ผ่อง	วรรณภา ผ่อง	64-22 wai	wai@com	03/25 03/00	00	xj 0C	rx7	03/20
สิริพงษ์	บุญ	สิริพงษ์ บุญ	92-35 bu	bu@pracom	03/25 03/00	00	HQ 0C	sPo	03/20
จิราภา	พินิจ	จิราภา พินิจ	93-83 nij	nij@mail.com	22/25 03/00	00	iSz 0C	ssN	03/20
นงนุช	นฤ	นงนุช นฤ	97-97 nac	nac@com	01/25 03/00	00	khv 0C	tl5	03/20

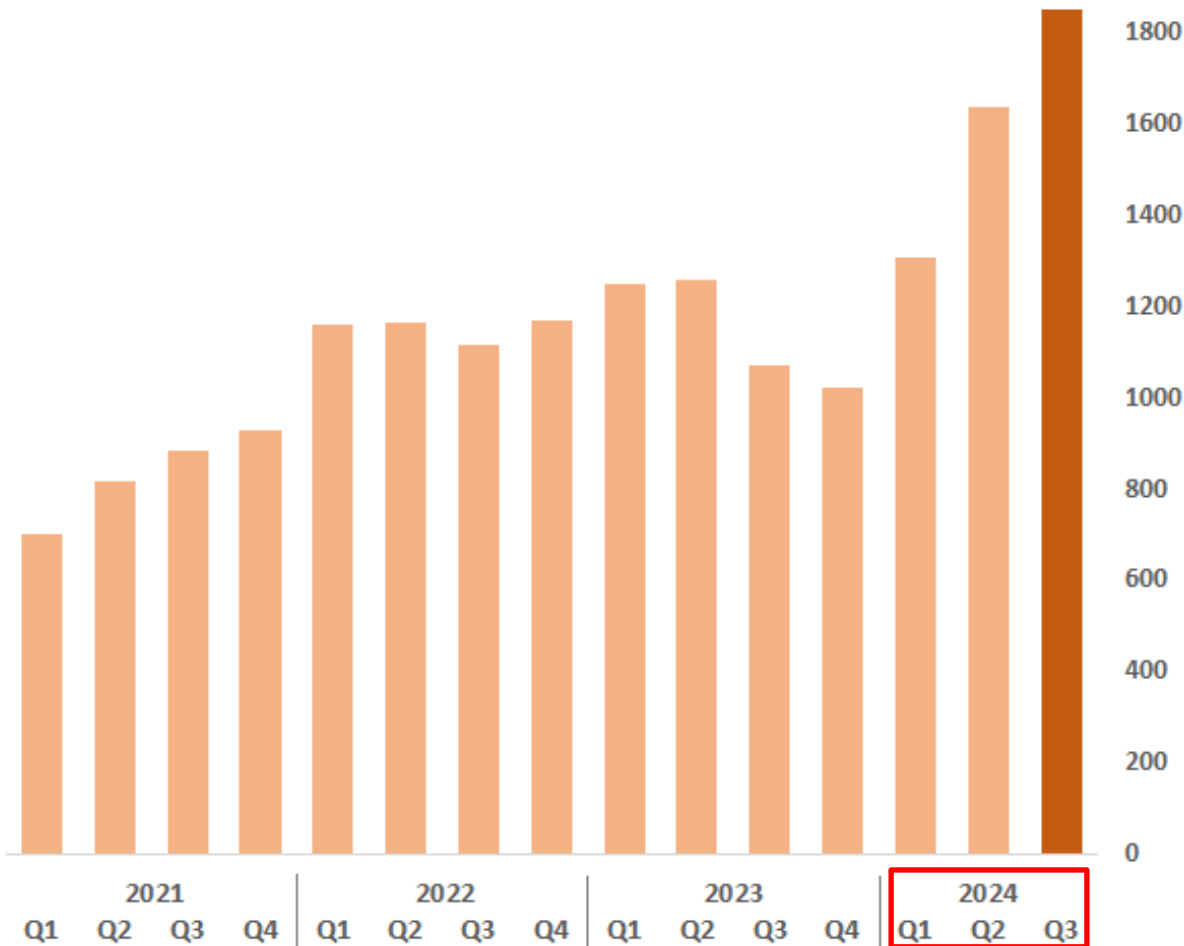
Citizen ID.	Consent	Update Date/Time	Contact Info	Customer	Date of Men	Email..	First Name	First Name	Frequently Use			
31		09	amuramur EMail:amuramur@gmail.com	T.0611	TH	amuramur@gmail.com	amuramur	amuramur	Parent Directory		-	
 Executive_office/	2023-03-11 10:57	-										
 Facebook Messenger C..>	2023-06-28 16:59	1.2K										
 Facebook Messenger C..>	2022-07-18 10:29	1.1K										
 Logo.png	2020-06-23 09:59	93K										
 PM25.php	2024-03-12 09:17	10K										
 UpRightSchool/	2022-06-14 13:50	-										
 _groups/	2022-06-14 13:50	-										
 about.html	2020-06-19 11:07	23K										

Index of /wp-content/uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 2016/	2020-11-07 11:08	-	
 2017/	2020-11-07 11:08	-	
 2018/	2022-10-24 14:00	-	
 2019/	2020-12-30 14:39	-	
 2020/	2020-12-01 00:05	-	
 2021/	2021-12-01 07:00	-	
 2022/	2022-12-01 07:01	-	
 2023/	2023-12-01 00:07	-	
 2024/	2024-12-01 00:04	-	

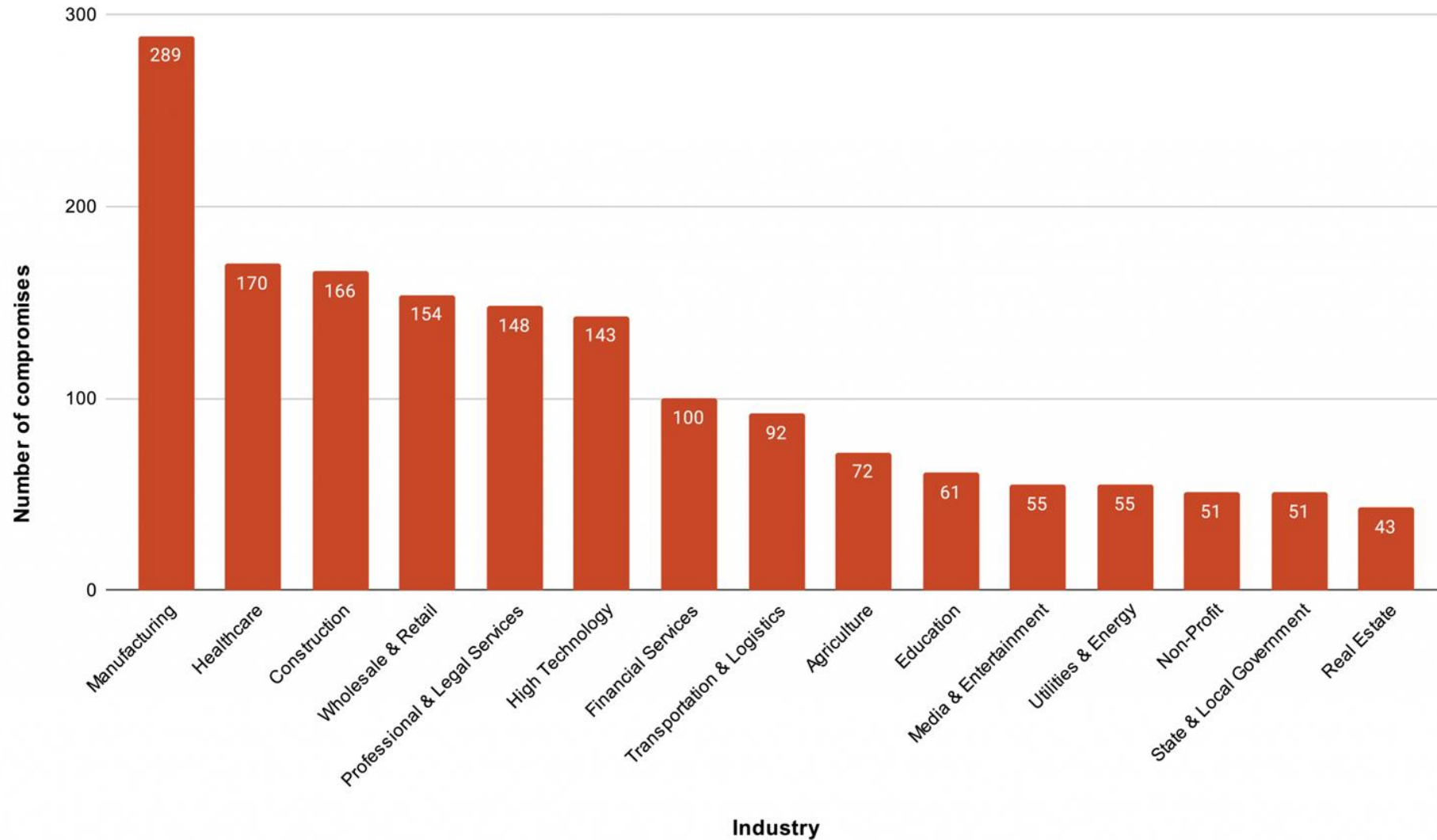
2024: การโจมตีทางไซเบอร์ทั่วโลกพุ่งสูงขึ้น 75%

Avg. Weekly Cyber Attacks per Organization
(Global 2021-2024)

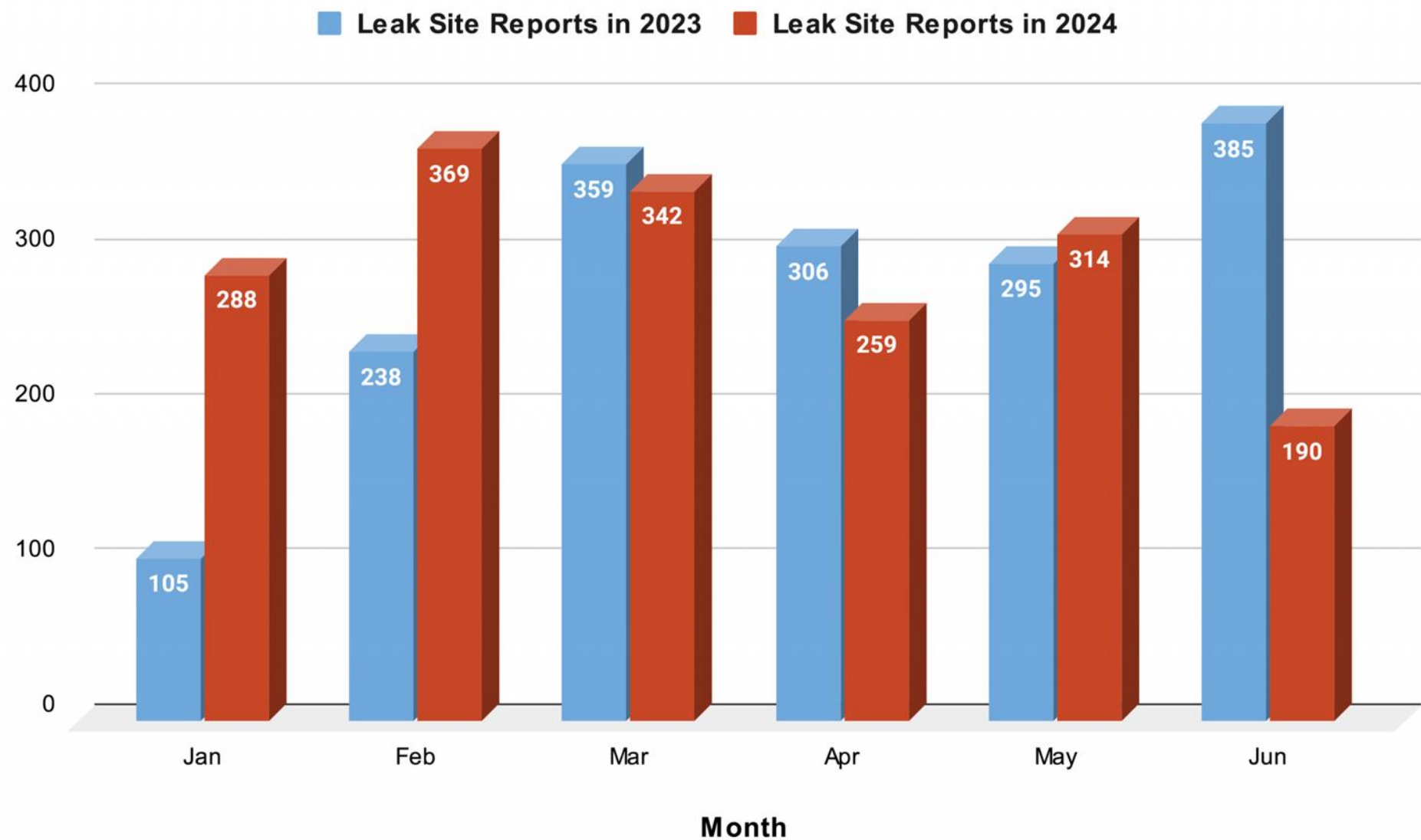


- จำนวนการโจมตีที่พุ่งสูงเป็นประวัติการณ์: ในไตรมาสที่ 3 ปี 2567 มีการบันทึกการโจมตีทางไซเบอร์เฉลี่ย 1,876 ครั้งต่อองค์กร ซึ่งเพิ่มขึ้น 75% เมื่อเทียบกับช่วงเวลาเดียวกันในปี 2566 และเพิ่มขึ้น 15% เมื่อเทียบกับไตรมาสก่อนหน้า
- การแยกย่อยตามอุตสาหกรรม: ภาคการศึกษา/การวิจัยเป็นเป้าหมายมากที่สุด โดยมีการโจมตีรายสัปดาห์จำนวน 3,828 ครั้ง รองลงมาคือภาครัฐบาล/ทหาร และภาคการดูแลสุขภาพ โดยมีการโจมตี 2,553 และ 2,434 ครั้ง ตามลำดับ
- ระดับภูมิภาค: แอฟริกาเผชิญกับการโจมตีเฉลี่ยสูงสุดที่ 3,370 ครั้งต่อสัปดาห์ (+90% เมื่อเทียบกับปีที่แล้ว) ในขณะที่ยุโรปและละตินอเมริกาก็พบว่าเพิ่มขึ้นอย่างมีนัยสำคัญเช่นกัน
- Ransomware: ภัยคุกคามที่คงอยู่: มีรายงานเหตุการณ์ ransomware มากกว่า 1,230 ครั้ง โดยอเมริกาเหนือได้รับผลกระทบมากที่สุด (57% ของเหตุการณ์) รองลงมาคือยุโรป (24%)

Industries Most Impacted by Ransomware



Year-over-Year Ransomware Activity Comparison





ข้อมูล LOCKBIT 2.0 และ 3.0 ที่โจมตีในประเทศไทย

LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. I attach the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger.

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxD:

ปีที่พบ	จำนวนหน่วยงาน	มูลค่าความเสียหาย
2022	14	619,000,000
2023	17	690,000,000
2024	5	1,002,000,000
รวม	36	2,311,000,000

LOCKBIT 3.0

LEAKED DATA

- TWITTER
- CONTACT US
- AFFILIATE RULES
- HOW TO BUY BITCOIN
- PRESS ABOUT US
- MIRRORS

7D 16h 59m 05s

\$ 100000

The Institute of [redacted] was established in 1977 as an academic institution of higher education dedicated to the study of Islam, with a particular

Updated: 12 Jul, 2022, 15:42 UTC 529

2D 09h 19m 00s

[redacted] is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part 2

Updated: 11 Jul, 2022, 15:00 UTC 926

PUBLISHED

[redacted] Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part 1)

Updated: 11 Jul, 2022, 14:03 UTC 1500

6D 16h 53m 02s

\$ 200000

[redacted] partitioning specialist VLP has specialised since 1982 in bespoke "flexible partitioning" for a wide variety of sectors, with products including:

Updated: 11 Jul, 2022, 13:34 UTC 764

PUBLISHED

[4.7 TB Files] [redacted] document and printing solutions tailored to address each client's unique needs

Updated: 12 Jul, 2022, 23:15 UTC 1376

PUBLISHED

[part 1] [redacted] is one of the Top 100 Fitness and Wellness Clubs in America.

Updated: 13 Jul, 2022, 15:15 UTC 1608

12D 19h 35m 39s

\$ 1000000

[redacted] Carnbrea is a privately-owned boutique W [redacted] group with a proud

Updated: 07 Jul, 2022, 01:17 UTC 2741

7D 02h 21m 28s

\$ 200000

[redacted] operates as a cabbage producer. The Company offers a variety of cabbage and organic products including spring m [redacted] red, green.

Updated: 11 Jul, 2022, 13:34 UTC 2280

1D 13h 08m 56s

\$ 100000

[redacted] was founded in 1957 in Milan thanks to the

2D 15h 34m 45s

\$ 40000

[redacted] [redacted] [redacted]

2D 15h 33m 03s

\$ 225000

[redacted] with more than 20 years of experience in



ความเสียหายที่เกิดจากจาก LOCKBIT 2.0 และ 3.0

รวม 2,311,000,000 บาท

#ประมาณการจาก ขนาดธุรกิจ กุณจตละเบียน จำนวนข้อมูลที่ถูกเผยแพร่ และข้อมูลงบการเงินของบริษัทที่

LockBit ransomware กลับมาอีกครั้ง

จากตู้คั่นเซิร์ฟเวอร์ หลังถูกจัดการไป

ได้ย้ายเว็บไซต์ที่มีข้อมูลที่ถูกรั้วไหลไปยังที่อยู่ .onion ใหม่ โดยเว็บไซต์ดังกล่าวมีรายชื่อผู้เสียหาย 5 ราย พร้อมนับถอยหลังสำหรับการเผยแพร่ข้อมูลที่ขโมยมา

24 ก.พ. 2024

ไม่ได้อัปเดต PHP ให้เป็นเวอร์ชันล่าสุด"
อาจถูกโจมตีโดยใช้ช่องโหว่

CVE-2023-3824

Notes
References
First Reference
Latest Reference
Curated
Recorded Future Community

1 Insikt Group Note
1 000+
Jul 21, 2023
May 26, 2024
★
Vulnerability



7 of 23 Risk Rules Triggered

Show recent events or cyber events

LOCKBIT 3.0 LEAKED DATA

5D 13h 56m 34s
1D 07h 52m 17s
5D 13h 48m 10s
5D 13h 46m 26s

Updated: 24 Feb, 2024, 21:35 UTC 1803
Updated: 24 Feb, 2024, 21:13 UTC 1025
Updated: 24 Feb, 2024, 21:27 UTC 1713
Updated: 24 Feb, 2024, 21:25 UTC 1507

1D 07h 44m 53s

fbi.gov
PUBLISHED

The Federal Bureau of Investigation is the domestic intelligence and security service of the United States and its principal federal law enforcement agency. An agency of the United

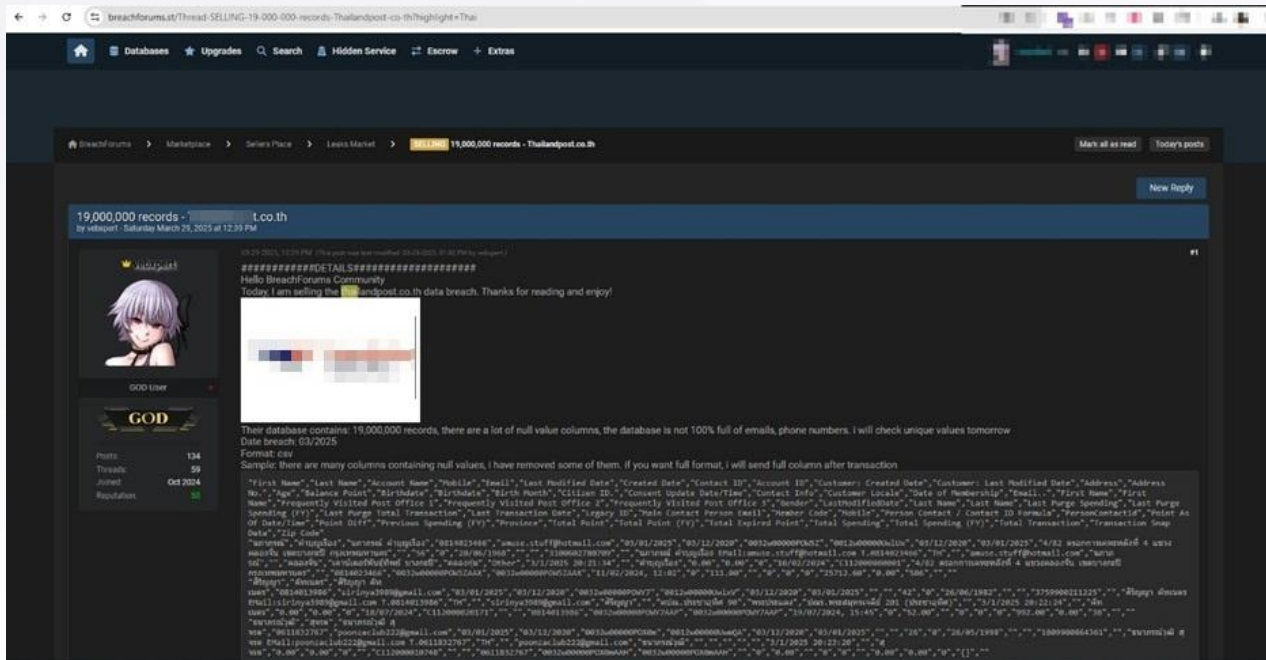
Updated: 24 Feb, 2024, 21:03 UTC 856
Updated: 24 Feb, 2024, 19:37 UTC 3461

ที่มา : i-secure



ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

DATA BREACH



First Name	Last Name	Account Name	Mobile	Email	Last Modified Date	Created Date	Contact ID	Account ID	Customer: Created Date
นภา	คำ	นภา	814	am	03/25	03/20	00	V5Z	03/20
ศิริ	ศิริ	ศิริ	814	siri	03/25	03/20	00	VY7	03/20
ธน	ธน	ธน	61	po	03/25	03/20	00	0m	03/20
ปณ	ปณ	ปณ	88	mo	15/23	03/20	00	TF	03/20
สร	สร	สร	65	kw	19/25	03/20	00	vm	03/20
นภา	นภา	นภา	61	taw	01/25	03/20	00	OM	03/20
กมล	กมล	กมล	86	djd	07/25	03/20	00	r4	03/20
ปณ	ปณ	ปณ	92	pa	07/25	03/20	00	Jj	03/20
นภา	นภา	นภา	90	bo	03/24	03/20	00	MA	03/20
นภา	นภา	นภา	85	e	04/25	03/20	00	Eg	03/20
กมล	กมล	กมล	61	che	03/25	03/20	00	wh	03/20
สกล	สกล	สกล	81	thw	20/25	03/20	00	9k	03/20
สกล	สกล	สกล	98	kar	07/25	03/20	00	co	03/20
สกล	สกล	สกล	80	nar	03/25	03/20	00	53	03/20
วรา	วรา	วรา	64	wai	03/25	03/20	00	Xj	03/20
สกล	สกล	สกล	92	buc	03/25	03/20	00	IQ	03/20
นภา	นภา	นภา	93	nij	22/25	03/20	00	is	03/20
ศิริ	ศิริ	ศิริ	97	pa	01/25	03/20	00	vh	03/20

Citizen ID	Consent Update Date/Time	Contact Info	Customer	Date of Men	Email..	First Name	First Name	Frequently Use
31	09	Email: amus	mail.com T.06TH		amus	am		storage > uploads PDF :

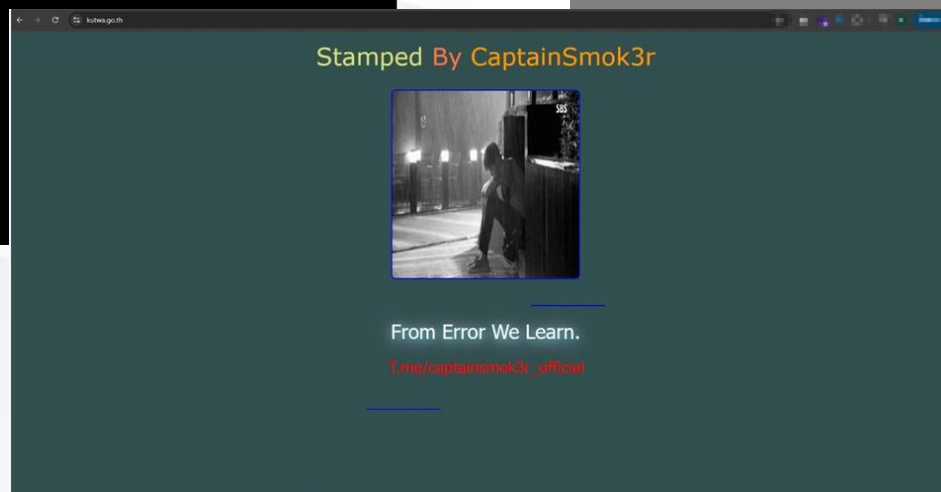
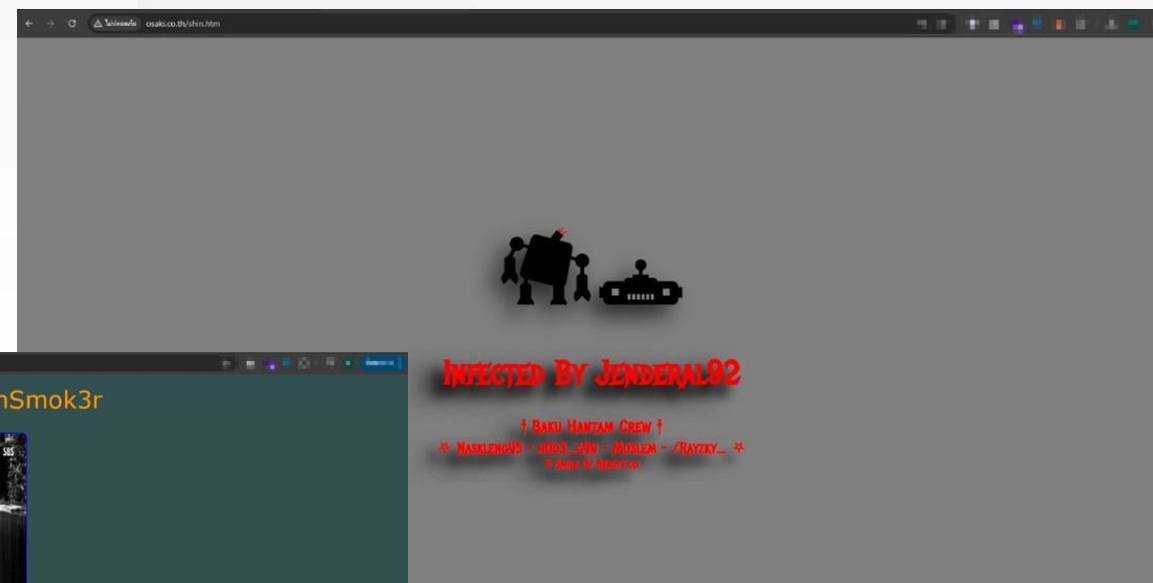
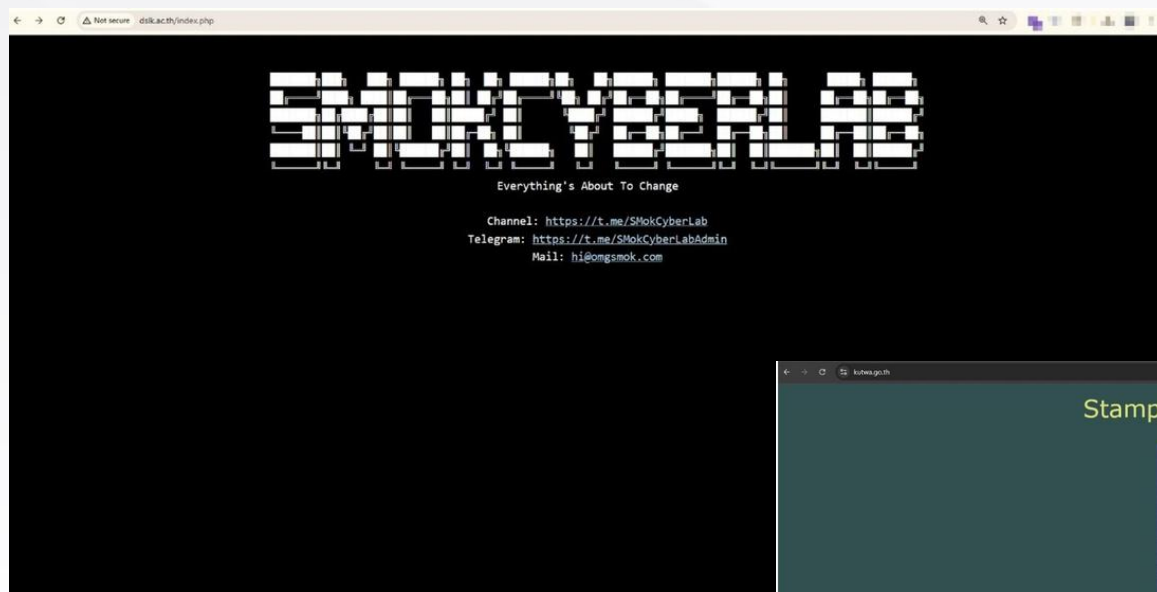
ลำดับ บ้านเลขที่ เลขบัตรประชาชน วันเกิด อายุ ห

ลำดับ, บ้านเลขที่, เลขบัตรประชาชน, วันเกิด, อายุ, หมายเลข, 1 นาย, 50/4, 36 44
20/03/2498 66, 2 นาง, 20/03/2498 66, 2 นาง, 20/03/2498 66

เทศบาลตำบล

https://www. go.th > storage > uploads PDF :

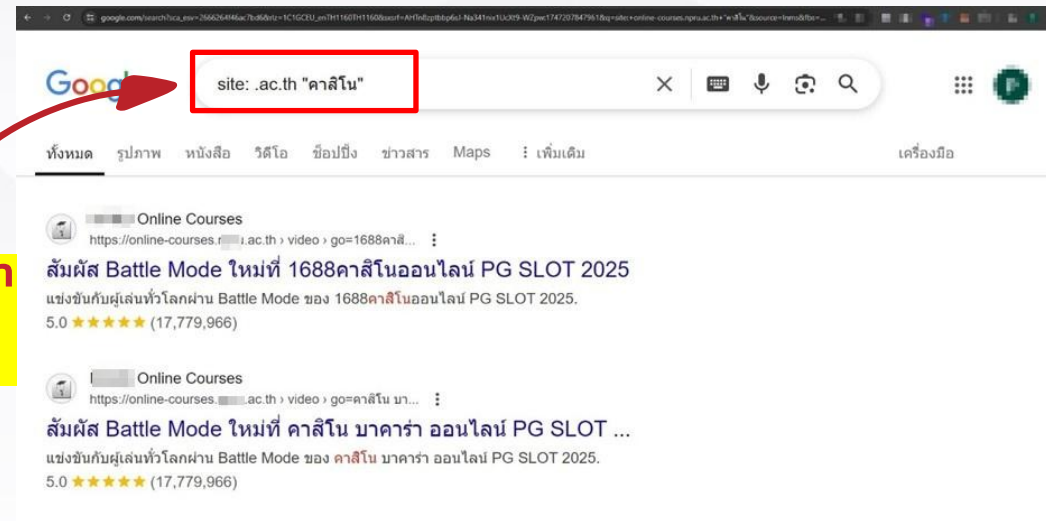
HACKED WEBSITE (DEFACEMENT)



ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (GAMBLING)

site: .go.th หรือ .ac.th
"คาสีโน" slot บาคาร่า
sbobet เป็นต้น



SECURITY MISCONFIGURATION

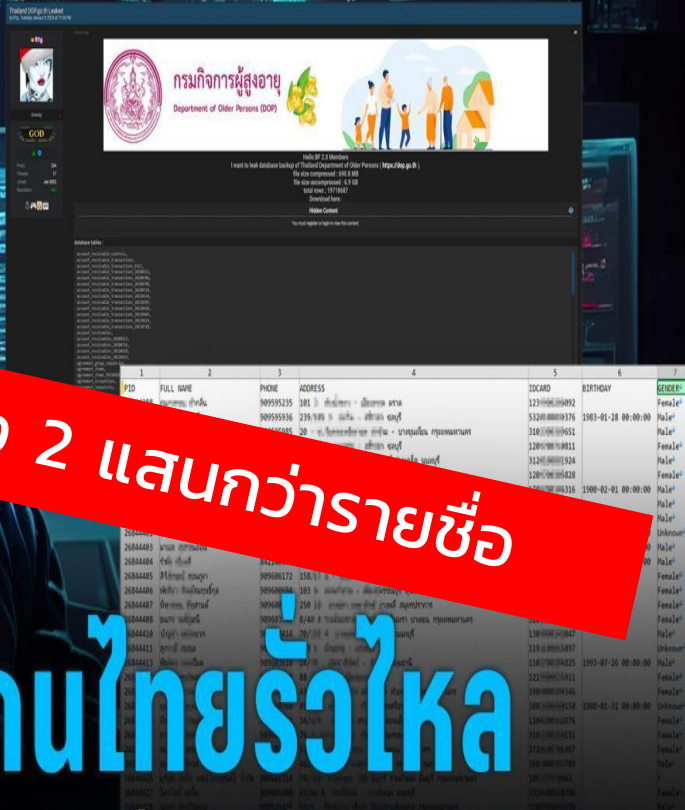
DIRECTORY LISTING

Index of /Web2024

Name	Last modified	Size	Description
 Parent Directory	-	-	-
 Executive_office/	2023-03-11 10:57	-	-
 Facebook Messenger C..>	2023-06-28 16:59	1.2K	-
 Facebook Messenger C..>	2022-07-18 10:29	1.1K	-
 Logo.png	2020-06-23 09:59	93K	-
 PM25.php	2024-03-12 09:17	10K	-
 UpRightSchool/	2022-06-14 13:50	-	-
 _groups/	2022-06-14 13:50	-	-
 about.html	2020-06-19 11:07	23K	-

Index of /wp-content/uploads

Name	Last modified	Size	Description
 Parent Directory	-	-	-
 2016/	2020-11-07 11:08	-	-
 2017/	2020-11-07 11:08	-	-
 2018/	2022-10-24 14:00	-	-
 2019/	2020-12-30 14:39	-	-
 2020/	2020-12-01 00:05	-	-
 2021/	2021-12-01 07:00	-	-
 2022/	2022-12-01 07:01	-	-
 2023/	2023-12-01 00:07	-	-
 2024/	2024-12-01 00:04	-	-



รู้แหละจริง 2 แสกว่ารายชื่อ

ข้อมูลคนไทยรั่วไหล ถูกประกาศขายกว่า 20 ล้านบัญชี!



MCOT NEWS FM100.5

ชี้อข้อมูลคนไทยหลุดจริง 2.3 แสนคน

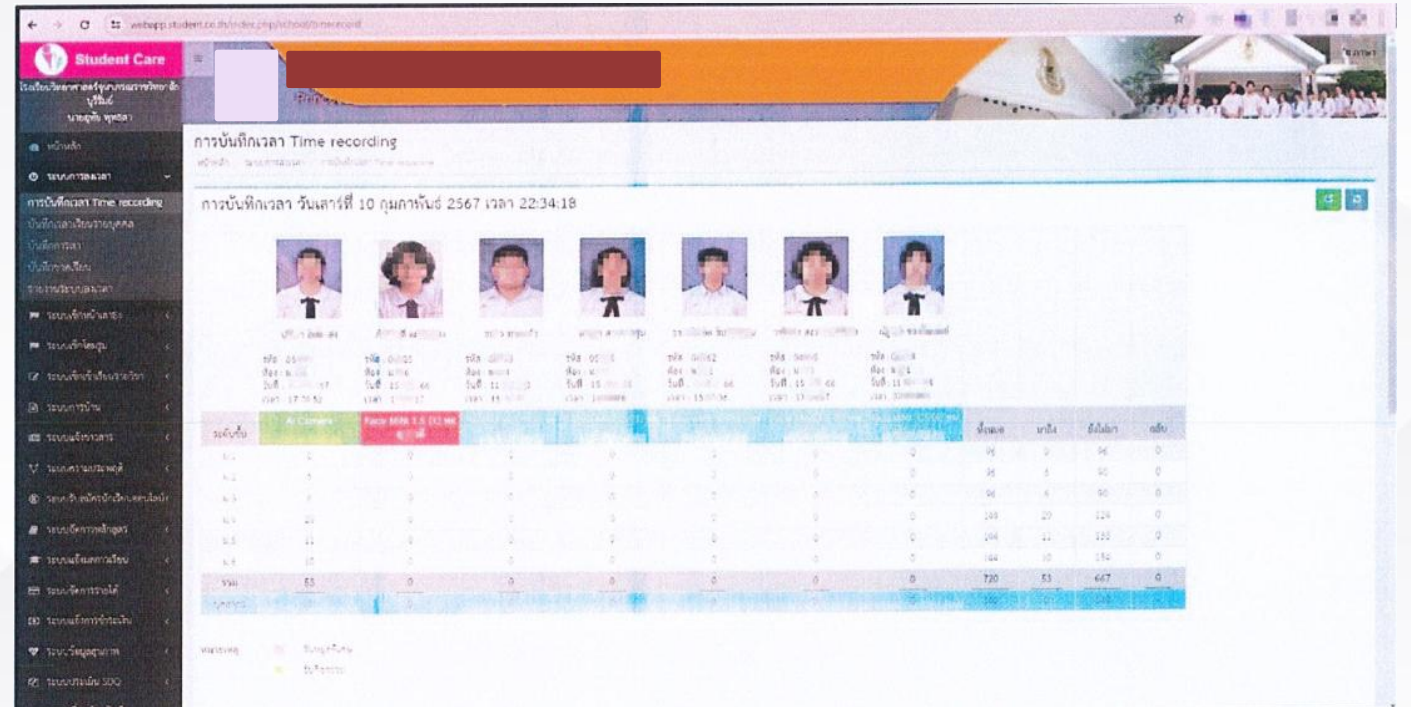
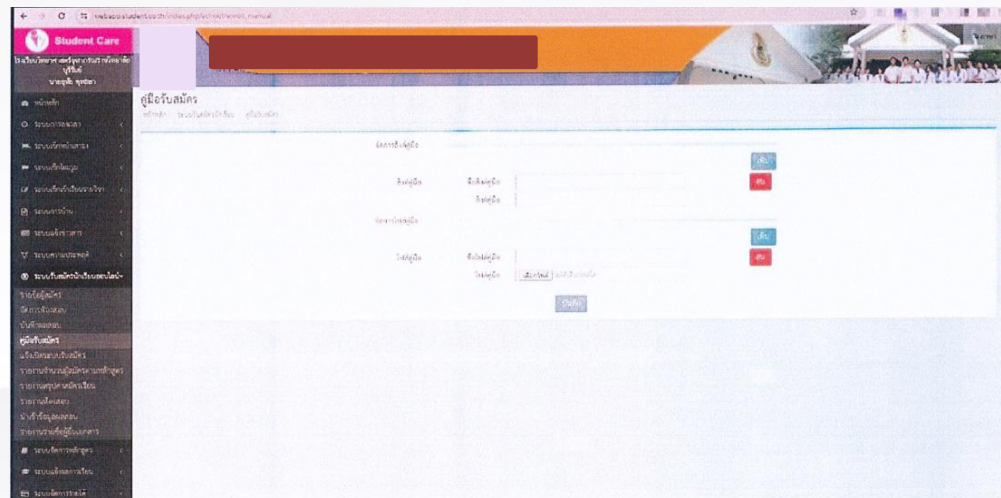
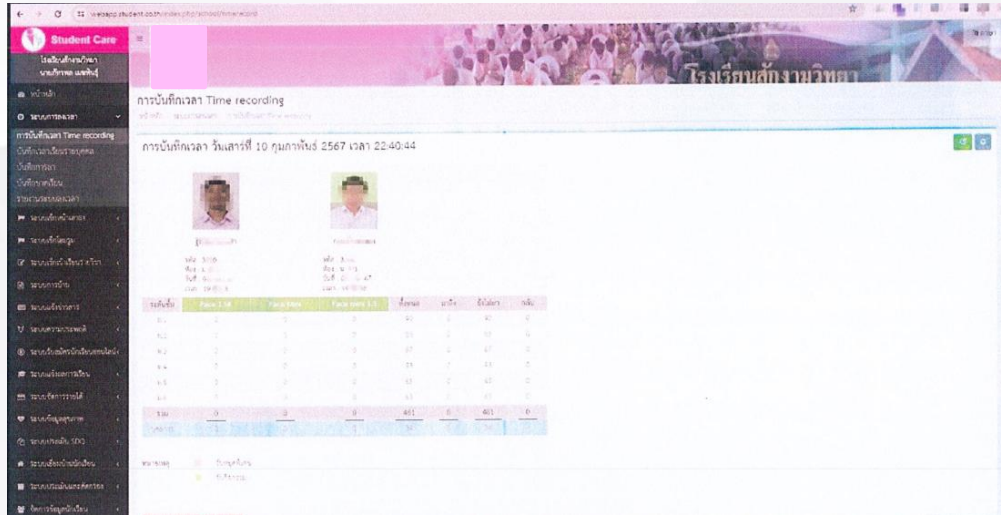
ประกาศขายข้อมูลหน่วยงานการศึกษาจากเว็บไซต์ **BreachForums**
เป็นข้อมูลของโรงเรียนแห่งหนึ่ง

[illegible][illegible]

1, 1, '9 มี.ค. 2565 / 11:42:03', 5, 6, 7, 8, 4, 'รับสมัครโดย นายณัฏฐ์ ชัยสิทธิ์', 1, '3.88', 0, 'นักเรียนนอกเขตจังหวัดเพชรบูรณ์', 2, '0015', '2022-03-09'),
 (16, 'นายณัฏฐ์ ชัยสิทธิ์', 1, '11/11/2539', '2007-02-28', 'พุทธ', 'ไทย', 'ไทย', '5' หมู่ 9 ซอย - ถนน - ค.ลาดหลุม อ.หล่มเก่า จ.เพชรบูรณ์ 67120', '-',
 '0641857539', '55', 9, '-', '-', 'ลาดหลุม', 'หล่มเก่า', 'เพชรบูรณ์', '67120', '-', '06/11/2539', '-', 'อ.หล่มเก่า', 'เกษตรกร', 5000, 'มีชีวิต', 'ส.ร.ค.
 ชัยสิทธิ์', 'เกษตรกร', 5000, 'มีชีวิต', 'อยู่ด้วยกัน', 'มารดา', 'ส.ร.ค. ชัยสิทธิ์', 'เกษตรกร', 5000, '06/11/2539', 'อ.หล่มเก่า', 'ค.ลาดหลุม อ.หล่มเก่า จ.เพชรบูรณ์',
 'stu/image/11/stu/27511', 69348740_3030, 19654357_n.jpg', 1, '-', 0, '-', 0,
 'stu/image/11/stu/27511', 3095861_77973, 5420202_n.jpg', 1,
 'stu/image/11/stu/27511', 8355074_14210, 105728_n.jpg', 1,
 'stu/image/11/stu/27511', 8732956_74159, 3448747_n.jpg', 1, 'stu/image/11/stu/275250', 238230138_156', 9286138_n.jpg',
 1, 1, '9 มี.ค. 2565 / 11:42:03', 5, 6, 7, 8, 4, 'รับสมัครโดย นายณัฏฐ์ ชัยสิทธิ์', 1, '3.88', 0, 'นักเรียนนอกเขตจังหวัดเพชรบูรณ์', 2, '0015', '2022-03-09'),
 (16, 'นายณัฏฐ์ ชัยสิทธิ์', 1, '11/11/2539', '2007-02-28', 'พุทธ', 'ไทย', 'ไทย', '5' หมู่ 9 ซอย - ถนน - ค.ลาดหลุม อ.หล่มเก่า จ.เพชรบูรณ์ 67120', '-',
 '0641857539', '55', 9, '-', '-', 'ลาดหลุม', 'หล่มเก่า', 'เพชรบูรณ์', '67120', '-', '06/11/2539', '-', 'อ.หล่มเก่า', 'เกษตรกร', 5000, 'มีชีวิต', 'ส.ร.ค.
 ชัยสิทธิ์', 'เกษตรกร', 5000, 'มีชีวิต', 'อยู่ด้วยกัน', 'มารดา', 'ส.ร.ค. ชัยสิทธิ์', 'เกษตรกร', 5000, '06/11/2539', 'อ.หล่มเก่า', 'ค.ลาดหลุม อ.หล่มเก่า จ.เพชรบูรณ์',
 'stu/image/11/stu/27511', 75131256_1001101133947_409, 9316628_n.jpg', 1,
 'stu/image/11/stu/275032', 0287056_7, 33509002_n.jpg', 1,
 'stu/image/11/stu/274796', 086070_20, 8610128_n.jpg', 1,
 'stu/image/11/stu/275065', 0987229_2, 57099681_n.jpg', 1,
 'stu/image/11/stu/275009', 911015_47, 4028181_n.jpg', 1,
 'stu/image/11/stu/275008', 8498105_2, 91890079_n.jpg', 1,
 'stu/image/11/stu/275347', 1056689_6, 99648105_n.jpg', 1, 1, '9 มี.ค. 2565 / 12:22:02', 5, 8, 6, 4, 7, 'รับสมัครโดย นายณัฏฐ์ ชัยสิทธิ์',
 1, '2.68', 0, 'นักเรียนที่ปรึกษาอยู่ในทะเบียนบ้านในจังหวัดเพชรบูรณ์', 2, '0016', '2022-03-09'),
 (17, 'นายณัฏฐ์ ชัยสิทธิ์', 1, '11/11/2539', '2006-10-12', 'พุทธ', 'ไทย', 'ไทย', '2' หมู่ 11 ซอย - ถนน - ค.น้ำก้อ อ.หล่มสัก จ.เพชรบูรณ์ 67110', '-',
 '06/11/2539', '21', 12, '-', '-', 'น้ำก้อ', 'หล่มสัก', 'เพชรบูรณ์', '67110', '-', '06/11/2539', '-', 'อ.หล่มสัก', 'เกษตรกร', 15000, 'มีชีวิต', 'ส.ร.ค.
 ชัยสิทธิ์', 'เกษตรกร', 15000, 'มีชีวิต', 'อยู่ด้วยกัน', 'บิดา', 'ชัยสิทธิ์', 'เกษตรกร', 15000, '06/11/2539', 'อ.หล่มสัก', 'ค.น้ำก้อ อ.หล่มสัก จ.เพชรบูรณ์',
 'stu/image/11/stu/image/inputsu/110870_3177', 2697_857', 7476954_n.jpg', 1, 'stu/image/11/stu/275278957_99009', 5681011487220083736_n.jpg', 1,
 'stu/image/11/stu/YY.jpg', 1, 'stu/image/inputsu/YY.jpg', 1, '-', 0, 'stu/image/11/stu/275278957_99009', 5681011487220083736_n.jpg', 1,
 1, '9 มี.ค. 2565 / 15:13:30', 8, 6, 7, 5, 4, 'รับสมัครโดย นางสาวณัฏฐ์ ชัยสิทธิ์', 1, '2.77', 28065, 'นักเรียนที่ปรึกษาอยู่ในทะเบียนบ้านในจังหวัดเพชรบูรณ์', 1,
 '0017', '2022-03-09'),
 (18, 'นางสาวณัฏฐ์ ชัยสิทธิ์', 1, '11/11/2539', '2006-05-28', 'พุทธ', 'ไทย', 'ไทย', '6' หมู่ 11 ซอย - ถนน - ค.เข็กน้อย อ.เขาค้อ จ.เพชรบูรณ์ 67280', '-',
 '06/11/2539', '61', 6, '-', '-', 'เข็กน้อย', 'เขาค้อ', 'เพชรบูรณ์', '67280', '-', '06/11/2539', '-', 'อ.เขาค้อ', 'เกษตรกร', 10000, 'มีชีวิต', 'ส.ร.ค.
 ชัยสิทธิ์', 'เกษตรกร', 10000, 'มีชีวิต', 'อยู่ด้วยกัน', 'บิดา', 'ชัยสิทธิ์', 'เกษตรกร', 10000, '06/11/2539', 'อ.เขาค้อ', 'ค.เข็กน้อย อ.เขาค้อ จ.เพชรบูรณ์',
 'stu/image/11/stu/274367', 0396854_348128917_n.jpg', 1, '-', 0, '-', 0,
 'stu/image/11/stu/274354', 075435022_1792, 003679_n.jpg', 1,
 'stu/image/11/stu/274479', 2298666115_820, 0307346_n.jpg', 1,
 'stu/image/11/stu/275112', 034269090_4101, 08070_n.jpg', 1, 'stu/image/inputsu/3535_3473240306', 901360011_n.jpg',
 1, 1, '9 มี.ค. 2565 / 15:15:19', 7, 5, 4, 6, 8, 'รับสมัครโดย นางสาวณัฏฐ์ ชัยสิทธิ์', 1, '3.38', 0, 'นักเรียนที่ปรึกษาอยู่ในทะเบียนบ้านในจังหวัดเพชรบูรณ์', 2,
 '0018', '2022-03-09'),

โรงเรียน ใช้ Username และ Password

ด้วยเบอร์ส่วนตัว ระบบจึงเกิดการโดน แฮก มีข้อมูลนักเรียน/ผู้ปกครอง รั่วไหล



เมื่อวันที่ 10 กุมภาพันธ์ ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์ พบการเข้าถึงชื่อผู้ใช้งานและรหัสผ่าน ของหน่วยงานการศึกษา โดย ทางหน่วยงานได้เลือกใช้ชื่อผู้ใช้งานและรหัสผ่านเป็นเบอร์โทรศัพท์ส่วนตัว ซึ่งเป็นความเสี่ยง ทำให้สามารถโดนเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ โดยไม่ได้รับอนุญาต

ข้อมูลหน่วยงานการศึกษา รวบรวม

The collage displays various web interfaces from Thai educational institutions. The central, largest screenshot is a dashboard titled 'สถานการณ (ผู้ปกครอง)' (School Status for Parents) dated 9 June 2567. It includes a sidebar with navigation links and a main area with several colored tiles: a blue tile for 'ดูประวัติ' (View History), a brown tile for 'ดูผลการเรียน' (View Academic Results), an orange tile for 'ดูข้อมูลนักเรียน' (View Student Information), a green tile for 'ดูข้อมูลครู' (View Teacher Information), a purple tile for 'ดูข้อมูลโรงเรียน' (View School Information), and a red tile for 'ดูข้อมูลบุคลากร' (View Staff Information). Below these tiles are sections for 'ข้อมูลนักเรียน' (Student Information), 'ข้อมูลครู' (Teacher Information), and 'ข้อมูลโรงเรียน' (School Information). Other screenshots in the collage show login pages, student information forms, and school profiles.

ประเทศไทยได้เผชิญกับหลายเหตุการณ์ที่เป็นภัยคุกคามทางไซเบอร์ ซึ่งส่งผลกระทบต่อความมั่นคงในด้านต่างๆ ต่อไปนี้เป็นตัวอย่างเหตุการณ์สำคัญที่เคยเกิดขึ้น:



1. การโจมตีระบบสาธารณสุข

การโจมตีโรงพยาบาลบางแห่งในประเทศไทย: มีกรณีที่โรงพยาบาลในประเทศไทยถูกโจมตีด้วยแรนซัมแวร์ (Ransomware) ทำให้ระบบข้อมูลผู้ป่วยถูกเข้ารหัสและไม่สามารถเข้าถึงได้ โดยผู้โจมตีเรียกค่าไถ่เพื่อคืนข้อมูล ทำให้การให้บริการทางการแพทย์หยุดชะงัก และสร้างความตื่นตระหนกให้กับผู้ป่วยและบุคลากรทางการแพทย์

2. การโจมตีระบบการเงิน

การโจมตีธนาคารไทย: ในปี 2016 มีกรณีการโจมตีระบบเอทีเอ็มในประเทศไทย โดยการใช้มัลแวร์ทำให้เครื่องเอทีเอ็มหลายร้อยเครื่องสามารถจ่ายเงินสดออกมาโดยไม่ต้องใช้บัตร ทำให้เกิดความเสียหายหลายล้านบาทและส่งผลกระทบต่อความเชื่อมั่นในระบบการเงิน

3. การแฮกข้อมูลส่วนบุคคล

การแฮกข้อมูลจากหน่วยงานรัฐ: มีกรณีที่ข้อมูลส่วนบุคคลของประชาชนถูกแฮกจากฐานข้อมูลของหน่วยงานรัฐ ทำให้ข้อมูลสำคัญ เช่น หมายเลขบัตรประชาชน ที่อยู่ และเบอร์โทรศัพท์ถูกเผยแพร่สู่สาธารณะ ซึ่งสามารถนำไปใช้ในการหลอกลวงหรือการโจมตีทางไซเบอร์ต่อบุคคลเป้าหมาย

ประเทศไทยได้เผชิญกับหลายเหตุการณ์ที่เป็นภัยคุกคามทางไซเบอร์ ซึ่งส่งผลกระทบต่อความมั่นคงในด้านต่างๆ ต่อไปนี้เป็นตัวอย่างเหตุการณ์สำคัญที่เคยเกิดขึ้น:



4. การแพร่ข่าวสารเท็จและการโจมตีทางการเมือง

การแพร่ข่าวสารเท็จ (Fake News): การแพร่ข่าวสารเท็จเกี่ยวกับการเมืองและเหตุการณ์สำคัญของประเทศผ่านสื่อสังคมออนไลน์ ทำให้เกิดความขัดแย้งและความวุ่นวายในสังคม ตัวอย่างเช่น ข้อมูลที่บิดเบือนเกี่ยวกับการเลือกตั้งหรือสถานการณ์ฉุกเฉินต่างๆ ที่ทำให้ประชาชนเข้าใจผิดและตื่นตระหนก

5. การโจมตีโครงสร้างพื้นฐานสำคัญ

การโจมตีระบบโทรคมนาคม: มีกรณีการโจมตีระบบโทรคมนาคมและอินเทอร์เน็ตในประเทศไทย ทำให้การสื่อสารหยุดชะงักเป็นบางช่วงเวลา ส่งผลกระทบต่อการทำงานขององค์กรธุรกิจและการดำเนินชีวิตของประชาชน

กรณีศึกษา

กรณีการโจมตีเว็บไซต์หน่วยงานรัฐ: มีกรณีที่เว็บไซต์ของหน่วยงานรัฐและองค์กรสำคัญถูกโจมตีด้วยวิธีการ DDoS (Distributed Denial of Service) ทำให้เว็บไซต์ไม่สามารถให้บริการได้ชั่วคราว ซึ่งส่งผลกระทบต่อการทำงานของบริการข้อมูลและการติดต่อกับประชาชน

ความเข้าใจที่ผิด ต่อ Cyber Security

1. เข้าใจผิดว่าเป็นเรื่องของฝ่ายไอทีเท่านั้น ไม่เกี่ยวข้องกับฝ่ายอื่น
2. เข้าใจผิดว่าภาครัฐจัดการให้ทั้งหมด
3. เข้าใจผิดว่าเป็นเรื่องของความปลอดภัยของระบบเครือข่าย (Network) อย่างเดียว โดยไม่เกี่ยวข้องกับแอปพลิเคชันของผู้ใช้งาน (User Application)
4. เข้าใจผิดว่ามีพาสเวิร์ดสำหรับการล็อกอินก็ปลอดภัยพอแล้ว
5. เข้าใจผิดว่าเป็นเรื่องของการถูกโจมตีจากแฮกเกอร์ภายนอกเท่านั้น
6. เข้าใจผิดว่าเป็นเรื่องไกลตัว ยังไม่ต้องรีบ
7. เข้าใจผิดว่าเป็นการทำโครงการครั้งเดียวแล้วเลิก ไม่ต้องหมั่นซ้อม ไม่พัฒนาต่อเนื่อง

จากการวิเคราะห์สาเหตุกรณีหน่วยงานรัฐและเอกชน ในประเทศไทยถูกโจมตีของ ThaiCERT ในปี 2567



ระบบของภาครัฐและเอกชนจำนวนมากทั้งที่จ้างพัฒนาและพัฒนาเองมีความไม่ปลอดภัยและการเขียนโปรแกรมที่ไม่ปลอดภัย



การใช้ซอฟต์แวร์ที่มีช่องโหว่หรือล้าสมัย



การที่ผู้ดูแลระบบใช้ USERNAME และ PASSWORD เดิมที่ติดมากับอุปกรณ์หรือซอฟต์แวร์



ขาดระบบป้องกันและเฝ้าระวังการถูกโจมตี



การป้องกันการรั่วไหลของข้อมูลจากพนักงานภายใน (Insider Threat)



การใช้งานการเข้ารหัสที่ไม่ปลอดภัยหรือไม่มีการเข้ารหัส



หน่วยงานขาดบุคลากรที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



การขาดบุคลากรด้านการคุ้มครองข้อมูลส่วนบุคคล (DPO)



การจัดการสิทธิของพนักงานที่ออกจากงาน (Offboarding)



ขาดมาตรการกำกับดูแลและการป้องกันการเข้าถึงระบบจากบุคคลภายนอก

คำแนะนำในการป้องกันองค์กรของ สกมช. ในปี 2568

01

อัปเดตซอฟต์แวร์และระบบ
อยู่เสมอและ หลีกเลี่ยงการ
ดาวน์โหลดและติดตั้ง
ซอฟต์แวร์ละเมิดลิขสิทธิ์
(Software Updates &
Patching)

02

สำรองข้อมูลอย่าง
ปลอดภัยและเป็น
ประจำ (Data
Backup and
Disaster
Recovery)

03

ยกระดับความ
ปลอดภัยด้วยการ
ยืนยันตัวตน 2
ขั้นตอน (2FA)

04

แต่งตั้งและเสริม
บทบาทของ DPO และ
CISO

05

จัดตั้ง SOC ตลอดจน
ตรวจสอบและวิเคราะห์
กิจกรรมในเครือข่าย
อย่างสม่ำเสมอ

06

จัดการความเสี่ยง
จากการใช้ AI
อย่างมีจริยธรรม
(AI Risk
Management)

07

ส่งเสริมการใช้
รหัสผ่านที่
ปลอดภัยและ
นโยบาย Zero-
Trust

08

มีการกำกับดูแล
คัดเลือกบริษัทที่มี
ประสบการณ์และ
มาตรฐานความปลอดภัย
และหลีกเลี่ยงการใช้
ข้อมูลจริงในขั้นตอนการ
พัฒนา

09

ป้องกัน Insider
Threat และ
จัดการ
Offboarding
อย่างปลอดภัย

10

ให้ความรู้แก่พนักงาน
และปรับปรุงความรู้
ด้านความปลอดภัย
ไซเบอร์

การใช้ 2FA เพิ่มขึ้นความปลอดภัย

2FA คืออะไร? ทำไมช่วยชีวิตออนไลน์คุณได้

2FA หรือ Two-Factor Authentication เป็นการ **ยืนยันตัวตน** แบบ **2 ชั้น** เพื่อป้องกันรหัสผ่านหลุด ไม่ให้สูญเสียบัญชีส่วนบุคคล และป้องกันการโดนสวมรอย

ทำงานยังไง? : หลังจากใส่รหัสผ่าน ระบบจะขอ “หลักฐานยืนยันตัวตนอีกชั้น” เช่น

-  **OTP ONE USE**
**** รหัสผ่านแบบใช้ครั้งเดียว (OTP จากแอป)
-  **แจ้งเตือนผ่านแอป** เช่น Google Authenticator, Microsoft Authenticator
-  **รหัส OTP ที่ส่งมาทาง SMS/Email**
-  **ลายนิ้วมือ / สแกนใบหน้า**

ตั้งไว้ปลอดภัย
กว่านะทุกคน

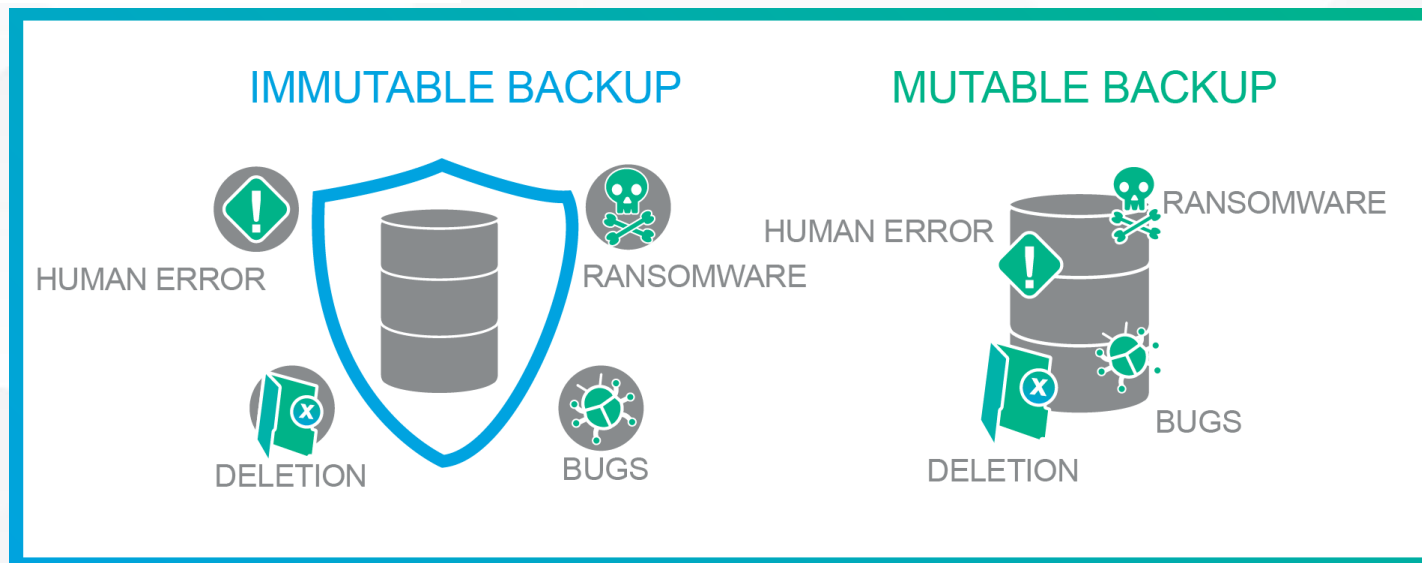
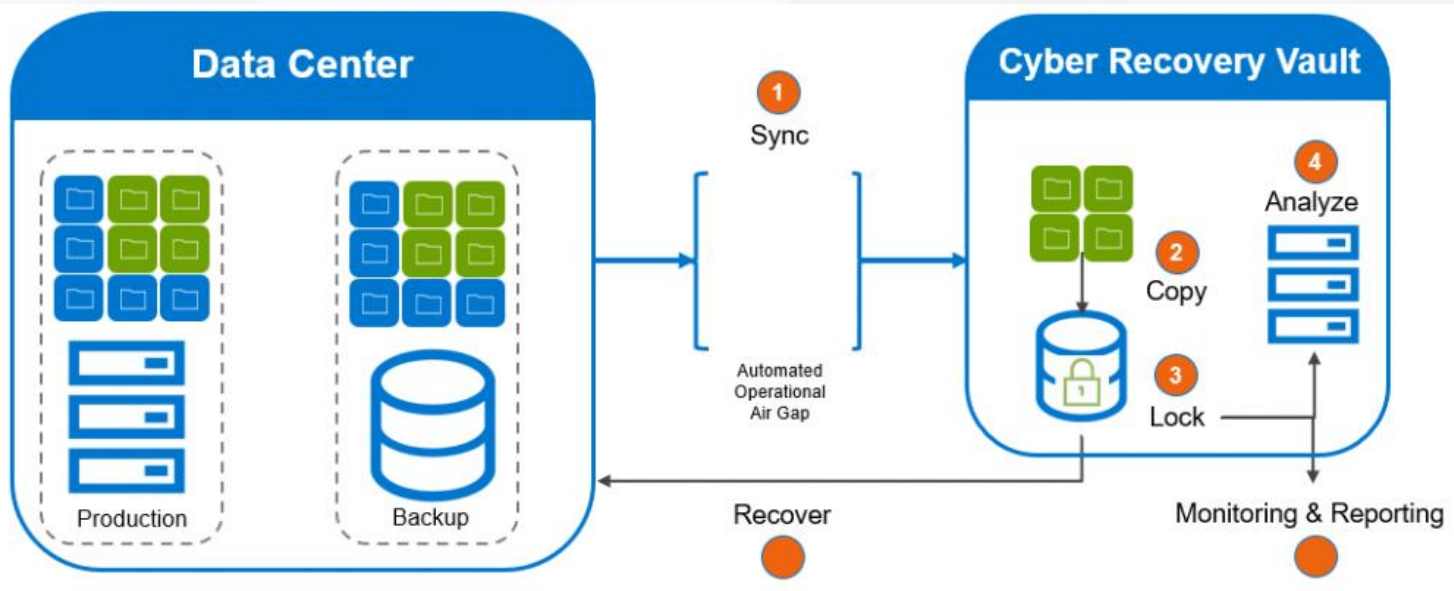
ปัจจัยที่นิยมใช้มี 3 ประเภท:

1. **สิ่งที่คุณรู้ (Something you know):** เช่น รหัสผ่าน, PIN
2. **สิ่งที่คุณมี (Something you have):** เช่น โทรศัพท์มือถือ, Token, แอปพลิเคชันสำหรับยืนยันตัวตน (เช่น Google Authenticator)
3. **สิ่งที่คุณเป็น (Something you are):** เช่น ลายนิ้วมือ, สแกนใบหน้า, ลายนิ้วมือ

ประโยชน์ของ 2FA: ป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาต แม้รหัสผ่านจะรั่วไหลลดความเสี่ยงจากการถูกโจมตีแบบ phishing หรือ brute-force



Air gap backup/immutable backup





พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ

พระวชิรเกล้าเจ้าอยู่หัว

โดยมีพระบรมราชโองการโปรดเกล้าฯ

พระราชบัญญัติ

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว

มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติฉบับนี้จึงตราขึ้นโดยมีพระบรมราชโองการโปรดเกล้าฯ

ให้ตราเป็นพระราชบัญญัติไว้ด้วย

มาตรา ๑ พระราชบัญญัตินี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา

มาตรา ๒ ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เป็นหน่วยงานกลางในการดำเนินการตามพระราชบัญญัตินี้

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้
เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน ระวัง และ
ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายใน
ประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับนโยบายที่บัญญัติไว้ในมาตรา ๖๖ ของรัฐธรรมนูญ
แห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัตินี้ขึ้นไว้โดยคำแนะนำและยินยอมของ
สภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

```
352 /* =Menu
353
354
355 #access {
356     display: inline-block;
357     height: 69px;
358     float: right;
359     margin: 11px 28px 0px 0px;
360     max-width: 800px;
361 }
362
363 #access ul {
364     font-size: 13px;
365     list-style: none;
366     margin: 0 0 0 -0.8125em;
367     padding-left: 0;
368     z-index: 99999;
369     text-align: right;
370 }
```

พ.ร.บ.การรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. 2562



พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว
มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล
ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๒๘ มาตรา ๓๒ มาตรา ๓๓ มาตรา ๓๔ มาตรา ๓๖ และ
มาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติ
แห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้
เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และ
ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายใน
ประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเจตนารมณ์ที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญ
แห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของ
สภานิติบัญญัติแห่งชาติทำหน้าทีรัฐสภา ดังต่อไปนี้

พระราชบัญญัติ

การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

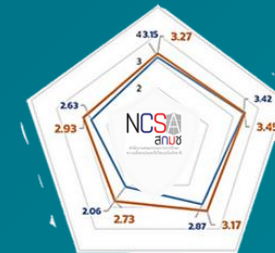
- ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562
- มีผลบังคับใช้ ตั้งแต่วันที่ 28 พฤษภาคม 2562 เป็นต้นไป



เฝ้าระวัง



รับมือ



ปราบปราม



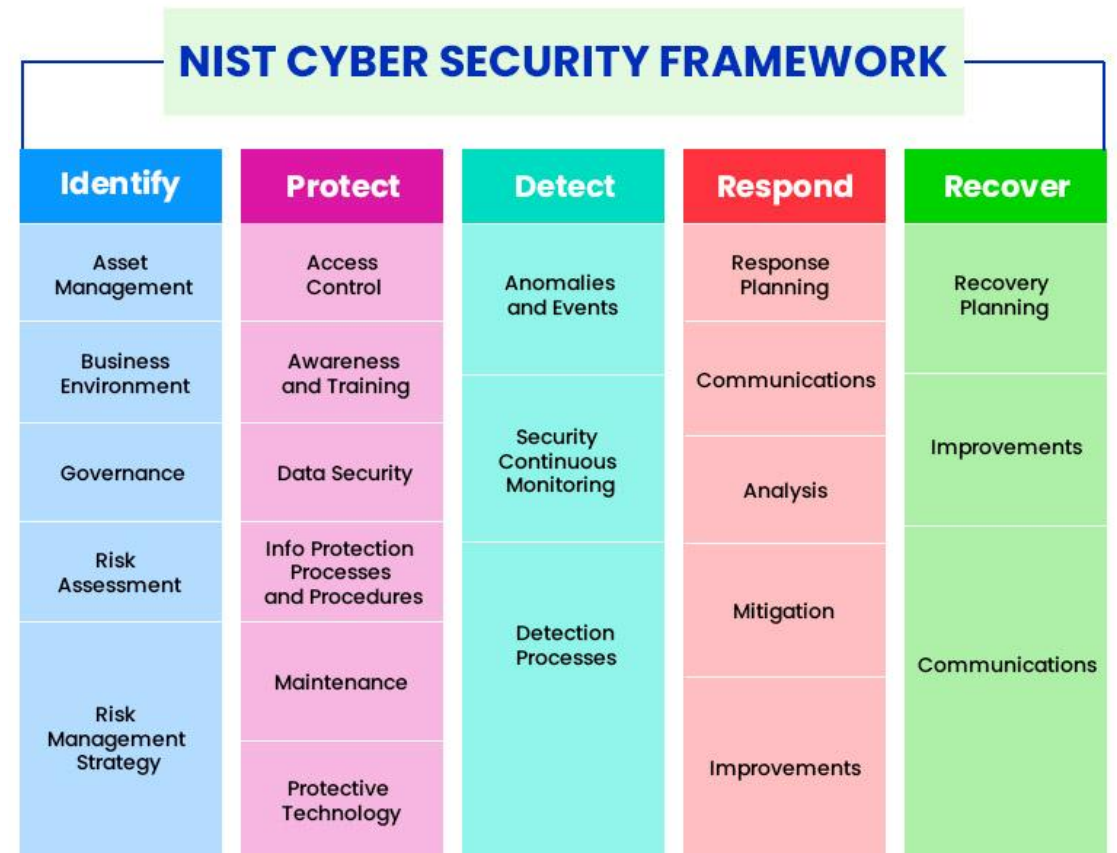
ระงับ

อ้างอิงจาก มาตรา 13 (6) ของพระราชบัญญัติการรักษาความมั่นคง
ปลอดภัยไซเบอร์ พ.ศ. 2562

มาตรา	หน่วยงาน CII	หน่วยงานของรัฐ*
43 ดำเนินการตามนโยบายและแผนฯ	/	/
44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ	/	/
45 มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	/	/
46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการไปยังสำนักงาน	/	/
52 แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์	/	
53 รับการตรวจสอบมาตรฐานขั้นต่ำจากหน่วยงานควบคุมหรือกำกับดูแล	/	
54 จัดให้มีการประเมินความเสี่ยงฯ รวมทั้งต้องจัดให้มีการตรวจสอบฯ	/	
56 มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์	/	
57 รายงานเหตุภัยคุกคามทางไซเบอร์ และปฏิบัติตามส่วนที่ 4	/	
58 ตรวจสอบ ประเมิน ป้องกัน รับมือ ลดความเสี่ยง และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว	/	/

*หมายถึง หน่วยงานของรัฐที่มีได้เป็นหน่วยงาน CII

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



เริ่มต้นยังไง?

Checklist สำหรับหน่วยงานในการรักษาความมั่นคงปลอดภัยไซเบอร์ ตาม พ.ร.บ.ไซเบอร์ 2562

หัวข้อในการกำหนด มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะ ความมั่นคงปลอดภัยไซเบอร์ ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
ประมวลแนวทางปฏิบัติ			
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		•	•
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	•	•	•
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	•	•	•
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑. การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)			
๑.๑ การจัดการทรัพย์สิน (Asset Management)	•	•	•
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	•	•	•
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			•
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)			•

๒. มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)			
๒.๑ การควบคุมการเข้าถึง (Access Control)	•	•	•
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	•	•	•
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)		•	•
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		•	•
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	•	•	•
๒.๖ การแบ่งปันข้อมูล (Information Sharing)			•
๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)			
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	•	•	•
๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)			
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	•	•	•
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	•	•	•
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	•	•	•
๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)			
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			•



ร่วมสร้างการตระหนักรู้ เสริมเกราะป้องกัน สร้างภูมิคุ้มกันภัยไซเบอร์ไปกับ สกมช.



หลอกล่อให้รัก หลอใจคน คนโสดโปรดระวัง!!
Romance Scam

รู้ทัน! ก่อนเป็นเหยื่อรัก

ตรวจสอบรายชื่อผู้ถูกหลอกล่อว่ามีชื่อคุณหรือไม่
ไม่เชื่อคนหรือเรื่องราวดูๆ ฟังๆ และอย่าโอนเงินให้ใครโดยเด็ดขาด
ไม่โพสข้อมูลส่วนตัวกับบุคคลอื่น ไม่ให้ข้อมูลส่วนตัวบนสื่อออนไลน์

รูปแบบของ Romance Scam

1. ปรากฏตัวในโซเชียลมีเดีย 2. ปรากฏตัวในแอปพลิเคชัน 3. ปรากฏตัวในอีเมล 4. ปรากฏตัวในโทรศัพท์ 5. ปรากฏตัวในสื่อออนไลน์

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



อย่าเป็นเหยื่อ
แอปเงินกู้

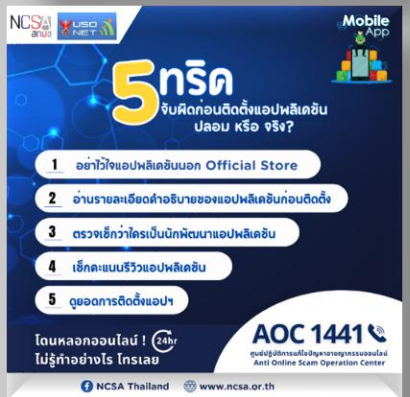
5 สัญญาณเตือนภัย

1. 1. ไม่มีการติดต่อจากทางธนาคาร
2. 2. ไม่มีการติดต่อจากทางธนาคาร
3. 3. ไม่มีการติดต่อจากทางธนาคาร
4. 4. ไม่มีการติดต่อจากทางธนาคาร
5. 5. ไม่มีการติดต่อจากทางธนาคาร

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



5 ทริค
จับผิดก่อนติดตั้งแอปพลิเคชันปลอม หรือ จิ้งจอก?

1. อย่าไว้วางใจแอปพลิเคชันนอก Official Store
2. อ่านรายละเอียดคำอธิบายของแอปพลิเคชันก่อนติดตั้ง
3. ตรวจสอบชื่อว่าเป็นนักพัฒนาแอปพลิเคชัน
4. เช็กคะแนนรีวิวแอปพลิเคชัน
5. ดูผลการติดตั้งแอป

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



มีสติ รู้เท่าทัน พร้อมป้องกัน
Ransomware

Mail ปลอม Link ปลอม Web ปลอม

7 วิธีป้องกัน

1. 1. ใช้ Backup File ตามกฎ 3-2-1 Backup Rule
2. 2. ไม่คลิก Link จาก Website ปลอมที่ไม่ใช่สื่อ
3. 3. ไม่เปิด File ที่แนบมาจากรายชื่อที่ไม่รู้จัก
4. 4. อัปเดตซอฟต์แวร์ให้เป็น Version ล่าสุด
5. 5. ติดตั้งโปรแกรมป้องกันไวรัส (Anti-malware)
6. 6. เปิดใช้ Multi-Factor Authentication (MFA)
7. 7. ไม่ใช้ Account ผู้ใช้บนระบบ Admin กับผู้ใช้งานทั่วไป

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



หลอกล่อซื้อขายสินค้าหรือบริการ

5 กลโกงซื้อขายออนไลน์

1. 1. หลอกล่อเงิน ไม่มีการส่งสินค้า
2. 2. สินค้าไม่ตรงปก
3. 3. ชื่อแบรนด์เนมแท้ แต่เป็นของปลอม
4. 4. มีการหลอกล่อเงิน
5. 5. ได้รับของชำรุดเสียหาย

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



เปลี่ยนรหัสผ่านใหม่

5 วิธีจัดการ
เมื่อข้อมูลส่วนบุคคลรั่วไหล

1. 1. เปลี่ยนรหัสผ่านใหม่
2. 2. ปิดบัญชีโซเชียลมีเดีย
3. 3. ตรวจสอบประวัติการใช้จ่าย
4. 4. ตรวจสอบประวัติการใช้จ่าย
5. 5. ตรวจสอบประวัติการใช้จ่าย

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



ตั้งรหัสผ่าน
อย่าจำได้ง่าย ไม่โดนแฮก

1. 1. รหัสผ่านมีความยาวอย่างน้อย 8 ตัวอักษร
2. 2. ประกอบด้วยตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก ตัวเลข และสัญลักษณ์
3. 3. หลีกเลี่ยงการใช้ชื่อ นามสกุล หรือข้อมูลส่วนตัว
4. 4. ไม่ควรใช้รหัสผ่านเดียวกันกับทุกบัญชีออนไลน์
5. 5. อย่าเผยแพร่ข้อมูลหรือรหัสผ่านของคุณด้วยวิธีใดๆ

โดนหลอกล่อออนไลน์! 24hr
ไม่รู้ทำอย่างไร โทรหา

AOC 1441
Anti Online Scam Operation Center

NCSA Thailand www.ncsa.or.th



Download Infographic
เพื่อเผยแพร่ประชาสัมพันธ์



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ขอเสนอ คลังความรู้ด้านไซเบอร์

แหล่งเรียนรู้ไซเบอร์สำหรับประชาชนทุกช่วงวัยที่คุณห้ามพลาด สำหรับการ Upskill และ Reskill เพื่อสร้างการตระหนักรู้และมีภูมิคุ้มกันภัยไซเบอร์ สามารถเข้าไปศึกษาได้ฟรี พร้อมรับใบ Certification ไม่เสียค่าใช้จ่าย

โดยมีชั่วโมงการเรียนรู้กว่า 1,000 ชั่วโมง



เรียนฟรี! ได้ใบ CERTIFICATE!

FREE

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CYBER KNOWLEDGE CENTER

NCSA
สทศ

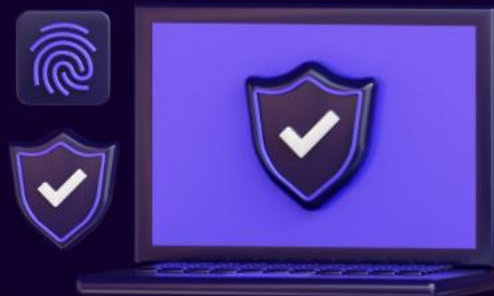
THNCA
Thailand National Cyber Academy
สำหรับการฝึกอบรมและวิจัยด้านความปลอดภัยทางไซเบอร์
by NCSA

SCAN ME

LINK : [HTTPS://LINKTR.EE/THNCA](https://linktr.ee/THNCA)



สแกนได้แล้ววันนี้
เรียนรู้ได้อย่างไร้ขีดจำกัด

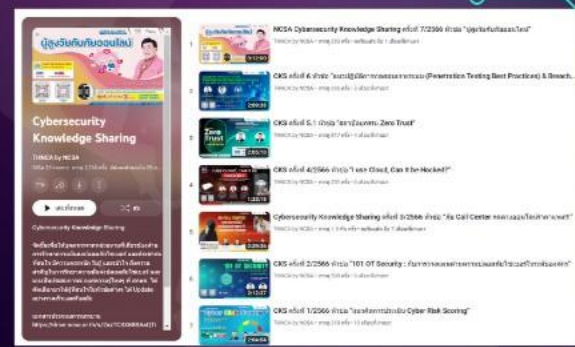


"คลังความรู้ด้านไซเบอร์"

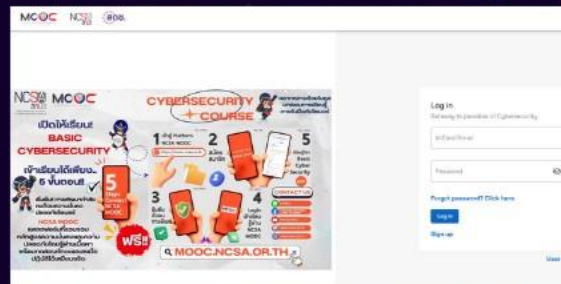
สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ส่งเสริมสังคมการเรียนรู้และเผยแพร่คลังความรู้ด้านไซเบอร์ เพื่อพัฒนาทักษะและการเรียนรู้ได้อย่างไร้ขีดจำกัด เข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์



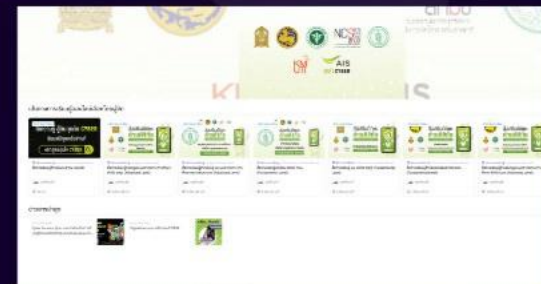
CYBERSECURITY AWARENESS



CYBERSECURITY KNOWLEDGE SHARING



NCSA MOOC CYBER-LEARNING



ούνไซเบอร์ AIS

✓ CYBERSECURITY AWARENESS

- ความสำคัญของ CYBERSECURITY
- รูปแบบภัยคุกคามทางไซเบอร์
- ประเภทของ CYBERSECURITY ที่ควรรู้จัก
- กฎหมายที่เกี่ยวข้องกับ CYBERSECURITY
- เกล็ดลับความปลอดภัยทางไซเบอร์และวิธีรับมือกับมัลแวร์รูปแบบต่างๆ
- นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)
- ประชาคมไซเบอร์

✓ CYBERSECURITY SKILL

- CYBERSECURITY SKILL
- NCSA CYBERSECURITY KNOWLEDGE SHARING ครั้งที่ 7/2566 หัวข้อ "ผู้ช่วยภัยกับภัยออนไลน์"
- CKS ครั้งที่ 6 หัวข้อ "แนวปฏิบัติการทดสอบเจาะระบบ (PENETRATION TESTING BEST PRACTICES) & BREACH
- CKS ครั้งที่ 5.1 หัวข้อ "สถาปัตยกรรม ZERO TRUST"

✓ NCSA MOOC CYBER-LEARNING

- BASIC CYBERSECURITY

✓ อุ่นใจไซเบอร์ AIS มีคอร์สทั้งหมดมากถึง 25 คอร์ส!

- รูปแบบภัยคุกคามทางไซเบอร์ ประเภทของ CYBERSECURITY ที่ควรรู้จัก กฎหมายที่เกี่ยวข้องกับ
- CYBERSECURITY เกล็ดลับความปลอดภัยทางไซเบอร์และวิธีรับมือกับมัลแวร์รูปแบบต่างๆ
- นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ประชาคมไซเบอร์และความรู้อื่นๆอีกมากมาย

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2502-7831 | อีเมล : academic@ncsa.or.th

รับฟังข่าวสารภัยคุกคามทางไซเบอร์
ได้ก่อนใครผ่านทางไลน์โอเพ่นแชท

SCAN NOW



เข้ารหัสเลย 4loTus



Q&A

Contact us

National Cyber Security Agency - NCSA



NCSA Thailand



Line ID : NCSA Thailand



E-Mail: saraban@ncsa.or.th



02-142-6885



shorturl.at/hkAC2

