NCSA สกมช

#MISSCONF8

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) ของประเทศไทยควรอยู่ตรงไหน

April 27, 2024, at Faculty of Public Health, Mahidol University

AVM Jadet Khuhakongkit

Assistant Secretary General, NCSA

ประสบการณ์ด้านไซเบอร์ที่เกี่ยวข้อง

ยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.2558 • หลักนิยมการปฏิบัติการร่วมทางไซเบอร์กองทัพไทย พ.ศ.2561 • นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ กองบัญชาการกองทัพไทย พ.ศ.2564 • การฝึกทางไซเบอร์ กองบัญชาการกองทัพไทย พ.ศ.2560, 2562 • การฝึกร่วมทางไซเบอร์ กองทัพไทย พ.ศ.2562-2563 • การแข่งขันทักษะทางไซเบอร์ในระดับ รร.ทหาร-ตำรวจ พ.ศ.2562-2563 • การแข่งขันทักษะทางไซเบอร์ กองทัพไทย พ.ศ.2562-2563 • ที่ปรึกษาในการจัดตั้ง สกมช. • ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศฯ พ.ศ.2564 • ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ พ.ศ.2564 • การฝึก Thailand's National Cyber Exercise 2022, 2023

การศึกษา

โรงเรียนเตรียมทหาร • โรงเรียนนายเรืออากาศ • สถาบันบัณฑิตพัฒนบริหารศาสตร์ • Squadron Officer School (USA) • Air Force Command and Staff Course (China) • Harvard Kennedy School (USA)

พลอากาศตรี จเด็ด คูหะก้องกิจ

ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CERTIFICATES

CISSP. CC. CQI IRCA LEADING QUALITY SINCE 1919 C|EH CERTIFIED ETHICAL HACKER CompTIA CASP+ CompTIA CySA+ CompTIA Cloud+ CompTIA PenTest+ CompTIA Security+

วัตถุประสงค์

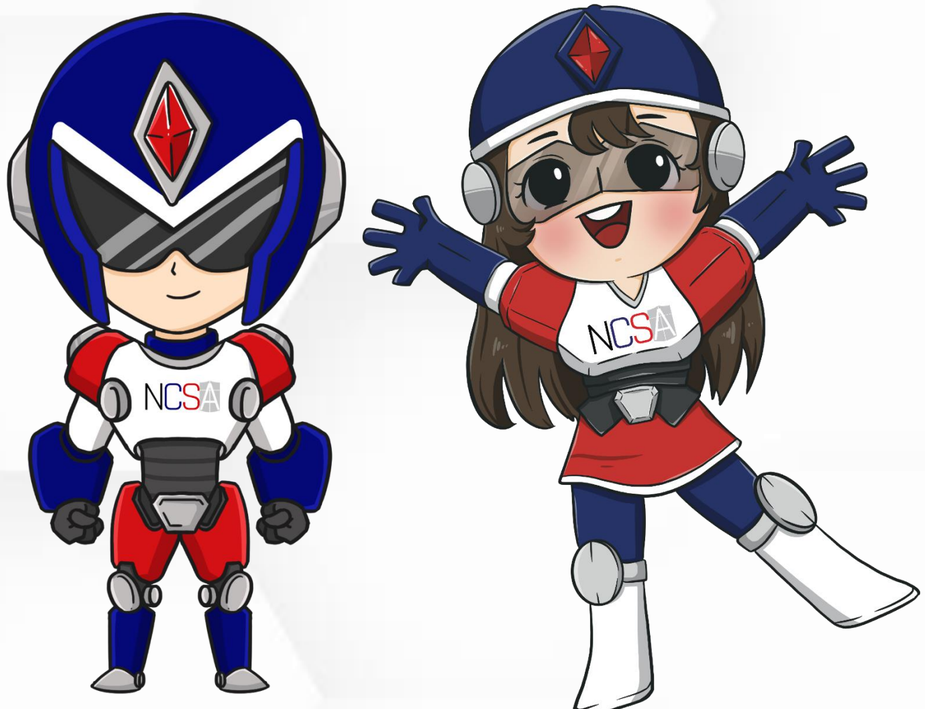
เพื่อให้ผู้เข้าร่วมกิจกรรมฯ **ได้มีโอกาสรับฟัง พูดคุย และ**

แลกเปลี่ยนมุมมองเกี่ยวกับ**ระดับความเสี่ยงที่ยอมรับได้จาก**

ภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทย

หัวข้อบรรยาย

- เกี่ยวกับ สกมช.
- นิยาม
- สภาวะแวดล้อมด้านไซเบอร์ของประเทศไทยในปัจจุบัน + ผลกระทบ
- พูดคุยเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้จากภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทย



เกี่ยวกับ สกมช.

วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

พันธกิจ MISSIONS

เสนอแนะนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดแนวทาง มาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

SECURE & TRUSTED ENVIRONMENT

❖ **PERSONAL DATA PROTECTTION**
กฎหมายคุ้มครองข้อมูลส่วนบุคคล
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- คุ้มครองข้อมูลส่วนบุคคล
- สิทธิเจ้าของข้อมูล
- ไกล่เกลี่ย ระงับข้อพิพาท

❖ **COMPUTER CRIME**
กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
สำนักงานตำรวจแห่งชาติ

- กำหนดความผิดและบทลงโทษ
- ความผิดที่ทำต่อข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยตรง

❖ **CYBERSECURITY**
กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

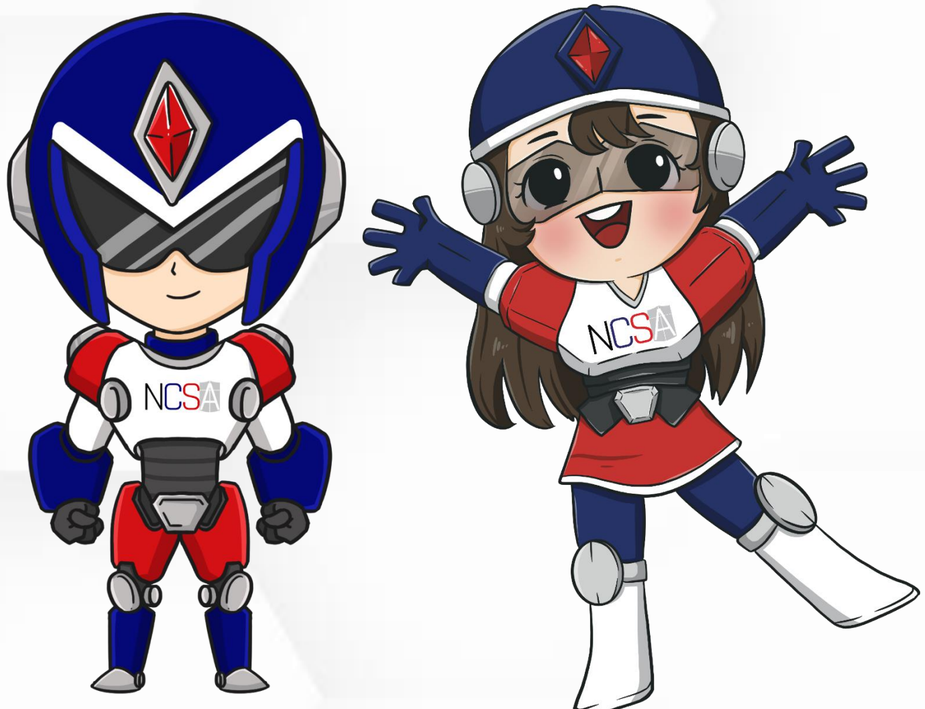
- Cyber Threats
- Protection & Incident Response
- Government & Critical Information Infrastructure

หมายเหตุ : ระดับวิกฤต เป็นอำนาจหน้าที่ สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)


“There are only two types of companies:
those that have been hacked,
and those that will be.”
Robert Mueller
FBI Director, 2001-2013

หัวข้อบรรยาย

- เกี่ยวกับ สกมช.
- นิยาม
- สภาวะแวดล้อมด้านไซเบอร์ของประเทศไทยในปัจจุบัน + ผลกระทบ
- พูดคุยเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้จากภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทย



นิยาม

NIST

Risk

Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation.

Sources:

NIST SP 800-30 Rev. 1 under Information System-Related Security Risk

Risk Appetite

The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.

Sources:

NISTIR 8170

Risk Tolerance

The organization or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.

Sources:

NIST SP 800-160v1r1 from ISO Guide 73

Ref: https://csrc.nist.gov/glossary

EY

Cyber risk

Cyber risk is the risk of financial loss, disruption of activities, impact on the company's image or reputation as a result of malicious and purposefully executed actions in the cyber space. Cyber risks may have an impact on the confidentiality, integrity and availability of information systems and their related data.

Risk appetite

Risk appetite is the risk you are willing to take, in other words, it is the aggregated level of risk an organization is willing to assume (within its risk capacity) to achieve its strategic objectives and business plans. It is a "range" as opposed to a target.

Risk tolerance

Risk tolerance is the maximum risk the organization is willing to take for a particular strategic objective, KPI or category of risk. Exceeding a risk tolerance will typically act as a trigger for corrective action at the executive level, immediate notification to the board, and a detailed review of the underlying causes of the high risk exposure or significant variation from expected performance.

Ref: https://www.ey.com/en_ch/cybersecurity/if-cyber-risk-is-an-unavoidable-truth-whats-your-true-cyber-risk-appetite

นิยาม (ต่อ)

NIST

Cyber Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Sources:

CNSSI 4009-2015 under threat from NIST SP 800-30 Rev. 1
NIST SP 800-128 under Threat from CNSSI 4009
NIST SP 800-137 under Threat from CNSSI 4009 - Adapted
NIST SP 800-39 under Threat from CNSSI 4009

Threat Actor

An individual or a group posing a threat.

Sources:

NIST SP 800-150 under Threat Actor

Ref: https://csrc.nist.gov/glossary

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

Risk appetite statements

Examples

Financial Services Company: "We are willing to accept a moderate level of risk in pursuit of our financial goals, with a maximum exposure of 5% of our total assets in high-risk investments."

Technology Startup: "Our risk appetite is aggressive, as we aim to innovate and grow rapidly. However, we will not take on risks that jeopardize our long-term sustainability or compromise the security of our customers' data."

Manufacturing Company: "We have a low risk appetite, focusing on operational efficiency and safety. We will not accept risks that could lead to significant downtime, harm to employees, or damage to our reputation."

Healthcare Provider: "Our risk appetite is conservative, prioritizing patient safety and regulatory compliance above all else. We will not take on risks that could compromise patient care or expose us to legal or ethical issues."

Retail Chain: "Our risk appetite is moderate, balancing growth opportunities with risk management. We will not take on risks that could lead to significant supply chain disruptions, financial losses, or damage to our brand."

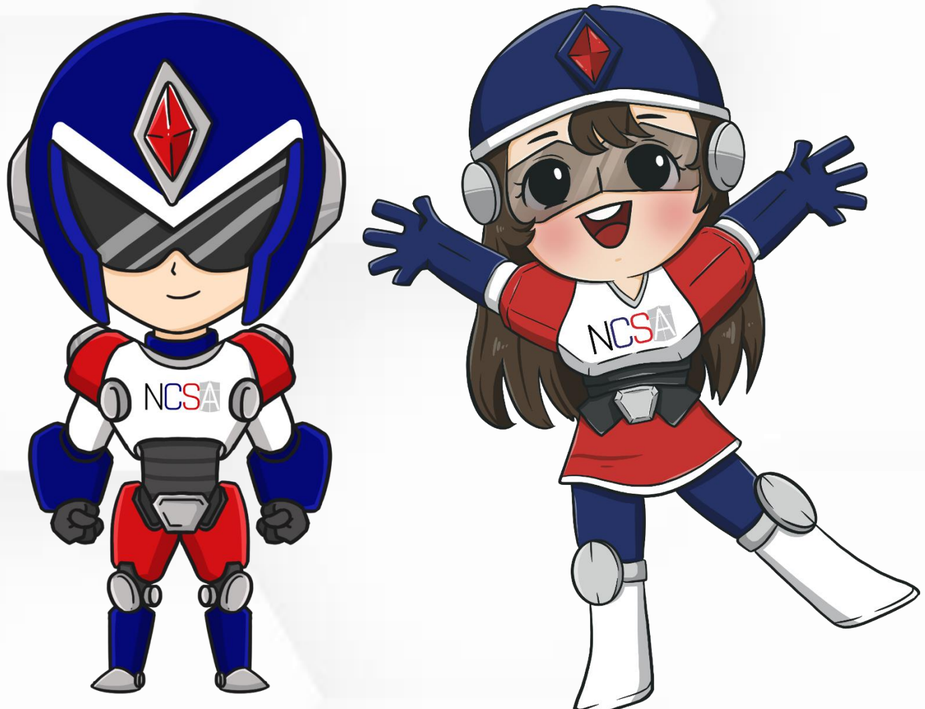
RESERVE BANK OF AUSTRALIA

Category	Sub Category	Category Description	Risk appetite	Sub Category Owner
Policy	Monetary and Banking Policy	Contribute to the stability of the currency, full employment, and the economic prosperity and welfare of the Australian people	Limited to Balanced	Governor (Note: management of these risks sits with the Reserve Bank Board)
	Payments Policy	Controlling risks in the financial system, promoting efficiency in the payments system and promoting competition in payment services	Limited to Balanced	Governor (Note: management of these risks sits with the Payments System Board)
Strategic	Strategy Selection	Development of suitable and viable strategies	High	Governor
	Strategy Implementation	Investment decisions support strategic goals	Balanced	Deputy Governor
		Implementation of strategic business goals through change programs or day to day work	Limited	Deputy Governor
	Analysis	Exploration and expansion of analysis and decisions to effectively support decision making	High	Governor
	Innovation	Considered and deliberate innovation and experiments to achieve our mission	High	Executives accountable within their functional area

Ref: https://www.rba.gov.au/about-rba/our-policies/risk-management-policy.html

หัวข้อบรรยาย

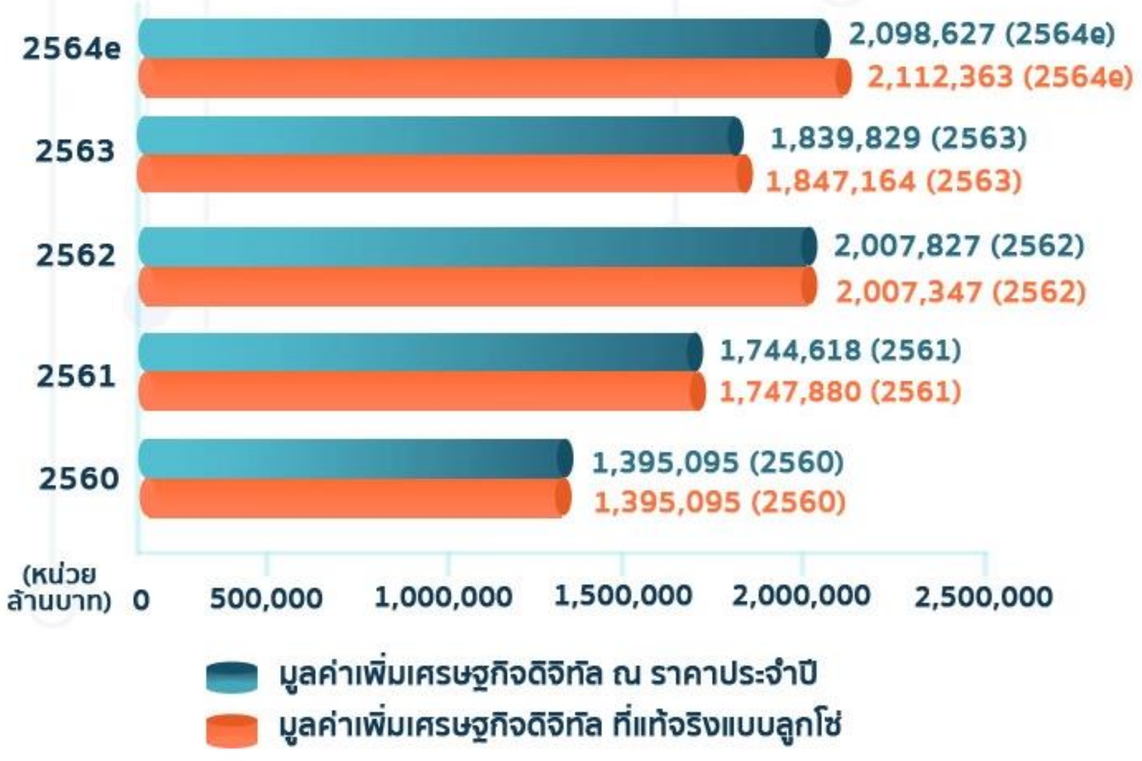
- เกี่ยวกับ สกมช.
- นิยาม
- สภาวะแวดล้อมด้านไซเบอร์ของประเทศไทยในปัจจุบัน + ผลกระทบ
- พูดคุยเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้จากภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทย



สดช.

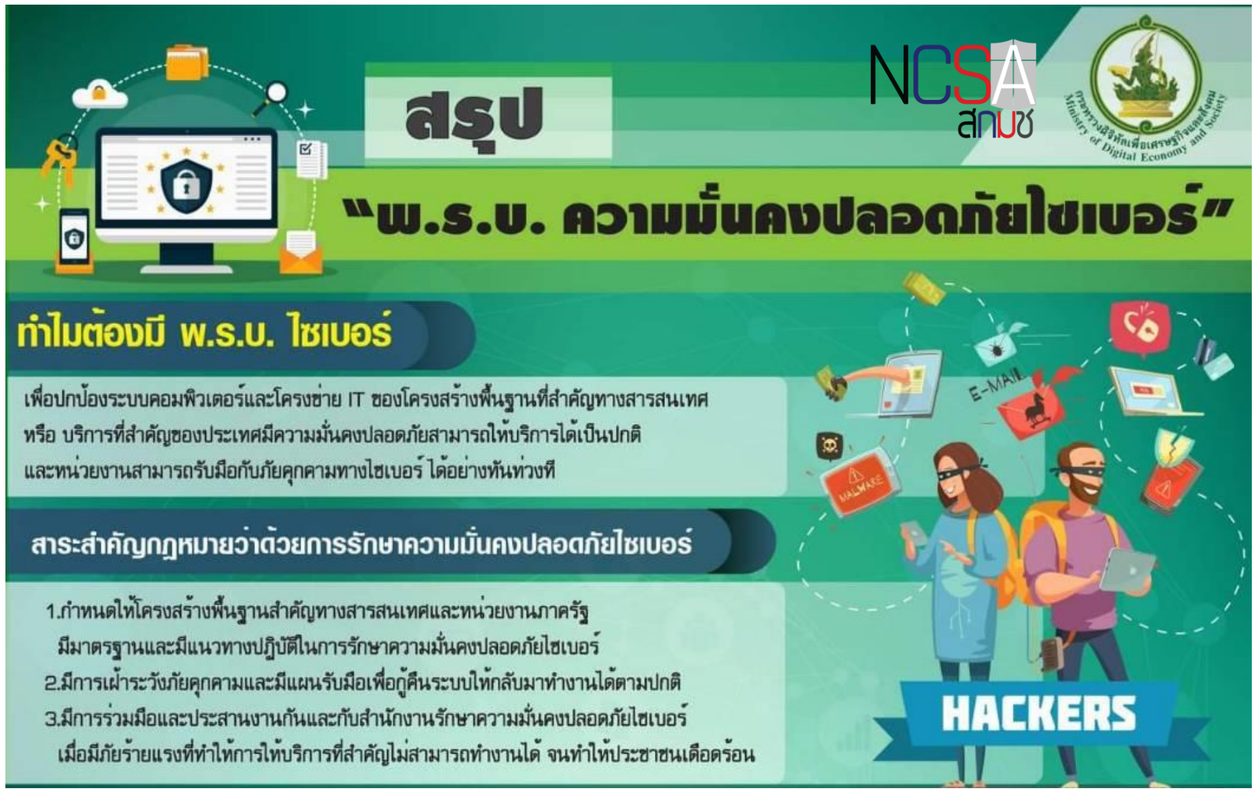
เศรษฐกิจดิจิทัล ปี 2560 - 2564e

มูลค่ารวม



ที่มา : https://www.onde.go.th/assets/portals/1/files/1-1.jpg

พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562



พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

NCSA สกมช

RMUTT
www.mutt.ac.th ราชมงคลธัญบุรี

PDPA คืออะไร ?

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ ย่อมาจาก Personal Data Protection Act
บทบัญญัติที่ให้ความคุ้มครองข้อมูลส่วนบุคคลของ “บุคคลธรรมดา”
ให้สิทธิ์ในการแก้ไข, เข้าถึง หรือ แจ้งลบข้อมูลที่ให้ไว้กับองค์กรเป็นต้น
และกำหนดบทบาทหน้าที่และบทลงโทษหากองค์กรไม่ปฏิบัติตาม

ข้อมูลแบบไหนเป็น “ข้อมูลส่วนบุคคล”

ข้อมูลส่วนบุคคลคือ ข้อมูลเกี่ยวกับบุคคล ที่ทำให้ระบุตัวบุคคลได้ ทั้งทางตรงและทางอ้อม

- เลขบัตรประจำตัวประชาชน
- ชื่อ - นามสกุล
- ที่อยู่
- เบอร์โทรศัพท์
- อีเมล
- ข้อมูลทางการเงิน
- เชื้อชาติ
- ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ

www.rmutt.ac.th มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

มหาวิทยาลัยมหิดล คณะวิทยาศาสตร์ | งานสารสนเทศและห้องสมุดสตางค์ มงคลสุข

สรุปสาระสำคัญ พระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อมูลส่วนบุคคล
ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

การคุ้มครองข้อมูลส่วนบุคคล
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูล

การเก็บข้อมูลส่วนบุคคล
การเก็บรวบรวมข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น และต้องกำหนดระยะเวลาการจัดเก็บภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย

การเปิดเผยข้อมูลส่วนบุคคล
ห้ามมิให้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูล
เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล ที่เกี่ยวกับตน หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

สิทธิการลบข้อมูลส่วนบุคคล
เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ดำเนินการลบ หรือ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

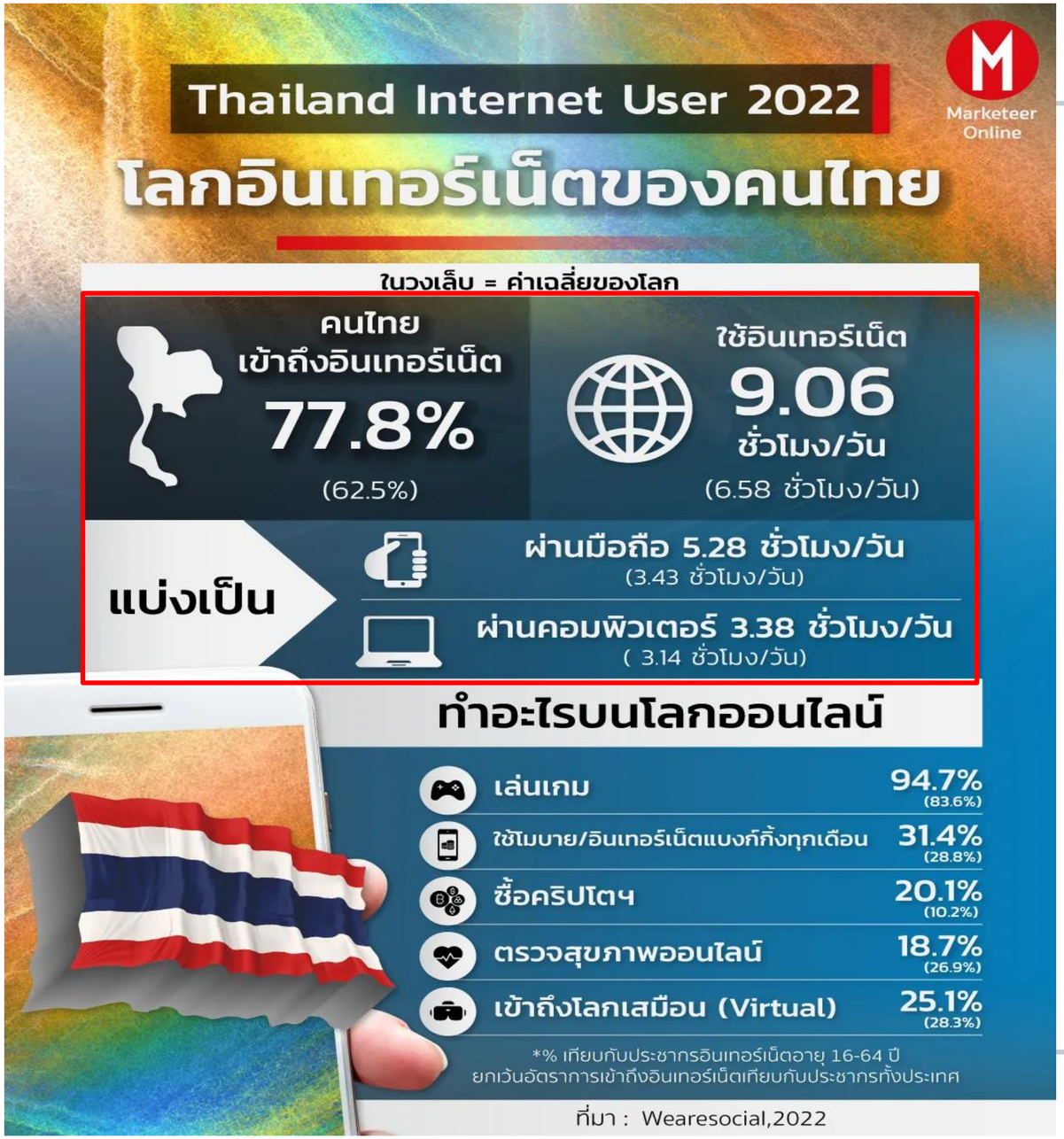
การร้องเรียน
เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
เล่ม 136 ตอนที่ 69 ก วันที่ 27 พฤษภาคม 2562

https://stang.sc.mahidol.ac.th StangMongkolsukLibrary @StangLibrary @StangLibrary

พ.ร.บ.การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ.2565

#โลกอินเทอร์เน็ตของคนไทย



วิทยากร
พลอากาศตรี จเด็ด คูหะก้องกิจ ● ติดตาม

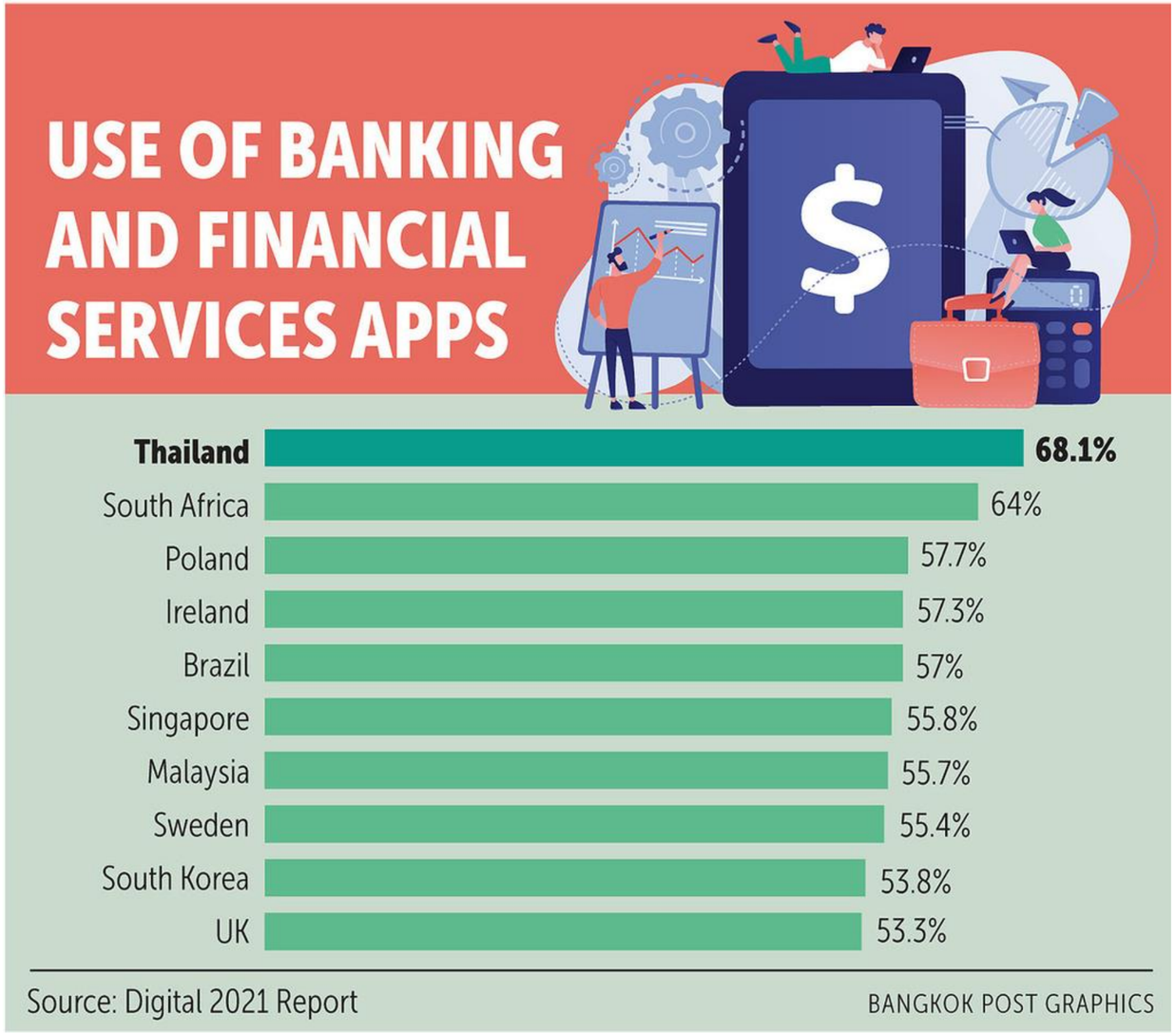
NCSA สกมช

พลอากาศตรี จเด็ด คูหะก้องกิจ

#คนไทยทำอะไร

วันนี้เราอยู่บนโลกอินเทอร์มากแค่ไหน และทำอะไรอยู่ผลสำรวจของ We Are Social ประจำต้นปี 2022 ในบรรทัดต่อไป ว่าประเทศไทยใช้เวลาแค่ไหนบนโลกอินเทอร์เน็ตในวันนี้**คนไทยมีสัดส่วนการเข้าถึงอินเทอร์เน็ต 77.8% เมื่อเทียบกับประชากรทั้งประเทศนับว่าเป็นค่าเฉลี่ยที่สูงกว่าค่าเฉลี่ยโลกที่มีสัดส่วนเข้าถึงอินเทอร์เน็ตเพียง 62.5% เท่านั้น**โดยประเทศที่มีการเข้าถึงอินเทอร์เน็ตต่ำสุดคือเคนยา มีสัดส่วนเข้าถึงเพียง 42.0% ส่วนประเทศเดนมาร์ก ไอร์แลนด์ และสหรัฐอาหรับเอมิเรตส์ เป็นประเทศที่มีสัดส่วนการเข้าถึงอินเทอร์เน็ตสูงสุดถึง 99.0% เมื่อเทียบกับประชากรทั้งประเทศถ้ามองไปที่ชั่วโมงบนโลกออนไลน์ของคนไทยต่อวันคนไทยใช้เวลาอยู่บนโลกออนไลน์มากถึง 9.06 ชั่วโมงต่อวัน เรียกได้ว่าอยู่บนโลกอินเทอร์เน็ตมากกว่า 1 ใน 3 ของวันเสียอีก ส่วนค่าเฉลี่ยโลก 6.58 ชั่วโมงต่อวันเท่านั้นเวลาที่อยู่บนโลกออนไลน์จะใช้ผ่านมือถือ 5.28 ชั่วโมงต่อวัน ทิ้งห่างค่าเฉลี่ยโลกที่ใช้อินเทอร์เน็ตผ่านมือถือเพียง 3.43 ชั่วโมงต่อวันเท่านั้นและคนไทยเชื่อมต่อโลกออนไลน์ผ่านคอมพิวเตอร์ 3.38 ชั่วโมงต่อวัน ใกล้เคียงกับค่าเฉลี่ยโลกที่ 3.14 ชั่วโมงต่อวัน

1h ถูกใจ 54,357 คน ตอบกลับ



ไทยยืนเบอร์ 1

ใช้งาน Mobile Banking มากที่สุดในโลก ครองแชมป์ 3 สมัยซ้อน

68.1% ของผู้ใช้อินเทอร์เน็ตอายุ 16-64 ปี
บอกว่าพวกเขามีการใช้งาน Application ทุกเดือน

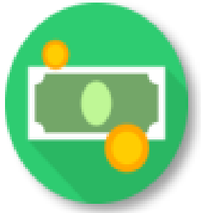
ผลการสำรวจ 10 อันดับกิจกรรมดิจิทัลที่คนไทยใช้งานในปี 2566

92.46%
ใช้งานสื่อสังคมออนไลน์

91.59%
สนทนา/แชท

72.98%
รับชม VDO Content

63.47%
สนทนาบน Blog/กระทู้



45.55%
โอนเงินผ่านเว็บไซต์/แอปพลิเคชัน/Scan QR Code

43.80%
เล่น/สตรีมมิ่งภาพยนตร์/ซีรีย์ ออนไลน์

40.00%
เล่น/สตรีมมิ่งเพลงออนไลน์

39.01%
รับฟังวิทยุ/ดูโทรทัศน์ผ่านทางออนไลน์

38.69%
โทรศัพท์ผ่านอินเทอร์เน็ต/VDO Call

33.79%
เรียนออนไลน์/เรียนทางไกล

CONTENT SHIFU

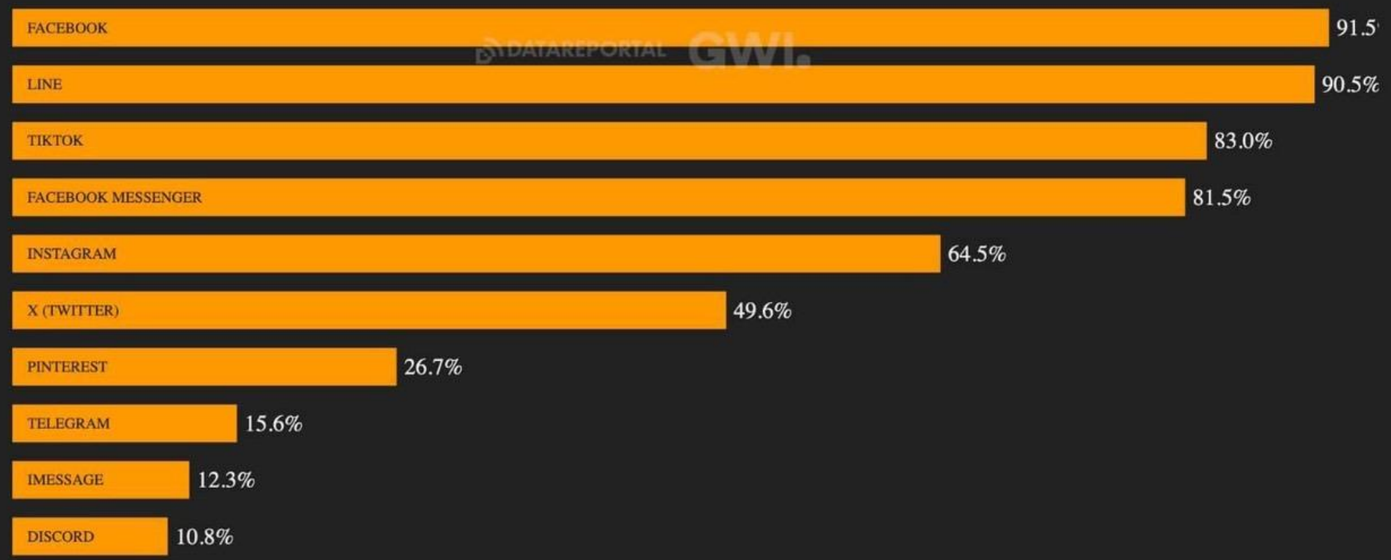
JAN 2024

MOST USED SOCIAL MEDIA PLATFORMS

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO USE EACH PLATFORM EACH MONTH

NOTE: YOUTUBE IS NOT OFFERED AS AN ANSWER OPTION FOR THIS QUESTION IN GWI'S SURVEY, SO IT WILL NOT APPEAR IN THIS RANKING

THAILAND



60

SOURCE: GWI (Q3 2023). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GWI.COM. **NOTE:** YOUTUBE IS **NOT** OFFERED AS AN ANSWER OPTION FOR THIS QUESTION IN GWI'S SURVEY. **COMPARABILITY:** A VERSION OF THIS CHART THAT APPEARED IN OUR PREVIOUS REPORTS WAS BASED ON A PREVIOUS QUESTION IN GWI'S SURVEY THAT INCLUDED YOUTUBE AS AN ANSWER OPTION. GWI'S CURRENT SURVEY FEATURES A REVISED VERSION OF THIS QUESTION THAT DOES **NOT** INCLUDE YOUTUBE AS AN ANSWER OPTION. WHILE OTHER CHANGES TO THE QUESTION'S WORDING MAY MEAN THAT THE VALUES AND RANK ORDER SHOWN HERE ARE **NOT DIRECTLY COMPARABLE** WITH THOSE SHOWN ON A SIMILAR CHART IN PREVIOUS REPORTS.

we are social Meltwater

Facebook, LINE & TikTok เป็น Social Media Platform ที่คนไทยใช้งานมากที่สุดตามลำดับ

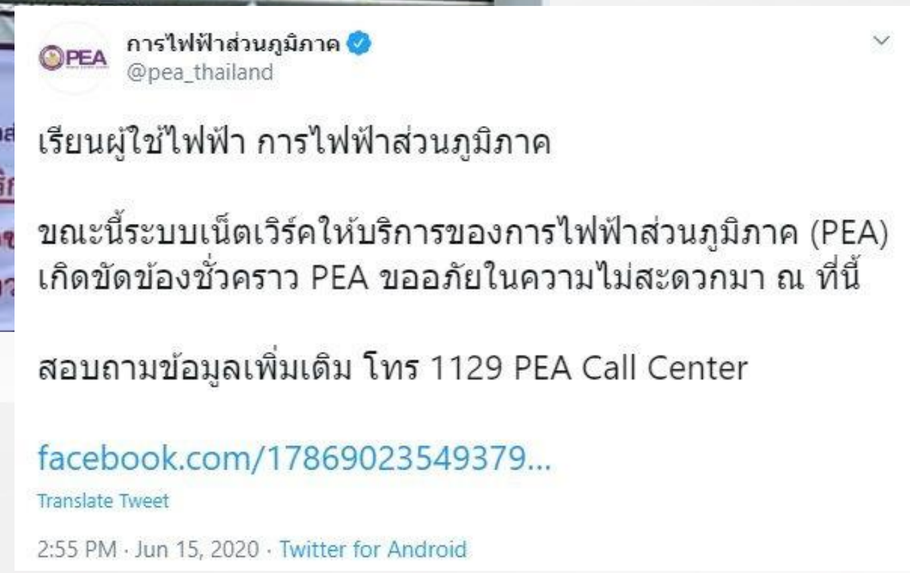
สรุปสถิติภัยคุกคามทางไซเบอร์ รวมทั้งสิ้น 80,667,100 เหตุการณ์

วันที่ 1 ต.ค. 65 – 30 ก.ย. 66

Hacked Website (Phishing, Defacement, Gambling, Malware)	26,139,981 เหตุการณ์
Fake Website	45 เหตุการณ์
จุดอ่อนช่องโหว่	95 เหตุการณ์
Data Breach	57 เหตุการณ์
Ransomware	7 เหตุการณ์
อื่นๆ	82 เหตุการณ์

การไฟฟ้าส่วนภูมิภาค (PEA) โดนโจมตี โดยกลุ่ม Maze ransomware

การไฟฟ้าส่วนภูมิภาค (PEA) โดนโจมตีโดยกลุ่ม Maze ransomware June 26, 2020
การไฟฟ้าส่วนภูมิภาค (PEA) ยอมรับว่าโดนไวรัสเรียกค่าไถ่จริง และเร่งแก้ไขอย่างเต็มที่ เมื่อวันที่ 18 มิ.ย. นายธนาเศรษฐ์ พงษ์ทรงเสถียร รองผู้ว่าการสนเทศและสื่อสาร การไฟฟ้าส่วนภูมิภาค (กฟภ.) กล่าวกรณีแอพพลิเคชั่นพีอีเอสมาร์ทพลัส ไม่สามารถใช้งานได้ เนื่องจากระบบถูกโจมตีด้วยไวรัสเรียกค่าไถ่ผ่านทางอีเมล
หลังจากนั้นมีรายงานจากทีมวิจัย Cyble ว่ามีข้อมูลจากการไฟฟ้าส่วนภูมิภาคของประเทศไทยถูกเผยแพร่โดยกลุ่ม Maze ransomware โดยข้อมูลที่โดนขโมยออกไปนั้นมีปริมาณมากกว่า 13GB เลยทีเดียว และประกอบข้อมูลเกี่ยวกับ เอกสารการตรวจสอบประจำปี เอกสารการลงทะเบียนขายสินค้า ใบแจ้งหนี้ เป็นต้น



#รพ.เพชรบูรณ์ ขอโทษ ปมโดนแฮกข้อมูลคนไข้ชี้เป็นข้อมูลทั่วไปไม่มีผลต่อการรักษา

ที่มา: https://www.bleepingcomputer.com/.../ransomware-attack-at-ge.../

วิทยากร
พลอากาศตรี จเด็ด คูหะก้องกิจ • ติดตาม

NCSA สกมช

พลอากาศตรี จเด็ด คูหะก้องกิจ

#รพ.เพชรบูรณ์

5 กันยายน 2564 มีการประกาศขายข้อมูลคนไข้โรงพยาบาลเพชรบูรณ์ทางอินเทอร์เน็ต **ขนาดข้อมูล 3.75 กิกะไบต์ จำนวน 16 ล้านเรคคอร์ด จาก 146 ฐานข้อมูล ในราคา 500$** ทางโรงพยาบาลฯ จึงรีบดำเนินการตรวจสอบโดยเร่งด่วน มีการจัดตั้งคณะกรรมการแก้ไขปัญหาภาวะคุกคามทางไซเบอร์ เพื่อตรวจสอบข้อเท็จจริงและประเมินความเสียหายที่เกิดขึ้น ข้อมูลที่มีการเผยแพร่ในอินเทอร์เน็ตแสดงข้อมูลทั่วไปของประชาชนที่มารับบริการและเจ้าหน้าที่บางส่วน ในขั้นต้นมีการปิดกั้นการเข้าถึงอินเทอร์เน็ตจากภายนอก ตรวจสอบความเสียหายระบบภายในโรงพยาบาล มีการตรวจสอบความปลอดภัยด้านไซเบอร์ ตรวจสอบระบบที่ข้อมูลรั่วไม่ให้มีการแฮกข้อมูลอยู่ในระบบ ผลการตรวจสอบไม่พบความเสียหายกับระบบปฏิบัติการที่ใช้ในการดูแลรักษาผู้ป่วย และจากการตรวจสอบขั้นต้นข้อมูลที่ประกาศขายเป็น**ข้อมูลเกี่ยวกับรายชื่อประชาชนที่มารับบริการโรงพยาบาลชื่อแพทย์ที่ดูแล และตารางเวรแพทย์ ข้อมูลสัญญาณชีพวันเวลาที่มารับบริการสิทธิการรักษา เลขประจำตัวผู้ป่วย ไม่ใช่ฐานข้อมูลการรักษา ไม่มีรายละเอียดเกี่ยวกับการวินิจฉัยและรักษาโรค** เป็นข้อมูลทั่วไปที่ไม่มีผลกระทบต่อการดูแลรักษา

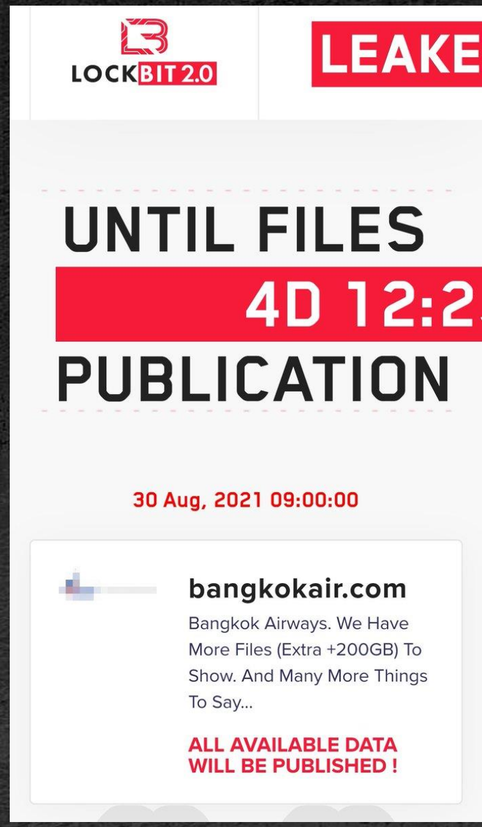
1h ถูกใจ 54,357 คน ตอบกลับ

ถูกใจโดย CYBERMAN_NCSA และคนอื่นๆ อีก 86,018 คน

ข้อมูลหลุด BANGKOK AIRWAYS

ตกเป็นเหยื่อแฮกเกอร์ โดนเจาะระบบ !!!

ล้วงข้อมูลส่วนตัว



BANGKOK AIRWAYS ออกมาประกาศเมื่อวันที่ 26 สิงหาคม 2564 ที่ผ่านมา ว่าได้พบความผิดปกติในระบบเครือข่ายของบริษัท โดยมีการเข้าถึงระบบสารสนเทศของบริษัทโดยไม่ชอบด้วยกฎหมายและไม่ได้รับอนุญาต ส่งผลให้ข้อมูลผู้ใช้ถูกขโมยไป

ข้อมูลดังกล่าวมีทั้ง ชื่อ นามสกุล สัญชาติ เพศ หมายเลขโทรศัพท์ อีเมล ที่อยู่ ช่องทางการติดต่อสื่อสาร ข้อมูลหนังสือเดินทาง ประวัติการเดินทาง ข้อมูลบัตรเครดิตบางส่วน และข้อมูลอาหารพิเศษของผู้โดยสาร ซึ่งตอนนี้บริษัทได้รายงานเหตุการณ์ดังกล่าวไปยังสำนักงานตำรวจแห่งชาติและหน่วยงานที่เกี่ยวข้องแล้ว

กลุ่มแฮกเกอร์ที่สร้างความปั่นป่วนนี้มีชื่อว่า LockBit เป็นแก๊ง Ransomware ที่ก่อนหน้านี้เตรียมประกาศว่าจะปล่อยข้อมูลลูกค้าของ Bangkok Airways จำนวนกว่า 103 GB ออกสู่สาธารณะในวันที่ 25 สิงหาคมนี้ แต่ล่าสุดเหมือนไม่มีข่าวใด ๆ ตามมา ซึ่งคาดว่า Bangkok Airways น่าจะมีการเจรจากับกลุ่มแฮกเกอร์แล้ว

เครดิต : techhub

"ข้อมูลหลุด" ทปอ. ยอมรับข้อมูล TCAS64 ช่วง พ.ค. โดนแฮกจริง 23,000 รายการ !!!!!

ทปอ
สมาคมที่ประชุมอธิการบดีแห่งประเทศไทย
Association of The Council of University Presidents of Thailand

ประกาศที่ประชุมอธิการบดีแห่งประเทศไทย
เหตุภัยคุกคามทางไซเบอร์ระบบการคัดเลือกกลางบุคคลเข้าศึกษาต่อในสถาบันอุดมศึกษา (TCAS)

ด้วยวันที่ 1 ก.พ. 2565 ปรากฏข้อมูลข่าวสารการประกาศจำหน่ายข้อมูลในอินเตอร์เน็ตจำนวน 23,000 รายการ ถูกกล่าวอ้างว่า เป็นข้อมูลส่วนบุคคลของระบบการคัดเลือกกลางบุคคลเข้าศึกษาในสถาบันอุดมศึกษา (TCAS) จากเว็บไซต์ mytcas.com ทั้งนี้ ได้มีการแสดงข้อมูลตัวอย่าง เช่น ชื่อ นามสกุล เลขที่บัตรประจำตัวประชาชน ผลคะแนนตามเกณฑ์การคัดเลือกของสาขาวิชาที่สมัคร เป็นต้น ขณะนี้ ทาง ทปอ. ได้ตรวจสอบทั้งหมดในไฟล์ตัวอย่างแล้ว พบว่า เป็นข้อมูลของระบบ TCAS64 ในรอบที่ 3 ซึ่งไม่ใช่ข้อมูลส่วนบุคคลทั้งหมดของผู้สมัครและเป็นข้อมูลในรูปแบบ CSV ที่เจ้าหน้าที่ที่ได้รับมอบหมายของแต่ละสถาบันอุดมศึกษาดึงออกจากระบบเพื่อประมวลผลคัดเลือกของแต่ละสาขาวิชาที่เปิดรับในสถาบันฯ โดยเจ้าหน้าที่สามารถเข้าถึงได้เฉพาะข้อมูลผู้สมัครในรอบ 3 ของสถาบันนั้น ๆ ซึ่งข้อมูลในรอบ 3 ของระบบ TCAS64 มีทั้งหมด 826,250 รายการ แต่ที่ผู้ขายข้อมูลกล่าวอ้างนั้น มี 23,000 รายการ โดยคาดว่าเป็นไฟล์ที่สร้างขึ้นในช่วงเดือนพฤษภาคม 2564 ที่เจ้าหน้าที่ของสถาบันอุดมศึกษาดึงข้อมูลคะแนนไปจัดเรียงลำดับผู้สมัคร(Ranking) ตามเกณฑ์คัดเลือกของแต่ละสาขาวิชา ซึ่งข้อมูลที่นำเสนอขายไม่มีผลการจัดเรียงลำดับ Ranking ของผู้สมัคร

ปัจจุบัน ทปอ. ได้ปิดระบบ TCAS64 ไปแล้วตั้งแต่เดือนธันวาคม 2564 และ สำหรับระบบ TCAS65 มีการเปลี่ยนระบบเป็นรูปแบบใหม่ และเว็บไซต์ที่พัฒนาขึ้นใหม่ในปีนี้ มีการจัดเก็บไฟล์ข้อมูลที่มีความอ่อนไหวในรูปแบบ Private ที่ไม่สามารถเข้าถึงโดยตรงได้ การที่จะเข้าถึงไฟล์ข้อมูลได้นั้น ผู้ใช้งานระบบต้องได้รับการอนุญาตจากระบบ (presigned URL) ที่มีอายุในเวลาที่กำหนดเท่านั้น ซึ่งผู้ใช้งานระบบสามารถเข้าถึงข้อมูลได้ชั่วคราว พร้อมระบบบันทึกการใช้งานอย่างละเอียด

อย่างไรก็ตาม ทปอ. ขออภัยอย่างสูงสำหรับผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคลที่ถูกกล่าวอ้าง ตลอดจนตระหนักถึงการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ จากเหตุการณ์ดังกล่าว จึงได้มีการตรวจสอบระบบและกระบวนการทำงานอย่างละเอียด ซึ่งได้รับการสนับสนุนจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และอยู่ระหว่างการรวบรวมพยานหลักฐานที่เกี่ยวข้องเพื่อดำเนินการแจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ และแจ้งเหตุไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อรับทราบสถานการณ์ต่อไป

ทปอ. ขอยืนยันว่า ระบบ TCAS65 มีความปลอดภัยในการใช้งาน และ มีการเฝ้าระวังสิ่งผิดปกติ ร่วมกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) อย่างใกล้ชิด เพื่อให้คงไว้ซึ่งความน่าเชื่อถือในระบบและกระบวนการคัดเลือกต่อไป

เครดิต : คมชัดลึก

1 ก.พ. 2565 ปรากฏข้อมูลข่าวสารการประกาศจำหน่ายข้อมูลในอินเทอร์เน็ต จำนวน 23,000 รายการ ถูกกล่าวอ้างว่า เป็นข้อมูลส่วนบุคคลของระบบการคัดเลือกบุคคลเข้าศึกษาในสถาบันอุดมศึกษา (TCAS) จากเว็บไซต์ mytcas.com

ทั้งนี้ ได้มีการแสดงข้อมูลตัวอย่าง เช่น ชื่อ นามสกุล เลขที่บัตรประจำตัวประชาชน ผลคะแนนตามเกณฑ์การคัดเลือกของสาขาวิชาที่สมัคร เป็นต้น

วิทยากร
พลอากาศตรี จเด็ด คูหะก้องกิจ

NCSA สกมช

แฮกทวิตเตอร์สรรพากร เป็น NFT

16 มกราคม 2565 อยู่ๆ หน้าบัญชีทวิตเตอร์ของกรมสรรพากรก็ถูกเปลี่ยนเป็นรูป ‘ลิงเบื่อ’ พร้อมกับเปลี่ยนชื่อและข้อมูลในบัญชีโดย มีการระบุถึงการซื้อขายทรัพย์สินด้วยเงินดิจิทัลหรือ NFT บนหน้าโปรไฟล์ ทั้งยังลบทวิตเก่าๆ ที่กรมสรรพากรโพสต์ออกไปทั้งหมด

แฮกเว็บกระทรวงพลังงาน

1 ธันวาคม 2564 เมื่อเข้าสู่หน้าเว็บไซต์ของกระทรวงพลังงานหลายคนก็ต้องงงไป เมื่อข้อมูลที่ปรากฏขึ้นกลายเป็นข้อมูลชักชวนให้ไปเล่นพนันออนไลน์แทน โดยเพจดัง Drama Addict เป็นผู้พบปัญหาและแจ้งให้กับทางกระทรวงพลังงานต่อมาหนึ่งวันทางกระทรวงจึงได้ออกมาแจ้งว่าสามารถแก้ไขและกู้คืนข้อมูลได้เรียบร้อยแล้ว

แฮกเว็บสำนักงานศาลรัฐธรรมนูญ

11 พฤศจิกายน 2564 เว็บไซต์ของสำนักงานศาลรัฐธรรมนูญถูกแฮกพร้อมอัปโหลดหน้าเว็บไซต์ใหม่ในชื่อ ‘Kangaroo Court’ หรือแสลงคำว่า ‘ศาลเตี้ย’ ในภาษาไทย และอัปโหลดเพลง Guillotine ขึ้นบนหน้าเว็บไซต์ ซึ่งเหตุการณ์นี้เกิดขึ้นหลังศาลรัฐธรรมนูญวินิจฉัยคดีของแกนนำกลุ่มราษฎร นายอานนท์ นำภา, นายภาณุพงศ์ จาดนอก (ไมค์) และ น.ส.ปนัสยา สิทธิจิรวัฒนกุล (รุ้ง) ซึ่งถูกวินิจฉัยว่าเป็นการใช้สิทธิหรือเสรีภาพเพื่อล้มล้างการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข

ข้อมูลนักท่องเที่ยวที่เคยเดินทางมาประเทศไทยรั่วไหล 106 ล้านคน

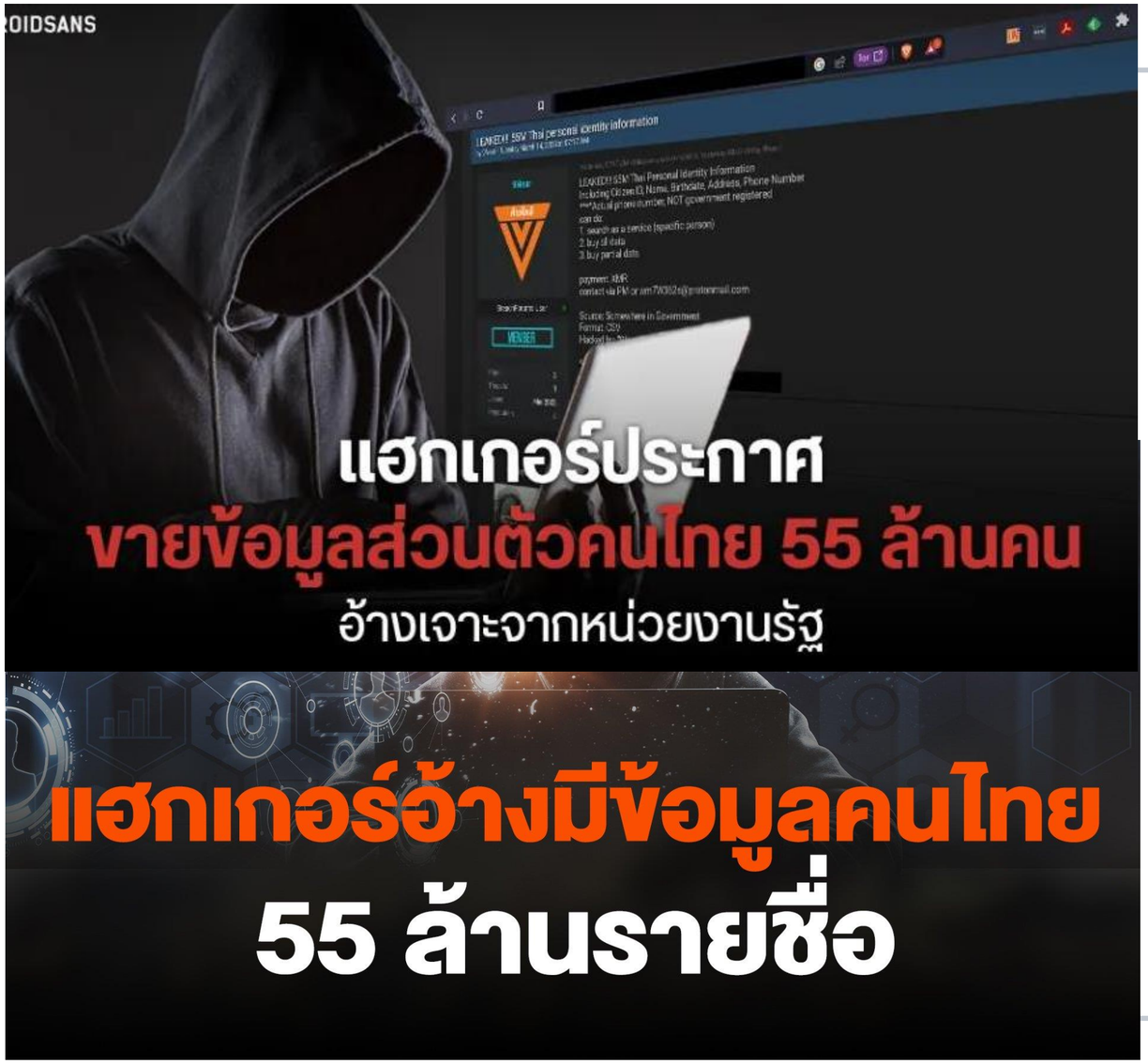
22 กันยายน 2564 สื่อต่างชาติรายงานว่าข้อมูลจากบริษัท คอมพาริเทค (Comparitech) บริษัทวิจัยได้สนใจความปลอดภัยทางไซเบอร์จากอังกฤษ พบข้อมูลนักท่องเที่ยวที่เคยเดินทางมาประเทศไทยในรอบ 10 ปีมากกว่า 106 ล้านคนถูกเปิดเผยข้อมูลส่วนตัวเช่น ชื่อ–สกุล หมายเลขพาสปอร์ต วันที่เดินทางเข้าประเทศไทย และอื่นๆ โดยคาดว่าน่าจะมีการรั่วไหลจากสำนักงานตรวจคนเข้าเมือง เนื่องจากมีข้อมูลการเดินทางและเลขพาสปอร์ต และสร้างความกังวลว่าข้อมูลรั่วไหลจะส่งผลกระทบต่อความเชื่อมั่นในการท่องเที่ยว

ประวัติคนไข้ถูกขาย 16 ล้านราย

วันที่ 6 กันยายน 2564 ได้มีรายงานข้อมูลพื้นฐานของคนไข้ในระบบสาธารณสุขรั่วไหลกว่า 16 ล้านรายชื่อ โดยมีข้อมูลเช่น ที่อยู่ โทรศัพท์ เลขบัตรประชาชน วันเดือนปีเกิด ชื่อโรงพยาบาล ชื่อบิดา สิทธิในการรักษา และข้อมูลทางการแพทย์ที่รวมถึงชื่อโรงพยาบาลและรหัสทั่วไป โดยมีการลงขายข้อมูลเหล่านี้บนหน้าเว็บไซต์

#NCSA

#คนไทยถูก "แฮก 55 ล้านรายชื่อ"



ที่มา: https://www.bleepingcomputer.com/.../ransomware-attack-at-ge.../

วิทยากร
พลอากาศตรี จเด็ด คูหะก้องกิจ • ติดตาม

NCSA สกมช

พลอากาศตรี จเด็ด คูหะก้องกิจ

#9Near

กรณี ผู้ใช้งานบัญชี **9near** ได้โพสต์ขายข้อมูลที่อ้างว่าเป็นข้อมูลส่วนตัวของคนไทยกว่า 55 ล้านรายการ บนเว็บไซต์ Bleach Forums โดย**อ้างว่าได้มาจากหน่วยงานรัฐแห่งหนึ่งในไทย (Somewhere in government) และโพสต์ตัวอย่างไฟล์ ซึ่งมี ชื่อ นามสกุล ที่อยู่ วันเกิด เบอร์โทรศัพท์ และเลขประจำตัวประชาชน** รวมทั้งมีการโพสต์ ลักษณะข่มขู่หน่วยงานและประชาชนในวงกว้าง วันที่ 31 มีนาคม 2566 รายการเรื่องเล่าเช้านี้ ช่อง 3 รายงานว่า กรณีนี้ผู้ประกาศข่าวชื่อดัง สรยุทธ สุทัศนะจินดา ยืนยันว่า ได้รับการส่ง SMS ดังกล่าวพร้อมกับแนบลิงก์หน้าเว็บไซต์ โดยข้อความนั้นมีข้อมูลทั้งหมายเลขบัตรประชาชน ที่อยู่ วัน เดือน ปีเกิด เบอร์โทรศัพท์ ตรงกับข้อมูลจริง และนอกจากตนเองแล้ว ยังมีผู้ประกาศข่าวโดนลักษณะเช่นนี้หลายคน เช่น หนุ่ม กรรชัย และ อ๊อฟ ชัยนนท์ เป็นต้น

1h ถูกใจ 54,357 คน ตอบกลับ

ถูกใจโดย CYBERMAN_NCSA และคนอื่นๆ อีก 86,018 คน


PPTV HD 36
กรมกิจการผู้สูงอายุ
Department of Older Persons (DOP)
รั่วไหลจริง 2 แสนกว่ารายชื่อ
ข้อมูลคนไทยรั่วไหล
ถูกประกาศขายกว่า 20 ล้านบัญชี!


FM 100.5
MCOT NEWS
MCOT NEWS FM100.5
ชี้ข้อมูลคนไทยหลุดจริง 2.3 แสนคน

pdpc สคส. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

นายศิวรักษ์ ศิวโมกษธรรม เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) หรือ PDPC กล่าวว่า PDPC จะเร่งรัดและเคร่งครัดในการตรวจ ปราบปราม ข้อมูลส่วนบุคคลรั่วไหล และ การลักลอบซื้อขายข้อมูลส่วนบุคคล ซึ่งได้มีการทำงานร่วมกันระหว่าง PDPC Eagle Eye และ บช.สอท. กับ สกมช. อย่างเข้มข้นในช่วง 4 เดือนที่ผ่านมา โดยในช่วงดังกล่าว มีกรณีที่ศาลได้ตัดสินลงโทษจำคุกผู้กระทำความผิด 2 ปี โดยไม่รอลงอาญา นอกจากนี้สำนักงานยังคงเดินหน้าเพื่อสนองรับนโยบายในการมีมาตรการในการจัดการกับหน่วยงานที่ไม่มีการคุ้มครองข้อมูลส่วนบุคคล เดินสายให้ความรู้แก่ประชาชน ตลอดจนถึงการเร่งปรับแก้การบังคับใช้กฎหมายให้มีบทลงโทษที่หนักยิ่งขึ้นสำหรับการลักลอบซื้อขายข้อมูลส่วนบุคคล

Ref : https://www.opt-news.com/news/41041

โทษทางแพ่ง (มาตรา 77, 78)

การทำให้เกิดความเสียหายแก่เจ้าของข้อมูล จะต้องชดใช้ “ค่าสินไหมทดแทน”

- จ่ายค่าสินไหมทดแทน ไม่เกิน 2 เท่า ของสินไหมทดแทนที่แท้จริง
- อายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหาย หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

โทษทางอาญา (มาตรา 79, 80)

- กระทำการอันน่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง ได้รับความอับอาย ฯลฯ ระวางโทษจำคุกไม่เกิน 6 เดือน หรือ ปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ
- กระทำการเพื่อแสวงหาผลประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย ระวางโทษจำคุกไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ระวางโทษจำคุกไม่เกิน 6 เดือน หรือ ปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ

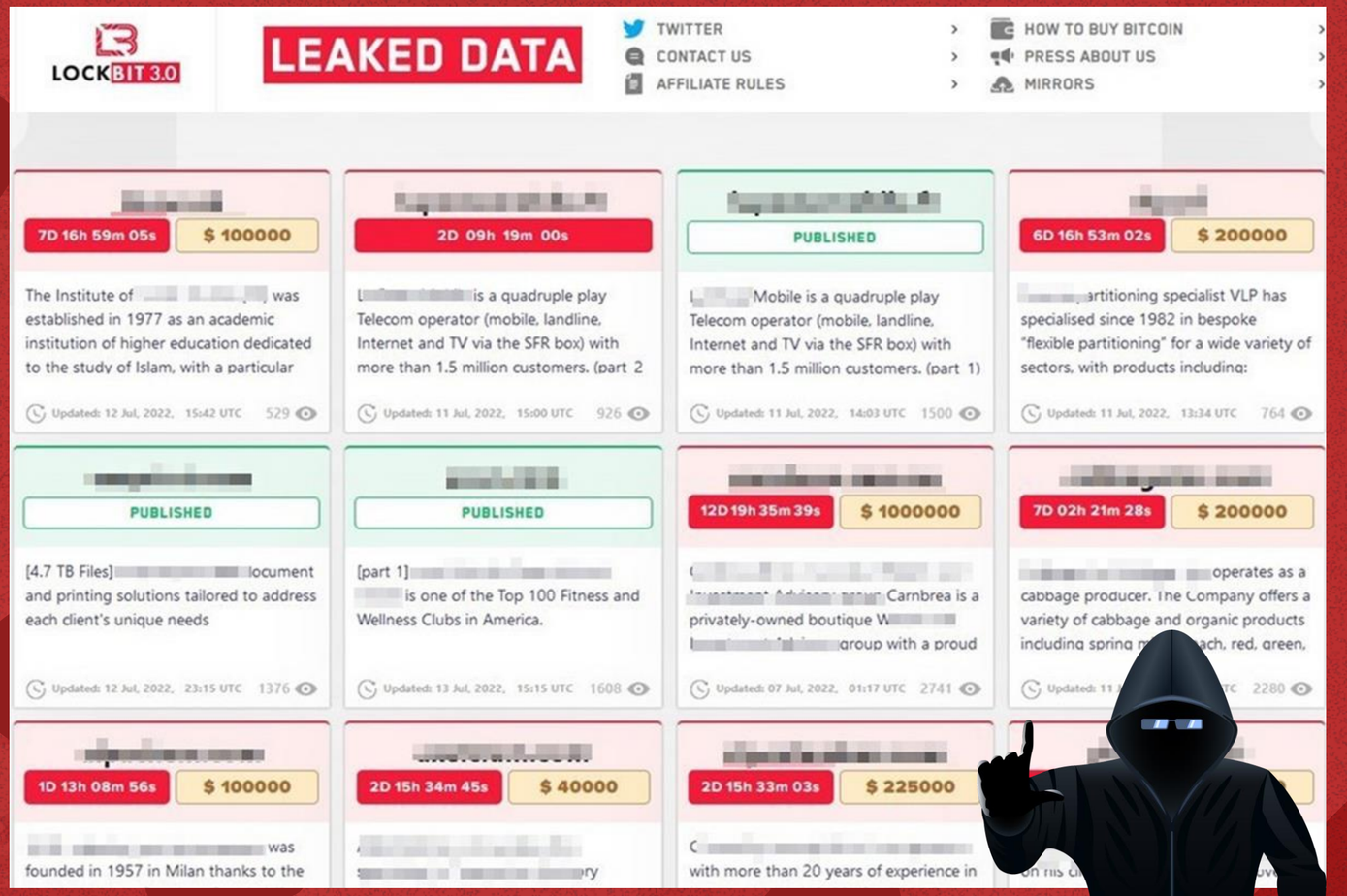
โทษทางปกครอง (มาตรา 82-90)

- ไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ ไม่จัดทำบันทึกรายการ ฯลฯ มีโทษปรับไม่เกิน 1,000,000 บาท
- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่แจ้งวัตถุประสงค์การใช้งาน เก็บข้อมูลเกินความจำเป็น ฯลฯ มีโทษปรับไม่เกิน 3,000,000 บาท
- เก็บรวบรวม ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย มีโทษปรับไม่เกิน 5,000,000 บาท

ศึกษารายละเอียดเพิ่มเติมจาก
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

NCSA สกมช

ข้อมูล LOCKBIT 2.0 และ 3.0 ที่โจมตีในประเทศไทย



ปีที่พบ	จำนวนหน่วยงาน	มูลค่าความเสียหาย
2022	14	619,000,000
2023	17	690,000,000
2024	3	152,000,000
รวม	34	**1,461,000,000**

ความเสียหายที่เกิดจากจาก LOCKBIT 2.0 และ 3.0

รวม 1,461,000,000 บาท

#ประมาณการจาก ขนาดธุรกิจ ทุนจดทะเบียน จำนวนข้อมูลที่ถูกเผยแพร่ และข้อมูลงบการเงินของบริษัทที่เสียหาย

#พบบริษัทจดทะเบียนตลาดหุ้น "โดนแฮกข้อมูล" จ่ายเงินเข้าบัญชีแฮกเกอร์นับร้อยล้าน

ที่มา: https://mgronline.com/onlinesection/detail/9630000018139

วิทยากร
พลอากาศตรี จเด็ด คูหะก้องกิจ ● ติดตาม

NCSA สกมช

พลอากาศตรี จเด็ด คูหะก้องกิจ

#แฮพบบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ

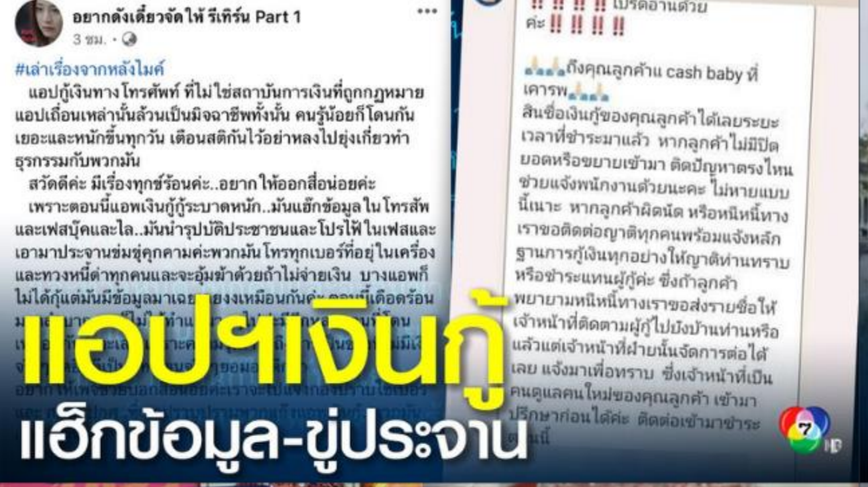
พบบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ รายหนึ่งยอมรับว่า ค่าใช้จ่ายในการบริหาร**เพิ่มขึ้นจาก 200 กว่าล้านเป็นเกือบพันล้าน เหตุเพราะโดนแฮกข้อมูลทางอีเมล** ทำให้มีการจ่ายเงินไปยังบัญชีแฮกเกอร์ ตอนนี้พยายามเพิ่มระบบป้องกันภายในและหาทางเรียกคืนค่าเสียหายวันนี้ (23 ก.พ.) รายงานข่าวแจ้งว่า ได้มี**บริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยรายหนึ่ง** (ขอสงวนนาม) ได้เผยแพร่คำอธิบายและการวิเคราะห์ทางการเงิน สำหรับผลการดำเนินงานประจำไตรมาส 4 และประจำปี 2562 โดยพบว่าผลการดำเนินงานทางการเงินของบริษัทฯ ไตรมาส 4/62 ขาดทุนสุทธิ 2,975 ล้านบาท ส่งผลทำให้ในปี 2562 ขาดทุนสุทธิ 2,809 ล้านบาท และพบว่าในไตรมาส 4/62 มีค่าใช้จ่ายในการบริหาร (Selling, General & Administrative Expense หรือ SG&A) เพิ่มขึ้นจาก 252 ล้านบาทในช่วงเดียวกันของปีก่อน (ไตรมาส 4/61) เป็น 939 ล้านบาท หรือเพิ่มขึ้น 687 ล้านบาท

1h ถูกใจ 54,357 คน ตอบกลับ

ถูกใจโดย CYBERMAN_NCSA และคนอื่นๆ อีก 86,018 คน

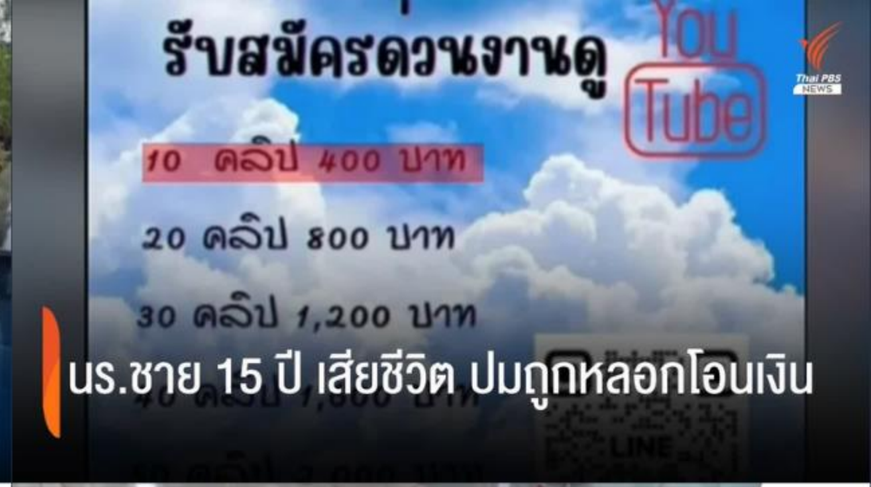
MENU 01 07 12

รู้ไหมภัยออนไลน์ที่คนไทยถูกหลอกมีอะไรบ้าง ?



แอปฯเงินกู้
แฮ็กข้อมูล-ขู่ประจาน

ม.3 ฆ่าตัวตาย สำนึกผิด
ขโมยเงินแม่ไปลงทุนแต่ถูกหลอก



นร.ชาย 15 ปี เสียชีวิต ปมถูกหลอกโอนเงิน

หลอก ม.4 เกลี้ยงบัญชี!

สาวช้ำ ลีมินโฮปลอม
หลอกสูบเงิน 7 หมื่น

ผู้จัดการธนาคารยังโดน!
เหยื่อคอลเซนเตอร์ สูญเงิน 1 ล้าน

โดนบูลลี่ยันตาย

ผู้ประกาศดัง เจอภัยแก๊งคอลเซ็นเตอร์ !

หลอกยันพระ!
“กู้เงินออนไลน์”

แจ้งความออนไลน์

www.thaipoliceonline.go.th

สะสม 1 มี.ค.65 - 15 เม.ย.67

ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ

แจ้งความผ่านระบบ www.thaipoliceonline.go.th 518,163 เรื่อง

คดีออนไลน์	คดีอาญาอื่นๆ	จำหน่ายออกจากระบบ
488,955 เรื่อง	13,099 เรื่อง	21,256 เรื่อง

สายด่วน (1441) 484,889 สาย

คดีออนไลน์	คดีอื่นๆ	เรื่องทั่วไป
256,069 สาย	37,167 สาย	47,366 สาย

Walk In แจ้งความที่หน่วย 80,900 เรื่อง

เป็นคดีที่เชื่อมโยงกัน 231,291

เป็นคดีที่ไม่เชื่อมโยงกัน 257,664

คดีออนไลน์ 488,955

ผลการอายัดบัญชี

ขออายัด 191,986 CaseID 322,533 บัญชี

ยอดเงิน 22,785,495,178 บาท

อายัดได้ทัน 5,485,343,286 บาท

รวมมูลค่าความเสียหาย

66,463,371,501 บาท

สถิติการรับแจ้งคดีออนไลน์

14 ประเภทคดีออนไลน์

	จำนวน	คิดเป็น	ความเสียหาย
1 หลอกลวงซื้อขายสินค้าหรือบริการ ไม่เป็นขบวนการ	205,854	42.34%	3,758,758,676
2 หลอกให้โอนเงินเพื่อทำงานฯ	62,962	12.92%	7,953,768,044
3 หลอกให้กู้เงิน	52,367	10.74%	2,400,101,719
4 หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	38,075	7.81%	20,873,345,053
5 ข่มขู่ทางโทรศัพท์ (Call Center)	32,733	6.72%	8,158,654,974
6 หลอกเป็นบุคคลอื่นเพื่อยืมเงิน	19,859	4.09%	579,099,451
7 หลอกให้โอนเงินเพื่อรับรางวัลฯ	15,990	3.28%	2,260,416,569
8 หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ	14,671	3.01%	2,002,511,569
9 หลอกลวงซื้อขายสินค้าหรือบริการ เป็นขบวนการ	9,181	1.88%	90,772,572
10 หลอกเกี่ยวกับสินทรัพย์ดิจิทัล	5,916	1.21%	4,956,666,913
11 กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ฯ	5,317	1.09%	1,185,415,900
12 หลอกให้รักแล้วโอนเงิน(Romance Scam)	3,806	0.78%	1,207,817,761
13 หลอกให้ลงทุนตามพ.ร.ก.กู้ยืมเงินฯ	3,574	0.73%	710,892,335
14 เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่น (Ransomware)	487	0.10%	155,830,851
คดีออนไลน์อื่นๆ	11,084	2.27%	10,170,865,485

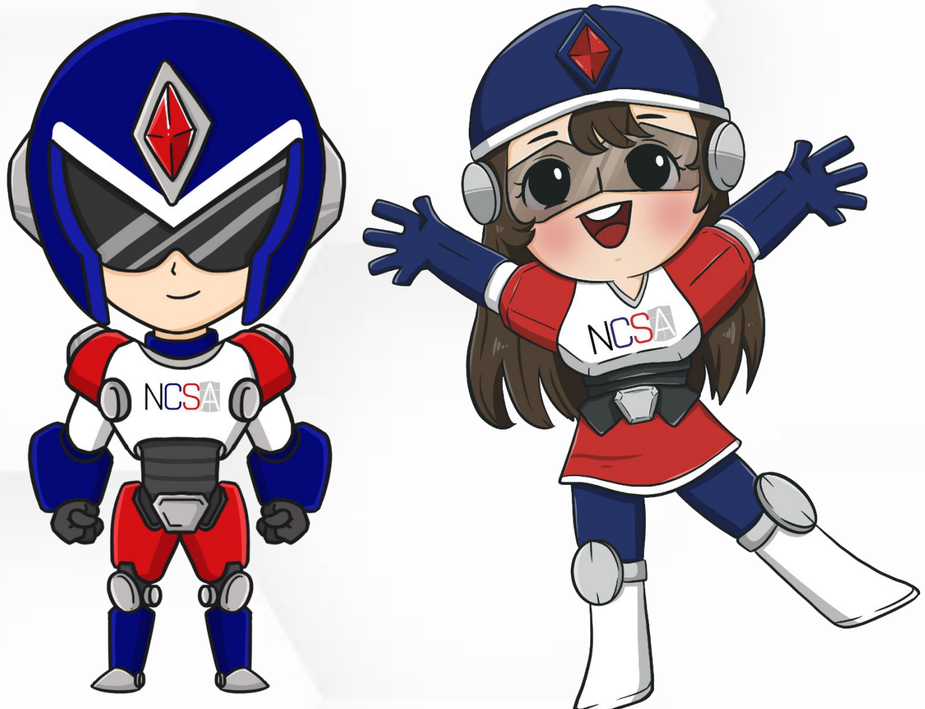
NCSA สกมช

ปี 66 คนไทยตกเป็นเหยื่อ 'มิจฉาชีพ' โดนหลอกเงินไปแล้ว 50,000 ล้านบาท

		มีอัตราการหลอกลวงที่
อินเดีย	(89.5 พันล้านรายการ)	44.6%
บราซิล	(29.2 พันล้านรายการ)	22.6%
จีน	(17.6 พันล้านรายการ)	10.7%
ไทย	(16.5 พันล้านรายการ)	25.7%
เกาหลีใต้	(8.0 พันล้านรายการ)	6.2%

หัวข้อบรรยาย

- เกี่ยวกับ สกมช.
- นิยาม
- สภาวะแวดล้อมด้านไซเบอร์ของประเทศไทยในปัจจุบัน + ผลกระทบ
- พูดคุยเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้จากภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทย



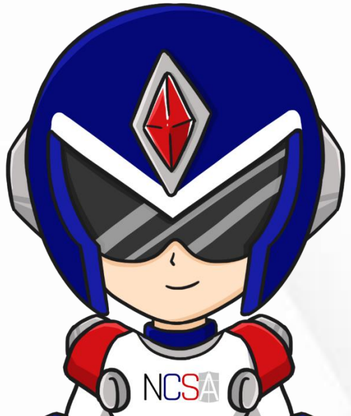
ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) จากภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทยควรอยู่ตรงไหน

Q: National information assets/สิ่งที่เรากำลังพยายามจะปกป้องมีอะไรบ้าง?
A:

Q: Cyber threat actors/จากผู้ก่อให้เกิดภัยคุกคามทางไซเบอร์ประเภทใด?
A:

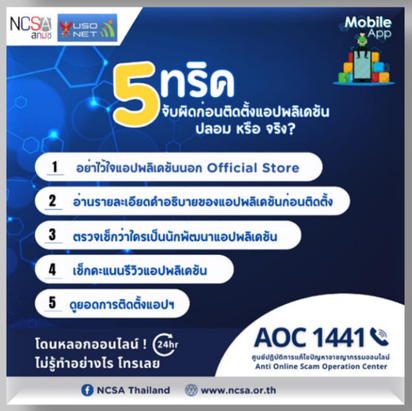
Q: Authorized official/ใครควรเป็นผู้กำหนดระดับความเสี่ยงที่ยอมรับได้ของประเทศไทย?
A:

Q: Risk appetite statement(s)/ระดับความเสี่ยงที่ยอมรับได้ของประเทศไทย?
A:



การรักษาความมั่นคงปลอดภัยไซเบอร์ไม่มี**สูตรสำเร็จ**
แต่ต้องมีกระบวนการบริหารจัดการ การวางแผน และติดตามผลอย่างต่อเนื่อง

ร่วมสร้างการตระหนักรู้ เสริมเกราะป้องกัน
สร้างภูมิคุ้มกันภัยไซเบอร์ไปกับ สกมช.



Download Infographic

เพื่อเผยแพร่ประชาสัมพันธ์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ขอเสนอ **คลังความรู้ด้านไซเบอร์**

แหล่งเรียนรู้ไซเบอร์สำหรับประชาชนทุกช่วงวัยที่คุณห้ามพลาด สำหรับการ Upskill และ Reskillเพื่อสร้างการตระหนักรู้และมีภูมิคุ้มกันภัยไซเบอร์ สามารถเข้าไปศึกษาได้ฟรี พร้อมรับใบ Certification ไม่เสียค่าใช้จ่าย

โดยมีชั่วโมงการเรียนรู้กว่า 1,000 ชั่วโมง

เรียนฟรี! ได้ใบ CERTIFICATE! FREE

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CYBER KNOWLEDGE CENTER

"คลังความรู้ด้านไซเบอร์"

NCSA สกมช

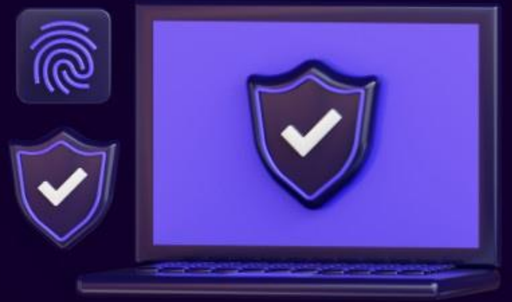
THNCA Thailand National Cyber Academy สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ by NCSA

SCAN ME

LINK : HTTPS://LINKTR.EE/THNCA

สแกนได้แล้ววันนี้
เรียนรู้ได้อย่างไร้ขีดจำกัด

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ส่งเสริมสังคมการเรียนรู้และเผยแพร่คลังความรู้ด้านไซเบอร์
เพื่อพัฒนาทักษะและการเรียนรู้ได้อย่างไร้ขีดจำกัด เข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์



CYBERSECURITY AWARENESS

CYBERSECURITY KNOWLEDGE SHARING

NCSA MOOC CYBER-LEARNING

อุ่นใจไซเบอร์ AIS

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

CYBERSECURITY SKILL
- CYBERSECURITY SKILL
- NCSA CYBERSECURITY KNOWLEDGE SHARING ครั้งที่ 7/2566 หัวข้อ "ผู้สูงวัยกับภัยออนไลน์"
- 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 เคล็ดลับความปลอดภัยทางไซเบอร์และวิธีรับมือกับมิจฉาชีพรูปแบบต่างๆ
- นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ประชาคมไซเบอร์และความรู้อื่นๆอีกมากมาย

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


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