

รายงานสรุปผลการจัดฝึกอบรม

กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของรัฐสภา ให้แก่ข้าราชการสำนักงานเลขาธิการสภาผู้แทนราษฎร

รายงานสรุปผลการจัดฝึกอบรม

กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา ให้แก่ข้าราชการสำนักงานเลขาธิการสภาผู้แทนราษฎร

๑. หลักการและเหตุผล

สืบเนื่องจากความก้าวหน้าของวิทยาการทางด้านเทคโนโลยีสารสนเทศและการสื่อสารที่รวดเร็ว และมีการพัฒนาเปลี่ยนแปลงอยู่ตลอดเวลา กอปรกับแนวนโยบายภาครัฐ ที่ต้องการสนับสนุนให้หน่วยงานของรัฐ มีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้ในการปฏิบัติงานเพิ่มมากขึ้น เพื่อให้ทันสมัย เพิ่มประสิทธิภาพในการปฏิบัติงาน และเสริมสร้างความรวดเร็วในการให้บริการกับประชาชน และเพื่อให้เป็นไปตามแผนยุทธศาสตร์ สำนักงานเลขาธิการสภาผู้แทนราษฎร พ.ศ. ๒๕๖๑-๒๕๖๔ ในยุทธศาสตร์ที่ ๑ พัฒนาองค์กรให้ก้าวไปสู่การเป็น Digital Parliament & Smart Parliament และยุทธศาสตร์ที่ ๔ ยกระดับศักยภาพของบุคลากรให้มีขีดสมรรถนะสูง มีธรรมาภิบาล และความผาสุกในการปฏิบัติงาน และเป็นไปตามแผนการขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการสภาผู้แทนราษฎร (พ.ศ. ๒๕๖๑-๒๕๖๕) ยุทธศาสตร์ที่ ๓ ส่งเสริมและสนับสนุนให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ความสามารถ และทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ

โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภานี้ เป็นกิจกรรมที่สำคัญกิจกรรมหนึ่งในการเสริมสร้างความรู้ความเข้าใจในการดูแลรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐสภา ซึ่งต้องอาศัยความร่วมมือจากผู้ใช้งานร่วมกันทุกฝ่าย การจัดกิจกรรมนี้จึงเป็นการให้ความรู้ สร้างความเข้าใจในการดูแล รักษาความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศด้วยตนเอง รวมถึงให้เกิดความตระหนักถึงความสำคัญในการใช้งานเทคโนโลยีสารสนเทศให้มีความปลอดภัย และรู้เท่าทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๒.๑ เพื่อเสริมสร้างความรู้ ความเข้าใจให้แก่ข้าราชการของสำนักงานเลขาธิการสภาผู้แทนราษฎร ให้มีความรู้ ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศให้ถูกต้อง และปลอดภัย

๒.๒ เพื่อให้ข้าราชการของสำนักงานเลขาธิการสภาผู้แทนราษฎร สามารถนำความรู้ ประสบการณ์ที่ได้รับจากการฝึกอบรมมาประยุกต์ใช้ในการปฏิบัติงานได้

๓. ระยะเวลาดำเนินการ เดือนมีนาคม พ.ศ. ๒๕๖๕

๔. กลุ่มเป้าหมาย

ข้าราชการของสำนักงานเลขาธิการสภาผู้แทนราษฎร จำนวน ๑๐๐ คน

๕. เป้าหมายการดำเนินงาน

จัดฝึกอบรมความรู้ ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา ให้แก่ข้าราชการสำนักงานเลขาธิการสภาผู้แทนราษฎร จำนวน ๑๐๐ คน

๖. งบประมาณ

ค่าใช้จ่ายในการจัดกิจกรรมบรรยาย ได้แก่ ค่าสมนาคุณวิทยากร งบประมาณทั้งสิ้น ๗,๒๐๐.- บาท (เจ็ดพันสองร้อยบาทถ้วน)

๗. ผลที่คาดว่าจะได้รับ

๗.๑ ผู้เข้าร่วมกิจกรรมได้รับความรู้ ความเข้าใจเกี่ยวกับความรู้ในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๗.๒ ผู้เข้าร่วมกิจกรรมเกิดแนวคิดด้านเทคโนโลยีสารสนเทศและการสื่อสาร และนำไปปรับใช้ในการปฏิบัติงานของตนได้

๘. ตัวชี้วัด

๘.๑ ผลผลิต : ผู้เข้าฝึกอบรม ไม่น้อยกว่าร้อยละ ๘๐ ผ่านเกณฑ์การประเมิน

๘.๒ ผลลัพธ์ : ผู้เข้าฝึกอบรมสามารถนำความรู้ที่ได้รับไปปรับใช้ในการปฏิบัติงานได้

๙. การติดตามและประเมินผล

๙.๑ ประเมินผลความพึงพอใจด้วยแบบสอบถาม

๙.๒ ประเมินผลการเรียนก่อน-หลังเรียนด้วยแบบทดสอบ

๑๐. ผู้รับผิดชอบโครงการ :

กลุ่มงานวิทยาการคอมพิวเตอร์ สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร

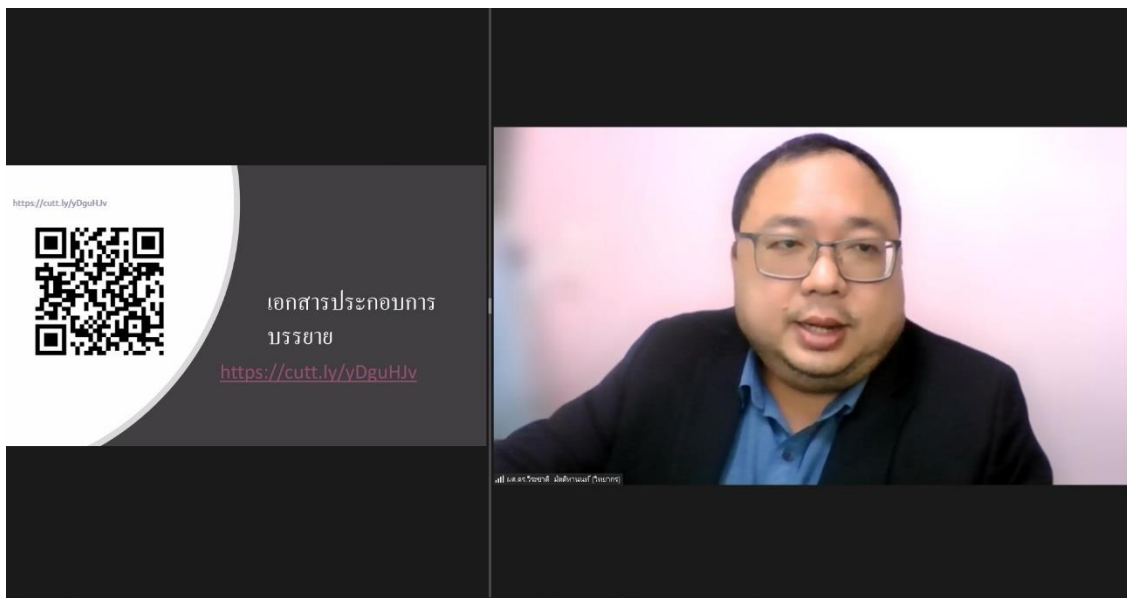
๑๑. สรุปผลการจัดโครงการ มีดังนี้

รูปแบบการดำเนินการ :	จัดกิจกรรมผ่านระบบออนไลน์
กลุ่มเป้าหมาย :	เป็นข้าราชการของสำนักงานเลขาธิการสภาผู้แทนราษฎร มีผู้เข้าร่วมกิจกรรม จำนวน ๒๒๐ คน
กรอบระยะเวลา :	ระยะเวลา ๖ ชั่วโมง วันที่ ๒๙ มี.ค. ๖๕ เวลา ๐๙.๐๐-๑๖.๐๐ น.
ผลประเมินด้านความรู้ของผู้เข้ารับการอบรม :	<div>☞ ผู้เข้าร่วมกิจกรรมมีความรู้ ความเข้าใจเพิ่มขึ้น เฉลี่ยร้อยละ ๙๒</div> <div>☞ คะแนนเฉลี่ยก่อนเรียน = ๖.๙๓ และคะแนนเฉลี่ยหลังเรียน = ๙.๕๗ (คะแนนเต็ม ๑๐)</div> <div>☞ ภาพรวมความพึงพอใจของการฝึกอบรม ร้อยละ ๘๙.๕๗</div>

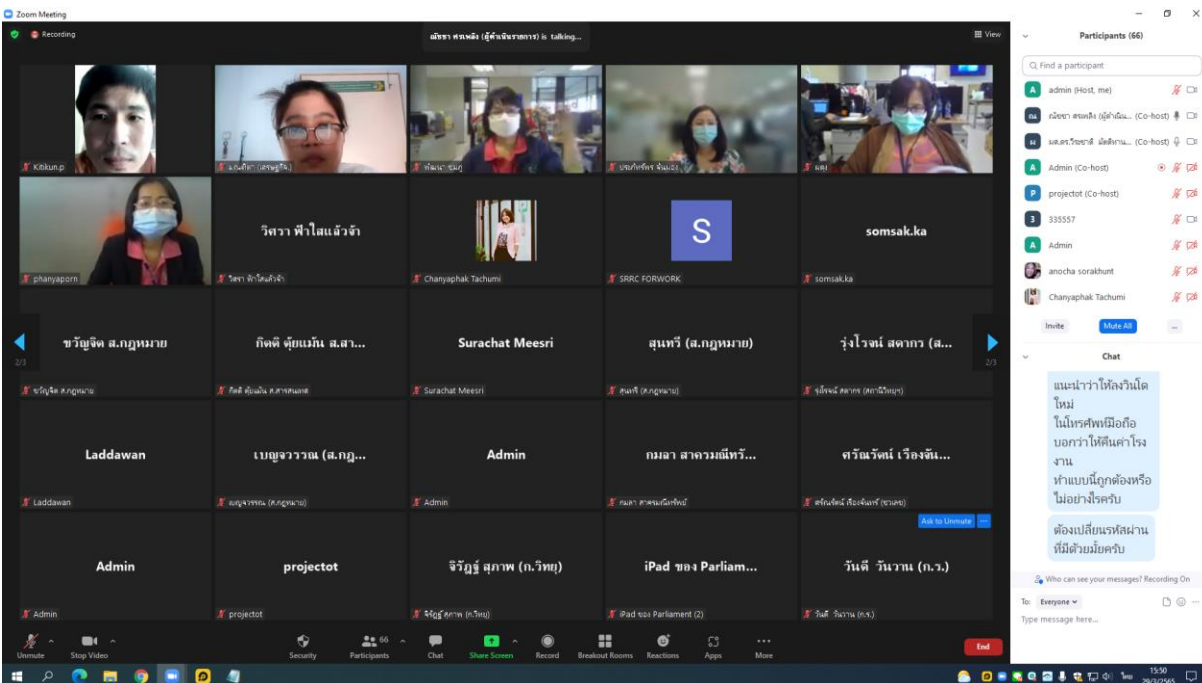
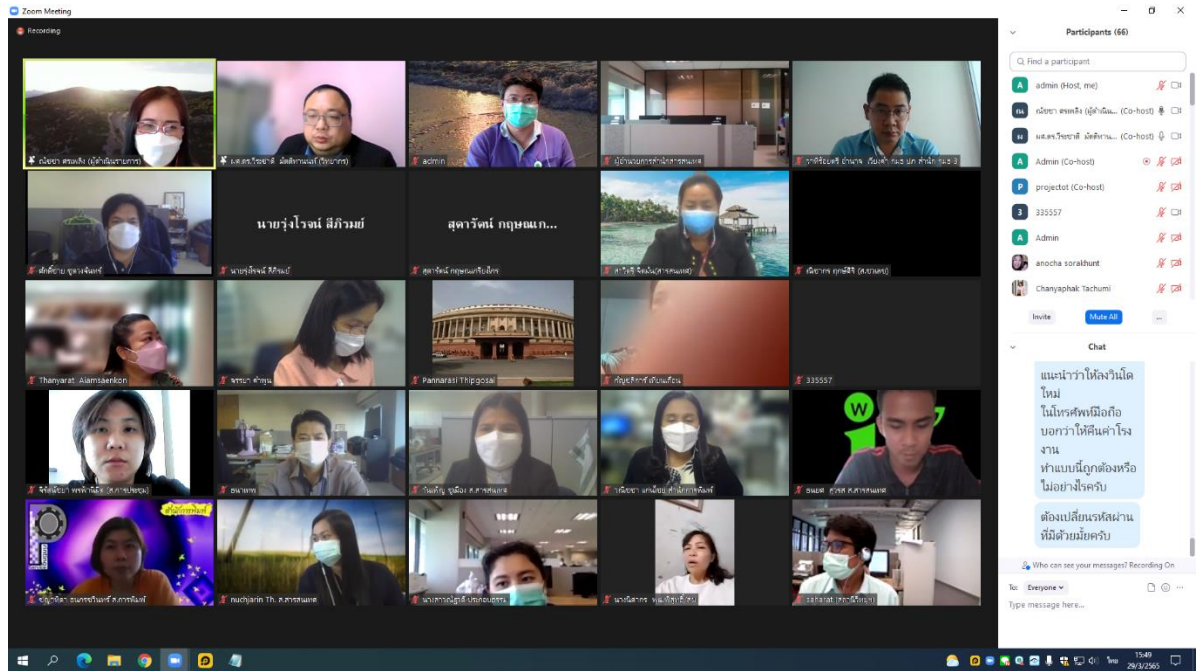
รายชื่อผู้เข้าร่วมการฝึกอบรมตามโครงการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรของ
สำนักงานเลขาธิการสภาผู้แทนราษฎร ประจำปีงบประมาณ ๒๕๖๕
กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๙.๐๐-๑๖.๐๐ นาฬิกา
ณ ห้องฝึกอบรมคอมพิวเตอร์ ๒ สำนักสารสนเทศ ชั้น ๓
สำนักงานเลขาธิการสภาผู้แทนราษฎร อาคารรัฐสภา ในรูปแบบออนไลน์ (Online)
ภาพแสดงตัวตน ระหว่างเวลา ๙.๐๐-๑๖.๐๐ นาฬิกา

ลำดับ	ชื่อ-สกุล	ตำแหน่ง	ลายเซ็น/ภาพแสดงตัวตน เข้าร่วมกิจกรรม
	ผู้บริหาร		
๑	นางสาวสิตาวีร์ อีร์วิรุฬห์	ผู้อำนวยการสำนักสารสนเทศ	
	วิทยากร		
๒	ผู้ช่วยศาสตราจารย์ ดร. วีระชาติ มัตติทานนท์	รองผู้อำนวยการฝ่ายระบบ เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยี สารสนเทศ มหาวิทยาลัยเทคโนโลยี ราชมงคลตะวันออก	
	เจ้าหน้าที่		
๓	นางนทียา แก้วประทุม	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	
๔	นางณัชชา ศรีเพลิง	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๕	พันจ่าเอกกิตติ ตัญแมน	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๖	นายสุรพงษ์ รัตตมณี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
๗	นายธนวุฒิ จันทิมา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
๘	นายธนยศ สุวรรณ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	

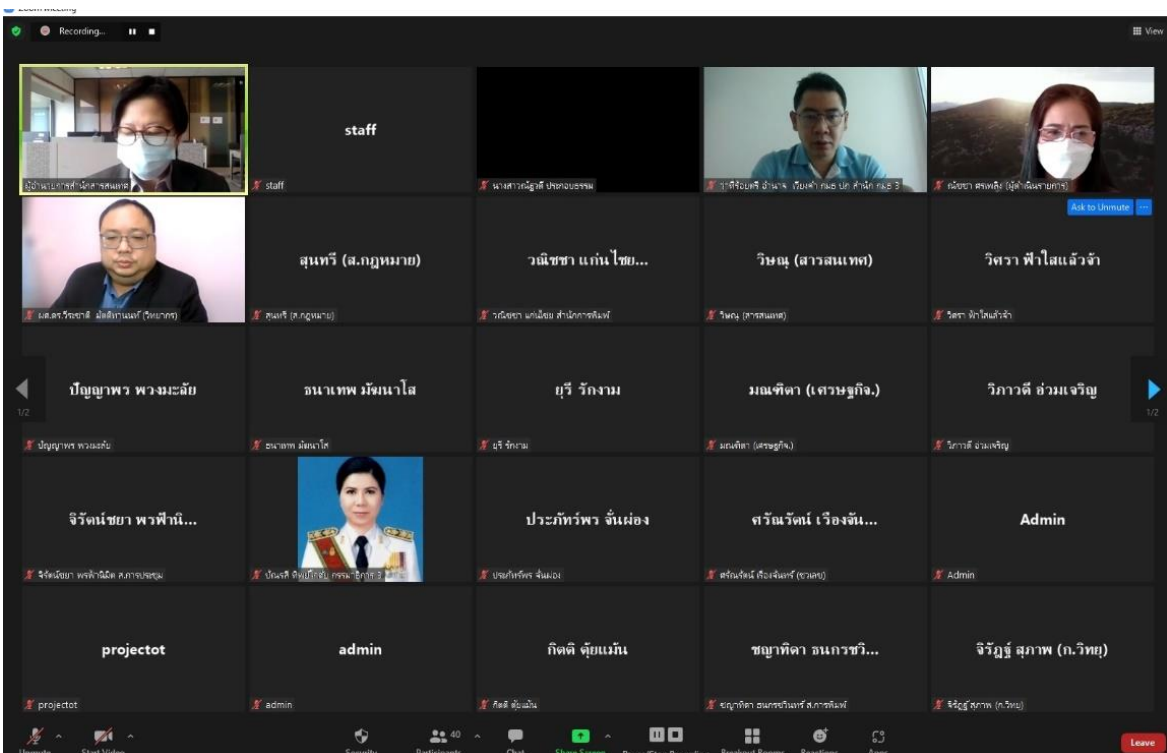
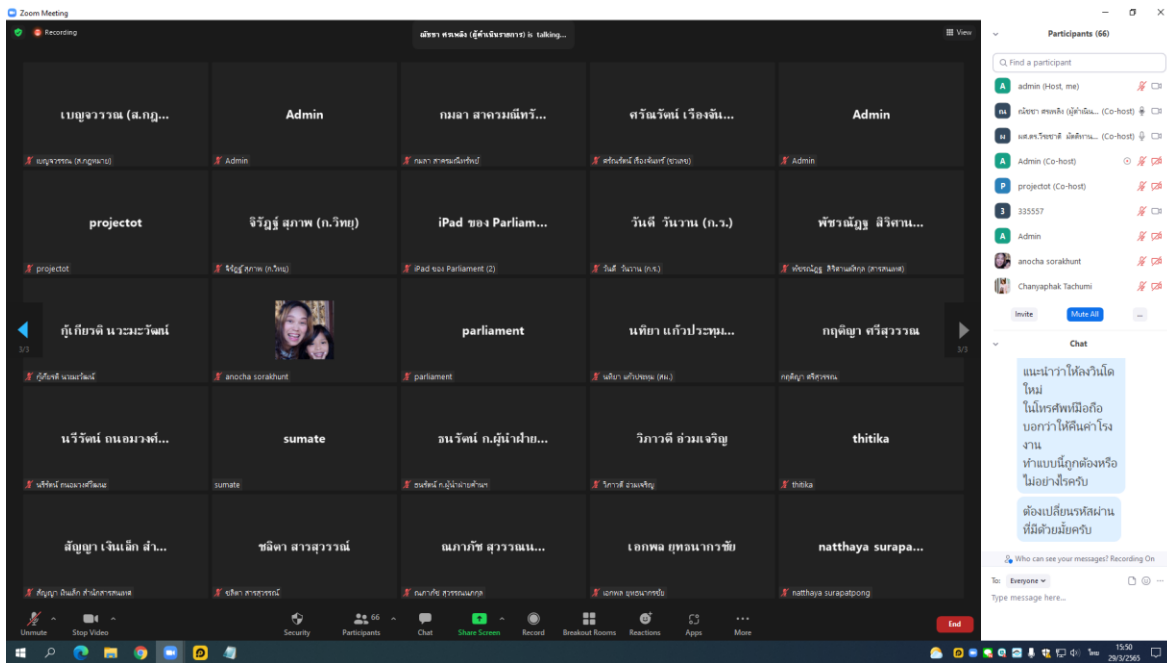
รายชื่อผู้เข้าร่วมการฝึกอบรมตามโครงการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรของ
สำนักงานเลขาธิการสภาผู้แทนราษฎร ประจำปีงบประมาณ ๒๕๖๕
กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๙.๐๐-๑๖.๐๐ นาฬิกา
ณ ห้องฝึกอบรมคอมพิวเตอร์ ๒ สำนักสารสนเทศ ชั้น ๓
สำนักงานเลขาธิการสภาผู้แทนราษฎร อาคารรัฐสภา ในรูปแบบออนไลน์ (Online)
ภาพแสดงตัวตน ระหว่างเวลา ๙.๐๐-๑๖.๐๐ นาฬิกา



รายชื่อผู้เข้าร่วมการฝึกอบรมตามโครงการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรของ
สำนักงานเลขาธิการสภาผู้แทนราษฎร ประจำปีงบประมาณ ๒๕๖๕
กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๙.๐๐-๑๖.๐๐ นาฬิกา
ณ ห้องฝึกอบรมคอมพิวเตอร์ ๒ สำนักงานสารสนเทศ ชั้น ๓
สำนักงานเลขาธิการสภาผู้แทนราษฎร อาคารรัฐสภา ในรูปแบบออนไลน์ (Online)
ภาพแสดงตัวตน ระหว่างเวลา ๙.๐๐-๑๖.๐๐ นาฬิกา



รายชื่อผู้เข้าร่วมการฝึกอบรมตามโครงการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรของ
 สำนักงานเลขาธิการสภาผู้แทนราษฎร ประจำปีงบประมาณ ๒๕๖๕
 กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
 วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๙.๐๐-๑๖.๐๐ นาฬิกา
 ณ ห้องฝึกอบรมคอมพิวเตอร์ ๒ สำนักสารสนเทศ ชั้น ๓
 สำนักงานเลขาธิการสภาผู้แทนราษฎร อาคารรัฐสภา ในรูปแบบออนไลน์ (Online)
 ภาพแสดงตัวตน ระหว่างเวลา ๙.๐๐-๑๖.๐๐ นาฬิกา



Participants (62)

Q Find a participant

S

staff (Co-host, me)

A

admin (Host)

M

ผศ.ดร.วิระชาติ มิตติทานนท์ (วิทยากร) (Co-host)

A

Admin (Co-host)

P

projectot (Co-host)

na

ณัชชา สรพลัง (ผู้ดำเนินรายการ) (Co-host)

ส

สุรพงษ์ สัตตมณี ส.สารสนเทศ (Co-host)

anocha sorakhunt

Chanyaphak(ส.สารสนเทศ)

lei

iPad ของ Parliament (2)

khunchay sapa

Ask to Unmute

More >

K

Kitikun.p

L

Laddawan

N

Nat

nuchjarin Th. ส.สารสนเทศ

P

parliament

Ss

Suthavee ส.สารสนเทศ

n

กฤติญา ศรีสุวรรณ

กัญชศึกษา วัฒนสิทธิ์

n

กิตติ ตัญมณี ส.สารสนเทศ

n

กัญชวลิต นามะวัฒน์

Participants (62)

Q Find a participant

n

กิตติ ตัญมณี ส.สารสนเทศ

n

กัญชวลิต นามะวัฒน์

จ

จรรยา คำขุน

จ

จิรัฐ ศุภาพ (ก.วิทย์)

จ

จิรัตน์ยา พงษ์วัฒน์ ส.การประชุม

ช

ชญาติลา ธนกรชินทร์ ส.การพิมพ์

na

ณัชชา สรพลัง (ส.ชาวเลข)

S

ณิศา สกานี

เ

เอนดZak

ธมด สุวธ สำนักระสนเทศ

ส

ธนาพร มั่นนาโถ

Ask to Unmute

More >

S

ธนาพร จันทิมา ส.สารสนเทศ

อ

ธีราพร สดส่องกฤษ

น

นภียา แก้วบุญม (สผ.)

น

นางสาวณัฐวิทย์ ปะกอบอรุณ

ร

ธัญจวรรณ (ส.กฎหมาย)

ป

ปชภัทร พันธ์มิ่ง

ป

ปัทมพร พรมชัย ส.สารสนเทศ

ปณธิ์ ภัทย์โกศล กรมการ 3

ม

ผู้ช่วยการสำนักสารสนเทศ

พ

พัชรณัฐ สิริวัฒนศิริกุล (สารสนเทศ)

Participants (62)

Q Find a participant

นพพร วัฒนสิทธิ์ กรมการ 3

ม

ผู้ช่วยการสำนักสารสนเทศ

พ

พัชรณัฐ สิริวัฒนศิริกุล (สารสนเทศ)

พ

พณณา ชมภู

ม

มนทิลา (ส.ชชช.)

บ

บุษกรณ สอนสุด สำนักการประชุม

บ

บุษ จันทาม ส.สารสนเทศ

จ

จุฬิรณ สดาก

จ

จุฬิรณ สดาก (สถานีวิทยุ)

ว

วณิชา วัฒนชัย สำนักการพิมพ์

ว

วันดี วันวาน (ก.ร.)

ว

วันเพ็ญ ชูเมือง สำนักสารสนเทศ

Ask to Unmute

More >

ว

วาทิรณศิริ อำนวย เนื่องคำ กมธ ปก สำนัก กมธ 3

ว

วิภาวดี อำนวยเจริญ ส.สารสนเทศ

ว

วิธรา พิลาโณลวิจา

ส

สรณรัตน์ เรืองจันทร์ (ชาวเลข)

ส

ศิริพร พรหมวาส

ส

สุธาธณ กฤษณกรนิยกร

ส

สุนารี (ส.กฎหมาย)

เ

เอกสรณ์

เ

เอวณีย์ สุทธิ ส.สารสนเทศ

เ

เอกพล ยุทธนากรชัย

Participants (62)

Q Find a participant

พ

พณณา ชมภู

ม

มนทิลา (ส.ชชช.)

บ

บุษกรณ สอนสุด สำนักการประชุม

บ

บุษ จันทาม ส.สารสนเทศ

จ

จุฬิรณ สดาก

จ

จุฬิรณ สดาก (สถานีวิทยุ)

ว

วณิชา วัฒนชัย สำนักการพิมพ์

ว

วันดี วันวาน (ก.ร.)

ว

วันเพ็ญ ชูเมือง สำนักสารสนเทศ

ว

วาทิรณศิริ อำนวย เนื่องคำ กมธ ปก สำนัก กมธ 3

ว

วิภาวดี อำนวยเจริญ ส.สารสนเทศ

ว

วิธรา พิลาโณลวิจา

ส

สรณรัตน์ เรืองจันทร์ (ชาวเลข)

ส

ศิริพร พรหมวาส

ส

สุธาธณ กฤษณกรนิยกร

ส

สุนารี (ส.กฎหมาย)

เ

เอกสรณ์

เ

เอวณีย์ สุทธิ ส.สารสนเทศ

เ

เอกพล ยุทธนากรชัย

S

saharat

เ

เอวณีย์ พิลาโณลวิจา

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ.๒๕๖๐

ผู้ช่วยศาสตราจารย์ ดร. วีระชาติ มัตติทานนท์

รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

เอกสารที่อ้างอิง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

<https://cutt.ly/7Q8DmsP>



<https://cutt.ly/MQ8DIjn>



พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

ประกาศใช้เมื่อวันที่ ๑๘ มิถุนายน ๒๕๕๐

เริ่มบังคับใช้ วันที่ ๑๘ กรกฎาคม ๒๕๕๐

มี ๒ หมวด ๓๐ มาตรา

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ (มาตรา ๕ - ๑๗)

หมวด ๒ เกี่ยวกับให้อำนาจ พนักงานเจ้าหน้าที่ (มาตรา ๑๘- ๓๐)

เหตุผลในการประกาศใช้ฯ สรุปได้ว่า ระบบคอมพิวเตอร์เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำทำให้ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ฯ ก่อให้เกิดความเสียหาย กระทบกระทบต่อเนื่องเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดดังกล่าว

ประกาศใช้เมื่อวันที่ ๒๔ มกราคม ๒๕๖๐

เริ่มบังคับใช้ วันที่ ๒๓ พฤษภาคม ๒๕๕๐ (๑๒๐ วัน)

มี ๒๑ มาตรา เป็นการแก้ไขข้อความใน พรบ. ของฉบับ พ.ศ. ๒๕๕๐

เหตุผลฯ พรบ.พ.ศ.๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามฯ มีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้น

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดย มิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

มาตรา ๘ ผู้ใดกระทำความผิดใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

มาตรา ๑๐ ผู้ใดกระทำความผิดใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

“ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ และลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย”

(พรบ.ฯ ๒๕๖๐ เพิ่ม วรรคสองและสาม เรื่อง ก่อให้เกิดความรำคาญ (SPAM) โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกฯ และ รว.กำหนดลักษณะและวิธีการส่ง ปริมาณ...)

ไม่ได้นำข้อความที่ระบุเกี่ยวกับโทษมาแสดง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

— (๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้น
จะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่

— (๒) เป็นการกระทำความผิดโดยประการที่น่าจะเกิดความเสียหายต่อ
ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการรักษาความ
มั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง
ในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการ
กระทำความผิดต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์
สาธารณะ

— ถ้าการกระทำความผิดตามมาตรา (๒) เป็นเหตุให้ผู้ถึงแก่ความตาย
ต้องระวางโทษ...

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็น
การกระทำความผิดต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของ
ประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐาน
อันเป็นประโยชน์สาธารณะ

ถ้าการกระทำฯ ตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบ
คอมพิวเตอร์

ถ้าการกระทำฯ ตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำความผิดต่อข้อมูลคอมพิวเตอร์หรือ
ระบบคอมพิวเตอร์

ถ้าการกระทำฯ ตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่
ความตาย ฯ

มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตรายแก่
บุคคลอื่นหรือทรัพย์สินของผู้อื่นฯ

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคล
อื่นถึงแก่ความตาย

ไม่ได้นำข้อความที่ระบุเกี่ยวกับโทษมาแสดง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้น โดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด ตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือ มาตรา ๑๑ ฯ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้น โดยเฉพาะเพื่อนำไปใช้เป็น เครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสามฯ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้น โดยเฉพาะเพื่อนำไปใช้เป็น เครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ฯ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับ ผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจ เห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้น โดยเฉพาะเพื่อนำไปใช้เป็น เครื่องมือในการกระทำความผิดตามมาตรา ๑๒ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่ง ดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ฯ ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุด แต่กระทางเดียว

(พรบ.ฯ ๒๕๖๐ เพิ่ม วรรคสอง วรรคสาม วรรคสี่ และวรรคห้า)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

~~มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้~~

- ~~———— (๑) นำเข้าสู่ระบบฯ ซึ่งข้อมูลฯ ~~ปลอม~~ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลฯ อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน~~
- ~~———— (๒) นำเข้าสู่ระบบฯ ซึ่งข้อมูลฯ ~~อันเป็นเท็จ~~ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน~~
- ~~———— (๓) นำเข้าสู่ระบบฯ ซึ่งข้อมูลฯ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา~~
- ~~———— (๔) นำเข้าสู่ระบบฯ ซึ่งข้อมูลฯ ที่มีลักษณะอัน ~~ลามก~~และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้~~
- ~~———— (๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลฯ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)~~

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้

- (๑) โดยทุจริต หรือโดยหลอกลวง ๑ บิดเบือนหรือปลอม ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน ~~อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา~~
 - (๒) นำเข้าข้อมูลฯ เท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
 - (๓) นำเข้าฯ เกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
 - (๔) นำเข้าฯ ลามก ๑
 - (๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลฯ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)
- ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

~~มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔~~

มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

-มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

—ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าสู่ข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

—ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

—ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือ บุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณา หรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษถึงหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี

(พรบ.ฯ ๒๕๖๐ เพิ่ม มาตรา ๑๖/๑ และ ๑๖/๒)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้ นอก
ราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศ
ที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทย
หรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ
จะต้องรับโทษภายในราชอาณาจักร

มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง
มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่
รัฐมนตรีแต่งตั้ง มีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคน
หนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงิน
ค่าปรับ ตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่า
คดีนั้นเป็นอันเลิกกัน ตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความ
ในการฟ้องคดีใหม่ นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว

(พรบ.ฯ ๒๕๖๐ เพิ่ม มาตรา ๑๗/๑ และ ๑๖/๒)



ดูแลความเป็นส่วนตัว (Privacy)
ให้ปฏิเสธไม่รับ Spam ข่ายขึ้น
พร้อมให้เกณฑ์ที่ชัดเจนว่า **แค่ไหน...เพียงใด**
จึงไม่เป็น Spam

(มาตรา 11)



ปรับปรุงความผิดฐานเผยแพร่ข้อมูล
แต่ไม่ใช้กับหมิ่นประมาท
เอาผิดกับการฉ้อโกง ปลอม
หรือข้อมูล อันเป็นเท็จ

(มาตรา 14(1))

ดูแล **CRITICAL
INFRASTRUCTURE**



หรือโครงสร้างพื้นฐานสำคัญของประเทศ
ส่งผลกระทบต่อประชาชนในวงกว้าง
เช่น ระบบการเงิน การธนาคาร ระบบพลังงาน ไฟฟ้า ประปา
ระบบสาธารณสุข เป็นต้น

(มาตรา 12) **CRITICAL
INFRASTRUCTURE**

ยกเว้นความรับผิดผู้ให้บริการ

เมื่อทำตามขั้นตอนตามกฎหมายจะรับผิดชอบ
เฉพาะยินยอมหรือรู้เห็นเป็นใจเท่านั้น
กำหนดขั้นตอนการแจ้งเตือน
การนำข้อมูลออกจากระบบคอมพิวเตอร์
เพื่อให้มีความชัดเจน เป็นไปในแนวทางที่ยอมรับได้
มีความโปร่งใส ตรวจสอบการดำเนินการได้



(มาตรา 15)

ดูแลความเสียหาย ต่อตัวบุคคล



ที่รวมถึงการติดต่อภาพของผู้ตาย
และกำหนดช้อยกเว้นในการติชม ด้วยความเป็นธรรม
(มาตรา 16)

เพิ่มมาตรการบรรเทา
ความเสียหายสำหรับ **เนื้อหา (CONTENT)**
ที่ศาลพิพากษาว่าผิด



โดยศาลอาจสั่งให้ทำลาย / โฆษณาหรือเผยแพร่คำพิพากษา /
หรือใช้มาตรการอื่นๆ) และสั่งให้ผู้ครอบครองข้อมูลทำลายข้อมูลนั้น
ตามหลักสิทธิที่จะถูกลืม (**RIGHT TO BE FORGOTTEN**)

(มาตรา 16/1, 16/2)

เพิ่มมาตรการเปรียบเทียบ ในความผิดที่มีโทษสถานเบา
ลดภาระประชาชนดำเนินคดีชั้นศาล

เพื่อไม่ให้ติดอยู่ในกระบวนการยุติธรรมที่ต้องใช้เวลา และมีค่าใช้จ่าย
(มาตรา 17/1)





จะอย่างไร

ให้พนักงานเจ้าหน้าที่ซึ่งเชี่ยวชาญ

ช่วยเหลือทางเทคนิค

แก่พนักงานเจ้าหน้าที่ตามกฎหมายอื่น

**เพื่อบรรเทาความเสียหาย
ให้กับประชาชนเร็วที่สุด**

(มาตรา 18, 19)

เทคโนโลยีที่เปลี่ยนแปลง
รูปแบบการกระทำความผิดที่ซับซ้อนมากขึ้น



จึงอาจจำเป็นต้อง**ขยายเวลา
เก็บข้อมูลจราจร** ทางคอมพิวเตอร์

ที่ใช้เป็นพยานหลักฐาน ไม่น้อยกว่า 90 วัน หากจำเป็นอาจขยายเป็น 2 ปี
(มาตรา 26)



**ทำอะไรให้มี
พนักงานเจ้าหน้าที่
ที่เชี่ยวชาญ**

จึงต้องให้ค่าตอบแทน
ที่พอจะสู้ได้ในราคาตลาด

(มาตรา 28)

กรณีศึกษา: การทำผิดตาม พ.ร.บ. คอมพิวเตอร์

หลังจากมีการประกาศใช้ พ.ร.บ.
คอมพิวเตอร์ ฉบับที่ 2 ก็มีกรณีที่เข้าข่าย
กระทำความผิดพ.ร.บ.ออกมาให้เห็นกันบ้าง
เพื่อสร้างความเข้าใจมากขึ้น เราเลยขอ
ยกตัวอย่างกรณี ที่อาจผิดตาม พ.ร.บ.
คอมพิวเตอร์

ณ สถานพินิจฯ ตรง โครงการสร้างตึก เหมตรงข้ามตึกมหาทุน นกสวจะหก
(ตึกNobleติดๆกันด้วย) #js100radio ช่วยประสานต่อที่



กรณีศึกษาที่

มีข่าวอย่าง โด่งดังในโลกอินเทอร์เน็ต

เป็นกรณีที่มีชายหนุ่มคนหนึ่งถ่ายรูปตึกที่มีลักษณะเอนๆ พร้อมโพสต์ข้อความประมาณว่า ตึกทรุดตัว ลงบนเฟสบุ๊ก เลยทำให้เกิดเป็นประเด็นที่หลายเอาตอกกตใจ ไปกันใหญ่ แต่ต่อมาก็มีการเปิดเผยว่า ตึกที่เห็นนั้นเป็นเพียงคีย์ไชน์ของตึกที่ตั้งใจจะให้เอนแบบนั้นอยู่แล้ว เลยทำให้เจ้าของโพสต์ถูกตำรวจเรียกสอบสวน เพราะเข้าข่ายความผิดพ.ร.บ.คอมพิวเตอร์ ม.14 (2) นำข้อความเท็จเข้าระบบคอมพิวเตอร์ อันเป็นเท็จก่อให้เกิดความตื่นตระหนก



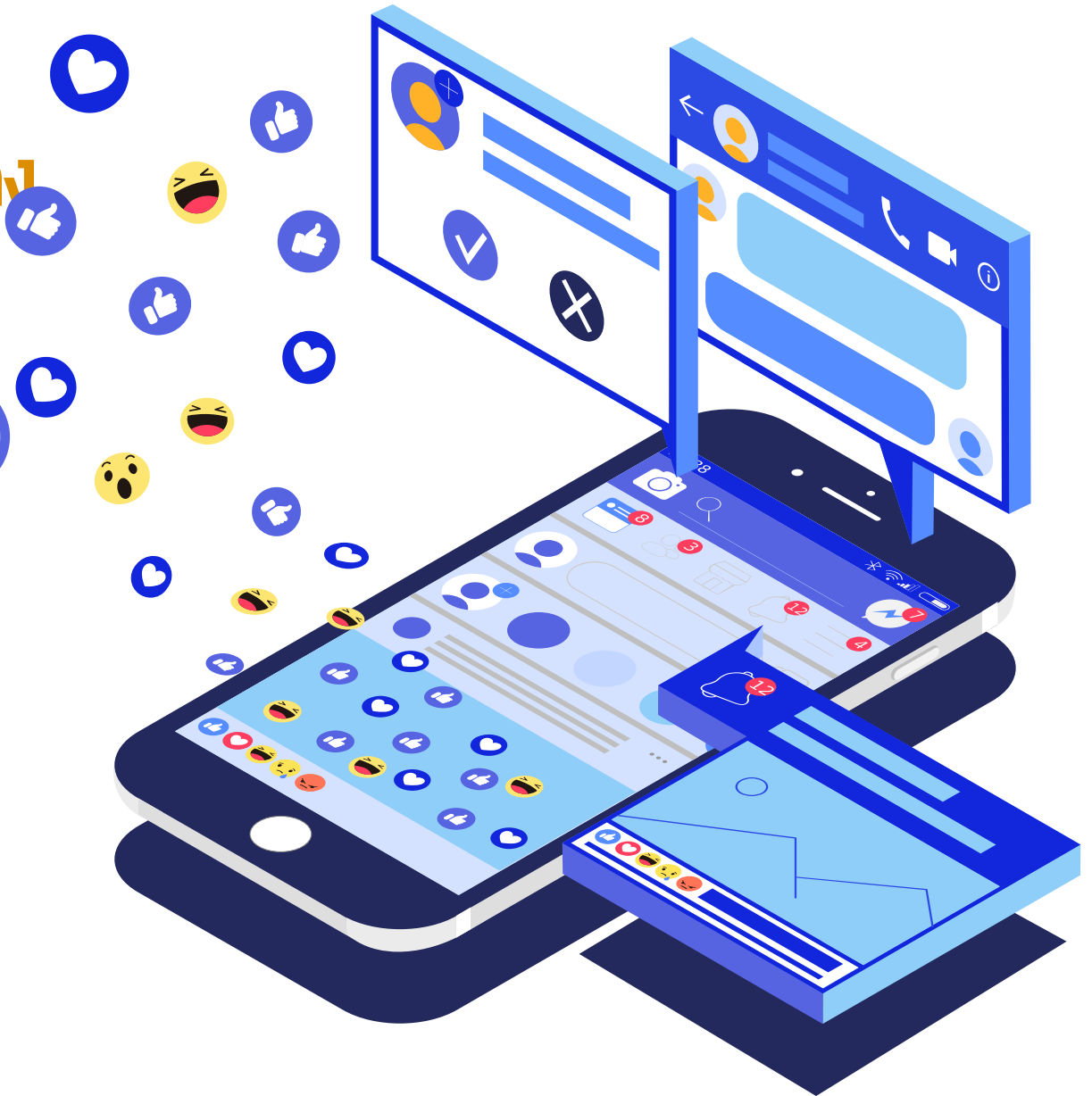
สิ่งที่ผู้ใช้คอมพิวเตอร์ และอินเทอร์เน็ตไม่พึงกระทำ

- พยายามเข้าใช้งานระบบ/ข้อมูลคอมพิวเตอร์ รวมถึงการลบ แก้ไข เปลี่ยนแปลง และทำลายข้อมูลของผู้อื่น
- ดาวน์โหลดและติดตั้งโปรแกรมที่ไม่รู้จักหรือไม่มีสิทธิ (ละเมิดลิขสิทธิ์) รวมถึงการเผยแพร่โปรแกรมดังกล่าว
- ให้ผู้อื่นใช้บัญชีผู้ใช้งานของตนเอง รวมถึงการตั้งรหัสผ่านให้ง่ายต่อการคาดเดา
- นำเข้า สร้าง แชร์ ส่งต่อข้อมูลที่เป็นข้อมูลเท็จ บิดเบือน ลามก
- นำเครื่องคอมพิวเตอร์ของหน่วยงานไปใช้งานอื่นๆ (นอกเหนือภารกิจหน้าที่)
- นำเครื่องคอมพิวเตอร์ภายนอกที่ยังไม่ผ่านการตรวจสอบความปลอดภัยมาใช้งานภายในหน่วยงาน

การปฏิบัติและการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ไม่เข้าระบบคอมพิวเตอร์ หรือดู/เปิดข้อมูลคอมพิวเตอร์ที่ตนไม่มีสิทธิหรือหน้าที่
- ไม่เปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์
- ไม่ดักจับ/ดักเก็บข้อมูลที่มีการส่งในระบบคอมพิวเตอร์
- ไม่ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ข้อมูลคอมพิวเตอร์ของผู้อื่น (โดยมิชอบ)
- ไม่กระทำการใดๆ ที่ส่งผลให้ถูกระงับ ชะลด ชัดขวาง หรือรบกวนการทำงานปกติฯ ของผู้อื่น
- ไม่ส่งข้อมูลหรืออีเมลที่ปลอมแปลงแหล่งที่มา รวมถึงการส่ง **SPAM**
- ไม่จำหน่ายหรือเผยแพร่ชุดคำสั่ง ที่อาจถูกนำไปกระทำความผิด
- ไม่นำเข้า เผยแพร่ หรือส่งต่อ ข้อมูลเท็จ ปลอม ลามก หลอกลวง บิดเบือน (ตรวจสอบข้อเท็จจริงและแหล่งข้อมูล)
- ระมัดระวัง การติดต่อ ดัดแปลง ภาพของผู้อื่น โดยเฉพาะผู้เสียชีวิต
- ไม่ยินยอมให้ผู้ใดผู้หนึ่งกระทำ หรือให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจ ในการกระทำความผิดฯ ตามข้างต้น

ความตระหนักรู้ในการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศ
(Information Security Awareness)



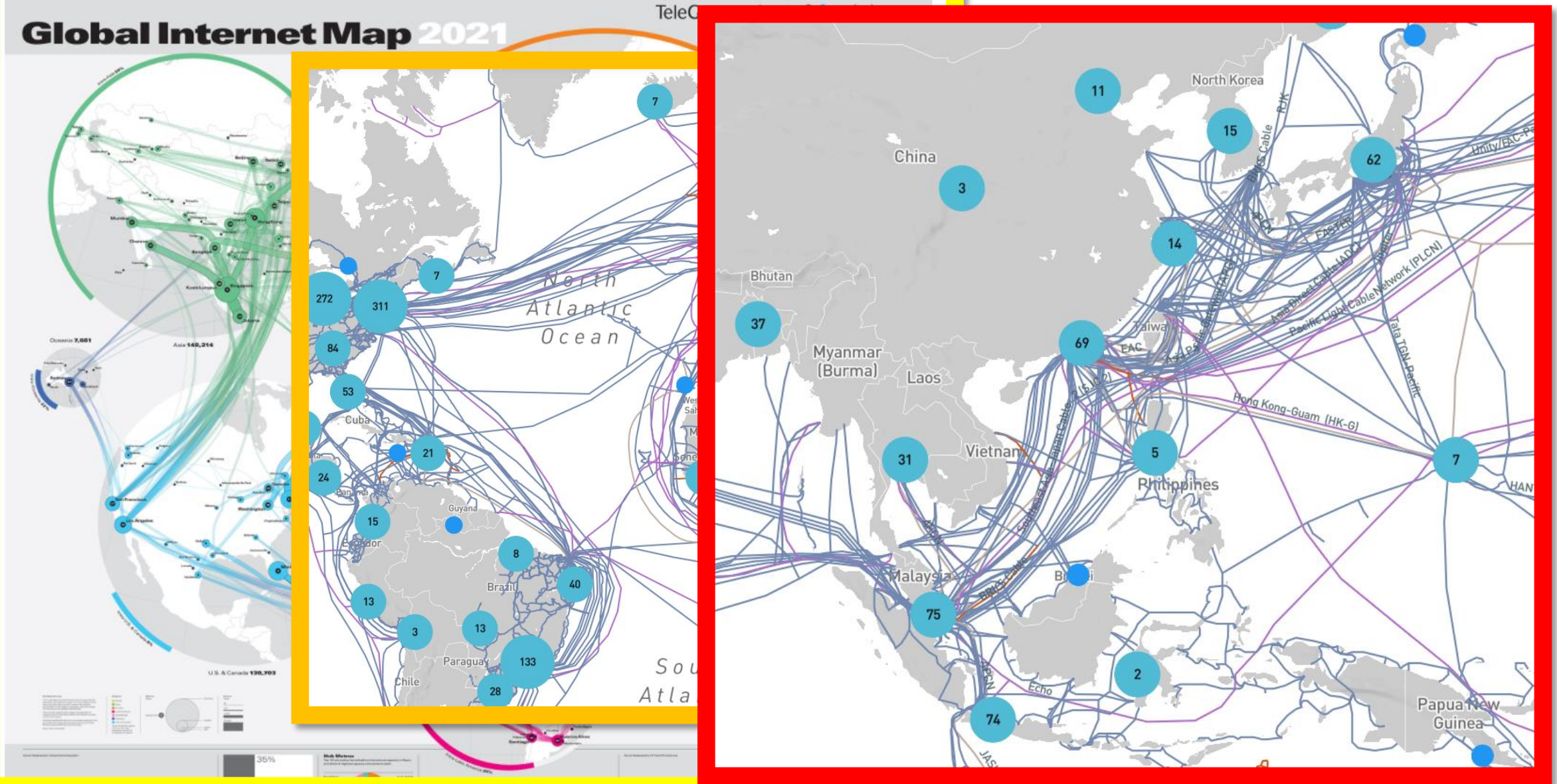
ความรู้ ความเข้าใจในเรื่องระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบอินเทอร์เน็ต



ความรู้ ความเข้าใจในเรื่องระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบอินเทอร์เน็ต











ความรู้ ความเข้าใจในเรื่องระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบอินเทอร์เน็ต



ความรู้ ความเข้าใจในเรื่องระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบอินเทอร์เน็ต

Top Security and Risk Trends for 2021

01 Cybersecurity mesh		02 Cyber-savvy boards	
03 Vendor consolidation		04 Identity-first security	
05 Managing machine identities becoming a critical security capability			
06 “Remote work” now just “work”		07 Breach and attack simulation	
08 Privacy-enhancing computation techniques			

gartner.com

© 2021 Gartner, Inc. All rights reserved. CTMKT_1187855

Gartner

5 ภัยคุกคาม

- Hacking the home
- Beware of the ‘wares’
- Cloud-based threats
- QR code abuse
- ฟิชซิง (Phishing)

ที่มา: [entrepreneur.com](https://www.entrepreneur.com)

อยู่บนโลกออนไลน์ คนไทย ไม่แพ้ชาวโลก

ไทย

โลก

Internet User	69.5%	59.5%
ใช้อินเทอร์เน็ต	8.44 ชั่วโมง/วัน	6.54 ชั่วโมง/วัน
ใช้อินเทอร์เน็ตบนมือถือ	5.07 ชั่วโมง/วัน	3.39 ชั่วโมง/วัน
ใช้อินเทอร์เน็ตบนคอมพิวเตอร์	3.38 ชั่วโมง/วัน	3.16 ชั่วโมง/วัน
เล่นเกม	96.6%	86.9%
ใช้เวลาเล่นเกม Console	1.38 ชั่วโมง/วัน	1.12 ชั่วโมง/วัน
ซื้อของออนไลน์	83.6%	76.8%
ซื้อของออนไลน์ผ่านมือถือ	74.2%	55.4%
ใช้โซเชียลมีเดีย	78.7%	53.6%
ใช้เวลากับโซเชียลมีเดีย	2.48 ชั่วโมง/วัน	2.25 ชั่วโมง/วัน
ใช้โซเชียลมีเดียหาข้อมูล แบรนด์ที่สนใจ	55.5%	44.8%
ใช้โซเชียลมีเดียทำงาน	47.0%	40.4%
มีปัญหาโซเชียลมีเดีย	10 บัญชี	8.4 บัญชี
เข้าเว็บไซต์ผ่านมือถือ (ด้วย Web Browsers)	60.2%	55.7%
ใช้บริการฟูลเดลิเวอรี่	61.0%	55.5%
ดู TV Streaming	60.8%	70.0%
บล็อกโฆษณา	40.0%	42.7%
ความเร็วของอินเทอร์เน็ตมือถือ	51.75 Mbps	42.70 Mbps
ความเร็วของอินเทอร์เน็ตบ้าน	308.35 Mbps	96.43 Mbps

คัดลอกส่วนจาก Internet user อายุ 16-64 ปี

ที่มา : We Are Social, มกราคม 2564

ยกเว้น Internet User, ความเร็วของอินเทอร์เน็ตมือถือ/บ้าน, ใช้สัดส่วนผู้ใช้งานโซเชียลมีเดีย

ที่มา : <https://marketeeronline.co/archives/208372>

JAN
2021

THAILAND

ESSENTIAL HEADLINES FOR MOBILE, INTERNET, AND SOCIAL MEDIA USE

⚠ CHANGES TO DATA SOURCES FOR INTERNET USERS AND SOCIAL MEDIA USERS MEAN THAT VALUES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS



TOTAL
POPULATION



69.88
MILLION

URBANISATION:

51.8%

MOBILE
CONNECTIONS



90.66
MILLION

vs. POPULATION:

129.7%

INTERNET
USERS



48.59
MILLION

vs. POPULATION:

69.5%

ACTIVE SOCIAL
MEDIA USERS



55.00
MILLION

vs. POPULATION:

78.7%

we
are
social



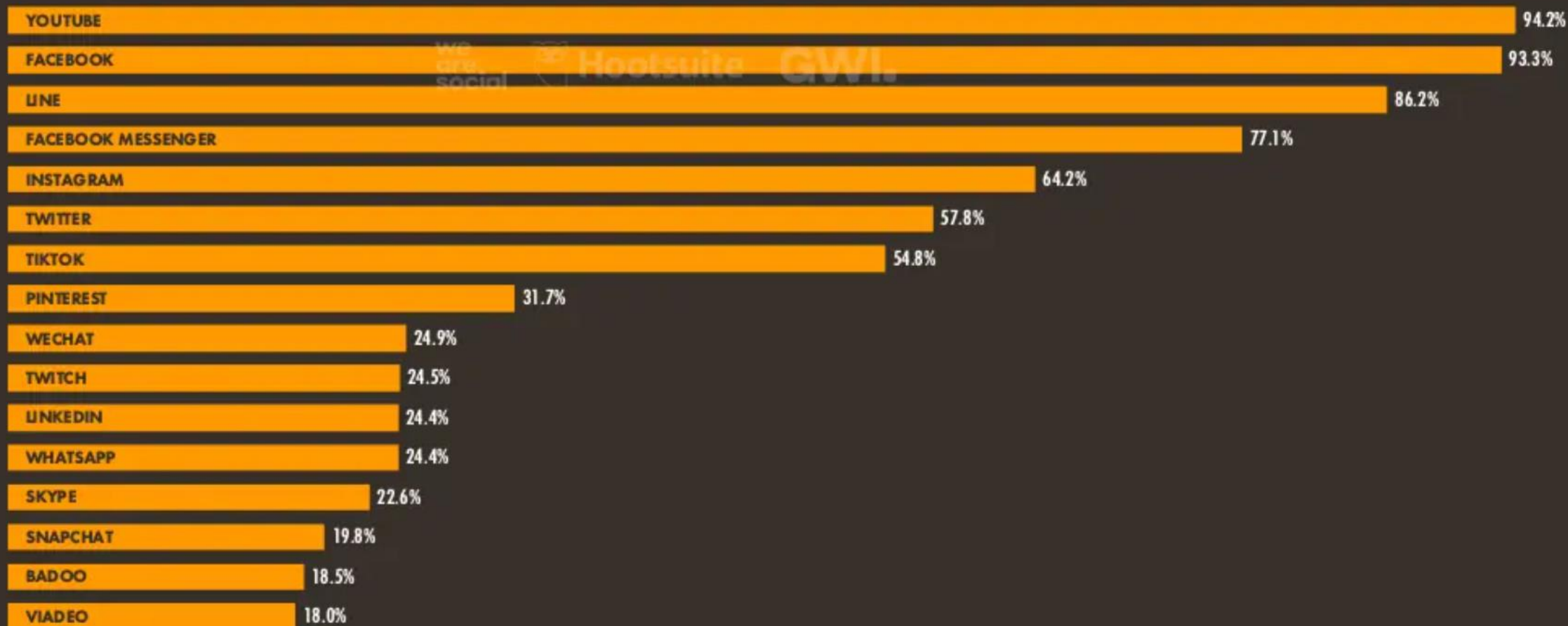
JAN
2021

MOST-USED SOCIAL MEDIA PLATFORMS

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 THAT HAS USED EACH PLATFORM IN THE PAST MONTH



THAILAND



JAN
2021

GOOGLE SEARCH: TOP QUERIES IN 2020

THE MOST COMMON QUERIES THAT PEOPLE ENTERED INTO GOOGLE SEARCH BETWEEN 01 JANUARY AND 31 DECEMBER 2020



THAILAND

#	SEARCH QUERY	INDEX
01	หนัง	100
02	แปล	81
03	ห่วย	67
04	ผลบอล	65
05	ไม่ทิ้งกัน	49
06	เราไม่ทิ้งกัน	48
07	เพลง	41
08	แปลภาษา	41
09	www	38
10	บอลสด	35

#	SEARCH QUERY	INDEX
11	ตรวจหวย	32
12	ภาษาอังกฤษ	32
13	FACEBOOK	30
14	ผลบอลสด	28
15	บ้านบอล	28
16	YOUTUBE	25
17	www เราไม่ทิ้งกัน	25
18	บ้านผลบอล	24
19	ดูหนัง	23
20	GOOGLE	22

35

SOURCE: GOOGLE TRENDS (ACCESSED JAN 2021). **NOTE:** GOOGLE DOES NOT PUBLISH SEARCH VOLUMES, BUT THE "INDEX" COLUMN SHOWS RELATIVE VOLUMES FOR EACH QUERY COMPARED TO SEARCH VOLUMES FOR THE TOP QUERY (AN INDEX OF 50 MEANS THAT THE QUERY RECEIVED 50% OF THE SEARCH VOLUME OF THE TOP QUERY).

we
are
social

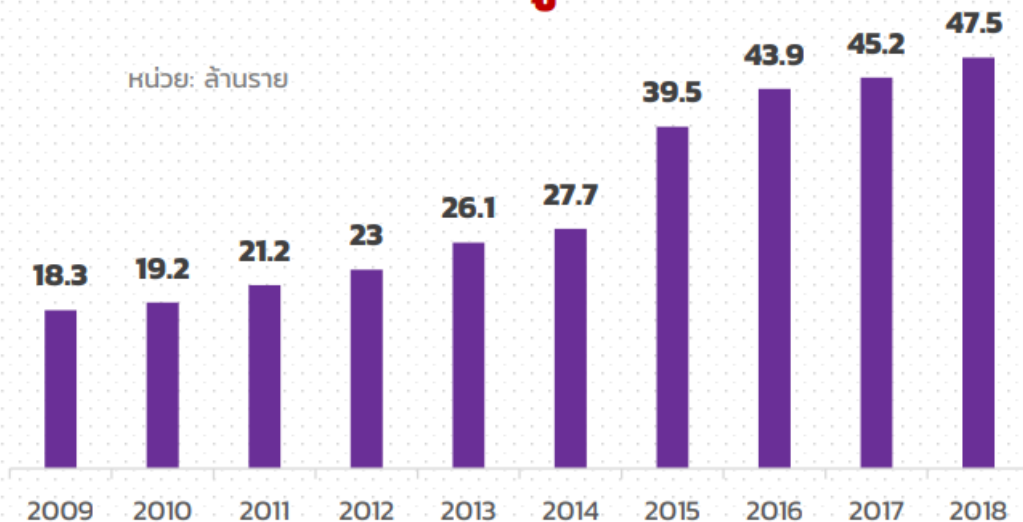


Hootsuite®

อินเทอร์เน็ต กับ Lifestyle ของคนไทยที่เปลี่ยนไป

ประชากรไทย 66.4 ล้านคน
เป็นผู้ใช้อินเทอร์เน็ต 47.5 ล้านราย

คิดเป็นสัดส่วนผู้ใช้อินเทอร์เน็ตกว่า **70%**
9 ปีที่ผ่านมา เติบโตสูงกว่า **150%**



แหล่งที่มา : สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ



" ภาครัฐจะดูแลคนไทยอย่างไร
ให้ใช้อินเทอร์เน็ตอย่าง
สร้างสรรค์ มั่นคง และปลอดภัย "

ETDA ให้ความสำคัญในการเก็บตัวเลข
พฤติกรรมผู้ใช้อินเทอร์เน็ต
ของประเทศไทย
อย่างต่อเนื่องเป็น **ปีที่ 7**



มีค่า

ผลการสำรวจ **พฤติกรรม**
ผู้ใช้อินเทอร์เน็ตในประเทศไทย
ปี 2563

คนไทยใช้อินเทอร์เน็ตเฉลี่ย

11.25 ชม./วัน

วันธรรมดา

มีการใช้อินเทอร์เน็ตเฉลี่ย

11.23 ชม./วัน

วันหยุด

มีการใช้อินเทอร์เน็ตเฉลี่ย

11.29 ชม./วัน

เมื่อเทียบกับสถิติในปี 2562

ยอดการใช้อินเทอร์เน็ตเฉลี่ย

ต่อวัน

เพิ่มขึ้น 1.03 ชม.

ยอดการใช้อินเทอร์เน็ตเฉลี่ย

วันธรรมดา

เพิ่มขึ้น 1.31 ชม.

ยอดการใช้อินเทอร์เน็ตเฉลี่ย

วันหยุด

ลดลง 6 นาที

คนไทยใช้อินเทอร์เน็ตเพิ่มขึ้น 3 เท่าตัว

เมื่อเทียบสถิติปี 2556

ที่คนไทยใช้อินเทอร์เน็ตเฉลี่ยวันละ 4 ชั่วโมง 36 นาที

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

มีค่า



10 กิจกรรม ยอดนิยม บนโลก ออนไลน์

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

95.3%

ใช้งาน
Social Media

85.0%

ดูคลิป / ดูหนัง /
ฟังเพลงออนไลน์

82.2%

ค้นหาข้อมูล

77.8%

การติดต่อสื่อสาร
ออนไลน์

69.0%

การรับ - ส่ง
อีเมล

67.3%

การซื้อสินค้า
ออนไลน์

64.2%

การอ่านข่าว /
บทความ / e-Book

57.5%

การเรียนรู้
ออนไลน์

56.8%

การเล่นเกม
ออนไลน์

56.5%

การทำธุรกรรม
ทางการเงินออนไลน์



Gen ใหม่

ใช้งานอินเทอร์เน็ต

มากที่สุด

Gen Z



อายุน้อยกว่า 20 ปี
ใช้อินเทอร์เน็ตเฉลี่ย

12.08 ชม./วัน

Gen Y



อายุ 20-39 ปี
ใช้อินเทอร์เน็ตเฉลี่ย

12.26 ชม./วัน

Gen X



อายุ 40-55 ปี
ใช้อินเทอร์เน็ตเฉลี่ย

10.20 ชม./วัน

Baby Boomer



อายุ 56-74 ปี
ใช้อินเทอร์เน็ตเฉลี่ย

8.41 ชม./วัน



การรู้เท่าทันสื่อใหม่ (New Media)

- รับข้อมูลผ่านช่องทางที่น่าเชื่อถือ
(Trusted Channel)
- พัฒนาองค์ความรู้
(Upskills)
- เปิดรับข้อมูลหลายช่องทาง
(Multiple Information)



ความหมายข้อเท็จจริง(Fact) และข้อคิดเห็น(Opinion)

“ข้อเท็จจริง”	ข้อความแห่งเหตุการณ์ที่เป็นมาหรือเป็นอยู่ตามจริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง
“ข้อคิดเห็น”	ความเห็น ความรู้สึกนึกคิดของผู้ส่งสารที่สอดแทรกอยู่ในเนื้อหา

อาจกล่าวได้ว่า

ข้อเท็จจริง	นั้นต้องสามารถพิสูจน์สนับสนุนยืนยันได้
ข้อคิดเห็น	นั้นไม่สามารถสนับสนุนยืนยันได้

ลักษณะข้อเท็จจริง(Fact) และข้อคิดเห็น(Opinion)

“ข้อเท็จจริง”

- มีความเป็นไปได้
- มีความสมจริง
- มีหลักฐานเชื่อถือได้
- มีความสมเหตุสมผล

“ข้อคิดเห็น”

- เป็นข้อความที่แสดงความรู้สึก
- เป็นข้อความที่แสดงความคิดเห็น
- เป็นข้อความที่แสดงการเปรียบเทียบ อุปมาอุปมัย
- เป็นข้อความที่เป็นข้อเสนอแนะหรือเป็นความคิดเห็นของผู้พูดเอง

Cyberbullying กลั่นแกล้งกันบนโลกไซเบอร์

การกลั่นแกล้งในโลกไซเบอร์

คือการประทุษร้ายหรือทำให้ผู้อื่นอับอายผ่านทางการใช้สื่ออิเล็กทรอนิกส์ เช่น อีเมล, การส่งข้อความ, บล็อก, เว็บไซต์, ชุมชนออนไลน์, เมสเสจ, และโทรศัพท์ สิ่งที่น่ากลั่นแกล้งในโลกไซเบอร์ตั้งใจคือการแสดงความเป็นศัตรูหรือแสดงออกในแง่ลบต่ออีกฝ่ายนั่นเอง

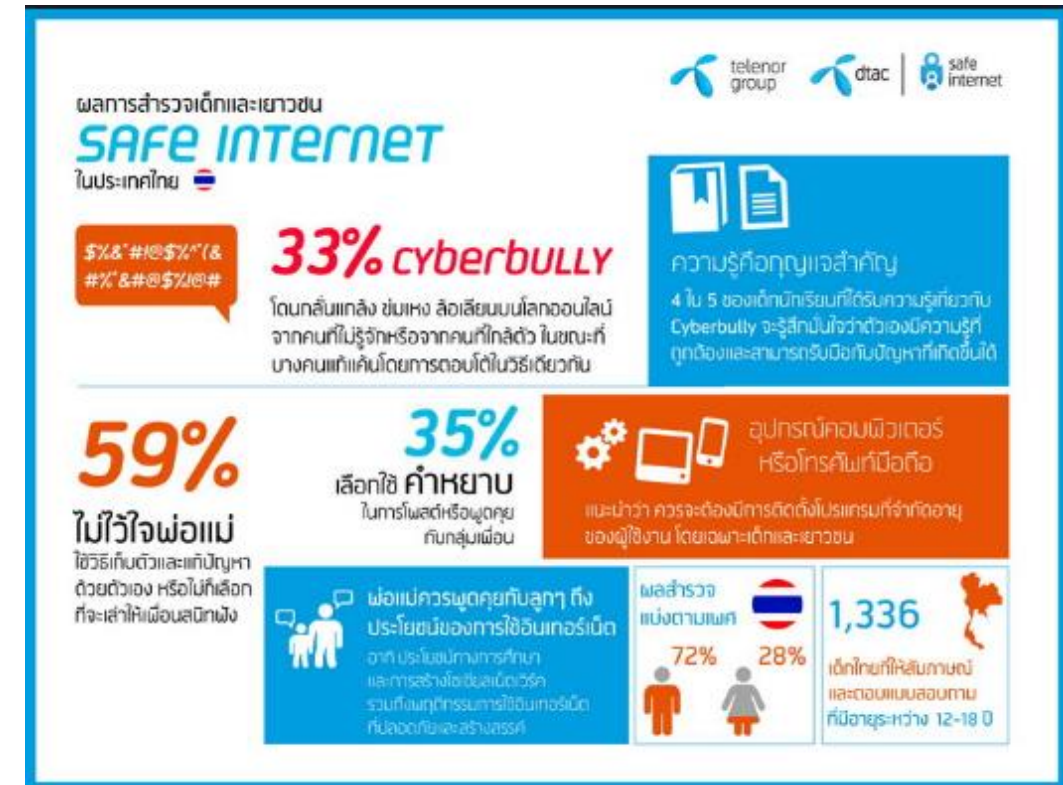


Cyberbullying กลั่นแกล้งกันบนโลกไซเบอร์ (ต่อ)

33% ของเด็กไทยมีประสบการณ์ของการเป็นทั้งผู้ที่ถูกกลั่นแกล้งหรือก่อวบนโลกออนไลน์ จากคนที่ไม่รู้จัก และหรือจากคนที่รู้จักซึ่งเป็นคนเดียวกับที่แกล้งอยู่ในโลกของความเป็นจริง และในขณะเดียวกันเด็กเหล่านี้ก็กลับเป็นผู้กลั่นแกล้งคนอื่นบนโลกออนไลน์โดยปิดบัง ไม่เปิดเผยชื่อจริงในการใช้อินเทอร์เน็ต

35% ของเด็กไทย จะถูกสิ่งเร้าต่างๆ ได้ง่าย โดยเฉพาะกับเว็บไซต์ที่ไม่เหมาะสมต่างๆ อาทิ เกมอันตราย หรือเว็บอนาจาร ที่เต็มไปด้วยคำก้าวร้าวและหยาบคาย ซึ่งจะเข้าไปดูและเกิดพฤติกรรมเลียนแบบ

59% ของเด็กไทย จะรู้สึกว่าตนเองสามารถแก้ปัญหาหรือเผชิญหน้ากับความเลวร้ายบนโลกออนไลน์นี้ได้ด้วยตัวเอง หรือจะปรึกษาเพื่อนเป็นอันดับแรก



ตัวอย่าง Cyber Bullying

Video



จะช่วยลดการเกิด Cyberbullying ได้อย่างไรบ้าง



คิด วิเคราะห์ แยกแยะ

ก่อนโพสต์ภาพ วิดีโอ
และเนื้อหาทุกครั้งว่าส่งผลกระทบต่อคนอื่นหรือไม่ รวมถึงตัวเองด้วย



ไม่แน่ใจอย่าแชร์

งดการโพสต์ และแชร์ในสิ่งที่ไม่รู้ว่า
เป็นความจริงหรือไม่



ใจเขาใจเรา

ก่อนโพสต์หรือแชร์สิ่งใด
ควรคิดถึงใจเขาใจเราบ้าง
ถ้าเป็นเราเอง ก็ไม่อยากโดนแบบนี้เช่นกัน

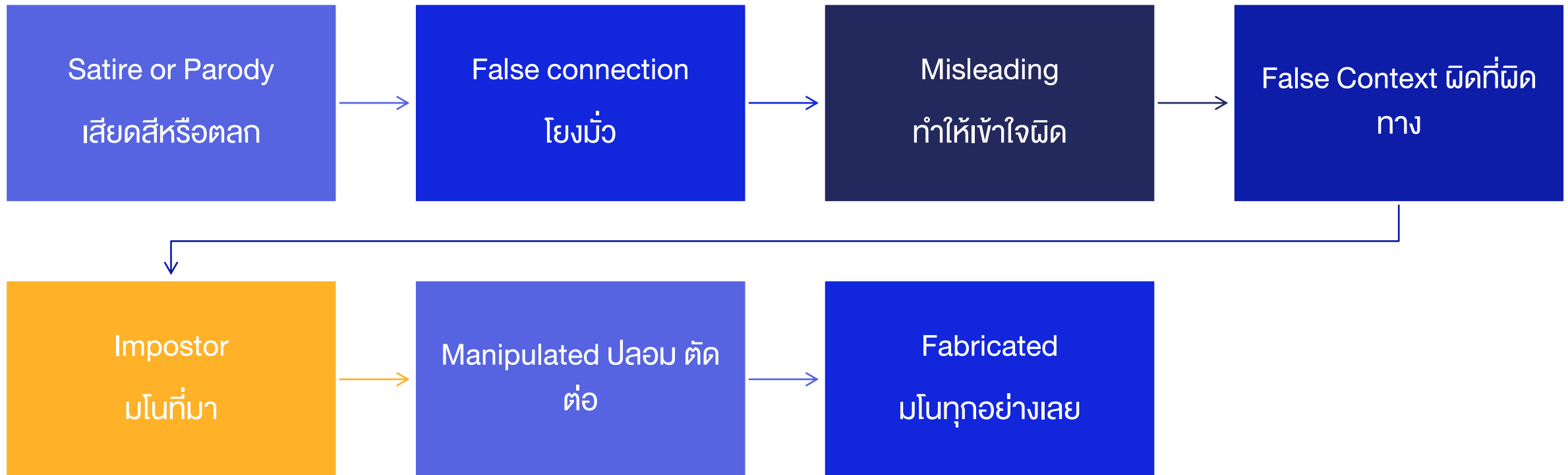
Cyberbullying

ความไม่ตั้งใจ ที่ส่งผลร้ายกว่าที่คิด!

“หยุดโพสต์ หยุดแชร์ คำพูดแย่ๆ บนโลกโซเชียล”

Cyberbullying คือ การกลั่นแกล้งบนโลกออนไลน์ทุกรูปแบบ เช่นการโพสต์ การแสดงความคิดเห็น และแชร์ บนสื่อโซเชียลมีเดียต่างๆ เพื่อเป็นการก่อกวน อาจส่งผลกระทบต่อผู้ที่ถูกกระทำทั้งทางใจ จนอาจร้ายแรงจนถึงส่งผลกระทบทางกายได้

Fake news



เสียสหรือตลก & โยมมัว

เพลงตลก เพลงล้อเลียน พระนพดล, ขวอปด, The Double Standard ต่าง ๆ ที่ทุกคนก็จะรู้ว่าเป็นเพลงที่ทำขึ้นมาเพื่อล้อเลียน ทำให้มีพิษมีภัยน้อยที่สุดเนื่องจากทางผู้จัดทำเองก็ ไม่ได้มีเจตนาในการสร้างความเข้าใจผิดหรือมีวัตถุประสงค์ต้องการให้คนมาเชื่อ



Khaopod-ขาวปด เนื่องจากมีกระแสไม่ใจเป็นอย่างมาก ทางขาวปดจึงได้ทำการทบทวนสิ่งที่ทำลงไปและพบว่ามันเป็นสิ่งที่ไม่ถูกต้องจริงๆ จึงอยากกราบขอโทษทุกท่านที่ใช้คำพูดไม่เหมาะสมครับ

กองบรรณาธิการขาวปด

กราบขอภัย

กรณีคำขานนาที่ตลกขาวปดบนถนน

ทางกองบรรณาธิการขาวปดรู้สึกเสียใจเป็นอย่างยิ่งที่ได้ทำการล้อเลียนขานนาที่ตลกขาวปดบนถนน ถึงแม้มันเป็นเพียงพฤติกรรมที่เห็นแก่ตัว ซึ่งก็อาจทำลายนานา มักง่ายอยากให้อ้วนแถมใจๆ โดยไม่สนใจผู้ใช้นาน คิดว่านี่จึงทำครั้งเดียวเท่านั้น กันได้ ไม่เป็นไรหรอกน่า พร้อมกับสำนึกบุญคุณที่ไม่เคยมีไว้

กองบรรณาธิการรู้สึกผิดเป็นอย่างยิ่งที่ใช้คำพูดที่ไม่เหมาะสม จึงขอแสดงความสำนึกผิดด้วยการงดขานนาขาวปดเป็นเวลา 1 เดือน โดยจะทานสปาแก้ดีแทน เพื่อที่ว่าจะได้ทานแบบสบายใจ อย่างน้อยขานนาอิตาลีที่ปลูกข้าวสาลีคงจะไม่ทวงบุญคุณ

ด้วยความเคารพอย่างสูง
กองบรรณาธิการขาวปด



125

Like · Reply · 1d

สูตรมะนาวโซดา 10 วิธีทำน้ำมะนาวโซดาเครื่องดื่มล้างพิษ

โพสต์เมื่อวันที่ : 30 ก.ค. 2557 เปิดอ่าน : 102,854 ครั้ง



ลิงก์ผู้สนับสนุน

≡แชร์>



LINE it!

Tweet

LINE Add Friends

ถ้าพูดถึงเครื่องดื่มล้างพิษ เชื่อเลยว่า คนที่รักสุขภาพหลาย ๆ คนน่าจะคิดถึง น้ำมะนาวโซดา เป็นอันดับต้น ๆ ยิ่งในตอนนี้ มะนาวโซดา หรือ มะนาวผสม โซดา กลายเป็นเครื่องดื่มยอดฮิตเลยทีเดียว เพราะมีความเชื่อว่า น้ำมะนาวผสม โซดา จะช่วยรักษามะเร็งได้ แต่ก็มีแพทย์ออกมาเตือนแล้วว่า น้ำมะนาวผสม โซดาไม่ได้ช่วยรักษามะเร็งแต่อย่างใด เพียงแต่ช่วยด้านสารอนุมูลอิสระที่เป็นตัวก่อเซลล์มะเร็งได้เท่านั้นเอง

แต่ถึงแม้ว่าน้ำมะนาวโซดาก่อนนี้ จะไม่ได้ช่วยรักษาโรคมะเร็งอย่างที่หลายคนคาดหวังไว้ได้ แต่น้ำมะนาวโซดา สามารถช่วยล้างพิษ หรือดีที่

ตัวอย่างของคอนเทนต์ที่เป็น False Connection ก็
เช่น “น้ำมะนาวรักษาโรคมะเร็ง” หรือบทความที่ชอบขึ้น
ว่า “งานวิจัยเผย ...” แล้วกลายเป็นว่าโยงไปทางของ

ทำให้เข้าใจผิด & ผิดที่ผิดทาง

Misleading คือการเขียนข่าวหรือทำคอนเทนต์โดย
จงใจให้เข้าใจผิด ตัวอย่างของคอนเทนต์ Misleading
เราจะพบเห็นได้บ่อยกับพวกข่าวการเมือง



นาซา เร่งหาทางสกัดก่อนสาย ดาวเบเนนุ ชนโลก ถึงขั้น
คิดใช้ นิวเคลียร์ทำลาย



การที่เอาสิ่งที่เกิดขึ้นจริง เช่น รูป, ข้อความ,
คำพูด แต่เอามาใช้แล้วพูดถึงอีกเรื่องนึง
เช่น การเอารูปภัยธรรมชาติในต่างประเทศ
มา แล้วเขียนบอกว่าเกิดขึ้นที่ประเทศไทย

มโนที่มา & ปลอม ตัดต่อ

การมโนที่มาคือการรายงานข่าวแบบปกติ แล้วถ้าไม่ตรวจสอบดี ๆ ก็จะไม่รู้เลยว่าเป็น Fake News

ธนาธร จ๋อดำเนินคดีเฟจข่าวปลอม คุเรื่อง 'ห้ามวัดติ
ระขัง' ล่าสุดต้นทางลบโพสต์หนีแล้ว

Home > NEWS UPDATE > ธนาธร จ๋อดำเนินคดีเฟจข่าวปลอม คุเรื่อง 'ห้ามวัดติระขัง' ล่าสุดต้นทางลบโพสต์หนีแล้ว

Happy Three Time 2018-10-05



จัสติน ทรูโด นายกแคนาดาจูบกับผู้นำฝ่ายค้าน
เพื่อประณามเหตุกราดยิงในบาร์เกย์ที่ออร์แลนโด
เป็นภาพตัดต่อจากเว็บข่าวปลอม



6 hours ago — จูบปากของจริง!!

นายภฯ VS ผู้นำฝ่ายค้าน ประเทศแคนาดา

นายภฯ แคนาดาและหัวหน้าฝ่ายค้าน จูบปากกัน
ประณามเหตุกราดยิง

จัสติน ทรูโด นายกรัฐมนตรีแคนาดา และ โธมัส มัล
แคร์ หัวหน้าพรรคประชาธิปไตยใหม่ ได้จูบปากกัน
สร้างเซอร์ไพรส์... See more



CANADIAN PRIME
MINISTER AND
OPPOSITION LEADER
SHARE KISS TO
DENOUNCE
ORLANDO
MASSACRE

การ Manipulated คือการปลอมหรือตัดต่อ
ความรุนแรงของมันคือถ้าไม่สังเกตเราจะดูไม่ออก

มโนทุกอย่างเลย

การ Fabricated คือขั้นที่รุนแรงที่สุดของ Fake News ตัวอย่างของมันเป็นเช่นการปลอมมันทั้งเว็บ เช่น การปลอมเป็น ข่าวสด ปลอมเป็นไทยรัฐ หรือการปลอมเป็นบุคคล แล้วรายงานข่าว อันนี้ร้ายแรงมาก เนื่องจากคนก็จะเข้าใจว่าเป็นสำนักข่าวนั้นจริง ๆ และก็ไม่ได้เป็นการล้อเลียนหรือ Parody ด้วย

www.เราไม่ทิ้งกัน.com



อย่าหลงเชื่อ!
เว็บลงทะเบียนรับเงิน
ปลอม

1. เราไม่ทิ้งกัน.net
2. เราไม่ทิ้งกัน.org
3. เราไม่ทิ้งกัน.in.th
4. เราไม่ทิ้งกัน.co.th
5. เราไม่ทิ้งกัน.or.th
6. เราไม่ทิ้งกัน.in
7. เราไม่ทิ้งกัน.cc
8. เราไม่ทิ้งกัน.com
9. เราไม่ทิ้งกัน.org
10. เราไม่ทิ้งกัน.in.th
11. เราไม่ทิ้งกัน.co.th

12. เราไม่ทิ้งกัน.or.th
13. เราไม่ทิ้งกัน.net.th
14. เราไม่ทิ้งกัน.in
15. เราไม่ทิ้งกัน.cc
16. เราไม่ทิ้งกัน.com
17. เราไม่ทิ้งกัน.org
18. เราไม่ทิ้งกัน.in.th
19. เราไม่ทิ้งกัน.co.th
20. เราไม่ทิ้งกัน.or.th
21. เราไม่ทิ้งกัน.net.th
22. เราไม่ทิ้งกัน.in

23. เราไม่ทิ้งกัน.cc
24. เราไม่ทิ้งกัน.org
25. เราไม่ทิ้งกัน.in.th
26. เราไม่ทิ้งกัน.co.th
27. เราไม่ทิ้งกัน.or.th
28. เราไม่ทิ้งกัน.net.th
29. เราไม่ทิ้งกัน.in
30. เราไม่ทิ้งกัน.cc
31. เราไม่ทิ้งกัน.org
32. เราไม่ทิ้งกัน.in.th
33. เราไม่ทิ้งกัน.co.th

34. เราไม่ทิ้งกัน.or.th
35. เราไม่ทิ้งกัน.net.th
36. เราไม่ทิ้งกัน.in
37. เราไม่ทิ้งกัน.cc
38. เราไม่ทิ้งกัน.org
39. เราไม่ทิ้งกัน.in.th
40. เราไม่ทิ้งกัน.co.th
41. เราไม่ทิ้งกัน.or.th
42. เราไม่ทิ้งกัน.net.th
43. เราไม่ทิ้งกัน.in
44. เราไม่ทิ้งกัน.cc

ศูนย์ข้อมูล COVID-19 สายด่วน 1111

มโนทุกอย่างเลย



ไทยชนะ **ของจริง vs ของปลอม**

จริง

เป็นเว็บไซต์ เพื่อใช้ในการควบคุม
และป้องกันโรค

ชื่อเว็บ

- www.ไทยชนะ.com
- www.thaichana.com

ใช้งานผ่านเว็บไม่ต้อง
โหลดแอปใดๆ



ปลอม

เป็นเว็บ หลอกล่อให้โหลดแอป
เพื่อขโมยข้อมูลส่วนบุคคล

ชื่อเว็บ

- thaichana.pro
- thai-chana.asia
- thaichana.asia
- ฯลฯ



ANTI-FAKE NEWS CENTER THAILAND ศูนย์ต่อต้านข่าวปลอม ประเทศไทย

Copyright © 2020, Anti-Fake News Center Thailand, All rights reserved



ตัวอย่าง Fake News

5 ข่าวปลอม
เรื่องวัคซีนโควิด
ป่วนทั้ง ไทย -เทศ

วัคซีนฝึงไมโครชิป

ข่าวลือเรื่องวัคซีนโควิดฝึงไมโครชิปกลับมาพูดถึงอีกครั้งในช่วงปลายปี 2563 ทำให้ทางไฟเซอร์ ซึ่งแจ้งส่วนผสมของวัคซีนซึ่งมีอยู่ประมาณ 10 ชนิด ซึ่งเป็นส่วนผสมที่ใช้ในวัคซีนหลายชนิด แต่ไม่มีอะไรที่เกี่ยวข้องกับไมโครชิป อนึ่ง วันที่ 8 เม.ย. 2564 กระทรวงสาธารณสุขของออสเตรเลีย ย้ำอีกครั้งว่า **ไม่พบการติดตั้งซอฟต์แวร์หรือไมโครชิปในวัคซีนโควิด-19 ที่ใช้กันอยู่ในขณะนี้**

วัคซีนเปลี่ยนแปลงดีเอ็นเอมนุษย์

มีความกังวลว่าผู้ที่ได้รับวัคซีนจะเกิดอาการแพ้หรือผลข้างเคียงของวัคซีนจะเปลี่ยนไปจนมีความรุนแรงและต้องรักษาที่โรงพยาบาล (CDC) ยืนยันว่าวัคซีนที่ใช้เทคโนโลยี mRNA 2 ชนิด แม้จะส่งสารพันธุกรรมเข้าไปในร่างกายมนุษย์แต่สารนั้นจะไม่เข้าไปที่นิวเคลียสอันเป็นที่เก็บดีเอ็นเอ จึงไม่ส่งผลกระทบต่อดีเอ็นเอแต่อย่างใด

วัคซีนทำให้คนเป็นหมัน

กระทรวงสาธารณสุขของออสเตรเลีย โดยหน่วยงานบริหารสินค้าด้านยา (Therapeutic Goods Administration-TGA) ระบุว่าข่าวลือนี้ อ้างถึงโปรตีนซินไซติน-1 (Syncytin-1) ซึ่งใช้ในการพัฒนาวัคซีนที่มีอยู่ในหน่วยผสมของเชื้อโควิด-19 เช่นกัน แต่ยืนยันยังไม่พบหลักฐานทางวิทยาศาสตร์ที่บ่งชี้ว่า **การได้รับวัคซีนโควิด-19 หรือแม้แต่ตัววัคซีนป้องกันโรคอื่นๆ ส่งผลกระทบต่อการตั้งครรภ์หรือการพัฒนาของทารกแต่อย่างใด**

วัคซีนช่วยเพิ่มขนาดอวัยวะเพศชาย

มีการแชร์ไปทั่วว่า การฉีดวัคซีนโควิด-19 จะเพิ่มขนาดอวัยวะเพศชายให้ยาวขึ้น โดยอ้างงานวิจัย แต่จากการตรวจสอบพบว่า เป็นข่าวปลอมทั้งหมด ตั้งแต่วางวิจัยจากมหาวิทยาลัยแคลิฟอร์เนีย ที่อ้างกลุ่มตัวอย่างทำการศึกษารวม 1,500 คน ที่ไม่ได้อยู่จริง หรืออ้างวารสารวิชาการ The New England Journal of Medicine ที่อ้างถึงที่ไม่มีอยู่จริง

วัคซีนมีส่วนผสมของเนื้อสัตว์ต้องห้ามตามหลักศาสนา

มีข่าวบิดเบือนเกี่ยวกับการมีส่วนผสมของเนื้อสัตว์ต้องห้ามตามหลักศาสนา แต่จากการตรวจสอบพบว่า สำนักงานสุขภาพแห่งชาติ ประเทศอังกฤษ (NHS) ได้ทำงานอย่างหนักเพื่ออธิบายว่า **วัคซีนโควิด-19 ไม่มีเนื้อสัตว์เป็นส่วนผสม** นอกจากนี้องค์กรต่างๆ ที่เกี่ยวข้อง เช่น Indonesia's Ulama Council และ the British Islamic Medical Association ได้ยืนยันและให้ความเห็นต่อวัคซีนโควิด-19 อีกด้วย

เผยแพร่ 19 เม.ย. 64
เช็คให้ชัวร์ที่ โคแฟค
www.Cofact.org

ตัวอย่าง Fake News

วัคซีนโควิด-19
ทำมาจากไขมันหมู



เผยแพร่ 19 เม.ย. 64
เช็คให้ชัวร์ที่ โคแฟค
www.Cofact.org

เผยแพร่ 19 เม.ย. 64
เช็คให้ชัวร์ที่ โคแฟค
www.Cofact.org

ໂຈສນສຸ Cyber

ขออนุญาตเปิดข้อความนี้เป็นสาธารณะ และรบกวนเพื่อนทุกท่านในเฟสช่วยแชร์ข้อความนี้ทีนะคะ!!!!

วันนี้มีเพื่อนส่งรูปมาให้ดูเกี่ยวกับการรับบริจาคช่วยเหลือการรักษาเด็กคนหนึ่ง และเด็กในรูปคือน้องเพอเซีย และบรรยายอาการป่วยไว้อย่างน่าสงสาร เปิดรับบริจาค ซึ่งมีคนเข้าใจว่าเด็กในภาพป่วยจริง บริจาคเงินเป็นจำนวนมาก บางรายบริจาคเป็นหมื่น

จริงๆอยากบอกว่าแพค่อนข้างระวังตัวในระดับหนึ่งในการรับเพื่อน การเล่นเฟสบุ๊ค การลงรูปลูก เป็นเหมือนการบันทึกเรื่องราวของลูก แพคแทบจะไม่รับเพื่อน เพราะด้วยเหตุผลแบบนี้ แต่ขนาดระวังยังมาโดนกับตัวเอง

อยากบอกคนที่ทำว่าการนำรูปภาพลูกคนอื่น อธิบายคนอื่นว่าลูกป่วยหนัก รบกวนเถอะค่ะถ้าลูกคุณป่วยจริง ใช้รูปลูกคุณเถอะ เพราะลูกใครใครก็รัก ไม่มีใครอยากให้ลูกตัวเองป่วย แล้วการใช้รูปลูกคนอื่นหากินแบบนี้ เป็นสิ่งที่ไม่ถูกต้อง คุณต้องรู้จักเฟสเราเป็นอย่างดี คุณเอารูปลูกเราทุกอิริยาบถลงในเฟสคุณ ไม่ต้องกังวลนะคะ ตอนนี้เรากำลังดำเนินการแจ้งความค่ะ



Lookja Jalook is with [redacted]

1/8/2563 เวลา 12.00น. เช้านี้น้องลูกจำไม่มีไข้ แต่ยังต้องให้ยาปฏิชีวนะ/ยากระตุ้นการทำงานของหัวใจ/ยาละลายลิ่มเลือด/ยาปรับสมดุลระบบเลือด ต่อเนื่อง คุณหมอได้เปลี่ยนนมที่ดื่มเป็นชนิดดูดซึม และเฝ้าติดตามระบบเลือด ระบบขับของเสียของร่างกาย...อีกซักระยะบริเวณปอดยังพบความชื้นจากน้ำที่ท่วมปอดเมื่อสัปดาห์ที่ผ่านมา ...อาการที่แสดงชัดเจนตอนนี้ คือ ขอนมบ่อย



Lookja Jalook

21h •

..5/8/2563 ...อัปเดตอาการลูกจำเวลา17.00น ยังหายใจลำบากเนื่องจากมีลิ่มเลือดอุดตัน ยาเดินทางมาถึงสนามบิน และไปปรับมาแล้ว แต่ทางโรงพยาบาลยังไม่อนุญาตให้จ่ายยาแก่น้องลูกจำได้ จนกว่าจะมาชำระค่าคัดการที่คงค้างอยู่ ซึ่งคุณพ่อกำลังพยายามรวบรวมอยู่ในตอนนี้ จึงขออนุญาตนำกระเปาะสฟายข้างขนาด10นิ้ว ออกมาจำหน่ายเพื่อนำไปชำระให้กับโรงพยาบาล เพื่อให้ลูกจำได้รับการรักษาที่... See More



Lookja Jalook is with [redacted]


6/8/63 เช้านี้คุณหมอมองต้องการทำอัลต้าซาวด์ระบบการกลืน การย่อยของลำไส้ น้องลูกจำยังหายใจลำบาก แน่นหน้าอก เพราะยังไม่ได้ให้ยาละลายลิ่มเลือด น้องนอนในไอซียูตอนนี้.ขอกำลังใจให้น้องน้อยนะครับวันนี้#

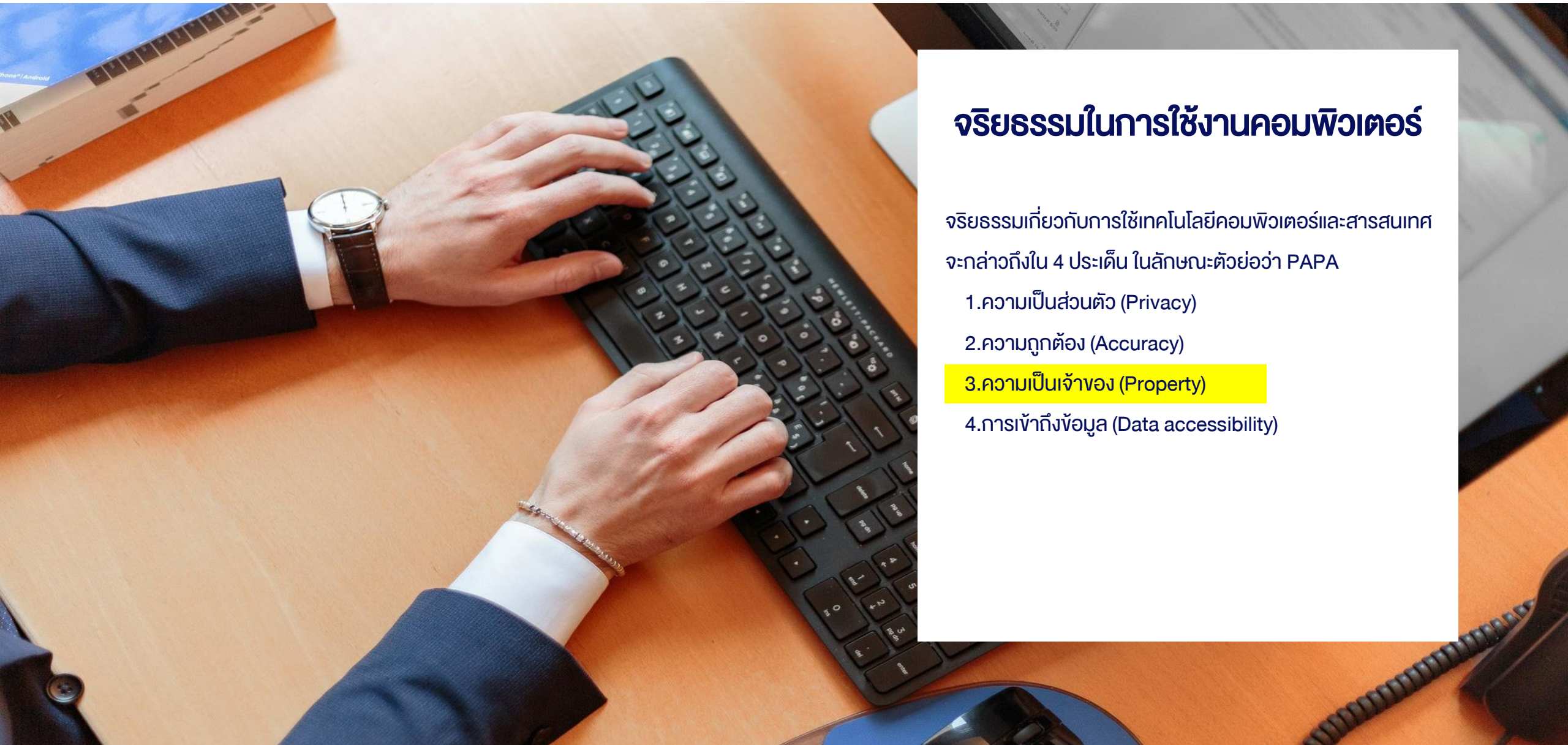


Lookja Jalook is with [redacted]

2d •

หลายต่อหลายครั้งที่ต้องรอการรักษา หลายต่อหลายครั้งที่ต้องรอยา เหตุการณ์แบบนี้ไม่ควรเกิดขึ้นเลย#พ่อขอโทษ





จริยธรรมในการใช้งานคอมพิวเตอร์

จริยธรรมเกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศ
จะกล่าวถึงใน 4 ประเด็น ในลักษณะตัวย่อว่า PAPA

- 1.ความเป็นส่วนตัว (Privacy)
- 2.ความถูกต้อง (Accuracy)
- 3.ความเป็นเจ้าของ (Property)
- 4.การเข้าถึงข้อมูล (Data accessibility)

ดีเอสไอ ทลายเว็บ fwiptv.cc ละเมิดลิขสิทธิ์หนังเถื่อนรายใหญ่ ระดับประเทศ

Fwiptv.cc เป็นเว็บไซต์ที่มีสมาชิกเข้าชม **ยอดวิวต่อเดือนมากกว่า 7 แสนวิว** ซึ่งเป็นเว็บไซต์ละเมิดลิขสิทธิ์อันดับหนึ่งที่มีการเก็บค่าสมาชิกในการเข้าชม (โดยเก็บค่าสมาชิกเดือนละ 300 บาท) และอยู่ในการจัดลำดับที่ 729 สำหรับประเทศไทยที่คนดูเข้าชมมากที่สุด จากการประเมินมูลค่าความเสียหายในเชิงธุรกิจมากกว่า **2,000,000,000 บาท (สองพันล้านบาท)**

ข่าว

อาชญากรรม



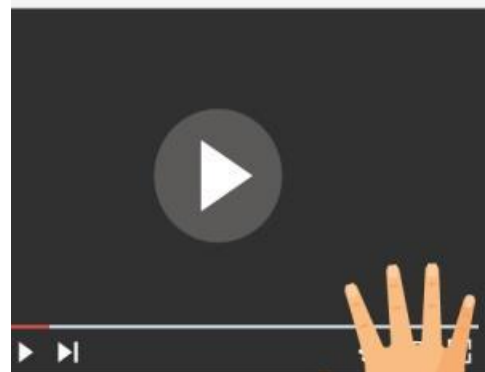
บันทึก

SHARE



ที่มา : ไทยรัฐออนไลน์

แฮร์และคัดลอก เป็นปัญหาอย่างไร?



งาน Original
ที่ผ่านการคิด
และสร้างสรรค์
อย่างดี



ผู้ชม
งาน Original



รายได้ไปไม่ถึง
เจ้าของผลงาน



งานละเมิดลิขสิทธิ์โพสต์และไลฟ์
คัดลอก-ตัดต่องานผู้อื่น
โดยไม่ได้รับอนุญาต



ผู้ชมสนับสนุนด้วย
การดู LIKE & Share



สร้างรายได้จำนวนมาก
ให้ผู้ละเมิดลิขสิทธิ์

ภาพนี้ของใคร...?



ข่าว หนังสือพิมพ์ ไทยรัฐทีวี ไลฟ์สไตล์ กีฬา บันเทิง ดวง หวอย นิยาย วิดีโอ โปรแกรม MIRA



การต่อสู้ทางกฎหมายขององค์การพิทักษ์สิทธิสัตว์ (พีต้า) ทำให้การเรียกรังสัตว์ ให้นำรูปถ่ายลิงแสมสีดำในป่าบนเกาะสุลาเวสีของอินโดนีเซีย เพื่อให้ได้เป็นเจ้าของภาพถ่ายเซลฟี่แย่งของมันเอง ได้ข้อสรุปแล้วเมื่อเร็ว ๆ นี้

เป็นข้อยุติที่ลิงแสมก็ไม่ได้เป็นเจ้าของลิขสิทธิ์ภาพตัวเอง แต่สิ่งที่ได้เป็นผลผลิตพลอยได้ เป็นนายโปรดัคส์

ที่มา : โพสต์ทูเดย์

ความเป็นมา...

เมื่อนายเดวิด สเลเตอร์ ช่างภาพถ่ายแนวธรรมชาติชาวอังกฤษ ผู้ตั้งกล้องไว้ขณะเฝ้าถ่ายรูปในป่าบนเกาะสุลาเวสีเมื่อปี 2554 แล้วทิ้งช่วงไปทำอย่างอื่นได้ไม่กี่นาที พอกลับ มาก็คพบว่ากล้องถูกลิงนารูโตะมาฉวยเอาไปแล้วยังถ่ายภาพเซลฟี่หน้าทะเล้นตัวเอง สัญญาจะแบ่งรายได้เข้าองค์กรการกุศล

สเลเตอร์สัญญาจะบริจาคเงิน 25% ของรายได้ในอนาคตจากการขายภาพของนารูโตะ เข้าองค์กรการกุศลที่คุ้มครองผืนป่าแหล่งอยู่อาศัยของนารูโตะ และเพื่อนร่วมพิภพวานรอื่นๆในอินโดนีเซีย

บทสรุปท้ายสุด

เรื่องนี้ได้ข้อสรุป หลังทั้งสองฝ่ายเป็นคดีความกันมาร่วม 2 ปี โดยพิต้าและสเลเตอร์ ตกลงยอมความกันในชั้นอุทธรณ์ที่ศาลในนครซานฟรานซิสโกของสหรัฐฯ เมื่อวันที่ 11 ก.ย.ที่ผ่านมา หลังจากก่อนหน้านี้ ศาลชั้นต้นตัดสินเข้าข้างคน ให้ช่างภาพชนะคดี เพราะกฎหมายปกป้องลิขสิทธิ์ใช้กับลิงไม่ได้

ทั้งนี้ หลังจากกลุ่มพิต้าได้ฟ้องร้องต่อศาลเมื่อปี 2558 หลังเห็นหนังสือภาพถ่ายธรรมชาติ เป็นภาพเซลฟี่ของลิงแสมด่านารูโตะ ยึดแน่นหน้าทะเลและภาพถ่ายอื่นๆ ที่นายสเลเตอร์พิมพ์ออกขาย

โดยในแถลงการณ์ร่วม พิต้าและสเลเตอร์ ยังเห็นร่วมกันยกคดีนี้เป็นคดีตัวอย่าง และมีความสำคัญ เพื่อขยายสิทธิทางกฎหมายคุ้มครองถึงสิทธิ์ของสิ่งมีชีวิต แม้ครั้งนี้จะไม่สำเร็จ แต่จะพยายามเคลื่อนไหวไปสู่เป้า หมายให้ได้ต่อไป

คดีนี้เป็นคดีตัวอย่างและเป็นเรื่องใหม่ทำให้ระหว่งการไต่สวนคดีในศาล มี นักเรียนกฎหมายเข้าร่วมรับฟังหลายคน แต่เมื่อคดีจบแบบนี้ กลุ่มพิต้าคงต้องเหนื่อยอีกนาน.

จำไว้ 3 ข้อ “พ.ร.บ.ลิขสิทธิ์”

- หลัก 3 ประการของการไม่ละเมิดกฎหมายลิขสิทธิ์ คือ
หนึ่ง... “ขออนุญาต”
สอง... “ให้เครดิต” และ
สาม... “ห้ามดัดแปลง”
- สำหรับผู้ใช้ทั่วไปเน้นที่สองข้อหลัง

แสดงโทษผู้กระทำความผิดฐานละเมิด
พ.ร.บ.ลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558



มีโทษปรับ 10,000-100,000 บาท

กรณีทำเพื่อการค้า
จะมีโทษจำคุกตั้งแต่ 3 เดือน-2 ปี หรือ
ปรับตั้งแต่ 50,000-400,000 บาท หรือ
ทั้งจำทั้งปรับ และให้รับสิ่งของละเมิดลิขสิทธิ์
หรือศาลสั่งให้ทำลาย
โดยผู้ละเมิดลิขสิทธิ์ต้องเป็น
ผู้ออกค่าใช้จ่ายในการทำลาย



ป้องกันตัวเอง ไม่ให้**ละเมิดลิขสิทธิ์**

วิธีที่ 1 ให้เครดิตแก่เจ้าของ

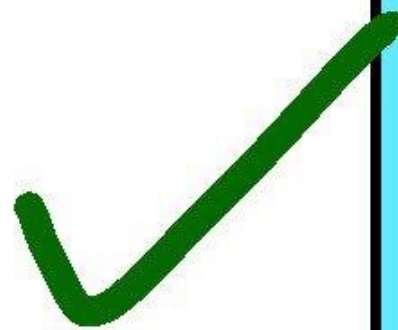
“แม้จะมีการให้เครดิตแต่นำไปเพื่อ หากำไร ย่อมเป็นละเมิด แม้ใช้ส่วนตัวก็อาจจะ
เป็นละเมิด ถ้ามีการขัดต่อการแสวงหาผลประโยชน์ของเจ้าของในงาน หรือ มีการ
กระทบกระเทือนในสิทธิของเจ้าของงาน”

-- IP Chula (สำนักงานกฎหมายและทนายความ)

วิธีการให้เครดิต by เรือนช่างศิลป์



Cr. @pasu
Cr. เรือนช่างศิลป์
Cr. #เรือนช่างศิลป์



Cr. on pic
Cr. ในรูป
ขอบคุณเจ้าของผลงานนะคะ



ตัวอย่างการใส่เครดิตที่ถูกต้อง

ภาพวาด

ชื่อภาพ....ผู้สร้างสรรค์.....จากหนังสือ.....

ภาพยนตร์

ภาพยนตร์จากเรื่อง.....ผู้สร้าง.....

ภาพเหตุการณ์

ได้รับการสนับสนุนภาพจาก.....

ข้อมูล/ตัวเลข

จัดทำโดย.....จากหนังสือ.....

ดนตรีหรือเพลง

ชื่อเพลง.....ผู้แต่งคำร้อง/ทำนอง/ผู้เรียบเรียง

ที่มา: กรมทรัพย์สินทางปัญญา

วิธีที่ 2 ใช้ของฟรี!!





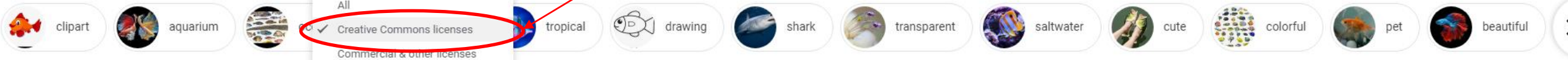
fish



All Images Videos Maps News More

Tools

Size Color Type Time Creative Commons licenses Clear



fish (2152054969).jpg - Wikimedia Commons commons.wikimedia.org



Fish Fins Scales - Free image on Pixabay pixabay.com



Suriname fish | Coastal... flickr.com



File:Skipjack tuna (Katsuwonus pelamis... commons.wikimedia.org



fish, sea, blue, ocean, nature ... pxhere.com



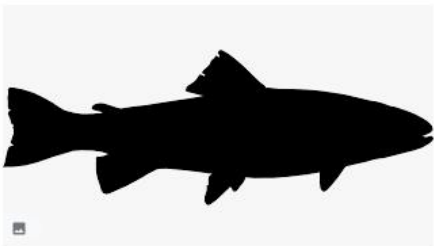
Koi Fish Animal Nature Green - Free ... pixabay.com



fish.png - Wikimedia Commons commons.wikimedia.org



Free Images : dolphin fish, fishery ... pxhere.com



Fish Black Fishing - Free vector ... pixabay.com



carlos the fish | I suggested to... flickr.com



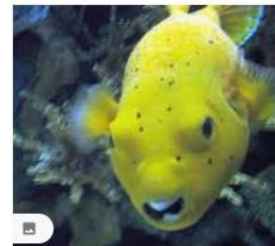
Fish Raw Seafood - Free photo on Pixa... pixabay.com



bass, red seabream, tilefish, oily fish ... pxhere.com



Classic Fish fingers - Vici - 450 g e world.openfoodfacts.org



File:Yellow fish in the aquarium.J... commons.wikimedia.org



https://pixabay.com/

pixabay

Photos

Illustrations

Vectors

Videos

Music

Explore ▾

Log in

Join

Upload

Stunning free images & royalty free stock

Over 2.3 million+ high quality stock images, videos and music shared by our talented community.

🔍 Search images, vectors and videos

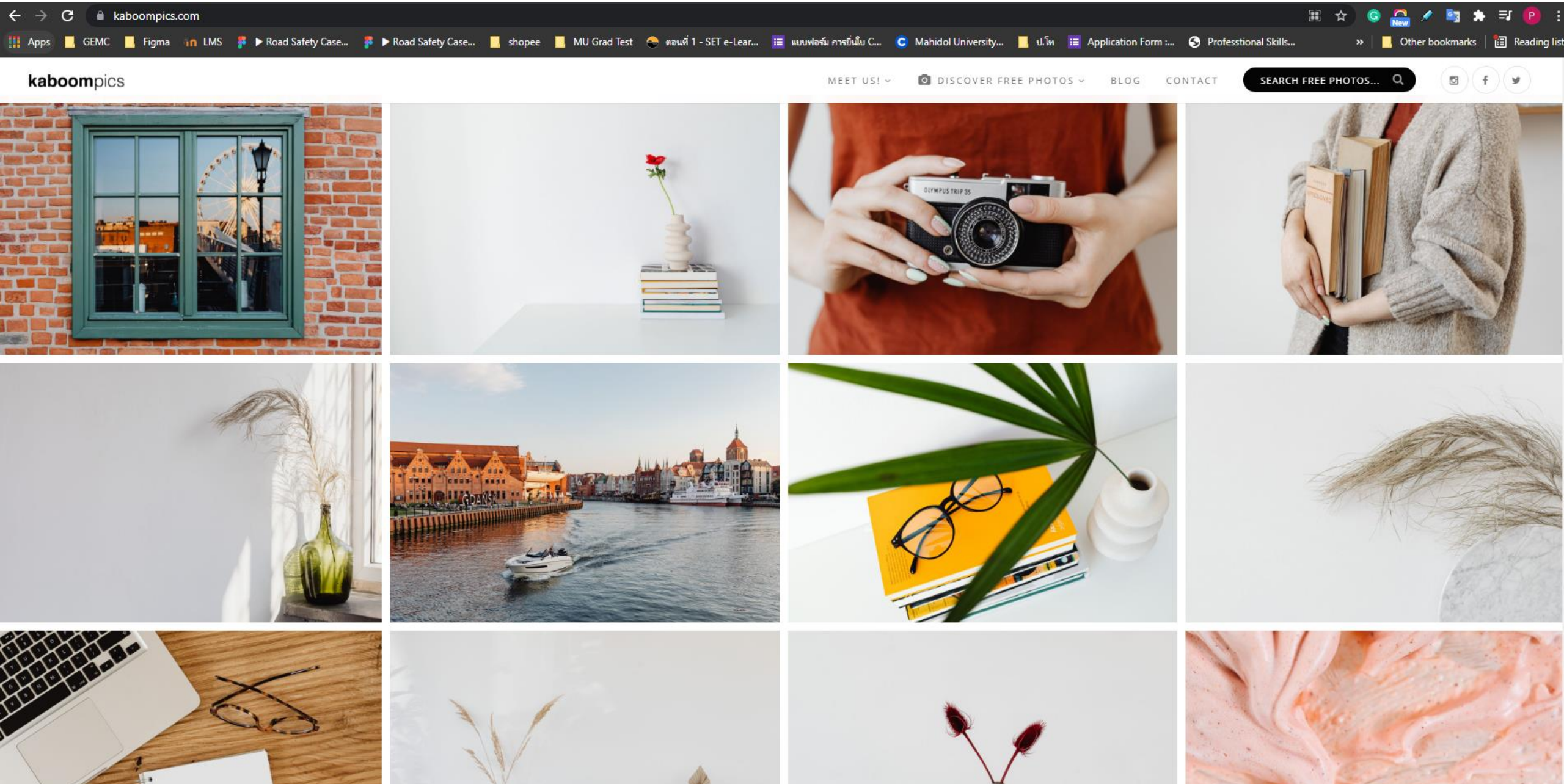
Images ▾

Popular Images: nature, wallpaper, background, summer, food, beach, sky, flower, dog, cat, money, love, flowers, coronavirus

Free image by Leolo212



<https://kaboompics.com/>



https://www.flickr.com/

← → ↺ flickr.com/search/?text=product

Apps GEMC Figma LMS Road Safety Case... Road Safety Case... shopee MU Grad Test ตอนี่ 1 - SET e-Lear... แผนการสอน การเขียน C... Mahidol University... ป.โท Application Form ... Profesional Skills... Other bookmarks Reading list

flickr You Explore Prints Get Pro

product

Photos People Groups

Advanced

Any license SafeSearch on

Share Relevant

View all 2,188,219

Everyone's photos

Connecting...

Feedback

https://www.pexels.com/th-th

← → ↺ pexels.com/th-th/search/ครีมทาหน้า/

Apps GEMC Figma LMS Road Safety Case... Road Safety Case... shopee MU Grad Test ตอนที่ 1 - SET e-Lear... แบบฟอร์ม การยื่นใบ C... Mahidol University... » Other bookmarks Reading lis

Pexels

ครีมทาหน้า

สำรวจ การอนุญาตสิทธิ์ใช้งาน อัปโหลด ...

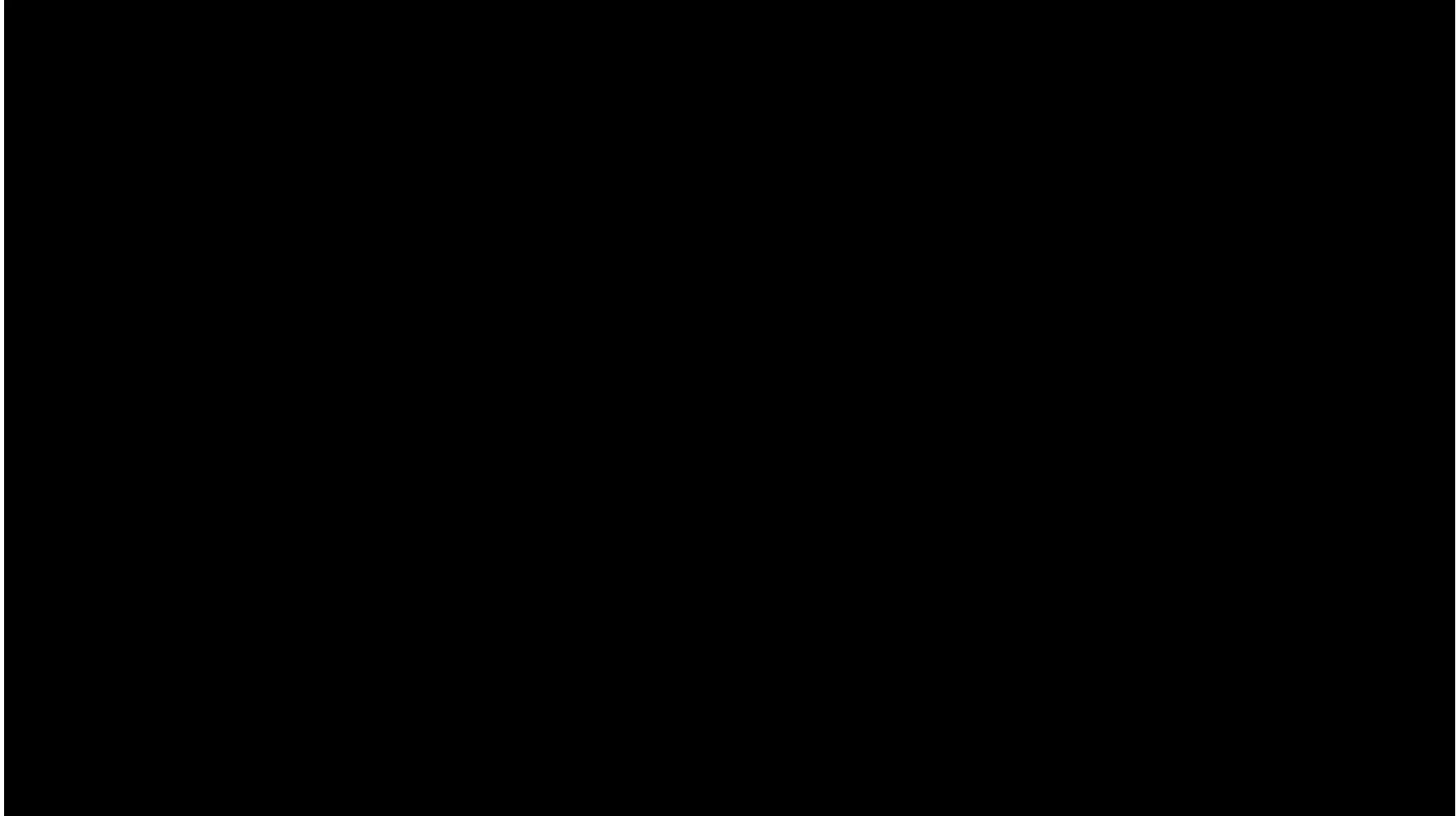
เข้าร่วม





Ransomware

Ransomware





โรงพยาบาลสระบุรี

! ระบบคอมพิวเตอร์ขัดข้อง !

Ransomware ชื่อ VoidCrypt เข้ารหัสข้อมูลคนไข้

ด้วยระบบคอมพิวเตอร์ของโรงพยาบาลสระบุรีขัดข้อง

ทำให้ไม่สามารถให้บริการผู้ป่วยในระบบต่างๆ ของโรงพยาบาลได้

ซึ่งโรงพยาบาลกำลังดำเนินการแก้ไขอย่างเร่งด่วน

ดังนั้นจึงขอความกรุณาจากผู้รับบริการทุกท่าน

ที่เข้ามาใช้บริการตรวจรักษาในโรงพยาบาลสระบุรี

กรุณานำบัตรแสดงสิทธิการรักษา สำหรับใบส่งยา หรือใบส่งใบรับยา
บัตรแพทย์ และใบรายการยาครั้งสุดท้ายที่ได้รับพร้อมนำยาเดิมมาด้วยทุกครั้ง

จนกว่าโรงพยาบาลจะดำเนินการแก้ไขระบบคอมพิวเตอร์แล้วเสร็จ

เรียกค่าไถ่ในการถอดรหัส 63,000 ล้านบาท

ข่าวแจ้งสาเหตุเกิดจากบุคลากรนำเครื่องส่วนตัวมาใช้

ขออภัยในความไม่สะดวกจึงประกาศมาให้ทราบโดยทั่วกัน

Ransomware

บริษัทซอฟต์แวร์ 'Kaseya' ถูกแฮกเกอร์ โจมตี คาดกระทบลูกค้า 1,500 รายทั่วโลก

By TopTen - July 7, 2021



กลุ่มเรียกแฮกเกอร์ **REvil** ได้เรียกร้องให้จ่ายเงิน **70 ล้านดอลลาร์** หรือราว **2.1 พันล้านบาท** เป็น Bitcoin สำหรับเครื่องมือถอดรหัส หลังจากโจมตีผู้จำหน่ายซอฟต์แวร์ Kaseya ซึ่งถือเป็นการโจมตี **ซัพพลายเชนที่ใหญ่ที่สุด** ที่ไม่เคยมีมาก่อน และอาจเป็นการโจมตีของ **Ransomware** ที่ใหญ่เป็น **อันดับสอง** เท่าที่เคยมีมา

ขณะที่บริษัทผู้จำหน่ายซอฟต์แวร์ Kaseya คาดว่า จำนวนบริษัทที่ได้รับผลกระทบจากการโจมตีครั้งนี้มีอยู่ประมาณ **800-1,500 รายทั่วโลก** โดยมีลูกค้าที่ได้รับผลกระทบโดยตรงประมาณ **50 ราย** และบริษัทอีกหลายร้อยแห่งที่ได้รับผลกระทบเพราะลูกค้าของ Kaseya จำนวนมากให้บริการด้านไอทีแก่ธุรกิจขนาดเล็ก เช่น ร้านอาหารและสำนักงานบัญชี

เมื่อช่วงวันศุกร์ที่ผ่านมา Kaseya ได้ออกมายอมรับว่าตนเองถูกผู้ไม่หวังดีทำการเจาะซอฟต์แวร์ VSA ซึ่งเป็นระบบ Endpoint Management และ Network Monitoring เพื่อใช้เป็นช่องทางในการกระจาย Ransomware REvil ซึ่งการโจมตีนี้เกิดขึ้นในผู้ให้บริการแบบ MSP จำนวน 8 ราย ทำให้มีลูกค้ามากกว่า 100 รายได้รับผลกระทบ โดยมีการเรียกค่าไถ่เป็นจำนวนเงินตั้งแต่ 1,400,000 บาท ไปจนถึง 160 ล้านบาทเลยทีเดียว

อย่างไรก็ตาม ทาง Kaseya กำลังร่วมมือกับผู้เชี่ยวชาญเพื่อพยายามอุดช่องโหว่ Zero Day ในครั้งนี้ โดยแนะนำให้ลูกค้าที่ใช้ VSA แบบ On Premise อยู่ทำการ Shutdown ระบบเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นเอาไว้ก่อน โดย Kaseya ได้ทำการปิดระบบ SaaS ที่มีลูกค้าใช้งานกว่า 36,000 รายของตนเองเรียบร้อยแล้ว

<https://positioningmag.com/1341090>

<https://www.techtalkthai.com/kaseya-vsa-exploited-to-distribute-ransomware/>

Recommendations



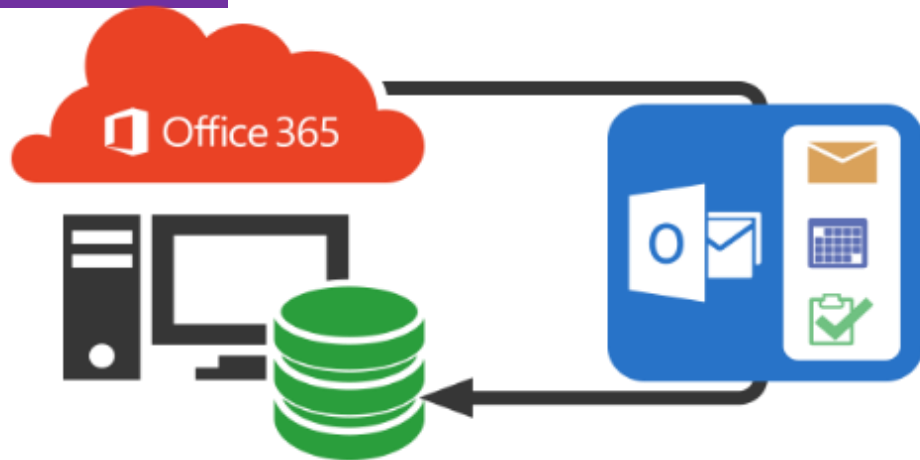
Initial Version



Continuous File Versioning



Cloud Versioning



เลือกผู้ให้บริการ Cloud Services ที่มี
Backup features หรือ Recovery
Plans

ใช้โปรแกรม Backup จาก Cloud ไปยัง Local

Recommendations

ใช้โปรแกรมที่ถูกลิขสิทธิ์

ปรับปรุงโปรแกรม
Antivirus สม่ำเสมอ

เปิดใช้งาน Host-based
Firewall

ใช้โปรแกรม Anti-
Ransomware

สำรองข้อมูลใน External
Hard drive และบน
Cloud อย่างสม่ำเสมอ

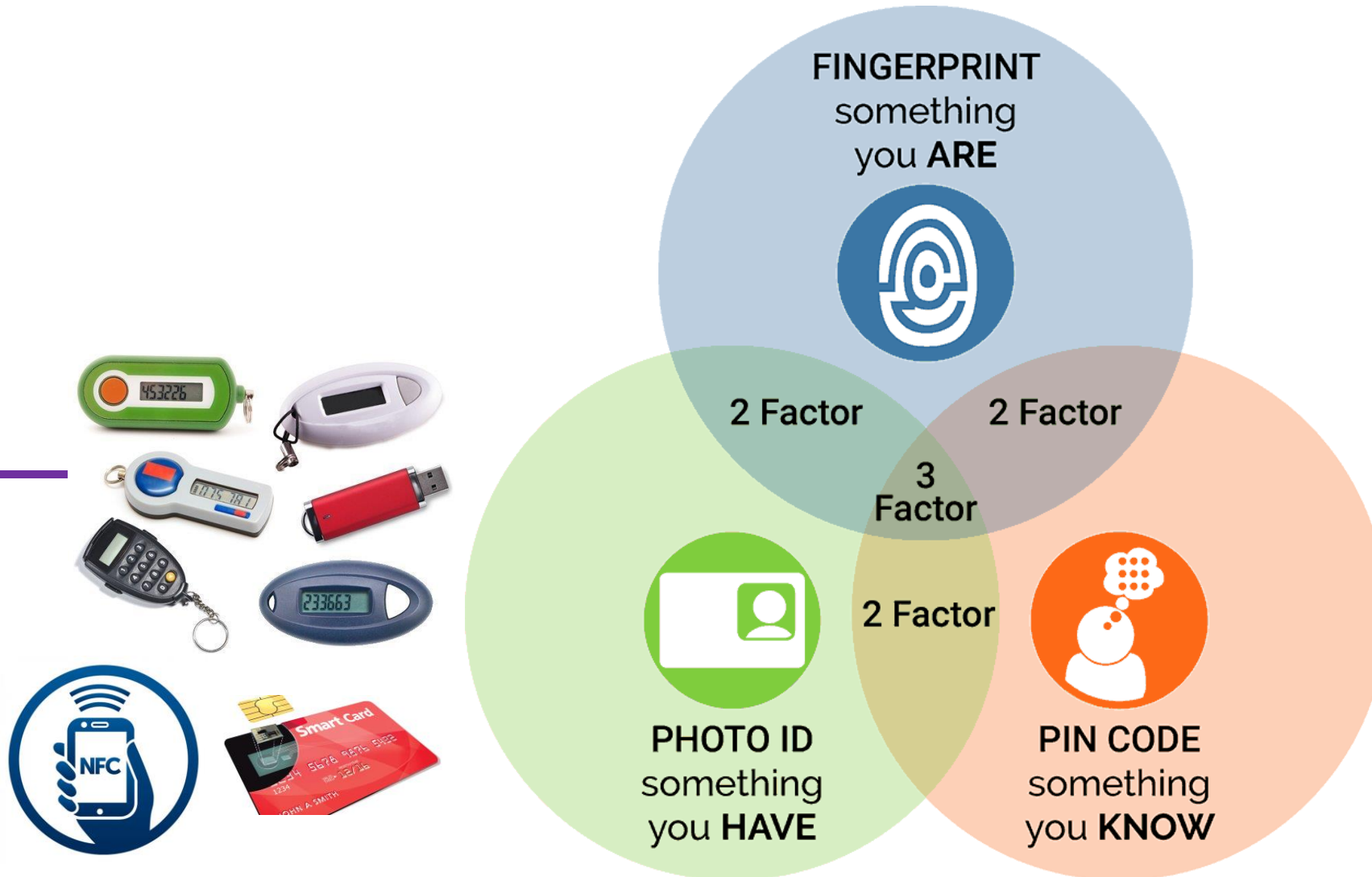
ปรับปรุง Patches ของ
โปรแกรม OS และอุปกรณ์
ต่าง ๆ อย่างสม่ำเสมอ

ใช้ Multi-Factor
Authentication

ควบคุมการเข้าถึงและใช้
งานเครือข่ายด้วย NAC

ใช้ Privilege Access
Management

Multi-Factor Authentication



- Static Password
- One-time password
- Cognitive password
- Passphrase

<https://www.borer.co.uk/borer-technology/multi-factor-identity-authentication/>

Multi-Factor Authentication

- Something you do
- Somewhere you stay



Location-based authentication



Keystroke Dynamic

Passwordless Authentication



IoT Attack

Connected Car Hacked



Recommendations

ติดต่อผู้ผลิตสำหรับ Car
Security Solutions และ
นโยบายความปลอดภัย

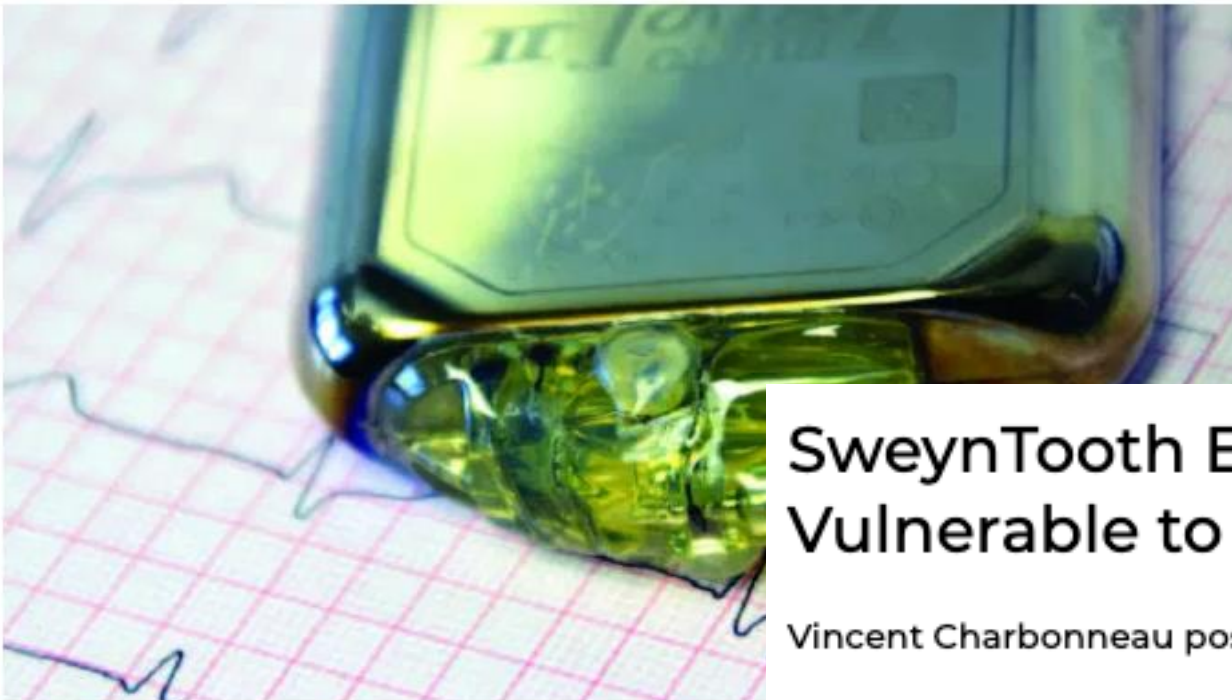
ปรับปรุง Firmware และ
แก้ Car Bugs สม่ำเสมอ

ระวังการเชื่อมต่ออุปกรณ์
ภายนอกกับรถคุณ

Smart Medical Devices with BLE Hacked

FDA warns about hacking in medical devices

© March 10, 2020 Branding Iron Features, NewTop 0



ตัวอย่างอุปกรณ์ทางการแพทย์ที่ใช้ BLE (Bluetooth Low Energy มีใน Bluetooth v4.3 ขึ้นไป)

- เครื่องกระตุ้นไฟฟ้าหัวใจ (Pacemaker)
- เครื่องกระตุ้นกล้ามเนื้อ (Stimulator)
- เครื่องปล่อยอินซูลิน (Insulin Pump)
- เครื่องวัดระดับน้ำตาล (Glucose Monitor)
- เครื่องตรวจอัลตราซาวด์ (Ultrasound device)

SweynTooth Exploit Leaves Medical Hardware Vulnerable to Cyberattacks

Vincent Charbonneau posted on March 25, 2020 | Comment

SweynTooth has the potential to cause havoc for many IoT and Bluetooth devices

<https://www.engineering.com/IOT/ArticleID/20062/SweynTooth-Exploit-Leaves-Medical-Hardware-Vulnerable-to-Cyberattacks.aspx>

SweynTooth Vulnerabilities – 12 Vuls of IoT devices



(a) FitBit
Inspire



(b) Eve Energy



(c) August
Smart Lock

An illustration of products that are vulnerable to SweynTooth (ASSET Research Group)



(d) CubiTag



(e) eGeeTouch

<https://asset-group.github.io/disclosures/sweyntooth/>

Recommendations

ซื้ออุปกรณ์จากผู้ผลิตที่
น่าเชื่อถือ

ติดต่อผู้ผลิตเรื่องการ
ปรับปรุง Firmware และ
Bugs อย่างสม่ำเสมอ

ใช้สิทธิ์ตาม พรบ.
คุ้มครองข้อมูลส่วนบุคคล

ระวังการเก็บข้อมูล
ประวัติในอุปกรณ์ IoT

Drone Hijacking Attack



Recommendations

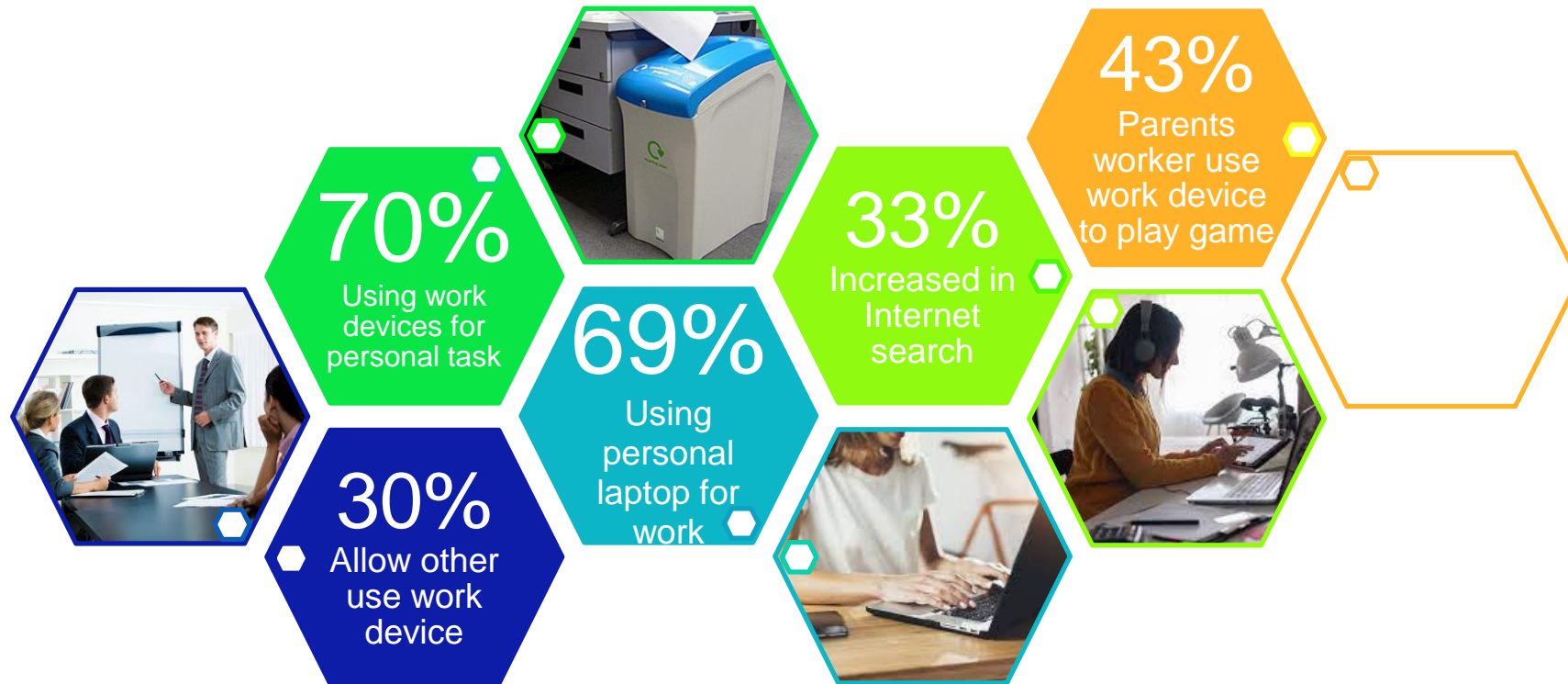
- ใช้ Drone Detect & Protect System





Remote Working Risks

Work from Home Risk



HP Wolf Security, "Blurred Lines and Blindspots". May 2021

Recommendations for Employees

ตั้งค่าให้ปรับปรุง Patches
OS และ Applications ที่ใช้
งานแบบอัตโนมัติ

ติดตั้งและปรับปรุง
โปรแกรม EndPoint
Protection

ตั้งรหัสผ่านที่มีความ
แข็งแรง

ใช้ VPN ในการเข้าถึง
ระบบที่องค์กร

สำรองข้อมูลบน External
Drive และ Centralize
Storage ขององค์กรอย่าง
สม่ำเสมอ

ตั้งค่าความปลอดภัยของ
ระบบ Video
Conference

ตั้งค่าความปลอดภัย
ของระบบ WIFI

ห้ามให้ครอบครัวใช้งาน
อุปกรณ์ที่ทำงาน

ใช้ตัวปิดหน้ากล้องเครื่อง
คอมพิวเตอร์

Recommendations for Organization

กำหนดนโยบายและวิธี
ปฏิบัติเกี่ยวกับการทำงานที่
บ้าน

สร้างความตระหนักรู้ด้าน
Cyber Security กับ
พนักงาน

ใช้ Multi-factor
Authentication

ใช้ระบบ Zero Trust
Network Access

สร้างให้พนักงานรู้สึกสบายใจ
ในการแจ้งการกระทำที่
ผิดพลาด



AI Risks

ตัวอย่างการใช้งานปัญญาประดิษฐ์ในบริษัทเทคโนโลยีระดับโลก



คาดเดาสิ่งที่ลูกค้าต้องการจะซื้อ



โทรและนัดนัดหมายแทนคุณ



Siri ผู้ช่วยอัจฉริยะ, แนะนำเพลง, ช่วยค้นหารูป

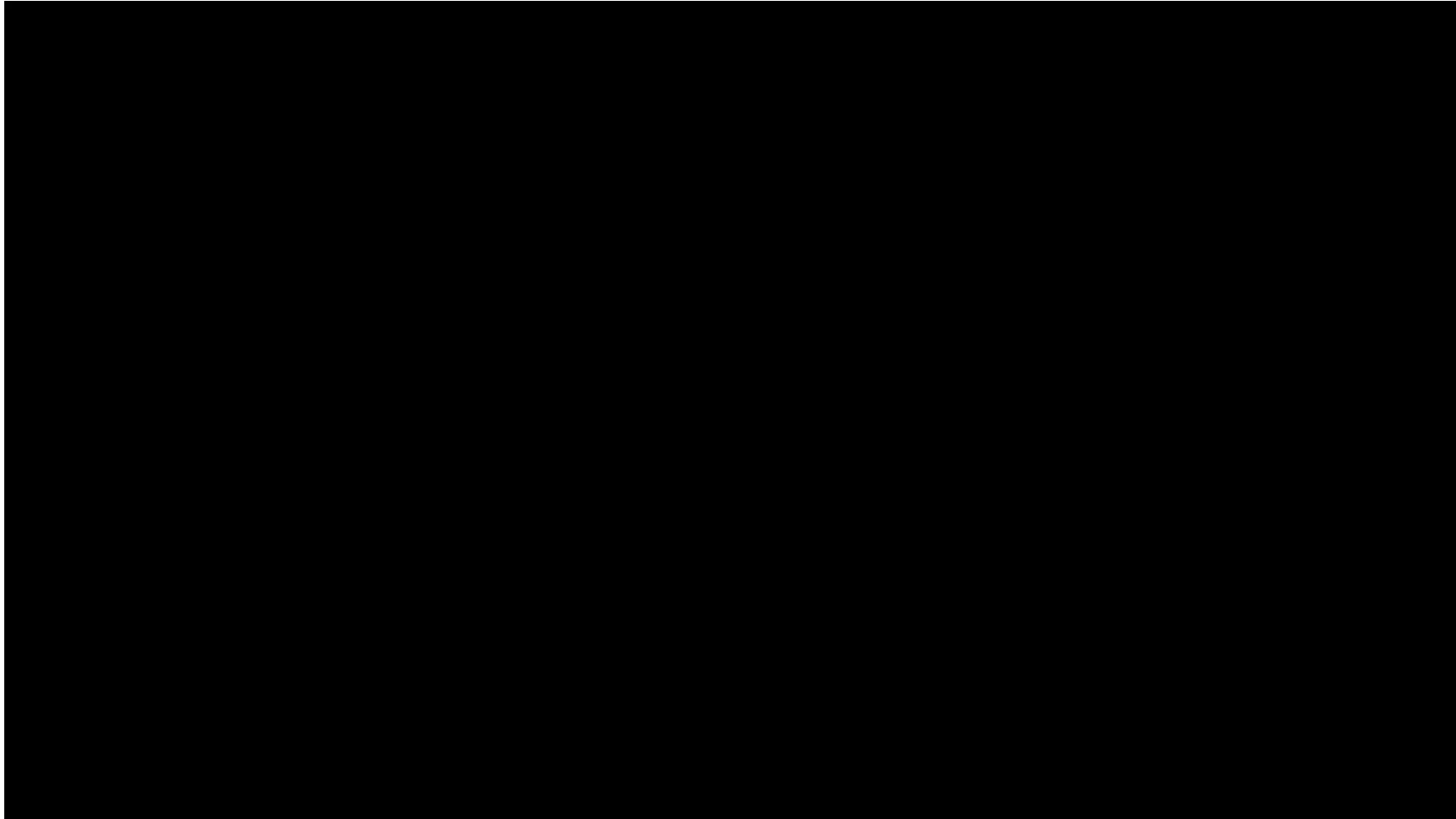


ใช้ AI ในทุก Products & บริการ



แปลความหมายและความรู้สึกของข้อความในโพสต์,
ระบุตัวตนจากรูปถ่ายในโพสต์

Deepfakes



AI Provider Hacked

[24]7.ai – บริษัทที่ให้บริการ AI Customer Services ถูก Malware โจมตี

TIME

U.S. POLITICS WORLD TECH ENTERTAINMENT

BUSINESS • DATA BREACH

Data Breach at Sears and Delta May Have Hit 'Several Hundred Thousand' Customers



Unfairness in AI

จากปัญหา COVID-19 เมื่อปีที่แล้ว ทำให้โรงเรียนหลายโรงเรียนทั่วโลกไม่สามารถสอบปลายภาคให้กับเด็กได้ ทำให้ IBO ซึ่งเป็นองค์กรที่พัฒนาหลักสูตร IB (International Baccalaureate) ซึ่งเป็นที่ยอมรับกันในโรงเรียนนานาชาติต่าง ๆ ตัดสินใจใช้ AI ทำการประเมินคะแนนให้กับนักเรียนแทน โดยใช้ข้อมูลผลการเรียนในห้องเรียน ผลคาดการณ์คะแนนของคุณครู และ*คะแนนโดยรวมของโรงเรียนนั้น ๆ* ผลลัพธ์ที่เกิดขึ้นทำให้นักเรียนที่เรียนเก่งแต่ยากจน ซึ่งมักจะเรียนในโรงเรียนที่นักเรียนส่วนใหญ่มีคะแนนต่ำ ได้คะแนนที่ต่ำไปด้วย

Global exam grading algorithm under fire for suspected bias

July 2020



<https://news.trust.org/item/20200721145229-gm15u/>

Recommendations

ตรวจสอบข้อมูลทั้งภาพ
เสียง ข้อความ และวิดีโอ
จากหลายแหล่งข้อมูล

ศึกษาเพื่อให้รู้เท่าทัน
พัฒนาการด้าน AI อย่าง
สม่ำเสมอ

ปรับปรุง Patches ของ
โปรแกรม OS และอุปกรณ์
ต่าง ๆ อย่างสม่ำเสมอ

ตรวจสอบความ
น่าเชื่อถือของผลิตภัณฑ์
ก่อนรับใช้งาน

ร้องขอรายละเอียด
หลักการจริยธรรมที่ใช้ใน
ผลิตภัณฑ์และบริการ

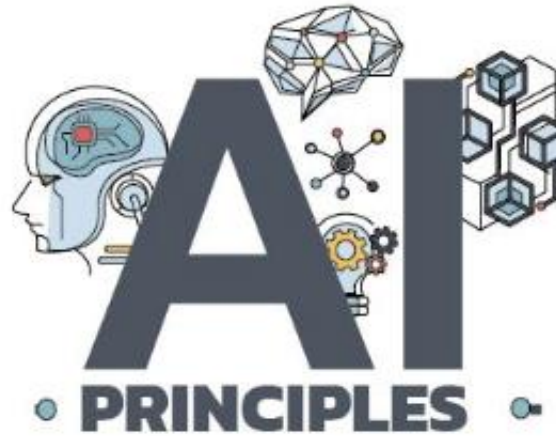
แจ้งผลการใช้งาน **AI**
กลับไปยังผู้ผลิต

ใช้สิทธิตามกฎหมาย
พรบ.คุ้มครองข้อมูลส่วนบุคคล

Deepfake Detection Challenge



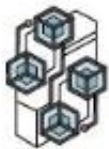
หลักการจริยธรรมปัญญาประดิษฐ์ประเทศไทย



ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน
(Competitiveness and Sustainability Development)



ความมั่นคงปลอดภัยและความเป็นส่วนตัว
(Security and Privacy)



ความสอดคล้องกับกฎหมายจริยธรรมและมาตรฐาน
สากล (Laws Ethics and International Standards)



ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม
(Fairness)



ความโปร่งใสและการความรับผิดชอบ
(Transparency and Accountability)



ความน่าเชื่อถือ
(Reliability)

นโยบาย และแนวทางปฏิบัติงานในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐสภา



เอกสารที่อ้างอิง

นโยบาย และแนวทางปฏิบัติงานในการรักษาความมั่นคง
ปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐสภา

<https://cutt.ly/Om1lcro>



<https://cutt.ly/Rm1lh18>



โครงการจัดทำกฎ/
ระเบียบ/มาตรการ/
แนวปฏิบัติด้วยความ
มั่นคงปลอดภัยด้าน
สารสนเทศของรัฐสภา



- 1) นโยบายในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของรัฐสภา
- 2) แผนรองรับสถานการณ์ฉุกเฉินของรัฐสภา
(IT Contingency Plan)
- 3) แผนสำรองข้อมูลของรัฐสภา (Backup Plan)
- 4) แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา
(IT Risk Management Plan)
- 5) แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยี
สารสนเทศและการสื่อสารของรัฐสภา

คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
และการสื่อสารของรัฐสภา ระยะ 4 ปี (พ.ศ. 2562 – 2565)

กฎหมายที่เกี่ยวข้อง

- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ (๓ ประเด็น)
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๒ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายใน การรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง **มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕** (กำหนดมาตรฐานฯ ๑๑ ข้อ ๓ ระดับ)
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ แก้ไขให้ผู้บริการระดับสูงสุดของหน่วยงาน (CEO) เป็นผู้รับผิดชอบ (เดิม CIO)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

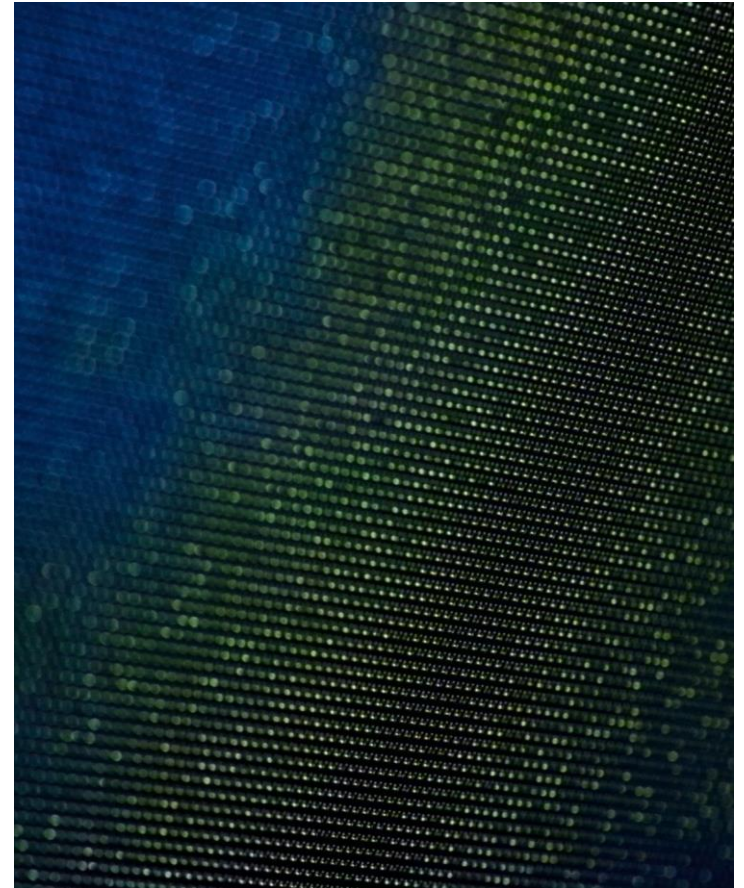
๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
๓. การบริหารจัดการทรัพยากรสารสนเทศ
๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด
๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง
๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายมาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

แบ่งเป็น
2 ฉบับ

นโยบายในการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศของรัฐสภา

แนวปฏิบัติในการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศของรัฐสภา



นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

วัตถุประสงค์

ISO/IEC 27001 : 2013

1. เพื่อให้มีนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นกรอบในการกำหนดมาตรฐาน ขั้นตอนปฏิบัติงาน ผู้รับผิดชอบ และใช้งานระบบรักษาความมั่นคงปลอดภัยของสารสนเทศ รัฐสภา
2. เพื่อกำหนดให้มีการการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีแผนเตรียมความพร้อมสำหรับกรณีฉุกเฉิน และให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม สามารถใช้งานได้เป็นปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องตามภารกิจ
3. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ
4. เพื่อส่งเสริมให้มีการเผยแพร่ความรู้แก่บุคลากรของรัฐสภา รวมถึงบุคคลที่เกี่ยวข้อง เพื่อสร้างความเข้าใจ ให้เกิดความตระหนัก และมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

แบ่งได้ **14** หมวด

ISO/IEC 27001 : 2013

1. นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) [1]
2. โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of information security) [2]
3. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security) [4]
4. การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset management) [3]
5. การควบคุมการเข้าถึง (Access control) [7]
6. การควบคุมการเข้ารหัส (Cryptography)
7. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) [5]

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

แบ่งได้ **14** หมวด

ISO/IEC 27001 : 2013

8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) [6]
9. *ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)*
10. การจัดหา พัฒนา และการบำรุงรักษาระบบ (Systems Acquisition, Development And Maintenance) [8]
11. *ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)*
12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) [9]
13. ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management) [10]
14. การปฏิบัติตามข้อกำหนด (Compliance) [11]

นิยามคำศัพท์ (ตัวอย่าง)

“ความมั่นคงปลอดภัยของสารสนเทศ” หมายถึง การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้อง (integrity) สภาพพร้อมใช้งาน (availability) ของสารสนเทศ

“สารสนเทศ” หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐบาล

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

ใครต้องปฏิบัติตามบ้าง ?

ข้าราชการ สมาชิกสภา รวมถึงบุคคลภายนอก

หรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของรัฐบาล

และได้รับอนุญาตให้เข้าใช้งานสารสนเทศของรัฐบาล

ทุกคนที่ใช้หรือเข้าถึงระบบสารสนเทศ ทั้งภายในพื้นที่และจากภายนอก

การอนุญาตและมอบสิทธิในการเข้าถึงทุกระบบฯ ต้องดำเนินการตามนโยบายฯ และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจเกิดขึ้น

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

แบ่งความรับผิดชอบ

- 1) ผู้บริหาร (CEO) และผู้บริหารของทุกสำนักฯ
- 2) ผู้ใช้งาน (User)
- 3) ผู้พัฒนาและผู้ดูแลระบบ

กำหนดหน้าที่ความรับผิดชอบ และ เพิ่ม **SOC Manager**

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

แนวปฏิบัติฯ กำหนดหน้าที่ความรับผิดชอบ

- 1) SOC Manager (8 ข้อ)
- 2) เจ้าของระบบ/ผู้ดูแลระบบ (13 ข้อ)
 - 1) แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบ (MA หรือ เปลี่ยนแปลงระบบ) จำกัดหรือระดับสิทธิของผู้ใช้งานระบบอย่างเหมาะสม ติดตามข่าวสาร ภาวะภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ เป็นต้น)
- 3) เจ้าของข้อมูล (5 ข้อ)
 - 1) อนุมัติและตรวจทานสิทธิของผู้ใช้งานให้ถูกต้องเหมาะสม
 - 2) ตรวจสอบให้มั่นใจว่าข้อมูลที่ได้มีการระบุหรือแสดงระดับความปลอดภัยตามที่จัดระดับไว้อย่างถูกต้องและเหมาะสม
- 4) ผู้ใช้งาน (20 ข้อ)
 - 1) ต้องให้ข้อมูลประจำตัวที่ถูกต้อง สำหรับการเปิดบัญชีผู้ใช้งาน
 - 2) ต้องรับผิดชอบในการเลือกรหัสผ่าน ที่ปลอดภัย
 - 3) ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด
 - 4) ต้องแจ้งผู้ดูแลระบบ หากพบหรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต
 - 5) ไม่ล่วงล้ำเข้าไปในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต
 - 6) ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของรัฐสภาเพื่อทำธุรกิจส่วนตัว
 - 7) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์หรืออุปกรณ์ในเครื่องของรัฐสภา (ป้องกันปัญหา ลิขสิทธิ์ และอื่นๆ) รวมถึงการติดตั้ง Access Point ด้วยตนเอง
 - 8) หากพบข้อบกพร่องหรือผู้ใดกระทำการที่น่าสงสัย ให้แจ้งต่อผู้ดูแลระบบโดยทันที

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของรัฐสภา




หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

อุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากระยะไกล (บางส่วน)

- 1) อุปกรณ์ฯ ต้องรับการอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ เท่านั้น
- 2) ต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย
- 3) ไม่ควรเก็บข้อมูลสำคัญของรัฐสภาไว้บนอุปกรณ์ฯ
- 4) ข้อมูลมีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์ฯ
- 5) ระบบคอมพิวเตอร์อื่นๆ ที่ต้องการเชื่อมต่อกับระบบของรัฐสภา ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรฯ
- 6) ต้องมีการรักษาความปลอดภัยทางกายภาพ เช่น ปิดห้องทำงานฯ
- 7) การส่งซ่อมอุปกรณ์ฯ ให้สำเนาข้อมูลหรือลบข้อมูลทั้งหมดก่อนส่งซ่อม
- 8) ห้ามนำซอฟต์แวร์การควบคุมจากระยะไกล เช่น PC-Anywhere หรือ Carbon copy มาใช้กับคอมพิวเตอร์ของรัฐสภา

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

- ก่อนจ้างงาน  เป็นลายลักษณ์อักษร
- ระหว่างจ้างงาน  อบรมเพิ่มพูนความรู้/ความตระหนักรู้
- สิ้นสุดหรือเปลี่ยนการจ้าง  ถอน/เปลี่ยนแปลงสิทธิ

การตรวจสอบคุณสมบัติผู้สมัคร (ก่อนจ้าง) กระบวนการทางวินัยเพื่อลงโทษ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 4 การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

- จัดทำบัญชีสินทรัพย์สารสนเทศฯ ให้ถูกต้องและเป็นปัจจุบัน
- จัดระดับชั้นความลับ และความสำคัญต่อรัฐสภา
- ป้องกันการเปิดเผย/ย้าย/ทำลาย โดยไม่ได้รับอนุญาต

ความถี่ในการตรวจสอบ (ปีละ **1** ครั้ง) การใช้เพื่อกิจการของรัฐสภา
สิทธิการเข้าถึง/ใช้ การจัดชั้นความลับสารสนเทศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

- บริหารจัดการการเข้าถึงของผู้ใช้งาน (กำหนดบัญชีผู้ใช้งาน)
- การพิสูจน์ตัวตนและตรวจสอบสิทธิ์

ทั้งทางกายภาพ และระบบสารสนเทศ (เน้นผู้ดูแลระบบ)

กำหนดแนวปฏิบัติการบริหารจัดการรหัสผ่าน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

แนวปฏิบัติการบริหารจัดการรหัสผ่าน

- 1) รหัสผ่านเป็นวิธีพื้นฐานในการระบุตัวตน ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบข้อมูลของรัฐสภาจริง
- 2) ต้องกำหนดให้ผู้ใช้งานมีการพิสูจน์ตัวตน เพื่อป้องกันการปฏิเสธความรับผิดชอบ
- 3) ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ
- 4) เก็บรหัสผ่านไว้เป็นความลับ
- 5) ไม่ทำการใด ๆ เพื่อให้ตนเองทราบถึงบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น
- 6) ควรมีความยาวอย่างน้อย 8 ตัว มีส่วนประกอบของอักษรอักขระพิเศษหรือตัวเลขประสมกัน
- 7) รหัสผ่านของผู้ใช้งานต้องเปลี่ยนอย่างน้อยทุก 6 เดือน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

- การประเมินความเสี่ยง เพื่อบรรระดับการป้องกัน

(ไม่ใช่ทุกข้อมูลสารสนเทศ)

- การบริหารจัดการการเข้ารหัส (**key management**) และมาตรฐานอื่น ๆ

มาตรการการเข้ารหัสข้อมูล เช่น ไม่น้อยกว่า **56** บิต

การบริหารจัดการกุญแจ

- เจ้าของข้อมูลต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากล เช่น อัลกอริทึม RSA, DES, 3DES เป็นต้น และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศเพื่อให้ทราบถึงสถานะ
- อัลกอริทึมที่เรียกใช้ต้องรองรับซอฟต์แวร์ประยุกต์ที่นำไปใช้งานได้ เช่น PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

- การเข้าถึงอุปกรณ์ (ทางกายภาพ)
- การมีแผนบำรุงรักษาอุปกรณ์อย่างต่อเนื่อง
- การนำอุปกรณ์ออกนอกหน่วยงาน

ระบบไฟฟ้า บำรุงรักษาอุปกรณ์

นอกเหนือจากห้องศูนย์ข้อมูล ยังรวมถึงสำนักงาน/ห้องทำงาน*

ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็น “ชั้นลับมาก” ไว้ในที่
สามารถพบเห็นได้ง่าย และเมื่อสั่งพิมพ์เอกสารที่มีข้อมูลสำคัญต้องเก็บเอกสารทันที

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

- ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ
มีเอกสารขั้นตอนการปฏิบัติงานที่ได้บันทึกไว้เป็นลายลักษณ์อักษร
- การป้องกันโปรแกรมที่ไม่พึงประสงค์
- การสำรองข้อมูล
- การบันทึกข้อมูลล็อกและการเฝ้าระวัง
- การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ
- การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

จัดทำเอกสาร/คู่มือ

แยกเครื่องทดสอบกับการใช้งานจริง

ห้ามติดตั้งหรือถอนโปรแกรมฯ เอง

Logging and Monitoring

มาตรฐานซอฟต์แวร์ปฏิบัติงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 9 ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

- การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

การติดตามสภาพการใช้งาน วิเคราะห์ความสามารถ การบำรุงรักษาให้ใช้งานได้ดีอยู่เสมอ

- การเชื่อมต่อ/โอนย้าย/แลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอก

ป้องกันการใช้งานเครือข่าย และ แบ่งแยกเครือข่าย(ภายใน/ภายนอก)

อุปกรณ์เครือข่ายและ**Server** (ปิด **Port** ที่ไม่ได้ใช้งาน) (เน้นผู้ดูแลระบบ)

การส่งข้อความทางอิเล็กทรอนิกส์ ต้องมั่นใจว่าที่อยู่ปลายทางและการส่งข้อความถูกต้อง

ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ ระหว่างผู้ใช้งานและรัฐสภา

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของรัฐสภา

หมวดที่ 10 การจัดหา พัฒนา และการบำรุงรักษาระบบ (Systems Acquisition, Development, and Maintenance)

- การจัดหาและการพัฒนาระบบสารสนเทศใหม่
- การปรับปรุง
- การทดสอบระบบ
- การป้องกันข้อมูลรั่วไหล

จัดทำข้อกำหนดฯ

กำหนดแนวปฏิบัติการพัฒนาบบอย่างปลอดภัย

แนวปฏิบัติด้านข้อมูลในการทดสอบระบบ

(เน้นผู้ดูแลระบบ)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

- มีข้อตกลงเป็นลายลักษณ์อักษร

(NDA : Non-Disclosure Agreement)

- มีการตรวจสอบ บันทึกการปฏิบัติงาน เฝ้าระวัง และจัดทำรายงานการดำเนินงานอย่างสม่ำเสมอ

(ไม่ใช่เฉพาะตอนสิ้นสุดการดำเนินงาน)

กำหนด แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศต่อผู้ให้บริการภายนอก
และ แนวปฏิบัติด้านการบริหารจัดการการส่งมอบงานของผู้ให้บริการภายนอก

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security Incident Management)

- การบริหารจัดการสถานการณ์/เหตุการณ์

การแจ้งเหตุ/เมื่อพบจุดอ่อน/ช่องโหว่

แนวปฏิบัติการบริหารจัดการสถานการณ์ฯ ที่ไม่เพียงประสงค์หรือไม่อาจคาดคิด

- กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติฯ
- การรายงานเหตุการณ์น่าสงสัย/จุดอ่อนฯ
- การประเมินเหตุการณ์ฯ
- การตอบโต้ต่อสถานการณ์ฯ
- การเรียนรู้จากสถานการณ์
- การเก็บรวบรวมหลักฐาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของรัฐสภา

หมวดที่ 13 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

- กำหนดความต้องการด้านสารสนเทศเพื่อความต่อเนื่องในการปฏิบัติงาน
- การเตรียมอุปกรณ์ประมวลผลสำรอง

แนวปฏิบัติฯ ตามที่คณะอนุกรรมการฯ จัดทำแผนฯ

- 1) แผนรองรับสถานการณ์ฉุกเฉินของรัฐสภา (IT Contingency Plan)
- 3) แผนสำรองข้อมูลของรัฐสภา (Backup Plan)
- 4) แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)
- 5) แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของรัฐสภา

หมวดที่ 14 การปฏิบัติตามข้อกำหนด (Compliance)

- ศึกษา ตรวจสอบ ทบทวน ให้เป็นไปตามข้อกำหนดของสัญญาและกฎหมาย

กำหนดแนวปฏิบัติด้านการปฏิบัติตามข้อกำหนดของสัญญาและกฎหมาย

และ แนวปฏิบัติการสอบทานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

- กฎหมายธุรกรรมทางอิเล็กทรอนิกส์
- กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- กฎหมายลิขสิทธิ์ — เช่น โปรแกรม/ซอฟต์แวร์ต่างๆ
- กฎหมายคุ้มครองข้อมูลส่วนบุคคล

เอกสารที่อ้างอิง

นโยบาย และแนวทางปฏิบัติงานในการรักษาความมั่นคง
ปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐสภา

<https://cutt.ly/Om1lcro>



<https://cutt.ly/Rm1lh18>



ขั้นตอนการลงทะเบียนเข้าร่วมกิจกรรมโครงการพัฒนาทักษะดิจิทัล
สำหรับบุคลากรของสำนักงานเลขาธิการสภาผู้แทนราษฎร ประจำปีงบประมาณ ๒๕๖๕
กิจกรรมที่ ๘ โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕


ผ่านโปรแกรม Zoom ที่เว็บไซต์ <https://learn.parliament.go.th/>

๑. เข้าสู่ระบบจัดการเรียนการสอนออนไลน์แบบเปิด และพื้นที่การเรียนรู้ร่วมกัน

<https://learn.parliament.go.th/>



๒. กรอกชื่อ ผู้ใช้ รหัสผ่าน และคลิกปุ่ม เข้าสู่ระบบ (บัญชีรายชื่อเดียวกับระบบ PIS นะคะ)

 เข้าสู่ระบบ

ชื่อผู้ใช้

รหัสผ่าน

☐ จำชื่อผู้ใช้

เข้าสู่ระบบ

สมัครเป็นสมาชิก

ลืมรหัสผ่าน ?

๓. คลิกเพื่อเข้าสู่บทเรียน โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
และ เมื่อเข้าสู่บทเรียนได้แล้ว คลิกปุ่ม **Enrol me**



โครงการให้ความรู้ความเข้าใจ
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๐๙.๐๐-๑๖.๐๐ นาฬิกา
ในรูปแบบออนไลน์ (online) ผ่านโปรแกรม Zoom
62E695679281F1012EF 300000683

โครงการให้ความรู้ความเข้าใจการ
รักษาความมั่นคงปลอดภัยด้าน
สารสนเทศของรัฐสภา
วันอังคารที่ 29 มีนาคม 2565
เวลา 09.00-16.00 นาฬิกา

คลิกที่นี่เพื่อเข้าสู่บทเรียน

หน้าหลัก | วิชาเรียนของฉัน | Thai (th)

หน้าหลัก > รายวิชาทั้งหมด > เทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล > วันที่ 25 มีนาคม 2565 เวลา 09.00-16.00 นาฬิกา > สมัครเข้าเป็นนักเรียนในวิชานี้ > Enrolment options

Enrolment options



โครงการให้ความรู้ความเข้าใจ
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
วันอังคารที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๐๙.๐๐-๑๖.๐๐ นาฬิกา

โครงการให้ความรู้ความเข้าใจการ
รักษาความมั่นคงปลอดภัยด้าน
สารสนเทศของรัฐสภา
วันอังคารที่ 29 มีนาคม 2565
เวลา 09.00-16.00 นาฬิกา

อาจารย์: กิตติ ดุ้ยแมน

Self enrolment (นักเรียน)

No enrolment key required.

Enrol me

----- จบขั้นตอนการลงทะเบียนเรียบร้อยแล้ว -----

สรุปผล
การติดตามและประเมินผลภายหลังการฝึกอบรม
โครงการพัฒนาทักษะดิจิทัลให้แก่บุคลากรของสำนักงานเลขาธิการสภาผู้แทนราษฎร
ประจำปีงบประมาณ ๒๕๖๕

กิจกรรมที่ ๘ : โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา ฝึกอบรมในวันที่ ๒๙ มีนาคม ๒๕๖๕ เวลา ๐๙.๐๐-๑๖.๐๐ นาฬิกา ผ่านระบบออนไลน์ โดยแยกความคิดเห็น ออกเป็นแต่ละกลุ่ม ได้แก่ กลุ่มผู้บริหาร กลุ่มผู้ปฏิบัติงานเฉพาะด้านเทคโนโลยี กลุ่มผู้ทำงานด้านนโยบายและงานวิชาการ กลุ่มผู้ปฏิบัติงานอื่น

๑) เกณฑ์การใช้คะแนนของแบบสอบถาม ดังนี้

- คะแนน ๕ หมายถึง ผู้ตอบเห็นว่ามีความคิดเห็นในระดับมากที่สุด
- คะแนน ๔ หมายถึง ผู้ตอบเห็นว่ามีความคิดเห็นในระดับมาก
- คะแนน ๓ หมายถึง ผู้ตอบเห็นว่ามีความคิดเห็นในระดับปานกลาง
- คะแนน ๒ หมายถึง ผู้ตอบเห็นว่ามีความคิดเห็นในระดับน้อย
- คะแนน ๑ หมายถึง ผู้ตอบเห็นว่ามีความคิดเห็นในระดับน้อยที่สุด

๒) เกณฑ์การพิจารณาค่าเฉลี่ยของน้ำหนักคะแนนความคิดเห็น ดังนี้

- ๔.๕๑ – ๕.๐๐ หมายถึง มีความคิดเห็นในระดับมากที่สุด
- ๓.๕๑ – ๔.๕๐ หมายถึง มีความคิดเห็นในระดับมาก
- ๒.๕๑ – ๓.๕๐ หมายถึง มีความคิดเห็นในระดับปานกลาง
- ๑.๕๑ – ๒.๕๐ หมายถึง มีความคิดเห็นในระดับน้อย
- ๑.๐๐ – ๑.๕๐ หมายถึง มีความคิดเห็นในระดับน้อยที่สุด

กลุ่มผู้บริหาร

ความคิดเห็นภายหลังการฝึกอบรม

รายการ	คะแนนเฉลี่ย	S.D	ร้อยละ	แปลผล
๑. ท่านได้นำความรู้ที่ได้รับจากการฝึกอบรมไปประยุกต์ใช้ในการปฏิบัติงานเพียงใด	๔.๖	๐.๔๙	๙๒	มากที่สุด
๒. ท่านมีแนวทางในการนำความรู้ที่ได้รับจากการฝึกอบรมมาใช้ให้เกิดประโยชน์แก่หน่วยงานเพียงใด	๔.๗	๐.๔๖	๙๔	มากที่สุด
๓. ท่านสามารถนำความรู้ที่ได้รับจากการอบรมไปใช้ในการพัฒนาหน่วยงานเพียงใด	๔.๖	๐.๖๖	๙๒	มากที่สุด
๔. ท่านได้นำองค์ความรู้ที่ได้รับจากการอบรมไปเผยแพร่หรือแลกเปลี่ยนเรียนรู้ระหว่างผู้ร่วมงานเพียงใด	๔.๖	๐.๖๖	๙๒	มากที่สุด
รวม	๔.๖๓		๙๒.๕	

ได้นำความรู้ที่ได้รับจากการฝึกอบรมไปปฏิบัติงานในด้านต่างๆ ดังนี้

๑. มอบหมายให้ผู้ได้บังคับบัญชาปฏิบัติ
๒. สื่อสารและถ่ายทอดความรู้ความเข้าใจด้านการรักษาความปลอดภัยระบบสารสนเทศไปสู่ผู้ปฏิบัติเพื่อนำไปสู่การปฏิบัติ

ข้อเสนอแนะ

๑. ควรจัดฝึกอบรมในลักษณะดังกล่าวอย่างต่อเนื่อง
๒. ควรจัดให้มีการศึกษาดูงานกับหน่วยงานที่ใช้ดิจิทัลเพื่อเพิ่มวิสัยทัศน์ที่หลากหลาย

กลุ่มผู้ปฏิบัติงานเฉพาะด้านเทคโนโลยี

ความคิดเห็นภายหลังการฝึกอบรม

รายการ	คะแนนเฉลี่ย	S.D	ร้อยละ	แปลผล
๑. ท่านได้นำความรู้ที่ได้รับจากการฝึกอบรมไปประยุกต์ใช้ในการปฏิบัติงานเพียงใด	๔.๕๐	๐.๗	๙๐	มาก
๒. ท่านมีแนวทางในการนำความรู้ที่ได้รับจากการฝึกอบรมมาใช้ให้เกิดประโยชน์แก่หน่วยงานเพียงใด	๔.๕๘	๐.๗	๙๑.๖๗	มากที่สุด
๓. ท่านสามารถนำความรู้ที่ได้รับจากการอบรมไปใช้ในการพัฒนาหน่วยงานเพียงใด	๔.๕๔	๐.๖๘	๙๐.๘๓	มากที่สุด
๔. ท่านได้นำองค์ความรู้ที่ได้รับจากการอบรมไปเผยแพร่หรือแลกเปลี่ยนเรียนรู้ระหว่างผู้ร่วมงานเพียงใด	๔.๕๐	๐.๗๙	๙๐	มาก
รวม	๔.๕๓		๙๐.๖๓	

ได้นำความรู้ที่ได้รับจากการฝึกอบรมไปปฏิบัติงานในด้านต่างๆ ดังนี้

๑. ใช้งานคอมพิวเตอร์และระบบงานต่าง ๆ ได้อย่างปลอดภัย
๒. ได้รับความรู้เพิ่มเติมเพื่อใช้ประกอบการปฏิบัติงาน และพัฒนาระบบงาน
๓. รับทราบนโยบายและแนวทางในการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา
๔. รับทราบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๕. รับทราบวิธีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security คอมพิวเตอร์) เพื่อใช้ในการดำเนินงานของตนเองภายใต้ข้อกำหนดของกฎหมาย
๖. นำความรู้มาปรับใช้ในเรื่องการใช้คอมพิวเตอร์ Pc และ Smart Phone ในการทำงานให้ปลอดภัยทางไกลไวรัส และป้องกันตนเองต่อการทำผิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๗. การทำ Hardening และติดตั้ง Certificate ระบบงาน

๘. ปฏิบัติงานเกี่ยวกับการดูแลเครื่องแม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ และงานอื่นๆ ที่ได้รับมอบหมาย
๙. ศึกษา รวบรวมข้อมูลเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศ
- ข้อเสนอแนะ
๑. อยากให้มีอบรมเกี่ยวกับเทคโนโลยีบ่อยๆ

กลุ่มผู้ทำงานด้านนโยบายและงานวิชาการ

ความคิดเห็นภายหลังการฝึกอบรม

รายการ	คะแนนเฉลี่ย	S.D	ร้อยละ	แปลผล
๑. ท่านได้นำความรู้ที่ได้รับจากการฝึกอบรมไปประยุกต์ใช้ในการปฏิบัติงานเพียงใด	๔.๑๐	๐.๕๖	๘๑.๙๓	มาก
๒. ท่านมีแนวทางในการนำความรู้ที่ได้รับจากการฝึกอบรมมาใช้ให้เกิดประโยชน์แก่หน่วยงานเพียงใด	๔.๐๒	๐.๖	๘๐.๔๕	มาก
๓. ท่านสามารถนำความรู้ที่ได้รับจากการอบรมไปใช้ในการพัฒนาหน่วยงานเพียงใด	๔.๑๖	๐.๖๕	๘๓.๑๘	มาก
๔. ท่านได้นำองค์ความรู้ที่ได้รับจากการอบรมไปเผยแพร่หรือแลกเปลี่ยนเรียนรู้ระหว่างผู้ร่วมงานเพียงใด	๔.๔๙	๐.๖๕	๘๙.๗๗	มาก
รวม	๔.๑๙		๘๓.๘๔	มาก

ได้นำความรู้ที่ได้รับจากการฝึกอบรมไปปฏิบัติงานในด้านต่างๆ ดังนี้

๑. การปฏิบัติงานจริงในการประชุมรัฐสภาระหว่างประเทศ หรือการประชุมอื่นๆ ที่เกี่ยวข้อง
๒. การรักษาข้อมูลของคณะกรรมการการป้องกันและปราบปรามการทุจริตแห่งชาติให้มีความมั่นคงปลอดภัย
๓. นำความรู้มาใช้ในการปฏิบัติงาน ดูแลรักษา เครือข่ายระบบงานของหอสมุดรัฐสภา
๔. ได้นำความรู้ด้านการรู้เท่าทันด้านดิจิทัล การระมัดระวัง ในชีวิตประจำวัน และความเสี่ยงของสื่อต่างๆ ก่อนนำไปปรับใช้กับการเผยแพร่ข่าวสารประชาสัมพันธ์ผ่านทางสื่ออิเล็กทรอนิกส์ Facebook สภาสาร ให้มีความปลอดภัยสูงสุด
๕. มีการตรวจสอบ ข้อมูล และแหล่งที่มาของข้อมูล ก่อนที่จะนำข้อมูลมาใช้ในการออกแบบ
๖. การหน้าที่ฝ่ายเลขานุการคณะกรรมการการป้องกันและปราบปรามการทุจริตแห่งชาติและสาธารณภัย สภาผู้แทนราษฎร ในส่วนที่เกี่ยวข้องกับการใช้งานอุปกรณ์คอมพิวเตอร์และระบบเครือข่ายของรัฐสภา ซึ่งได้ติดตั้งไว้ประจำกลุ่มงาน
๗. ปฏิบัติงานเกี่ยวกับระบบสารสนเทศตามหลักเกณฑ์ความปลอดภัยทางไซเบอร์
๘. การบันทึกข้อมูลการทำงาน ให้เกิดความปลอดภัยทางข้อมูล
๙. ป้องกันการโจมตีจากเว็บไซต์อื่นได้

ข้อเสนอแนะ

๑. ควรมีการฝึกอบรมที่เน้นการฝึกอบรมเชิงปฏิบัติการให้มากขึ้น

กลุ่มผู้ปฏิบัติงานอื่น

ความคิดเห็นภายหลังการฝึกอบรม

รายการ	คะแนนเฉลี่ย	S.D	ร้อยละ	แปลผล
๑. ท่านได้นำความรู้ที่ได้รับจากการฝึกอบรมไปประยุกต์ใช้ในการปฏิบัติงานเพียงใด	๔.๕๖	๐.๖	๙๑.๑๙	มากที่สุด
๒. ท่านมีแนวทางในการนำความรู้ที่ได้รับจากการฝึกอบรมมาใช้ให้เกิดประโยชน์แก่งานเพียงใด	๔.๕๔	๐.๕๖	๙๐.๗๕	มากที่สุด
๓. ท่านสามารถนำความรู้ที่ได้รับจากการอบรมไปใช้ในการพัฒนาหน่วยงานเพียงใด	๔.๕๖	๐.๖	๙๑.๑๙	มากที่สุด
๔. ท่านได้นำองค์ความรู้ที่ได้รับจากการอบรมไปเผยแพร่หรือแลกเปลี่ยนเรียนรู้ระหว่างผู้ร่วมงานเพียงใด	๔.๒๕	๐.๖๓	๘๔.๙๓	มาก
รวม	๔.๔๗		๘๙.๔๙	มาก

ได้นำความรู้ที่ได้รับจากการฝึกอบรมไปปฏิบัติงานในด้านต่างๆ ดังนี้

๑. การใช้งานคอมพิวเตอร์อย่างปลอดภัย
๒. ได้ศึกษาและเรียนรู้เกี่ยวกับระบบความปลอดภัยเพิ่มมากขึ้น
๓. รับทราบแผน และแนวทางในการเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภามากขึ้น
๔. นำมาใช้ในการรักษาความปลอดภัยของข้อมูลในการปฏิบัติงาน
๕. จัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ เผยแพร่ความรู้ให้แก่บุคคลต่าง ๆ ในสำนัก
๖. สแกนไวรัสก่อนเริ่มทำงาน ติดตั้งโปรแกรมที่อาจทำให้เครื่องติดไวรัส
๗. นำความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาประยุกต์ใช้ในการดูแล รักษาความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

ข้อเสนอแนะ

๑. เนื่องจากมีการปฏิบัติงานจำนวนมาก ทำให้ไม่มีเวลาในการฝึกอบรม อยากให้จัดเป็นรุ่นหลาย ๆ รุ่น เพื่อได้เลือกการฝึกอบรม
๒. เป็นการอบรมที่มีประโยชน์ต่อการทำงานอย่างมาก