

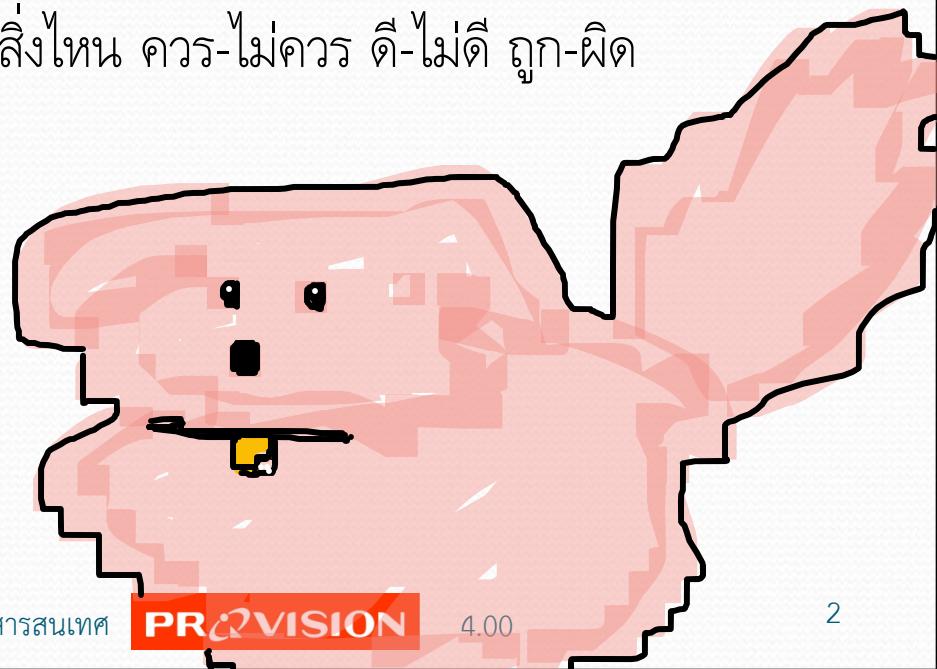
บทที่ 12

จริยธรรมและความปลอดภัย

บทที่ 12 จริยธรรมและความปลอดภัย

● ความหมายของจริยธรรม

- แบบแผนความประพฤติ หรือความมีสามัญญาณีกต่อสังคมในทางที่ดี
- ไม่มีกฎเกณฑ์ตายตัวขึ้นอยู่กับกลุ่มสังคมหรือการยอมรับในสังคมนั้นเป็นหลัก
- เกี่ยวข้องกับการคิดและตัดสินใจได้ว่าสิ่งไหน ควร-ไม่ควร ดี-ไม่ดี ถูก-ผิด

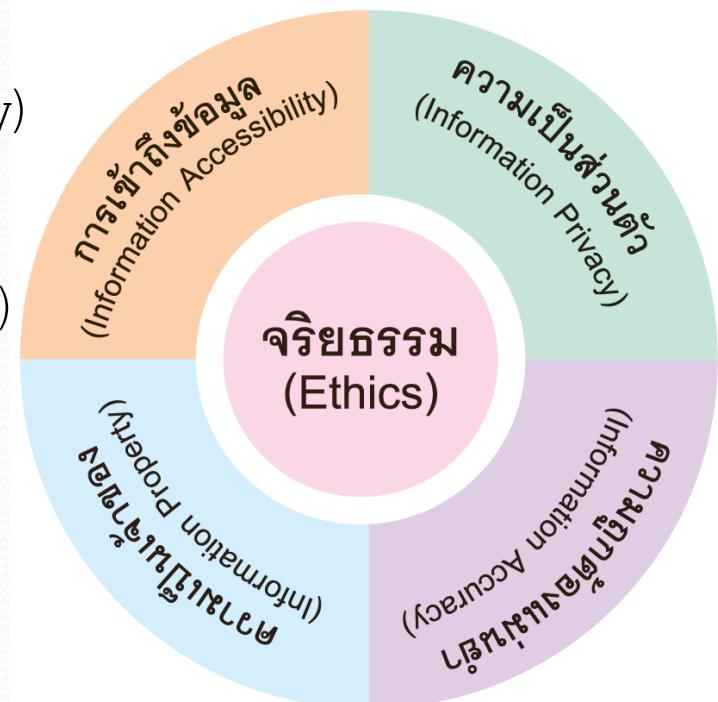


จริยธรรมกับภูรະเบี้ยบ

- “มีจริยธรรม” มีสามัญสำนึกดี ประพฤติปฏิบัติดี ไม่ก่อให้เกิดผลเสียหาย ต่อสังคมโดยรวม
- “ขาดจริยธรรม” มีรูปแบบการประพฤติหรือปฏิบัติงานที่ไม่มีประโยชน์ หรืออาจส่งผลไม่ดีต่อสังคม
- การควบคุมให้คนมีจริยธรรมที่ดี อาจใช้ข้อบังคับ กฎ หรือระเบียบของสังคม มาเป็นส่วนสนับสนุนให้เกิด “จริยธรรมที่ดี” ได้

จริยธรรมกับสังคมยุคสารสนเทศ

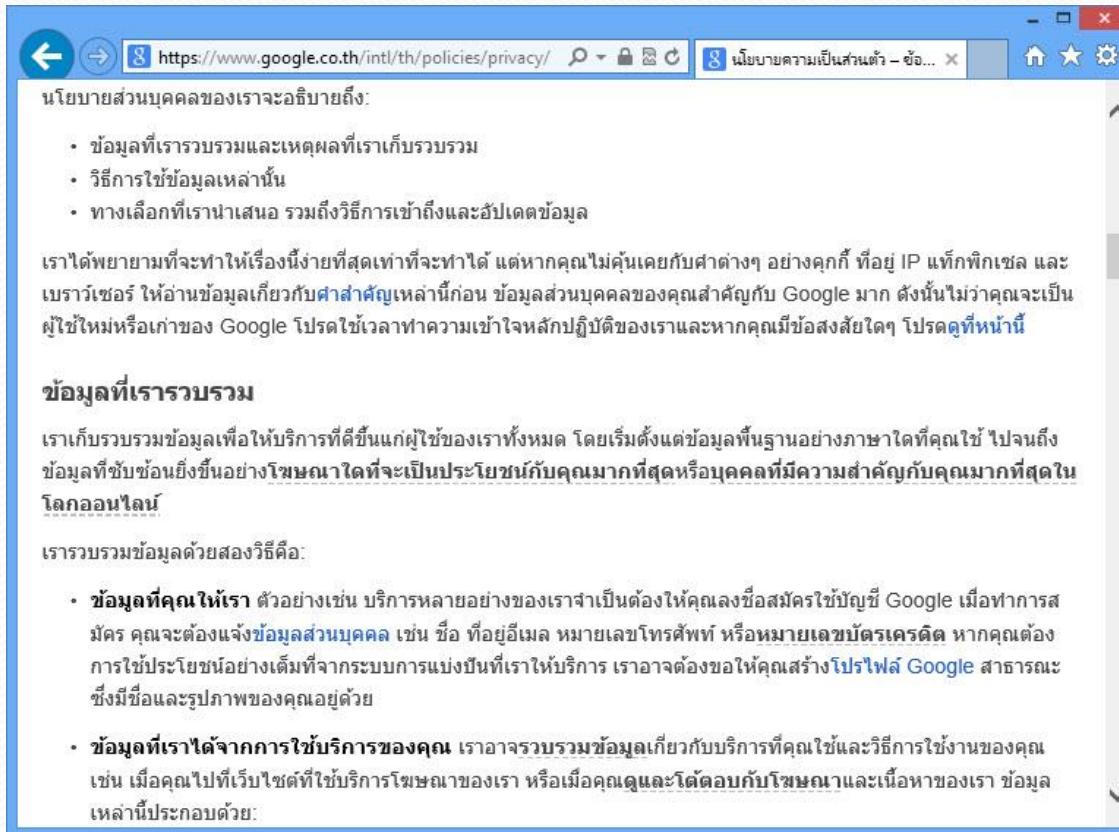
- ตั้งอยู่บนพื้นฐาน 4 ประเด็นคือ
 - ความเป็นส่วนตัว (Information Privacy)
 - ความถูกต้องแม่นยำ (Information Accuracy)
 - ความเป็นเจ้าของ (Information Property)
 - การเข้าถึงข้อมูล (Information Accessibility)



ความเป็นส่วนตัว (Information Privacy)

- ความเป็นส่วนตัว หมายถึง สิทธิส่วนตัวของบุคคล หน่วยงาน หรือองค์กร ที่จะคงไว้ซึ้งสารสนเทศที่มีอยู่นั้น เพื่อตัดสินใจได้ว่าจะสามารถเปิดเผยให้ผู้อื่น นำไปใช้ประโยชน์ต่อหรือเผยแพร่ได้หรือไม่
- การละเมิดความเป็นส่วนตัว เช่น
 - ใช้โปรแกรมติดตามและพฤติกรรมผู้ที่ใช้งานบนเว็บไซต์
 - การเอาจานข้อมูลส่วนตัว รวมถึงอีเมลของสมาชิกส่งไปให้กับบริษัทผู้รับทำโฆษณา
 - ฯลฯ

ความเป็นส่วนตัว (ต่อ)



นนโยบายส่วนบุคคลของเราจะอธิบายถึง:

- ข้อมูลที่เรารวบรวมและเหตุผลที่เราเก็บรวบรวม
- วิธีการใช้ข้อมูลเหล่านั้น
- ทางเลือกที่เรา奉าเสนอ รวมถึงวิธีการเข้าถึงและอปเปเดตข้อมูล

เราได้พยายามที่จะทำให้เรื่องนี้ง่ายที่สุดเท่าที่จะทำได้ แต่หากคุณไม่คุ้นเคยกับคำศัพท์ อย่างเช่น ที่อยู่ IP แท็กพิกเซล และเบราว์เซอร์ ให้อ่านข้อมูลเกี่ยวกับ **ค่าสำคัญเหล่านี้ก่อน** ข้อมูลส่วนบุคคลของคุณสำคัญกับ Google มาก ดังนั้นไม่ว่าคุณจะเป็นผู้ใช้ใหม่หรือเก่าของ Google โปรดใช้เวลาทำความเข้าใจหลักปฏิบัติของเราระหว่างคุณมีข้อสงสัยใดๆ โปรดคุยกันหน้านี้

ข้อมูลที่เรารวบรวม

เราเก็บรวบรวมข้อมูลเพื่อให้นำมาใช้ในการที่ต้องแก้ไขข้อบกพร่องของเราทั้งหมด โดยเริ่มตั้งแต่ข้อมูลพื้นฐานอย่างภาษาใดที่คุณใช้ไปจนถึงข้อมูลที่ซับซ้อนยิ่งเช่นอย่างโฆษณาใดที่จะเป็นประโยชน์กับคุณมากที่สุดหรือบุคคลที่มีความสำคัญกับคุณมากที่สุดในโลกออนไลน์

เรารวบรวมข้อมูลด้วยสองวิธีคือ:

- ข้อมูลที่คุณให้เรา ด้วยการเขียนบัญชี Google เมื่อทำการสมัครใช้งาน คุณจะต้องแจ้งข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่อีเมล หมายเลขโทรศัพท์ หรือหมายเลขบัตรเครดิต หากคุณต้องการใช้ประโยชน์อย่างเต็มที่จากการบันทึกบัญชี Google สามารถตั้งค่า **โปรไฟล์ Google** สาธารณะ ซึ่งมีชื่อและรูปภาพของคุณอยู่ด้วย
- ข้อมูลที่เราได้จากการใช้บริการของคุณ เราอาจรวบรวมข้อมูลเกี่ยวกับบริการที่คุณใช้และวิธีการใช้งานของคุณ เช่น เมื่อคุณไปที่เว็บไซต์ที่ใช้บริการโฆษณาของเรา หรือเมื่อคุณดูและโต้ตอบกับโฆษณาและเนื้อหาของเรา ข้อมูลเหล่านี้จะถูกบันทึกโดยอัตโนมัติ

คำชี้แจงสิทธิส่วนบุคคลก่อนใช้บริการ

ความเป็นส่วนตัว (ต่อ)

● ความเป็นส่วนตัวในยุคสังคมออนไลน์ (Social Network)

- เจ้าของข้อมูลตั้งใจเปิดเผยเรื่องราวส่วนตัวเอง
- ความเป็นส่วนตัวในยุคของเครือข่ายสังคมออนไลน์ถูกมองข้ามไปมาก
- เหตุการณ์หรือกิจกรรมต่างๆถูกเปิดเผยแบบตลอดเวลา
- ผู้ไม่ประสงค์ดีอาจคุยกิตติ์ตามข้อมูลข่าวสารของเราได้
- อาจเกิดอันตรายต่อทรัพย์สินและความมั่นคงของชีวิตได้

ความถูกต้องแม่นยำ (ต่อ)

- สารสนเทศที่นำเสนอ ควรเป็นข้อมูลที่มีการกลั่นกรองและตรวจสอบความถูกต้อง และสามารถนำเอาไปใช้ประโยชน์ได้โดยไม่ส่งผลกระทบกับผู้ใช้งาน
- ตัวอย่างเช่น แหล่งข่าวทางอินเทอร์เน็ต อาจนำเสนอเนื้อหาที่ไม่ได้กลั่นกรอง เมื่อนำไปตีความและเข้าใจว่าเป็นจริง จะทำให้เกิดความผิดพลาดได้
- ผู้ใช้งานสารสนเทศควรเลือกรับข้อมูลจากแหล่งที่น่าเชื่อถือ และตรวจสอบที่มาได้

ความถูกต้องแม่นยำ (ต่อ)



▲ ตัวอย่างข้อมูลที่แชร์ต่อกันไปทางอินเทอร์เน็ต

กรมวิทยาศาสตร์การแพทย์ ได้ข่าวลือยัง นำข้าพลาสติกเก็บในรถยนต์ ไม่ก่อสารพิษ ดีมีได้ หลังทดสอบไม่พบสารก่อมะเร็งตามข่าวในโลกออนไลน์



รายงานข่าวแจ้งว่า วนี้ (2 มี.ย. 57) กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข (สธ.) นำโดย พน.อ.กีชัย มงคล อธิบดี ได้ออกมาเปิดเผยข้อมูล หลังมีข่าวลือในโลกออนไลน์ว่า การดื่มน้ำบรรจุขวด พลาสติกที่เก็บในหลังรถยนต์และจอดแข็งกลางแดดนานๆ เสี่ยงอการเป็นโรคมะเร็งต้านม และมะเร็ง อีนๆ เป็นอย่างแสเดดตะไปท้าภัยก็เขียนขวดพลาสติก จนเกิดมีสารไดออกซินปนมาด้วยนั้น ว่า ยังไม่มีหลักฐานทางวิทยาศาสตร์ยืนยันตรวจพบได้ออกซินในพลาสติก และสารเคมีต่าง ๆ ละลายออกม จำกขวดพลาสติก ทั้งในสภาวะอุณหภูมิสูง หรือสภาพการแข็งแข็ง และจากการทดลองได้ผลเป็นยืนว่า ไม่พบสารประกอบกลมไดออกซิน และพืชีปีลະลายออกมานในทกตัวอย่าง สัตว์นั้นจึงอย่างเดือนญี่ปุ่นโภคควร พิจารณาแหล่งของข่าวสารต่างๆ ที่ได้รับจากสื่อสังคมออนไลน์และตรวจสอบที่มาด้วยเพื่อให้ได้ข้อมูลที่ถูก ต้องนาเชื่อถือ

สำหรับ สารไดออกซิน (Dioxins) เป็นผลผลิตทางเคมีที่เกิดขึ้นโดยมีได้ตั้งใจ จากการเผาไหม้ที่ไม่สมบูรณ และกระบวนการการเผาไหม้อุณหภูมิสูงทุกชนิด โดยมีแหล่งมาในอาหารกลุ่มนี้คือกระบวนการการเลี้ด เหลือกษาที่มีสารคลอเร็นเป็นองค์ประกอบ ก็ได้สูงมากพอกเพื่อจะทำให้เกิดสารไดออกซินขึ้นมาได้ และขวด อุณหภูมิของน้ำในขวดที่ถูกวางไว้ในรถไม่ได้สูงมากพอที่จะทำให้เกิดสารไดออกซินขึ้นมา กัน ชนิดตอกล่าวก็ไม่เป็นไปตามธรรมชาติที่มี

▲ ข่าวที่ออกมาก็แจงความถูกต้องของเนื้อหาที่แชร์กัน

ความเป็นเจ้าของ (Information Property)

- สังคมยุคสารสนเทศมีการเผยแพร่ข้อมูลอย่างง่ายดาย มีเครื่องมือและอุปกรณ์สนับสนุนมากขึ้น
- ก่อให้เกิดการลอกเลียนแบบ ทำซ้ำ หรือละเมิดลิขสิทธิ์ (Copyright) โดยเจ้าของผลงานได้รับผลกระทบทั้งทางตรงและทางอ้อม
- ตัวอย่างเช่น การทำซ้ำหรือผลิตซ้ำเพลิง และโปรแกรมละเมิดลิขสิทธิ์

ความเป็นเจ้าของ



shutterstock

ค้นหาภาพตือกปลอกค่าลิขสิทธิ์

ภาพหั้งหมด ▾

🔍

ส่วนที่ 1 สิทธิใช้งานเนื้อหาภาพ

1. Shutterstock ให้คุณมีสิทธิ์ที่ไม่จำกัดเฉพาะแต่เพียงวัสดุเดียวและโอนต่อให้ผู้อื่นไม่ได้ในภายหลัง แก้ไข (ยกเว้นที่ห้ามไว้อ้างถึงข้อต่อไปนี้) และทำซ้ำเนื้อหาภาพทั้งโลกโดยไม่ลิขสิทธิ์ ตามที่อนุญาตไว้โดยข้อต่อไปนี้

a. สิทธิใช้งานภาพ

i. สิทธิใช้งานภาพแบบมาตรฐาน ให้สิทธิ์แก่คุณในการใช้งานภาพ:

1. ในการทำซ้ำแบบเดิมๆ ซึ่งรวมถึงแบบรีบบิลด์ ในการเผยแพร่องค์ประกอบในสื่อทางคอมพิวเตอร์ ไม่ว่าจะด้วยซอฟต์แวร์ การ์ดอิเล็กทรอนิกส์ สิ่งพิมพ์ อิเล็กทรอนิกส์ (หน้าจออิเล็กทรอนิกส์ นิตยสารอิเล็กทรอนิกส์ บล็อก ฯลฯ) และในสื่อดิจิทัล (เช่น YouTube Dailymotion Vimeo ฯลฯ โดยเป็นไปตามข้อจำกัดด้านงบประมาณที่กำหนดไว้ในรายละเอียดที่ 1.a.i.4 ด้านล่าง)
2. จัดพิมพ์ในรูปแบบที่จับต้องได้โดยเป็นสำเนาหนึ่งของบรรณกุกันท์หรือเอกสารลิขสิทธิ์ ทั้งหมดหมาย และนามบัตร โฆษณา กุญแจ บัลลังก์ ภาพปก CD และ DVD หรือในรูปแบบและรูปแบบของที่จับต้องได้ ซึ่งรวมถึงนิตยสาร หนังสือพิมพ์ และหนังสือ ภายใต้ที่ต้องไม่ทำซ้ำกัน ทำซ้ำมากกว่า 500,000 ครั้ง
3. เป็นส่วนหนึ่งของแคมเปญโฆษณาที่เรียกว่า "แคมเปญที่" ภายใต้เงื่อนไขที่ว่ามีจำนวนการทำซ้ำมากกว่า 500,000 รายการ

ข้อความประกาศแจ้งลิขสิทธิ์ในการใช้งานรูปภาพของเว็บ Shutterstock

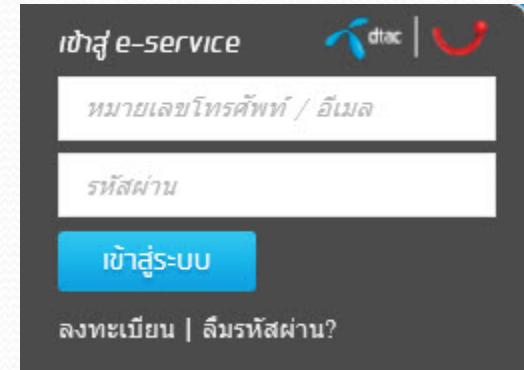
ความเป็นเจ้าของ (ต่อ)

การอนุญาตให้ใช้งาน (License)

-
- Copyright © หากมีข้อความนี้จะหมายถึงส่วนลิขสิทธิ์ ห้ามนำเอาผลงานไปใช้หรือทำซ้ำโดยเด็ดขาด นอกจากมีการขออนุญาตอย่างเป็นทางการจากเจ้าของผลงานก่อน
 - Creative Commons cc หรือเรียกว่า Copyleft © (เพื่อให้สอดคล้องกับคำว่า Copyright) เป็นการอนุญาตให้นำผลงานไปใช้ต่อยอดได้ในบางกรณี แบบมีเงื่อนไข
 - Public Domain ✘ เป็นผลงานที่ไม่ส่วนลิขสิทธิ์ จะนำไปใช้งานอะไรได้แต่ในทางปฏิบัติควรให้เครดิตเจ้าของผลงานกำกับไว้ด้วยเสมอ

การเข้าถึงข้อมูล (Information Accessibility)

- ผู้ดูแลระบบ จะเป็นผู้ที่กำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้แต่ละคน เช่น เข้าถึงข้อมูลโดยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
- ผู้ใช้ข้อมูลก็กำหนดได้ว่าจะให้ใครเห็นข้อมูลนั้นๆ บ้าง เช่น กำหนดให้สิ่งที่โพสต์บน Facebook เห็น Kong คนเดียว เห็นเฉพาะเพื่อน หรือเปิดสาธารณะ



การเข้าถึงข้อมูล (Information Accessibility) (ต่อ)

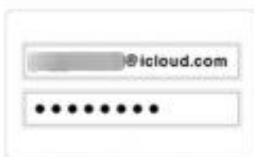
● ระบบล็อคสองขั้นตอน (Two-Step Verification)

- บางระบบมีบริการ “ล็อคสองขั้นตอน” เพื่อป้องกันผู้ไม่หวังดีแอบล็อกอินเข้าใช้บัญชีส่วนตัว
- ตัวอย่างเช่น บัญชี *Gmail* ของ *Google* หรือ บัญชี *Apple ID* บนสมาร์ตโฟนระบบ *iOS* โดยจะผูกเบอร์โทรศัพท์ไว้กับบัญชีอีเมล
- ถ้ามีการล็อกอินเข้าระบบจากคอมพิวเตอร์ หรืออุปกรณ์เครื่องอื่นที่เราไม่เคยใช้ระบบจะส่ง SMS แจ้งรหัสพิเศษมายังโทรศัพท์

การเข้าถึงข้อมูล (Information Accessibility) (ต่อ)

Two-step verification for Apple ID.

Two-step verification will require you to verify your identity using one of your devices before you can make changes to your account or make an iTunes or App Store purchase from a new device.



You enter your Apple ID and password as usual.



We send a verification code to one of your devices.



You enter the code to verify your identity and complete sign in.

Google

การลงชื่อเข้าใช้ด้วยการยืนยันแบบสองขั้นตอน



การลงชื่อเข้าใช้จะแตกต่างกัน

คุณต้องใช้รหัสยืนยัน:
หลังจากนั้น คุณต้องป้อนรหัส
ที่คุณจะได้รับผ่านทางข้อความ การให้รหัส
นี้จะช่วยให้คุณสามารถเข้าสู่ระบบได้



ใช้งานอย่างง่ายดาย

เนื่องด้วยลักษณะของคุณพ่อคุณแม่
หรือทุกคนในครอบครัว คุณสามารถจัดให้
เราไปท่องเที่ยวได้โดยไม่ต้องกังวลว่า
คุณพ่อคุณแม่ที่อยู่บ้านจะเข้าสู่ระบบได้



ช่วยป้องกันบุคคลภายนอก

คุณจะยังคงได้รับการคุ้มครอง:
เราขอสงวนสิทธิ์
พยายามลงชื่อเข้าใช้บัญชีของคุณจาก
คอมพิวเตอร์ที่คุณไม่ได้ใช้งาน

การยืนยันแบบสองขั้นตอน

ป้องกันบุคคลที่ไม่หวังดีให้ห่างจากบัญชีของคุณโดย
ใช้ทั้งรหัสผ่านและรหัสทรัพย์
ของคุณ

เริ่มการตั้งค่า »

เรียนรู้เพิ่มเติม

▲ <https://appleid.apple.com>

▲ <https://accounts.google.com/SMSAuthConfig>

อาชญากรรมคอมพิวเตอร์ (Computer Crime)

- การลักลอบนำเอาข้อมูลไปใช้โดยไม่ได้รับอนุญาต รวมถึงการสร้างความเสียหายต่อบุคคลและสังคมโดย “ผู้ไม่ประสงค์ดี” เกิดขึ้นจากการขาด “จริยธรรมที่ดี”
- บางกรณีถือว่าเป็นการกระทำที่ผิดกฎหมาย ซึ่งมีบทลงโทษแตกต่างกันไป
- ตัวอย่างของอาชญากรรมคอมพิวเตอร์ เช่น
 - การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต
 - การขโมยและทำลายอุปกรณ์
 - การใช้ซอฟต์แวร์เกือน (ละเมิดลิขสิทธิ์)
 - การก่อภัยระบบด้วยสปายแวร์
 - การก่อภัยระบบด้วยสแปมเมล
 - การหลอกลวงเหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต

- อาชญากรรมที่เกี่ยวข้องกับการลักลอบ หรืออ่านข้อมูลและนำไปใช้โดยไม่ได้รับอนุญาต
- เช่น การลักลอบเข้าไปแก้ไขข้อมูลเว็บเพจ หน้าแรกขององค์กร
- กลุ่มคนที่เกี่ยวข้อง เช่น
 - แฮกเกอร์ (Hacker) / แครกเกอร์ (Cracker)
 - สคริปต์คิดดี้ (Script Kiddie)



ตัวอย่างการเข้าไปเปลี่ยนแปลงข้อมูล

เว็บเพจหน้าแรก แทนที่หน้าเว็บเดิม

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

● แฮกเกอร์ (Hacker)

- เป็นกลุ่มคนที่มีความรู้ทางด้านคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เป็นอย่างดี
- บางคนอาจ **ไม่ได้มีเจตนา** แต่ทำเพื่อต้องการทดสอบความรู้ของตนเอง
นิยมเรียกคนกลุ่มนี้ว่า **แฮกเกอร์สายขาว** หรือ **White Hat**

白帽

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

● แครกเกอร์ (Cracker)

- เป็นกลุ่มคนที่มีความรู้ความสามารถเช่นเดียวกับกลุ่มแฮกเกอร์
- มุ่งทำลายระบบหรือลักลอบนำเอาข้อมูลนั้นไปแก้ไข เปลี่ยนแปลง หรือทำลายทิ้ง
- มักเรียกว่าเป็น แฮกเกอร์สายดำ หรือ *Black Hat*
- มีเจตนาจะใช้ข้อมูลเกิดความเสียหายมากกว่าแฮกเกอร์

(สองคำนี้บางทีก็เรียกร่วมๆ กันเป็น แฮกเกอร์ ไปเลย)

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

“ก่อน ทำการ ภัย”

● สคริปต์คิดดี (Script Kiddie)

- มักเป็นคนอยากรู้อยากรู้อยากเห็น ไม่จำเป็นต้องมีความรู้เกี่ยวกับการเจาะเข้าระบบมากนัก
- มีการเลกเปลี่ยนโปรแกรมหรือสคริปต์ (Scripts) ที่มีคนเขียนและนำออกมานำเสนอทดลองใช้กัน
- อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่สามารถใช้ เช่น การแฮกอีเมล การขโมยรหัสผ่านของผู้อื่น หรือการใช้โปรแกรมก่อภัยอย่างง่าย

การลักลอบเข้าถึงโดยไม่ได้รับอนุญาต (ต่อ)

- การลักลอบดักข้อมูลด้วยวิธี **Skimming** เป็นวิธีการที่ผู้ร้ายใช้จารกรรมข้อมูล เช่น
 - นำอุปกรณ์อ่านข้อมูลขนาดเล็กไปแนบติดตั้งไว้ตามตู้ ATM เพื่อขโมยรหัส
 - ใช้เครื่อง Skimmer แนบดึงข้อมูลบัตรเครดิต

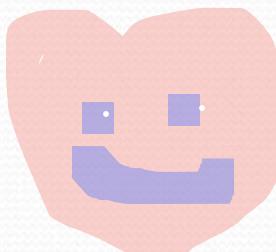


▲ บุมกดปลอมเพื่อแนบเก็บรหัสบัตร ATM



การขโมยและทำลายอุปกรณ์

- เกิดจากการไม่รอบคอบ และวางแผนอุปกรณ์ไว้ในบริเวณที่เลี้ยงต่อการโจมตีได้ง่าย
- อาจเกิดจากบุคคลภายนอกหรือภายในองค์กร
- ความมีการติดตั้งอุปกรณ์ป้องกันและรักษาความปลอดภัย ตรวจการเข้าออกของบุคคลที่มาติดต่อ รวมถึงวางแผนมาตรการในการใช้อุปกรณ์อย่างเข้มงวด



ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

PR&VISION

4.00



การใช้ซอฟต์แวร์และเมดลิขสิทธิ์

- อาจมีกฎหมายที่เกี่ยวข้องกับการขโมยเอาข้อมูลโปรแกรม รวมถึงการคัดลอกโปรแกรมโดยผิดกฎหมาย
- สามารถทำซ้ำได้ง่าย ก่อให้เกิดความเสียหายกับบริษัทผู้ผลิต
- ลักลอบทำซ้ำข้อมูลโปรแกรม และนำออกวางจำหน่ายแทนที่โปรแกรมต้นฉบับจริง
- กลุ่มผู้ผลิตมีการออกกฎหมายคุ้มครองการใช้ซอฟต์แวร์ และรวมกลุ่มกันเรียกว่า *BSA* (*Business Software Alliance*)

การใช้ซอฟต์แวร์และเมดิบลิชสิทธิ์ (ต่อ)

● กลุ่ม BSA (Business Software Alliance)

- คือกลุ่มพันธมิตรธุรกิจซอฟต์แวร์
- มีเครือข่ายครอบคลุมอยู่มากกว่า 80 ประเทศทั่วโลก
- จัดตั้งขึ้นเพื่อควบคุมและดูแลเรื่องการละเมิดลิขสิทธิ์
- รวมถึงการทำความเข้าใจกับผู้บริโภคให้ตระหนักรถึงการใช้งานโปรแกรมที่ถูกต้อง



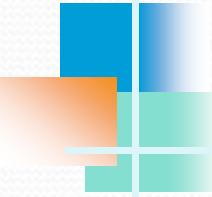
โปรแกรมมุ่งร้าย (Malicious Software)

- เป็นการใช้โปรแกรมที่มุ่งเน้นก่อความเสียหายและทำลายระบบข้อมูลคอมพิวเตอร์
- สร้างความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์เป็นอย่างมาก
- กลุ่มโปรแกรมประสงค์ร้ายต่างๆ มีดังนี้
 - ไวรัสคอมพิวเตอร์ (Computer Virus)
 - เวิร์มหรือหนอนอินเทอร์เน็ต (Worm)
 - มาโทรจัน (Trojan horses)

โปรแกรมมุ่งร้าย (Malicious Software) (ต่อ)

ไวรัสคอมพิวเตอร์ (Computer Virus)

- เขียนโดยนักพัฒนาโปรแกรมที่มีความชำนาญเฉพาะด้าน แค่ทำโปรแกรมแจกออกมามาก็ให้ไวรัสก็เอาไปใช้เบื้องต้นในระดับหนึ่ง
- การทำงานจะอาศัยคำสั่งที่เขียนขึ้นภายใต้ตัวโปรแกรมเพื่อกระจายไปยังเครื่องคอมพิวเตอร์เป้าหมาย
- แพร่กระจายโดยอาศัยคนกระทำการอย่างได้อย่างหนึ่งกับ **พำนะที่โปรแกรมไวรัสนั้น** แห่งตัวอยู่ เช่น รันโปรแกรม อ่านอีเมล เปิดดูเว็บเพจ หรือเปิดไฟล์ที่แนบมา



โปรแกรมมุ่งร้าย (Malicious Software) (ต่อ)

● เวิร์ม หรือหนอนอินเทอร์เน็ต (Worm)

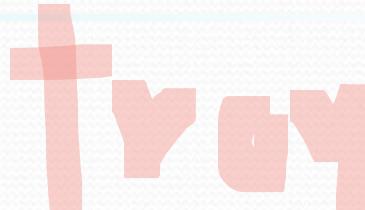
- เป็นโปรแกรมที่มีความรุนแรงกว่าไวรัสคอมพิวเตอร์
- จะทำลายระบบทรัพยากรคอมพิวเตอร์ให้มีประสิทธิภาพลดลง และไม่อาจทำงานต่อไปได้
- การทำงานจะตรวจสอบเพื่อ **โจมตีห้าเครื่องเป้าหมายก่อน** จากนั้นจะวิ่งเจาะเข้าไปเอง
- ลักษณะเด่นคือ **สามารถทำสำเนาซ้ำตัวเองได้อย่างมหาศาลภายในเวลาเพียงไม่กี่นาที**



โปรแกรมมุ่งร้าย (Malicious Software) (ต่อ)

● ม้าโทรจัน (Trojan horses)

- ทำงานโดยอาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น และจะไม่แพร่กระจายตัว
- โปรแกรมจะถูกตั้งเวลาการทำงาน หรือควบคุมการทำงานระยะไกลจากผู้ไม่ประสงค์ดี เพื่อเข้ามาทำงานยังเครื่องคอมพิวเตอร์เป้าหมายได้
- ตัวอย่างเช่น แสร้งทำเป็นโปรแกรมยูทิลิตี้ให้ใช้งาน แต่แท้จริงคือโปรแกรมอันตราย เมื่อถึงเวลา ก็จะทำงานบางอย่างทันที

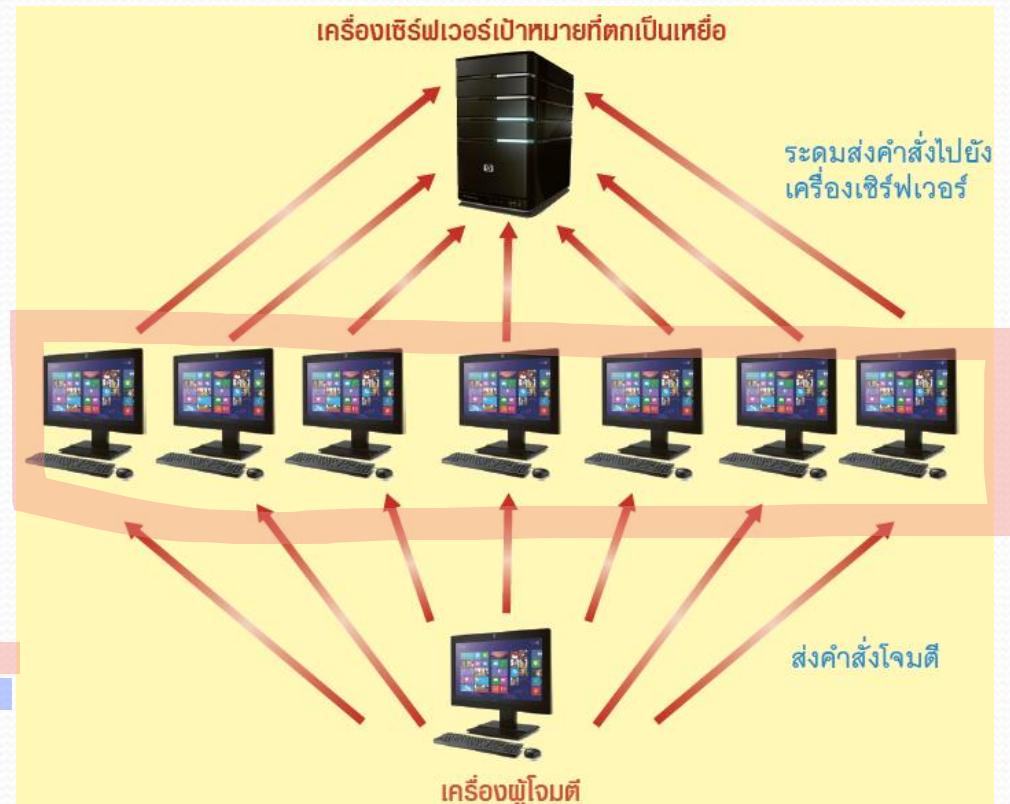


โปรแกรมมุ่งร้าย (Malicious Software) (ต่อ)

● การโจมตีเครื่องคอมพิวเตอร์ด้วยวิธี DoS (Denial of Service)

- มุ่งโจมตีเครื่องคอมพิวเตอร์ เป้าหมายด้วยการส่งข้อมูล จำนวนมหาศาล เพื่อให้เครื่อง ดังกล่าวไม่สามารถให้บริการได้ (Denial of Service)

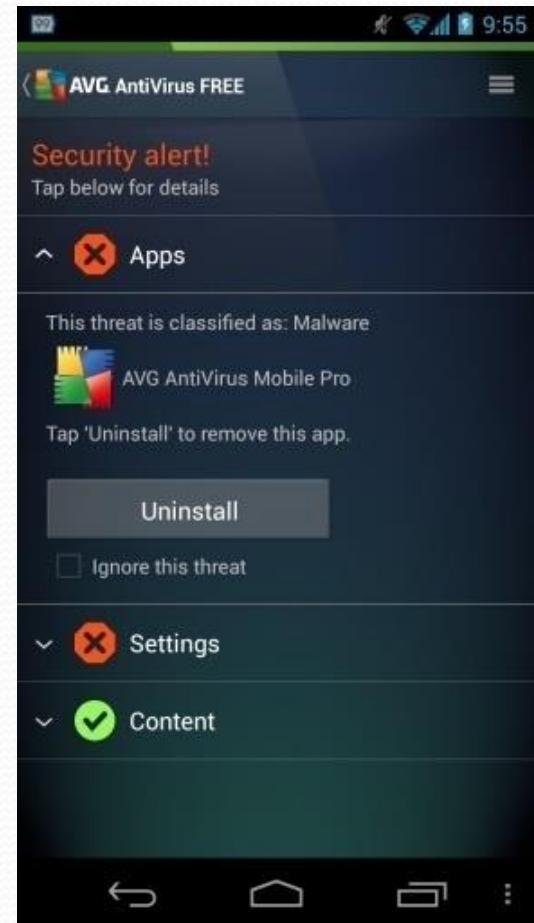
- เรียกวิธีการโจมตีเหล่านี้ว่า DoS Attack ถ้ามาจากหลายๆ แหล่งจะเรียกว่า Distributed Dos (DDoS)



โปรแกรมมุ่งร้าย (Malicious Software) (ต่อ)

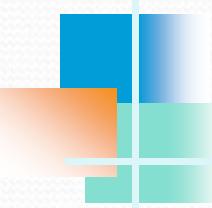
ตัวอย่างแอปพลิเคชันปลอม/ขยะบนมือถือ

- แอปพลิเคชันประเภทคีย์บอร์ด ซึ่งค่อยดักจับข้อมูลส่วนตัวที่พิมพ์ผ่านคีย์บอร์ด (Keyboard Logger) เช่น Username, Password หรือหมายเลขบัตรเครดิต
- แอปพลิเคชันสแกนไวรัส โดยแจ้งรายละเอียดว่าจะตรวจหาไวรัสบนเครื่อง แต่กลับไมyx อ้อมูล SMS บนมือถือเครื่องนั้นส่งไปยังแฮกเกอร์



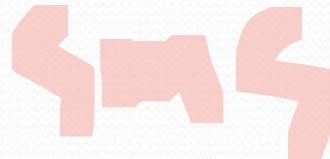
การก่อการระบบด้วยสปายแวร์ (Spyware)

- สปายแวร์ เป็นโปรแกรมประเภทสหกิจอยข้อมูล
- ไม่ได้มีความร้ายแรงต่อคอมพิวเตอร์ เพียงแต่อาจทำให้เกิดความน่ารำคาญ
- โดยปกติมักแฝงตัวอยู่กับเว็บไซต์บางประเภทรวมถึงโปรแกรมที่เจ้าให้ใช้งานฟรีทั้งหลาย
- บางโปรแกรมสามารถควบคุมการเชื่อมต่ออินเทอร์เน็ตแทรกโฆษณาหรือเปลี่ยนหน้าแรกของบราวเซอร์ได้

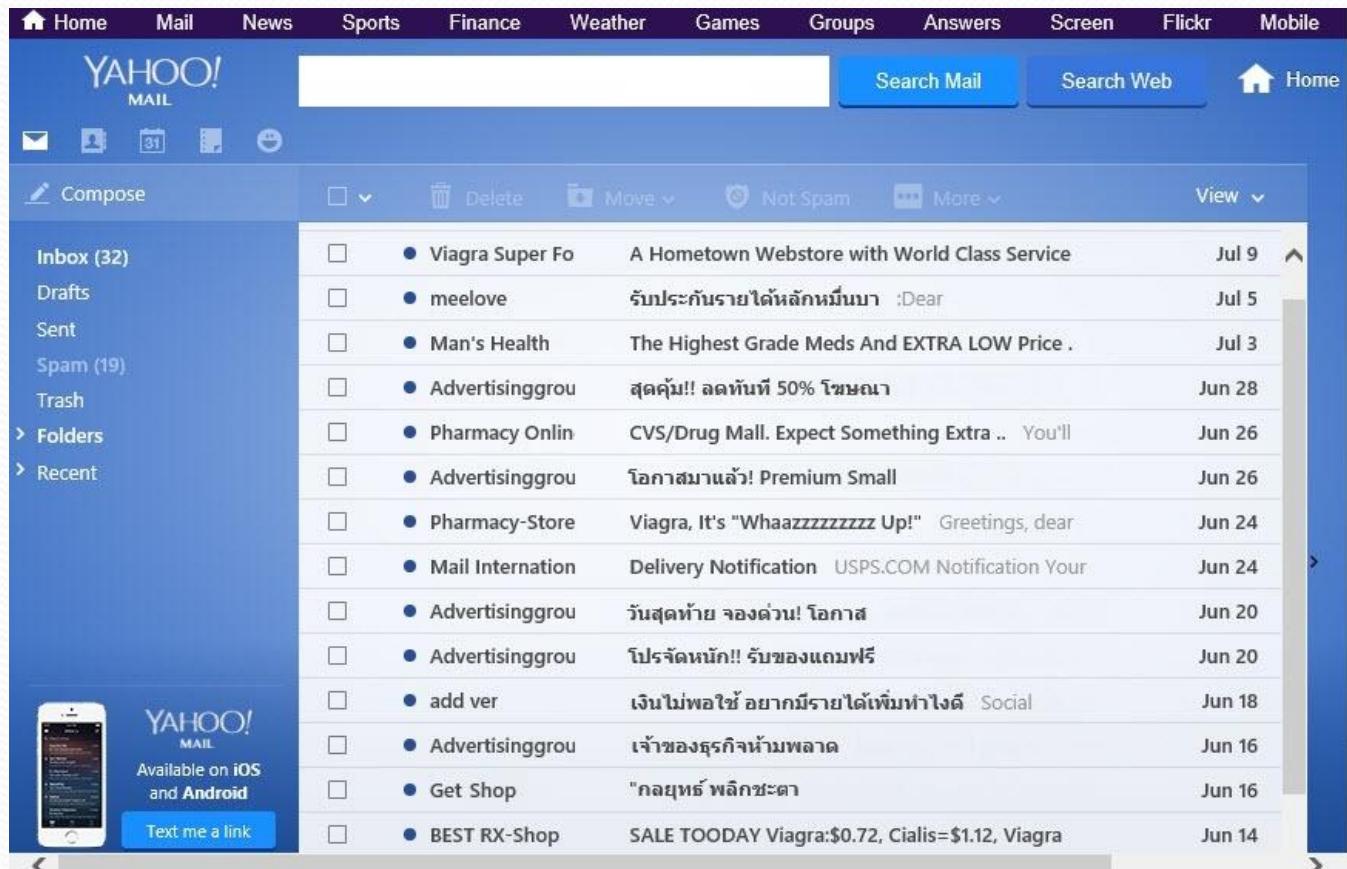


การก่อภัยระบบด้วยสแปมเมล์ (Spam Mail)

- สแปมเมล์ คือรูปแบบของอีเมลที่ผู้รับไม่ต้องการอ่าน
- วิธีการก่อภัยจะอาศัยการส่งอีเมลแบบหัวนแหะ และส่งต่อให้กับผู้รับจำนวนมาก
- อาจถูกก่อภัยโดยแฮกเกอร์ หรือเกิดจากการถูกสอดร้อยด้วยโปรแกรมประเภทสปายแวร์
- ส่วนมากเป็นเมล์ประเภทเชิญชวนให้ซื้อสินค้าหรือเลือกใช้บริการของเว็บไซต์นั้นๆ



การก่อการุณระบบทด้วยสแปมเมล (ต่อ)



การหลอกลวงเพื่อเอาข้อมูลส่วนตัว

- เป็นการหลอกลวงเพื่อล้วงข้อมูลส่วนตัว เช่น รายละเอียดหมายเลขบัตรเครดิต ชื่อผู้ใช้ หรือรหัสผ่านสำหรับใช้งานบนเว็บไซต์ โดยใช้กลวิธีต่างๆ เช่น
 - **Phishing** หลอกให้คลิกลิงก์ไปยังเว็บปลอม โดยใช้อารมณ์ที่เขียนขึ้นมาเอง หลอกลวงให้เหยื่อatyใจและหลงเชื่อการอักข้อมูลส่วนตัวในเว็บปลอมนั้น
 - **Pharming** เป็นการเข้าโฉมตีเซิร์ฟเวอร์ของเว็บไซต์ที่ตากเป็นเหยื่อ เพื่อเปลี่ยนแปลงค่าจากเครื่องเซิร์ฟเวอร์โดยตรง (DNS Hijacking หรือ DNS Redirection) โดยแก้ไขให้ DNS Server ไปเรียกลิงก์ของเว็บปลอมที่ผู้โฉมตีสร้างขึ้น เมื่อมีผู้ใช้งานเรียกใช้เว็บไซต์ที่ถูกโฉมตี ก็จะถูกส่งต่อไปยังเว็บปลอมโดยไม่รู้ตัว
- ** ผู้ใช้งานควรลังเกตชื่อ URL ว่าเรียกไปยังเว็บไซต์ที่ถูกต้อง ก่อนจะกรอกข้อมูลส่วนตัว

ตัวอย่าง Phishing

V 2 0 N



ร บ า ง 4 ห ี ท 2
ร บ า ง 4 ห ี ท 2

ปรับปรุงล่าสุด 23 พฤษภาคม 2557

แจ้งระวัง โปรแกรมโทรจัน/spyware* จาก SMS ปลอมและอีเมล์ปลอม

ห้ามคลิก ห้ามกรอกเมื่อโทรศัพท์ ห้ามติดตั้ง Application บนโทรศัพท์มือถือ/Smartphone

ด้วยช่องทางหลอกลวง



เรียน คุณใช้บริการ

เรามีมาตรการเพิ่มรักษาความปลอดภัยของผู้ใช้บริการของเราอย่างต่อเนื่อง เป็นความพยายามของเรารักษาให้ไม่เกิดข้อผิดพลาดในกระบวนการนี้ แต่หากมีการหลอกลวงจากบุคคลภายนอก ทางบริษัทฯ ขอสงวนสิทธิ์ไม่รับผิดชอบใดๆ รวมถึงความเสียหายที่อาจเกิดขึ้น ด้วยการดำเนินการทางกฎหมายและทางแพลตฟอร์มที่ได้ระบุไว้

ในปัจจุบัน อาชญากรรมออนไลน์ได้มีการใช้บริการโทรศัพท์เคลื่อนที่หรือ SMS ขโมย แอดแวร์ ไปยังบัญชีของคุณ ด้วยวิธีการหลอกลวง เช่น แจ้งเตือนว่าบัญชีของคุณมีภัยคุกคาม หรือมีการซ่อนเงื่อน ให้คุณกดติดต่อเรา หรือเข้าสู่ระบบโดยไม่ต้องรู้สึกว่ามีภัยคุกคาม ด้วยการรับรองทราบผลลัพธ์ด้วยบัญชีของคุณ

มิชั่นคือการทำงานอย่างไร?

การรับรองจะดำเนินการโดยอัตโนมัติ ไม่ต้องติดต่อเรา ระบบจะทำการตรวจสอบ และประเมินผลลัพธ์ของคุณทันที ด้วยการส่ง SMS ของเราระบุว่าคุณได้รับการรับรองแล้ว หรือไม่ ด้วยการรับรองทราบผลลัพธ์ด้วยบัญชีของคุณ

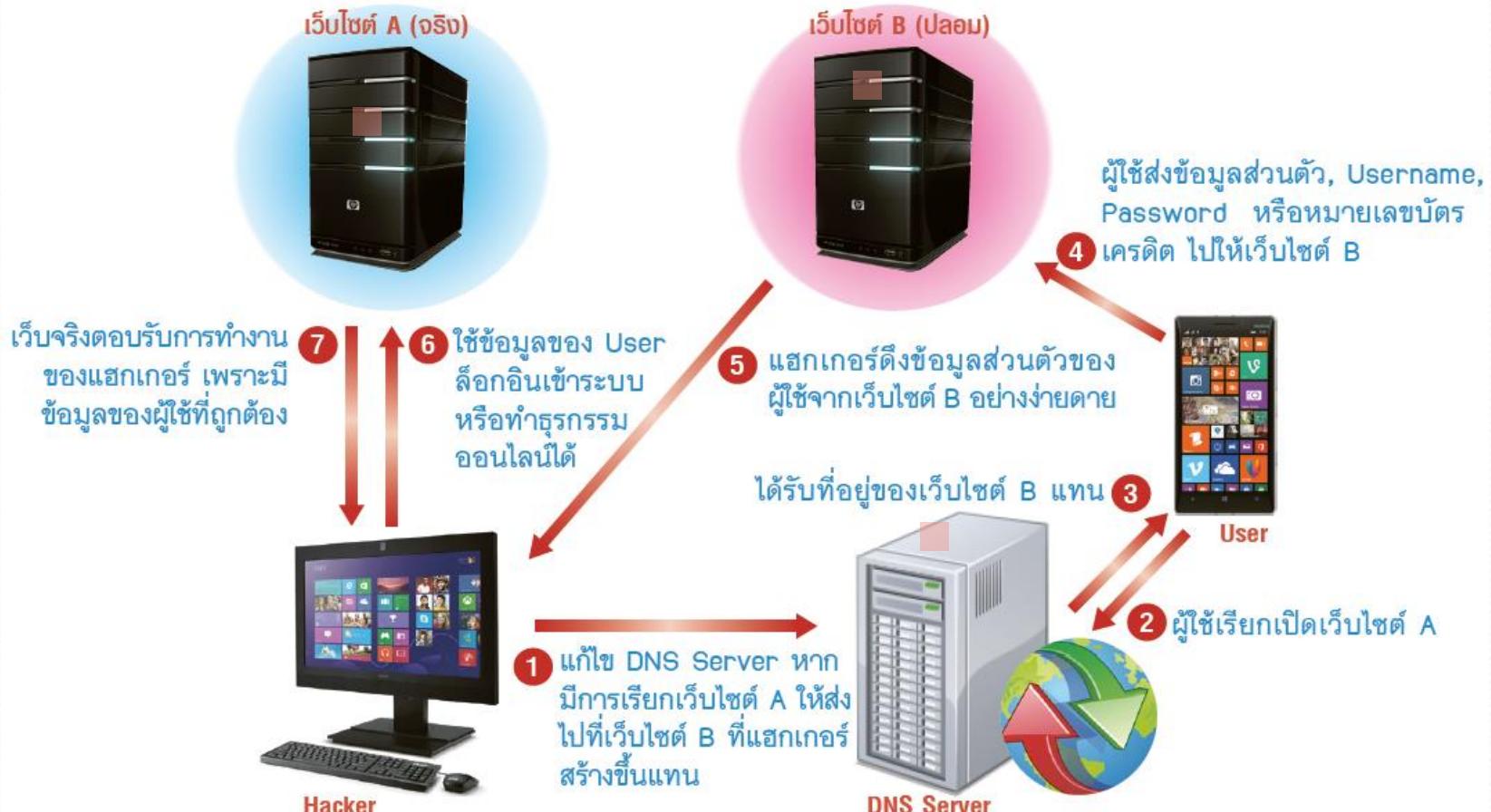
คุณต้องทำตามที่ติดต่อมาเพื่อให้เราทราบว่าคุณได้รับการรับรองแล้ว ด้วยการติดต่อเรา หรือติดต่อเราโดยอัตโนมัติ ด้วยการรับรองทราบผลลัพธ์ด้วยบัญชีของคุณ

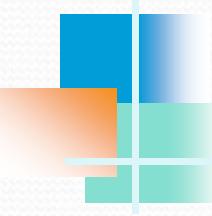
ห้ามคลิก! บุ่มไดๆ บนหน้าจอหลอกลวง

ปิด



ตัวอย่าง Pharming



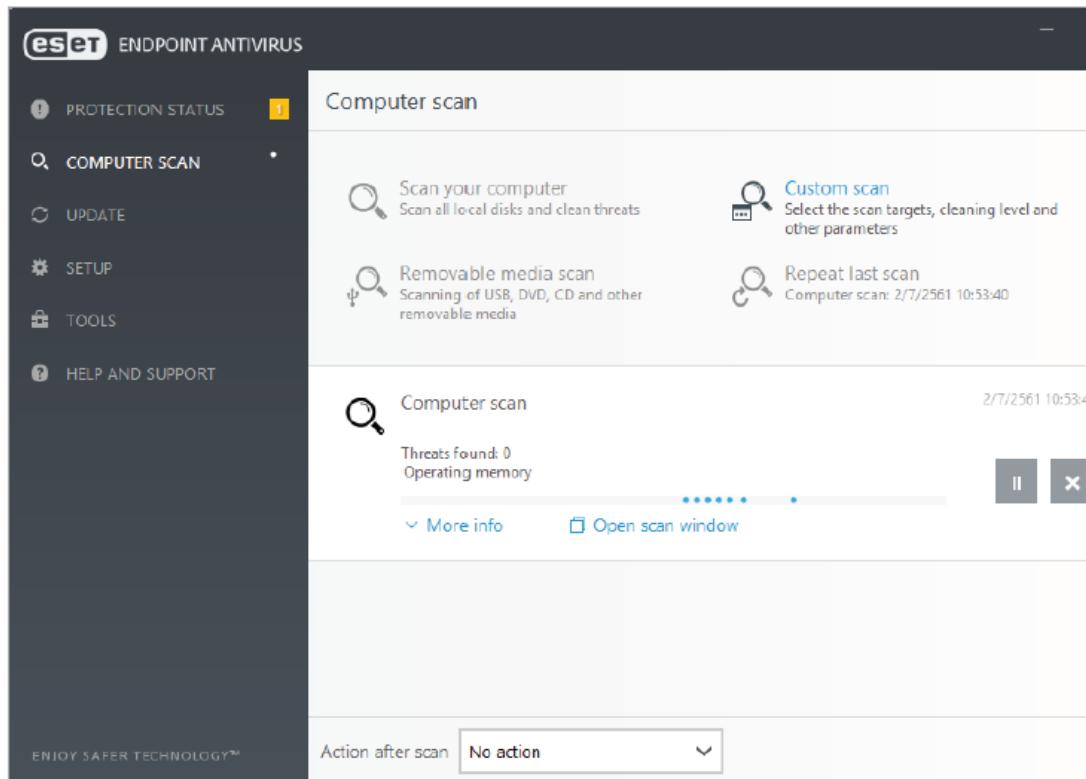


การรักษาความปลอดภัยระบบคอมพิวเตอร์

● การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Program)

- เปรียบเสมือนยา.rักษาความปลอดภัยที่มาเฝ้าดูแลบ้าน
- ทำหน้าที่คอยตรวจสอบและติดตามการบุกรุกของโปรแกรมประสงค์ร้าย เมื่อตรวจพบเจอก็สามารถกำจัดและแจ้งให้ผู้ใช้ทราบได้ทันที
- ต้องหมั่นอัพเดทโปรแกรมใหม่ข้อมูลใหม่ๆอยู่เสมอ เพื่อให้ป้องกันไวรัสได้มีประสิทธิภาพ

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

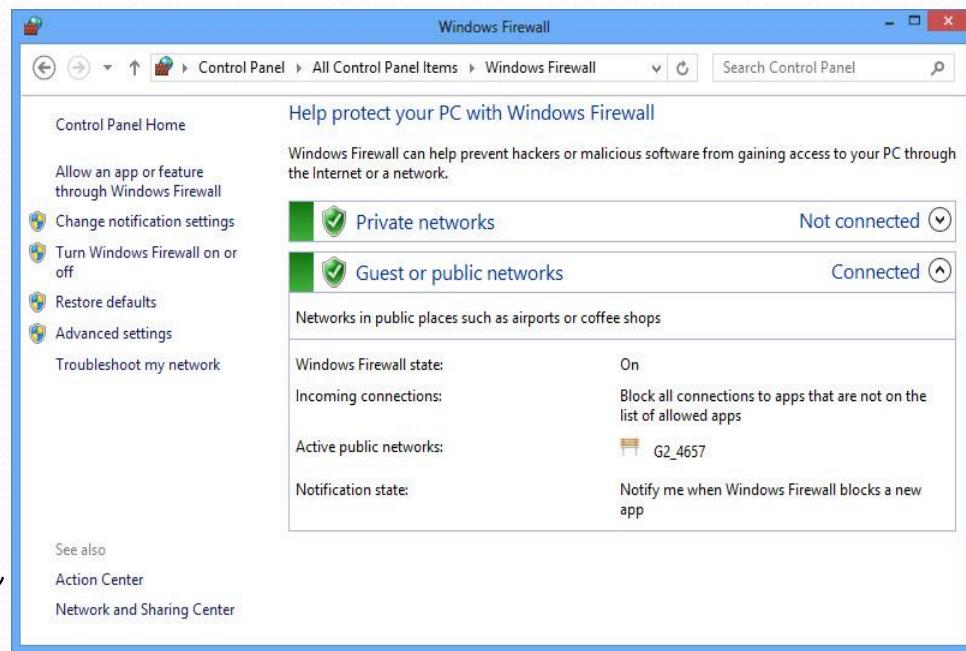


ตัวอย่างโปรแกรมป้องกันไวรัส ESET NOD32 Antivirus

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

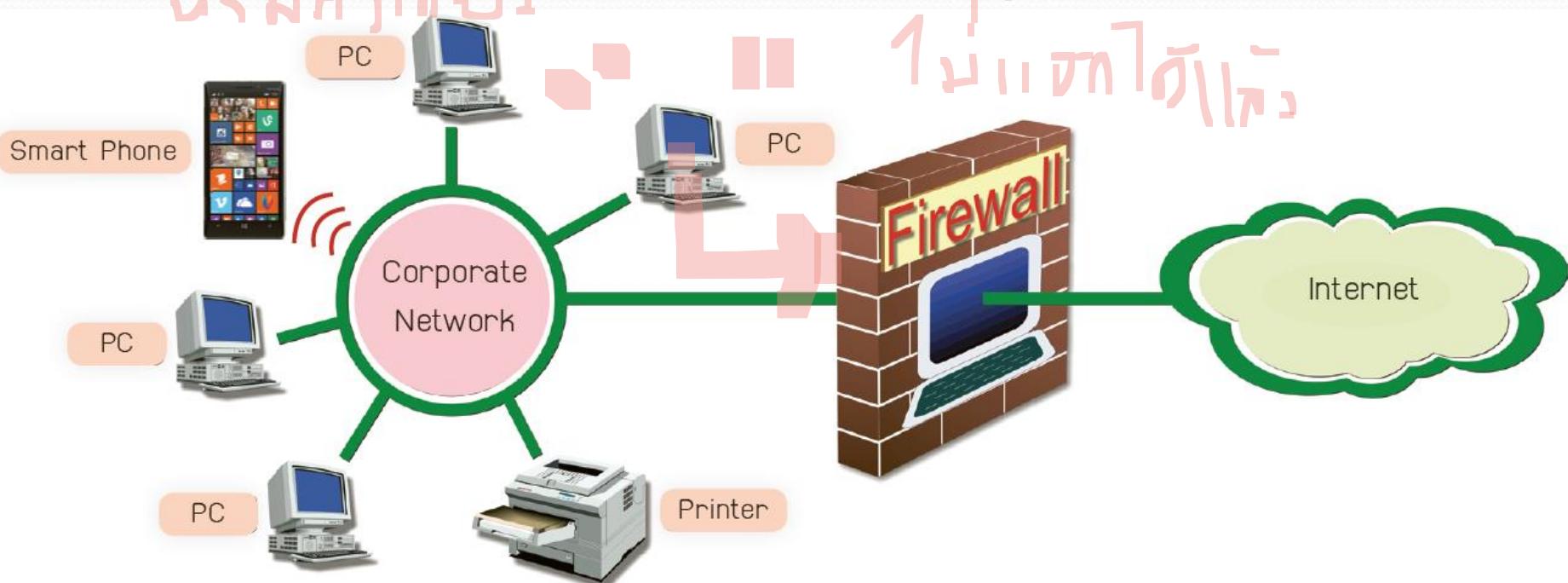
● การใช้ระบบไฟร์wall (Firewall System)

- เป็นระบบรักษาความปลอดภัยที่ป้องกันด้วยฮาร์ดแวร์หรือซอฟต์แวร์ได้
- ทำหน้าที่ดักจับ ป้องกันและตรวจสอบการบุกรุก (Intrusion)เข้าถึงระบบของผู้ไม่ประสงค์ดี
- ระบบจะให้ข้อมูลเฉพาะที่ได้รับการอนุญาตผ่านเข้าออกเท่านั้น หากไม่ตรงกับเงื่อนไขข้อมูลนั้น จะไม่สามารถผ่านเข้าออกระบบได้



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

บันทึกเข้ามา → https
บันทึก出去



ภาพแสดงการติดตั้งระบบไฟร์วอลล์สำหรับเครือข่าย

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

● การเข้ารหัสข้อมูล (Encryption)

- สำคัญสมการทางคณิตศาสตร์ที่ซับซ้อน เพื่อเปลี่ยนแปลงข้อมูลที่อ่านได้ปกติ (Plaintext) ให้เป็นรูปแบบที่ไม่สามารถอ่านได้ (Ciphertext)
- ผู้ไม่ประสงค์ดีที่แอบเอาข้อมูลไปใช้ จะไม่สามารถอ่านข้อมูลที่มีความลับนั้นได้ เพราะมีการเข้ารหัส (Encryption) ไว้
- การอ่านข้อมูลนั้นจำเป็นต้องถอดรหัสข้อมูล (Decryption) ก่อน โดยใช้กุญแจ (Key) สำหรับไข้อ่านข้อมูลนั้นๆ



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

(Plaintext)

ข้อมูลที่เป็นความลับ
Intel's Pentium4 processors
have been showing excellent
performance scalability for..



เข้ารหัส (Encrypt)

ถอดรหัส (Decrypt)

(Plaintext)

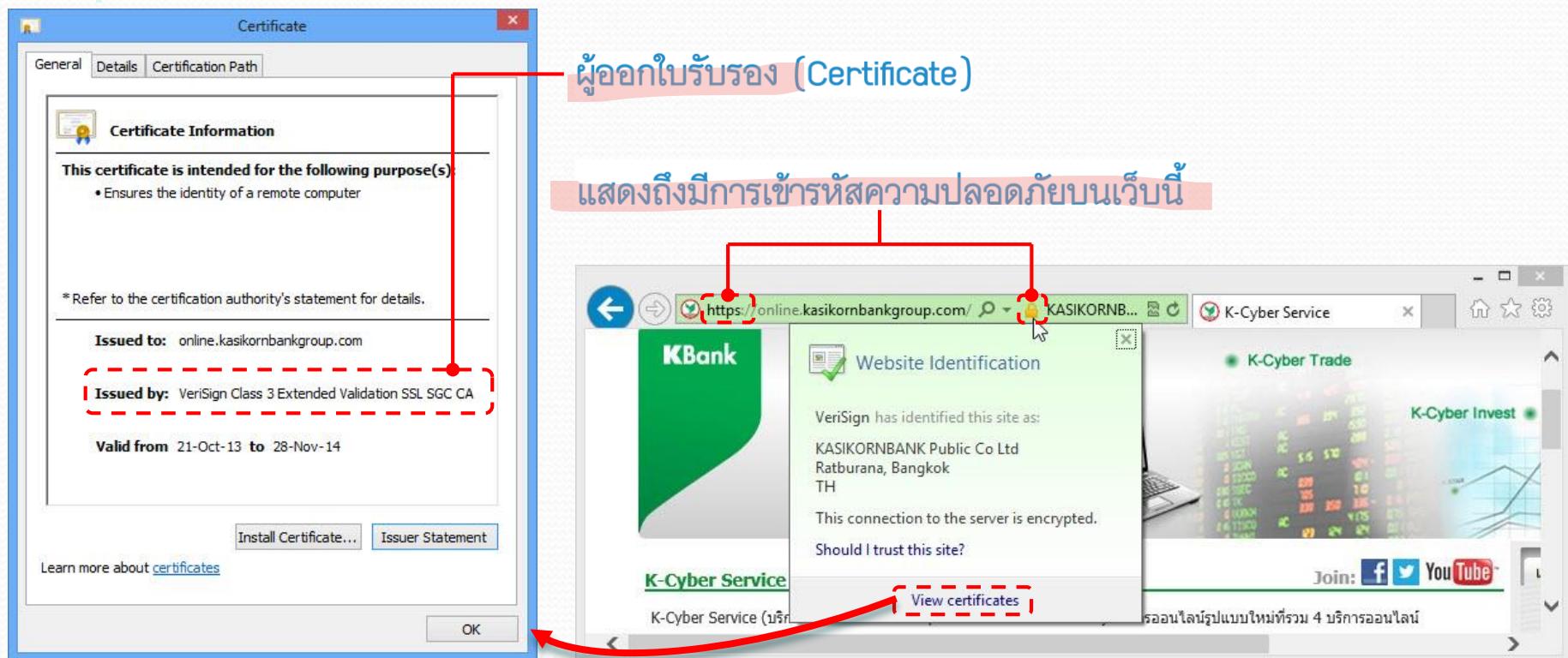
ข้อมูลที่เป็นความลับ
Intel's Pentium4 processors
have been showing excellent
performance scalability for..



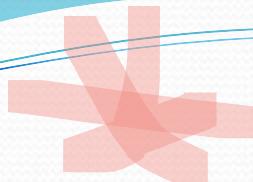
ข้อมูลที่อ่านไม่ได้ (Ciphertext)

เทคนิคการเข้าและถอดรหัสของข้อมูล

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)



ตัวอย่างหน้าเว็บที่มีการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูล



การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

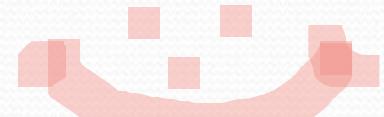
● การสำรองข้อมูล (Back up)

- คือการทำซ้ำข้อมูล ไฟล์ หรือโปรแกรมที่อยู่ในพื้นที่เก็บข้อมูล เพื่อให้สามารถนำกลับมาใช้ได้อีก กรณีที่ข้อมูลต้นฉบับนั้นเกิดสูญหายหรือถูกทำลาย
- วิธีการสำรองข้อมูลอาจทำห้องระบบหรือเครื่องบางส่วน โดยเก็บลงหน่วยเก็บบันทึกข้อมูลสำรอง เช่น ฮาร์ดดิสก์, DVD หรือเทปบันทึกข้อมูล เป็นต้น
- หากข้อมูลมีความสำคัญมากอาจต้องสำรองข้อมูลทุกวัน หรือทุกสัปดาห์ แต่หากข้อมูลนั้นมีความสำคัญระดับทั่วไป ก็อาจสำรองข้อมูลเป็นรายเดือน

การรักษาความปลอดภัยระบบคอมพิวเตอร์ (ต่อ)

● ความปลอดภัยบนสื่อสังคมออนไลน์

- ภัยจากการใช้งาน เช่น ถูกผู้ไม่หวังดีแอบเจาะระบบบัญชี Social Media ของเรา เลี้ยวโมยข้อมูลไปใช้ได้
- ภัยทางด้านสังคม เช่น ถูกหลอกลวงจากคนในสังคมออนไลน์ ทำให้เลี่ยทรัพย์สิน เลี้ยซื้อเสียง เกิดความไม่ปลอดภัยในชีวิต



พ.ร.บ. ว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์

ตาม

- กำหนดมาตรการต่างๆ เพื่อควบคุมและเอาผิดกับผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์มาแล้ว 2 ฉบับ ฉบับแรกออกในปี พ.ศ. 2550 อีกฉบับออกในปี พ.ศ. 2560 ซึ่งมีการแก้ไขและปรับบทลงโทษให้ครอบคลุมระบบอินเทอร์เน็ตและลือออนไลน์ด้วย เช่น
 - การเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันเอาไว้โดยไม่ได้รับอนุญาต
 - การทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ผู้อื่น
 - การระงับ ชั่วloth ขัดขวาง รบกวนระบบของผู้อื่นจนไม่สามารถทำงานปกติ
 - การนำข้อมูลที่บิดเบือน หรือปลอม เข้าสู่ระบบคอมพิวเตอร์
 - การนำข้อมูลเท็จที่อาจทำให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความปลอดภัยของประชาชน
 - หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ หรือทำให้เกิดความตื่นตระหนกแก่ประชาชนทั่วไป
 - การนำเข้าข้อมูลที่กระทบถึงความมั่นคงแห่งราชอาณาจักร - การก่อการร้าย

พ.ร.บ. ว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์ (ต่อ)

- การลั่งต่อข้อมูลที่เป็นความผิด (เช่น การกด Share ในลือออนไลน์) ถือเป็นการเผยแพร่ซึ่งหากข้อมูลที่แชร์นั้นมีความผิดหรือกระทบต่อผู้อื่น ผู้แชร์ก็อาจมีความผิดตามไปด้วย
- การแก้ไขเปลี่ยนแปลงทำให้ระบบทำงานไม่ปกติ ทำให้บาดเจ็บ ทรัพย์สินเสียหาย
- การนำภาพلامก่อนการเข้าสู่ระบบให้สามารถแซร์ฟต์wareชนิดนี้ได้
- การนำภาพตัดต่อ หรือดัดแปลง ที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง เข้าสู่ระบบ
- การนำเสนอภาพเยาวชนให้มีการปิดบังใบหน้า (เว้นกรณียกเว้นเชิดชูเกียรติ)
- การนำเสนอภาพผู้เสียชีวิต ในลักษณะที่ทำให้ญาติพี่น้องต้องเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย
- การส่งอีเมลหรือนำเสนอข้อมูลโดยที่ผู้รับที่ไม่ได้ร้องขอ จะต้องมีช่องทางให้แจ้งยกเลิก (unsubscribe) ได้ไม่เช่นนั้นจะถือเป็นความผิด
- ผู้ให้บริการอินเทอร์เน็ต (ISP) จะต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เอาไว้ไม่น้อยกว่า 90 วัน และกรณีที่จำเป็น อาจสั่งให้ขยายเป็น 2 ปี