





มหาวิทยาลัยราชภัฏนครปฐม



การประยุกต์เทคโนโลยีดิจิทัลสำหรับธุรกิจสตาร์ทอัพ Technology Application for Start-up Business

กศมล ชนะสุข



การรักษาความปลอดภัยดิจิทัล

5

กสมล ชนะสุข

TOPIC



- ▶ ความปลอดภัยยุคดิจิทัล
- ▶ ร่องรอยดิจิทัล
- ▶ แนวทางการป้องกันและลดร่องรอยดิจิทัล
- ▶ การพิสูจน์ตัวตน/การเข้ารหัสข้อมูล/มัลแวร์/การหลอกลวง
- ▶ ความปลอดภัยและความเป็นส่วนตัวจากการใช้อุปกรณ์
- ▶ กฎหมายดิจิทัล

ความปลอดภัยยุคดิจิทัล



ความปลอดภัยเป็นสิ่งที่ทุกคนต้องการและมีการป้องกันตนเองอยู่แล้วในชีวิตประจำวัน ไม่ว่าจะเป็นบ้านที่มีการป้องกันคือการมีรั้วรอบขอบชิด รถยนต์มีระบบป้องกันการขโมย เครื่องจักรในโรงงานอุตสาหกรรมที่ต้องมีฝ่ายซ่อมบำรุงหรือการรักษาให้สามารถทำงานได้อย่างไม่ติดขัด แต่เมื่อก้าวถึงความปลอดภัยยุคดิจิทัล ระบบหรือวิธีการที่ป้องกันในรูปแบบของข้อมูลหรือการเข้าถึง

ความปลอดภัยยุคดิจิทัล

การรักษาข้อมูลส่วนตัวอย่างไรให้ปลอดภัยในยุคดิจิทัล

การใช้เทคโนโลยีการสื่อสารผ่านดิจิทัลช่วยให้ชีวิตประจำวันของเรามีความสะดวกง่ายในการบริหารจัดการงานต่าง ๆ ทั้งเรื่องส่วนตัวเรื่องของงานซึ่งทำให้ดีขึ้นในทุกด้าน แต่อย่างไรก็ตามการติดต่อสื่อสารผ่านช่องทางดิจิทัลก็ทำให้บุคคลอื่น ๆ สามารถเข้าถึงข้อมูลส่วนตัวของเราได้ง่ายขึ้น โดยยุคการพัฒนาของเทคโนโลยียังคงมีผู้ให้ความรู้ วิธีการพื้นฐานที่การจับเก็บข้อมูลของเราให้ปลอดภัย



ความปลอดภัยยุคดิจิทัล

การรักษาข้อมูลส่วนตัวอย่างไรให้ปลอดภัยในยุคดิจิทัล

วิธีรักษาข้อมูลส่วนตัวอย่างไรให้ปลอดภัยในยุคดิจิทัล รูปแบบและวิธีการที่ไม่ยุ่งยากและมีประสิทธิภาพการรักษาความปลอดภัยของข้อมูลส่วนตัวทั้งในโลกออนไลน์ และออฟไลน์

ONLINE

อย่าเปิดเผยข้อมูลบนโซเชียลมีเดียมากเกินไป

ป้องกันระบบการเชื่อมต่อกับสัญญาณ Wifi

ติดตั้งระบบจัดการตรวจสอบไวรัส

เปลี่ยนพาสเวิร์ดเป็นประจำ

หมั่น Back Up ข้อมูล

ระวังการใช้อีเมล



OFFLINE

เก็บสำเนาเอกสารสำคัญ

เปลี่ยนพาสเวิร์ดเป็นประจำในทุกอุปกรณ์ที่จำเป็น

ปิดเครื่องทุกครั้งเมื่อไม่ใช้งาน

ทำลายเอกสารสำคัญทุกครั้ง



ร่องรอยดิจิทัล



ทุกวันนี้สิ่งที่เกิดจากการใช้หรือเปิดเข้าสู่เว็บไซต์หรือโลกออนไลน์ จะพบกับข้อมูลในสิ่งที่ค้นหาและนั่นจึงเรียกร่องรอยเท้าหรือร่องรอยการเข้าใช้ จากการนำร่องรอยข้อมูลที่ใช้ได้เคยกรอก ข้อมูลที่เกี่ยวข้องกับตนเองลงไปในเว็บไซต์หรือบริการต่าง ๆ ในโลกออนไลน์ด้วยความสมัครใจและอาจไม่ได้เกิดจากการสมัครใจ หรือเกิดจากความบังเอิญ หรือเกิดจากเจ้าของเว็บไซต์และบริการที่ผู้ใช้เคยเข้าถึงทำการเก็บข้อมูลการเข้าถึงของ ผู้ใช้ไว้ หรือเกิดจากการเก็บข้อมูลการใช้งานของผู้ใช้โดยผู้ให้บริการอินเทอร์เน็ต ซึ่งข้อมูลดังกล่าวถูกจัดเก็บไว้ให้เหลือเป็นร่องรอยของผู้ใช้อยู่บนอินเทอร์เน็ต เช่น รูปภาพ ข้อความ การบันทึกลง Social Media หรือช่องทางอื่น

ร่องรอยดิจิทัล

สิ่งที่เป็นข้อมูลพื้นฐานของร่องรอยดิจิทัล



- ภาพหรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ ที่อยู่ เลขบัตรประชาชน
- การดำเนินชีวิต และ การเป็นอยู่ของเรา
- ภาพกับเพื่อน กลุ่มต่าง ๆ
- ความสัมพันธ์กับคนต่าง ๆ ยกตัวอย่างเช่น
- เพื่อนใน Facebook (เพื่อนร่วมงาน เจ้านาย)

อันตรายของการทิ้งร่องรอยดิจิทัล



- ทดสอบค้นหาชื่อตัวเอง
- ข้อมูลมีโอกาสโดนทำสำเนาไปนับไม่ถ้วน
- อยู่ในมือผู้ไม่หวังดี
- เสียภาพพจน์และภาพลักษณ์โดยไม่อาจแก้ไขได้

แนวทางการป้องกันและลดร่องรอยดิจิทัล



การพิจารณาความเสี่ยงของการเกิดร่องรอยดิจิทัลก่อนการโพสต์รูปหรือข้อความลงในเว็บไซต์ หรือสื่อออนไลน์ต่าง ๆ ตั้งค่าเพื่อควบคุมการติดตามร่องรอยดิจิทัลในเว็บไซต์และสื่อออนไลน์ต่างๆ ผ่านทางระบบการจัดการความเป็นส่วนตัวของในแต่ละบริการ ซึ่งในระบบดังกล่าว ผู้ใช้สามารถ ควบคุมในกิจกรรมที่ผู้ให้บริการได้จัดเก็บไว้ในการเข้าใช้งานอินเทอร์เน็ตแต่ละครั้ง หากตรวจสอบพบว่าการละเมิดข้อมูลส่วนตัวให้เก็บหลักฐานที่พบ พร้อมรายละเอียดต่าง ๆ ที่เกี่ยวข้องแจ้งความที่สำนักงานตำรวจท้องที่หรือที่กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

การพิสูจน์ตัวตน/การเข้ารหัสข้อมูล/มัลแวร์/การหลอกลวง

การพิสูจน์ตัวตน

การพิสูจน์ตัวบุคคล โดยใช้หลายปัจจัย กลไกของการพิสูจน์ตัวตนสามารถแบ่งออกได้เป็น 3 คุณลักษณะ

1. สิ่งที่คุณมี กุญแจหรือบัตรเครดิต
2. สิ่งที่คุณรู้ เช่น รหัสผ่าน หรือการใช้พิน
3. สิ่งที่คุณเป็น เช่น ลายนิ้วมือ รูปแบบเรตินาหรือใช้รูปแบบ

การพิสูจน์ตัวตน



มัลแวร์



- Virus
- Worm
- Trojan Horse
- Spyware

การเข้ารหัสข้อมูล



การหลอกลวง



ความปลอดภัยและความเป็นส่วนตัวจากการใช้อุปกรณ์

ค ความเป็นส่วนตัวและความปลอดภัยบนมือถือ ซึ่งในยุคปัจจุบันเราใช้อุปกรณ์ประเภทเคลื่อนที่ได้ จัดเก็บข้อมูลสำคัญมากขึ้น อาทิเช่น รายชื่อผู้ติดต่อ รูปภาพ ภาพเคลื่อนไหว รวมทั้งเอกสารสำคัญเรื่องงานไว้บนอุปกรณ์ประเภทเคลื่อนที่มากขึ้น ทางที่ดีที่สุดควรตรวจตราการตั้งค่า ความเป็นส่วนตัวไว้เสมอเพื่อป้องกันไม่ให้ขนาดของ Digital Footprint ของเราแพร่กระจายออกไปจนควบคุมไม่ได้



กฎหมายดิจิทัล

กฎหมายดิจิทัล(Digital Law) โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.); Electronic Transactions Development Agency หรือ ETDA (เอ็ตด้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

หัวข้อเนื้อหา กฎหมายดิจิทัล

- 1) พระราชบัญญัติลิขสิทธิ์ ปี พ.ศ.2537,2558,2561
- 2) พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550,2560
- 3) พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ปี พ.ศ. 2562
- 4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี พ.ศ. 2562



การประกอบธุรกิจในปัจจุบันต้องยอมรับว่าสื่อดิจิทัลเป็นตัวจุดประกายให้เกิดธุรกิจใหม่ ๆ การสร้างความเป็นตัวตน อัตลักษณ์ การขายกระบวนการผลิต วิธีการผลิต ความเป็นมา สิ่งสร้างแรงจูงใจ สิ่งเหล่านี้ล้วนแล้วแต่ก็ให้เกิด 2 ด้าน คือ ด้านดีและด้านลบ หากมองให้รอบคอบสิ่งที่เป็นตัวกำหนดความถูกต้อง ความเป็นระเบียบในการทำธุรกิจ คงหนีไม่พ้นกฎหมายที่ออกมาเพื่อรองรับเส้นทางการทำธุรกิจให้ขึ้นไปตามรูปแบบที่ถูกต้อง

กฎหมายดิจิทัล

พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันทั่วถึงที่ สมควรกำหนดลักษณะของ ภารกิจหรือบริการที่มีความสำคัญ เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและ หน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

	ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา 70 (ตรงมาตรา 22 พ.ร.บ.คอม ปี 50,60)	เปิดเผย/ส่งข้อมูลจราจร ข้อมูลระบบคอมพิวเตอร์ ข้อมูลผู้ให้บริการ	ไม่เกิน 3 ปี	ไม่เกิน 60,000
มาตรา 71 (ตรงมาตรา 23 พ.ร.บ.คอม ปี50,60)	ประมาทเลินเล่อทำให้ผู้อื่นล่วงรู้ข้อมูลจราจร ข้อมูลระบบคอมพิวเตอร์ ข้อมูลผู้ให้บริการ	ไม่เกิน 1 ปี	ไม่เกิน 20,000
มาตรา 72 (ตรงมาตรา 24 พ.ร.บ.คอม ปี50,60)	ผู้ล่วงรู้ข้อมูลและนำไปเปิดเผยต่อ	ไม่เกิน 2 ปี	ไม่เกิน 40,000
มาตรา 73	หน่วยงานโครงสร้างพื้นฐานไม่รายงานเหตุภัยคุกคามทางไซเบอร์	-	ไม่เกิน 20,000
มาตรา 74	ไม่ปฏิบัติตามหนังสือเรียกหรือไม่ส่งข้อมูลแก่พนักงานเจ้าหน้าที่	-	ไม่เกิน 200,000

กฎหมายดิจิทัล

พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันทั่วถึงที่ สมควรกำหนดลักษณะของ ภารกิจหรือบริการที่มีความสำคัญ เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและ หน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา 75 <ul style="list-style-type: none"> ฝ่าฝืนไม่ปฏิบัติตามคำสั่งตามมาตรา 65(1),(2) การเฝ้าระวัง,การตรวจสอบผลกระทบต่อความมั่นคงปลอดภัยวิเคราะห้ ประเมินผลกระทบจากภัยคุกคามไซเบอร์ ฝ่าฝืนไม่ปฏิบัติตามคำสั่งตามมาตรา65(3),(4),(5) แก่ไขภัยคุกคามรักษาสถานะข้อมูล,การเข้าถึงข้อมูล 	- ไม่เกิน 1 ปี	ไม่เกิน 200,000 (ปรับวันละ 10,000 บาท นับแต่ครบคำสั่งให้ปฏิบัติ) ไม่เกิน 20,000 บาท
มาตรา 76 <ul style="list-style-type: none"> ขัดขวาง ไม่ปฏิบัติตามคำสั่ง ตามมาตรา 66(1),(2),(3),(4) เข้าตรวจสอบสถานที่, เข้าถึงข้อมูล/ระบบคอมพิวเตอร์, ทดสอบการทำงานของคอมพิวเตอร์, ยึดหรืออายัดคอมพิวเตอร์ 	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 77 <ul style="list-style-type: none"> การกระทำผิดเกิดจากการสั่งการจากคณะกรรมการหรือบุคคล ซึ่งรับผิดชอบในการดำเนินงานหรือบุคคลนั้นต้องสั่งการ หรือละเว้นไม่สั่งการจนเป็นเหตุกระทำผิด 	รับโทษตามบัญญัติไว้ สำหรับความผิดนั้น ๆ ด้วย	รับโทษตามบัญญัติไว้ สำหรับความผิดนั้น ๆ ด้วย

กฎหมายดิจิทัล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี พ.ศ. 2562

ประกาศ เมื่อวันที่ 24 พฤษภาคม พ.ศ. 2562

ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

เหตุผลกฎหมาย

เกิดการล่วงละเมิด สิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล

ความคุ้มครอง

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ผู้ควบคุม

ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติ แห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

บทลงโทษ

ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติหรือละเว้นการปฏิบัติ
-โทษทางอาญา
-โทษทางปกครอง

บทสรุป

การรักษาความปลอดภัยในทางดิจิทัล การปกป้องระบบและอุปกรณ์ดิจิทัลจากการบุกรุกโดยผู้ใช้ ภายนอก และจากความผิดพลาดของระบบที่เกิดจากผู้ให้บริการ การพัฒนาของเทคโนโลยีดิจิทัล และระบบออนไลน์ทำให้ผู้ใช้งานต้องบันทึกข้อมูลส่วนตัวลงในอุปกรณ์ดิจิทัลซึ่งอุปกรณ์เหล่านี้ในวัน จะเชื่อมต่อถึงกันมากยิ่งขึ้น ทั้งในอินเทอร์เน็ต ในสื่อสังคมออนไลน์และในแอปพลิเคชันที่เราใช้ในชีวิตประจำวัน จึงมีความเสี่ยงด้านความปลอดภัย การรักษาความปลอดภัยทางดิจิทัลจึงมีความสำคัญ เพื่อรักษาความเป็นส่วนตัวและความลับ ป้องกันการขโมยอัตลักษณ์ ป้องกันการโจรกรรมข้อมูล และเพื่อป้องกันความเสียหายของข้อมูลและอุปกรณ์

ทั้งนี้การใช้เทคโนโลยีการสื่อสารผ่านดิจิทัลช่วยให้ชีวิตเราทั้งง่ายขึ้นและจัดการกับเรื่องต่างๆ ได้ดีขึ้น แต่อย่างไรก็ตามการติดต่อสื่อสารผ่านช่องทางดิจิทัลก็ทำให้บุคคลอื่นๆ สามารถเข้าถึงข้อมูลส่วนตัวของเราได้ง่ายขึ้นเช่นกัน นั่นหมายความว่าหากข้อมูลของเราตกไปอยู่ในมือของผู้ที่ไม่ประสงค์ดีคือการประสงค์ร้ายก็อาจจะทำให้ข้อมูลของเราไม่ปลอดภัย เพื่อให้การดำเนินกิจการขององค์กรภาครัฐจึงได้ออกกฎหมายเพื่อคุ้มครองสำหรับผู้ใช้งานให้สามารถมั่นใจในระบบที่ได้นำมาประกอบกิจการนั่นเอง



กรณีศึกษา



การกระทำความผิดกฎหมายคอมพิวเตอร์/กฎหมายทางดิจิทัล วันที่ 3 พฤษภาคม 2565 เวลา 06.00 น.

คำถามท้ายบท

จงตอบคำถามต่อไปนี้

1. ความปลอดภัยยุค ดิจิทัล คืออะไร
2. ร่องรอยดิจิทัล (Digital Footprint) คืออะไร
3. การพิสูจน์ตัวบุคคลโดยใช้ 2 ปัจจัย มีอะไรบ้างจงอธิบาย
4. Malware คืออะไร
5. การหลอกลวง (Scam) คืออะไร
6. รหัสผ่านที่ไม่ควรตั้ง ของ **Mobile Security and Privacy** มีอะไร
7. รหัสผ่านที่ดี ของ **Mobile Security and Privacy** มีอะไร
8. จงอธิบายพระราชบัญญัติลิขสิทธิ์ ปี พ.ศ. 2537, 2558, 2561
9. จงอธิบาย พรบ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 71-74
10. จงอธิบายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี พ.ศ. 2562





อ้างอิง

<https://www.thaifintech.com/2019/05/23/automation-and-bot-will-teamwork-with-human/>

<https://www.salika.co/2019/07/03/cyber-security-thai-organization/>

<https://generali.co.th/genhealthylife/guide-to-protecting-your-personal-details/>

<https://review.thaiware.com/1822.html>

<https://sites.google.com/a/cp.ac.th/ekkarin/article/digitalfootprint>

<https://blog.pttexpresso.com/what-is-digital-footprint/>

<https://611031263article.blogspot.com/2019/07/digital-footprint.html>

<https://www.bangkokbiznews.com/lifestyle/902363>

<https://tips.thaiware.com/1245.html>

<https://www.vectorstock.com/royalty-free-vector/mobile-security-and-privacy-isometric-landing-page-vector-26089156>

<https://www.itnews24hrs.com/2014/07/password-crack-time/>

<https://sites.google.com/ska1.go.th/digitalalliteracy/>

<https://www.internetsociety.org/learning/digital-footprints/>

<https://www.one31.net/>



มหาวิทยาลัยราชภัฏนครปฐม

