



สรุปเนื้อหา บทที่ 7-12



บทที่ 7

การจดทะเบียนพาณิชย์อิเล็กทรอนิกส์

7. การจดทะเบียนพาณิชย์อิเล็กทรอนิกส์

- ▶ ประโยชน์ของการจดทะเบียน
- ▶ ใครที่ต้องจด
- ▶ จดกี่ใบ อย่างไร
- ▶ บลลงโทบ
- ▶ สิ่งที่จะได้รับ
- ▶ เครื่องหมายรับรองการจดทะเบียนพาณิชย์ (DBD Registered)

7.1. การจดทะเบียนพาณิชย์อิเล็กทรอนิกส์

- ▶ ผู้ขายสินค้าหรือบริการทางอินเทอร์เน็ต ก็งเว็บไซต์ร้านค้าออนไลน์ หรือ Social Media ต้องจดทะเบียนพาณิชย์การประกอบธุรกิจ พาณิชย์อิเล็กทรอนิกส์เพื่อให้ผู้ประกอบการแสดงตนอย่างเปิดเผย ต่อทางราชการ
- ▶ จดทะเบียนกับกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์
- ▶ ต้องข้อจดทะเบียนภายใน 30 วัน นับตั้งแต่วันเริ่มค้าขาย

7.1. การจดทะเบียนพาณิชยอิเล็กทรอนิกส์

▶ หากไม่ “จดทะเบียนพาณิชยอิเล็กทรอนิกส์” มีสิทธิถูกปรับ!!!

- การขายสินค้าออนไลน์ เป็นพาณิชยกิจที่ต้องจดทะเบียนตาม “ประกาศกระทรวงพาณิชย์ ฉบับที่ 11 พ.ศ. 2553 มาตรา 5”
- ▶ “พ.ร.บ.ทะเบียนพาณิชย์ พ.ศ.2499” กฎหมายที่กำหนดบทลงโทษในมาตรา 19 ระบุว่า
 - หาก “ร้านค้าออนไลน์” ไม่จดทะเบียนตาม พ.ร.บ. ฉบับนี้ หรือแสดงรายการเท็จ หรือไม่มาให้ นายทะเบียนพาณิชย์สอบสวน ไม่ยอมให้ถ้อยคำ หรือไม่ยอมให้ทะเบียนพาณิชย์หรือพนักงานเจ้าหน้าที่เข้าไปตรวจสอบนั้น จะต้องระวางโทษปรับไม่เกิน 2,000 บาท และให้ปรับอีกวันละ 100 บาท จนกว่าจะจดทะเบียนแล้วเสร็จ

7.1. การจดทะเบียนพาณิชย์อิเล็กทรอนิกส์

▶ ใครบ้างที่ต้องจดทะเบียนพาณิชย์อิเล็กทรอนิกส์?

1. ผู้ขายสินค้า/บริการ ผ่านระบบอินเทอร์เน็ต และ Social Media
2. ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP)
3. ผู้ให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Web Hosting)
4. ผู้ให้บริการเป็นตัวกลางในการซื้อขายสินค้า/บริการ ผ่านอินเทอร์เน็ต (E-Marketplace) เช่น Lazada Shopee ฯลฯ

7.2. ประโยชน์การจดทะเบียนพาณิชยอิเล็กทรอนิกส์

1. เพื่อให้ธุรกิจมีความน่าเชื่อถือจากการมีสถานะตัวแทนทางกฎหมาย
2. เพื่อการประโยชน์ในการกำรธุรกรรมกับหน่วยงานต่างๆ
 - ช่วยสร้างเครดิตให้กับ “ร้านค้าออนไลน์” เช่น การขอสินเชื่อเงินกู้ ยื้นหักกู้ เงินทุนหมุนเวียน หรือการขอสินเชื่อเรื่องอื่นๆ สามารถใช้ทะเบียนร้านค้า พาณิชย์เป็นหลักฐานประกอบการยื้นเอกสารทางการเงินได้
3. สร้างความมั่นใจให้ผู้บริโภค

7.2 ประโยชน์การจดทะเบียนพาณิชยอิเล็กทรอนิกส์

4. มีสิทธิในการเข้ารับการอบรม ตามหลักสูตรที่กรมพัฒนาธุรกิจการค้ากำหนด แบบไม่มีค่าใช้จ่าย
5. ช่วยให้หน่วยงานภาครัฐเก็บข้อมูลสถิติร้านค้าออนไลน์ได้ง่ายขึ้น เพื่อ
 - ดำเนินการตามนโยบายทางเศรษฐกิจได้อย่างเหมาะสม
 - การช่วยเหลือผู้ประกอบการ
 - การสนับสนุนธุรกิจออนไลน์
 - การลงทุนต่างประเทศ ฯลฯ

7.3. ขั้นตอนการยื่นจดทะเบียนพาณิชย์

▶ สถานที่ยื่น

- ผู้ขายสินค้าหรือบริการผ่านทางอونไลน์จะต้องยื่นจดทะเบียนพาณิชย์ ที่
 - สำนักงานเขตในกรุงเทพมหานคร
 - เมืองพัทยา
 - เกศบุล หรือ
 - องค์การบริหารส่วนตำบล (อบต.)

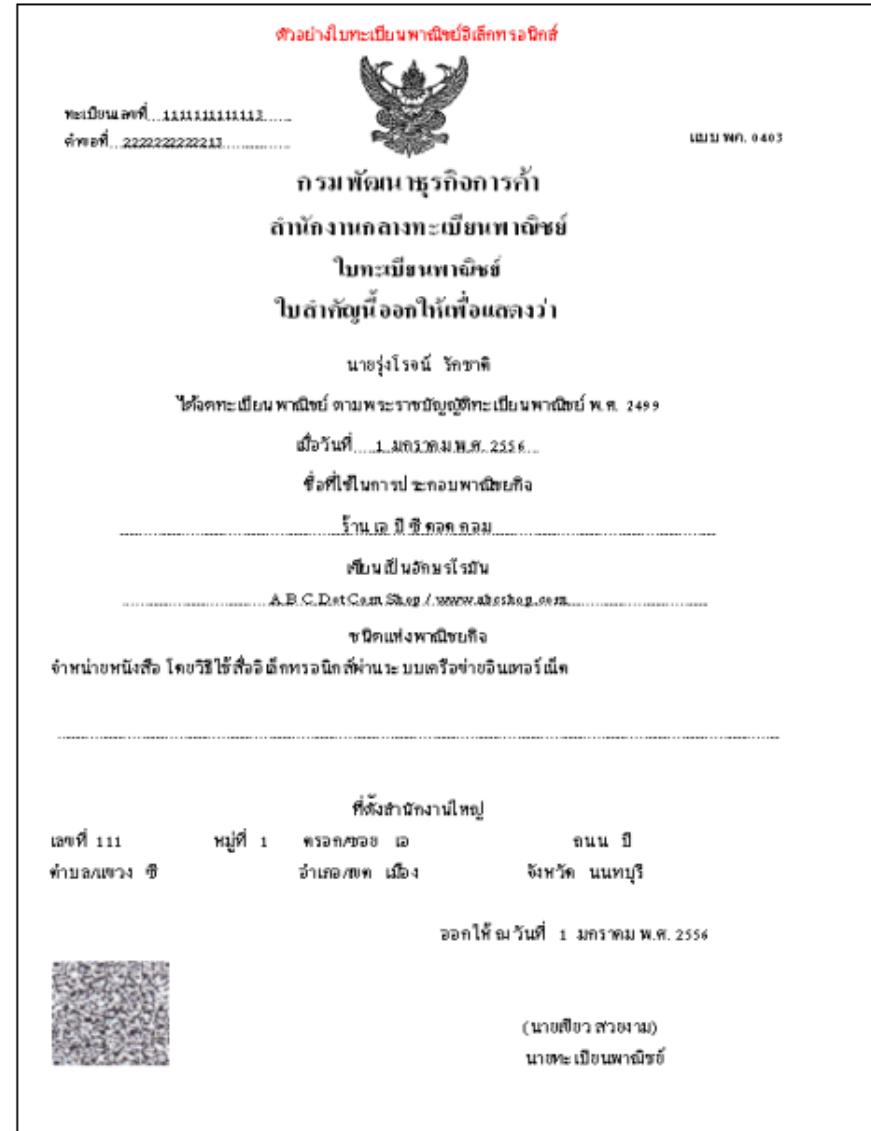
▶ ตามที่ตั้งของสถานประกอบการหรือตามที่อยู่ของผู้ขาย

7.4. เอกสารที่ใช้จดทะเบียนพาณิชย์ลึกรอบบ้าน

1. ถ้ายื่นเอกสารด้วยตนเอง ให้แสดงบัตรประจำตัวประชาชนไม่ต้องใช้สำเนาบัตรประจำตัวประชาชนและสำเนาทะเบียนบ้าน
2. แบบคำขอจดทะเบียนพาณิชย์ (แบบ กว.)
3. รายละเอียดเกี่ยวกับเว็บไซต์ (เอกสารแบบแบบ กว.) กรอก 1 ใบ ต่อ 1 เว็บไซต์
4. Print หน้าแรกของเว็บไซต์
5. วัดแผนที่ตั้งการประกอบพาณิชยกิจ
6. หนังสือรับรองการจดทะเบียนของห้างหุ้นส่วนหรือบริษัท (กรณีจดในนามบุคคล)
7. กรณีมีได้เป็นเจ้าของบ้าน (เอกสารเพิ่มเติม)
 1. หนังสือยินยอมให้ใช้สถานที่หรือสัญญาเช่า
 2. สำเนาบัตรประชาชนเจ้าของสัญญาที่พร้อมสำเนาทะเบียนบ้านหรือเอกสารสิทธิ์ที่แสดงว่าเป็นเจ้าของกรรมสิทธิ์
8. กรณีมอบอำนาจให้ผู้อื่นมาจดแทน ต้องมีหนังสือมอบอำนาจ พร้อมสำเนาบัตรประชาชนของกั้งผู้มีอำนาจและผู้รับมอบอำนาจ

7.5 เอกสารที่ได้รับ

- ▶ เมื่อจดทะเบียนพาณิชย์อิเล็กทรอนิกส์ สำเร็จ สิ่งที่จะได้รับคือ
 1. ใบทะเบียนพาณิชย์ (แบบ พค. 0403)
 2. ใบเสร็จค่าธรรมเนียม



7.6 เครื่องหมายรับรองการจดทะเบียนพาณิชย์ (DBD Registered)

- ▶ เป็นเครื่องหมายรับรองการจดทะเบียนพาณิชย์การประกอบพาณิชย์อิเล็กทรอนิกส์ของกรมพัฒนาธุรกิจการค้า
- ▶ เพื่อแสดงความมีตัวตนตามกฎหมาย ส่งผลต่อการเพิ่มความน่าเชื่อถือ
- ▶ ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือร้านค้าออนไลน์ ที่จดทะเบียนแล้วสามารถใช้เครื่องหมาย เพื่อแสดงความมีตัวตนในการประกอบธุรกิจ e-Commerce
- ▶ เครื่องหมายมีอายุการใช้งาน 5 ปี นับตั้งแต่วันที่กรม



7.7 เครื่องหมายรับรองความน่าเชื่อถือ

- ▶ เครื่องหมายรับรองความน่าเชื่อถือ (DBD Verified)
- ▶ เว็บไซต์ผ่านเกณฑ์ประเมินตามมาตรฐาน คุณภาพธุรกิจ e-Commerce ของกรมพัฒนาธุรกิจการค้า จะได้รับเครื่องหมายรับรองความน่าเชื่อถือ
- ▶ มีอายุใช้งาน 1 ปี และสามารถยืนยันต่ออายุได้คราวละ 1 ปี



7.7 เครื่องหมายรับรองความน่าเชื่อถือ

- ▶ ระดับของเครื่องหมายรับรองความน่าเชื่อถือ (DBD Verified) แบ่งเป็น 3 ระดับ คือ
 - Silver ระดับดี
 - Gold ระดับดีมาก
 - Platinum ระดับดีเด่น



7.7 เครื่องหมายรับรองความน่าเชื่อถือ

DBD
Verified
มี 3 ระดับ

 Silver	 Gold	 Platinum
ผ่านคุณสมบัติ ดังนี้ จดทะเบียนพาณิชย์สำหรับ ธุรกิจพาณิชย์อิเล็กทรอนิกส์ และได้รับเครื่องหมาย DBD Registered	ผ่านคุณสมบัติ ดังนี้ จดทะเบียนพาณิชย์สำหรับ ธุรกิจพาณิชย์อิเล็กทรอนิกส์ ไม่น้อยกว่า 1 ปี จดสิ่งบการเงิน ไม่น้อยกว่า 1 ปี	ผ่านคุณสมบัติ ดังนี้ จดทะเบียนพาณิชย์สำหรับ ธุรกิจพาณิชย์อิเล็กทรอนิกส์ ไม่น้อยกว่า 2 ปี จดสิ่งบการเงิน ไม่น้อยกว่า 2 ปี
ผ่านเกณฑ์มาตรฐานคุณภาพ ธุรกิจพาณิชย์อิเล็กทรอนิกส์	ผ่านเกณฑ์มาตรฐานคุณภาพ ธุรกิจพาณิชย์อิเล็กทรอนิกส์	ผ่านเกณฑ์มาตรฐานคุณภาพ ธุรกิจพาณิชย์อิเล็กทรอนิกส์ คุณสมบัติอื่นคือได้รับรางวัล ประกวดเว็บไซต์ e-Commerce

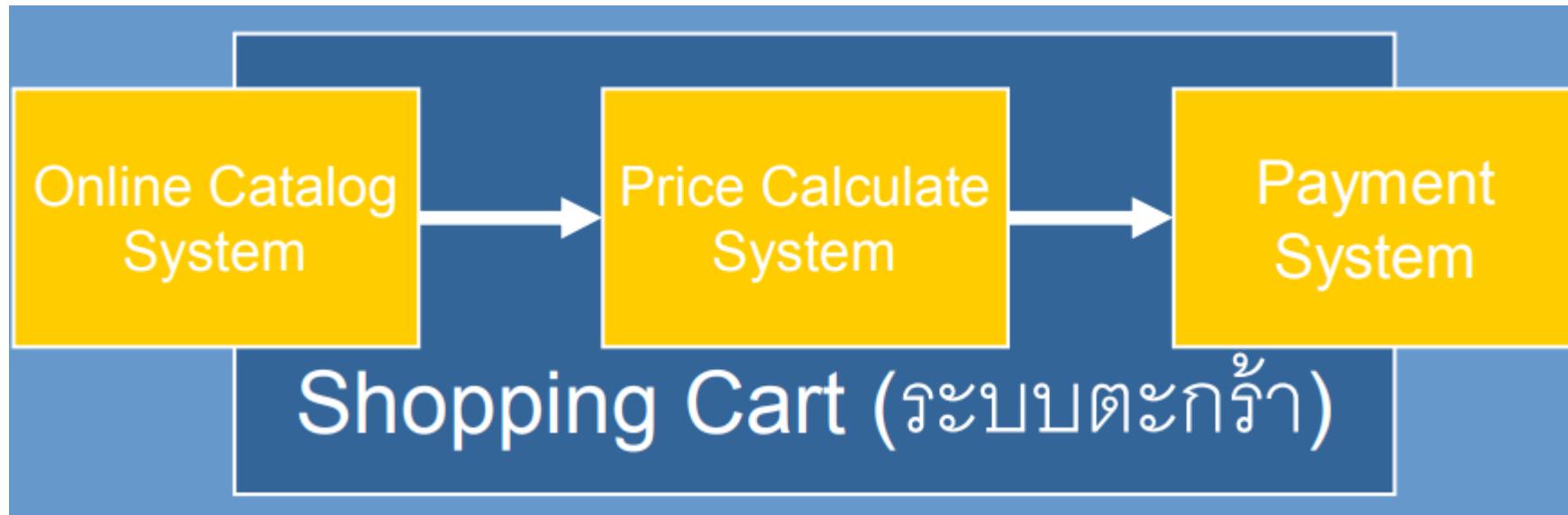


บทที่ 8 ระบบชำระเงินพาณิชย์อิเล็กทรอนิกส์

8. ระบบชำระเงินพาณิชย์อิเล็กทรอนิกส์

- ▶ การชำระเงินในระบบ E-Commerce ประกอบด้วย
 1. ระบบตะกร้า (Shopping Cart)
 2. ระบบการชำระเงิน (Payment System)

8.1. องค์ประกอบของระบบตະกรາ



- ▶ ຕະກົດຮັບສິນຄ້າທີ່ມີໃຫຍ້ຢູ່ອຳນວຍ ແລ້ວຮັບຄໍາສັ່ງຊື້ຈາກ Online Catalog
- ▶ ນຳມາຄຳນວນຮາຄາສິນຄ້າ ຮວມຄ່າຂັນສົ່ງ
- ▶ ແລ້ວສົ່ງຕ່ອໄປຢັງຮະບບການທຳຮະເງິນ

8.2. ระบบชำระบิญ

- ▶ พัฒนาระบบทำงานที่จัดการในเรื่องของการชำระบิญสินค้า
- ▶ วิธีชำระบิญ ได้แก่
 - แบบ Offline
 - แบบ Online

8.1 องค์ประกอบหลักของระบบการชำระเงิน

1. ลูกค้า
2. ร้านค้า
3. ธนาคาร หรือ สถาบันทางการเงิน
4. ผู้กำหนดกฎระเบียบปฏิบัติมาตรฐาน
5. เครือข่ายธนาคาร

8.3 ประเภทของการชำระเงินธุรกิจ e-Commerce

1) แบบ Offline

- โอนเงินเข้าบัญชีธนาคาร
- ชำระเงินเมื่อได้รับสินค้า
- ชำระเงินทางไปรษณีย์

2) แบบ Online

- E-payment
 - ◆ บัตรเอทีเอ็ม
 - ◆ บัตรเดบิต
 - ◆ บัตรเครดิต
 - ◆ เงินสดอิเล็กทรอนิกส์

8.4 การชำระเงินทางอิเล็กทรอนิกส์ (e-Payment)

- ▶ การชำระเงินทางอิเล็กทรอนิกส์
 - หรือ Electronic Payment หรือ e-Payment
 - หมายถึง การชำระเงินทางอิเล็กทรอนิกส์ หรือ Electronic payment หรือ e-Payment ก็คือ การชำระเงินด้วยวิธีการที่มีการนำระบบการทางอิเล็กทรอนิกส์ หรือระบบคอมพิวเตอร์มาใช้

8.4 บริการชำระเงินทางอิเล็กทรอนิกส์

บัตรเอทีเอ็ม



บัตรเดบิต



e-Money



บริการ e-Payments

บัตรเครดิต



Mobile payment



Internet payment



8.5. เงินอิเล็กทรอนิกส์ (e-Money)

- ▶ เงินอิเล็กทรอนิกส์อยู่ในรูปของ
 - 1) บัตรพลาสติก เรียกว่า “บัตรเงินอิเล็กทรอนิกส์” (หรือเรียกว่า บัตรเงินสด Cash Card หรือ บัตรเงินดิจิตอล Digital Money Card)
 - 2) Mobile Money คือ กระเป๋าเงินอิเล็กทรอนิกส์ในโทรศัพท์มือถือ ที่เป็นที่รู้จักในนาม M-wallet หรือ E-Wallet

8.5 เงินอิเล็กทรอนิกส์ (e-Money)

- ▶ ตัวอย่างเงินอิเล็กทรอนิกส์ เช่น
 - บัตรโดยสารรถไฟฟ้า
 - บัตรซื้ออาหารในศูนย์อาหาร
 - บัตรเติมเงินโทรศัพท์มือถือ
 - บัตรเติมเงินช้อปชิป몽อันເກວຣີເນັຕ
 - บัตรบ่มภาพยบຕົກ
 - กระเปาเงินบนโทรศัพท์มือถือ
 - บัญชีเงินสดบนเครือข่ายอันເກວຣີເນັຕสำหรับการซื้อปิงปองไลน์

8.6. Web Payment

- ▶ การชำระเงินระหว่างบุคคลผ่านเว็บไซต์ที่เป็นผู้ให้บริการทางการเงิน
- ▶ เช่น Paypal.com, Paysbuy.com

Paypal

- ▶ Paypal Inc. เป็นบริษัทอونไลน์ที่ให้บริการระบบโอนและชำระเงินผ่านระบบ Internet ระหว่างผู้บุคคลกับผู้บุคคล (C-to-C Payment) ที่ใหญ่ที่สุดในโลก



Paypal

- ▶ บริการที่ลูกค้านิยมใช้บริการ
 - การโอนเงินระหว่างบุคคลกับบุคคล
 - การชำระเงินค่าสินค้าในตลาด
 - ประมูลต่างๆ โดยเฉพาะตลาดประมูลระหว่างบุคคลกับบุคคลของ Ebay





บทที่ 9 การขนส่งสินค้าของธุรกิจ e-Commerce



9.1 การขนส่งสินค้าของธุรกิจ e-Commerce

- ▶ การทำธุรกิจ E-commerce ให้ประสบผลสำเร็จ ต้องทำให้กั้ง 3 E เกิดความลงตัวและเชื่อมโยงกัน คือ
 - E-commerce
 - E-payment
 - E-logistics



9.2 รูปแบบบริการขนส่งสินค้าสำหรับร้านออนไลน์

- 2.1) บริการส่งของด้วยไปรษณีย์ไทย
- 2.2) บริการส่งของด้วยบริษัทโลจิสติกส์/บริษัทขนส่ง
- 2.3) บริการรับฝาก-ส่งของ ด้วยบริษัทรถกัวร์
- 2.4) ส่งของกับบริษัทขนส่งที่สนับสนุนด้าน E-Commerce โดยตรง (E-Commerce Fulfillment)
- 2.5) การส่งรูปแบบใหม่

1) ไปรษณีย์ไทย

- ▶ ให้บริการ
 - ขนส่งและกระจายสินค้า
 - บริหารจัดการคลังสินค้า
- ▶ จัดส่งกั้งในประเทศและต่างประเทศ
- ▶ คิดค่าบริการตามน้ำหนัก
- ▶ มีระยะเวลาในการจัดส่งประมาณ 1-5 วัน
ขึ้นกับรูปแบบการส่ง แบบธรรมดา, แบบ
ลงทะเบียน หรือแบบ EMS เร่งด่วน



2) บริการส่งของด้วยบริษัทโลจิสติกส์ / บริษัทขนส่ง

- ▶ กำหนดที่เน้นไปยังประเทศไทย แต่เน้นบริการด้านการส่งพัสดุโดยเฉพาะ
- ▶ เมาะสำหรับร้านออนไลน์ เพราะส่งครั้งละหลายชิ้น และราคาถูกกว่า ประเทศญี่ปุ่น
- ▶ ตัวอย่าง
 - นิมเอ็กเพรส (Nim Express) ชื่อเดิมคือ นิมซีส์
 - เอ็นทีซี (NTC) ไม่มีบริการส่งของไปจังหวัดภาคใต้
 - เอ็นเอ็นแอล (NML) [NML](#)



3) บริการรับฝาก-ส่งของ ด้วยบริษัทรถทัวร์

- ▶ ส่งพัสดุขนาดใหญ่ไปต่างจังหวัด
- ▶ วิธีการส่ง-รับของกับบริษัททัวร์
 - ผู้ส่งนำสินค้าไปที่ศูนย์บริการรถทัวร์ หรือสถานีขนส่ง ที่มีอยู่ทุกจังหวัดทั่วประเทศไทย เพื่อให้อัดส่งสินค้าไปยังจังหวัดที่ต้องการภายใน 1-2 วัน
 - สินค้าที่ฝากส่งจะเดินทางถึงจังหวัดปลายทางโดยเร็วกว่าส่งด้วย EMS ธรรมดา
 - ในส่วนของผู้รับ จะต้องมารับสินค้าที่ศูนย์บริการของบริษัททัวร์ หรือสถานีขนส่งในจังหวัดนั้นๆ ด้วยตัวเอง หรือถ้ามาไม่ได้จริงๆ ก็ต้องมีหลักฐานยืนยันตัวตนมารับของที่สถานี

3) บริการรับฝาก-ส่งของ ด้วยบริษัทรถกัวร์

- ▶ บริษัทรถกัวร์ที่มีบริการนี้ ได้แก่
 - นครชัยแอร์
 - บขส.
 - สมบัติกัวร์ เป็นต้น
- ▶ แต่ละบริษัทมีเงื่อนไข และราคากี่แตกต่างกัน แต่เงื่อนไขการส่งของ-รับของ เหมือนกัน

นครชัยแอร์
NAKHONCHAI AIR

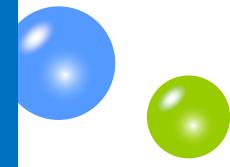


สมบัติกัวร์
บริษัทรถกัวร์พื้นเมืองไทย

4) ส่งของกับบริษัทขนส่งที่สนับสนุนด้าน E-Commerce โดยตรง (E-Commerce Fulfillment)

- ▶ หรือเรียกว่า E-Commerce Fulfillment
- ▶ บริษัทที่อยู่ในกลุ่มนี้จะนำเสนอบริการที่มากกว่าการขนส่งสินค้าธรรมดานะ เช่น
 - บริการเก็บเงินปลายทาง (จ่ายเงินตอนได้รับสินค้า-ไม่ต้องโอนมา ก่อน)
 - บริการสต็อกสินค้าหรือบริการ Warehouse
 - บริการ Door-to-Door (มีพนักงานมารับสินค้าที่บ้าน และไปส่งให้ที่ บ้านลูกค้า) ฯลฯ
- ▶ บริษัทเหล่านี้มี Solution พิเศษนอกเหนือจากการส่งของไว้ให้

2.4) สังของกับบริษัทขนส่งสนับสนุนด้าน E-Commerce โดยตรง (E-Commerce Fulfillment)



บริษัท	รูปแบบ
Kerry Express	Door-to-Door เก็บเงินปลายทาง (COD) ส่งต่างประเทศ
aCommerce	Door-to-Door เก็บเงินปลายทาง (COD) ส่งต่างประเทศ บริการ Warehouse ขนาดใหญ่ระดับภูมิภาค
dpxlogistics	ช่วยจัดเก็บสินค้า (Warehousing) แพ็คของ (Packing) ส่งของ Shipping และบริการนำเข้าและเคลียร์สินค้าจากต่างประเทศ
Ship yours	จัดเก็บสินค้า (Warehousing) แพ็คของ (Packing) ส่งของ Shipping

5) ส่งของรูปแบบใหม่

- ▶ นอกจากการส่งของในรูปแบบเดิมยังมีบริการอื่นๆ ที่ช่วยส่งสินค้าที่นำสนิใจ ได้แก่

บริษัท	รูปแบบบริการ
SkyBox	รับฝากของที่ BTS
GrabBike	ส่งเอกสาร/พัสดุ/ผู้โดยสาร ให้ชั่วโมงเร่งด่วนด้วย มอเตอร์ไซค์
Nikko Box	บริการ Warehouse เก็บของ สามารถฝากของด้วยโกรดัง ที่มีการรักษาความปลอดภัย เริ่มต้นที่ 1 กล่องโดยจะใช้เวลา ลง Ike ได้
ม้าขาว At All	บริการส่งพัสดุไปรษณีย์ในเครือซีพี ออลล์ เปิดบริการส่ง พัสดุกันทั้งหมดแล้ว ที่ร้านเซเว่น อีเลฟเว่น ตลอด 24 ชั่วโมง

9.3 นโยบายการจัดส่งสินค้าที่ดีและรักษาลูกค้า

1) นโยบายการจัดส่งสินค้า

- ▶ ทุกรุกิจจะแตกต่างกัน ขึ้นอยู่กับข้อกำหนดของผลิตภัณฑ์,
ประเภทน้ำหนักและการเข้าถึงฐานลูกค้า
 - เช่น จัดส่งเฉพาะต่างประเทศและก้องถิน

9.3 นโยบายการจัดส่งสินค้าที่ดีและรักษาลูกค้า

2) เวลาดำเนินการจัดส่ง

- ระบุเวลาโดยประมาณในการจัดส่ง เช่น ส่งในวันถัดไป, ส่งช่วง 16:00 น.
- หากมีค่าใช้จ่ายในการจัดการที่จะเรียกเก็บต้องระบุไว้ในนโยบายด้วย
- อาจระบุระยะเวลาการได้รับของลูกค้า เช่น
 - การส่งมอบภายในวันเดียว Same day delivery
 - ◆ ร้านดอกไม้หลายแห่งนิยมใช้บริการนี้
 - การจัดส่งในวันถัดไป Next day delivery

9.3 นโยบายการจัดส่งสินค้าที่ดีและรักษาลูกค้า

3) นโยบายการติดตาม

- ต้องจัดหาเว็บลิงค์หรือหมายเลขไปรษณีย์ให้กับลูกค้า เพื่อให้ลูกค้าทราบว่าสินค้าเริ่มต้นที่ใดและผ่านโหมดใดบ้าง เมื่อไหร่จะถึงเมืองปลายทางฯลฯ
- ต้องระบุรายละเอียดการติดต่อของผู้ให้บริการขนส่งที่ใช้สำหรับการขนส่งไปยังลูกค้า
- ควรระบุว่าลูกค้าสามารถนำตัวหรือใบปะไปแสดงได้อย่างไร
- ควรระบุขั้นตอน ในการนี้ที่สินค้าถูกส่งคืนเนื่องจากการจัดส่งที่ล้มเหลว

9.3 นโยบายการจัดส่งสินค้าที่ดีและรักษาลูกค้า

4) นโยบายการคืนสินค้า

- นโยบายการคืนสินค้าที่มีประสิทธิภาพจะกระตุ้นให้ลูกค้าซื้อสินค้า เพราะจะรับประกันว่าหากไม่พอใจสินค้าสามารถส่งคืนให้ผู้ขายได้เสมอ
- นโยบายการคืนสินค้าควรมีรายละเอียด เช่น
 - ระยะเวลาของคืนสินค้า ภายในกี่วันหลังจากการจัดส่ง
 - วิธีที่จะขอคืน
 - หากสินค้าเป็นแบบพรีแพดและสินค้าพิเศษ ลูกค้าจะได้รับการแลกเปลี่ยนหรือคืนเงินหรือไม่
 - บริการขนส่งใดที่ใช้สำหรับส่งคืน

9.3 นโยบายการจัดส่งสินค้าที่ดีและรักษาลูกค้า

5) การประกันภัย

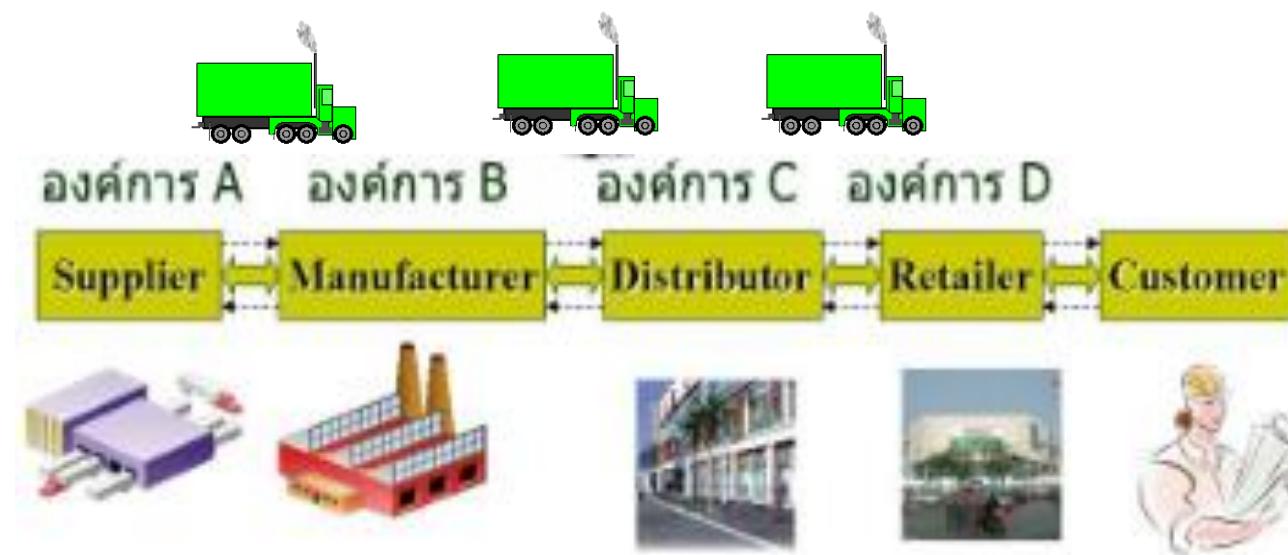
- เป็นองค์ประกอบสำคัญของนโยบายการจัดส่งสินค้า
- ผู้ขายต้องให้ความรู้แก่ลูกค้าเกี่ยวกับประโยชน์ของการประกันสินค้า
- สินค้าบางชนิดอาจให้ประกันภาคบังคับหรือบางชนิดให้ลูกค้าเลือกซื้อประกันสินค้า
 - เช่น การจอดรถ ความเสียหาย ไฟไหม้ ฯลฯ

9.4 โลจิสติกส์ (Logistics)

- ▶ คือ ระบบการจัดการการส่งสินค้าและทรัพยากรอย่างอื่น จากจุดต้นทางไปยังจุดบริโภคตามความต้องการของลูกค้า
- ▶ โลจิสติกส์เกี่ยวข้องกับการผสมผสานของ **ข้อมูลการขนส่ง การบริหารวัสดุคงคลัง การจัดการวัตถุดิบ การบรรจุหีบห่อการขนส่ง**

9.4 โลจิสติกส์ (Logistics)

- ▶ ระบบโลจิสติกส์เป็นกระบวนการหนึ่งของการจัดการสินค้าและบริการตลอดห่วงโซ่อุปทาน (Supply Chain)



1) หลักในการเลือกผู้ให้บริการโลจิสติกส์

1. บริษัทมีมาตรฐานระดับสากล

- มีชื่อเสียงและได้รับการยอมรับตามมาตรฐานระดับสากล

2. สามารถจัดส่งรวดเร็วตรงต่อเวลา และสินค้าอยู่ในสภาพที่สมบูรณ์

- เป็นคุณสมบัติพื้นฐานที่ผู้ให้บริการโลจิสติกส์ที่ดีต้องมี
- มีความใส่ใจและพิถีพิถันในทุกขั้นตอนจนส่งสินค้าถึงมือลูกค้าในสภาพที่ “สมบูรณ์” ไม่ชำรุด ฉีกขาด หรือเสียหาย

1) หลักการเลือกผู้ให้บริการโลจิสติกส์

3. มีรูปแบบการให้บริการที่หลากหลาย

- นำเสนอ “รูปแบบ” การให้บริการที่หลากหลายให้กับผู้ประกอบการและลูกค้า เช่น
 - บริการรับสินค้าถึงสถานประกอบการโดยตรง ทำให้ผู้ประกอบการไม่ต้องเสียเวลาไปกับการขนย้ายพัสดุ
 - บริการส่ง SMS แจ้งเตือนลูกค้าก่อนการจัดส่งสินค้าทุกครั้ง เพื่อให้ลูกค้าทราบช่วงเวลาในการจัดส่ง
 - บริการชำระเงินปลายทาง (COD) สำหรับลูกค้าที่ไม่สะดวกชำระเงินออนไลน์

2) หลักการเลือกผู้ให้บริการโลจิสติกส์

4. มีระบบการติดตาม และตรวจสอบสถานะการจัดส่งที่แม่นยำและกันสมัย

- ลูกค้าสามารถตรวจสอบสถานะพัสดุของตัวเองได้ง่าย เช่น
 - การตรวจสอบผ่านทางเว็บไซต์หรือแอพพลิเคชันบนมือถือ

2) หลักการเลือกผู้ให้บริการโลจิสติกส์

5. มีฝ่ายบริการลูกค้า (Customer Service) กี่เข้าถึงได้ง่ายและสะดวกรวดเร็ว

- สามารถให้ข้อมูลที่ถูกต้องแม่นยำให้กับลูกค้า
- มีระบบการติดต่อสื่อสารที่สามารถเข้าถึงได้ง่าย

9.5 E-Logistics

▶ E-Logistics

- หมายถึง ระบบสารสนเทศที่ทำหน้าที่ให้ปัจจัยต่างๆ เข้าสู่การผลิต และนำสินค้าไปส่งถึงยังลูกค้า
- โดยมีการติดต่อและจัดส่งสินค้าที่รวดเร็ว
- เพื่อให้สามารถจัดส่งสินค้าถึงมือลูกค้าได้เร็วที่สุดและสะดวกที่สุด ประหยัดค่าขนส่งที่สุดและเกิดความพิเศษน้อยที่สุด

1) ระบบสารสนเทศของ E-Logistics

▶ E-Logistics ประกอบด้วย

1. PMS (Parking Management System)

- ระบบการจัดการการขนส่งทางรถ ตั้งแต่การรับคำสั่ง การวางแผน การจ่ายงาน การเก็บประวัติรถและพนักงาน รวมถึงการวางแผน

2. WMS (Warehouse Management System)

- ระบบบริหารคลังสินค้า การรับสินค้า การจัดเก็บ การจ่ายสินค้า

1) ระบบสารสนเทศของ E-Logistics

▶ E-Logistics ประกอบด้วย

3. PMS (Phase Management System)

- ระบบบริหารการขนส่งเป็นการเฉพาะเน้นค่าบริหารการขนส่งในแต่ละรูปแบบ

4. CMS (Container Yard Management System)

- รูปแบบการจัดการกับลานตู้ Container

1) ระบบสารสนเทศของ E-Logistics

▶ E-Logistics ประกอบด้วย

5. SMS (Ship Management System)

- การจัดการสินค้าในเรือ เพื่อให้การขนถ่ายมีประสิทธิภาพ

6. MMS (Maintenance Management System)

- การบริการการจัดการการซ่อมบำรุงควบคุมอะไหล่ ปริมาณช่าง ประวัติการซ่อม

1) ระบบสารสนเทศของ E-Logistics

▶ E-Logistics ประกอบด้วย

7. LMS (Logistics Management System)

- ระบบการบริการการจัดการ Logistics ในรูปแบบของ One stop service

8. ระบบ EDI

- การรับ-ส่งเอกสารแบบอิเล็กทรอนิกส์ เพื่อใช้สำหรับบริหารจัดการส่งต่อเอกสารต่างๆ ที่ใช้ในกระบวนการนำเข้า-ส่งออกในรูปแบบอิเล็กทรอนิกส์ไปยังผู้เกี่ยวข้อง

2) ประโยชน์ของ e-Logistics

1. ช่วยให้กระบวนการทำงานขององค์กรเป็นไปอย่างอัตโนมัติ ทำให้เกิดความถูกต้องรวดเร็ว
2. ช่วยให้การบริการที่รวดเร็วขึ้น กลุ่มลูกค้าพึงพอใจกับการให้บริการมาก
3. ได้รับข้อมูลข่าวสารครบถ้วน รวดเร็ว
4. เพิ่มความได้เปรียบกับคู่แข่งทางการค้า



บทที่ 10

ความปลอดภัยของธุรกิจอีคอมเมิร์ซ (e-Commerce Security)



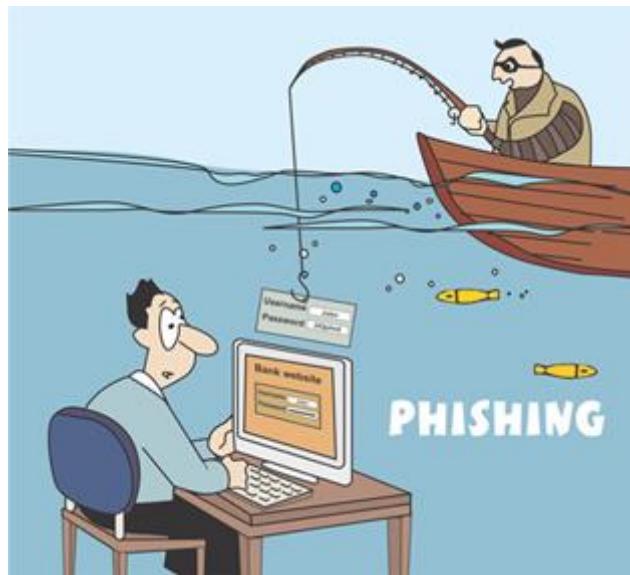
10.1 กัยจากการถูกขโมยชื่อผู้ใช้และรหัสผ่าน

1) กัยจากการถูกขโมยชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบออนไลน์ผ่านทางอินเทอร์เน็ต (Username/Password and Identity Theft)

- Phishing Attack
- Pharming Attack
- Vishing หรือ Voice SPAM Attack
- Spyware / Keylogger Attack
- Remote Access Trojan (RAT) Attack
- HOAX/SCAM หรือจดหมายหลอกลวง
- Theft of Notebook/PC or Mobile Device

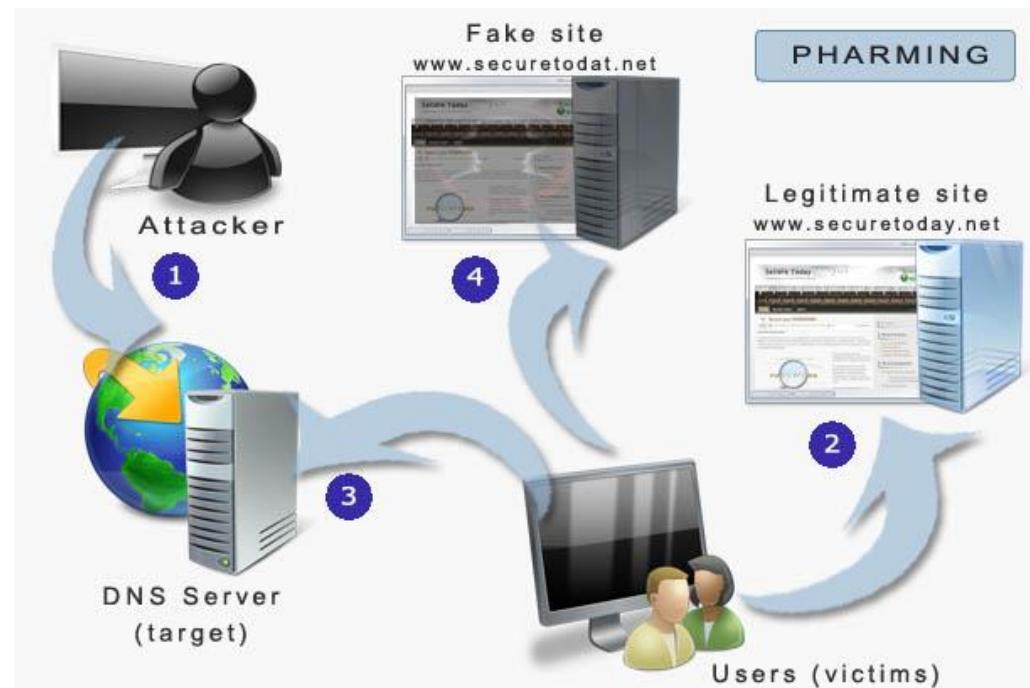
1) Phishing Attack

- ▶ ใช้ E-mail กี่มีเนื้อหาในเชิงหลอกลวง เพื่อหลอกเราข้อมูลส่วนตัวที่สำคัญ เช่น รหัสผ่าน, เลขบัตรเครดิต หรือ ข้อมูลบัญชี จาก ผู้ใช้งาน



2) Pharming Attack

- ▶ โจรตีกี่ไฟล์ HOSTS ของเครื่องลูกบ่าย โดยการ “Re-Direct” หรือ “ย้าย” ชื่อของเว็บไซต์ ให้เข้าไปยัง “IP Address ลวง” ที่ไม่ตรงกับ “IP Address จริง” ของเว็บไซต์นั้นๆ ซึ่งเหยื่อจะแยกความแตกต่างแทบไม่ออก ระหว่างเว็บไซต์จริงกับเว็บไซต์ปลอมที่ทางแฮกเกอร์ได้เตรียมไว้



3) Vishing គឺវិនិយោគ Voice SPAM Attack

- ▶ เป็นการโจมตีโดยการใช้ระบบໂករសាក់
- ▶ การใช้ระบบ “Automated Calling” អីវីជីរបែប “Voice Over IP” មានចំណាំ
ក្នុងការអេក្រង់អេក្រង់ ដែលគឺជាប្រព័ន្ធឌៃប្រឈមទូទៅនៃការសារបាន
ការចុះហត្ថលេខា ឬប្រាកបតាមលក្ខណៈ ដើម្បីការអេក្រង់អេក្រង់ដែលមានប្រព័ន្ធ
- ▶ គេអេក្រង់ តាមបញ្ជីអ៊ូលស៊ុនតុវិក ឬបញ្ជីអ៊ូលការងារដោយការចុះហត្ថលេខា ឬប្រាកបតាមលក្ខណៈ ដើម្បីការអេក្រង់អេក្រង់ដែលមានប្រព័ន្ធ

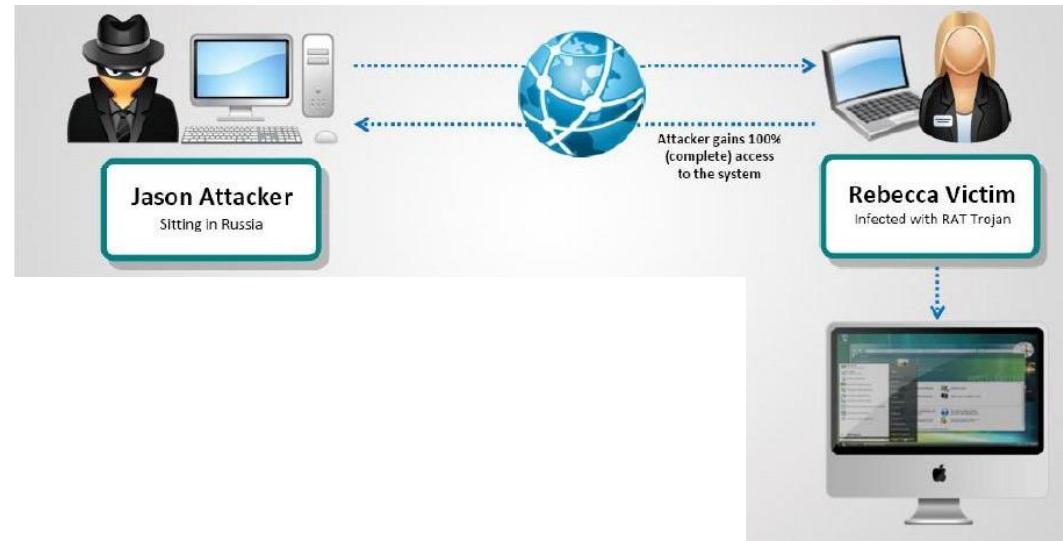


4) Spyware / Keylogger Attack

- ▶ โปรแกรมดักข้อมูลจากคีย์บอร์ด หรือ Keylogger เป็นโปรแกรมประเภท “Spyware”
- ▶ มีจุดประสงค์ดักข้อมูลโดยที่เหยื่อไม่รู้ตัว
- ▶ จากการที่เหยื่อมักจะเปิดเครื่องกังไว้โดยไม่ได้ Lock หน้าจอคอมพิวเตอร์ เป็นเหตุให้ผู้ไม่หวังดี สามารถทำการติดตั้งโปรแกรม Spyware หรือ Keylogger ผ่านทางการใช้ Thumb Drive หรือ USB Drive
- ▶ หลังจากนั้นไม่ว่าเหยื่อจะพิมพ์อะไรก็จะถูกดักข้อมูลบนคีย์บอร์ดและข้อมูลหน้าจอ ส่งไปยัง ฟรีอีเมล์ของแฮกเกอร์เป็นระยะๆ ทำให้ข้อมูลส่วนตัวของเหยื่อหลุดเข้าไปอยู่ในมือคนร้ายอย่างง่ายดาย

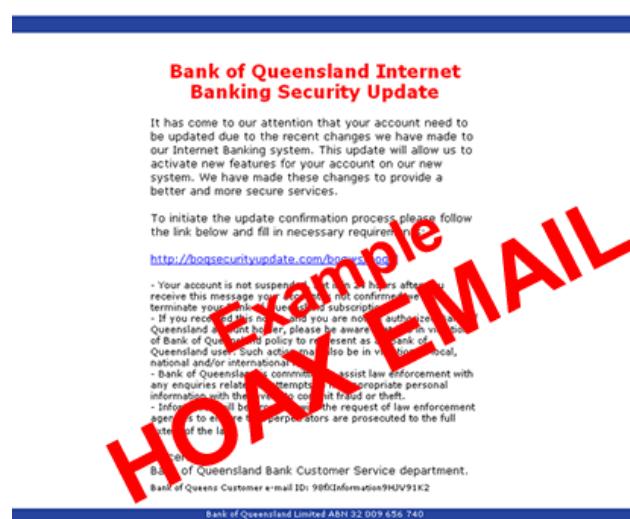
5) Remote Access Trojan (RAT) Attack

- ▶ การโจมตีระยะไกลโดยใช้โปรแกรมประเภทม้าโทรจันส่งผ่านมาทางอีเมล
- ▶ โดยหลอกว่าเป็นโปรแกรมประยุกต์ทั่วไป เช่น โปรแกรมเกมส์ หรือ โปรแกรมที่ใช้ในการข่าไวรัส เป็นต้น เมื่อเหยื่อคลิกเข้าใจผิดแล้วสั่ง “Run” โปรแกรมดังกล่าว
- ▶ เหยื่อจะถูกควบคุมคอมพิวเตอร์ของตนจากระยะไกล (Remote Access) โดยไม่รู้ตัว แรกเกอร์สามารถเข้ามาล้วงความลับของเหยื่อได้



6) HOAX/SCAM หรือจดหมายหลอกลวง

- ▶ SCAM เป็นการ “SPAM” อย่างหนึ่งผ่านทางอีเมล
- ▶ มีวัตถุประสงค์ในการส่งอีเมลหลอกให้เหยื่อเข้าใจผิด ว่าได้รับรางวัลหรือได้รับเงินผ่านทางอินเทอร์เน็ต ซึ่งเหยื่อจะเกิดความโลภที่จะได้รับเงินก้อนโต
- ▶ จากนั้นมิจฉาชีพจะหลอก ให้เหยื่อโอนเงินค่าธรรมเนียม (เงินก้อนเล็ก) เพื่อให้ได้รางวัล (เงินก้อนโต) ดังกล่าว



7) Theft of Notebook/PC or Mobile Device

- ▶ การขโมยแบบดั้งเดิมทางกายภาพ โดยไม่ต้องใช้เทคนิคทางคอมพิวเตอร์
- ▶ การขโมย PC, Notebook, PDA หรือໂໂກຣຄັພທີ່ມີວິດີ້ຈາກນັ້ນນຳໄປດອດເວາ
ຫາຣົດດີສົກ໌ຫຼື SIM Card ອອກຈາກເຄຣື່ອງເພື່ອນຳໄປ “Copy” ຂ້ອມຸລບອນເໜື້ອ
- ▶ ກັບນຳວຸປກຮນົມພິວເຕອຣີໄປຈຳນ່າຍຕ່ວໃນຕລາດນີ້ສອງ



10.2 ภัยจากการโจมตี Web Server และ Web Application

2) ภัยจากการโจมตี Web Server และ Web Application

- Popular Web Site Attack
- Web 2.0 and Social Network Attack

1) Popular Web Site Attack

- ▶ เว็บไซต์ดังที่กำลังเป็นที่นิยมมีโอกาสที่จะถูกแฮกเกอร์เข้ามาโจมตี
- ▶ แอบผิงโปรแกรมไวรัส หรือ เม้าໂගรຈັນ เพื่อเป็นที่ปล่อยไวรัสเข้าสู่ผู้เข้าเยี่ยมชมเว็บไซต์ดังกล่าว
- ▶ ตัวอย่างเช่น เว็บไซต์ของ Super Bowl ก็ถูกโจมตีในลักษณะนี้ ทำให้ผู้ที่เข้าชมเว็บไซต์ Super Bowl ติดไวรัส

2) Web 2.0 and Social Network Attack

- ▶ การใช้เทคโนโลยี Web 2.0 อยู่ เช่น Blogs, Wikis, RSS หรือ AJAX มาใช้ในเว็บไซต์ประเภท “Social Network” เช่น Open social ของ Google , Widgets ของ Facebook ตลอดจนเว็บไซต์ Myspace หรือ Youtube
- ▶ ใช้เทคนิค “Mash-ups” อนุญาติให้ผู้เล่นเว็บสามารถก่อจงใจพัฒนา “Application” เล็กๆ ในการติดต่อสื่อสารกับผู้ใช้คนอื่นๆ ได้
- ▶ “Application” ดังกล่าวมีโอกาสก่อจงใจเกิดช่องโหว่หรือ อาจเป็น “Trojan Application” กี่แรกเกอร์มาสร้างไว้ให้คนเข้ามา Download Application ไปใช้งาน

10.3 กัยข้ามระบบ (Cross-platform Attack)

- ▶ การโจมตีระบบคอมพิวเตอร์ของโปรแกรม Malware ในปัจจุบันสามารถทำงานบน Platform อื่นๆ ได้
- ▶ เป็นการโจมตีผ่านทาง Web Browser เป็นส่วนใหญ่ เพราะทุก Platform ใช้ Web Browser เมื่อൺกัน เช่น Firefox หรือ Safari เป็นต้น
- ▶ โปรแกรมไม่ประสงค์ดีส่วนใหญ่เขียนด้วยภาษา Java หรือ JavaScript ที่สามารถทำงานบน Web Browser ดังกล่าวได้เป็นอย่างดี



10.4 กัยจากการถูกขโมยข้อมูล

- ▶ กัยจากการถูกขโมยข้อมูล หรือ ข้อมูลความลับรั่วไหลออกจากองค์กร (Data Loss/Leakage and Theft)
 - ข้อมูลถูกจัดเก็บในรูปแบบของไฟล์ที่อยู่ในรูปแบบดิจิตอลฟอร์แมต เก็บไว้ในฮาร์ดดิสก์ หรือ เก็บไว้ใน Storage ขนาดใหญ่ เช่น ระบบ NAS หรือ SAN
 - ผู้ไม่หวังดีแอบทำสำเนา หรือ “Copy” ข้อมูลออกไป

10.5 กัยจากมัลแวร์

- ▶ กัยจากมัลแวร์และสามเหลี่ยมแห่งความชั่วร้าย (SPAM , VIRUS and SPYWARE)
 - มัลแวร์ (Malware) คือ โปรแกรมมุ่งร้ายหรือโปรแกรมไม่ประสงค์ดี
 - จะมีรูปแบบของการทำงานที่แตกต่างกัน
 - เกี่ยวโยงกับ Spam Mail ที่ได้รับ คือ Spam Mail เป็นพาหนะหรือตัวนำมาซึ่งมัลแวร์ในรูปแบบต่างๆ
 - กัยจาก Spam Mail
 - สร้างความรำคาญ
 - นำโปรแกรมมุ่งร้าย ที่อาจแนบมากับไฟล์แบบ (Attached File) หรืออยู่ในรูปแบบของ Download Link



www.shutterstock.com - 577481197

10.5 Malicious Viruses

▶ Viruses : ไวรัส

- คือ โปรแกรมคอมพิวเตอร์ประเภทหนึ่ง
- ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์
- ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็ว ไปยังทุกไฟล์ภายใน คอมพิวเตอร์ หรืออาจทำให้ไฟล์เอกสารติด เชื้อย่างช้าๆ แต่ ไวรัส จะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไป ยังอีกเครื่องหนึ่งได้ด้วย ตัวมันเอง โดยทั่วไปเกิดจากการที่ผู้ใช้เป็น พาหะ นำไวรัสจากเครื่อง หนึ่งไปยังอีกเครื่องหนึ่ง

10.5 Malicious Viruses

- ▶ Worms :
 - حنอนอินเตอร์เน็ต
 - เป็นโปรแกรมคอมพิวเตอร์ชนิดหนึ่ง ที่สามารถก่อубปีตัวเองจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้โดยอัตโนมัติผ่านทางเครือข่ายเน็ตเวิร์คหรือว่าอินเทอร์เน็ต เวิร์มนี้สามารถขยายพันธุ์และเคลื่อนย้ายตัวเองไปยังเครื่องอื่นๆ บน เน็ตเวิร์คได้ไม่ยาก

10.5 Malicious Viruses

▶ Trojan Horse :

- โปรแกรมที่มีหน้าที่กำลังล้างโดยตรง โดยอาศัยผู้ใช้งานเป็นผู้เรียกขึ้นมาทำงาน
- ถูกส่งต่อทางอีเมล์ โดยว้างตัว ว่าเป็นเครื่องมือต่างๆ เช่น ว้างเป็น โปรแกรมสำหรับช่วยงานพาวเวอร์พอยน์ต เป็นไดร์เวอร์ IDE ให้มีที่จะทำให้เครื่องทำงานเร็วขึ้น
- หากใครเปิดไฟล์ที่รับขึ้นมามักจะใช้งานเครื่องคอมพิวเตอร์ไม่ได้อีกเลย

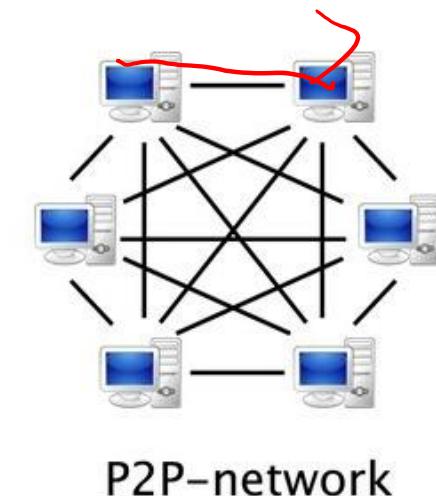
10.5 Malicious Viruses

- ▶ Bad applets (malicious mobile code):
 - โปรแกรมประยุกต์ Java applets หรือ ActiveX controls ซึ่งถูกดาวน์โหลดมาอยังเครื่องผู้ใช้งาน หลังจากนั้นโปรแกรมจะทำงานเมื่อเชื่อมต่อเข้าสู่อินเทอร์เน็ต

10.6 กัยจากการใช้โปรแกรมประเภท Peer-to-Peer

6) กัยจากการใช้โปรแกรมประเภท Peer-to-Peer (P2P)

- ▶ ผู้ใช้อินเทอร์เน็ตตามบ้านนิยมใช้โปรแกรม P2P เช่น BitTorrent, eMule, Limewire, eDonkey หรือ Kazaa
- ▶ โปรแกรม P2P จะใช้ Bandwidth ขององค์กรในการ Download ไฟล์ต่างๆ (ในกรณีที่ผู้ใช้โปรแกรม P2P ในองค์กร)
- ▶ โปรแกรม P2P ยัง “Share” ไฟล์ต่างๆที่อยู่ในฮาร์ดดิสก์ของเรา ข้อมูล จะถูกนำไป “Share” ให้คนหลายร้อยล้านคน สามารถเข้ามา Download ไฟล์ได้อย่างง่ายดาย นอกจานี้
- ▶ และมัลแวร์ ถูกปล่อยอยู่ตามเครือข่าย P2P โดยจะตั้งชื่อโปรแกรมให้มีความน่าสนใจ เพื่อหลอกให้ผู้อ่านโปรแกรม P2P ทำการ Download ไปใช้งาน



10.7 กัยจากแฮกเกอร์มืออาชีพข้ามชาติ

▶ กัยจากแฮกเกอร์มืออาชีพข้ามชาติ (Professional International Blackhat Attack)

- แฮกเกอร์มีเป้าหมายและวางแผนล่วงหน้ามาเป็นอย่างดี
- ส่วนใหญ่หวังผลทางด้านการเงิน หรือวัตถุประสงค์ทางด้านการเมือง
- เช่น โจมตีเป้าหมายประเทศไทยโดยการเข้ามาล้วงความลับ หรือ “Spy”



Hacking

- ▶ Hacker :
 - คนที่ลักลอบ หรือโฉมตีระบบเพื่อให้ได้สิทธิ์ในการเข้าไปยังเครือข่ายหรือระบบคอมพิวเตอร์นั้นๆ
- ▶ Cracker :
 - คล้ายกับ hacker เพียงแต่ว่า Cracker เมื่อเข้าไปสู่ระบบได้แล้วมีจุดมุ่งหมายในการกระทำการอาชญากรรมต่อระบบ
- ▶ Cybervandalism :
 - คนที่โฉมตีระบบ โดยมีจุดมุ่งหมายเพื่อก่อความ และกำลายเว็บไซต์

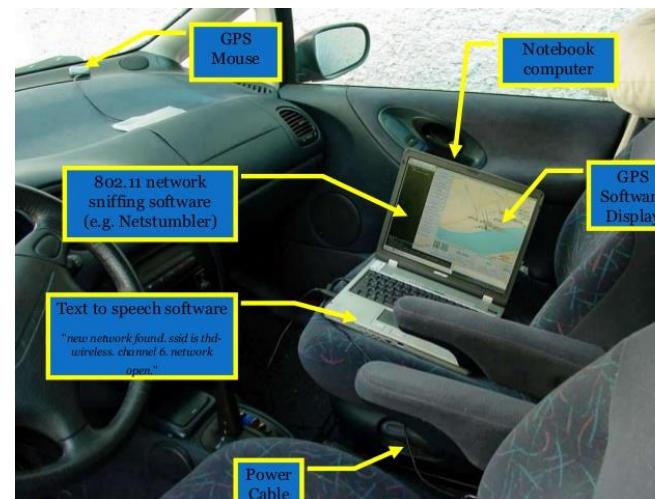
10.8 กัยจากการใช้งานอุปกรณ์ Mobile และ Wireless

- ▶ การโจรตีผ่านทางระบบไร้สายกำลังเป็นที่นิยมมากขึ้นในหมู่แฮกเกอร์เนื่องจากเป็นการยกที่จะแกละรอยแฮกเกอร์และง่ายที่จะเข้าระบบ Wireless LAN ที่ไม่มีความปลอดภัยเพียงพอ



10.8 กัยจากการใช้งานอุปกรณ์ Mobile และ Wireless

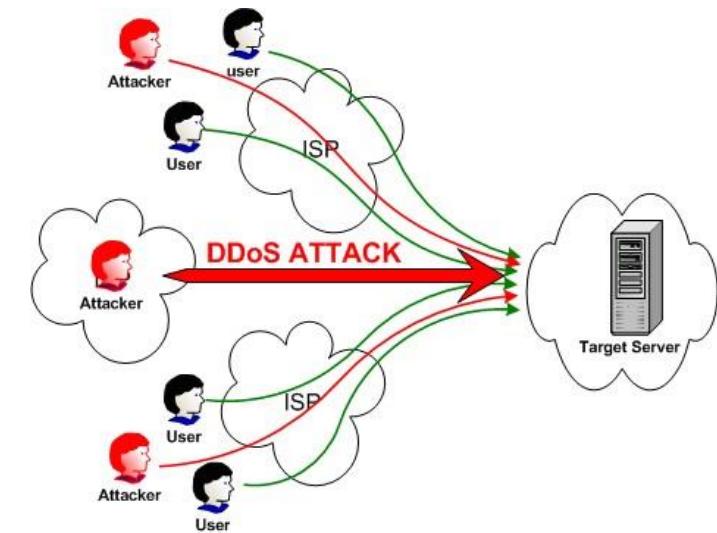
- ▶ ให้แฮกเกอร์สามารถใช้สิ่งที่เรียกว่า “ War Driving” และ “War Chalking” ในการเข้าโฉนดต่เครือข่าย Wireless LAN ผ่านทาง Access Point ที่ไม่ได้เข้ารหัส หรือมีการเข้ารหัสที่อ่อนแอกันไป เช่น เข้ารหัสด้วย WEP Algorithm



10.9 กัยจากการโจมตีด้วยเทคนิค DoS

▶ กัยจากการโจมตีด้วยเทคนิค DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) Attack

- การโจมตีเพื่อให้ระบบเป้าหมายไม่สามารถทำงานได้ตามปกติ (ละเมิด Availability) โดยวิธีการที่เรียกว่า DoS หรือ DDoS Attack
- เว็บไซต์ประเภทอ่อนไหว เช่น วิสหรือเว็บไซต์มักตกเป็นเป้าหมายการโจมตีในลักษณะนี้
- ทำให้เว็บไซต์ไม่สามารถให้บริการได้ ส่งผลให้ลูกค้าเกิดความไม่พอใจ หรือ ทำให้ธุรกิจขาดรายได้ที่ควรจะได้ตามปกติ



10.10 กัยที่เกิดขึ้นจากตัวของเราเอง

- ▶ จุดอ่อนที่อ่อนที่สุดในระบบ คือ ตัวของเราเอง
- ▶ Concept การโจมตีระบบ ส่วนใหญ่ในปัจจุบันเน้นการใช้เทคนิค “Social Engineering” เพื่อหลอกให้หลงเข้าใจผิดในเรื่องที่หากเกอร์ปลอมแปลงแต่งขึ้น ตามวัตถุประสงค์ที่จะให้เหยื่อทำตามในสิ่งที่หากเกอร์ได้กำหนดไว้ล่วงหน้า เช่น ให้เหยื่อเปิดไฟล์มัลแวร์ที่เป็นโปรแกรมม้าโทรจัน เป็นต้น

10.11 มาตรการระบบรักษาความปลอดภัยของข้อมูล EC

▶ มาตรการระบบรักษาความปลอดภัยของข้อมูล EC จำเป็นต้องมี

1. การระบุตัวบุคคล และ อำนาจหน้าที่
2. การรักษาความลับของข้อมูล
3. การรักษาความถูกต้องของข้อมูล
4. การป้องกันการปฏิเสธความรับผิดชอบ
5. สากลส่วนบุคคล

1) การระบุตัวบุคคล (Authentication)

- ▶ กระบวนการกำหนดลักษณะส่วนบุคคลของผู้ใช้ก้าวไป
 - แจ้งชื่อผู้ใช้และรหัสผ่าน
 - เมื่อผู้ใช้ต้องการเข้าระบบ ให้ระบุชื่อผู้ใช้และรหัสผ่าน
 - ถ้าข้อมูลตรงกับแฟ้มของ Server ก็จะได้รับอนุญาตเข้าถึงเว็บ เพื่อต่อไปได้
 - เปรียบเหมือนการแสดงตัวด้วยประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือ
 - การล็อกซึ่งผู้ก็จะเปิดได้จะต้องมีกุญแจเท่านั้น หรือ
 - บัตรเข้าออกอาคาร, เจ้าหน้าที่รักษาความปลอดภัย

2) การอนุญาติ- อำนาจ (Authorization)

- ▶ อำนาจในการจ่ายเงิน
- ▶ การอนุญาติวงเงินที่จะเรียกเก็บจากธนาคารที่ออกบัตร เครดิต
- ▶ ตรวจสอบวงเงินในบัญชีว่ามีเพียงพอหรือไม่

3) การรักษาความลับของข้อมูล (Confidentiality)

- ▶ เช่น การเข้ารหัส, การใช้บาร์โค๊ด, การใส่รหัสลับ (password), Firewall
- ▶ การรักษาความลับของข้อมูลที่เก็บไว้หรือส่งผ่านทางเครือข่าย
- ▶ ป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้

4) การรักษาความถูกต้องของข้อมูล (Integrity)

- ▶ การป้องกันไม่ให้ข้อมูลถูกแก้ไข
- ▶ เปรียบเหมือนกับการเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบ
- ▶ หรือ การใช้ซอฟแวร์กำกับบนบัตรเครดิต
- ▶ หรือ ลายน้ำบนบัตร



5) การป้องกันการปฏิเสธ หรืออ้างความรับผิดชอบ (Non-repudiation)

- ▶ คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือรับข้อมูลจากฝ่ายต่าง ๆ ที่เกี่ยวข้อง
- ▶ การป้องกันการอ้างที่เป็นเท็จว่าได้รับ หรือส่งข้อมูล
- ▶ เช่น ในการขายสินค้า เราต้องมีการแจ้งให้ลูกค้าทราบถึงขอบเขต ของการรับผิดชอบที่มีต่อสินค้า หรือระหว่างการซื้อขาย โดยระบุ ไว้บน web
- ▶ หรือการส่งจดหมายลงทະเบียน

6) สิทธิส่วนบุคคล (Privacy)

- ▶ การรักษาสิทธิส่วนตัวของข้อมูลส่วนตัว
- ▶ เพื่อป้องข้อมูลจากการลอบดูโดยผู้ที่ไม่มีสิทธิในการใช้ข้อมูล
- ▶ ข้อมูลที่ส่งมาถูกดัดแปลงโดยผู้อื่นก่อนถึงเราหรือไม่

10.12 การใช้เทคโนโลยีในการป้องกันความปลอดภัยของระบบ E – Commerce

- ▶ การใช้เทคโนโลยีในการป้องกันความปลอดภัยของระบบ E –Commerce หรือเรียกว่า Technology Solutions
 - Protecting Internet communications (encryption)
 - Securing channels of communication (SSL, S-HTTP, VPNs)
 - Protecting networks (firewalls)

1) การเข้ารหัส (Encryption)

- ▶ การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ด้วยการเข้ารหัส (Encryption)
- ▶ ผู้มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัส (Decryption)
- ▶ ใช้สมการทางคณิตศาสตร์
- ▶ ใช้กุญแจซึ่งอยู่ในรูปของพารามิเตอร์ที่กำหนดไว้(มีความยาวเป็น บิต โดยยิ่ง กุญแจมีความยาวมาก ยิ่งปลอดภัยมาก เพราะต้องใช้ เวลานานในการคาดเดา กุญแจของผู้คุกคาม)

5.1) การเข้ารหัส (Encryption)

- ▶ ประกอบด้วยฝ่ายผู้รับ และฝ่ายผู้ส่ง
- ▶ ตกลงกฎเกณฑ์เดียวกัน ในการเปลี่ยนข้อความต้นฉบับ ให้เป็น ข้อความอ่านไม่รู้เรื่อง (cipher text)
- ▶ ใช้สมการ หรือสูตรทางคณิตศาสตร์ที่ซับซ้อน
- ▶ กฎการเพิ่มค่า 13
- ▶ แฮชฟังก์ชัน (Hash function)

2) ลายมือชื่ออิเล็กทรอนิกส์

- ▶ ลายมือชื่ออิเล็กทรอนิกส์(Electronic Signature) หมายถึง วัสดุระตัวเลข เสียง หรือสัญลักษณ์อื่นใด ที่สร้างขึ้นโดยวิธีทาง อิเล็กทรอนิกส์
- ▶ วิธีการนำมาประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดง ความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์
- ▶ วัตถุประสงค์
 - เพื่อรับตัวบุคคลผู้เป็นเจ้าของ (Authentication)
 - เพื่อแสดงว่าบุคคลยอมรับและผูกพันกับข้อมูลอิเล็กทรอนิกส์หรือเพื่อ ป้องกัน การปฏิเสธความรับผิดชอบ (Non-Repudiation)

ຕົວຢ່າງລາຍມື້ອຊ່ວອົບເລີກໂຄນິກສ

- ▶ ຮහສປະຈຳຕັ້ງ (ID) , ຮහສລັບ (Password)
- ▶ Biometrics
- ▶ ລາຍມື້ອຊ່ວດິຈິກັລ (Digital Signature)
 - ໃຫ້ຮະບປຣຮສແບບວສມາດ (private key & public key)
- ▶ E-Mail Address

3) Secure Socket Layer (SSL)

- ▶ SSL เป็นโปรโตคอลสำหรับจัดการความปลอดภัยในระบบอินเทอร์เน็ตที่ใช้ในการสื่อสารข้อมูลกันระหว่างคอมพิวเตอร์กับเซิร์ฟเวอร์
- ▶ ปกติแล้วข้อมูลที่ส่งไปหากันจะไม่มีการเข้ารหัสข้อมูลแต่อย่างใด ทำให้การดักจับข้อมูลเป็นไปได้โดยง่าย
- ▶ แต่ถ้าเป็นระบบที่ใช้ SSL ข้อมูลจากคอมพิวเตอร์ที่จะส่งไปที่เซิร์ฟเวอร์ จะถูกเข้ารหัสก่อนที่จะส่งไปที่เซิร์ฟเวอร์ ทำให้ข้อมูลที่รับส่งกันมีความปลอดภัยมากยิ่งขึ้น

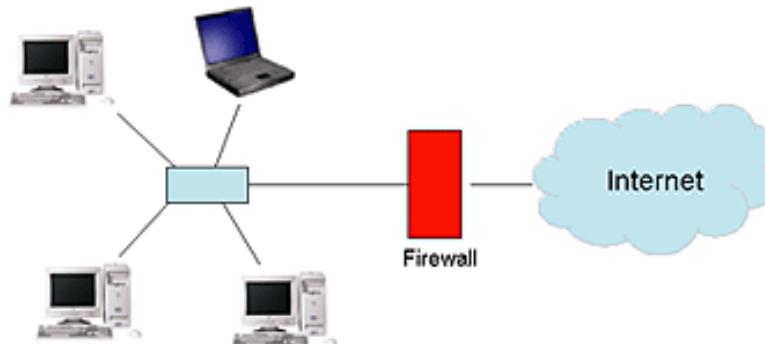
4) Firewall

- ▶ Firewall เป็นอุปกรณ์ที่ใช้สำหรับ "ป้องกันผู้บุกรุกระบบ" ในเครือข่าย (Network)
- ▶ กำหนดที่เป็นตัวคั่นกลางระหว่าง Network กับ Network ที่ไม่ไว้ใจ ตามกฎ(Rule) หรือนโยบาย(Policy) ที่ผู้ดูแลระบบ (Admin)ได้ตั้งไว้
- ▶ เป็นระบบที่ทำงานร่วมกันระหว่าง Hard และ Software โดย Firewall จะวางแผนอยู่ระหว่าง เครือข่ายภายในองค์กร (Local Network) และ เครือข่ายภายนอก (Internet) เพื่อป้องกันการบุกรุกจากบุคคลภายนอกที่ไม่ได้รับอนุญาตเข้ามาบนยีนบูนุลหรือแก้ไขเปลี่ยนแปลงข้อมูล

4) Firewall

▶ คุณสมบัติของ Firewall

- Protect Firewall เป็นเครื่องมือที่ใช้ในการป้องกัน โดยข้อมูลที่เข้า-ออก Network จะถูกกำหนดเป็น Rule หรือ Policy เพื่อใช้บังคับในการสื่อสาร ภายใน Network
- Rule Base หรือ Policy คือข้อกำหนดในการควบคุมการเข้า-ออกของข้อมูล ภายใน Network
- Access Control คือการควบคุมระดับการเข้าถึงข้อมูลต่างๆใน Network





บทที่ 11

กฎหมายและจริยธรรม e-Commerce



จริยธรรม (Ethics)

- ▶ เป็นกฎเกณฑ์และมาตรฐานของการประพฤติปฏิบัติในสังคม
- ▶ หลักคุณธรรมการประพฤติปฏิบัติหมายความว่าดูแลต้องของผู้ที่อยู่ร่วมกัน
- ▶ โดยมีพื้นฐานมาจากหลักการทางคือธรรม ค่านิยม วัฒนธรรมและประเพณี เพื่อการอยู่ร่วมกันในสังคมอย่างมีความสุบร่มเย็น
- ▶ โดยสังคมจะเป็นตัวตัดสินผลของการกระทำนั้น ว่าเป็นการกระทำที่ถูกหรือผิด



จริยธรรม (Ethics)

▶ จริยธรรม (Ethics) ในความหมายทางคอมพิวเตอร์

- หมายถึง หลักศีลธรรมจรรยาที่กำหนดขึ้น เพื่อใช้เป็นแนวทางปฏิบัติ หรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ หรือ
- หลักเกณฑ์และมาตรฐานที่ประชาชนใช้ในการตัดสินใจ เพื่อกำกับดูแลสังคมต้องและหลักเลี้ยงการกระทำความผิดต่อผู้อื่น

จริยธรรม (Ethics)

- ▶ ตัวอย่างการกระทำความผิดในด้านจริยธรรมคอมพิวเตอร์ เช่น
 - การใช้ถ้อยคำที่ไม่สุภาพ
 - การโฆษณาชวนเชื่อเกินจริง
 - การกระทำที่ก่อให้เกิดความรำคาญแก่ผู้อื่น
 - การกล่าวพาดพิงถึงผู้อื่นโดยไม่ได้รับอนุญาต
 - การใช้คอมพิวเตอร์ของผู้อื่นโดยผู้อื่นไม่เต็มใจ

กฎหมาย (Law)

- ▶ กฎหมาย คำสั่ง หรือข้อบังคับที่ถูกตั้งขึ้นโดยรัฐหรือผู้มีอำนาจสูงสุด
- ▶ เพื่อใช้เป็นเครื่อง มือสำหรับดำเนินการให้บรรลุเป้าหมายอย่างหนึ่งอย่าง ใดของสังคม
- ▶ และมีสภาพบังคับเป็นเครื่องมือในการตรุกทำให้บุคคลในสังคมต้องปฏิบัติ ตามกฎหมาย คำสั่ง หรือข้อบังคับนั้น



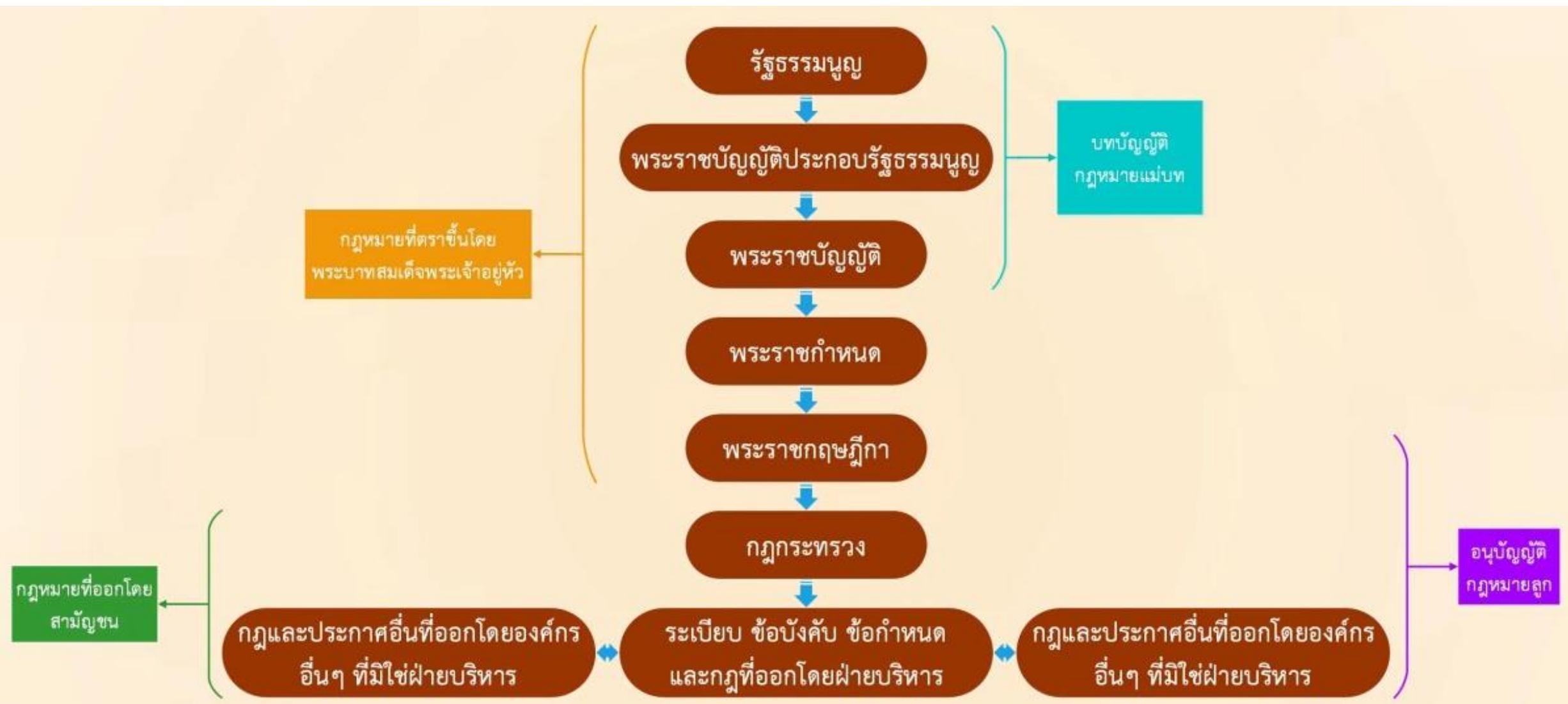
กฎหมาย & จริยธรรม

กฎหมาย	จริยธรรม
1. สร้างขึ้นมีเจตนาเพื่อรักษาความสงบเรียบร้อย และความสงบสุขในสังคมและให้ความคุ้มครองแก่ประชาชนทุกคน	1. สร้างขึ้นเพื่อช่วยให้ผู้คนตัดสินใจได้ว่าอะไรถูก หรือผิดและทำอย่างไร
2. เกิดขึ้นอย่างเป็นระบบ	2. เกิดขึ้นจากการสืบทอด
3. เป็นข้อบังคับจากรัฐที่เป็นลายลักษณ์อักษร	3. เป็นข้อบังคับจากสังคมที่ไม่เป็นลายลักษณ์อักษร
4. เป็นบทบัญญัติว่าต้องทำหรือต้องละเว้น ไม่สามารถหลีกเลี่ยงได้	4. เป็นเรื่องของจิตสำนึก ทำ เพราะเห็นว่าถูกต้อง และภูมิใจที่ได้ทำ
5. มีบก烙โภชที่ชัดเจน	5. ไม่มีการลงโทษตามกฎหมายแต่ลงโทษโดยสังคม
6. ตัดสินด้วยคำว่าผิดหรือไม่ผิด	6. ตัดสินด้วยคำว่า ควรหรือไม่ควร

2. ลำดับชั้นของกฎหมาย

- ▶ **รัฐธรรมนูญ** กฎหมายสูงสุดในการจัดระเบียบการปกครองประเทศ
- ▶ **พระราชบัญญัติ พระราชกำหนด**
 - **พระราชบัญญัติ** กฎหมายที่พระมหากษัตริย์ทรงตราขึ้นโดยคำแนะนำและยินยอมของรัฐสภา เป็นกฎหมายหลักกีสำคัญกับบังคับใช้ในปัจจุบัน
 - **พระราชกำหนด** กฎหมายที่พระมหากษัตริย์ทรงตราขึ้นตามคำแนะนำของคณะรัฐมนตรี การตราพระราชกำหนดให้กระทำได้เฉพาะเมื่อคณะรัฐมนตรีเห็นว่าเป็นกรณีฉุกเฉิน เร่งด่วน
- ▶ **พระราชกฤษฎีกา** กฎหมายที่พระมหากษัตริย์ทรงตราขึ้นตามคำแนะนำของคณะรัฐมนตรี พระราชกฤษฎีกาวางออกได้ต่อเมื่อพระราชบัญญัติให้สำนักงานไว้
- ▶ **กฎกระทรวง** เป็นกฎหมายบริหารที่กำหนดรายละเอียดของกฎหมายแม่บทอีกด้วยหนึ่ง
- ▶ **ระเบียบ ข้อบังคับ ประกาศ คำสั่ง** คือ กฎหมายปลดย่อyley ประเภทที่เป็นเรื่องเล็กๆน้อยๆ เช่น ระเบียบการปฏิบัติราชการ

2.1 ลำดับชั้นของกฎหมาย



2.2 กฎหมายที่เกี่ยวข้องกับ e-Commerce

1. กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544
2. กฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
3. กฎหมายขายตรงและตลาดแบบตรง พ.ศ.2545
4. กฎหมายคุ้มครองผู้บริโภค
5. กฎหมายทะเบียนบุพานิชย์
6. กฎหมายลิขสิทธิ์ พ.ศ.2537
7. กฎหมายว่าด้วยราคาน้ำหนักและปริมาณ พ.ศ.2542
8. กฎหมายจดแจ้งการพิมพ์
9. กฎหมายผลิตภัณฑ์ อาหารและยา
10. กฎหมายธุรกิจนำเข้าและมัคคุเทศก์ พ.ศ.2551
11. กฎหมายการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551(E-Payment)
12. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA)



1. ພຣະราชບັນຍຸຕົວ່າດ້ວຍຮູຮກຮມກາງອີເລິກໂຕອິນິກສ ພ.ສ. 2544

1) WSU.ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

- ▶ ข้อมูลอิเล็กทรอนิกส์ มีผลเท่ากับ กระดาษ
- ▶ รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ เมื่องกับการทำหลักฐานเป็นกระดาษหรือหนังสือรับรองการส่งและรับข้อมูลอิเล็กทรอนิกส์ รวมถึง ใช้เป็นพยานหลักฐาน
- ▶ มีหลักการ คือ
 - **หลักความเท่าเทียมกัน (Functional Equivalence)** ระหว่าง “กระดาษ” และ “ข้อมูล อิเล็กทรอนิกส์” เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ มีผลทางกฎหมาย เทียบเท่าการใช้กระดาษ
 - **หลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality)** ที่ไม่ระบุ เวพะเจาะจงเทคโนโลยีใดเทคโนโลยีหนึ่ง แต่รองรับพัฒนาการของเทคโนโลยีที่จะ เกิดขึ้นในอนาคต และ
 - **หลักเสรีภาพการแสดงเจตนา (Party Autonomy)** ของคู่สัญญา

1. พรະราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- ▶ "ธุรกรรม" หมายความว่า การกระทำใดๆ ที่เกี่ยวข้องกับกิจกรรมในการแพ่งและพานิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนด ใน หมวด 4
- ▶ "อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่าด้าน
- ▶ "ธุรกรรมทางอิเล็กทรอนิกส์" หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมด หรือแต่บางส่วน

1. พระราชบัณฑิตธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544)

- ▶ "ข้อความ" หมายความว่า เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ
- ▶ "ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

1. พระราชบัณฑิตธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- ▶ "ลายมือชื่ออิเล็กทรอนิกส์" หมายความว่า อักษร อักษรตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อรับบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกสนั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์
- ▶ "**ระบบข้อมูล**" หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์ สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวล ผลข้อมูลอิเล็กทรอนิกส์

1. พระราชบัณฑิตธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- ▶ "การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" หมายความว่า การส่งหรือรับข้อมูลความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า
- ▶ "ผู้ส่งข้อมูล" หมายความว่า บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการ ที่ผู้นั้นกำหนด โดยบุคคลนั้น อาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น
- ▶ "ผู้รับข้อมูล" หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประسูงค์จะส่งข้อมูล อิเล็กทรอนิกส์ให้ และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

1. พระราชบัณฑิตธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- ▶ "บุคคลที่เป็นสื่อกลาง" หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่งรับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใด อันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น
- ▶ "ໃบรับรอง" หมายความว่า ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูล สำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์
- ▶ "เจ้าของลายมือชื่อ" หมายความว่า ผู้ซึ่งถือข้อมูลส่วนตัวไว้ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ในนามตนเองหรือแทนบุคคลอื่น

1. พระราชบัณฑิตธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- ▶ "คู่กรณีที่เกี่ยวข้อง" หมายความว่า ผู้ซึ่งอาจกระทำการใด ๆ โดยขึ้นอยู่กับ ให้รับรองหรือ 赖以มีอิทธิพลต่ออิเล็กทรอนิกส์
- ▶ "หน่วยงานของรัฐ" หมายความว่า กระทรวง กบwing กรม ส่วนราชการที่เรียกชื่อ อย่างอื่น และมีฐานะเป็นกรรมการราษฎร์ส่วนภูมิ ภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัณฑิตหรือพระราชกฤษฎีกา และให้หมายความ รวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจ หน้าที่ดำเนินงานของรัฐไม่ ว่าในกรณีใด ๆ

หมวด 1 รุกกรรมทางอิเล็กทรอนิกส์

- ▶ (มาตรา 7, 8) การรับรองรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการรับ การส่งผ่านสื่ออิเล็กทรอนิกส์ สามารถใช้เป็นหนังสือ หรือหลักฐานเป็นหนังสือ
- ▶ (มาตรา 9) การยอมรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ (ลายมือชื่ออิเล็กทรอนิกส์) ให้ถือว่าเป็นการลงลายมือชื่อตามกฎหมาย หากใช้วิธีการตามที่กฎหมายกำหนดไว้
- ▶ (มาตรา 10, 12) การนำเสนอและเก็บรักษาข้อความที่เป็นข้อมูลอิเล็กทรอนิกส์ อย่างตั้งจริงใจ
- ▶ (มาตรา 15-24) การรับ การส่งข้อมูลอิเล็กทรอนิกส์
- ▶ (มาตรา 25) รุกกรรมทางอิเล็กทรอนิกส์ที่ดำเนินการที่น่าเชื่อถือ

WSU. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 7 ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา 8 ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

WSU. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 9 ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

- (1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และ
- (2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้

มาตรา 10 ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

WSU. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

มาตรา 13 คำเสนอ หรือคำสนองในการกำสัญญา อาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ และห้ามมิให้ปฏิเสธการมีผลทางกฎหมายของสัญญางานเพียงเราเหตุที่สัญญานั้นได้ทำคำเสนอ หรือคำสนองเป็นข้อมูลอิเล็กทรอนิกส์

WSU. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 22 การส่งข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการส่งเมื่อข้อมูลอิเล็กทรอนิกสนั่นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล

มาตรา 23 การรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่ามีผลบันดาลเวลาที่ข้อมูลอิเล็กทรอนิกสนั่นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล

WSU. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 32 บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่ในกรณีที่จำเป็นเพื่อรักษาความมั่นคงทางการเงินและการพำนิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือและยอมรับในระบบลายมือชื่ออิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณะชนให้มีการตราพระราชบัญญัติกำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ได้เป็นกิจการที่ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อนก็ได้

wsu. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- มาตรา 33** ในกรณีที่มีพระราชบัญญัติกำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ได้เป็นกิจการที่ต้องแจ้งให้ทราบ หรือต้องขึ้นทะเบียนให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้ง หรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชบัญญัติกำหนดเริ่มประกอบธุรกิจนั้น
- มาตรา 34** ในกรณีที่มีพระราชบัญญัติกำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องได้รับใบอนุญาต ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชบัญญัติ

พระบรมราชโองการ ว่าด้วยรัฐธรรมนูญอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 44 ผู้ได้ประกอบธุรกิจบริการเกี่ยวกับรัฐธรรมนูญอิเล็กทรอนิกส์ โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชบัญญัติตามมาตรา 33 วรรคหนึ่ง หรือโดยฝ่าฝืนคำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตามมาตรา 33 วรรคหก ต้องระหว่างโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 45 ผู้ได้ประกอบธุรกิจบริการเกี่ยวกับรัฐธรรมนูญอิเล็กทรอนิกส์ โดยไม่ได้รับใบอนุญาต ตามมาตรา 34 ต้องระหว่างโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ

กรณีศึกษา

- ▶ นายสัมโวได้ขอยืมเงินจากนางสาวน้อยหน้าโดยติดต่อกันทาง LINE และนางสาวน้อยหน้าได้ทำการโอนเงินให้รวม 4 ครั้งๆ ละ 50,000 บาท รวมเป็นเงิน 200,000 บาทด้วยวิธีทางอิเล็กทรอนิกส์ แต่นายสัมโวได้ชำระค่างวดไม่ครบ และนางสาวน้อยหน้ามีการทวงเงินที่ยังชำระไม่ครบทาง LINE
- ▶ **ตอบ**
 - ถือว่าบันติกรรมระหว่างนายสัมโวและนางสาวน้อยหน้าที่เกิดขึ้นเป็นธุรกรรมทางอิเล็กทรอนิกส์ประणegration ถูกกฎหมายโดยใช้เงินประणegration หนึ่งว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 7 มาตรา 8 และมาตรา 9

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

▶ ลายมือชื่ออิเล็กทรอนิกส์

- หมายความว่า อักษร อักษร ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์
- ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์
- โดยมีวัตถุประสงค์เพื่อรับบุคคลผู้เป็นเจ้าของลูกยมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นและเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อมูลอิเล็กทรอนิกส์นั้น

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

- ▶ ลักษณะของ “ลายมือชื่ออิเล็กทรอนิกส์” ตามกฎหมาย
 1. เป็นอักษร อักษร ตัวเลข เสียงหรือสัญลักษณ์อื่นใดในรูปของอิเล็กทรอนิกส์
 2. วัตถุประสงค์หรือหน้าที่ของลายมือชื่ออิเล็กทรอนิกส์คือ
 - เพื่อรับตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น
 - เพื่อแสดงว่าบุคคลดังกล่าวยอมรับในข้อมูลอิเล็กทรอนิกส์นั้น

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

- ▶ ลายมือชื่อจะเป็นลายมือชื่อที่บีบลงทางกฎหมาย ต้องปฏิบัติตามเงื่อนไข 2 ประการ (มาตรา 9) คือ
 - 1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูล อิเล็กทรอนิกส์นั้นว่าเป็นของตน และ
 - 2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้ เหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติกรรมนิเวศล้อมหรือข้อตกลงของคู่กรณัม

2. กฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2550

- ▶ ระบุการกระทำผ่าน/หรือโดยอาศัยคอมพิวเตอร์ในการกระทำความผิด มีวัตถุประสงค์มุ่งต่อระบบคอมพิวเตอร์ ข้อมูลของคอมพิวเตอร์ หรือบุคคล เพื่อให้เกิดความเสียหาย

2.1 ความผิด ตาม พ.ส.อ.คอมพิวเตอร์ พ.ศ. 2550

▶ จำแนกความผิดหลักได้ดังนี้

1. ใช้ username/password ของผู้อื่น Log in เข้าสู่ระบบ ([ผิด ม.5](#))
2. Forward email ที่มีข้อความ เนื้อหา หรือรูปภาพที่ไม่เหมาะสม เป็นเก็จ กระทำความมั่นคง หรือลามกอนาจาร ([ผิด ม.14](#))
3. โพสข้อความตามกระทู้ต่างๆที่มีเนื้อหา ไม่เหมาะสม เป็นเก็จ ([ผิด ม.14](#))
4. เพย์แพร์ภาพตัดต่อให้ผู้อื่นได้รับความเสียหาย หรืออับอาย ([ผิด ม.16](#))

2.1 ความผิด ตาม พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550

ฐานความผิด	โทษจำคุก	โทษปรับ
เข้าถึงคอมพิวเตอร์โดยไม่ชอบด้วยตั้งใจ	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
ล่วงรู้มาตราการป้องกัน	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
เข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ชอบด้วยตั้งใจ	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
การดักข้อมูลคอมพิวเตอร์	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
การรบกวนข้อมูลคอมพิวเตอร์	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
การรบกวนระบบคอมพิวเตอร์	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
ISP ที่ยอมให้เผยแพร่ข้อมูลที่ไม่เหมาะสม	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
สแปมเมล	ไม่มี	ไม่เกิน 100,000 บาท
การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
การจำหน่าย/เผยแพร่ Software ที่ใช้กระทำการผิด	ไม่เกิน 2 ปี	ไม่เกิน 20,000 บาท
การตัดต่อภาพผู้อื่น (โดยไม่สุจริต)	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท

ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: ใช้ user name/password ของผู้อื่น Log in เข้าสู่ระบบ

ฐานความผิด: มาตรา 5 ปรับไม่เกิน 10,000.- จำคุกไม่เกิน 6 เดือน



ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: Forward email ที่มีข้อความ เนื้อหา หรือรูปภาพที่ไม่เหมาะสม เป็นเก็จ กระทำความมั่นคง หรือลามกอนาจาร

ฐานความผิด: มาตรา 14 ปรับไม่เกิน 100,000.- จำคุกไม่เกิน 5 ปี

สื่อสารก หมายถึง สื่อที่ทำให้ผู้pubเห็นมีความรู้สึกซึ้งน่าอุจاذบัดสู่ นำอับอาย ส่วนใหญ่จะแสดงออกในรูปของภาพเปลือยมนุษย์ ภาพอวัยวะเพศกั้งหลังและชายน หรือภาพการร่วมเพศของมนุษย์

อนาจาร หมายถึง การกระทำที่ไม่สมควรในทางเพศ และก่อให้เกิดความอับอาย ในทางเพศ ซึ่งพิดไปจากประเพณีนิยมตามกาลเทศะ เช่น จุดแบบหลัง กอด จูบ จุดแบบหลังโดยที่หลังไม่ยันยอในที่สาธารณะ เป็นต้น

ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: โพสต์ข้อความตามกระทู้ต่างๆ ที่มีเนื้อหาไม่เหมาะสม เป็นเท็จ
กระทำความมั่นคง หรือลามกอนาจาร

ฐานความผิด: มาตรา 14 ปรับไม่เกิน 100,000.- จำคุกไม่เกิน 5 ปี

ข้อแนะนำ: ใช้วิจารณญาณในการแสดงความคิดเห็น และคำนึงถึงผลที่จะ
ตามมา



ตัวอย่างการกระกำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: พฤกที่ชอบเจาะระบบคอมพิวเตอร์ของผู้อื่น กีมีการสร้างระบบป้องกันไว้ (ถ้าเข้าเว็บสารานะ ก็ยอมไม่มีความผิด)

ฐานความผิด: มาตรา 5 ปรับไม่เกิน 10,000 บาท จำคุกไม่เกิน 6 เดือน



ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: เปิดเผยรหัส (Password) ที่ตัวเองรู้มา สำหรับเพื่อใช้เข้าระบบคอมพิวเตอร์

ฐานความผิด: มาตรา 6 ปรับไม่เกิน 20,000 บาท โทษจำคุก 1 ปี



ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: กำลังข้อมูล หรือไปเปลี่ยนแปลงข้อมูลของคนอื่น ไม่ว่าด้วย
วิธีใด จะใช้ไวรัส หรือแอบเข้าไปกำลังตรงๆ หรือพนักงานที่
ทำงานอยู่แล้วกำลังจะออกไปกำลังข้อมูล

ฐานความผิด: มาตรา 9 ปรับไม่เกิน 100,000 บาท จำคุกไม่เกิน 5 ปี

- ถ้าการกระทำดังกล่าวกระทำดึงความมั่นคงของประเทศ โดยจำคุก 3-15 ปี
- ถ้าการกระทำดังกล่าวเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย โดยจำคุก 10- 20 ปี

ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: ชอบส่งเมล์อันเป็นข้อมูลปลอม ข้อมูลเท็จ ใช้ร้ายป้ายสีคนอื่น หรือพากข่าวลือ ชอบปล่อยข่าวให้เกิดความวุ่นวาย รวมถึง ส่งภาพلامก่อน乍ด รวมถึงพากที่ได้รับแล้วส่งต่อ

ฐานความผิด: มาตรา 9 ปรับไม่เกิน 100,000 บาท จำคุกไม่เกิน 5 ปี

ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: ชوبส์ส่งเมล์ก่อความเสียหายสันค้าหรือบริการ
หรือส่งเมล์ขยะที่เข้าไม่ต้องการ

ฐานความผิด: มาตรา 11 ฐานก่อความชำรุด ปรับไม่เกิน 100,000 บาท

ตัวอย่างการกระกำความผิดเกี่ยวกับคอมพิวเตอร์

พฤติกรรม: ใช้ศิลปะเว็บตัว ตัดต่อภาพของคนอื่น และนำไปเผยแพร่ทางอินเตอร์เน็ต ทำให้เจ้าของภาพ อับอาย ยกเว้นกระทำการโดยสุจริตไม่ถือเป็นความผิด

ฐานความผิด: มาตรา 16 จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 60,000 บาท

การกระทำผิดจริยธรรมและผิดกฎหมาย

1. การขโมยข้อมูลทางอินเตอร์เน็ต ซึ่งรวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
2. ว่าชญากรนำเอาระบบการสื่อสารมาปกปิดความผิดของตนเอง
3. การละเมิดลิขสิทธิ์ปลอมแปลง เลียนแบบระบบซอฟต์แวร์ โดยมิชอบ
4. ใช้คอมพิวเตอร์พรั่งพราย เสียง لامก อนาจาร และข้อมูลที่ไม่เหมาะสม
5. ใช้คอมพิวเตอร์ฟอกเงิน
6. ก่อโภน กำลัยระบบสารานุปโภค เช่น ระบบจ่ายน้ำ จ่ายไฟ ระบบการจราจร
7. หลอกลวงให้ร่วมค้าขายหรือลงทุนปลอม
8. แทรกแซงข้อมูลแล้วนำข้อมูลนั้นมาเป็นประโยชน์ต่อตนโดยมิชอบ เช่น ลักทรัพย์คันหารหัสบัตรเครดิตของคนอื่นมาใช้ดักข้อมูลทำการค้า เพื่อเอาผลประโยชน์นั้นมาเป็นของตน
9. ใช้คอมพิวเตอร์แอบโอนเงินในบัญชีผู้อื่น เข้าบัญชีตัวเอง

3. กฎหมายขายตรงและตลาดแบบตรง พ.ศ.2545

- ▶ กำหนดให้ผู้ประกอบธุรกิจขายสินค้าทางอونไลน์ที่เข้าข่ายการ “ตลาดแบบตรง” ต้องจดทะเบียนการประกอบธุรกิจกับสำนักงานคณะกรรมการคุ้มครองผู้บริโภคก่อนทำการค้า

4. กฎหมายคุ้มครองผู้บริโภค

- ▶ “การโฆษณา” จะต้องไม่ใช้ข้อความที่ไม่เป็นธรรมต่อผู้บริโภคหรือใช้ข้อความที่อาจก่อให้เกิดผลเสียต่อสังคมเป็นส่วนรวม ไม่ว่าข้อความที่เกี่ยวกับแหล่งกำเนิด สภาพ คุณภาพ หรือลักษณะสินค้าหรือบริการ ตลอดจนการส่งมอบ จัดหา หรือใช้สินค้าหรือบริการ

5. กฎหมายทະเบียนพาณิชย์

- ▶ กระทรวงพาณิชย์ กำหนดให้ผู้ประกอบพาณิชย์กิจการซื้อขายสินค้าหรือบริการออนไลน์ การให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Web Hosting) และการบริการเป็นตลาดกลางพาณิชย์อิเล็กทรอนิกส์ (e-Marketplace) ต้องจดทะเบียนพาณิชย์

6. กฎหมายลิขสิทธิ์ พ.ศ.2537

- ▶ กำหนดสิทธิประโยชน์ให้แก่เจ้าของทรัพย์สินทางปัญญา และป้องกันดูแลผู้อื่นละเมิดลิขสิทธิ์ กังขาย เสนอขาย เพยแพร่ แจกจ่าย แสวงหากำไร วันสร้างความเสียหายให้แก่เจ้าของลิขสิทธิ์

7. กฎหมายว่าด้วยราคานิสิตและบริการ พ.ศ.2542

- ▶ ดูแลราคานิสิตต่างๆ ให้อยู่ในระดับราคากู้เหมาสม เพื่อให้เกิดการแบ่งขันทางการค้าที่เป็นธรรม ไม่มีการหั่นราคา รายใหญ่รั่งแกร่งรายเล็ก และกำหนดราคานิสิตตามอัตราเงินเฟ้อ

8. กฎหมายจดแจ้งการพิมพ์

- ▶ ตาม พ.ร.บ.จดแจ้งการพิมพ์ พ.ศ. 2550 กำหนดให้ผู้ประกอบการสื่อสิ่งพิมพ์ต้องจดแจ้งการพิมพ์ ซึ่งหมายรวมถึง ผู้ประกอบธุรกิจหนังสืออ่อนไลน์ หรือ e-book ด้วย แต่ไม่รวมถึงผู้ขายหรือร้านขายหนังสืออ่อนไลน์ที่ไม่ใช่ผู้ผลิตเอง

9. กฎหมายผลิตภัณฑ์อาหารและยา

- ▶ การขายผลิตภัณฑ์เกี่ยวกับอาหารและยา ก็งผลิตเอง หรือนำเข้า ต้องเป็นผลิตภัณฑ์อยู่ภายใต้การดูแลของสำนักงานคณะกรรมการอาหารและยา (อย.)

10. กฎหมายธุรกิจนำเที่ยวและมัคคุเทศก์ พ.ศ.2551

- ▶ ธุรกิจออนไลน์ที่ประกอบธุรกิจนำเที่ยวและมัคคุเทศก์ จะต้องดำเนินการข้อใบอนุญาตประกอบธุรกิจนำเที่ยวและมัคคุเทศก์ต่อกรมการท่องเที่ยว เสียก่อน



3. พรະราชาດุษฎีกา ว่าด้วย การควบคุมดูแลธุรกิจ
บริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551
(E-Payment)

พระราชบัญญัติ ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (E-Payment)

การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (e-Money) ได้แก่

1. ธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ที่ผู้ให้บริการต้องแจ้งให้ทราบ เช่น

- บัตรโดยสารสาธารณะ
- บัตรชำระค่าผ่านทางสาธารณะ
- บัตรชำระค่าอาหารและเครื่องดื่มภายในศูนย์อาหาร



พระราชบัญญัติ ว่าด้วยการควบคุมดูแลธุรกิจการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (E-Payment)

การประกอบธุรกิจการการชำระเงินทางอิเล็กทรอนิกส์ (e-Money) ได้แก่

2. ธุรกิจการการชำระเงินทางอิเล็กทรอนิกส์ที่ผู้ให้บริการต้องขึ้นทะเบียนก่อนให้บริการ เช่น

- การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network)
- การให้บริการเครือข่ายอีดีซี (EDC Network)
 - เครือข่ายการรับส่งข้อมูลที่มีศูนย์กลาง หรือจุดเชื่อมต่อการรับส่งข้อมูลระหว่างผู้ให้บริการเครือข่ายอีดีซี ด้วยอุปกรณ์หรือเครื่องมือ
 - สำหรับการรับส่งข้อมูลการชำระเงินทางอิเล็กทรอนิกส์จากบัตรเครดิต บัตรเดบิต เงินอิเล็กทรอนิกส์ หรือบัตรอิเล็กทรอนิกส์อื่นใด ไปยังผู้ให้บริการซึ่งออกบัตร

พระราชบัญญัติ ว่าด้วยการควบคุมดูแลธุรกิจการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (E-Payment)

การประกอบธุรกิจการการชำระเงินทางอิเล็กทรอนิกส์ (e-Money) ได้แก่

3. ธุรกิจการการชำระเงินทางอิเล็กทรอนิกส์ที่ผู้ให้บริการต้องได้รับอนุญาตก่อนให้บริการ เช่น

- การให้บริการหักบัญชี (Clearing)
- การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างใดอย่างหนึ่งหรือผ่านเครือข่าย



พระราชกฤษฎีกา ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทาง อิเล็กทรอนิกส์ พ.ศ. 2551 (E-Payment)

- การควบคุมดูแลและการประกอบธุรกิจของผู้ให้บริการแต่ละประเภท จะมีการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการให้บริการที่จำเป็น ซึ่งประกาศโดยธนาคารแห่งประเทศไทยในเรื่องดังต่อไปนี้
 - การออกหลักฐานการชำระเงิน
 - การเก็บรักษาเงินที่จะต้องส่งมอบ
 - การกำหนดผลสินสุดของการโอนเงินซึ่งผู้รับสามารถใช้เงินได้กับที่โดยปราศจากเงื่อนไข
 - การดำเนินการเพื่อรักษาสถานภาพทางการเงินของผู้ให้บริการ หรือ
 - การจัดให้มีผู้ตรวจสอบอิสระทางด้านความมั่นคงปลอดภัย

พระราชบัญญัติ ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (E-Payment)

- ผลของการที่ผู้ให้บริการผ้าฝ้ายหรือไม่ปฏิบัติพระราชบัญญัติพระราชบัญญัติ หรือประกาศของธนาคารแห่งประเทศไทย หรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
 - การห้ามประกอบธุรกิจ
 - การพักใช้ใบอนุญาต
 - การเพิกถอนใบอนุญาต



บทที่ 12

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)

- ▶ ย่อมาจาก Personal Data Protection Act B.E. 2562 (2019)
 - กฎหมายว่าด้วยการใช้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล
 - สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และ
 - นำไปใช้ให้ถูกตุณตามค่าธรรมเนียมที่เจ้าของข้อมูลส่วนบุคคล อนุญาต
- ▶ กฎหมาย PDPA Thailand (w.r.b.คุ้มครองข้อมูลส่วนบุคคล) ประกาศ ไว้ในราชกิจจานุเบกษาวันที่ 27 พฤษภาคม 2562 และให้มีผลบังคับใช้ ในวันที่ 1 มิถุนายน 2565

1. ข้อมูลส่วนบุคคล (Personal Data)

▶ ข้อมูลส่วนบุคคล

- คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ กังกางตรง หรือทางอ้อม แต่จะไม่รวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว

1. ข้อมูลส่วนบุคคล (Personal Data)

▶ ตัวอย่าง

- ชื่อ-นามสกุล หรือชื่อเล่น
- เลขประจำตัวประชาชน,
- เลขหนังสือเดินทาง,
- เลขบัตรประกันสังคม,
- เลขใบอนุญาตขับขี่,
- เลขประจำตัวผู้เสียภาษี,
- เลขบัญชีธนาคาร,
- เลขบัตรเครดิต
- (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาอยู่บนสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)
- ที่อยู่, อีเมล,
- เลขโทรศัพท์ / ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID /

- ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน /
 - ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิด และสถานที่เกิด, เชื้อชาติ, สัญชาติ, นำหน้า, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location),
- ข้อมูลการแพทย์,
- ข้อมูลการศึกษา,
- ข้อมูลทางการเงิน,
- ข้อมูลการจ้างงาน
- ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม่ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอิเล็กทรอนิกส์จะสามารถระบุไปถึงตัวบุคคลได้ /
- ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง /
- ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file /
- ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

1. ข้อมูลส่วนบุคคล (Personal Data)

▶ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

- ข้อมูล เชื้อชาติ, เผ่าพันธุ์,
- ความคิดเห็นทางการเมือง,
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา,
- พฤติกรรมทางเพศ,
- ประวัติอาชญากรรม,
- ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต,
- ข้อมูลสหภาพแรงงาน,
- ข้อมูลพันธุกรรม,
- ข้อมูลชีวภาพ,
- ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม เป็นต้น
- และข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

2. ធ្វើស៊ុនកំពើរបាយការណ៍ទូទៅ

- ▶ សាមរណដៃបង្ហាញអ្នកស៊ុនកំពើរបាយការណ៍ទូទៅ នៅក្នុងក្រុមហ៊ុន PDPA ត្រូវបានបញ្ជាក់ និងចាប់ផ្តើមនៅក្នុងក្រុមហ៊ុន នៅក្នុងក្រុមហ៊ុន និងចាប់ផ្តើមនៅក្នុងក្រុមហ៊ុន
- 1. **គោលការណ៍ទូទៅ** (Data Subject) គឺជាបុគ្គលកំពើរបាយការណ៍ទូទៅ ដែលមានសំណង់នៅក្នុងក្រុមហ៊ុន
- 2. **ជួយគោលការណ៍ទូទៅ** (Data Controller) គឺជាបុគ្គលកំពើរបាយការណ៍ទូទៅ ដែលមានសំណង់នៅក្នុងក្រុមហ៊ុន និងចាប់ផ្តើមនៅក្នុងក្រុមហ៊ុន
- 3. **ជួយគោលការណ៍ទូទៅ** (Data Processor) គឺជាបុគ្គលកំពើរបាយការណ៍ទូទៅ ដែលមានសំណង់នៅក្នុងក្រុមហ៊ុន និងចាប់ផ្តើមនៅក្នុងក្រុមហ៊ុន

2.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)

- ▶ คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้
- ▶ **สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right) ตามกฎหมาย**
 1. สิทธิได้รับการแจ้งให้ทราบ
 2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล
 3. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
 4. สิทธิขอให้ลบหรือกำลัง
 5. สิทธิในการเพิกถอนความยินยอม
 6. สิทธิขอให้ระงับการใช้ข้อมูล
 7. สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล
 8. สิทธิในการขอให้อ่อนข้อมูลส่วนบุคคล

2.1.1 สิทธิได้รับการแจ้งให้ทราบ

- ▶ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล
 - ยกเว้นเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว เช่น
 - ไปนาคราเพื่อจะไปเปิดบัญชี หรือ
 - การสมัครใช้พัลตภัณฑ์หรือบริการต่างๆ
 - โดยมีรายละเอียดการแจ้งให้ทราบ เช่น เก็บข้อมูลส่วนบุคคลอะไรบ้าง, วัตถุประสงค์การเก็บข้อมูล, การนำไปใช้หรือส่งต่อไปมีให้ใครบ้าง, วิธีเก็บข้อมูลอย่างไร, เก็บข้อมูลนานแค่ไหน, วิธีของการเปลี่ยนแปลง แก้ไข เพิกถอนข้อมูลส่วนบุคคลที่ให้ไปสามารถทำได้อย่างไรบ้าง

2.1.2 สิทธิขอเข้าถึงข้อมูลส่วนบุคคล

- ▶ เจ้าของข้อมูลส่วนบุคคล มีสิทธิ
 - ขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือ
 - ขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ ความยินยอมได้
- ▶ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น
- ▶ ถ้าไม่ขัดหรือส่งผลกระทบดังกล่าว เจ้าของข้อมูลส่วนบุคคลจะได้รับสิทธิภายใน 30 วันนับจากวันที่ ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับคำขอ

2.1.3 สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- ▶ เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเมื่อใดก็ได้
- ▶ แต่ต้องไม่ขัดด้วยกฎหมายที่สำคัญยิ่งกว่า หรือขัดต่อสิทธิการเรียกร้องตามกฎหมาย หรือข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สติ๊ติ

2.1.4 ສັກຮີຂອໃຫ້ລັບກົງເກົ່າໄລຍ

- ▶ ກຽນນີ້ກ່ຽວຂ້ອງຜູ້ຄວບຄຸມບັນດາມີສຳເນົາກັບຜູ້ອຳນວຍຕົວຢ່າງທີ່ມີຄວາມຮັບຮັດກັບຜູ້ອຳນວຍຕົວຢ່າງ
- ▶ ແລະຜູ້ຄວບຄຸມບັນດາມີສຳເນົາກັບຜູ້ອຳນວຍຕົວຢ່າງທີ່ມີຄວາມຮັບຮັດກັບຜູ້ອຳນວຍຕົວຢ່າງ
- ▶ ໂດຍຜູ້ຄວບຄຸມບັນດາມີສຳເນົາກັບຜູ້ອຳນວຍຕົວຢ່າງທີ່ມີຄວາມຮັບຮັດກັບຜູ້ອຳນວຍຕົວຢ່າງ

2.1.5 สิทธิในการเพิกถอนความยินยอม

- ▶ ถ้าเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไปแล้ว ต่อมา
ภายหลังต้องการยกเลิกความยินยอมนั้น ก็สามารถทำเมื่อใดก็ได้
- ▶ การยกเลิกความยินยอมนั้นจะต้องทำได้ง่ายเหมือนกับตอนแรกที่เจ้าของ
ข้อมูลให้ความยินยอมด้วย
- ▶ โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทาง
กฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้
ความยินยอมไปก่อนหน้านี้

2.1.6 สิทธิขอให้ระงับการใช้ข้อมูล

- ▶ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล
- ▶ ไม่ว่าจะในกรณีที่เกิดการรุ่เปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการกำล่ายข้อมูลเมื่อระบบกำหนดก็ต้องกำลัย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในการกฎหมาย หรือการเรียกร้องสิทธิ ก็สามารถทำได้

2.1.7 สีทึรีในการขอให้แก้ไขข้อมูลส่วนบุคคล

- ▶ เจ้าของข้อมูลมีสีทึรีกี่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้
- ▶ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย

2.1.8 สิทธิในการขอให้โอนข้อมูลส่วนบุคคล

- ▶ ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่ง ไปใช้กับผู้ควบคุมข้อมูลอีกราย
 - เช่น ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกได้ทำจัดทำข้อมูลส่วนบุคคลของเราไปในอยู่ในรูปแบบต่างๆ ที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ
- ▶ เจ้าของข้อมูลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลที่จัดทำข้อมูลนั้น ทำการส่งหรือโอนข้อมูลดังกล่าวให้ได้ หรือจะขอให้ส่งไปยังผู้ควบคุม ข้อมูลส่วนบุคคลรายอื่นโดยตรงก็สามารถทำได้ หากไม่ติดขัดทางวิธีการ และเทคนิค
- ▶ โดยการใช้สิทธินี้ต้องไม่ขัดต่อกฎหมาย สัญญา หรือลงทะเบียนสิทธิ เสรีภาพของบุคคลอื่น

2.2 ຜູ້ຄວບຄຸມຂ້ອມູລສ່ວນບຸຄຄລ (Data Controller)

- ▶ ຄໍ່ອ ບຸຄຄລຫຼືອົບຕິບຸຄຄລ ກີ່ມີສ່ວນໃນການ
 - ເກີບຮວບຮົມຂ້ອມູລສ່ວນບຸຄຄລ,
 - ໃຊ້ຂ້ອມູລສ່ວນບຸຄຄລ ກັບ
 - ເປີດເພຍຂ້ອມູລສ່ວນບຸຄຄລ
- ▶ ພາກເຮົາມີກາຣເກີບຂ້ອມູລສ່ວນບຸຄຄລຂອງຜູ້ອັນໄວ ກີ່ຄໍ່ວ່າເຮົາເປັນຜູ້ຄວບຄຸມ
ຂ້ອມູລສ່ວນບຸຄຄລ ກີ່ຈະຕ້ອງປະຕິບັດຕາມກັງໝາຍ PDPA ໄປດ້ວຍ
ເໜື້ອນກັນ

2.2 ຜູ້ຄວບຄຸມຂ້ອມູລສ່ວນບຸຄຄລ (Data Controller)

- ▶ ບຸຄຄລຣຣມດາ ມີຄວບຄຸມຂ້ອມູລສ່ວນບຸຄຄລ (ບຣິເຫັກ ພ້າງຮ້ານ ມູລນິຣີ ສາມາຄມ ມີນຳຍົງຈານ ວົງຄົກຮ້ານຄ້າ ມີຄວບຄຸມຂ້ອມູລສ່ວນບຸຄຄລໄວ້ ມີຄວບຄຸມຂ້ອມູລສ່ວນບຸຄຄລໄປໃຫ້ ມີນຳຍົງຈານໄດ້ຮັບ ຄໍາຍົນຍອມ (Consent) ຈາກເຈົ້າຂອງຂ້ອມູລດ້ວຍ ເວັນແຕ່ຈະເປັນໄປຕາມ ຂ້ອຍກເວັນທີ ພ.ຮ.ບ.ກໍາເນັດໄວ້ ໂດຍມີຂ້ອຍກເວັນໄວ້

2.2 ຜູ້ຄວບຄຸມຂໍ້ມູນສ່ວນບຸຄຄລ (Data Controller)

▶ ບ້າຍກເວັນ

- ຈັດທຳເວັກສາປະຈິບປາສຕຣ໌ ອີເວັບໄຊ ແຫ່ງທີ່ເກີດຂອງ ກັບ ການສຶກສາ ວິຈີຍ ອີເວັກສາ ຈັດທຳ ສົດໃຫຍ້
- ເພື່ອປົ້ນກັນ ອີເວັບໄຊ ດ້ວຍຕົວຢ່າງ ຕ່ອງຊີວິຕ ຮ່າງກາຍ ອີເວັບໄຊ ສຸຂພາພຂອງບຸຄຄລ
- ຈຳເປັນເພື່ອປົງປັງ ຕາມສັລະງົບ ແລະ ຂໍ້ມູນ ເຊັ່ນ ການຊ້ອຍຊາຍຂອງອອນໄລນ໌ ຕ້ອງ ໃຊ້ໂສ່ວນ ທີ່ໄວ້ຢູ່ ເບຣົຣ ຖຣສັພທ໌ ວິເມັລ
- ຈຳເປັນເພື່ອປະໂຫຍດ ສັດໃຫຍ້ ແລະ ການປົງປັງ ຕ່ອງຊີວິຕ ທີ່ໃນການໃຊ້ວຳນາຈරັດ
- ຈຳເປັນເພື່ອປະໂຫຍດ ດ້ວຍກົງໝາຍຂອງຜູ້ຄວບຄຸມ ຂໍ້ມູນສ່ວນບຸຄຄລ ອີເວັບໄຊ ອີເວັບໄຊ ອີເວັບໄຊ
- ເປັນການປົງປັງ ຕາມກົງໝາຍຂອງຜູ້ຄວບຄຸມ ຂໍ້ມູນສ່ວນບຸຄຄລ ເຊັ່ນ ສົ່ງຂໍ້ມູນພັກງານ ໃຫ້ກຽມສຽງພາກ ເຮືອງການ ເປັນຕົ້ນ

2.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

▶ ข้อยกเว้น

- การดำเนินกิจกรรมที่ขอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไร เช่น เรื่องศาสนาหรือความคิดเห็นทางการเมือง ซึ่งจำเป็นต้องเปิดเผยให้ทราบก่อนเข้าองค์กรนั้น ๆ เป็นต้น
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล ส่วนบุคคล เช่น บุคคลสาธารณะที่มีข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วในความ ยินยอมของเจ้าของข้อมูล

2.2 ຜູ້ຄວບຄຸມຂ້ອມຸລສ່ວນບຸຄຄລ (Data Controller)

▶ ບ້າຍກເວັນ

- ເປັນການຈຳເປັນເພື່ອກາຮັດວຽກກ່ອຕັ້ງສີທິເຣີກຮ້ອງຕາມກົງໝາຍ ກາຮັດວຽກຕາມກົງໝາຍ ແລະ ປົບປັດຕົວກົງໝາຍ ແລະ ດັບລາຍນິ້ວມືອຂອງຜູ້ທີ່ບຸກຮຸກເພື່ອນຳໄປໃຫ້ໃນຫຼັນສາລ ເປັນຕົ້ນ
- ເປັນການຈຳເປັນໃນກາຮັດວຽກຕາມກົງໝາຍເພື່ອໃຫ້ບຣລຸວັຕຖຸປະສົງຄ ເກີຍວັກບ ເວຊ ສາລຕົຮປ້ອງກັນຫຼືອວັນເວຊາສາລຕົຮ ເຊັ່ນ
 - ◆ ກາຮັດວຽກຂ້ອມຸລສຸຂພາພຂອງພນັກງານທີ່ຈຳເປັນຕົ້ນເກີບຂ້ອມຸລສ່ວນບຸຄຄລທີ່ມີຄວາມລະເວີຍດອ່ອນ (Sensitive Personal Data)
- ອົງຄໍກຮັດວຽກໃຫ້ຂ້ອນນີ້ໃນກາຮັດວຽກທີ່ຈຳເປັນຕົ້ນເກີບຂ້ອມຸລນີ້ໄວ້ ເປັນຕົ້ນ / ປະໂຍ່ນ໌ ດ້ວຍສາລາຮັດວຽກ, ກາຮັດວຽກຕົ້ມຄຮອງແຮງງານ, ກາຮັດວຽກຕົ້ມສັ່ນຄມ, ອັດກປະກັນສຸຂພາພ ແຮ່ງໜ້າຕົກ / ກາຮັດວຽກຕົ້ມກົງໝາຍທາງວິທຍາສາລຕົຮ, ປະວັດທິສາລຕົຮ, ສົດຕິ, ຫຼືອປະໂຍ່ນ໌ ສາລາຮັດວຽກ / ປະໂຍ່ນ໌ສາລາຮັດວຽກທີ່ສຳຄັນ

3. ข้อมูลเก่าที่เคยเก็บไว้ก่อนที่ W.S.U

- ▶ คำถาม: ข้อมูลเก่าที่เคยเก็บไว้ก่อนที่ W.R.U. นี้จะบังคับใช้ ต้องทำอย่างไร?
- ▶ ข้อมูลส่วนบุคคลที่ได้เก็บรวมไว้ ก่อน PDPA จะบังคับใช้ใน วันที่ 1 มิถุนายน 2565 ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องตามมาตรา ๙๕ ใน W.R.U. ได้ระบุไว้ว่า
 - ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม
 - ห้าม ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอม และเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวม และใช้ข้อมูลส่วนบุคคลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

4. սանցութ

- ▶ Այս 3 պրեգե լինենք՝
 1. Խեցացքային
 2. Խեցացքային
 3. Խեցացքային

4.1 ໂທເຫາງແພັ່ງ

- ▶ ໃຫ້ໃຊ້ຄ່າສິນໄໝມກດແກນທີ່ເກີດຂຶ້ນຈົງໃຫ້ກັບເຈົ້າຂອງຂ້ວມູລສ່ວນບຸຄຄລທີ່ໄດ້ຮັບຄວາມເສີຍຫາຍຈາກກາຣະເມີດ
- ▶ ແລະຈາວຈະຕ້ອງຈ່າຍບວກເພີ່ມອັກເປັນຄ່າຄ່າສິນໄໝມກດແກນເພື່ອກາຣົງໂທເປີເພີ່ມເຕີມສູງສຸດໄດ້ອັກ 2 ເຖ່ງຄ່າເສີຍຫາຍຈົງ
- ▶ ຕັວຢ່າງ
 - ຂາກສາລຕັດສິນໃຫ້ຜູ້ຄວບຄຸມຂ້ວມູລສ່ວນບຸຄຄລ ຕ້ອງໃຊ້ຄ່າສິນໄໝມກດແກນແກ່ເຈົ້າຂອງຂ້ວມູລສ່ວນບຸຄຄລ ເປັນຈຳນວນ 1 ແສນບາກ ສາລວາຈມີຄຳສັ້ງ ກຳນົດຄ່າສິນໄໝມເພື່ອກູຣົງໂທເປີເພີ່ມອັກ 2 ເຖ່ງຄ່າເສີຍຫາຍຈົງ ເຖ່ກັບ ຈະຕ້ອງຈ່າຍເປັນຄ່າປັບກັງໜົດ ເປັນຈຳນວນເຈີນ 3 ແສນບາກ

4.2 ໂທເຫາງອານຸາ

- ▶ ຈະມີກັ້ງໂທເຈົ້າຄຸກແລະໂທເປັບ
- ▶ ມີໂທເຈົ້າຄຸກສູງສຸດໄມ່ເກີນ 1 ປີ ມີກັ້ງໂທເປັບໄມ່ເກີນ 1 ລ້ານບາທ ມີກັ້ງຈຳກັ້ງໂທເປັບ
- ▶ ໂທເສູງສຸດດັ່ງກ່າວຈະເກີດຈາກການໃນປະເທດຕາມ PDPA ໃນສ່ວນການໃຫ້ຂ້ອມຸລ ມີກັ້ງເປີດເພຍຂ້ອມຸລ ມີກັ້ງສົ່ງໂວນຂ້ອມຸລໄປຢັງຕ່າງປະເທດ ປະເກດຂ້ອມຸລທີ່ມີຄວາມລະເວີຍດວອນ(Sensitive Personal Data)
- ▶ ກຣນີ້ຫາກຜູ້ກະໜາຄວາມພິດ ຄື່ວ ບຣິເຫັກ(ບົດບຸດຄລ)
 - ໃຄຣຈະເປັນຜູ້ຄຸກຈຳກຸກ ເພຣະບຣິເຫັກຕິດຄຸກໄມ່ໄດ້ ອາຈຈະເປັນຜູ້ບຣິຫາຽງ, ກຣນກາຣ ມີກັ້ງບຸດຄລຊື່ງຮັບພິດຂອບໃນການດຳເນີນງານຂອງບຣິເຫັກນັ້ນ ຫຼື ຈະຕ້ອງໄດ້ຮັບການລອງໂທເຈົ້າຄຸກແກບ

4.3 ໂທເທາງປກຄຣອງ

- ▶ ໂທເປີປັບ
- ▶ ມີຕັ້ງແຕ່ 1 ລ້ານບາກຈົນດຶງສູງສຸດໄມ່ເກີນ 5 ລ້ານບາກ
- ▶ ໂທເປີປັບສູງສຸດ 5 ລ້ານບາກ ຈະເປັນກຽນຂອງການໄມ່ປັບປຸດຕາມ PDPA ໃນສ່ວນການໃຫ້ຂ້ອມຸລ ຮັ້ອເປີດເພຍຂ້ອມຸລ ຮັ້ອສ່ົງໂວນຂ້ອມຸລໄປຢັງ ຕ່າງປະເທດຂອງປະເທດຂ້ອມຸລທີ່ມີຄວາມລະເວິຍດວ່ອນ(Sensitive Personal Data)
- ▶ ໂທເທາງປກຄຣອງນີ້ຈະແຍກຕ່າງໆກັບການຊັບໃຊ້ຄ່າເສີຍຫາຍທີ່ເກີດຈາກໂທເທາງແພິ່ງແລະໂທເທາງອານາ