



กฎหมายทางด้านเทคโนโลยีสารสนเทศ

พ.ต.ท.ดร.ณ จาดเจริญ

รองผู้กำกับการ กลุ่มงานตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี
กองบังคับการสนับสนุนทางเทคโนโลยี



ความรู้เบื้องต้นเกี่ยวกับกฎหมายแพ่ง-กฎหมายอาญา

	กฎหมายแพ่ง	กฎหมายอาญา
ลักษณะของกฎหมาย	จะว่าด้วย สิทธิ หน้าที่ และ ความสัมพันธ์ระหว่างเอกชนด้วยกัน	ว่าด้วยความสัมพันธ์ระหว่างรัฐกับเอกชน ที่มีการบัญญัติความผิดที่ห้ามกระทำไว้ โดยส่วนใหญ่ต้องรับโทษในฐานะความผิดที่ได้กระทำนั้น
วัตถุประสงค์ของกฎหมาย	รักษาความยุติธรรมในความสัมพันธ์ระหว่างเอกชนด้วยกัน หรือ ระหว่างรัฐกับเอกชนในกรณีที่รัฐมีสิทธิในฐานะเอกชน	มีไว้เพื่อรักษาความสงบเรียบร้อยของบ้านเมือง ผู้ใดละเมิดกฎหมายอาญา ถือได้ว่าจะละเมิดต่อรัฐโดยตรง
การตีความกฎหมาย	- ต้องตีความตามตัวอักษร หรือตามความมุ่งหมายของบทบัญญัติแห่งกฎหมาย - หากไม่มีบทกฎหมายที่จะยกขึ้น ปรับแก้คดีได้ ให้วินิจฉัยคดีนั้นตามจารีตประเพณีแห่งท้องถิ่น	- ต้องตีความอย่างเคร่งครัด ตามตัวอักษรที่กฎหมายได้บัญญัติไว้ ไม่สามารถขยายความไปถึงฐานความผิดที่เทียบเคียงกันได้ - ไม่มีผลย้อนหลัง และ จะไม่มีความผิด ถ้ากฎหมายไม่ได้บัญญัติความผิดไว้
สภาพบังคับ	การล่วงละเมิดทางแพ่ง จะต้องชดใช้คืนเจ้าหน้าที่	บัญญัติโทษไว้ 5 สถาน คือ ประหารชีวิต จำคุก กักขัง ปรับ และ ริบทรัพย์สิน



การกระทำธุรกรรม/การทำนิติกรรม

ผู้ทำนิติกรรมคู่สัญญา

ตัวสัญญาหรือข้อตกลงใน
การทำธุรกรรม

การยืนยันความถูกต้องของ
การทำธุรกรรม / นิติกรรม

แนวทางการวินิจฉัย กรณี
คู่สัญญาเห็นไม่ตรงกัน หรือ
เกิดข้อพิพาท

คู่สัญญารู้จักกัน/แสดงเจตนาต่อหน้า

มีสัญญาฉบับ / เอกสารที่ใช้ในการ
ตรวจสอบกรณีเกิดการผิดไปจากเดิม

คู่กรณีเห็นพ้องกันต่อหน้า
หรือการมีพยานยืนยัน

มีบทบัญญัติเป็นแนวทางการวินิจฉัย
เช่นประมวลกฎหมายแพ่ง ฯ

ทำให้เกิดความน่าเชื่อถือในการทำธุรกรรม

High Tech Crime Center



การกระทำธุรกรรมทางอิเล็กทรอนิกส์

คู่สัญญารู้จักกัน/แสดงเจตนาต่อหน้า

มีสัญญาฉบับ / เอกสารที่ใช้ในการ
ตรวจสอบกรณีเกิดการผิดไปจากเดิม

คู่กรณีเห็นพ้องกันต่อหน้า
หรือการมีพยานยืนยัน

มีบทบัญญัติเป็นแนวทางการวินิจฉัย
เช่นประมวลกฎหมายแพ่ง ฯ

คู่สัญญาไม่ได้พบหน้า หรือไม่เคยรู้จักกัน

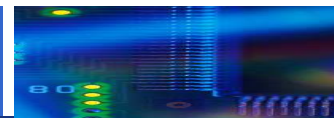
ตัวสัญญาไม่ได้อยู่ในรูปแบบ
ของกระดาษ

อาจไม่ต้องกระทำต่อหน้า
และไม่มีพยานบุคคล

แนวทางการวินิจฉัยเดิมอาจ
ไม่สามารถปรับใช้ได้

ต้องมีกระบวนการสร้างความน่าเชื่อถือใหม่

High Tech Crime Center

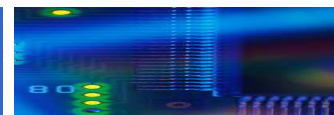


กระบวนการสร้างความน่าเชื่อถือ

- 1 **การกำหนดให้มีผลบังคับใช้ทางกฎหมาย**
- 2 **กำหนดแนวทางในการระบุตัวผู้ทำธุรกรรม/คู่สัญญา**
- 3 **กำหนดแนวทางรักษา/ตรวจสอบความถูกต้องของสัญญา**
- 4 **กำหนดแนวทางการตรวจสอบความถูกต้องของการทำธุรกรรม**
- 5 **กำหนดแนวทางการวินิจฉัย**

หลักการทางคอมพิวเตอร์คือ **การระบุตัวตน (Authenticity)** , **การรักษาความลับ (Confidentiality)** **การรักษาความถูกต้อง (Integrity)**, **การป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation)**

High Tech Crime Center



การกำหนดให้มีผลในทางกฎหมาย (Functional Equivalent Approach)

ให้มีผลผูกพันและบังคับใช้ได้ตามกฎหมาย รวมถึงสามารถใช้เป็นหลักฐานในทางคดีใดๆได้

เอกสารใดหากต้องมีหลักฐานเป็นหนังสือ ก็สามารถใช้ข้อมูลอิเล็กทรอนิกส์ที่จัดทำขึ้น โดยความหมายไม่เปลี่ยนแปลงมาใช้แทนได้ หรือหากเอกสารนั้นต้องมีการลงลายมือชื่อ ต้องจัดให้มีวิธีลงลายมือชื่อ แต่สามารถเลือกวิธีลงลายมือชื่อตามที่ตกลงกัน

High Tech Crime Center



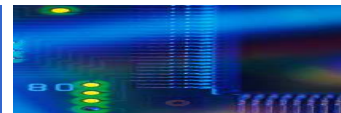
กำหนดแนวทางในการระบุตัวคู่สัญญา

มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ในการเชื่อมโยงไปยังตัวบุคคล
โดยการใช้งานดังกล่าวต้องมีส่วนที่ทำให้ตรวจสอบได้

มีตัวแทนที่ถือแทนตัวได้ เช่น ผู้ทำการแทน
หรือ ระบบที่ใช้ในการส่งข้อมูลอัตโนมัติ

เพื่อสร้างความน่าเชื่อถือที่ทั้งสองฝ่ายยอมรับ
อาจจะให้มีผู้ออกใบรับรองการใช้ลายมือชื่อดังกล่าวได้

High Tech Crime Center



กำหนดแนวทางรักษาความถูกต้องของสัญญา

ยึดถือความหมายของข้อความในเอกสาร
มากกว่ารูปแบบทางดิจิทัลที่สามารถเปลี่ยนแปลงรูปแบบได้

สามารถใช้ข้อมูลอิเล็กทรอนิกส์แทนเอกสารที่บอกว่าเป็นต้นฉบับได้
หากกระบวนการจัดทำเอกสาร และการจัดเก็บมีความน่าเชื่อถือ

วัดความน่าเชื่อถือจากกระบวนการสร้าง เก็บรักษา สื่อสาร
และ ข้อมูลเกี่ยวกับการสร้าง การเก็บรักษาและการสื่อสาร

High Tech Crime Center



กำหนดแนวทางการวินิจฉัย

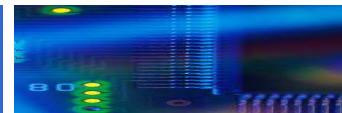
ผู้ใดเป็นผู้ส่งข้อมูล ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้นั้น

ผู้รับ(คำสนอง) สามารถดำเนินการได้ หากเชื่อว่า เป็นข้อมูลของผู้ส่ง(คำเสนอ)ที่แท้จริง (เว้นแต่มีการโต้แย้ง หรือควรรู้ว่าอาจไม่ใช่ข้อมูลของผู้ส่ง หรือเป็นข้อมูลที่มีความผิดพลาดหากได้ใช้ความระวังพอสมควรซึ่งอาจมีการตรวจสอบตามสมควร)

ผู้ส่งต้องได้รับการตอบรับโดยวิธีหนึ่งวิธีใด หากไม่ได้รับการตอบรับให้ถือว่า ข้อมูลที่ส่งนั้นมิได้มีการส่ง หากมีการตอบรับ สันนิษฐานได้เพียงว่า มีการรับ แต่ไม่ได้หมายความว่าได้รับข้อมูลนั้นอย่างถูกต้อง

การนับเวลาการส่งและการรับข้อมูล , การถือว่าสถานที่ใดเป็นสถานที่รับ-ส่งข้อมูล

High Tech Crime Center



การกระทำความผิดอาญาที่เกี่ยวข้องกับคอมพิวเตอร์



High Tech Crime Center

คอมพิวเตอร์เข้ามาเกี่ยวข้องกับอาชญากรรมอย่างไร

1

การใช้คอมพิวเตอร์เป็นเครื่องมือ (Tools)

2

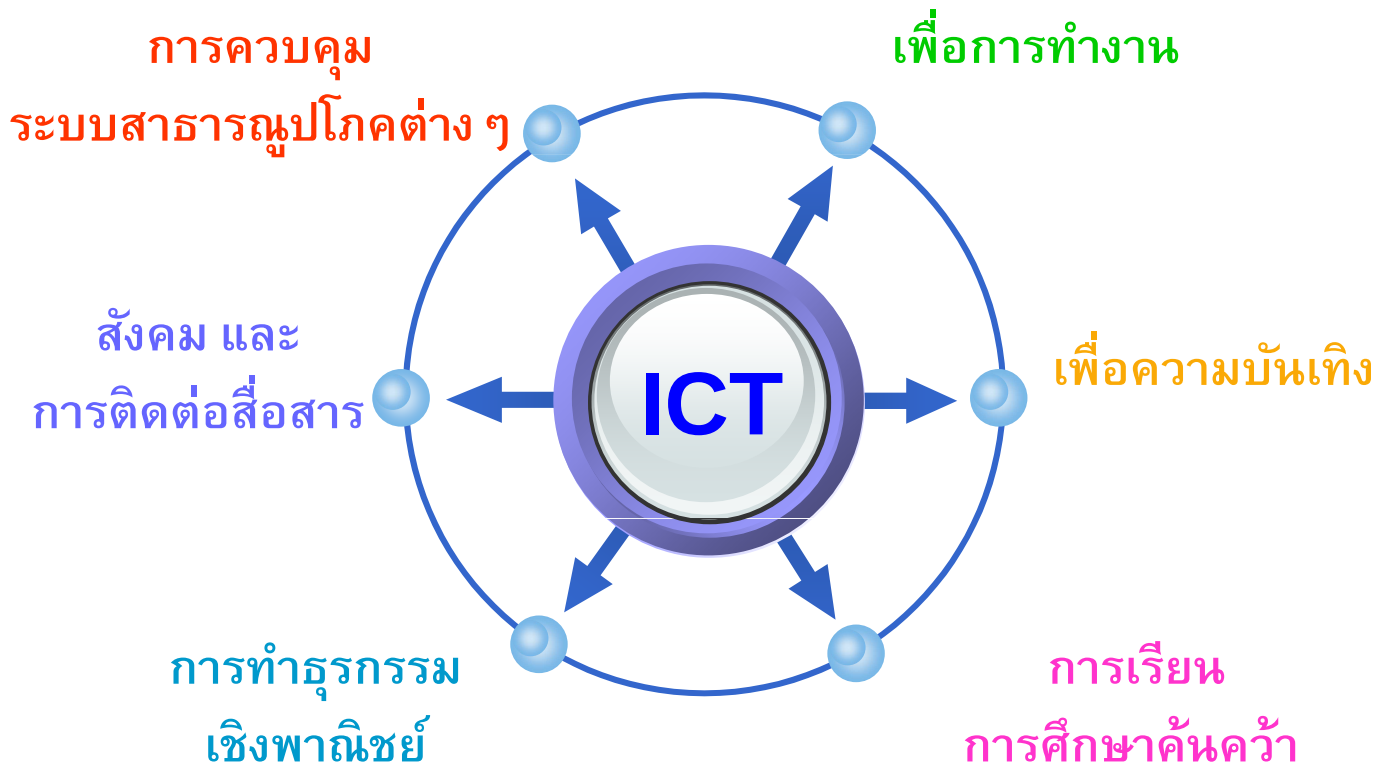
การมองคอมพิวเตอร์เป็นเป้าหมาย (Target)

3

การใช้คอมพิวเตอร์เป็นเครื่องช่วยในการกระทำความผิด

High Tech Crime Center – Royal Thai Police

การใช้งานเทคโนโลยีในปัจจุบัน



High Tech Crime Center – Royal Thai Police



เหตุที่มาของพ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

1

ลักษณะการกระทำความผิดที่ไม่ครอบคลุม

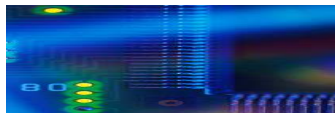
2

พยานหลักฐานที่ต้องการจากเดิม

3

พยานหลักฐานและแนวทางปฏิบัติในการรวบรวม
พยานหลักฐาน

HIGH-TECH CRIME
CENTER



พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

1

ความผิดใหม่ที่ถูกบัญญัติเพิ่ม

2

พยานหลักฐาน และบุคคลที่เกี่ยวข้อง

3

เจ้าหน้าที่และอำนาจดำเนินการ

HIGH-TECH CRIME
CENTER



ลักษณะความผิดที่ถูกระบุไว้ตาม พ.ร.บ.

- 1 ความผิดที่เกี่ยวกับระบบคอมพิวเตอร์และสารสนเทศ
- 2 ความผิดที่เกี่ยวกับการเผยแพร่เนื้อหา
- 3 ความผิดเกี่ยวกับผู้ให้บริการ
- 4 ความผิดเกี่ยวกับการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่

HIGH-TECH CRIME
CENTER



ความผิดที่เกี่ยวข้องโดยตรงกับระบบสารสนเทศ

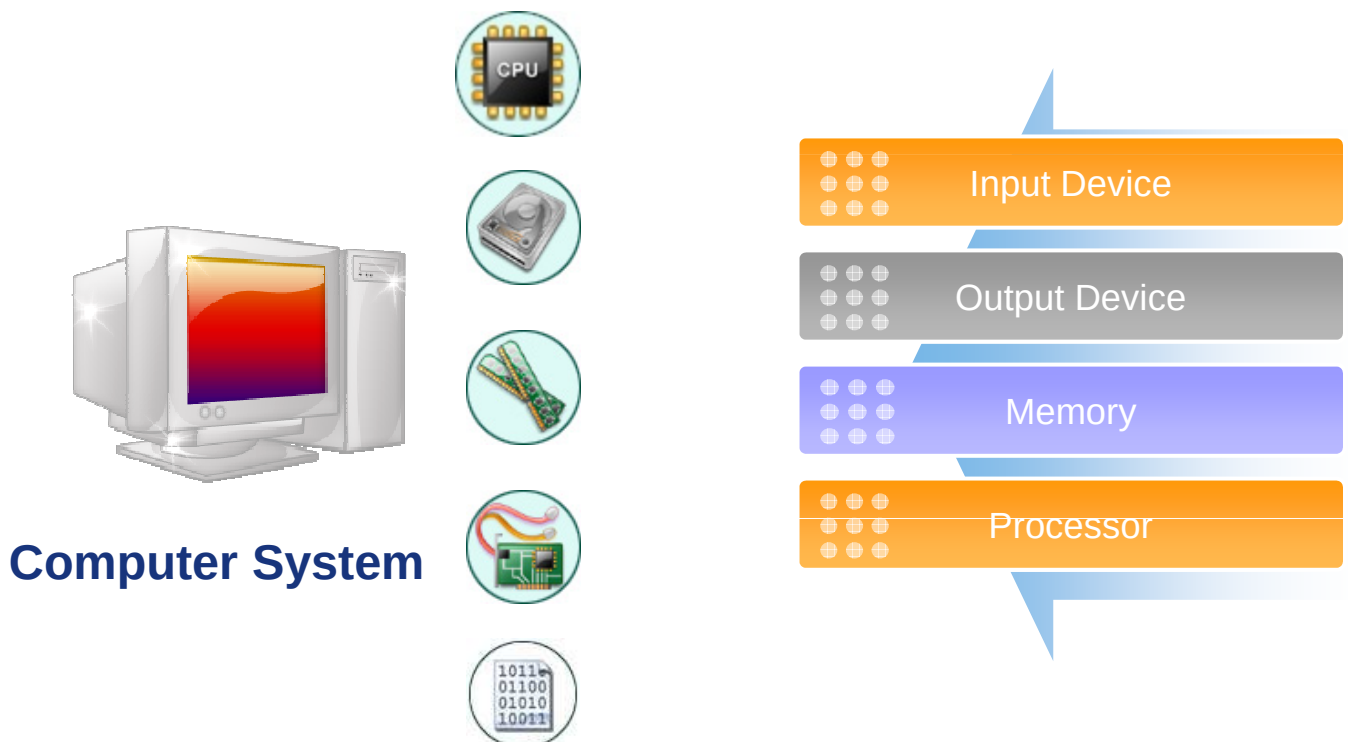
- 1 การเข้าถึงระบบและข้อมูลคอมพิวเตอร์โดยมิชอบ
- 2 การเปิดเผยมาตรการป้องกันระบบ
- 3 การแก้ไข เปลี่ยนแปลง ข้อมูลคอมพิวเตอร์โดยมิชอบ
- 4 การดักจับข้อมูลทางอิเล็กทรอนิกส์
- 5 การรบกวนระบบคอมพิวเตอร์
- 6 การส่งข้อมูลอิเล็กทรอนิกส์รบกวนการใช้งาน

HIGH-TECH CRIME CENTER

นิยาม : ระบบคอมพิวเตอร์

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

นิยาม : ระบบคอมพิวเตอร์



นิยาม : ระบบคอมพิวเตอร์



Network & Communication Device

HIGH-TECH CRIME CENTER

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์
ที่มีมาตรการป้องกันการเข้าถึง
โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้อง
ระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกิน
หนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

องค์ประกอบฐานความผิด

การเข้าถึง

การเข้าถึงทาง
กายภาพ

การเข้าถึงผ่านทาง
ระบบเครือข่าย

ระบบคอมพิวเตอร์
มีลักษณะที่เป็น
Live

โดยมิชอบ

ไม่มีอำนาจ หรือไม่มี
สิทธิในการเข้าถึงใน
ส่วนนั้น ๆ

หรือเคยมีสิทธิ แต่
ปัจจุบันไม่มีสิทธิ

ต้องรู้ว่าตนเองไม่มีสิทธิ

ไม่จำเป็นต้องมีเจตนา
ทุจริต

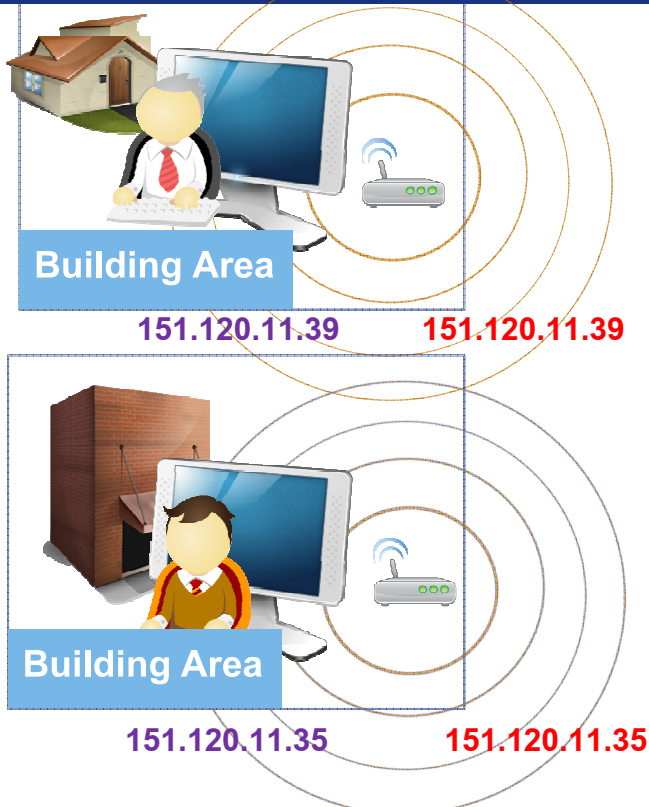
มาตรการป้องกัน

ความหมายของ
มาตรการป้องกัน

การรับทราบเรื่อง
มาตรการป้องกัน

การรองรับมาตรการ
ป้องกันของระบบ
คอมพิวเตอร์บาง
ประเภท

War Driving



151.120.11.40





การเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่น

1.

ระบบต้องมีมาตรการในการป้องกัน

2.

ไม่ได้ระบุว่าต้องผ่านมาตรการป้องกัน
เข้าไปในระบบ

3.

มีความหมายครอบคลุม ทั้งการเข้าถึงทางอุปกรณ์
(Hardware) โดยตรง และ การเข้าถึงจากระยะไกล

4.

การวินิจฉัยเรื่องคำว่า “เข้าถึง” และ
“พยายาม” (เพื่อระบุมิให้เกิดความเสียหาย
ขึ้น ก่อนที่ระบบจะถูกเข้าถึงได้อย่างสมบูรณ์)



ภาระงานของผู้ดูแลระบบที่ต้องเพิ่มขึ้น (ตาม ม.5)

1

กำหนดนโยบายในการเข้าถึงระบบ (ทางกายภาพ) ที่ชัดเจน

2

กำหนดตัวผู้ใช้ระบบ(Account) และสิทธิที่ชัดเจน

3

ให้ความรู้แก่ผู้ใช้ระบบให้เห็นถึงความสำคัญของสิทธิ

4

ให้ความรู้แก่ผู้ใช้ระบบด้านความปลอดภัยและความเสี่ยง

5

กำหนดแผนในการรองรับการเข้าถึงระบบโดยมิชอบ

6

กำหนดแนวทางในการการรวบรวมพยานหลักฐาน



กฎหมายที่เกี่ยวข้องกับการบริหารจัดการผู้ใช้ในองค์กร

การกำหนดสิทธิในการเข้าใช้งานระบบ	<u>พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 5</u>
การกำหนดสิทธิในการเข้าถึงข้อมูล	<u>พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 7</u>
การตรวจสอบข้อมูลการใช้งาน	<u>พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 8</u>
การจัดเก็บข้อมูลของผู้ใช้บริการ	<u>ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์</u>

High Tech Crime Center

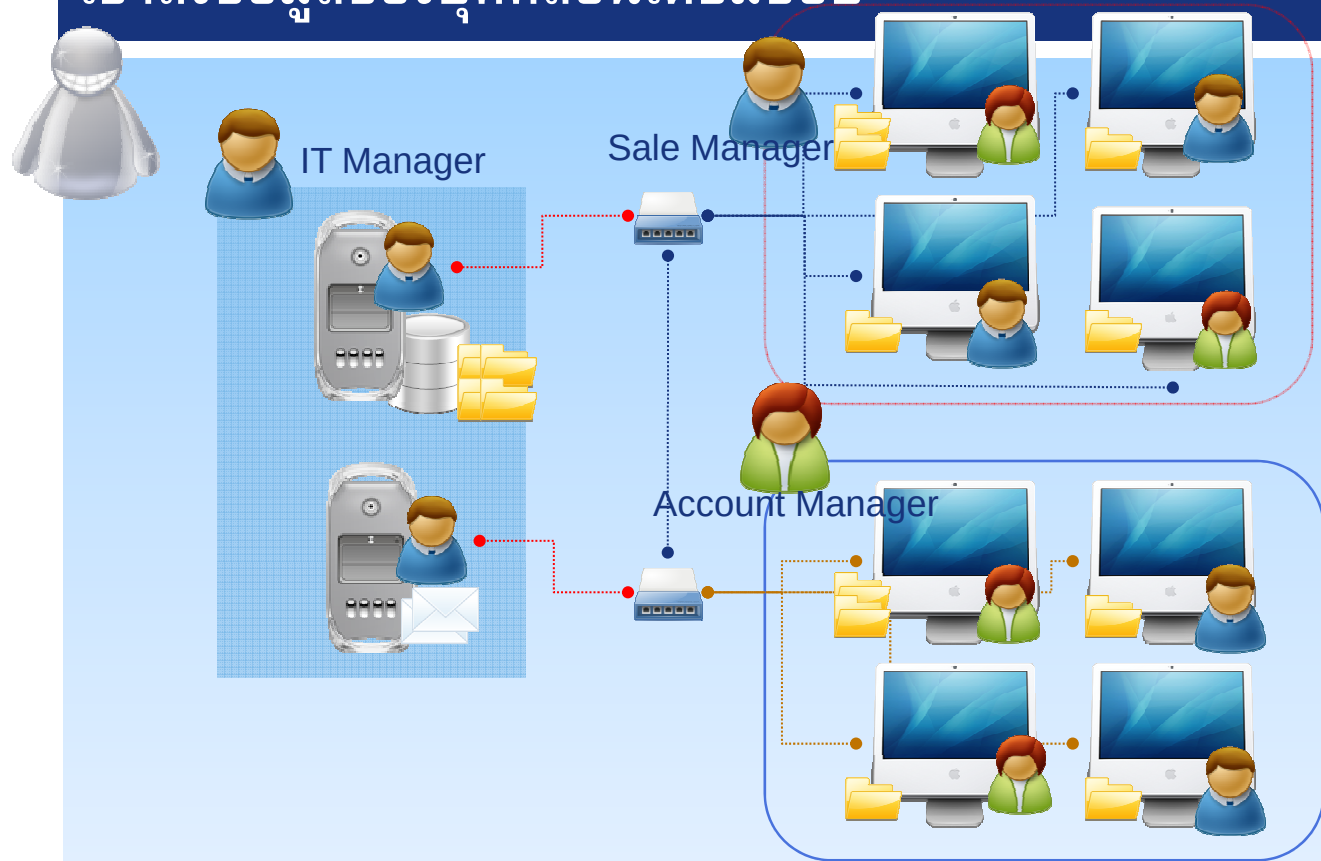


เข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

HIGH-TECH CRIME CENTER

เข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ



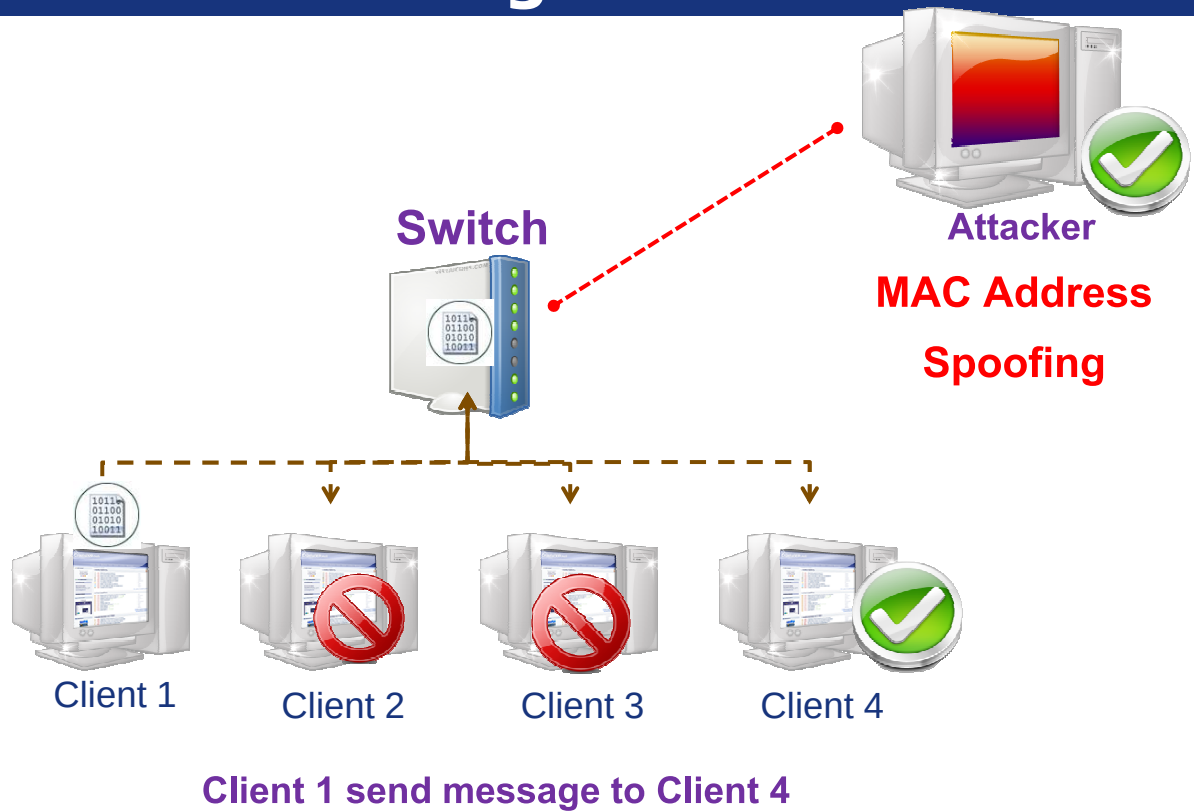
HIGH-TECH CRIME
CENTER

การดักจับข้อมูลคอมพิวเตอร์

มาตรา ๘ ผู้ใดกระทำความผิดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกิน สามปี หรือปรับไม่เกิน หกหมื่นบาท หรือทั้งจำทั้งปรับ

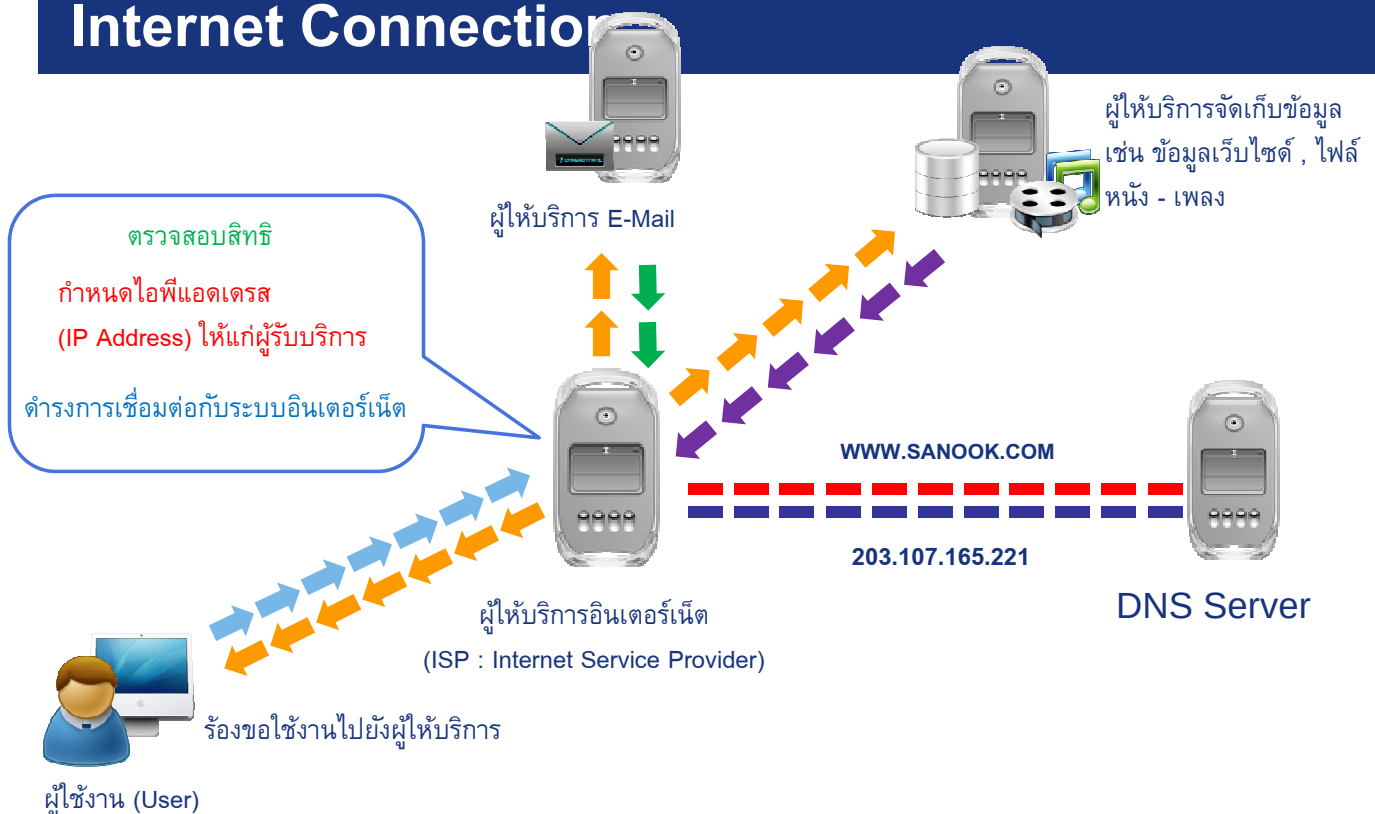
HIGH-TECH CRIME CENTER

Packet Sniffing

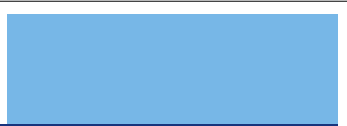
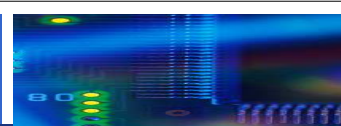


HIGH-TECH CRIME CENTER

Internet Connection



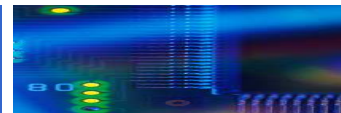
High Tech Crime Center



การแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูล

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือ บางส่วน ซึ่ง ข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ ต้องระวางโทษ จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

HIGH-TECH CRIME CENTER



รบกวนการทำงานของเครื่องคอมพิวเตอร์

มาตรา ๑๐ ผู้ใดกระทำความผิดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกรับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุก ไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

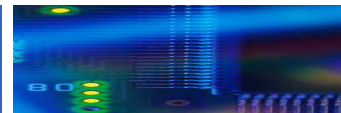
HIGH-TECH CRIME CENTER



Spam Mail

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

HIGH-TECH CRIME CENTER



การบริหารจัดการความเสี่ยงทาง IT(IT Risk Management)

➔ Incident Response Planning

➔ Business Continuity Planning & Disaster Recovery Planning

High Tech Crime Center



Computer Incident



การขัดขวาง / รบกวน กระบวนการตามปกติ และ
นำไปสู่ระดับที่มีความเสียหาย



สถานการณ์ที่ข้อมูลสารสนเทศอยู่ในสถานะเสี่ยง



เกิดความผิดพลาดในการรักษาความปลอดภัย หรือ
มีกระบวนการคุกคาม



Computer Incident



อุปกรณ์เกิดความเสียหาย



Unauthorized Access



การโจมตีทางระบบเครือข่าย Network Attack



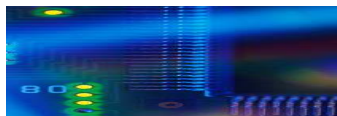
Virus Infection



Theft of Resource

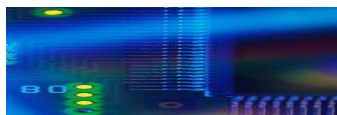


Pornographic



CERT Team Service

- 1 การกระบวนกรตอบโต้เบื้องต้น
- 2 การจัดเก็บและสงวนรักษาพยานหลักฐาน
- 3 การกู้คืนสถานะจากความเสียหาย
- 4 การวิเคราะห์รูปแบบการคุกคาม/โจมตี
- 5 การทำงานร่วมกับเจ้าหน้าที่บังคับใช้กฎหมาย



Tools & Process

- 1 Penetration Testing Tools
- 2 Intrusion Detection Tools
- 3 Network Analysis Tools
- 4 Forensic & Analysis Tools





Q & A