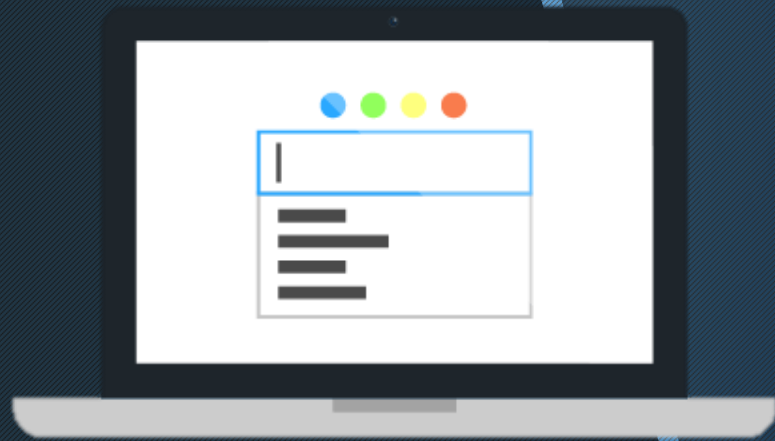


# กฎหมาย และ จริยธรรมในการใช้ งานเทคโนโลยีดิจิทัล

ภาวิตา คำชาย ไพบุลย์ ชูวัฒน์กิจ ผู้เขียน  
พิมพ์พลอย ธีรสกิตธรรม ผู้บรรยาย



# ความเป็นมาและความสำคัญ ของจริยธรรมสารสนเทศ

“

จริยธรรมสารสนเทศเป็นแนวคิดที่พัฒนามานานหลายปีในสาขาของบรรณรักษ์ศาสตร์และสารสนเทศ แพร่หลายมาสู่ศาสตร์สาขาอื่น ๆ

“

ความรู้เท่าทันสารสนเทศกลายเป็นทักษะชีวิตที่สำคัญทักษะหนึ่งในศตวรรษที่ 21



# ความเป็นมาและความสำคัญของจริยธรรมสารสนเทศ

จริยธรรมสารสนเทศมีความสำคัญ

“

จริยธรรมสารสนเทศสร้างสรรค์วัฒนธรรมของความไว้วางใจ

“

ความรับผิดชอบ

“

ความสมบูรณ์และความเป็นเลิศของการใช้ทรัพยากรสารสนเทศ

“

ส่งเสริมความเป็นส่วนตัว ความลับของสารสนเทศ

“

ช่วยป้องกันความขัดแย้ง ความคดโกงในการใช้สารสนเทศและการใช้สารสนเทศ  
ในทางที่ผิด

## ความเป็นมาและความสำคัญของจริยธรรมสารสนเทศ

จุดประสงค์ของการมีจริยธรรมสารสนเทศ จำแนกได้ ดังนี้

“

ตอบสนองการเติบโตในยุคโลกาภิวัตน์ (Globalization) เทคโนโลยีสารสนเทศถือเป็นกลไกสำคัญ

“

ประการที่สอง สนับสนุนความสงบ คือ รักษาสิทธิพื้นฐานของมนุษย์เท่า ๆ กับส่งเสริมความหลากหลาย จริยธรรมสารสนเทศจะช่วยดำรงไว้ซึ่งสิทธิมนุษยชน ส่งเสริมศักดิ์ศรีของความเป็นมนุษย์ และก่อให้เกิดความเท่าเทียมกันและการยอมรับนับถือซึ่งกันและกัน ซึ่งถือเป็นฐานแห่งความสงบแบบยั่งยืนของสังคม

“

ประการที่สาม ประกันคุณภาพของการเรียนรู้ เป็นมาตรการสำคัญประการหนึ่งที่ใช้ประกันคุณภาพของการเรียนรู้อย่างต่อเนื่อง

## กรอบความคิดและความหมายของจริยธรรมสารสนเทศ

ความรู้เท่าทันสารสนเทศนั้นหากเริ่มจากเฉพาะเจาะจงขึ้นมาจะได้แก่

“

สารสนเทศด้านเทคโนโลยี

“

สารสนเทศด้านสังคม

“

สารสนเทศด้านชีวิต เป็นทักษะการสื่อสารที่มีความหมายกว้าง



# พฤติกรรมและรายละเอียดที่ควรพิจารณาในเชิงจริยธรรมสารสนเทศ ในชีวิตประจำวัน

## “ การได้มาซึ่งสารสนเทศ

การเข้าถึงสารสนเทศ การเลือกสารสนเทศ การลงรหัส การทวนสอบ ความถูกต้อง  
พยากรณ์ผลที่ตามมา ความต้องการใช้ตามบริบท (งาน ปัญหา ประเภทเครื่องมือและความ  
ขาด)

## “ การใช้สารสนเทศ

การเสีย/ไม่เสียค่าใช้จ่าย การเซ็นเซอร์ ลิขสิทธิ์ การใช้ในด้านต่าง ๆ (กฎหมาย การค้า  
การศึกษา)

# พฤติกรรมและรายละเอียดที่ควรพิจารณาในเชิงจริยธรรมสารสนเทศ ในชีวิตประจำวัน

“

## การเรียบเรียงความรู้

ความตรงของสารสนเทศ โครงสร้างของความรู้ ความน่าเชื่อถือ คุณภาพของสารสนเทศ และ การกลั่นกรอง

“

## รูปแบบเครือข่ายสังคม

ชุมชนความรู้ การคุ้มครองสารสนเทศ ความรับผิดชอบ และการสื่อสาร ของเครือข่าย

# พฤติกรรมและรายละเอียดที่ควรพิจารณาในเชิงจริยธรรมสารสนเทศ ในชีวิตประจำวัน

“

## การแบ่งปันสารสนเทศ

ความเป็นส่วนตัว การจัดการความรู้ เสรีภาพในการแสดงออก และการเป็นความลับของสารสนเทศ

“

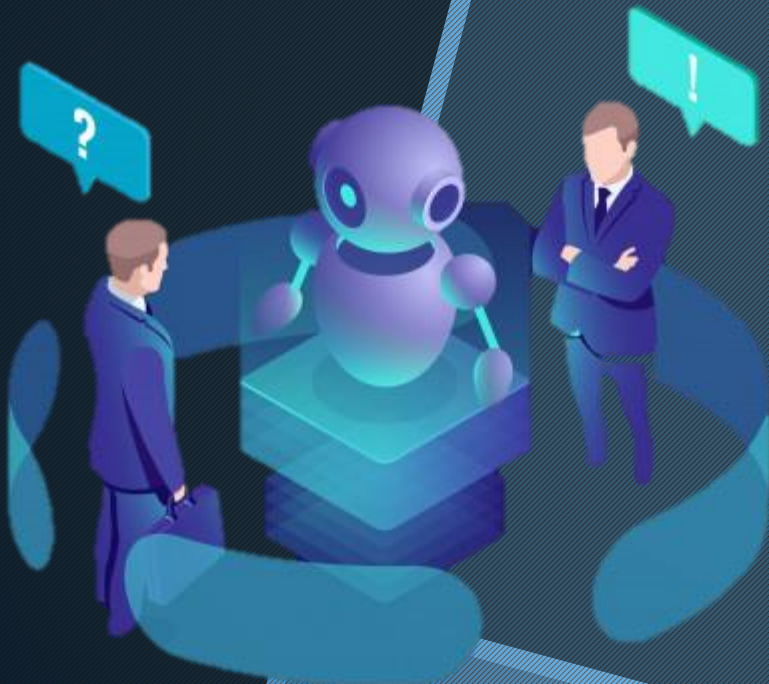
## การติดต่อ online

ความปลอดภัย การคุ้มครอง การทวนสอบว่าเป็นความจริง พฤติกรรมต่อต้านสังคม (การขโมย การก่ออาชญากรรม การใส่ความ การหลอกลวง การส่งสารสนเทศไปยังคนกลุ่มใหญ่โดยที่ไม่ได้รับอนุญาต (spamming))



## ประเด็นการพิจารณาจริยธรรมสารสนเทศ

1. ความเป็นส่วนตัว
2. ความถูกต้องแม่นยำ
3. ความเป็นทรัพย์สิน
4. การเข้าถึง



## วิธีการป้องกันการละเมิดจริยธรรมสารสนเทศ

1. ทวนกลับไปยังจุดเริ่มต้น
2. ประเมินแหล่งข่าว
3. ประเมินข่าวสาร
4. ทำทนายข่าวสาร
5. ถ้ามชุมชนในเว็บไซต์
6. ตรวจสอบตนเองก่อนเผยแพร่ต่อ



## กรณีตัวอย่างที่เสี่ยงต่อการเข้าข่ายละเมิดจริยธรรมสารสนเทศ

“กรณี 1 นักท่องเที่ยวเปิดดูเว็บไซต์เพื่อหาที่พักราคาประหยัดในต่างจังหวัด พบว่า มีสถานที่พักเสนอภาพห้องพัก สวยและสะอาด แต่เมื่อไปถึงพบว่าห้องที่ได้พักจริงต่างออกไปจากห้องที่นำเสนอ แม้ว่าจะมีการจัดห้องเหมือนกันแต่สภาพเก่าและทรุดโทรม

“กรณี 2 มีสินค้ามือสองประกาศขายทางเว็บโดยอ้างว่าเป็นสินค้ายี่ห้อดัง เกรด A ผลิตจากประเทศอิตาลี เจ้าของใช้มือเดียว และประกาศขายครึ่งราคาของราคาจริง เมื่อผู้ซื้อพอใจและสั่งซื้อและจ่ายเงินไปแล้ว ปรากฏว่าเป็นสินค้าเลียนแบบ ผลิตจากประเทศเพื่อนบ้านแต่สภาพใหม่และดูผาดูๆจะคล้ายของจริง

## กรณีตัวอย่างที่เสี่ยงต่อการเข้าข่ายละเมิดจริยธรรมสารสนเทศ

“ กรณี 3 มีโทรศัพท์จากสายนอกมาถึงขณะที่เรากำลังทำงานอยู่ โดยถามถึงเพื่อนร่วมงานที่ทำงานห้องเดียวกับเรา เมื่อตอบว่าไม่อยู่ก็ขอโทรศัพท์และอีเมล โดยอ้างว่าจะติดต่องานด้วย เราเลยให้ไป

“ กรณี 4 นาย A ปลุกพืชสมุนไพร และทดลองใช้ผสมกันเพื่อรักษาโรคปวดเมื่อย และเห็นว่าได้ผลจึงแจกเพื่อนบ้าน โดยอ้างว่าได้ผ่านการทดลองทางวิทยาศาสตร์มาแล้ว

## กรณีตัวอย่างที่เสี่ยงต่อการเข้าข่ายละเมิดจริยธรรมสารสนเทศ

“

กรณี 5 นางสาวนก ได้รับข้อมูลทางไลน์ว่ามีผู้ยินดีให้ทุนสนับสนุนโรงเรียนยากจน โรงเรียนละ 1 ล้านบาท โดยให้ติดต่อไปยังเบอร์โทรศัพท์ที่แจ้งไว้ นางสาวนกจึงส่งต่อทางเฟซบุค ปรากฏว่าเมื่อโทรไปเจ้าของเบอร์โทรศัพท์บอกว่าไม่เคยรู้เรื่องนี้

“

กรณี 6 เพื่อนถ่ายรูปเพื่อนขณะใส่ชุดว่ายน้ำลงโปสในเฟซบุคครั้งไปเที่ยวทะเลด้วยกันโดยเจ้าของภาพไม่รู้เรื่องนี้

การประยุกต์ความเข้าใจ  
เชิงกฎหมาย

# การพัฒนากฎหมายสารสนเทศของประเทศไทยในยุคดิจิทัล

กฎหมายเทคโนโลยีสารสนเทศทั้ง 6 ฉบับ

- 1) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- 2) กฎหมายว่าด้วยลายมือชื่ออิเล็กทรอนิกส์
- 3) กฎหมายว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์
- 4) กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์
- 5) กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
- 6) กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน



# กฎหมายว่าด้วยลิขสิทธิ์

## การคุ้มครองลิขสิทธิ์

- (1) เป็นการสร้างสรรค์งานนั้นด้วยตนเอง
- (2) เป็นการแสดงออกซึ่งงานในชนิดที่กฎหมายรับรอง
- (3) เป็นการแสดงออกซึ่งทางความคิดกฎหมายลิขสิทธิ์
- (4) ต้องไม่ใช่งานที่กฎหมายกำหนดไม่ให้มีลิขสิทธิ์
- (5) เป็นงานที่ไม่ขัดต่อกฎหมาย





# กฎหมายว่าด้วยลิขสิทธิ์

## งานที่กฎหมายรับรอง

- 1) งานวรรณกรรม (literary work)
- 2) โปรแกรมคอมพิวเตอร์ (computer software)
- 3) งานนาฏกรรม (dramatic work)
- 4) งานศิลปกรรม (artistic work)
- 5) งานดนตรีกรรม (musical work)
- 6) งานโสตทัศนวัสดุ (audio-visual work)
- 7) ภาพยนตร์ (cinematographic works)
- 8) งานแพร่เสียงแพร่ภาพ (sound and video broadcasting works)



# กฎหมายว่าด้วยลิขสิทธิ์

สิทธิแต่เพียงผู้เดียว (Exclusive Right)

- (1) ทำซ้ำ
- (2) ดัดแปลง
- (3) นำเผยแพร่ต่อสาธารณชน
- (4) การให้เช่าต้นฉบับหรือสำเนาบางส่วนประเภท



# ปัญหาทางกฎหมายเกี่ยวกับการละเมิดงานอันมีลิขสิทธิ์ทางอินเทอร์เน็ต

## การละเมิดงานแพร่เสียงแพร่ภาพ

“

การนำออกสู่สาธารณชนโดยกฎหมายบัญญัติไว้ 3 วิธีการ ได้แก่ (1) การแพร่เสียงทางวิทยุกระจายเสียง (2) การแพร่เสียงและหรือภาพทางวิทยุโทรทัศน์ และ (3) โดยวิธีอย่างอื่นอันคล้ายคลึงกัน

“

ปัญหาคือ จะถือว่าผู้แพร่เสียงแพร่ภาพผ่านทางอินเทอร์เน็ตจะได้รับการคุ้มครองในฐานะเป็นเจ้าของงานแพร่เสียงแพร่ภาพในฐานะเป็นโดยวิธีอย่างอื่นอันคล้ายคลึงกับการแพร่เสียงทางวิทยุกระจายเสียง หรือทางวิทยุโทรทัศน์ ตามความในกฎหมายหรือไม่

# ปัญหาทางกฎหมายเกี่ยวกับการละเมิดงานอันมีลิขสิทธิ์ทางอินเทอร์เน็ต

“

การเปิดเว็บไซต์ผ่านเบราว์เซอร์ (browser) และการแคชชิ่ง (caching)

“

ปัจจุบันพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558 ได้เพิ่มมาตรา 32/2 ในพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ว่า

“

“การกระทำแก่งานอันมีลิขสิทธิ์ที่ทำหรือได้มาโดยชอบด้วยกฎหมายในระบบคอมพิวเตอร์ที่มีลักษณะเป็นการทำซ้ำที่จำเป็นต้องมีสำหรับการนำสำเนามาใช้เพื่อให้อุปกรณ์ที่ใช้ในระบบคอมพิวเตอร์ หรือกระบวนการส่งงานอันมีลิขสิทธิ์ทางระบบคอมพิวเตอร์ทำงานได้ตามปกติ มิให้ถือว่าเป็นการละเมิดลิขสิทธิ์”

# ปัญหาทางกฎหมายเกี่ยวกับการละเมิดงานอันมีลิขสิทธิ์ทางอินเทอร์เน็ต

การเชื่อมโยงด้วยไฮเปอร์ลิงก์ (Hyperlink) และการเชื่อมโยงแบบลึก (deep link)

“

ภายใต้พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 การเชื่อมโยงแบบลึก หรือ deep linking น่าจะถือไม่ได้ว่าเป็นการทำซ้ำงานอันมีลิขสิทธิ์ของผู้อื่น เพราะการลิงก์เข้าสู่เว็บไซต์เป็นเพียงช่องทางไปสู่เว็บไซต์นั้นเท่านั้น แม้จะไม่ได้เข้าผ่าน home page แต่ก็ไม่มีลักษณะทำซ้ำแต่ประการใด



## ข้อมูลการบริหารสิทธิ

“

“ข้อมูลที่บ่งชี้ถึงผู้สร้างสรรค์ งานสร้างสรรค์ นักแสดง การแสดง เจ้าของ ลิขสิทธิ์ หรือระยะเวลาและเงื่อนไขการใช้งานอันมีลิขสิทธิ์ ตลอดจนตัวเลขหรือ รหัสแทนข้อมูลดังกล่าว โดยข้อมูลเช่นนี้ติดอยู่หรือปรากฏเกี่ยวข้องกับงาน อันมีลิขสิทธิ์หรือสิ่งบันทึกการแสดง”

“

การกระทำต่อข้อมูลการบริหารสิทธิเป็นความผิดในตัวเอง



## มาตรการทางเทคโนโลยี

“

“เทคโนโลยีที่ออกแบบมาเพื่อป้องกันการทำซ้ำหรือควบคุมการเข้าถึงงานอันมีลิขสิทธิ์หรือสิ่งบันทึกการแสดง โดยเทคโนโลยีเช่นว่านี้ได้นำมาใช้กับงานอันมีลิขสิทธิ์หรือสิ่งบันทึกการแสดงนั้นอย่างมีประสิทธิภาพ”

“

การกระทำต่อข้อมูลการบริหารสิทธิ์เป็นความผิดในตัวเอง



## กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 แบ่ง  
อธิบายในที่นี่ออกเป็น 2 ส่วน

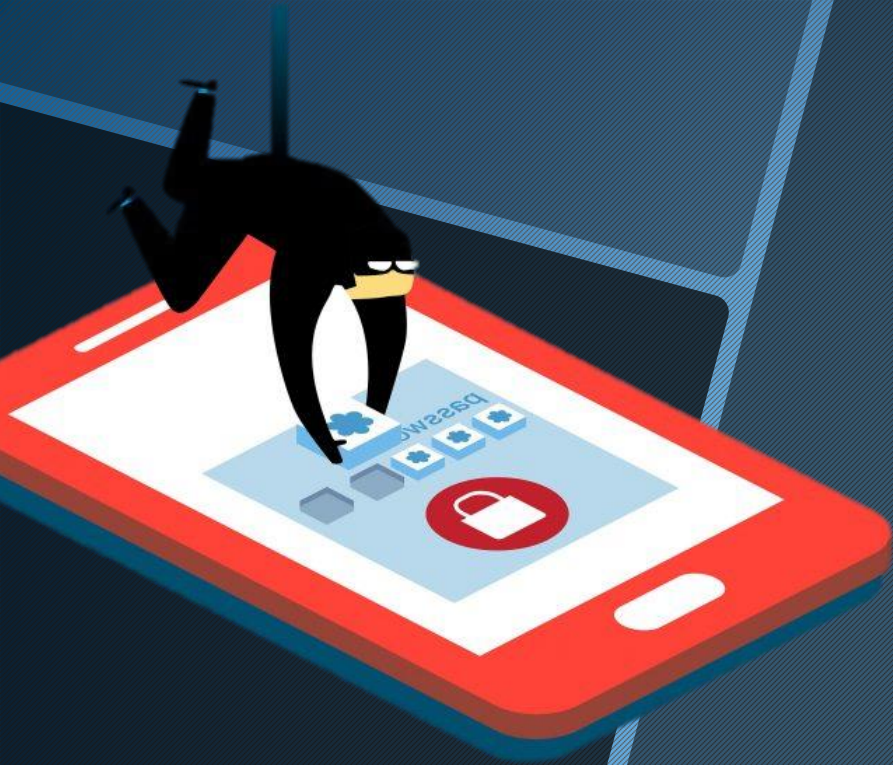
“

ส่วนแรก เป็นการกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์และบทกำหนดโทษ

“

ส่วนที่สอง เป็นเรื่องเกี่ยวกับอำนาจหน้าที่และความรับผิดชอบของพนักงานเจ้าหน้าที่ในการปฏิบัติงานตามกฎหมายฉบับนี้





## ลักษณะการกระทำความผิด

- (1) การกระทำต่อระบบคอมพิวเตอร์
- (2) การกระทำต่อข้อมูลคอมพิวเตอร์

“

นอกจากนี้ ยังมีฐานความผิดอื่นที่มิได้มีเจตนากระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ แต่ใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการให้เกิดความเสียหายต่อสังคมด้วย

## การกระทำต่อระบบคอมพิวเตอร์

“

“ระบบคอมพิวเตอร์” คือ

“

“อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ”



## การกระทำต่อระบบคอมพิวเตอร์

“

จากนิยามดังกล่าว ระบบคอมพิวเตอร์ ประกอบด้วย

- (1) ตัวเครื่องคอมพิวเตอร์ ได้แก่ อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน เช่น จอภาพคีย์บอร์ดเมาส์และเคสซีพียู และ
- (2) ซอฟต์แวร์ที่ทำให้ตัวเครื่องคอมพิวเตอร์ประมวลผลข้อมูลอัตโนมัติ เช่น ระบบปฏิบัติการวินโดวส์ เป็นต้น ดังนั้น หากคอมพิวเตอร์ที่ต่ออุปกรณ์เข้ากันหมด ยังไม่ได้ลงซอฟต์แวร์ให้คอมพิวเตอร์สามารถประมวลผลได้โดยอัตโนมัติ ก็ไม่ถือเป็นระบบคอมพิวเตอร์

## การกระทำต่อระบบคอมพิวเตอร์

ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

“

ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมีได้มีไว้สำหรับตน โดยเจตนา



## การกระทำต่อระบบคอมพิวเตอร์

เข้าถึง -- ไม่จำกัดวิธีการการ อาจแยกได้ เป็น

(1) การเข้าถึงทางกายภาพ

(2) การเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้บุคคลนั้นจะอยู่ห่างจากเครื่องคอมพิวเตอร์

(3) การเข้าถึงผ่านทางเครือข่ายสาธารณะ

## การกระทำต่อระบบคอมพิวเตอร์

“

ความผิดฐานเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิ

ชอบ

“

“ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”



## การกระทำต่อระบบคอมพิวเตอร์

ความผิดฐานเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ  
ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้น  
เป็นการเฉพาะ นำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิด  
ความเสียหายแก่ผู้อื่นเจตนา

## การกระทำต่อระบบคอมพิวเตอร์

การรบกวนระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

“

“ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”



## การกระทำต่อระบบคอมพิวเตอร์

การรบกวนระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

“

ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้

“

ตัวอย่างของการกระทำความผิดตามมาตรานี้ ได้แก่ การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service : DoS)

## การกระทำต่อระบบคอมพิวเตอร์

“

การรบกวนระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

ความผิดฐานนี้บทกำหนดโทษหนักขึ้น หากการกระทำความผิดดังกล่าว เข้าลักษณะอย่างใดอย่างหนึ่งดังนี้

- ก) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าจะความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่
- ข) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

## การกระทำต่อข้อมูลคอมพิวเตอร์

การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ระบบคอมพิวเตอร์  
ของบุคคลอื่น

“

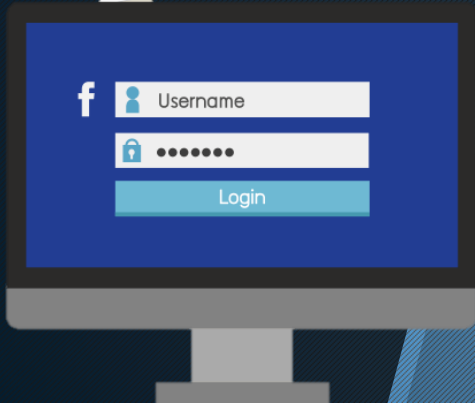
“ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดย  
ปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการ  
รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษ  
ปรับไม่เกินหนึ่งแสนบาท”

## การกระทำต่อข้อมูลคอมพิวเตอร์

การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ระบบคอมพิวเตอร์  
ของบุคคลอื่น

“

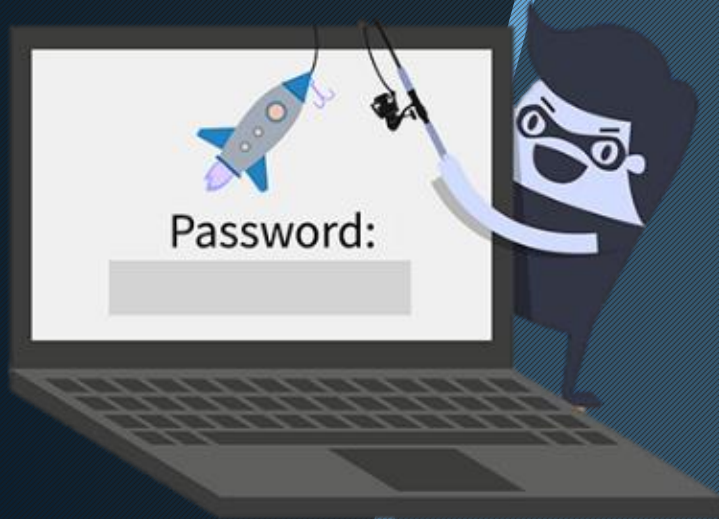
ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดย  
ปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการ  
รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข โดยเจตนา



## การกระทำต่อข้อมูลคอมพิวเตอร์

“

ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด  
บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบ  
คอมพิวเตอร์อาจประมวลผลได้ และให้หมายความ  
รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วย  
ธุรกรรมทางอิเล็กทรอนิกส์ด้วย”



## การกระทำต่อข้อมูลคอมพิวเตอร์

การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ

“

ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มี  
มาตรการป้องกันการเข้าถึงโดยเฉพาะและ  
มาตรการนั้นมีได้มีไว้สำหรับตน ต้องระวางโทษ  
จำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท  
หรือทั้งจำทั้งปรับ”



## การกระทำต่อข้อมูลคอมพิวเตอร์

การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ

“

ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน โดยเจตนา



# การกระทำต่อข้อมูลคอมพิวเตอร์

## การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ

“ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมีได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”





## การกระทำต่อข้อมูลคอมพิวเตอร์

การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ

“

ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมีได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ โดยเจตนา



## การกระทำต่อข้อมูลคอมพิวเตอร์



การรบกวนข้อมูลคอมพิวเตอร์โดยมิชอบ

“

“ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

# การกระทำต่อข้อมูลคอมพิวเตอร์

การรบกวนข้อมูลคอมพิวเตอร์โดยมิชอบ

“

ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ โดยเจตนา



# ความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันต้องห้ามเผยแพร่

“ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

- (1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน
- (2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
- (3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- (4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้
- (5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)”

# ผู้ใช้งานเทคโนโลยีดิจิทัล ควร มีคุณธรรมจริยธรรมในการใช้ งาน โดยสังเขป ดังนี้

- “ ยึดถือ ปฏิบัติตามแนวทาง แนวปฏิบัติ ระเบียบ กฎเกณฑ์ตามที่กำหนด
- “ ใช้สื่อโซเชียลมีเดียอย่างมีความรับผิดชอบต่อสังคม
- “ ไม่ละเมิดลิขสิทธิ์ ทรัพย์สินทางปัญญา เช่น ใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง
- “ ไม่ละเมิดสิทธิของผู้อื่น เช่น ใช้อุปกรณ์เทคโนโลยีของผู้อื่นโดยไม่ได้รับอนุญาต ตลอดจน การเข้าถึงข้อมูลส่วนบุคคลของผู้อื่น
- “ การใช้เทคโนโลยีดิจิทัล ต้องไม่รบกวนการทำงานของผู้อื่น
- “ ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมอันติดตามมาจากการกระทำของตน
- “ ไม่ควรให้ข้อมูลที่เป็นเท็จ หรือนำข้อมูลที่เป็นเท็จเข้าสู่ระบบอินเทอร์เน็ต
- “ ไม่บิดเบือนความถูกต้องของข้อมูล ให้ผู้รับคนต่อไปได้ข้อมูลที่ไม่ถูกต้อง
- “ ต้องไม่โจรกรรมข้อมูลข่าวสาร ทำร้ายหรือละเมิดสิทธิของผู้อื่น
- “ ต้องไม่สอดแนมหรือแก้ไขเปิดดูในแฟ้มของผู้อื่น
- “ ไม่ควรเปิดเผยข้อมูลกับผู้ที่ไม่ได้รับอนุญาต
- “ ต้องไม่คัดลอกโปรแกรมผู้อื่นที่มีลิขสิทธิ์
- “ ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน
- “ ไม่ทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นอีกบุคคลหนึ่ง ตัวอย่างเช่น การปลอมอีเมล การปลอมแปลงบัตรเครดิต เป็นต้น
- “ ไม่ควรแชร์สิ่งที่เป็นเท็จ หรือสิ่งที่ยังไม่ได้ตรวจสอบให้แน่ใจเสียก่อน หรือสิ่งที้อาจจะส่งผลเสียต่อบุคคลอื่น

# แนวปฏิบัติในการใช้สื่อดิจิทัลอย่างปลอดภัย

## 1. ป้องกันไม่ให้ตกเป็นเหยื่อของไวรัส สปายแวร์ และมัลแวร์ เช่น

“

อัปเดตคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ

“

ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์

“

ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดรฟ์ (USB) เป็นต้น

“

ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน

“

ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มต้น โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ

“

ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่ และ

“

หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใดๆที่ส่งมาจากอีเมลล์ที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา



## แนวปฏิบัติในการใช้สื่อดิจิทัลอย่างปลอดภัย

2. ใช้การยืนยัน 2 ขั้นตอน (2 factor authentication) การยืนยันแบบ 2 ขั้นตอนเป็นวิธีการพิสูจน์ตัวตนที่ต้องใช้ข้อมูล 2 ส่วนร่วมกัน เพื่อเพิ่มความมั่นคงปลอดภัยให้กับการเข้าสู่ระบบหรือบริการ โดยจะใช้ข้อมูลจาก 2 ใน 3 ส่วนนี้คือ สิ่งที่คุณรู้ เช่น รหัสผ่าน สิ่งที่คุณมี เช่น โทรศัพท์มือถือ, รหัสบัตรเติมเงิน และ สิ่งที่เป็น เช่น ลายนิ้วมือ, ม่านตา เป็นต้น การยืนยันแบบ 2 ขั้นตอนช่วยลดโอกาสในการถูกขโมยข้อมูลส่วนตัวในบัญชีอีเมลของเราลงได้ เพราะต่อให้ใส่ชื่อผู้ใช้และรหัสผ่านถูกต้องแล้ว ก็ยังไม่สามารถเข้าถึงบัญชีอีเมลได้ จนกว่าจะใส่รหัสผ่านที่ 2 ที่ได้รับจาก SMS ผ่านโทรศัพท์มือถือที่ลงทะเบียนไว้ เสียก่อน ซึ่งจะเพิ่มความปลอดภัยให้แก่ข้อมูลส่วนตัว ไม่ให้ถูกโจรกรรมได้

3. การตรวจสอบประวัติการใช้งานบัตรเครดิตอยู่เสมอ ถ้ามีรายการเบิกเงินที่เจ้าของบัตรไม่ได้ทำ ให้ติดต่อธนาคารเพื่อขอเปลี่ยนบัตรทันที

4. ผู้ใช้งานควรตรวจสอบว่ามีผู้ไม่หวังดี แอบเข้ามาล็อกอินใช้บัญชีอีเมลของเราหรือไม่ อาจสังเกตความผิดปกติจากช่วงเวลาหรือประเทศที่พบการใช้งาน เช่น พบการล็อกอิน ณ เวลาเที่ยงคืน จากต่างประเทศ

## แนวปฏิบัติในการใช้สื่อดิจิทัลอย่างปลอดภัย

5. ควรตรวจสอบว่าผู้ไม่หวังดีเปลี่ยนค่าต่าง ๆ อาจเพิ่มอีเมลหรือหมายเลขโทรศัพท์ที่ใช้ ในการยืนยันตัวตน เพื่อแอบล็อกอินเข้ามาขโมยข้อมูล หากผู้ใช้งานพบความผิดปกติ ควรเปลี่ยนช่องทางในการเข้าถึงบัญชี เช่น รหัสผ่าน, หมายเลขโทรศัพท์, อีเมลสำหรับกู้คืนบัญชี รวมถึงเฟิกถอนรหัสเฉพาะสำหรับแอปพลิเคชัน, สิทธิในการเข้าถึงข้อมูลของแอปพลิเคชันต่าง ๆ

6. ควรระวังในการเข้าใช้งานจากเครื่องคอมพิวเตอร์สาธารณะ ในการใช้งานเครื่องคอมพิวเตอร์สาธารณะ เราไม่สามารถรู้ได้เลยว่าเครื่องนั้นมีซอฟต์แวร์อะไรติดตั้งอยู่บ้าง บางเครื่องอาจมีโปรแกรม Keylogger แอบแฝงอยู่ ซึ่งเป็นโปรแกรมที่จะคอยดักจับการใช้งานต่างๆ เช่น การกดปุ่มคีย์บอร์ด หากเราทำการล็อกอินเข้าใช้งาน บัญชีอีเมลผ่านเครื่องคอมพิวเตอร์สาธารณะ ที่มีโปรแกรม Keylogger อยู่ ข้อมูลชื่อผู้ใช้และรหัสผ่านของเรา หรือทุกอย่างที่เราพิมพ์ลงไปก็จะถูก บันทึกไว้ทั้งหมด หากจำเป็นต้องใช้คอมพิวเตอร์สาธารณะในการเช็คอีเมล ควรใช้วิธีการพิมพ์ผ่าน On-Screen Keyboard ซึ่งเป็นโปรแกรมที่จำลองการทำงานของคีย์บอร์ด โดยการใช้เมาส์คลิกแทนการกดปุ่มในคีย์บอร์ด ทำให้เราสามารถป้อนข้อมูลต่างๆ ได้เหมือนการพิมพ์ในคีย์บอร์ดจริง ซึ่งจะช่วยป้องกันซอฟต์แวร์ Keylogger ได้ โปรแกรม On-Screen Keyboard จะถูกติดตั้งมาพร้อมกับระบบปฏิบัติการ Windows ตั้งแต่ XP ขึ้นไป สามารถเรียกใช้งานได้ตามรูปที่ 1 แต่หากไม่มีก็สามารถดาวน์โหลดโปรแกรม On-Screen Keyboard ของผู้พัฒนาภายนอกมาติดตั้งเพิ่มเติมได้



## แนวปฏิบัติในการใช้สื่อดิจิทัลอย่างปลอดภัย

7. การตั้งรหัสผ่านที่ทำให้คาดเดาได้ยาก การตั้งรหัสผ่านที่ดีก็ เป็นสิ่งสำคัญในการที่จะป้องกันอีเมล เพราะ จะทำให้ยากต่อ การคาดเดา หรืออาจต้องใช้เวลาานมาก ส่วนการตั้ง รหัสผ่านที่ไม่ดี จะทำให้ผู้ที่ไม่ประสงค์ดี สามารถเข้าสู่ระบบ ของเราได้โดยง่าย

8. เมื่อสงสัยว่า อาจจะตกเป็นเหยื่อของมิจฉาชีพทาง อินเทอร์เน็ต ต้องรีบดำเนินการแก้ไขในส่วนที่เกี่ยวข้อง โดยเร็ว ถ้าก่อให้เกิดความเสียหาย ควรรีบแจ้งเจ้าหน้าที่ ตำรวจให้ดำเนินการตามกฎหมาย





**Q&A**