บทที่ 5

ความเป็นส่วนตัว

Information Privacy

นำเสนอโดย

ผศ.ดร.ชุติมา ประสาทแก้ว

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มทร.ธัญบุรี

ภาพรวมในการบรรยาย

- ความหมายความเป็นส่วนตัว
- ภัยคุกคามความเป็นส่วนตัวและข้อมูลส่วนบุคคล
- กรอบในการคุ้มครองข้อมูล/สารสนเทศส่วนบุคคล
- กฎหมายคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล
- สิทธิส่วนบุคคลในโลกออนไลน์

นิยามของคำว่า “ความเป็นส่วนตัว”

“Privacy” เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ ที่สังคมยุคใหม่ เกือบทุกประเทศให้ความสำคัญอย่างมาก ดังจะเห็นได้จากการรับรองหลักการดังกล่าวไว้ในรัฐธรรมนูญ หรือแม้บางประเทศจะไม่ได้บัญญัติรับรองไว้โดยตรงในรัฐธรรมนูญ แต่ก็ได้ตราบทบัญญัติรับรองไว้ในกฎหมายเฉพาะ “ความเป็นส่วนตัว” ได้รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการตีความคำว่า “ความเป็นส่วนตัว” ในด้านการจัดการข้อมูลส่วนบุคคล ความเป็นส่วนตัวเกี่ยวกับข้อมูล (**Information Privacy)** เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล

นิยามของคำว่า “ความเป็นส่วนตัว” (ต่อ)

“ข้อมูลส่วนบุคคล (**Data Privacy)**” ภายใต้ร่าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาสิ่งที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ รูปถ่าย หรือแผ่นบันทึกลักษณะเสียงของคน เป็นต้น และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมด้วย

นิยามของคำว่า “ความเป็นส่วนตัว” (ต่อ)

ความเป็นส่วนตัวของข้อมูลข่าวสาร (**Information Privacy**) หมายถึง สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ใช้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มบุคคล และองค์กรต่าง ๆ

จึงมีประเด็นเกี่ยวกับความเป็นส่วนตัวที่ส่งผลกระทบให้พิจารณาดังนี้

1. การเข้าไปดูข้อความในจดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึก-แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร
2. การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล ซึ่งทำให้สูญเสียความเป็นส่วนตัว ซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม

นิยามของคำว่า “ความเป็นส่วนตัว” (ต่อ)

3. การใช้ข้อมูลของลูกค้าจากแหล่งต่าง ๆ เพื่อผลประโยชน์ในการขยายตลาดในเชิงธุรกิจ

4. การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล์ หมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่น ๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น

ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลและสารสนเทศ จึงควรจะต้องระวังการให้ข้อมูล โดยเฉพาะการใช้อินเตอร์เน็ตที่มีการใช้โปรโมชั่น หรือระบุให้มีการลงทะเบียนก่อนเข้าใช้บริการ เช่น ข้อมูลบัตรเครดิต และที่อยู่อีเมล์ เป็นต้น

ภัยคุกคามความเป็นส่วนตัว

อาจพบเห็นการละเมิดความเป็นส่วนตัวโดยทั่วไป เช่น

- ใช้โปรแกรมติดตามและสำรวจพฤติกรรมผู้ที่ใช้งานบนเว็บไซต์

- การเอาฐานข้อมูลส่วนตัวรวมถึงอีเมล์ของสมาชิกส่งไปให้กับบริษัทผู้รับทำโฆษณาหรือให้กับบริษัทคู่ค้า

- การใช้กล้องวงจรปิดตรวจสอบดูพฤติกรรมการทำงานของลูกจ้าง

แนวทางหลีกเลี่ยงการละเมิดความเป็นส่วนตัว เช่น บริษัทที่ต้องการเข้าถึงข้อมูลลูกค้า อาจมีการแจ้งหรือสอบถามลูกค้าก่อนที่จะเข้าไปใช้บริการว่าจะยอมรับที่จะให้นำข้อมูลส่วนตัวนี้ไปเผยแพร่หรือนำไปให้กับบริษัทอื่นเพื่อใช้งานอย่างใดอย่างหนึ่งได้หรือไม่ เพื่อแลกกับรายได้ค่าโฆษณาที่ผู้ให้บริการนั้นจะได้มา เช่น บริการฟรีอีเมล์ บริการพื้นที่เก็บข้อมูล บริการใช้งานโปรแกรมฟรี เป็นต้น จะยินยอมหรือไม่

กรอบในการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล หมายรวมถึง – สิทธิในชีวิตและร่างกาย “เรื่องส่วนตัว” รัฐและบุคคลทั่วไปต้องเคารพและไม่แทรกแซง – สิ่งบ่งชี้ศักดิ์ศรีความเป็นมนุษย์ สิทธิที่จะดำรงชีวิต กำหนดวิถีชีวิตของตัวเอง ความเป็นมนุษย์ เป็นองค์รวมของข้อมูลส่วนบุคคลอีกมากมาย ที่ต้องได้รับการคุ้มครอง

กรอบในการคุ้มครองข้อมูลส่วนบุคคล (ต่อ)

กรอบในการคุ้มครองข้อมูลส่วนบุคคลที่นิยมของสากลประเทศและประเทศไทยใช้นำมาอ้างอิงเป็นแนวทางในการดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ซึ่งข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้นตอนตั้งแต่การเก็บรวบรวม การเก็บรักษา และการเปิดเผย คือ กรอบในการคุ้มครองข้อมูลขององค์กรร่วมมือและพัฒนาทางเศรษฐกิจ (**OECD : The Organization for Economic Cooperation and Development**) ในเรื่องแนวทางการคุ้มครอง (**Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data**) มีหลักการพื้นฐาน 8 ประการ

กรอบในการคุ้มครองข้อมูลส่วนบุคคล (ต่อ)

ข้อ	กรอบ OECD	สาระสำคัญ
1.	หลักข้อจำกัดในการเก็บรวบรวมข้อมูล	ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสม โดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล
2.	หลักคุณภาพของข้อมูล	ข้อมูลที่เก็บรวบรวมนั้น ต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า “จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด นอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ
3.	หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ	ต้องกำหนดวัตถุประสงค์ว่า ข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวมรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้น ไว้ให้ชัดเจน

กรอบในการคุ้มครองข้อมูลส่วนบุคคล (ต่อ)

ข้อ	กรอบ OECD	สาระสำคัญ
4.	หลักข้อจำกัดในการนำไปใช้	ข้อมูลส่วนบุคคลนั้น จะต้องไม่มีการเปิดเผย ทำให้มี หรือปรากฏในลักษณะอื่นใด ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย
5.	หลักการรักษาความมั่นคงปลอดภัยข้อมูล	จะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ
6.	หลักการเปิดเผยข้อมูล	ควรมีการประกาศนโยบายฯ ให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไข หรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการ ที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคล ด้วย
7.	หลักการมีส่วนร่วมของบุคคล	ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้นๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ ภายในระยะเวลาที่เหมาะสม”
8.	หลักความรับผิดชอบ	ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองความเป็นส่วนตัว

การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูล ส่วนบุคคลของหน่วยงานของรัฐให้มีมาตรฐานเดียวกัน

กฎหมายคุ้มครองความเป็นส่วนตัว (ต่อ)

อาศัยอำนาจตามความในมาตรา 6 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 บัญญัติว่า “ในกรณีที่หน่วยงานของรัฐมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือ ข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล” ดังนั้น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออก “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553” เพื่อให้หน่วยงานของรัฐให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล ด้วยการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐด้วย โดยในประกาศฯ ต้องมีสาระสำคัญ อย่างน้อย ประกอบด้วย 2 ส่วน ได้แก่

กฎหมายคุ้มครองความเป็นส่วนตัว (ต่อ)

ส่วนที่ 1 : นโยบายการคุ้มครองข้อมูลส่วนบุคคล การจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการแจ้งให้กับ ผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับหน่วยงานได้ทราบว่า หน่วยงานมีแนวทางในการบริหารจัดการ ข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งเป็นเจ้าของข้อมูลอย่างไร เพื่อให้ผู้ใช้บริการทราบและสามารถตัดสินใจได้ว่า สมควรให้ข้อมูลส่วนบุคคลของตนหรือไม่ เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ในส่วนของนโยบายฯ จะต้องมีหัวข้อหลักที่เป็นสาระสำคัญอย่างน้อย 8 ข้อ ดังนี้

กฎหมายคุ้มครองความเป็นส่วนตัว (ต่อ)

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด
2. คุณภาพของข้อมูลส่วนบุคคล
3. การระบุวัตถุประสงค์ในการเก็บรวบรวม
4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้
5. การรักษาความมั่นคงปลอดภัย
6. การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติและนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล
7. การมีส่วนร่วมของเจ้าของข้อมูล
8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

กฎหมายคุ้มครองความเป็นส่วนตัว (ต่อ)

ส่วนที่ 2 : แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล การจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการประกาศ ให้กับบุคลากรในหน่วยงานปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ทั้งนี้ แนวปฏิบัติต้องแสดงถึงขั้นตอนและวิธีการดำเนินการเพื่อให้บุคลากร ซึ่งเป็นผู้ปฏิบัติสามารถปฏิบัติได้อย่างถูกต้อง เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการฯ จะต้องมีหัวข้อหลักที่เป็นสาระสำคัญในแนวปฏิบัติอย่างน้อย 9 ข้อ ดังนี้

กฎหมายคุ้มครองความเป็นส่วนตัว (ต่อ)

1. ข้อมูลเบื้องต้น
2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล
3. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น
4. การรวมข้อมูลจากที่มาหลาย ๆ แห่ง
5. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
6. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ
7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน
8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
9. การติดต่อกับเว็บไซต์

กฎหมายคุ้มครองความเป็นส่วนตัว (ต่อ)

ในแนวปฏิบัติฯ บางข้อที่หน่วยงานมีการดำเนินการเพิ่มเติม ให้ระบุเนื้อหาเพิ่มเติมไว้ในนโยบาย โดยระบุเป็นข้อ ต่อจากนโยบายข้อ 8

แต่หากในแนวปฏิบัติฯ บางข้อที่หน่วยงานไม่มีการดำเนินการ ให้ระบุไว้ในแนวปฏิบัติข้อนั้นว่า “– ไม่มี –” แต่ทั้งการร่างแนวปฏิบัติฯ ยังคงต้องมีหัวข้อสาระสำคัญให้ครบตามกฎหมาย

สิทธิส่วนบุคคลในโลกออนไลน์

- บริษัท **Cambridge Analytica** เป็นบริษัทวิจัยข้อมูลเพื่อวัตถุประสงค์ทางการเมือง เช่น การระดมคะแนนเสียงเลือกตั้ง ได้เข้าถึงข้อมูลของผู้ใช้เฟซบุ๊กกว่า 50 ล้านคนเพื่อหาทางโน้มน้าวให้เลือกโดนัลด์ ทรัมป์ จนชนะการเลือกตั้งเมื่อปี ค.ศ. 2016 และดำรงตำแหน่งประธานาธิบดีของสหรัฐอเมริกา เป็นประเด็นให้เห็นว่าการนำข้อมูลสารสนเทศมาใช้นั้น สามารถนำมาใช้วิเคราะห์วางแผนก่อให้เกิดประโยชน์ต่อการแข่งขันได้เป็นอย่างดี มีความชอบธรรมหรือไม่
- องค์กรหลายแห่งทั้งภาครัฐและเอกชนตลอดจนพลเมืองเน็ตจำนวนมหาศาลต่างแสดงความไม่พอใจต่อเรื่องราวดังกล่าว และตั้งคำถามกับเฟซบุ๊กว่าปล่อยให้องค์กรวิเคราะห์ข้อมูลเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ได้อย่างไร และยังพูดกันว่าจะต้องมีการตรวจสอบเฟซบุ๊กว่ามีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้ไว้มากน้อยเพียงใด จึงเป็นที่มาให้ทั่วโลกให้ความสำคัญกับข้อมูลสารสนเทศอย่างมากในโลกออนไลน์

สิทธิส่วนบุคคลในโลกออนไลน์

- ทั้งนี้ปัจจุบันมีบัญชีผู้ใช้เฟซบุ๊กมากกว่า 1,600 ล้านบัญชี ส่วนในไทยก็มีมากถึง 40 ล้านบัญชี และมีแนวโน้มจะมาขึ้นอย่างมาก ส่งผลให้ประเทศไทยตระหนักให้ความสำคัญกับสิทธิส่วนบุคคลเกี่ยวกับข้อมูลสารสนเทศในโลกออนไลน์อย่างมาก โดยประกาศเป็นกฎหมายบังคับใช้จริงจัง เมื่อวันที่ 23 มิถุนายน พ.ศ.2565 กำหนดให้หน่วยงานทั้งภาครัฐและเอกชนจัดทำนโยบายและแนวทางปฏิบัติเกี่ยวกับความเป็นส่วนตัวของเจ้าของข้อมูล ให้ชัดเจนและแจ้งผู้มีส่วนเกี่ยวข้องให้รับรู้รับทราบอย่างเป็นระบบ ถ้าไม่ดำเนินการมีผลตามกฎหมาย

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- ความท้าทายของประเด็น **Privacy** หรือสิทธิส่วนบุคคลในโลกออนไลน์สูงขึ้นอย่างไม่เคยเป็นมาก่อน หลังจากโลกมีนวัตกรรมโซเชียลมีเดีย หรือสื่อสังคมออนไลน์เมื่อประมาณทศวรรษครึ่งที่ผ่านมา
- เมื่อเข้าสู่ทศวรรษที่ **1990** เกิดเครือข่ายอินเทอร์เน็ตที่มีการส่งต่อข้อมูลจำนวนมากและมีความรวดเร็วอย่างไม่เคยเป็นมาก่อน แนวทางการคุ้มครองข้อมูลส่วนบุคคลก็เริ่มมีการปรับเปลี่ยนไปตามกาลเวลา แต่ยังคงเน้นวัตถุประสงค์หลักคือการคุ้มครองปัจเจกบุคคลจากการควบคุมและอิทธิพลขององค์กรขนาดใหญ่ที่สามารถเข้าถึงและนำข้อมูลดิจิทัลมาใช้ได้ ซึ่งอาจจะส่งผลกระทบต่อตัวตนของบุคคลในโลกความเป็นจริง ซึ่งในต่างประเทศให้ความสำคัญอย่างมากในประเด็นดังกล่าว

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- เริ่มมีการศึกษาผลกระทบของตัวตนในโลกดิจิทัล (**digital self)** ซึ่งประกอบขึ้นจากข้อมูลส่วนบุคคลต่าง ๆ เข้าด้วยกันจนสร้างใหม่กลายเป็นโปรไฟล์ของพลเมืองหรือผู้บริโภค โดยองค์กรภาครัฐหรือเอกชนที่สามารถเข้าถึงข้อมูลที่ประมวลผลนี้ แล้วจะเอาข้อมูลไปใช้ประโยชน์เพื่อจัดการหรือควบคุมพฤติกรรมของประชาชนในแง่ต่าง ๆ
- แต่เมื่อข้อมูลส่วนบุคคลกลายเป็นสิ่งที่ผู้ใช้นำเข้าสู่ระบบและแชร์กันอย่างกว้างขวางโดยสมัครใจบนโซเชียลมีเดีย ซึ่งเพิ่มจำนวนอย่างรวดเร็ว และมีอิทธิพลอย่างมหาศาลต่อการดำเนินชีวิตของคนในโลกยุคปัจจุบัน การนำข้อมูลส่วนบุคคลไปใช้เพื่อแสวงหาผลประโยชน์จึงทำได้ง่ายดายและเจาะกลุ่มเป้าหมายได้เฉพาะเจาะจงมากกว่าเดิม

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- Business Model ของโซเชียลมีเดียอย่างเฟซบุ๊ก เป็นบริการนำเสนอ การแลกเปลี่ยน และการมีปฏิสัมพันธ์ระหว่างกันของผู้ใช้ผ่านข้อมูลในรูปแบบต่าง ๆ ผ่านระบบอัลกอริทึม หรือระบบประมวลผลของเครือข่าย เฟซบุ๊กมักอ้างตนเองว่าเป็นเพียงแพลตฟอร์มหรือตัวกลางออนไลน์ที่ให้พื้นที่แก่ผู้ใช้ในการสร้างสรรค์เนื้อหาของตนเอง จึงไม่ต้องรับภาระรับผิดหากข้อมูลเป็นเท็จ หรือมีลักษณะหมิ่นประมาท หรือผิดกฎหมายในบางประเทศ
- ปรากฏการณ์เฟซบุ๊กกับ Cambridge Analytica ที่สร้างความตื่นตระหนกแก่สมาชิกเครือข่ายสังคมออนไลน์ดูท่าจะไม่กระทบมากนักกับผู้ใช้ในเมืองไทย ซึ่งสังคมไทยที่ไม่ตื่นตัวกับภัยคุกคามด้านนี้ เพราะขาดความตระหนักรู้ และไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งร่างมาตั้งแต่ปี 1990 หรือปี 2533 ในต่างประเทศที่ให้ความสำคัญ จนปัจจุบัน ตอนนี้ประเทศไทยเริ่มบังคับใช้ในปี 2565

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- เรื่อง Privacy เป็นเรื่องที่จับต้องได้ยากกว่าเสรีภาพในการแสดงออกหรือสิทธิในการรับรู้ข้อมูล **ตราบใดที่ยังไม่เกิดกรณีอื้อฉาวแบบ Cambridge Analytica ในไทย เฟซบุ๊กก็จะยังคงเป็นพื้นที่แห่งสันทนาการราคาถูกสำหรับทุกเพศทุกวัย** และเป็นแฟลตฟอร์มของการทำการตลาดออนไลน์ที่เข้าถึงผู้บริโภคที่แบ่งส่วนตลาดตามพฤติกรรมได้อย่างดีต่อไป”
- **โลกอินเทอร์เน็ตก็ไม่ต่างจากโลกจริงที่เต็มไปด้วยความเสี่ยง** อาทิเช่น การสอดแนมความเป็นส่วนตัว อาชญากรรมคอมพิวเตอร์ การกลั่นแกล้งออนไลน์ เนื้อหาที่มีความรุนแรงทางเพศและประทุษวาจา **พลเมืองดิจิทัลต้องตระหนักและเรียนรู้วิธีรับมือกับความเสี่ยงใหม่ ๆ ไม่ปล่อยให้ใครมาสอดแนมหรือสะกดรอยตาม หรือไม่ปล่อยให้ใครมาขโมยข้อมูลสำคัญได้** ซึ่งข้อมูลสำคัญอาชญากรออนไลน์ส่วนมากต้องการคือข้อมูลส่วนบุคคลและรหัสผ่านเข้าสู่บัญชีออนไลน์ เช่น บัญชีเฟสบุ๊ค หรือธนาคารออนไลน์ เป็นต้น

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

ความปลอดภัยและความเป็นส่วนตัวในโลกออนไลน์นับเป็นประเด็นสำคัญที่พลเมืองดิจิทัลต้องเรียนรู้ไว้ไม่ต่างจากการสร้างความปลอดภัยและความเป็นส่วนตัวในโลกจริง มาทำความรู้จักเรียนรู้วิธีการเพิ่มความปลอดภัยและความเป็นส่วนตัว ที่จะช่วยให้ใช้ชีวิตในโลกออนไลน์ได้อย่างปลอดภัยไร้กังวลมากขึ้น คือ

- การตั้งรหัสผ่านและวิธีจัดการ

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

เทคนิคการตั้งรหัสผ่านง่าย ๆ มีดังนี้

- รหัสควรมีความยาวอย่างน้อย 8 อักขระขึ้นไป
- สร้างรหัสที่ประกอบด้วยตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์ผสมกัน
- หลีกเลี่ยงการใช้ข้อมูลส่วนตัวที่คาดเดาได้ง่ายและไม่เป็นความลับ เช่น วันเกิด บ้านเลขที่ เลขผู้เสียภาษี ทะเบียนรถ เบอร์โทรศัพท์ หรือชื่อเล่น ชื่อสัตว์เลี้ยง ชื่อโรงเรียน ชื่อทีมกีฬาทีมโปรด เป็นต้น

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- หลีกเลี่ยงคำศัพท์ที่เป็นคำสามัญทั่วไป (คำที่ปรากฏในพจนานุกรม) เช่น CAT, DOG, LOVE
- หลีกเลี่ยงการใช้ตัวอักษรหรือตัวเลขเรียงกันตามลำดับ เช่น ABCD 1234 หรือการเรียงรหัสตามตำแหน่งคีย์บอร์ด เช่น QWERT
- *เทคนิคการตั้งรหัสผ่าน*: สร้าง “วลีรหัสผ่าน” ด้วยประโยคที่คุ้นเคย เช่น I met Som in Chiang Mai in 2008. แล้วนำอักษรตัวแรกของแต่ละคำมาสร้างรหัสผ่านและเปลี่ยนบางคำให้เป็นสัญลักษณ์ (ImS@CM#2008) เทคนิคนี้ช่วยสร้างรหัสผ่านที่รัดกุม หลากหลาย และจำได้ง่าย

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

แนวทางจัดการกับรหัสผ่านดังนี้

- ไม่แชร์รหัสกับใครทั้งนั้น (ยกเว้นพ่อแม่หรือผู้ปกครองในกรณีที่เป็นผู้เยาว์)
- หากจำเป็นต้องจดรหัสผ่านกันลืมจริง ๆ ให้เก็บไว้ในที่ปลอดภัย ไม่วางไว้ในตำแหน่งที่เห็นได้ง่าย เช่น ข้างจอคอมพิวเตอร์หรือบนโต๊ะ เป็นต้น
- ตั้งรหัสให้แตกต่างกันในบัญชีสำคัญแต่ละบัญชี เช่น บัญชีเฟสบุ๊ค อีเมล ธนาคารออนไลน์ เป็นต้น เพราะการใช้รหัสเหมือนกันหมดในทุกบัญชีหมายความว่า ถ้ามีคนรู้รหัสผ่านของบริการออนไลน์หนึ่ง ๆ ก็จะสามารถเข้าถึงบริการออนไลน์อื่น ๆ ที่สำคัญได้โดยปริยาย
- เลือกผู้ให้บริการที่น่าเชื่อถือและให้ความสำคัญกับเรื่องความปลอดภัย โดยเฉพาะบริการสำคัญ เช่น บริการด้านการเงินที่อนุญาตให้ตั้งรหัสยาวพอและรองรับการเข้ารหัส HTTPS

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- ตั้งค่าแจ้งเตือนหากมีใครล็อกอินเข้าบัญชีจากเครื่องที่ไม่รู้จัก
- เปลี่ยนรหัสทุกครั้งเมื่อสงสัยว่ามีกิจกรรมไม่ปกติเกิดขึ้น เช่น มีการเข้าสู่บัญชีจากคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ไม่คุ้นเคย
- ตั้งค่าการกู้คืนรหัสผ่าน บริการส่วนมากจะให้ใส่เบอร์โทรศัพท์หรืออีเมลสำหรับส่งรหัสผ่านไปให้ใหม่หรือเพื่อรีเซ็ตรหัสผ่านใหม่ เมื่อต้องการกู้คืนหรือเปลี่ยนรหัสผ่าน
- เปิดใช้ระบบการพิสูจน์ตัวตนที่ปลอดภัยมากขึ้น เช่น การพิสูจน์ตัวตนสองระดับ (**two-factor authentication)** คือระบบที่ต้องพิสูจน์ตัวตนผ่านข้อมูลสองประเภทก่อนจึงจะล็อกอินเข้าระบบได้ เช่น รหัสผ่านและลายนิ้วมือ หรือที่เป็นที่นิยมกัน เป็นต้น

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

การใช้อินเทอร์เน็ตในที่สาธารณะ ควรคำนึงถึงสิ่งเหล่านี้

- หลีกเลี่ยงการล็อกอินเข้าบริการที่สำคัญ เช่น อีเมล โซเชียลมีเดีย และธนาคารออนไลน์ เป็นต้น
- เลือกใช้โหมดส่วนตัวในบราวเซอร์ เช่น โหมด **Incognito** ในกูเกิลโครม (เลือกคำสั่ง “หน้าต่างใหม่และไม่ระบุตัวตน” หรือกด **Ctrl + Shift + N)** หรือ **Private Browsing** ในไฟร์ฟ็อกซ์ (เลือกคำสั่ง “หน้าต่างส่วนตัวใหม่” หรือกด **Ctrl + Shift + P)** และปิดบราวเซอร์ทุกครั้งหลังใช้งานเสร็จ
- ออกจากระบบทุกครั้งหลังใช้งานและไม่ตั้งค่าให้เครื่องจำรหัสผ่านหรือสถานะของผู้ใช้
- ไม่บันทึกไฟล์ข้อมูลสำคัญลงในเครื่องคอมพิวเตอร์สาธารณะ
- ตรวจสอบตัวดักข้อมูล (**keylogger** หรือ **keystroke logger** เป็นได้ทั้งฮาร์ดแวร์และซอฟต์แวร์ ซึ่งจะบันทึกการกดแป้นพิมพ์เพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่านธนาคารออนไลน์) แบบฮาร์ดแวร์ โดยดูว่ามีสายไฟแปลกๆ ที่เชื่อมคีย์บอร์ดกับช่องเสียบด้านหลังคอมพิวเตอร์อยู่หรือไม่ ถ้ามีอุปกรณ์ที่ไม่แน่ใจเสียบอยู่ ให้สงสัยว่าเป็นตัวดักข้อมูล และหลีกเลี่ยงการใช้งานที่สุ่มเสี่ยง

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

การเชื่อมต่อ **Wi-Fi** สาธารณะ ต้องคำนึงถึงเมื่อใช้ คือ

- พยายามหลีกเลี่ยงการล็อกอินเข้าใช้บริการสำคัญ ๆ เช่น การลงชื่อเข้าใช้บัญชีอีเมล สั่งซื้อของ หรือโอนเงินผ่านระบบธนาคารออนไลน์ เนื่องจากอาจมีคนดักจับรหัสผ่านหรือข้อมูลการเงิน เป็นต้น
- ดูว่าเว็บไซต์ที่จะเข้ารองรับการเข้ารหัสหรือไม่ โดยให้สังเกตที่ยูอาร์แอล (**URL** หรือ **Uniform Resource Locator** คือที่อยู่ซึ่งใช้ระบุแหล่งข้อมูลในอินเทอร์เน็ต เช่น **https://pantip.com/** สำหรับการเข้าถึงเว็บไซต์พันทิป) ว่ามีคำว่า **HTTPS** (**S** ตัวท้ายย่อมาจาก **Secure** หมายถึงเวอร์ชั่นที่ปลอดภัยมากขึ้นของ **HTTP**) ซึ่งเป็นการเข้ารหัสจากเครื่องไปยังเซิร์ฟเวอร์ปลายทาง

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

การป้องกันการเข้าถึงผ่านอุปกรณ์เคลื่อนที่ สามารถเพิ่มความปลอดภัยจากการใช้อุปกรณ์เคลื่อนที่ได้ดังนี้

- *การตั้งค่าล็อกอุปกรณ์เคลื่อนที่:* อุปกรณ์เคลื่อนที่ส่วนใหญ่จะมีระบบล็อกพิน (**pin**) และระบบล็อกรหัสผ่าน (**password**) ในรูปแบบต่าง ๆ ข้อควรระวังคือ
  - พิน: ไม่ควรใช้เลขเรียงกัน หรือใช้ข้อมูลส่วนบุคคลที่คนคาดเดาได้ง่าย เช่น วัน/เดือน/ปีเกิด บ้านเลขที่
  - รูปแบบการลากเส้น: อย่าเลือกรูปแบบที่เดาง่าย เช่น รูปสี่เหลี่ยม สามเหลี่ยม รวมถึงควรซ่อนรูปแบบขณะลากเส้นเพื่อป้องกันผู้อื่นเห็น
  - *การดาวน์โหลดแอปพลิเคชัน:* ควรระมัดระวังการดาวน์โหลดแอปพลิเคชันและไฟล์ในมือถือ เพราะอาจเป็นอันตรายต่ออุปกรณ์และข้อมูลส่วนตัว เช่น แอปพลิเคชันบางตัวพยายามเข้าถึงบัญชีส่วนตัว ดังนั้นควรดาวน์โหลดเฉพาะแอปพลิเคชันจากแหล่งที่น่าเชื่อถือ เช่น จาก **Play Store** หรือ **App Store** รวมถึงควรอ่านความคิดเห็นด้านความปลอดภัยของคนที่เคยดาวน์โหลดไปก่อนหน้า
- *การอัปเดตระบบในอุปกรณ์เคลื่อนที่:* อุปกรณ์เคลื่อนที่จะมีระบบแจ้งเตือนให้ผู้ใช้ดาวน์โหลดอุปกรณ์เวอร์ชั่นล่าสุด ควรอัปเดตอุปกรณ์เสมอ เพราะเวอร์ชั่นล่าสุดมักแก้ไขช่องโหว่เรื่องความปลอดภัยในระบบเก่า

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

ระวังสารพัดกลโกงออนไลน์ กลวิธีหลัก ๆ ที่พบเห็นได้บ่อยมีดังนี้

- สร้างสถานการณ์เร่งด่วนหรือเอาผลประโยชน์มาล่อเพื่อให้โอนเงินหรือบอกข้อมูลส่วนบุคคล ยกตัวอย่างเช่น อีเมลแจ้งว่าถูกล็อตเตอรี่ออนไลน์ ได้รางวัลหลายสิบล้าน แต่ต้องโอนเงินบางส่วนไปเป็นค่าดำเนินการ หรืออาจจะแนบเนียนยิ่งขึ้น เช่น แอบอ้างว่ามาจากธนาคารโดยตั้งชื่ออีเมลคล้ายกับอีเมลของธนาคารจริง จากนั้นก็ขอให้ส่งรหัสผ่านกลับไป หรือในบางกรณีที่คนรู้จักถูกแฮ็กบัญชีอีเมล ซึ่งอาจได้รับอีเมลแจ้งว่าตอนนี้อยู่ต่างประเทศ และทำกระเป๋าหาย ขอให้ช่วยโอนเงินไปด่วน
- การสร้างเว็บไซต์ที่ล่อลวงให้เข้าใจผิดว่าเป็นเว็บไซต์จริง และหลอกให้กรอกข้อมูลส่วนบุคคลอย่างรหัสผ่านหรือหมายเลขบัตรเครดิต
- การสร้างป๊อปอัปมาแจ้งว่าเครื่องติดมัลแวร์และให้ดาวน์โหลดซอฟต์แวร์ต้านไวรัส ซึ่งแท้จริงแล้วเป็นมัลแวร์หรือซอฟต์แวร์ที่ไม่พึงประสงค์เพื่อขโมยข้อมูลส่วนบุคคล

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

หากเจอกับกลลวงออนไลน์ทั้งหลาย ควรทำตามแนวทางดังนี้

- ลองพินิจพิจารณาให้ดีว่า ข้อเสนอหรือรางวัลที่ได้รับทางอีเมลหรือเว็บไซต์ “ดีเกินจริง” หรือไม่ เช่น อยู่ดี ๆ ใครจะให้เงินเป็นสิบล้าน หรือเสนอไอโฟนรุ่นใหม่ให้ฟรี ๆ เป็นต้น
- อย่าโอนเงินหรือให้รายละเอียดบัตรเครดิต บัญชีธนาคาร หรือเอกสารส่วนบุคคลกับใครก็ตามที่ไม่รู้จักก่อนตรวจสอบให้แน่ใจ
- ตรวจสอบที่มาของอีเมล เช่น เข้าเว็บไซต์ทางการเพื่อติดต่อสอบถาม หรือลองเอาเนื้อหาอีเมลไปใส่ในเครื่องมือค้นหา ส่วนมากการหลอกลวงเหล่านี้จะมีคนเคยรายงานเอาไว้

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- ตรวจสอบความน่าเชื่อถือของเว็บไซต์ด้วยการเช็คว่าสะกดยูอาร์แอลถูกต้องและมีอะไรผิดสังเกตหรือเปล่า เช่น เปลี่ยนตัวอักษร O เป็นเลข 0 รวมถึงตรวจสอบว่าเว็บไซต์ใช้การเข้ารหัสแบบ HTTPS หรือมีอะไรรับรองความน่าเชื่อถือหรือไม่ เช่น มีตราสัญลักษณ์รับรองความปลอดภัยจากหน่วยงานที่น่าเชื่อถือ
- อัปเดตบราวเซอร์ให้อยู่ในเวอร์ชั่นล่าสุดอยู่เสมอ เพราะบราวเซอร์รุ่นใหม่จะมีการปรับปรุงระบบป้องกันให้ดีขึ้น
- หากพบว่าเป็นอีเมลหลอกลวง ให้ลบอีเมลนั้นทิ้ง ห้ามส่งต่ออีเมลหรือแชร์ผ่านโซเชียลมีเดีย และหาทางรายงานการต้มตุ๋มผ่านช่องทางที่เหมาะสม เมื่อรู้ตัวว่าถูกหลอก ควรเปลี่ยนรหัสบัญชีออนไลน์ทันที แจ้งให้เพื่อนที่อาจตกเป็นกลุ่มเป้าหมายระวังตัว และแจ้งความเพื่อลงบันทึกประจำวัน

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

การติดต่อโดยคนแปลกหน้า

- *รูปโปรไฟล์ดูน่าสงสัยหรือไม่*: ควรสงสัยคนที่ใช้รูปโปรไฟล์เบลอหรือเห็นไม่ชัดไว้ก่อน หรือคนที่แอบเอารูปของคนอื่นที่มีตัวตนจริง ๆ มาใช้เป็นรูปโปรไฟล์
- *ชื่อที่แสดงตรงกับบัญชีผู้ใช้หรือเปล่า*: ตรวจสอบได้ว่าชื่อที่ใช้แสดงตรงกับชื่อที่ปรากฏในยูอาร์แอลหรือไม่
- *มีรายละเอียดประวัติส่วนบุคคลหรือไม่*: บัญชีปลอมโดยมากมักจะไม่ค่อยใส่รายละเอียดข้อมูลเกี่ยวกับตัวเองเท่าไหร่ แต่ถ้ามีรายละเอียด ก็ควรตรวจสอบว่ารายละเอียดเหล่านั้นดูเป็นจริงขนาดไหน
- *มีการเปิดใช้บัญชีมานานแค่ไหน*: บัญชีปลอมมักจะไม่ค่อยมีการโพสต์และปฏิสัมพันธ์มากนัก

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

การกลั่นแกล้งออนไลน์ ภัยที่เกิดบนโลกออนไลน์

- การโพสต์วิดีโอที่น่าอับอายของคนอื่นในบริการฝากวิดีโอ เช่น ยูทูบหรือเฟสบุ๊ค เป็นต้น
- การส่งข้อความหรืออีเมลที่มีเนื้อหาคุกคามหรือน่ารังเกียจให้กับผู้อื่นอย่างต่อเนื่อง
- การโพสต์เนื้อหาที่คุกคามหรือมุ่งทำให้ผู้อื่นอับอายในโซเชียลมีเดีย
- การสร้างบัญชีในโซเชียลมีเดียสำหรับล้อเลียนคนอื่นเป็นการเฉพาะ
- การถ่ายวิดีโอการทำร้ายร่างกายผู้อื่นผ่านมือถือ แล้วนำไปแชร์ต่อให้คนได้เห็นซ้ำ ๆ
- การโพสต์หรือส่งต่อข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับอนุญาต (โดยเฉพาะภาพที่มีเนื้อหาทางเพศของคนอื่น)
- การส่งมัลแวร์ไปทำลายคอมพิวเตอร์ของผู้อื่น

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

หากต้องเผชิญกับการกลั่นแกล้งออนไลน์ แนวทางในการรับมือมีดังนี้

- ไม่ตอบโต้หรือคิดแก้แค้น เพราะไม่เพียงแต่ทำให้ผู้กลั่นแกล้งได้ใจ แต่ยังทำให้ไม่ต่างจากผู้ที่กลั่นแกล้ง
- ใช้เทคโนโลยีให้เป็นประโยชน์ บริการในอินเทอร์เน็ตไม่ว่าจะผ่านเว็บไซต์หรือแอปพลิเคชัน อนุญาตให้บล็อกคนที่ไม่ต้องการติดต่อได้ ถ้าไม่อยากเห็นข้อความ รูปภาพ หรือวิดีโอที่ทำให้คุณรู้สึกแย่ [วิธีการบล็อก: สำหรับอีเมลของกูเกิล เปิดอีเมลของคนที่คุณต้องการบล็อก > เลือกลูกศรชี้ลงเพื่อเปิดเมนู > เลือก บล็อก “ชื่ออีเมล” สำหรับเฟสบุ๊ค คลิกที่ลูกศรชี้ลงด้านขวาบนเพื่อเปิดเมนู > เลือกการตั้งค่า > เลือกเมนู การบล็อก (**blocking**) ทางแถบด้านซ้ายมือ > ใส่รายชื่อของคนที่ต้องการบล็อกเข้าไป]
- ขอความช่วยเหลือ ถ้ารู้สึกไม่สบายใจหรือสถานการณ์เลวร้ายลงเรื่อย ๆ ให้ขอความช่วยเหลือจากคนที่ไว้ใจ การมีใครสักคนที่คอยรับฟังปัญหาและหาทางออกร่วมกัน จะช่วยบรรเทาความรู้สึกจากการถูกกลั่นแกล้งได้ แต่ถ้าสถานการณ์เลวร้ายมากขึ้น ควรปรึกษามืออาชีพ หรือหากการกลั่นแกล้งรุนแรงไปถึงขั้นทำร้ายร่างกายหรือการคุกคามทางเพศ ให้แจ้งตำรวจ

สิทธิส่วนบุคคลในโลกออนไลน์ (ต่อ)

- เก็บหลักฐานไว้ การกลั่นแกล้งในโลกออนไลน์นั้นช่วยให้เก็บรวบรวมหลักฐานการกลั่นแกล้งไว้ได้ง่าย เช่น การเซฟหน้าจอ เพื่อใช้ในการสืบค้นตัวตนของผู้ที่รังแก (กรณีที่ทำโดยไม่เปิดเผย) หรือเป็นหลักฐานในการดำเนินคดี
- อย่าอยู่เฉยถ้าเห็นผู้อื่นโดนกลั่นแกล้ง ควรให้กำลังใจผู้ที่ถูกรังแกและรายงานเรื่องที่พบเห็นให้ผู้ที่เกี่ยวข้อง
- รายงานการกลั่นแกล้งออนไลน์ไปยังผู้ให้บริการอินเทอร์เน็ต (**Internet Service Provider** หรือ **ISP**) หรือผู้ให้บริการมือถือ
- เข้าใจว่าต้นเหตุของการกลั่นแกล้งออนไลน์เกิดจากรากของปัญหาสังคม เช่น ความยากจน ครอบครัวแตกสลาย ดังนั้นการแก้ไขปัญหาการกลั่นแกล้งออนไลน์ระยะยาวจึงอยู่ที่การแก้ไขที่รากของปัญหาจริง ๆ