# อย่าให้เขารู้...ความเป็นส่วนตัว (ยังมี) ในโลก Social

ดร. ปราณีสา อิศรเสนา
คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยี ไทย-ญี่ปุ่น

ผู้ใช้ Social Network หลายคนอาจไม่ทันคิดว่า ข้อมูลส่วนตัวของพวกเขาอาจรั่วไหลได้เพียงเพราะ การตั้งค่า “ความเป็นส่วนตัว” ใน Social Network Application ไม่เป็น หรือไม่ได้ตั้งค่าใดๆ เลย ตัวอย่างเช่น ใน Facebook ซึ่งจริงๆ แล้วเราสามารถกำหนดได้ว่าใครจะมีสิทธิ์เห็นสิ่งที่เราโพสต์บ้าง (รวมถึงรูปที่เพื่อน Tagged เรา) ใครบ้างมีสิทธิ์ติดต่อค้นหาชื่อเราจากอีเมล์หรือหมายเลขโทรศัพท์ได้ ทั้งนี้รวมถึงการค้นหาจากภายนอกเพื่อเข้ามา link กับโปรไฟล์ของเราใน Facebook อีกต่างหาก แต่จะมีผู้ใช้ Social Network สักกี่คนตระหนัก และป้องกันข้อมูลส่วนตัวนี้ ซึ่งเราสามารถปรับแต่งค่าได้ใน Social อื่นๆ เช่น Twitter Google+ Linkedin ด้วยเช่นกัน

นอกจาก Application ใน Social Media จำพวก Facebook หรือ Instagram แล้ว ตัว Web Browser เช่น Internet Explorer Google Chrome หรือ Firefox เอง ก็มีฟังก์ชั่นให้ผู้ใช้กำหนดค่าความเป็นส่วนตัวได้ เพียงแต่ผู้ใช้อาจไม่ได้สนใจจะกำหนดค่าหรือไม่รู้วิธี เช่น เราสามารถสั่งไม่ให้ Browser เก็บค่า Online password ไว้ใน Browser หรือสั่งไม่ให้ตาม track ว่าเราได้เคยไปท่องเว็บใดมาบ้าง เป็นต้น

คุณเป็นอีกคนหนึ่งหรือไม่ ที่จริงๆ ก็รู้หรอกนะว่าเรื่องความเป็นส่วนตัวบนโลกออนไลน์นั้นสำคัญ ข่าวในหนังสือพิมพ์ก็มีออกมาเสมอ แต่ถ้าต้องลงมือทำอะไรที่ยากขึ้นมาหน่อย ก็จะไม่ทำ และบอกกับคนรอบข้างว่า “ช่างมันเถอะ คนธรรมดาอย่างเรา ไม่มีความลับอะไร ถึงดูไปก็เอาไปทำอะไรไม่ได้” จากการศึกษาพบว่าคนส่วนใหญ่ก็คิดเหมือนคุณน่ะแหละ ทำให้เกิดอาชญากรรมทางคอมพิวเตอร์ และการสวมรอยบุคคลออนไลน์เพิ่มขึ้นทุกปี ทั้งที่เราสามารถป้องกันได้ง่ายๆ และการเพิกเฉย อาจส่งผลอย่างร้ายแรงจนคาดไม่ถึง

ผู้เขียนเองได้มีโอกาสดูโฆษณาต่างประเทศข้ำๆ ว่า มีหมอดูยิปซีในกระโจมคนหนึ่งทายข้อมูลส่วนตัวของคนแม่นมากจนน่าตกใจ เช่น รู้ว่าคุณเพิ่งซื้อรถมอเตอร์ไซค์ เพิ่งแต่งงาน ไปเที่ยวที่ไหนมาบ้าง คุณคิดอยากทำอะไรในอนาคต แต่พอเฉลยว่ารู้ได้อย่างไร เขาก็ดึงผ้าคลุมที่กั้นกระโจมออก เห็นเป็นจอคอมพิวเตอร์ยักษ์หลายๆ จอ ที่รวบรวมข้อมูลคนที่ไปดูหมอจากแหล่งต่างๆ เช่น Linkedin Facebook Instagram ที่ใช้ประจำวันนี่แหละ มาปะติดปะต่อกัน ดังนั้น จึงไม่ต้องสงสัยเลยว่าการให้คนอื่นรู้ข้อมูลส่วนตัวของเราขนาดนี้จะอันตรายเพียงไร

ตั้งค่าแบบนี้ดูคุ้นๆ ใช่คุณหรือเปล่า (ตัวอย่างจาก Facebook)

| Settings | Current | New |
|---|---|---|
| • Who can see your future posts? | Public → | Friends |
| • Who can see what others post on your timeline? | Friends of Friends → | Friends |
| • Do you want search engines outside of Facebook to link to your profile? | On → | Off |
| • Who can look you up using the email address you provided? | Everyone → | Friends |
| • Who can look you up using the phone number you provided? | Everyone → | Friends |

ตัวอย่างเช่น 1. ค่าปัจจุบันทุกคน (Public) เห็นโพสต์ในอนาคตของคุณได้ จะดีกว่าไหมถ้าแก้เป็นเฉพาะเพื่อนจึงจะเห็นได้ 2. ใครบ้างจะมีสิทธิ์เห็นข้อความที่คนอื่นโพสต์บนไทม์ไลน์ของคุณ ค่าตั้งต้น คือ เพื่อนของเพื่อนก็เห็นได้ แก้ใหม่เป็นเฉพาะเพื่อนเท่านั้นจะเหมาะกว่า 3. เครื่องมือค้นหาอื่นนอกจากในเฟสบุคสามารถลิงค์กับโปรไฟล์ของคุณได้ค่าตั้งต้นคือ เปิด เปลี่ยนเป็นปิดไว้จะดีกว่า

4. คนอื่นมีสิทธิ์ค้นหาคุณได้จากอีเมล์ที่ให้ไว้ เปลี่ยนจากให้ทุกคนเป็นเฉพาะเพื่อน 5. คนอื่นสามารถค้นหาคุณได้จากหมายเลขโทรศัพท์ที่ให้ไว้ เปลี่ยนจากทุกคนเป็นเฉพาะเพื่อนจะปลอดภัยกว่า

สมมติว่า คุณเป็นเหมือนตัวอย่างข้างต้น ก็ไม่ต้องตกใจไป มีคนอื่นอีกมากที่ตั้งค่าความเป็นส่วนตัวบนสื่อโซเชียล เป็นค่าเบื้องต้น (default) หรือตั้งไม่ค่อยเป็นเหมือนกัน จากการสำรวจของเทรนไมโครผู้นำด้านซอฟต์แวร์แอนตี้ไวรัส พบว่ามีผู้ใช้สื่อโซเชียลเพียง 38% เท่านั้นที่จะรู้วิธี ควบคุมสิ่งที่ตนเองโพสต์ออนไลน์ หลายคนอาจเผลอแชร์ข้อมูลมากกว่าที่ตั้งใจไว้ ซึ่ง จากข้อมูลส่วนตัวนี้ อาจทำให้ผู้โพสต์ถึงขั้นเสียชื่อเสียง หรือตัดโอกาสทางการเรียน การหางานทำได้เลยทีเดียว ตัวอย่างเช่น ครอบครัว อาจารย์หรือนายจ้างในอนาคตของคุณ อาจบังเอิญไปเห็นรูปที่คุณแชร์ตอนทำตัวไม่เหมาะสมเลยเปลี่ยนใจ เคยมีข่าวนักศึกษาถูกปฏิเสธไม่ให้ศึกษาต่อในสถาบันชั้นนำในต่างประเทศเพราะอาจารย์สืบประวัติแล้วนักศึกษาเคยโพสต์สนับสนุนนาซี เป็นต้น ในสหรัฐอมริกาก็มีการสวมรอยเป็นบุคคลอื่นเกิดขึ้นทุกๆ 3 วินาทีเลยทีเดียว

**แนะนำวิธีรักษาข้อมูลส่วนตัวบนโลกออนไลน์**

1. **ให้ระวังซอฟต์แวร์ Third Party ที่ขอสิทธิ์เกินจริง** ซอฟต์แวร์บุคคลที่สาม หมายถึง ซอฟต์แวร์นอกเหนือจากโปรแกรมที่คุณกำลังใช้งานอยู่ เช่น โปรแกรมดูดวง โปรแกรมชวนทดสอบ IQ เป็นต้น ซึ่งอาจมี link ให้เข้าไปดาวน์โหลดจากบน Social Network ที่คุณเล่น แต่จริงๆ แล้วไม่ใช่ว่า ผู้พัฒนา application หรือ Website เป็นรายเดียวกันกับที่คุณไว้ใจ App พวกนี้มักจะขอสิทธิ์เข้าถึงข้อมูลส่วนตัวของคุณมากกว่าที่จำเป็น ซึ่งถ้าคุณเอาแต่กดยอมรับรัวๆ เพราะอยากเล่นเกมส์หรืออะไรก็แล้วแต่ และติดตั้งลงไป ก็เรียบร้อย ตัวอย่างเช่น application ที่ขอตำแหน่งที่อยู่ ข้อมูลใน Contact ของคุณทั้งหมด และส่งข้อความไปหาเพื่อนคุณในนามของคุณเอง ทำลิงค์ไปเว็บที่มี Malware เป็นต้น ซึ่งจริงๆ แล้วถ้าเราตระหนักเรื่องความปลอดภัยก็ไม่น่าลงโปรแกรมพวกนี้ตั้งแต่แรกแล้ว

2. **ผู้สนับสนุน (sponsor) link** โฆษณา หรือ Sponser Link จากสื่อสังคมออนไลน์ก็เช่นกัน เราก็ไม่อาจแน่ใจได้ว่าเว็บของผู้โฆษณาเหล่านี้จะปลอดภัยหรือเปล่า จริงอยู่ว่าเราไม่สามารถบังคับ Social Media ให้ปราศจาก Sponsor ได้ เพราะเป็นรายได้ของเขา แต่เราสามารถกำหนด visibility ของ Application บน Timeline และ Feed ข่าวได้

3. **หัดอ่านนโยบายความเป็นส่วนตัว (Privacy Policy)** ของแต่ละเว็บไซต์ หรือ Social Media Apps บ้างก็ได้แม้อาจดูน่าเบื่อหรือดูจะเป็นภาษากฎหมายเกินไปสักหน่อย แต่จริงๆ แล้วหน้าคำอธิบายนโยบายความเป็นส่วนตัวของผู้ให้บริการ Social Media จะช่วยให้คุณได้แนวคิดว่า สื่อโซเชียลของคุณได้เปิดเผยข้อมูลส่วนตัวของคุณกับใครบ้าง มากน้อยแค่ไหน เขาเก็บข้อมูลคุณอย่างไร ใครมีสิทธิ์เข้าถึงข้อมูลส่วนตัวคุณบ้าง มีการลบข้อมูลทิ้งเมื่อเลิกใช้ไหม และวิธีติดต่อกลับเมื่อเกิดปัญหา เป็นต้น โดยส่วนใหญ่ Privacy Policy จะหาอ่านง่าย ถ้าอยู่ในหน้าเว็บก็จะเป็นหน้าแรกๆ แต่ให้ระวังด้วยว่านโยบายเหล่านี้อาจเปลี่ยนแปลงได้บ่อย เราในฐานะผู้บริโภคจึงควรติดตาม update เสมอ

4. **มีใครมาแอบ Tagged รูปเราไหม** การถูก tagged ในโพสต์อาจดูเหมือนไม่มีอะไร แต่ข้อมูลส่วนตัวของเราจะหลุดได้ก็เพราะถูก Tagged นี่เอง สมมติว่าเพื่อนของคุณ tagged รูปคุณกำลังเมาหรือทำอะไรไม่เหมาะสมโดยที่คุณไม่รู้ตัว คนที่อยู่ใน Contact List ของคุณ รวมทั้งเจ้านายก็จะเห็นรูปที่ไม่อยากให้เห็นนี้ด้วย

ตำแหน่ง Location ของคุณก็อาจถูกเปิดเผยได้เช่นกัน ถึงไม่ได้บอกเป็นพิกัด Latitude Longitude ละเอียด แต่ผู้ไม่หวังดีอาจยังคงได้รายละเอียดอื่นๆ จากคำบรรยายใน tagged อยู่นั่นเอง เช่น เพื่อนคุณ tagged สถานที่ถ่ายภาพ วัน เวลา เป็นต้น จริงๆ แล้วประเด็นนี้จัดการไม่ง่ายนัก เพราะเราควบคุมได้แต่ในส่วนของตัวเองเท่านั้น จะตามไปลบที่เพื่อนเขียนก็คงไม่ได้มีตัวช่วยอีกอย่างหนึ่งเรียกว่า Privacy Scanner ที่มากับแอนตี้ไวรัสชั้นนำ เช่น เทรนด์ไมโคร จะค้นหาว่ารูปเราถูก tagged จากใครที่ไหนบ้าง ถ้าเห็นว่าไม่เหมาะสมก็ต้องบอกโดยตรงไปที่คน tagged ค่ะ ในส่วนของตัวเราๆ สามารถ review tagged post เพื่อตรวจสอบรูปภาพก่อนลงไน Timeline ของเราเองได้

5. **Share ไปเรื่อยเพื่อนช่วยแชร์** บางครั้งความตระหนักในเรื่องความเป็นส่วนตัวของเพื่อนก็อาจส่งผลต่อคุณเช่นกัน เคยไหมที่คุณไปรู้เรื่องส่วนตัวของใครที่คุณไม่เคยรู้จักมาก่อนผ่านการแชร์ของเพื่อนอีกทีหนึ่ง ในทางกลับกันเพื่อนของเพื่อนของคุณก็บังเอิญรับรู้ข้อมูลส่วนตัวของคุณที่เป็นบุคคลที่สามทั้งที่ไม่เคยพบกันเลยด้วยซ้ำ

สำหรับกรณีนี้ ถึงอย่างไรเพื่อนของคุณก็ยังมีสิทธิ์แชร์สิ่งที่คุณโพสต์ได้อยู่ดี ต่อให้คุณ set privacy ให้แข็งแรงเพียงไร สำหรับเพื่อนก็ยังเห็นได้ บาง APP จะยอมให้เพื่อนใน Contact สามารถ copy และส่งต่อโพสต์ต้นฉบับได้จำนวนมากๆ

สิ่งที่เราทำได้ก็คือ

จำกัดคนเห็นสิ่งที่เราโพสต์เท่าที่จำเป็น เช่น โพสต์ให้เพื่อนเห็น แต่ไม่ให้เพื่อนของเพื่อนเห็นโดยอัตโนมัติ เพื่อจำกัดวงการแชร์ข้อมูลให้แคบลง พูดคุยกับเพื่อนให้เข้าใจว่าอย่าแชร์เรื่องที่คุณไม่สะดวกให้คนอื่นเห็น

6. **Deactivate กับ Delete Account ไม่เหมือนกัน**

บางคนคิดว่าเมื่อ Deactivate account บนสื่อออนไลน์ไปแล้วข้อมูลจะถูกลบ แต่จริงๆ หมายถึงการพักใช้บัญชีนั้นและสามารถเรียกกลับมาใช้ได้ต้องระวัง การลบบัญชีถาวรจะดีกว่า

สุดท้ายนี้ขอให้ทุกท่านรู้จักรักษาข้อมูลส่วนตัวมากขึ้น และใช้สื่อออนไลน์ได้อย่างสนุก และปลอดภัยค่ะ TPA news