

## การใช้งาน Social Network อย่างปลอดภัย

Social Network มีข้อดีมากมาย โดยเฉพาะในการแสดงออกทางความคิด และกิจกรรมต่างๆ รวมทั้งการรับรู้ข้อมูลจากผู้อื่น ด้านธุรกิจอีคอมเมิร์ซก็เช่นกัน Social Network ทำให้ผู้ขายได้ประชาสัมพันธ์สินค้าได้ง่ายขึ้น ผู้ซื้อก็มีโอกาสเข้าถึงสินค้าได้ง่ายเช่นกัน แต่การที่ผู้ใช้งาน Social Network มีโอกาสเผยแพร่ข้อมูลได้ง่าย รวมทั้งทุกคนสามารถใช้งานได้ ก็ทำให้ข้อมูลใน Social Network อาจจะเป็นข้อมูลที่ไม่ถูกต้อง อีกทั้งมีโอกาที่จะสูญเสียความเป็นส่วนตัวไปได้ ซึ่งแน่นอนว่าคงไม่เสมอไปที่เราจะเจอกับปัญหาต่างๆ ใน Social Network แต่การรู้ทันปัญหาที่อาจจะเกิดขึ้นได้นั้น ก็เป็นการที่เรจะได้ป้องกันและระวังภัยต่างๆ ได้ ดังนี้

1. คิดให้รอบคอบก่อนโพสต์ข้อมูลใดๆ เพราะอย่าลืมว่าข้อมูลเหล่านี้จะเปิดเผยให้ทุกคนสามารถเข้าถึงได้ง่าย โดยเฉพาะอย่างยิ่งการโพสต์ข้อมูลที่สุ่มเสี่ยงก็อาจจะส่งผลร้ายต่อตัวเราเองก็เป็นได้
2. ใช้ความระมัดระวังในการคลิกลิงก์ต่างๆ ที่มากับการแชร์หรือข้อความ หลีกเลี่ยงลิงก์แปลกปลอม หรือมาจากคนที่ไม่รู้จัก หรือแม้แต่เพื่อนซึ่งใช้ภาษาในการสื่อสารที่ดูแปลกไปจากปกติ เพราะอาจเป็นลิงก์ที่นำไปสู่ไวรัสหรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์
3. พิมพ์ที่อยู่ URL ของเว็บไซต์โซเชียลเน็ตเวิร์กนั้นๆ โดยตรง โดยบนเบราว์เซอร์ให้หลีกเลี่ยงการเข้าเครือข่ายทางสังคมผ่านทางคลิกลิงก์จากผลแสดงการค้นหา หรือจากอีเมล เพราะอาจเป็น URL ปลอมที่นำเราไปยังเว็บไซต์ปลอม เพื่อหลอกเอาบัญชีผู้ใช้และ Password ได้ เช่น [www.facebook.com](http://www.facebook.com) อาจมี URL หลอกเป็น [www.faeebook.com](http://www.faeebook.com) เป็นต้น
4. คัดกรองคนที่ขอเป็นเพื่อน หรือขอเชื่อมโยงกับเครือข่ายสังคมออนไลน์ของเรา หลีกเลี่ยงการตอบรับคนที่ไม่รู้จักกันมาก่อน เพราะผู้ไม่หวังดีอาจแฝงมากับคนที่ขอเข้ามาเป็นเพื่อนเรา และหากพบคนที่เป็เพื่อนซึ่งเราไม่รู้จักและน่าสงสัยก็ควรลบออกไป
5. ตั้งค่าความเป็นส่วนตัว ผู้ให้บริการแต่ละรายจะกำหนดการตั้งค่าส่วนตัวไว้เพื่อไม่ให้ข้อมูล หรือสิ่งที่เราทำหลุดออกไปยังคนที่ไม่พึงประสงค์ ดังนั้น เราควรตั้งค่าให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเรา และหลีกเลี่ยงการตั้งค่าสิ่งที่เราทำให้เป็นสาธารณะ หรือคนทั่วไปเห็นได้
6. ไม่แสดงข้อมูลส่วนตัวที่เป็นความลับ เช่น บัตรประจำตัวประชาชน บัตรเครดิตลงในโซเชียลเน็ตเวิร์ค ไม่ว่าจะอยู่ในรูปแบบข้อความ หรือรูปภาพ เพราะแฮกเกอร์และผู้ไม่หวังดีสามารถแฝงตัวมากับกลุ่มเพื่อนที่เราอนุญาตให้เข้าชมได้
7. เปิดใช้งาน Do Not Track เพื่อป้องกันการติดตามและการเก็บข้อมูลของผู้ให้บริการ ซึ่งอาจรวมไปถึงผู้ไม่หวังดีที่ลักลอบเข้ามาขโมยข้อมูลด้วย ซึ่งปัจจุบันมีเว็บเบราว์เซอร์ที่เปิดใช้งาน Do Not Track ได้แล้ว เช่น Internet Explorer 10

8. ใช้วิจารณญาณอย่างสูงในการรับข่าวสาร และอย่าปักใจเชื่อข้อมูลที่เผยแพร่เข้ามาในทันที รวมทั้งการกล่าวอ้างถึงแหล่งที่มาของข้อมูลนั้นๆ เพราะอาจมีการสวมรอย หรือสมอ้างจากผู้ไม่หวังดีเพื่อสร้างข่าว หรือสร้างความเสียหายต่อแหล่งที่มา นั้นได้

9. ดูแลและควบคุมการใช้งานของบุตรหลานอย่างใกล้ชิด สอนให้เด็กรู้จักวิเคราะห์ข้อมูล และรู้จักเล่นอย่างถูกวิธี เพราะความรู้ในโซเชียลเน็ตเวิร์คก็มีอยู่มากมาย และปัจจุบันครูอาจารย์ก็ทันสมัยจนแจ้งเรื่องต่างๆ แก่ลูกศิษย์ผ่านโซเชียลเน็ตเวิร์ค เช่น Facebook หรือ Twitter กันแล้ว นอกจากนี้ อาจหาเครื่องมือในการควบคุมการใช้งานของบุตรหลานได้ เช่น โปรแกรม Windows Live Family Safety ซึ่งเป็นโปรแกรมที่ไม่ใครซอฟต์แวร์เปิดให้ใช้งานได้ฟรีๆ นอกจากจะใช้ควบคุมการเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมได้แล้ว ยังสามารถกำหนดช่วงเวลาในการใช้คอมพิวเตอร์ และป้องกันการใช้โปรแกรม หรือเล่นเกมที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตได้อีกด้วย

10. ตระหนักว่าเป็นสังคมเสรี แม้ว่าทุกคนจะมีสิทธิ์ในการแสดงความคิดเห็น แต่ทุกคำพูดและการกระทำที่ไม่เหมาะสมก็สามารถเป็นเหตุในการฟ้องร้องได้ และศาลก็อาจจะรับฟังคำร้องด้วย

**เล่น Social Network ให้ปลอดภัย “รู้” ไว้เสี่ยงอันตราย**

ThaiCERT ETDA ICT  
etda.thailand ThaiCERT thaicert.or.th

- คิดให้รอบ**  
สติก่อนโพสต์  
เพราะมันเปิดเผยและทุกคนเข้าถึงได้ง่าย การโพสต์ข้อมูลก็เสี่ยงจึงอาจเป็นภัยต่อตัวเอง
- ระมัดระวัง**  
ในการคลิกลิงก์  
ที่มาบนโซเชียล เพราะอาจนำไปสู่ไวรัส หรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์
- พิมพ์ URL โดยตรง**  
เข้าโซเชียลเน็ตเวิร์ค  
เสี่ยงคลิกลิงก์ เพราะอาจเป็น URL ปลอมหลอกเอาบัญชีใช้งานของเรา เช่น facebook.com อาจมี URL ผิดเป็น faebook.com
- รอบคอบ**  
ก่อนตอบรับเป็นเพื่อน  
คัดกรองคนที่ขอเป็นเพื่อนโดยเข้าไปดูโปรไฟล์ก่อนทุกครั้ง เพราะอาจมีผู้ไม่หวังดีแฝงมาด้วย
- ตั้งค่า**  
ความเป็นส่วนตัว  
หลีกเลี่ยงตั้งค่าบนสาธารณะ และอนุญาตให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเราได้
- ไม่แสดงข้อมูล**  
ส่วนตัวที่เป็นความลับ  
เช่น บัตรประชาชน บัตรเครดิต  
ไม่ว่าจะอยู่ในรูปแบบข้อความหรือรูปภาพก็ตาม
- เปิดใช้งาน Do Not Track**  
ป้องกันการติดตามและเก็บข้อมูลจากผู้ใช้บริการโซเชียลเน็ตเวิร์ค รวมทั้งผู้ไม่หวังดีที่เข้ามาขโมยข้อมูล
- ใช้วิจารณญาณ**  
ในการรับข่าวสาร  
อย่าปักใจเชื่อทันที อาจมีการสร้างกระแส สวมรอย สมอ้างจากผู้ไม่หวังดี
- ควบคุมการใช้งาน**  
ของบุตรหลาน  
มองหาเครื่องมือมาเป็นตัวช่วย เช่น Windows Live Family Safety
- ตระหนักว่าเป็นสังคมเสรี**  
แม้ทุกคนมีสิทธิ์ในการแสดงความคิดเห็น แต่การกระทำที่ไม่เหมาะสมก็เป็นเหตุให้ถูกฟ้องร้อง และศาลก็อาจรับฟังคำร้องด้วย

ภาพประกอบจาก ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)