# ปกป้องอีเมลให้ปลอดภัย

เราเชื่อมต่อกันมากขึ้นกว่าแต่ก่อนผ่านทางอินเทอร์เน็ต เราสามารถส่งข้อความ 140 ตัวอักษร (ด้วย Twitter) แช็ตออนไลน์ (ด้วย Google Talk) คุยโทรศัพท์ (ด้วย Skype) หรือแลกเปลี่ยนรูปภาพและวิดีโอ (ด้วย Facebook และ YouTube)

อย่างไรก็ตาม อีเมลยังคงเป็นช่องทางการสื่อสารหลักของเราบนอินเทอร์เน็ต มันถูกใช้อย่างแพร่หลายสำหรับทั้งเรื่องส่วนตัวและเรื่องงาน เนื่องจากมันจะอยู่กับเราไปอีกนาน เราจึงควรรู้ถึงความปลอดภัย (หรือไม่ปลอดภัย) ของมัน และตระหนักถึงการรักษาความปลอดภัยข้อมูลของเรา ในระหว่างที่ข้อมูลนั้นเดินทางผ่านอินเทอร์เน็ต

เมื่อคุณเดินทางจากเมืองหนึ่งไปอีกเมืองหนึ่ง คุณสามารถแบ่งความปลอดภัยออกเป็น: ความปลอดภัยที่ต้นทาง, ที่ปลายทาง, บนท้องถนน, และความปลอดภัยของตัวคุณเองในฐานะผู้เดินทาง สำหรับเว็บไซต์ที่ให้บริการอีเมล ความปลอดภัยเหล่านี้เทียบได้กับ: ผู้ให้บริการอีเมล (ต้นทาง), หน้าจอรับส่งอีเมลของคุณ (ปลายทาง), การส่งผ่านอินเทอร์เน็ต (ถนน), และเนื้อหาอีเมล (ผู้เดินทาง)

## ผู้ให้บริการ: ผู้รักษาข้อมูลของคุณ

ในปี 2550 มีบริการอีเมล 'ฟรี' เพิ่มขึ้นอย่างมากและมีแนวโน้มเพิ่มขึ้นเรื่อย ๆ ทำให้การเข้าถึงอีเมลง่ายขึ้น (แม้แต่ผู้ที่ไม่มีคอมพิวเตอร์หรือไม่มีอินเทอร์เน็ตใช้เป็นประจำ ก็มีอีเมลได้) และมีพื้นที่เก็บข้อมูลออนไลน์เพิ่มขึ้นอย่างมาก สิ่งนี้ทำให้มีความเสี่ยงเพิ่มขึ้น เนื่องจากความง่ายในการเข้าถึงข้อมูล ทำให้ยากต่อการควบคุมข้อมูลของเรา ลองพิจารณาเรื่องต่อไปนี้ เมื่อคุณใช้บริการอีเมลฟรี:

- ข้อมูลของคุณ (อีเมล แฟ้มแนบ และอื่น ๆ) ถูกเก็บอยู่ที่เซิร์ฟเวอร์ของผู้ให้บริการ คุณไม่สามารถควบคุมการจัดการข้อมูลที่ฝั่งพวกเขาได้ ทำได้แค่เพียงเชื่อใจและฝากข้อมูลของคุณและคนที่คุณสื่อสารด้วยไว้เท่านั้น
- ทำความเข้าใจว่าผู้ให้บริการนั้นใช้ข้อมูลของคุณหรือไม่อย่างไร (อ่านก่อนคลิกปุ่ม 'ตกลง')
- สำหรับอีเมลและการสื่อสารที่อ่อนไหวมาก กรุณาเลือกใช้ผู้ให้บริการอีเมลฟรีที่กล่าวอย่างชัดเจนว่า เขาจะรักษาความปลอดภัย และไม่ใช้หรือเปิดเผยข้อมูลของคุณ (ลองอ่าน http://security.ngoinabox.org/en/riseup_main)
- การสื่อสารนั้นเป็นกระบวนการสองทาง คุณต้องแน่ใจว่าผู้ที่คุณสื่อสารด้วยนั้น ใช้บริการที่มีความปลอดภัยเช่นกัน อีเมลของคุณจะไม่มีทางปลอดภัย ถ้ามีเพียงฝ่ายเดียวที่ใช้บริการที่ปลอดภัย แต่อีกฝ่ายไม่ได้ใช้

## หน้าจอรับส่ง: วิธีการเข้าถึงอีเมล

วิธีที่ใช้กันมากที่สุดเพื่อเข้าถึงอีเมลนั้นคือ ผ่านทางเว็บเบราว์เซอร์ ซึ่งสะดวกและสามารถเข้าถึงจากคอมพิวเตอร์เครื่องใดก็ได้ การเข้าถึงอีเมลด้วยวิธีนี้ หมายความว่า ข้อมูลจะเดินทางจากเซิร์ฟเวอร์ (ซึ่งข้อมูลของคุณนั้นถูกเก็บอยู่) ไปยังคุณ (ที่หน้าจอเว็บเบราว์เซอร์ของคุณ)

เว็บเบราว์เซอร์ (เช่น Internet Explorer, Firefox, หรือ Chrome) นั้นมีความเสี่ยงต่อการถูกโจมตีทางอินเทอร์เน็ต เมื่อใช้เบราว์เซอร์เพื่ออ่านหรือส่งอีเมล เราจึงเพิ่มความเสี่ยงที่ข้อมูลของเราจะรั่วไหล

ให้พิจารณาเลือกใช้เบราว์เซอร์ที่มีความปลอดภัยมากขึ้น Firefox ถือเป็นตัวเลือกที่ดี และสามารถปลอดภัยขึ้นได้อีก ถ้าคุณติดตั้งส่วนเสริม (add-ons) เพื่อปกป้องความเป็นส่วนตัวและความปลอดภัยเพิ่มเติม ดูข้อมูลเรื่องนี้เพิ่มได้อีกที่ : https://security.ngoinabox.org/en/firefox_main

## การส่งผ่าน: อีเมลของคุณเดินทางอย่างไร

การรักษาความปลอดภัยที่ปลายทางของทั้งสองฝ่าย ทำให้ข้อมูลปลอดภัยขึ้นได้ระดับหนึ่ง แต่ถนนระหว่างจุดหมายและปลายทางก็สำคัญไม่น้อยกว่ากัน โดยทั่วไปแล้ว อีเมลเดินทางจากเซิร์ฟเวอร์อีเมลไปยังคุณด้วยความปลอดภัยที่ต่ำหรือไม่มีเลย อีเมลโดยปกติถูกส่งในรูปแบบข้อความธรรมดา ซึ่งหมายความว่าใครก็ตามที่สามารถเข้าสู่เส้นทางการส่ง ก็สามารถอ่านอีเมลของคุณได้ ลองพิจารณาคำแนะนำต่อไปนี้:

- ตรวจสอบที่อยู่อินเทอร์เน็ต (URL) เมื่อคุณใช้บริการอีเมลฟรี (ดูที่ด้านบนของเบราว์เซอร์) ถ้าที่อยู่ขึ้นต้นด้วย http แสดงว่าการเดินทางของอีเมลนั้นไม่ปลอดภัย และมันอยู่ในรูปแบบที่ถูกดักฟังได้
- อีเมลผ่านหน้าเว็บหลายแห่ง ใช้ https เพื่อเข้ารหัสข้อมูลไม่ให้ถูกดักฟัง แต่บางแห่ง (เช่น Yahoo! Mail) จะเข้ารหัสเฉพาะชื่อผู้ใช้และรหัสผ่านระหว่างล็อกอินเท่านั้น ขณะที่บางแห่ง (เช่น Gmail) จะใช้ https เข้ารหัสอีเมลทั้งหมดของคุณตลอดการสื่อสาร

## เนื้อหา: ข้อความที่แท้จริง

ในที่สุดแล้ว เนื้อหาของอีเมลคือสิ่งที่คุณพยายามรักษาไว้เป็นความลับ นั่นคือ คุณไม่ต้องการให้ใครเห็นหรือเข้าสู่ข้อมูลของคุณได้ ในระหว่างที่มันเดินทางจากคุณไปยังผู้ให้บริการอีเมล อย่างไรก็ตาม:

- เมื่อคุณส่งอีเมลออกไปแล้ว คุณไม่สามารถควบคุมอีเมลดังกล่าวได้อีกต่อไป ถ้าคนที่คุณสื่อสารด้วยไม่ระมัดระวังเรื่องความปลอดภัย อีเมลและความปลอดภัยของคุณก็มีความเสี่ยงเช่นกัน
- ถ้าคุณเก็บอีเมลไว้ในเครื่องคอมพิวเตอร์ส่วนตัว คนอื่นที่เข้าถึงคอมพิวเตอร์คุณได้ก็สามารถอ่านอีเมลของคุณได้เช่นกัน

วิธีแก้ปัญหานี้ คือการเข้ารหัส (encryption) ซึ่งเป็นหนึ่งในวิธีที่ดีที่สุดในการรักษาความปลอดภัยให้เนื้อหาอีเมล แฟ้ม หรือข้อมูลที่อ่อนไหวอื่น ๆ ของคุณ การเข้ารหัสข้อมูลคือการใช้โปรแกรมแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้ ซึ่งข้อมูลจะอ่านได้ก็ต่อเมื่อคุณใส่รหัสลับที่ใช้ถอดรหัส ดูข้อมูลเพิ่มเติมเรื่องนี้ได้ที่ : http://security.ngoinabox.org/en/chapter_7_4

TACTICAL TECHNOLOGY COLLECTIVE

Front Line PROTECTION OF HUMAN RIGHTS DEFENDERS

ดูชุดเครื่องมือ **ปลอดภัยทันใจ** ของเราได้ที่ security.ngoinabox.org

จัดพิมพ์โดย เครือข่ายพลเมืองเน็ต thainetizen.org ก.ค. 2554 - อนุญาตให้ทำซ้ำได้โดยไม่ต้องขออนุญาต