อินเทอร์เน็ตทำงานอย่างไร

อินเทอร์เน็ตเป็นเครื่องมือที่มีประโยชน์และทรงพลัง ที่ไม่เพียงแต่เพื่อการใช้งานส่วนตัวเท่านั้น แต่ยังใช้สำหรับงานรณรงค์ได้ด้วย เราส่วนใหญ่ที่ใช้อินเทอร์เน็ตกัน เพราะว่ามันมีข้อมูลจำนวนมาก และสื่อสารได้รวดเร็ว อย่างไรก็ตาม ถ้าคุณทำงานกับข้อมูลที่ต้องการความปลอดภัยสูง หรือกับผู้คนหรือองค์กรที่เน้นประเด็นที่เป็นความลับและต้องการความปลอดภัยสูง คุณควรทำความเข้าใจให้ถ่องแท้ว่าอินเทอร์เน็ตนั้นสื่อสารกันอย่างไร และเก็บข้อมูลของคุณไว้อย่างไร และมีความปลอดภัยจริงหรือไม่แค่ไหน

เพื่อทำความเข้าใจเรื่องความเป็นส่วนตัวและความปลอดภัยในอินเทอร์เน็ต คุณควรมีความรู้พื้นฐานว่าอินเทอร์เน็ตนั้นทำงานอย่างไร คุณเชื่อมต่อเข้ากับอินเทอร์เน็ตได้อย่างไร? อีเมลเดินทางจากคุณไปยังผู้รับเป้าหมายของคุณได้อย่างไร? ผลการค้นหาข้อมูลของคุณมาปรากฏที่เครื่องคอมพิวเตอร์ของคุณได้อย่างไร? ความเข้าใจสิ่งเหล่านี้ จะช่วยให้คุณรู้ว่ามีอะไรกำลังเกิดขึ้นอยู่หลังฉากของอินเทอร์เน็ต เมื่อคุณคลิก “ส่ง” หรือ “ค้นหา” ในครั้งต่อไป และจะมีความระมัดระวังมากขึ้นในเรื่องความปลอดภัยและความเป็นส่วนตัวในอินเทอร์เน็ต

ความรู้พื้นฐาน

- ทุกคนใช้บริการของผู้ให้บริการอินเทอร์เน็ต (ไอเอสพี) ในการเชื่อมต่ออินเทอร์เน็ต ซึ่งส่วนใหญ่เป็นบริษัทโทรคมนาคมขนาดใหญ่ หรือเป็นบริษัทผู้ให้บริการอินเทอร์เน็ตขนาดเล็ก ซึ่งไอเอสพีขนาดเล็กอาจเชื่อมต่อผ่านทางบริษัทโทรคมนาคมขนาดใหญ่อีกที
- เมื่อคุณเชื่อมต่อกับอินเทอร์เน็ต ไอเอสพีของคุณจะมอบหมายเลขที่เรียกว่าหมายเลขไอพี (IP address) ให้กับคุณ หมายเลขนี้เหมือนกับเลขที่บ้าน และทำหน้าที่เหมือนกับเลขที่บ้านด้วย การสื่อสารส่วนใหญ่ที่เกิดขึ้นในอินเทอร์เน็ตเป็นการสื่อสารแบบสองทาง หมายเลขไอพีช่วยให้คุณส่งและรับการสื่อสารทางอินเทอร์เน็ต ในรูปแบบของอีเมล การท่องเว็บ และการสื่อสารอื่น ๆ คุณไม่สามารถอยู่บนอินเทอร์เน็ตได้ถ้าไม่มีหมายเลขไอพี การไม่มีหมายเลขไอพีหมายถึงการไม่มีอินเทอร์เน็ตนั่นเอง
- หมายเลขไอพีนั้นถูกกำหนดตามตำแหน่งภูมิศาสตร์ ซึ่งหมายความว่า ในบางประเทศจะมีหมายเลขไอพีเพียงชุดเดียวเท่านั้น หมายเลขไอพีนั้นแตกต่างกันไปในแต่ละประเทศ และถูกควบคุมโดยไอเอสพี (บริษัทโทรคมนาคม) ด้วยวิธีการบางอย่าง
- ผู้ให้บริการอินเทอร์เน็ตยังให้บริการการจัดเส้นทาง (routing) ด้วย โดยการกำหนดเส้นทางเดินจราจรทางอินเทอร์เน็ตของคุณ มันทำหน้าที่เหมือนกับตำรวจจราจรตามทางแยก ที่คอยกำหนดทางเดินของคุณบนอินเทอร์เน็ต ไอเอสพีส่วนใหญ่ควบคุมทางแยกต่าง ๆ ดังกล่าวบนอินเทอร์เน็ต

ความไม่ปลอดภัย

- การสื่อสารส่วนใหญ่ทางอินเทอร์เน็ตมีที่อยู่ “ปลายทาง” และ “ต้นทาง” ซึ่งมันคือหมายเลขไอพี ตัวอย่างเช่น ข้อความอีเมลทั้งหมดมีที่อยู่ดังกล่าวนี้ เพียงแต่เรามองไม่เห็น ซึ่งหมายความว่าถ้ามีใครบางคนมีอีเมลของคุณฉบับหนึ่ง เขาจะรู้ได้อย่างแน่นอนว่ามันมาจากไหน และมันกำลังจะไปไหน จำไว้ว่าหมายเลขไอพีนั้นถูกกำหนดตามภูมิศาสตร์ ดังนั้นมันจึงระบุประเทศได้ และบางทีอาจระบุได้ถึงระดับบ้านเลขที่ หรือกระทั่งผู้สมัครใช้บริการ (นั่นก็คือ คุณ!) ทั้งนี้ขึ้นอยู่กับว่าไอเอสพีนั้นจัดสรรหมายเลขไอพีอย่างไร
- การท่องเว็บก็ทำงานลักษณะเดียวกัน ถ้าบางคนสามารถรู้ประวัติหรือบันทึกการจราจรทางอินเทอร์เน็ตของคุณ เขาอาจรู้ว่าคุณกำลังเข้าไปเยี่ยมชมเว็บไซต์ไหนอยู่ จำไว้ว่า ทุกคนบนอินเทอร์เน็ตมี หมายเลขไอพีเพื่อให้สามารถสื่อสารได้ ทุกเว็บไซต์ก็มีหมายเลขไอพีด้วย เมื่อคุณเข้าไปหน้าเว็บเพจหนึ่ง หมายถึงคุณได้เปิดเผย หมายเลขไอพีเพื่อให้เว็บไซต์ดังกล่าวนั้นสามารถส่งหน้าเว็บเพจที่คุณร้องขอดูให้คุณได้
- ทางแยกของอินเทอร์เน็ตที่กำหนดเส้นทางจราจรของคุณ (ปกติกำหนดโดยไอเอสพี) สามารถที่จะดูการจราจรทางอินเทอร์เน็ตทั้งหมดของคุณได้ เนื่องจากไอเอสพีเป็นผู้กำหนดเส้นทางให้กับคุณ เขาจึงรู้ว่าคุณอยู่ไหนและคุณกำลังจะไปที่ไหน เป็นเรื่องที่ต้องระวังอย่างมาก ถ้าไอเอสพีของคุณนั้นถูกควบคุมหรือถูกสั่งการโดยกลุ่มอาชญากรรมที่เป็นบุคคลภายนอก

สิ่งที่ต้องพิจารณา

- ให้ระวังเป็นพิเศษเมื่อทำการส่งและรับ และดูข้อมูลที่ต้องการความปลอดภัยสูงทางอินเทอร์เน็ต
- ตรวจสอบชื่อเสียงของไอเอสพีที่คุณใช้บริการ หรือสถานที่ที่คุณวางแผนที่จะเชื่อมต่อเข้ากับอินเทอร์เน็ต
- ต้องแน่ใจว่า คนที่คุณจะสื่อสารด้วย นั้นก็มีความระมัดระวังในเรื่องความลับและความปลอดภัยอย่างสูงด้วย การสื่อสารนั้นเป็นกระบวนการสื่อสารสองทาง จะไม่มีประโยชน์เลยในการป้องกันความลับและความปลอดภัยแต่เพียงฝ่ายเดียว ถ้าคู่สื่อสารอีกฝ่ายไม่ให้ความสำคัญ
- ให้ใช้บริการพร็อกซี (proxy) และโปรแกรมที่ช่วยปิดบังชื่อคุณทางอินเทอร์เน็ต ซึ่งจะช่วยให้คุณเข้าสู่อินเทอร์เน็ตและสื่อสารทางอินเทอร์เน็ต โดยใช้หมายเลขไอพีของคอมพิวเตอร์อีกเครื่องหนึ่ง ซึ่งช่วยปิดบังตัวตนของคุณได้อีกระดับหนึ่งในอินเทอร์เน็ต แหล่งข้อมูลเรื่องความปลอดภัยนี้ แนะนำให้เข้าไปดูที่ :
    - http://security.ngoinabox.org/en/chapter-8
    - http://security.ngoinabox.org/en/tor_main
    - http://www.torproject.org/
    - https://www.sesawe.net/
    - http://thainetizen.org/unblock

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

ใช้อินเทอร์เน็ตอย่างปลอดภัย

ไม่กี่ปีก่อนหน้านี้ อินเทอร์เน็ตถูกใช้ส่วนใหญ่เพื่อการค้นหาและอ่านข้อมูล แต่เมื่อเวลาผ่านไป มันกลายเป็นสถานที่เก็บข้อมูลของคุณมากขึ้นเรื่อย ๆ และค่อย ๆ แทนที่คอมพิวเตอร์ของคุณในฐานะที่เก็บแฟ้มข้อมูล ข้อความสั้น ข้อความแช็ต รูปภาพ อีเมล แม้กระทั่งบันทึกสัพเพเหระของคุณ บริการบางอย่างมักแนะนำให้คุณเก็บข้อมูลส่วนตัว เช่น แฟ้มงาน ไว้บนอินเทอร์เน็ต การมีพื้นที่เก็บอย่างไม่จำกัดและการเข้าสู่แฟ้มข้อมูลจากที่ไหนก็ได้ นั้นล่อตาล่อใจให้คุณใช้ (และต้องพึ่งพา) บริการและสิ่งอำนวยความสะดวกดังกล่าว ถ้าคุณทำงานกับข้อมูลที่อ่อนไหวหรือติดต่องานกับคนที่ทำงานเช่นนั้น คุณควรคิดให้รอบคอบว่าจะเก็บข้อมูลและแฟ้มข้อมูลไว้ที่ใด

ความไม่ปลอดภัย

- โดยมากแล้ว ก่อนจะใช้บริการได้ คุณอาจต้องมอบข้อมูลส่วนตัวให้กับบริการเหล่านี้ก่อน และบริการเหล่านี้จะมีสิทธิบางอย่างในการใช้ข้อมูลของคุณ
- บริการเหล่านี้เกือบทั้งหมด จะอนุญาตให้คุณใช้เพียงชื่อผู้ใช้และรหัสผ่าน เป็นมาตรการความปลอดภัย เพื่อป้องกันไม่ให้คนอื่นเข้าใช้ข้อมูลของคุณโดยไม่รับอนุญาต นอกเหนือจากนี้แล้ว คุณต้องเชื่อใจผู้ให้บริการว่าจะรักษาความปลอดภัยของแฟ้มและข้อมูลของคุณ
- บริการเหล่านี้ส่วนใหญ่ เข้าใช้ได้เฉพาะทางเบราว์เซอร์ ซึ่งตัวเบราว์เซอร์เองก็อาจมีช่องโหว่และความไม่ปลอดภัย
- การสื่อสารนั้นเกิดขึ้นบนอินเทอร์เน็ต ดังนั้นจึงมีความเสี่ยงต่อความไม่ปลอดภัยทั้งปวงที่เกิดขึ้นได้บนอินเทอร์เน็ต

สิ่งที่ต้องพิจารณา

- ตรวจสอบชื่อเสียงของบริการอินเทอร์เน็ตที่คุณต้องการใช้อยู่เสมอ บริการเหล่านี้เคยมีปัญหาเรื่องข้อมูลส่วนตัวรั่วไหลหรือปัญหาความปลอดภัยอื่นใดหรือไม่?
- อ่านข้อตกลงการใช้ (End User License Agreements - EULA) ของบริการเหล่านี้ให้ละเอียดเสียก่อน ข้อตกลงนี้อาจระบุให้คุณต้องมอบสิทธิความเป็นเจ้าของแฟ้มข้อมูลให้กับตัวบริ การ
- พิจารณาถึงความอ่อนไหวของข้อมูลและแฟ้มของคุณ การมีข้อมูลดังกล่าวบนอินเทอร์เน็ตจะทำให้ตัวคุณและผู้อื่นไม่ปลอดภัยหรือไม่ ?
- ตรวจสอบว่าแฟ้มและข้อมูลของคุณมีมาตรการรักษาความปลอดภัยอะไรอยู่ มาตรการเหล่านี้ควรตรวจสอบได้และผ่านการตรวจสอบโดยองค์กรภายนอกที่เกี่ยวกับความเป็นส่วนตัวและความปลอดภัย
- ตรวจสอบและระบุให้ชัดว่าข้อมูลอันไหนสามารถเก็บได้หรือได้เก็บไว้แล้วบนอินเทอร์เน็ต และอันไหนควรเก็บไว้ที่เครื่องคอมพิวเตอร์ของคุณจะดีกว่า
- ถ้าคุณใช้บริการเหล่านี้ คุณต้องแน่ใจว่ามีรหัสผ่านที่ปลอดภัย และเปลี่ยนรหัสผ่านเป็นประจำ

- ให้พิจารณาใช้เบราว์เซอร์ที่ปลอดภัย เช่น Firefox ที่มีมาตรการความปลอดภัยสูงอยู่ในตัว และมีส่วนเสริมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยเพิ่มมากขึ้นเรื่อย ๆ
- ใช้ **“https”** แทน “http” เมื่อเชื่อมต่อกับบริการออนไลน์ทุกครั้งที่เป็นไปได้ การใช้ “https” จะเข้ารหัสการเชื่อมต่อระหว่างเบราว์เซอร์กับบริการที่คุณกำลังใช้ ซึ่งหมายความว่าชื่อผู้ใช้ รหัสผ่าน และข้อมูลอื่น ๆ ของคุณจะถูกส่งอย่างปลอดภัย
- ถ้าคุณต้องการเก็บแฟ้มข้อมูลไว้บนบริการออนไลน์ คุณควรเข้ารหัสแฟ้มก่อนส่งไปเก็บไว้กับบริการดังกล่าว TrueCrypt เป็นโปรแกรมเข้ารหัสลับที่สามารถใช้เพื่อรักษาความปลอดภัยของข้อมูล จากการเข้าถึงที่ไม่ได้รับอนุญาต แม้ว่าแฟ้มของคุณจะถูกเผยแพร่ออกสู่สาธารณะก็ตาม

แหล่งข้อมูลที่ช่วยคุณได้

- http://security.ngoinabox.org/en/chapter-3
- http://security.ngoinabox.org/en/keepass_main
- http://security.ngoinabox.org/en/chapter-7
- http://security.ngoinabox.org/en/firefox_main
- https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/
- http://security.ngoinabox.org/en/truecrypt_main
- http://www.truecrypt.org/
- http://thainetizen.org/https-everywhere

อินเทอร์เน็ตรักษาข้อมูลของคุณให้เป็นส่วนตัวได้ดีแค่ไหน ?

> มันไม่ได้ถูกสร้างมาให้ทำอย่างนั้น

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

เชื่อมต่อเครือข่ายสังคมอย่างปลอดภัย

เครื่องมือและบริการเชื่อมต่อเครือข่ายสังคมเป็นบริการที่ได้รับความนิยมสูงสุดในอินเทอร์เน็ตทุกวันนี้ เครือข่ายสังคมทำให้คุณเชื่อมต่อกับกลุ่มเพื่อนและเพื่อนใหม่ของคุณได้มากกว่าเดิม เครื่องมือและบริการเหล่านี้อนุญาตให้คุณแบ่งปันข้อมูลในรูปแบบข้อความ รูปภาพ แฟ้ม แม้กระทั่งตำแหน่งและการเคลื่อนไหวต่าง ๆ ของคุณ เราสามารถส่งต่อข้อมูลได้ทันที หรือเก็บข้อมูลไว้ใช้เมื่อเราล็อกอินเข้าเครือข่ายสังคม

เครือข่ายสังคมยังเป็นสถานที่สำหรับการรวมตัวและการร่วมมือกัน นักรณรงค์ด้านสิทธิได้นำเครือข่ายสังคมมาใช้อย่างมีประสิทธิภาพในการรณรงค์ของพวกเขา เป็นที่ชัดเจนว่าเครือข่ายสังคมเหล่านี้จะอยู่กับเราไปอีกนาน เนื่องจากมีคนใช้มากขึ้นเรื่อย ๆ และมีบริการเสริมเพิ่มขึ้นเรื่อย ๆ

มีความกังวลเพิ่มขึ้นเกี่ยวกับความเป็นส่วนตัวและความปลอดภัยจากการใช้เครื่องมือและเครือข่ายเหล่านี้ มีข่าวบ่อย ๆ เกี่ยวกับการขโมยอัตลักษณ์และการขโมยข้อมูล ซึ่งทำให้เกิดความเสียหายทางการเงิน ชื่อเสียง และแม้กระทั่งความเสียหายกับร่างกาย ถ้าคุณข้องเกี่ยวกับข้อมูลหรือประเด็นอ่อนไหว คุณต้องระมัดระวังเรื่องข้อมูลส่วนตัวรั่วไหลและความไม่ปลอดภัยต่าง ๆ ที่อาจเกิดขึ้นได้จากการเชื่อมต่อกับเครือข่ายสังคม

คำแนะนำนี้จะช่วยให้คุณป้องกันตัวคุณเองและผู้อื่น และช่วยพิจารณาว่าประโยชน์จากเครือข่ายสังคมนั้น คุ้มค่ากับผลกระทบที่จะตามมาทั้งระยะสั้นและระยะยาวในเรื่องความปลอดภัยหรือไม่

ความไม่ปลอดภัย

- เครือข่ายสังคมส่วนใหญ่:
    - ให้คุณใช้บริการฟรี แต่คุณจำเป็นต้องมอบสิทธิในการใช้ข้อมูลส่วนตัวบางอย่าง ให้กับบริการเหล่านี้เสียก่อน
    - ให้คุณใช้แค่ชื่อผู้ใช้และรหัสผ่านเท่านั้น ในการเป็นมาตรการป้องกันข้อมูลส่วนตัวของคุณ ไม่ให้ถูกผู้อื่นใช้โดยไม่ได้รับอนุญาต
    - ใช้ได้ผ่านทางเบราว์เซอร์เท่านั้น ซึ่งเบราว์เซอร์เองก็มีความไม่ปลอดภัยของมันอยู่
    - ใช้งานผ่านทางอินเทอร์เน็ต ทำให้มีความเสี่ยงต่อความไม่ปลอดภัยและการโจมตีทางอินเทอร์เน็ต
- การแบ่งข้อมูลให้คนอื่น ๆ ดู เป็นหน้าที่มาตรฐานของเครือข่ายสังคม มันมักถูกมองข้าม โดยคนไม่รู้ถึงการตั้งค่าความเป็นส่วนตัวของบริการ
- เครือข่ายสังคมต่าง ๆ ก็แตกต่างกันในเรื่องการป้องกันหรือเปิดเผยข้อมูลของคุณ
- คุณไม่สามารถควบคุมได้ว่าเพื่อนคุณจะใช้ข้อมูลเกี่ยวกับคุณไปทำอะไร พวกเขาอาจแบ่งปันรูปภาพ ตำแหน่งที่อยู่ และข้อมูลอื่น ๆ ที่อาจเป็นอันตรายต่อความเป็นส่วนตัวและความปลอดภัยของคุณโดยไม่ตั้งใจ

สิ่งที่ต้องพิจารณา

- อ่านและทำความเข้าใจข้อตกลงการใช้ (End User License Agreement - EULA) เงื่อนไขการใช้ (Terms of Use) และนโยบายความเป็นส่วนตัว (Privacy Guidelines) เครือข่ายสังคมส่วนใหญ่มีเอกสารเหล่านี้อย่างน้อยหนึ่งอย่าง เอกสารเหล่านี้อาจเปลี่ยนแปลงเนื้อหาได้ในอนาคต มันจึงสำคัญที่จะต้องตรวจสอบอีกเป็นประจำ
- ควรทำความคุ้นเคยกับการตั้งค่าความเป็นส่วนตัวของบัญชีผู้ใช้เครือข่ายสังคมของคุณ อย่าเชื่อใจค่าเริ่มต้น (default) ที่ผู้ให้บริการตั้งให้คุณ ให้ปรับแต่งการตั้งค่าเพื่อให้คุณควบคุมข้อมูลของคุณเองได้ ควรตรวจสอบการตั้งค่าของคุณเป็นประจำ เนื่องจากนโยบายมักเปลี่ยนแปลงอยู่เสมอ
- ระมัดระวังในการติดตั้งโปรแกรมที่บริการเครือข่ายสังคมแนะนำให้ติดตั้ง ใช้โปรแกรมเหล่านี้ก็ต่อเมื่อคุณเชื่อใจแหล่งที่มาของมัน เข้าใจว่ามีข้อมูลอะไรบ้างของคุณที่จะถูกเปิดเผย และแน่ใจว่าคุณสามารถควบคุมการเผยแพร่ข้อมูลของคุณเองได้
- คิดให้รอบคอบก่อนจะแบ่งข้อมูลเกี่ยวกับคนอื่น ๆ ลงในเครือข่ายสังคม ถามความยินยอมเสียก่อนที่จะโพสต์ข้อมูล เอกสาร รูปภาพ และตำแหน่งที่อยู่ของบุคคลอื่น
- ให้แน่ใจว่ารหัสผ่านของคุณนั้นปลอดภัย และเปลี่ยนมันเป็นประจำ
- ระมัดระวังเมื่อใช้บัญชีผู้ใช้เครือข่ายสังคมของคุณ ตามสถานที่บริการอินเทอร์เน็ตสาธารณะ ร้านอินเทอร์เน็ตหรือร้านกาแฟที่มีอินเทอร์เน็ตไร้สาย เป็นสถานที่ยอดนิยมในการเชื่อมต่อเครือข่ายสังคม ให้ใช้เฉพาะร้านที่คุณไว้ใจเท่านั้น คุณควรลบรหัสผ่านและบันทึกการใช้อินเทอร์เน็ตของคุณ หลังการใช้เบราว์เซอร์หรือคอมพิวเตอร์ที่ใช้ร่วมกับผู้อื่น

แหล่งข้อมูลที่ช่วยคุณได้

- http://www.eff.org/deeplinks/2010/04/facebook-timeline
- http://security.ngoinabox.org/en/chapter-3
- http://security.ngoinabox.org/en/firefox_main
- http://www.eff.org/deeplinks/2010/06/encrypt-web-https-everywhere-firefox-extension

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

ใช้โทรศัพท์มือถืออย่างปลอดภัย

โทรศัพท์เคลื่อนที่ถูกใช้โดยบุคคล กลุ่ม และองค์กรต่าง ๆ ในทุกที่ กลุ่มรณรงค์และกลุ่มสิทธิมนุษยชนบางกลุ่มใช้เทคโนโลยีโทรศัพท์มือถือในวิธีใหม่ ๆ ที่สร้างสรรค์ เพื่อเตือนพิบัติภัย บริการสุขภาพ จับตาการเลือกตั้ง และอื่น ๆ บริการและโทรศัพท์มือถือส่วนใหญ่สามารถต่ออินเทอร์เน็ตได้ด้วย ทั้งนี้ขึ้นอยู่กับบริการและเครื่องที่คุณใช้ คุณอาจใช้โทรศัพท์ของคุณเพื่อดูเว็บ รับส่งอีเมล และใช้งานอินเทอร์เน็ตทั่วไป (อาจจะจำกัดอยู่สำหรับโทรศัพท์ที่มีราคาแพงสักหน่อย)

ความไม่ปลอดภัย

โทรศัพท์มือถือของคุณและข้อมูลของคุณ

โทรศัพท์มือถือส่วนใหญ่เก็บข้อมูลได้เป็นจำนวนมาก โดยเก็บไว้ในหน่วยความจำบนซิมการ์ดของโทรศัพท์ หรือการ์ดหน่วยความจำภายนอก (ในเครื่องรุ่นสูงหน่อย) คุณจะเข้าสู่ข้อมูลได้ผ่านเมนูของโทรศัพท์ ด้วยโครงสร้างเมนูที่ซับซ้อน ทำให้บางทีคุณอาจเก็บข้อมูลไว้ที่ไหนสักแห่งในโทรศัพท์ของคุณเองโดยไม่รู้ตัว

โชคไม่ดีนัก ที่ในโทรศัพท์มือถือส่วนใหญ่ คุณไม่สามารถลบข้อมูลที่อ่อนไหวหรือที่ไม่ต้องการได้ในปุ่มเดียว ตัวอย่างเช่น ถ้าจะลบหมายเลขโทรศัพท์ คุณอาจต้องเข้าไปที่สมุดโทรศัพท์ ถ้าจะลบข้อความ (เอสเอ็มเอส หรือ เอ็มเอ็มเอส) คุณอาจต้องเข้าไปที่กล่องขาเข้า (inbox) หรือกล่องขาออก (outbox)

ปัจจุบัน โทรศัพท์มือถือส่วนใหญ่ ไม่ได้เข้ารหัสข้อมูลของคุณ (ซึ่งถ้าเข้ารหัส มันจะปกป้องความเป็นส่วนตัวของคุณได้ดีที่สุด) สิ่งที่ดีที่สุดที่โทรศัพท์มือถือมีให้ขณะนี้ คือรหัสผ่านเพื่อล็อกหรือปลดล็อกเครื่องโทรศัพท์ของคุณเท่านั้น

ข้อความและเสียงสนทนาของคุณ

ปัจจุบัน อุปกรณ์และเทคโนโลยีที่ใช้ในโทรศัพท์เคลื่อนที่ (รวมทั้งข้อความเอสเอ็มเอส และการโทรคุยด้วยเสียง) นั้นไม่ปลอดภัยเท่าใดนัก อย่างน้อยที่สุด ผู้ให้บริการโทรศัพท์มือถือของคุณ สามารถเก็บข้อมูลเกี่ยวกับการใช้โทรศัพท์ของคุณได้ เช่น วันที่ เวลา ผู้รับ ผู้ส่ง ตำแหน่ง ความยาวของเอสเอ็มเอส ระยะเวลาการโทรและการเข้าสู่อินเทอร์เน็ต (ถ้าใช้ได้)

ข้อมูลเหล่านี้ปกติใช้เพื่อออกใบแจ้งค่าบริการ แต่อาจถูกนำมาใช้เพื่อคุกคามความปลอดภัยและความเป็นส่วนตัวของคุณและของเพื่อนคุณได้ด้วย ข้อความเอสเอ็มเอสสามารถถูกดักเก็บได้อย่างง่าย ๆ ในระหว่างทางที่คุณส่งหรือรับ

ข้อความและเสียงสนทนานั้นเสี่ยงต่อการถูกดักฟังและถูกบันทึก ข้อความเอสเอ็มเอสนั้นถูกส่งและรับในรูปแบบข้อความธรรมดา (plain text) หมายความว่า ใคร ๆ ก็สามาถอ่านได้ ถ้าเขาสามารถเข้าสู่โทรศัพท์ของคุณได้ หรือดักมันระหว่างทางที่ข้อความนั้นกำลังถูกส่ง

ดังนั้น ไม่เพียงแต่ผู้ให้บริการโทรศัพท์เท่านั้นที่สามารถดูเอสเอ็มเอสของคุณได้ แต่ยังมีคนอื่นที่สามารถดักข้อความนั้นได้ทางเครือข่ายโทรศัพท์มือถือ เนื่องจากมันถูกส่งผ่านเครือข่ายในรูปแบบข้อความธรรมดา

ตำแหน่งที่อยู่ของคุณ

เพื่อให้โทรศัพท์มือถือทำงานได้อย่างถูกต้อง มันจะสื่อสารอย่างต่อเนื่องกับเสาสัญญาณที่อยู่บริเวณรอบ ๆ เพื่อให้รู้แน่นอนว่าจะส่งสัญญาณไปที่ไหน เมื่อคุณเปิดเครื่องโทรศัพท์ สิ่งแรก ๆ ที่มันจะทำคือ ค้นหาสัญญาณจากผู้ให้บริการโทรศัพท์มือถือ เสาที่มีสัญญาณแรงที่สุดที่อยู่ใกล้คุณจะขึ้นทะเบียนโทรศัพท์ของคุณเข้าสู่ระบบ เพื่อที่ว่าการสื่อสารเข้าหรือออกใด ๆ จากโทรศัพท์ของคุณจะถูกดำเนินการโดยเสาต้นนั้น

เมื่อคุณเคลื่อนที่ โทรศัพท์ของคุณอาจถูกเชื่อมเข้ากับเสาสัญญาณต้นอื่นอีกต้น และตำแหน่งใหม่ของคุณ จะถูกบันทึกไว้โดยระบบ

ดังนั้น ตลอดเวลาที่โทรศัพท์ของคุณเปิดอยู่ มันจะแจ้งตำแหน่งโดยประมาณที่คุณอยู่ ให้กับเครือข่ายของผู้ให้บริการ การเดินทางของคุณจะทิ้งร่องรอยเอาไว้เช่นกัน เนื่องจากโทรศัพท์ของคุณถูก ‘เปลี่ยนมือ’ จากเสาต้นหนึ่งไปยังอีกต้นหนึ่ง ด้วยเหตุนี้ คุณ (และโทรศัพท์ของคุณ) จึงถูกเฝ้าติดตามโดยผู้ให้บริการโทรศัพท์มือถือ ทำให้เขาสามารถส่งผ่านเสียงรวมถึงข้อความเข้าและออกของคุณได้

สิ่งที่ต้องพิจารณา

- เปิดใช้รหัสผ่านหรือรหัสตัวเลข (PIN) ของโทรศัพท์
- อย่าบันทึกข้อมูลที่อ่อนไหวไว้ในโทรศัพท์ หรือถ้าจำเป็นจริง ๆ ให้บันทึกในแบบที่เข้าใจยาก มีเพียงคุณคนเดียวเท่านั้นที่เข้าใจ
- ลบข้อมูลที่อ่อนไหวหรือที่ไม่ต้องการในโทรศัพท์ของคุณอยู่เสมอ
- ระมัดระวังอยู่เสมอ ในการพกพาโทรศัพท์และการใช้โทรศัพท์ หลีกเลี่ยงการพกพาหรือใช้ในสถานที่หรือสถานการณ์ที่ดูเสี่ยงไม่น่าไว้ใจ
- ลบข้อมูลของคุณทั้งหมดทิ้ง ก่อนที่จะขายหรือนำโทรศัพท์ไปซ่อม
- ทำลายโทรศัพท์ที่เสียแล้วและซิมการ์ดเก่า ก่อนทิ้ง
- คิดให้รอบคอบก่อนใช้โทรศัพท์มือถือส่งข้อมูลที่อ่อนไหว มีทางเลือกอื่นที่ปลอดภัยกว่าหรือไม่ ?
- เมื่อทำงานกับบุคคลหรือองค์กรที่มีการส่งข้อมูลที่อ่อนไหว ควรมีโทรศัพท์และซิมการ์ดสำหรับการเรื่องงานและเรื่องส่วนตัวแยกออกจากกัน

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

ปกป้องอีเมลให้ปลอดภัย

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

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 เมื่อคุณใช้บริการอีเมล จากผู้ให้บริการอีเมลฟรี:

- ข้อมูลของคุณ (อีเมล แฟ้มแนบ และอื่น ๆ) ถูกเก็บอยู่ที่เซิร์ฟเวอร์ของผู้ให้บริการ คุณไม่สามารถควบคุมการจัดการข้อมูลของพวกเขาได้ ทำได้แค่เพียงเชื่อใจฝากข้อมูลของคุณและคนที่คุณสื่อสารด้วยไว้เท่านั้น
- ทำความเข้าใจว่าผู้ให้บริการนั้นใช้ข้อมูลของคุณหรือไม่อย่างไร (อ่านก่อนคลิกปุ่ม 'ตกลง')
- สำหรับอีเมลและการสื่อสารที่อ่อนไหวมาก กรุณาเลือกใช้ผู้ให้บริการอีเมลฟรีที่กล่าวอย่างชัดเจนว่า เขาจะรักษาความปลอดภัย และไม่ใช้/เผยข้อมูลของคุณ (ลองอ่าน http://security.ngoinabox.org/en/riseup_main)
- การสื่อสารนั้นเป็นกระบวนการสองทาง คุณต้องแน่ใจว่าผู้ที่คุณสื่อสารด้วยนั้นใช้บริการที่มีความปลอดภัยเช่นกัน อีเมลของคุณจะไม่ปลอดภัย ถ้ามีเพียงฝ่ายเดียวที่ใช้บริการที่ปลอดภัย แต่อีกฝ่ายไม่ได้ใช้

การเชื่อมต่อ: วิธีการเข้าถึงอีเมล

วิธีการที่ใช้กันมากที่สุดในการเข้าสู่อีเมลนั้นคือ ผ่านทางเว็บเบราว์เซอร์ ผู้ที่ไม่มีคอมพิวเตอร์ และอินเทอร์เน็ตใช้ สามารถเข้าสู่อีเมลได้อย่างง่ายดายผ่านทางเว็บ การเข้าถึงอีเมลด้วยวิธีนี้หมายความว่าข้อมูลเดินทางจากเซิร์ฟเวอร์ (ซึ่งข้อมูลของคุณนั้นถูกเก็บอยู่) ไปยังคุณ (ผ่านเบราว์เซอร์ของคุณ)

เบราว์เซอร์ (เช่น Internet Explorer หรือ Firefox) นั้นมีความเสี่ยงต่อการถูกโจมตีทางอินเทอร์เน็ต ดังนั้น เมื่อใช้เบราว์เซอร์เพื่ออ่านหรือส่งอีเมล เราจึงเพิ่มความเสี่ยงที่ข้อมูลของเราจะถูกเปิดเผยสู่คนอื่น

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

การส่งผ่าน: อีเมลของคุณเดินทางอย่างไร

การรักษาความปลอดภัยที่ปลายทางของทั้งสองฝ่าย ทำให้ข้อมูลปลอดภัยขึ้นได้ระดับหนึ่ง แต่ถนนระหว่างจุดหมายและปลายทางก็สำคัญไม่น้อยกว่ากัน ตามค่าเริ่มต้นแล้ว อีเมลเดินทางระหว่างเซิร์ฟเวอร์อีเมลไปยังคุณ ด้วยความปลอดภัยที่ต่ำหรือไม่มีเลย ข้อความอีเมลโดยปกติถูกส่งในรูปแบบข้อความธรรมดา ซึ่งหมายความว่า ใครก็ตามที่สามารถเข้าสู่เส้นทางการส่งผ่าน สามารถอ่านข้อความอีเมลของคุณได้ ลองพิจารณาคำแนะนำต่อไปนี้:

- ตรวจสอบ URL ของคุณ (แถบที่อยู่ในเบราว์เซอร์) เมื่อใช้บริการอีเมลฟรี ถ้าที่อยู่ขึ้นต้นด้วย http แสดงว่าการเดินทางของอีเมลคุณไม่ปลอดภัย และอีเมลของคุณเดินทางในรูปแบบข้อความธรรมดา
- อีเมลผ่านหน้าเว็บ (เช่น Yahoo! Mail) มีการเข้ารหัสเฉพาะแค่ตอนใส่ชื่อผู้ใช้และรหัสผ่านเพื่อล็อกอินเท่านั้น ขณะที่ผู้ให้บริการเจ้าอื่น (เช่น Google Mail) ใช้ https สำหรับการสื่อสารอีเมลทั้งหมดของคุณ

เนื้อหา: ข้อความที่แท้จริง

ในที่สุดแล้ว เนื้อหาของอีเมลคือสิ่งที่คุณพยายามรักษาไว้เป็นความลับ นั่นหมายความว่า จะไม่ให้ใครเห็น/เข้าสู่ข้อมูลของคุณได้ ในระหว่างที่มันเดินทางจากคุณไปยังผู้ให้บริการอีเมล อย่างไรก็ตาม:

- เมื่อคุณส่งอีเมลออกไปแล้ว คุณไม่สามารถควบคุมอีเมลดังกล่าวได้อีกต่อไป ถ้าคนที่คุณสื่อสารด้วยไม่ระมัดระวังเรื่องความปลอดภัย อีเมลและความปลอดภัยของคุณก็มีความเสี่ยงเช่นกัน
- ถ้าคุณเก็บอีเมลไว้ในเครื่องคอมพิวเตอร์ส่วนตัว คนอื่นที่อาจเข้าถึงคอมพิวเตอร์คุณได้ ก็สามารถอ่านอีเมลของคุณได้เช่นกัน

วิธีการแก้ปัญหานี้ คือการเข้ารหัส (encryption) ซึ่งเป็นหนึ่งในวิธีที่ดีที่สุดในการรักษาความปลอดภัยให้เนื้อหาอีเมล แฟ้ม หรือข้อมูลที่อ่อนไหวอื่น ๆ ของคุณ การเข้ารหัสข้อมูลคือการใช้โปรแกรมแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้

ซึ่งข้อมูลจะอ่านได้ก็ต่อเมื่อคุณใส่รหัสลับที่ใช้ถอดรหัส ดูข้อมูลเพิ่มเติมเรื่องนี้ได้ที่ : http://security.ngoinabox.org/en/chapter_7_4

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

รหัสผ่าน: การป้องกันด่านแรก

คุณมีรหัสผ่านกี่ชุด?

คุณจำมันได้หมดหรือไม่ โดยที่ไม่ต้องจด ?

คุณกลัวที่จะเปลี่ยนรหัสผ่านเพราะว่าคุณอาจลืมมันใช่หรือไม่ ?

คุณใช้เพียงรหัสผ่านเดียวกับทุกสิ่งหรือไม่ ?

รหัสผ่านที่ปลอดภัยเป็นส่วนสำคัญในการป้องกันข้อมูลของคุณทั้งออนไลน์และออฟไลน์ ด้วยบริการออนไลน์และเครือข่ายสังคมกันมากขึ้น ทำให้โอกาสในการใช้รหัสผ่านมีมากขึ้น

ทุกวันนี้ ข้อมูลของคุณไม่ได้อยู่แต่เฉพาะในเครื่องคอมพิวเตอร์ส่วนตัวและอุปกรณ์เก็บข้อมูลส่วนตัวของคุณอีกต่อไป แต่มันอยู่บนเว็บด้วย (ผ่านบริการอินเทอร์เน็ต เช่น Google Mail หรือ Facebook) ข้อมูลของคุณจึงอยู่ที่ไหนสักแห่งหนึ่งออนไลน์ และเสี่ยงต่อการถูกโจมตีทางอินเทอร์เน็ต

- จำได้ไหมว่า คุณเปลี่ยนรหัสผ่านครั้งสุดท้ายเมื่อใด ?
- คุณใช้รหัสผ่านเดียวกันกับการบริการอย่างน้อย 2 อย่างบนอินเทอร์เน็ตหรือไม่ ?
- คุณนำรหัสผ่านที่คุณเลิกใช้แล้วกลับมาใช้อีกหรือไม่ ?
- คุณเคยให้รหัสผ่านของคุณแก่คนอื่นหรือไม่ ?
- รหัสผ่านของคุณมีคำที่อยู่ในพจนานุกรมหรือข้อมูลเกี่ยวกับตัวคุณที่เป็นที่รู้กันทั่วไป (ชื่อญาติ วันเกิด ที่อยู่ และอื่น ๆ ที่คล้ายกัน) หรือไม่ ?
- คุณมีรหัสผ่านที่มีความยาว 8 ตัวอักษร หรือน้อยกว่านี้หรือไม่ ?
- คุณเคยจดรหัสผ่านไว้ในกระดาษหรือไม่ ?
- คุณเคยเข้าใช้การบริการออนไลน์ผ่านร้านอินเทอร์เน็ต ที่คุณไม่แน่ใจว่ามีมาตรการรักษาความเป็นส่วนตัวและความปลอดภัย หรือไม่ ?

เคล็ดลับ/วิธีการแก้ปัญหา:

- รหัสผ่านยิ่งยาวยิ่งดี รหัสผ่านของคุณควรยาวกว่า 20 ตัวอักษร (เช่น heer-iztwenti/twenti)
- เพื่อให้ปลอดภัยมากขึ้น ผสมคำให้ยุ่ง แทนบางตัวอักษรด้วยสัญลักษณ์หรือตัวเลข เช่น bank[gog ch@racter$ หรือ numb3rs ควรพิจารณาใช้วลีรหัสผ่านเป็นรหัสผ่านของคุณ วลีรหัสผ่านอาจมาจากชื่อหนังสือ (เช่น va dinci kode) หรือบางส่วนของเนื้อเพลง
- รหัสผ่านควรมีทั้งอักษรพิมพ์ใหญ่ อักษรพิมพ์เล็ก ตัวเลข และสัญลักษณ์ เช่น cH@r4cTer$ และ (ถ้าระบบหรือบริการออนไลน์นั้นอนุญาตให้มีได้) รหัสผ่านของคุณควรมีช่องว่าง
- รหัสผ่านไม่ควรมีคำตามพจนานุกรม และหรือข้อมูลเกี่ยวกับตัวคุณที่เป็นที่รู้กันทั่วไป เช่น หมายเลขโทรศัพท์ ชื่อสัตว์เลี้ยง ที่อยู่ และอื่น ๆ ที่คล้ายกัน
- เปลี่ยนรหัสผ่านของคุณบ่อย ๆ

- อย่าใช้รหัสผ่านเดียวกันสำหรับหลายบัญชีหรือหลายบริการอินเทอร์เน็ต
- อย่าจดรหัสผ่าน ให้ใช้วิธีการจำเท่านั้นถ้าเป็นไปได้ (คุณอาจใช้ซอฟต์แวร์จัดการรหัสผ่านได้)
- ไม่บอกรหัสผ่านของคุณให้คนอื่นทราบ
- ไม่ปล่อยให้เว็บไซต์และโปรแกรมต่าง ๆ จำรหัสผ่านของคุณ
- ตรวจสอบความปลอดภัยของร้านอินเทอร์เน็ตสาธารณะ ก่อนเข้าสู่บริการออนไลน์

แหล่งข้อมูลที่ช่วยคุณได้

- http://security.ngoinabox.org/en/chapter-3
- http://security.ngoinabox.org/en/keepass_main
- http://keepass.info/
- http://www.keepassx.org/

ใช้รหัสผ่านเดียวกันหมดกับทุกสิ่งออนไลน์ ?

> นั่นคือการเปิดทางสะดวกให้คนอื่นบุกเข้ามา

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