ความปลอดภัยในโลกไซเบอร์

life beats

lyondellbasell

โลกออนไลน์ของคุณมันเปราะบางอย่างไร?

ซอฟแวร์และแนวทางแก้ไขด้าน IT บางอย่าง ถูกนำเสนอมากมาย เพื่อวัตถุประสงค์ในการให้ข้อมูล และคุณสามารถที่จะติดตั้งมันลงบนคอมพิวเตอร์ส่วนตัวของคุณ(ไม่ใช่กับอุปกรณ์คอมพิวเตอร์ของ LyondellBasell)และมันก็เป็นความเสี่ยงของคุณ

LyondellBasell และกิจการอื่นๆ ไม่สามารถช่วยหรือรับผิดชอบกรณีใดๆ หรือความเสียหายทางกายภาคอันเนื่องมาจากอุปกรณ์และข้อมูลของคุณ

ตัวตนบนโลกออนไลน์ของคุณคือใบผ่านทางของคุณสู่การโต้ตอบกับคนนับล้านของบริการออนไลน์ตั้งแต่ E-mail มาที่งานขององค์กร, ร้านค้าออนไลน์และแม้กระทั่งโทรศัพท์มือถือ

คุณเคยคิดเกี่ยวกับความเสี่ยงของการสูญหายหรือการเปิดเผยตัวตนออนไลน์ของคุณหรือไม่?

ความเสี่ยงเกี่ยวกับ E-mail

- หากคุณมีเพียง Email หลักเดียว สำหรับทุกสิ่ง คุณจะ...
  - ทำให้ยากที่จะค้นหาระหว่าง ชื่อทางกฎหมายและอื่นๆ
  - ความล้มเหลวของการมีชื่อ email เพียงที่เดียว : หากคุณสูญเสียอันหลักไป คุณจะไม่มีแผนสำรอง
  - มีข้อบกพร่องในการป้องกันฟิชชิ่งอีเมลที่ทันสมัย

ทั้งหมดที่คุณจะทำนี้ ก็คือ การให้**Email** ของคุณใช้งานได้ดีตลอดเวลา**!**

ฟิชชิ่งคืออะไร?

ฟิชชิ่งเป็นหนึ่งในอีเมลที่พบมากที่สุดตามการโจมตีวิศวกรรมสังคม มันเป็นเทคนิคที่โจมตีไซเบอร์พยายามที่จะหลอกให้คุณในการดำเนินการหรือการเปิดเผยข้อมูล

ทำอย่างไรให้ Email ของคุณไม่อยู่ในความเสี่ยง

- กฎเหล็ก – การให้ข้อมูล Email ของคุณต่อสาธารณะมากไปเกินไป นำมาซึ่งความเสี่ยงในการได้รับ SPAM Email และ Phishing Email

- สร้างชื่อ Email ที่แตกต่างออกไป ตามสถานะการณ์และวัตถุประสงค์ในการใช้ที่ต่างกัน
  - เพื่อสื่อสารกับผู้คนทั่วไป
  - สำหรับข้อมูลการติดต่อสื่อสารต่างๆ
  - ประกาศต่างๆ
  - ซื้อขายเพียงครั้งเดียว
  - ซื้อขาย online

- เลือกลงทะเบียนสำหรับสิ่งที่เกี่ยวข้องจริงๆ เพื่อหลีกเลี่ยงข้อเสนออันสุดท้ายที่ให้คุณกรอกข้อมูลส่วนตัวของคุณ

- เมื่อไหร่ก็ตามที่มีการสมัครใช้งาน Email ใหม่ของคุณ **อย่าใช้รหัสผ่านซ้ำเหมือนกับอันอื่น ๆ ที่มี**

รหัสผ่าน – ข้อปฏิบัติเลี่ยงความเสี่ยง

- รหัสผ่าน († RIP)
  - ไม่เคยนำมาใช้งานเลย!
  - อาชญากรเรียกใช้สคริปต์สามารถตรวจสอบชื่อผู้ใช้และรหัสผ่านในหลากหลายเว็บไซต์
  - แม้ว่าคุณจะยอมรับในความเสี่ยง อะไรคือหนึ่งเดียวที่ผู้ให้บริการของคุณ ที่จะทำการ hacked ได้?
  - หากคุณเคยใช้มันในร้าน Internet Cafe, โรงแรมหรือที่เครื่องคอมพิวเตอร์ที่ใช้ร่วมกันอื่น ๆ ? มีโอกาสสูงมากที่ข้อมูลส่วนตัวและรหัสผ่านของคุณ จะตกอยู่ในมืออาชญากร

การป้องกันรหัสผ่านของคุณรั่วไหล

- **ไม่ควร , ไม่ว่าจะภายใต้สถานการณ์ใด ๆ ไม่ควรใช้รหัสผ่านคุณซ้ำกัน**

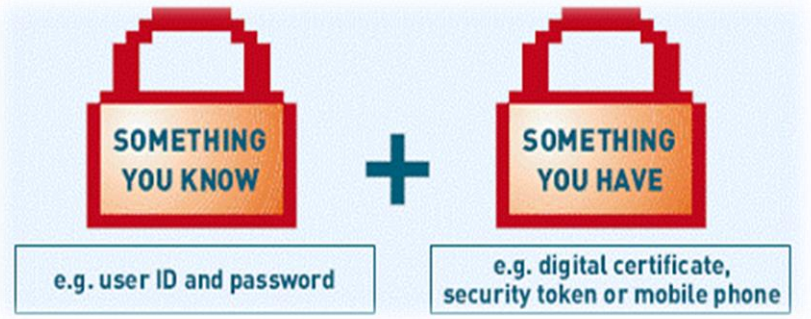
- เมื่อสมัครเพื่อรับบริการออนไลน์ **เราควรใช้แหล่งยืนยันตัวตนสำรองของเรา** (เช่น รหัสผ่านครั้งเดียว ระบบตอบรับอัตโนมัติ SMS หรือแม้กระทั่ง Email สำรองของคุณ)

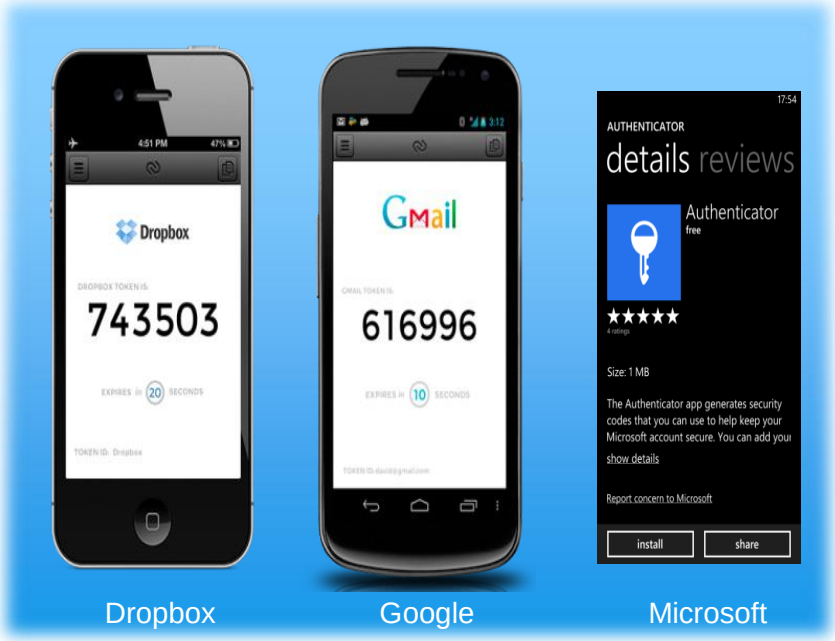
- การใช้ตัวโปรแกรมเข้ารหัสผ่านที่ดี สามารถสร้างการเข้ารหัสผ่านขั้นสูงที่มีประสิทธิภาพ และไม่ส่งมอบรหัสผ่านของคุณกลับไปทาง Internet เด็ดขาด

- หลีกเลี่ยงการออกจากหน้าจออุปกรณ์ Smartphone ของคุณโดยไม่มีการป้องกันรหัสผ่านหรือ PIN ใด ๆ

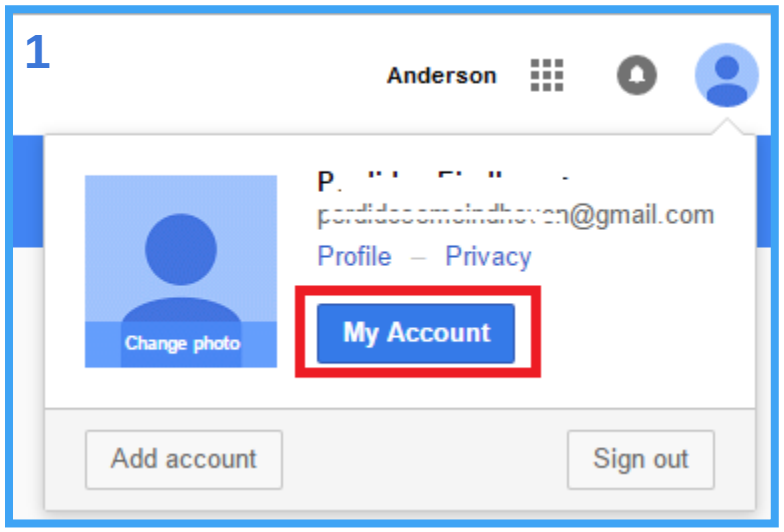
ป้องกันอีเมล์ของคุณ – เพิ่มการตรวจสอบสิทธิ์ด้วยระบบยืนยันที่ 2

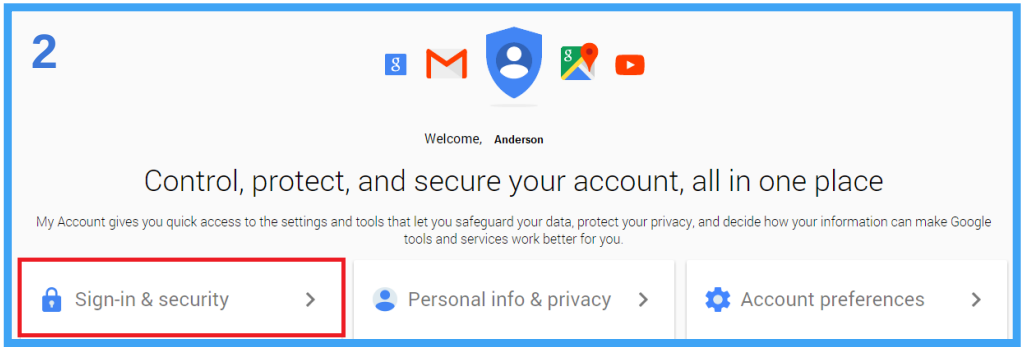
- การเข้าใช้งาน Email ของคุณบนผู้ให้บริการ โดยส่วนมากคุณจะใช้ระบบกรณียืนยันตัวตนเพียงหนึ่งเดียว ซึ่งก็มักจะเป็นอะไรที่คุณรู้อยู่แล้วเช่น รหัสผ่าน
- แน่นอนถ้าแฮ็กเกอร์ได้รับการเข้าถึงรหัสผ่านของคุณ มันเกือบจะแน่ใจว่าจะสามารถเข้าถึงอีเมลของคุณจนกว่า ... เมื่อเจอเข้ากับระบบยืนยันตัวตนเพิ่มเติมของคุณ

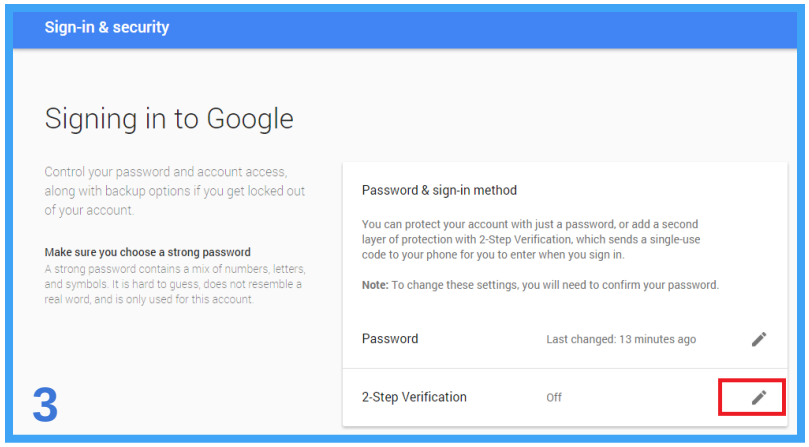


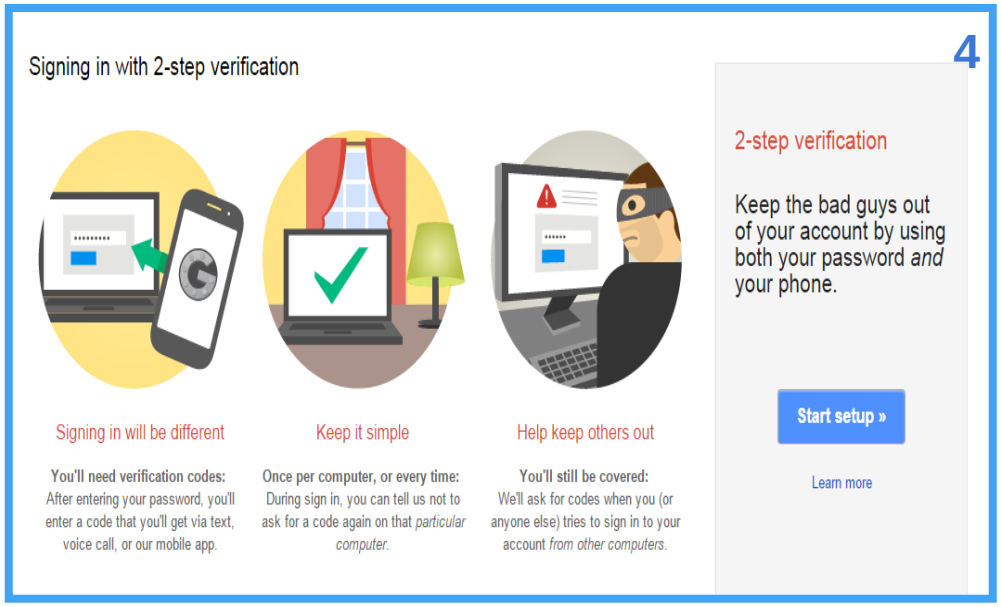


ขั้นตอนการเปิดใช้ ระบบยืนยันตัวตนที่สองบน Google

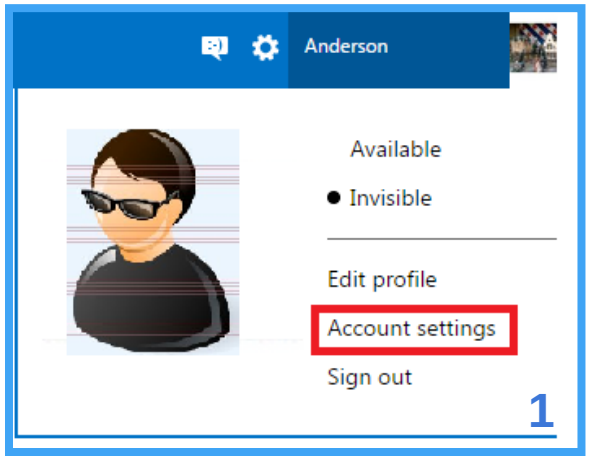


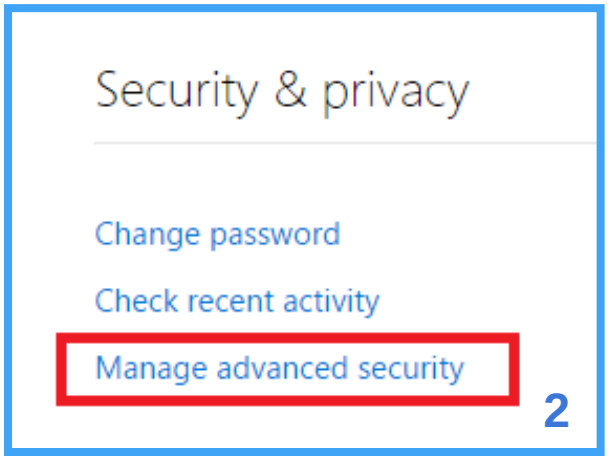


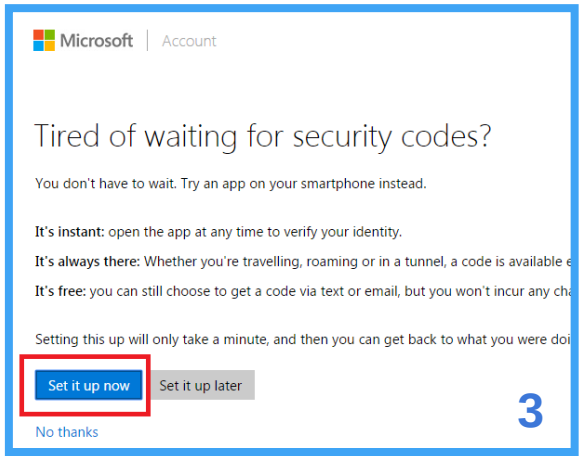


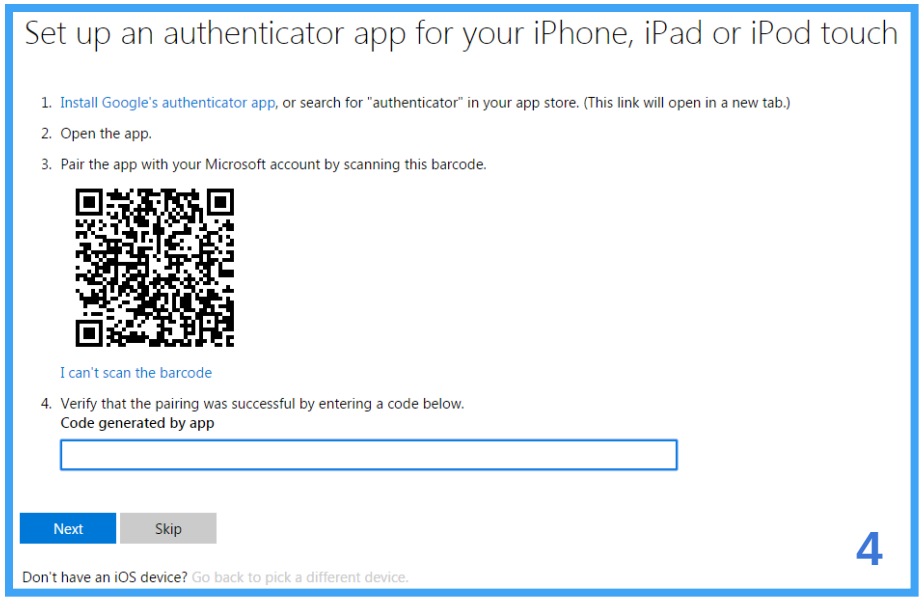


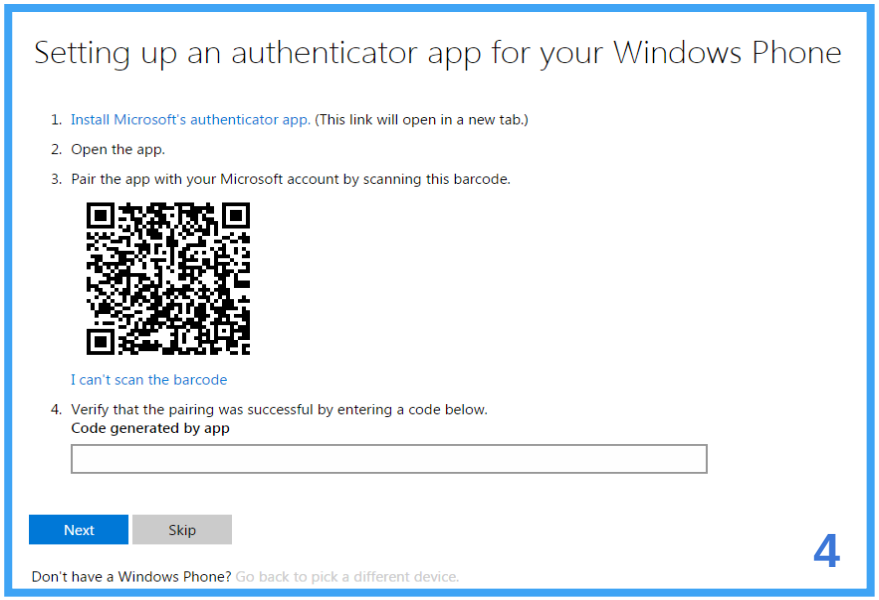
ขั้นตอนการยืนยันตัวตนที่สองของ Microsoft











คอมพิวเตอร์ที่บ้าน - ข้อปฏิบัติเลี่ยงความเสี่ยง

- เครื่องเดียวแต่ใช้กันหลายคน
  - สร้างรหัสผ่านด้วยการพิมพ์ให้ยาก ทำให้ยากต่อการเข้าถึง
  - มันเจอเข้ากับ (การละเมิดลิขสิทธิ์, การเล่นเกมและสื่อลามก) มักมีการใช้โดยอาชญากรไวรัสและ Malware
  - คุณไว้ใจเพื่อนที่ใช้งานคอมพิวเตอร์ร่วมกับคุณได้ไหม? เขาจะระวังเหมือนที่คุณทำอยู่หรือเปล่า?

- ระมัดระวังเกี่ยวกับการเชื่อต่อ อุปกรณ์สำรองข้อมูลภายนอก(Flash drive , External Harddisk) หรือ DVD Virus มักจะติดต่อผ่านอุปกรณ์เหล่านั้น ซึ่งมันเป็นวิธีการที่ใช้กันบ่อย

ใช้งานได้หลากหลายวัตถุประสงค์ กับ จำกัดการใช้งานบางอย่าง

≠

ทำอย่างไรให้คอมพิวเตอร์ของคุณไม่ตกอยู่ในความเสี่ยง

- แบ่งเรื่องงาน และ เรื่องส่วนตัว; คุณไม่สามารถใช้งานทั้งสองอย่างบนเครื่องเดียวกันได้ ซึ่งมันจะไม่ปลอดภัยเลย และเช่นกัน บนมือถือของคุณด้วย
- อย่างแบ่งบันข้อมูลของคุณบน Network ! ความผิดพลาดของคนอื่นอาจจะเป็นปัญหา ซึ่งรวมถึงคอมพิวเตอร์ในห้องประชุม ในโรงแรม และ Internet Cafe
- ซื้อระบบการป้องกันคอมพิวเตอร์ของคุณเพิ่ม (Firewall, Antivirus, AntiSpam)และเปิดใช้งานระบบป้องกันในตัวเองเพิ่มด้วย (Windows, Android, Mac OSX, or Linux XYZ) ตั้ง update อัตโนมัติ.
- หลีกเลี่ยงการดาวน์โหลดหรือซอฟต์แวร์ที่ได้รับจากแหล่งที่ไม่รู้จักหรือใช้ร่วมกันจากเพื่อนของคุณ
- หมั่น update คอมพิวเตอร์ของคุณเสมอ โดยติดตั้งผ่านระบบปฏิบัติการ และ Anti Virus ของคุณ

ความปลอดภัยโลกของไซเบอร์
มันอยู่ในมือคุณแล้ว!
เริ่มเลยวันนี้

Authored by: Anderson Domingues (LBR) & Suzanne Jurczik (LBR)