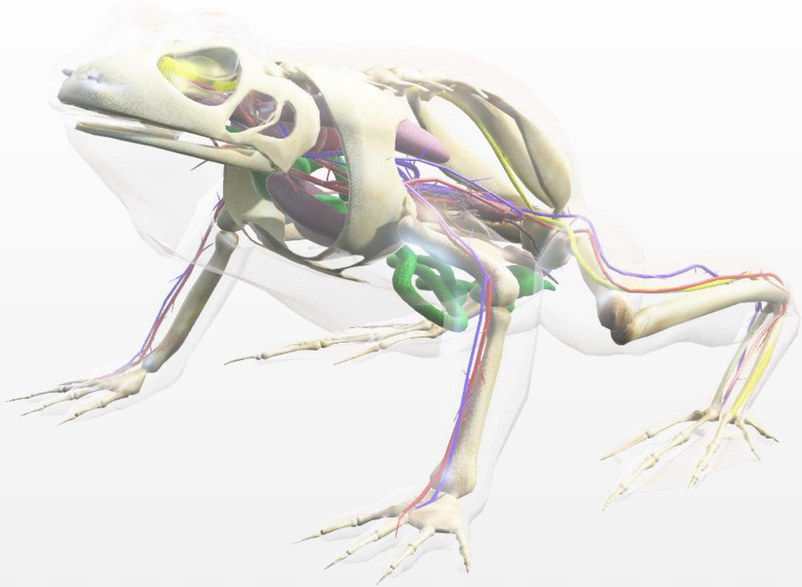
บทที่ 7: ความสำคัญของความปลอดภัย และการป้องกันข้อมูล



Part I

By Thawatwong Lawan

5 min

Lesson overview

ความปลอดภัยของการใช้งานดิจิทัลเป็นเรื่องสำคัญจำเป็นอย่างยิ่งในปัจจุบัน เนื่องจากความก้าวหน้าทางเทคโนโลยีและการสื่อสารที่เพิ่มขึ้นอย่างรวดเร็ว จนทำให้เราติดตามแทบไม่ทัน ดังนั้นหากเราไม่มีความรู้ความเข้าใจ หรือไม่ระมัดระวังในการใช้งาน อาจจะตกเป็นเหยื่อของมิจฉาชีพได้โดยง่าย ในบทนี้เราจะมาเรียนรื่องความปลอดภัย ความมั่นคงของข้อมูล ตลอดจนเรียนรู้ภัยคุกคามการใช้งานระบบดิจิทัลในรูปแบบต่างๆ และเรียนรู้วิธีการ หรือแนวทางการป้องกัน เพื่อให้การใช้งานดิจิทัลในชีวิตประจำวันมีความปลอดภัย ข้อมูลต่างๆมีความมั่นคง สามารถใช้งานระบบได้อย่างต่อเนื่อง

Learning objectives

- เพื่อให้นิสิตมีความรู้ความเข้าใจเกี่ยวกับความมั่นคงของระบบคอมพิวเตอร์
- เพื่อให้นิสิตมีความรู้ความเข้าใจเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- เพื่อให้นิสิตมามารถสำรองระบบคอมพิวเตอร์ส่วนบุคคลเพื่อป้องกันข้อมูลและโปรแกรมสำคัญ
- เพื่อให้นิสิตมีความรู้ความเข้าใจเกี่ยวกับการใช้/การกำหนดรหัสผ่านที่เหมาะสม

Keywords

Data Security, System Stability, System Threaten ,Password, OTP

Table of Contents

Activities

- ❑ ใบงาน-1
- ❑ ใบงาน-2
- ❑ ใบงาน-3
- ❑ แบบทดสอบก่อนเรียน
- ❑ แบบทดสอบหลังเรียน

https://upperrhine40.eu/en/evenements/trinational-cyber-security-days/

1. Introduction

ความมั่นคงปลอดภัย(Stability/Security) หมายถึง สถานะที่มีความปลอดภัยและได้รับการป้องกันจากภัยอันตรายต่างๆ ทั้งที่อาจจะเกิดขึ้นโดยตั้งใจหรือเกิดขึ้นโดยบังเอิญ เช่น ความมั่นคงปลอดภัยของประเทศ ย่อมเกิดขึ้นโดยมีระบบป้องกันหลายระดับ เพื่อปกป้องประเทศชาติ ผู้นำ ทรัพย์สิน ทรัพยากร และประชาชน

ความมั่นคงปลอดภัยของระบบสารสนเทศ(Information System Security) คือการป้องกันข้อมูลสารสนเทศรวมถึงองค์ประกอบอื่นๆ ที่เกี่ยวข้อง อาทิเช่น ฮาร์ดแวร์ ซอฟท์แวร์ระบบที่ใช้ในการจัดการ หรือการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้น ให้รอดพ้นจากอันตรายจากการโจมตี และอยู่ในสถานะที่มีความปลอดภัย

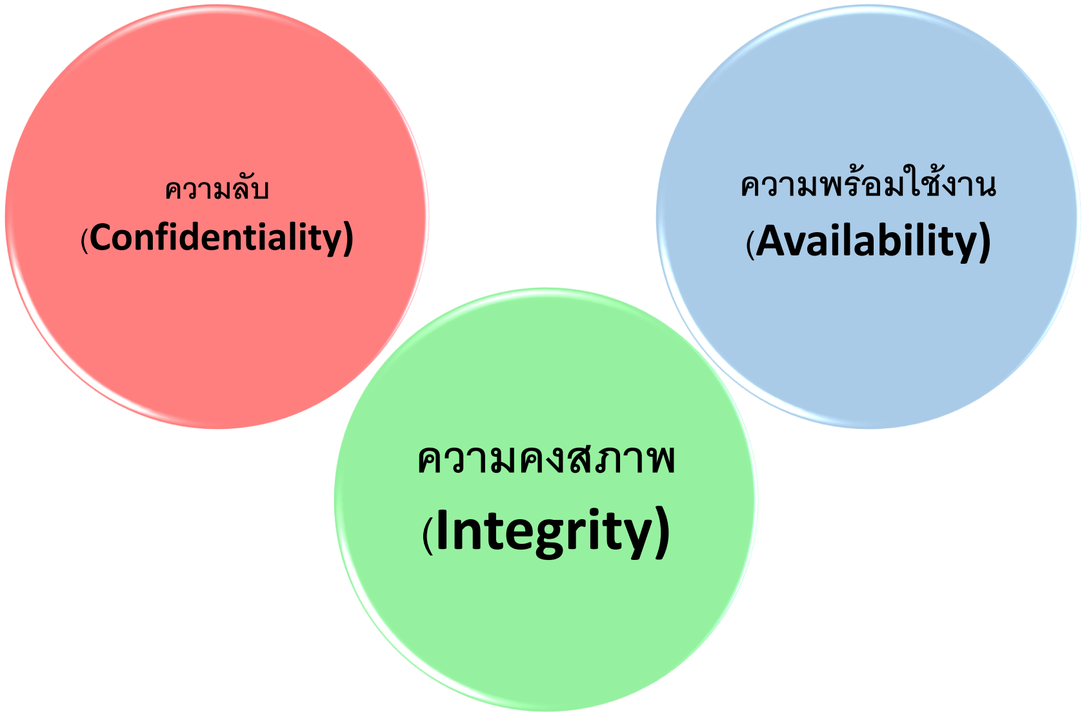
https://www.darkside.enterprises/cyber-security-crisis/

2. Cyber Security History

5 min

- การรักษาความปลอดภัยด้านกายภาพ (Physical Security)
- การรักษาความปลอดภัยด้านการสื่อสาร(Communication Security)
- การรักษาความปลอดภัยการแผ่รังสี (Emissions Security)
- การรักษาความปลอดภัยคอมพิวเตอร์(Computer Security)
- การรักษาความปลอดภัยเครือข่าย (Network Security)
- การรักษาความปลอดภัยข้อมูล (Information Security)

NSTISSC (Nation Security Telecommunications and Information Systems Security) หรือคณะกรรมการด้านความมั่นคงด้านโทรคมนาคมและระบบสารสนเทศแห่งชาติของสหรัฐอเมริกา ได้กำหนดแนวคิดความมั่นคงปลอดภัยขึ้นมาและกลายเป็นมาตรฐานการประเมินความมั่นคงของระบบสารสนเทศที่ได้รับการยอมรับ โดยหนดว่า ดำเนินงานความมั่นคงปลอดภัยของสารสนเทศนั้น มีสิ่งที่ต้องคำนึงถึงเป็นหลักได้แก่

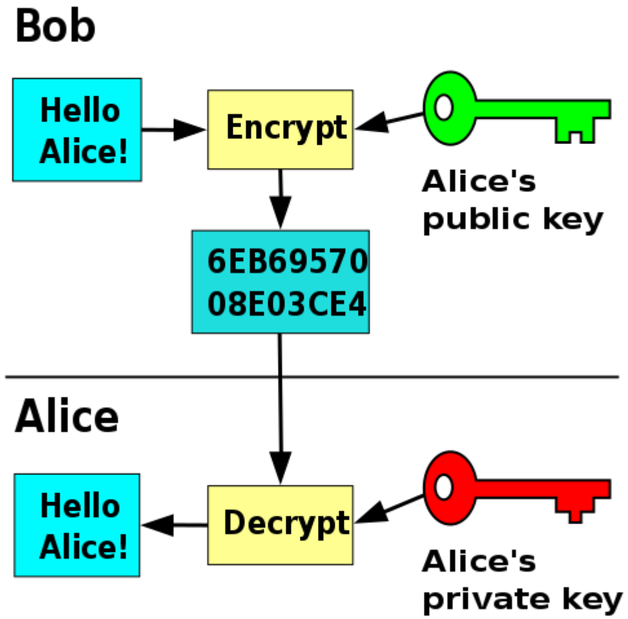


5 min

ความลับ (Confidentiality)

เนื่องจากข้อมูลบางอย่างมีความสำคัญจำเป็นต้องเก็บเป็นความลับ หากถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตราย เช่น ข้อมูลทางการทหาร ข้อมูลทางธุรกิจ เป็นต้น

การรักษาความลับ(ข้อมูล)ที่ดี คือ การเข้ารหัสข้อมูล (Cryptography or Encryption) โดยมีหลักการคือ การเปลี่ยนรูปแบบข้อมูลที่อ่านออกให้อยู่ในรูปแบบที่ไม่สามารถอ่านออกหรือเข้าใจได้ โดยมีการใช้ Key (Password) ในกระบวนการเข้ารหัสและถอดรหัส



https://commons.wikimedia.org/wiki/File:Public_key_encryption.svg

ความคงสภาพ (Integrity)

ความคงสภาพ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศจะขาดความคงสภาพเมื่อสารสนเทศนั้นถูกเปลี่ยนแปลงหรือปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ ซึ่งจะส่งผลต่อความเชื่อได้ของข้อมูลหรือแหล่งที่มา ผู้รับผิดชอบจึงต้องปกป้องข้อมูลให้คงสภาพเดิม ไม่ถูกดัดแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาตกลไกหลักที่ใช้ในการรักษาความคงสภาพ ประกอบด้วย 2 ส่วน คือ การป้องกัน (Prevention) และการตรวจสอบ (Detection)

5 min

การป้องกัน (Prevention)

เป็นการป้องกันไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต รวมถึงป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลนอกเหนือขอบเขตของผู้ได้รับอนุญาต ซึ่งอาจใช้การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) ในประเด็นแรก และใช้การตรวจสอบสิทธิ์ (Authorization)

การตรวจสอบ (Detection)

เป็นการดูว่าข้อมูลยังคงมีความน่าเชื่อถือได้อยู่หรือไม่ ซึ่งสามารถตรวจเช็ควิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นจาก Log File

5 min

ความพร้อมใช้ (Availability)

ความพร้อมใช้ หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด ความพร้อมใช้งานจัดเป็นส่วนหนึ่งของความมั่นคง ความน่าเชื่อถือ (Reliability) ของระบบ

https://www.123rf.com/photo_30193347_stock-illustration-this-illustration-concept-shows-the-choices-of-availability-the-availability-is-the-degree-to-which-.html

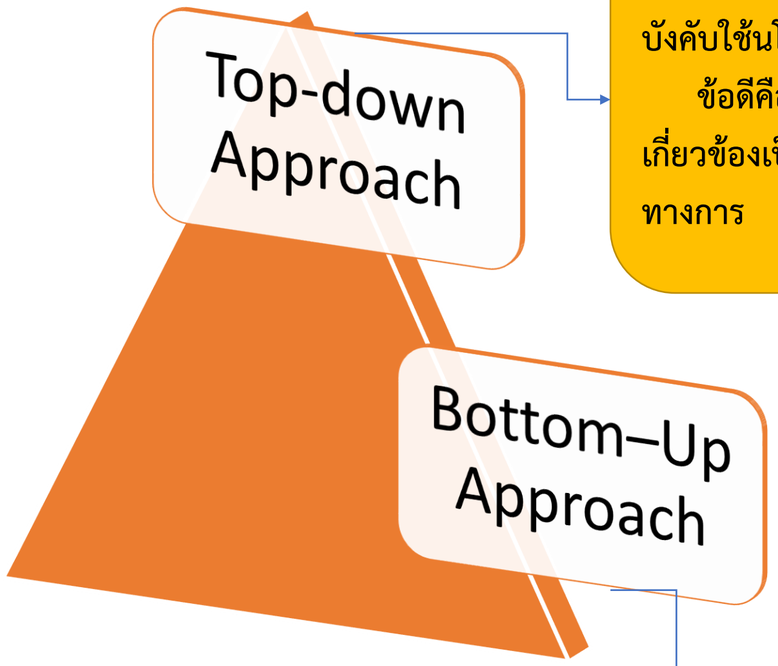
4. อุปสรรคของงานความมั่นคงปลอดภัย

10 min

- เพิ่มค่าใช้จ่าย เพื่อรักษาความปลอดภัยต้องมีการติดตั้งอุปกรณ์หรือเครื่องมือรักษาความปลอดภัย
- ความไม่สะดวก เช่น เสียเวลาในการป้อนรหัสผ่าน หรือต้องผ่านกระบวนการอื่น ๆ ในการพิสูจน์ตัวตน
- เพิ่มความซับซ้อนของระบบ ยิ่งมีความมั่นคงปลอดภัยเพิ่มขึ้น ระบบก็ต้องมีความซับซ้อนมากขึ้น
- ผู้ใช้ส่วนใหญ่ขาดความรู้ และไม่ใส่ใจเรื่องความมั่นคงปลอดภัยของสารสนเทศอย่างจริงจัง
- การพัฒนาซอฟต์แวร์ส่วนใหญ่คำนึงถึงฟังก์ชันการใช้งานเป็นหลัก เรื่องความปลอดภัยมักถูกตามมาปรับปรุงในภายหลัง
- มีการเข้าถึงข้อมูลได้จากทุกสถานที่ เป็นการเปิดทางให้ผู้อื่นเข้าถึงอุปกรณ์ของตนเองอย่างคาดไม่ถึง
- มิจฉาชีพมีความเชี่ยวชาญในการเจาะข้อมูลของผู้อื่น
- ฝ่ายบริหารมักจะไม่ให้ความสำคัญแก่ความมั่นคงปลอดภัยเท่าที่ควร

5.แนวทางในการดำเนินงานความมั่นคงปลอดภัย

10 min



การดำเนินงานความมั่นคงปลอดภัยจะเริ่มต้นโดยผู้บริหารหรือผู้มีอำนาจหน้าที่โดยตรง ซึ่งสามารถบังคับใช้นโยบาย และกำหนดบุคลากรที่รับผิดชอบได้เต็มที่

ข้อดีคือ สามารถดำเนินงานกระบวนการมั่นคงได้อย่างเต็มที่ เนื่องจากได้รับการสนับสนุนจากผู้ที่เกี่ยวข้องเป็นอย่างดี มีการวางแผน กำหนดเป้าหมาย และกระบวนการทำงานอย่างชัดเจนและเป็นทางการ

เป็นแนวทางที่ผู้ดูแลระบบหรือเจ้าหน้าที่ที่รับผิดชอบด้านความมั่นคงปลอดภัยโดยตรงเป็นผู้ริเริ่มหรือกำหนดมาตรการรักษาความปลอดภัยขึ้นมาระหว่างการพัฒนาระบบ

ข้อดีคือ เจ้าหน้าที่จะสามารถดูแลงานด้วยตนเองในทุก ๆ วัน และใช้ความรู้ความสามารถความเชี่ยวชาญที่มีการปรับปรุงกลไกควบคุมความปลอดภัยให้มีประสิทธิภาพอย่างเต็มที่

ข้อเสีย คือ มักจะขาดการสนับสนุนจากผู้เกี่ยวข้อง หรือขาดอำนาจหน้าที่ในการสั่งการ

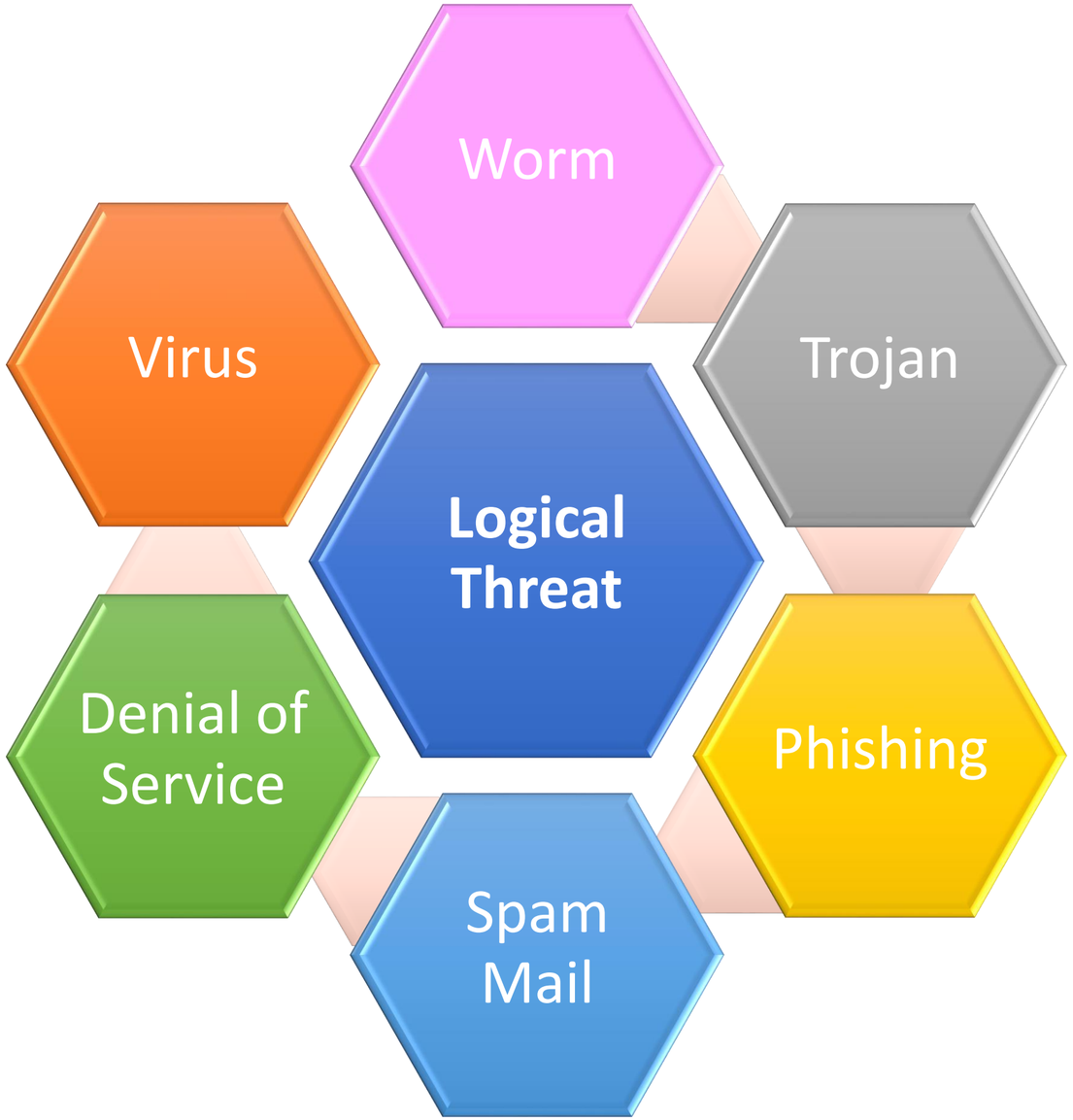
6.ภัยคุกคาม (Threat)

1.ภัยคุกคามทางกายภาพ (Physical Threat) เป็นลักษณะภัยคุกคามที่เกิดขึ้นกับฮาร์ดแวร์ที่ใช้ในระบบคอมพิวเตอร์และระบบเครือข่าย เช่น ฮาร์ดดิสก์เสีย หรือทำงานผิดพลาด โดยอาจเกิดจากภัยธรรมชาติเช่น น้ำท่วม ไฟไหม้ ฟ้าผ่า เป็นต้น แต่ในบางครั้งอาจเกิดจากการกระทำของมนุษย์ด้วยเจตนาหรือไม่เจตนาก็ตาม

2.ภัยคุกคามทางตรรกะ (Logical Threat) เป็นลักษณะภัยคุกคามที่เกิดขึ้นกับข้อมูลหรือสารสนเทศ หรือการใช้ทรัพยากรของระบบ เช่น การแอบลักลอบใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตการขัดขวางไม่ให้คอมพิวเตอร์ทำงานได้ตามปกติ การปรับเปลี่ยนข้อมูลหรือสารสนเทศโดยไม่ได้รับอนุญาต เป็นต้น

https://economictimes.indiatimes.com/industry/services/education/education-sector-worst-hit-by-cyber-threats-from-july-sept-seqrite/articleshow/72039698.cms?from=mdr

6.ภัยคุกคาม (Threat)-ภัยคุกคามทางตรรกะ (Logical Threat)



7. การรักษาความปลอดภัยข้อมูลส่วนบุคคล

10 min

8. Summary

5 min

การรักษาความปลอดภัยสารสนเทศ /ข้อมูลส่วนบุคคล เป็นเรื่องที่มีความสำคัญ จำเป็นที่ทุกๆคนจะต้องให้ความสำคัญและใส่ใจ เป็นพิเศษ เพราะหากเกิดเหตุการณ์ที่ไม่พึงประสงค์เกิดขึ้น อาจจะก่อให้เกิดความเสียหายทั้งชีวิตและทรัพย์สิน อย่างหลีกเลี่ยงไม่ได้

Part 2: Password

By Somnuk Puangpronpitag

https://isan.msu.ac.th

E-mail: somnuk.p (at) msu.ac.th

Bad passwords

- Running number eg., 123456
- Too famous : Abc123, iloveyou
- Running keyboard : Qwerty, asdfg
- All numbers (ใช้ตัวเลขทั้งหมด)
- All letters (ใช้ตัวอักษรทั้งหมด)
- Dictionary words (ใช้ศัพท์ในพจนานุกรม)

The 2019 Worst Password

Good Password

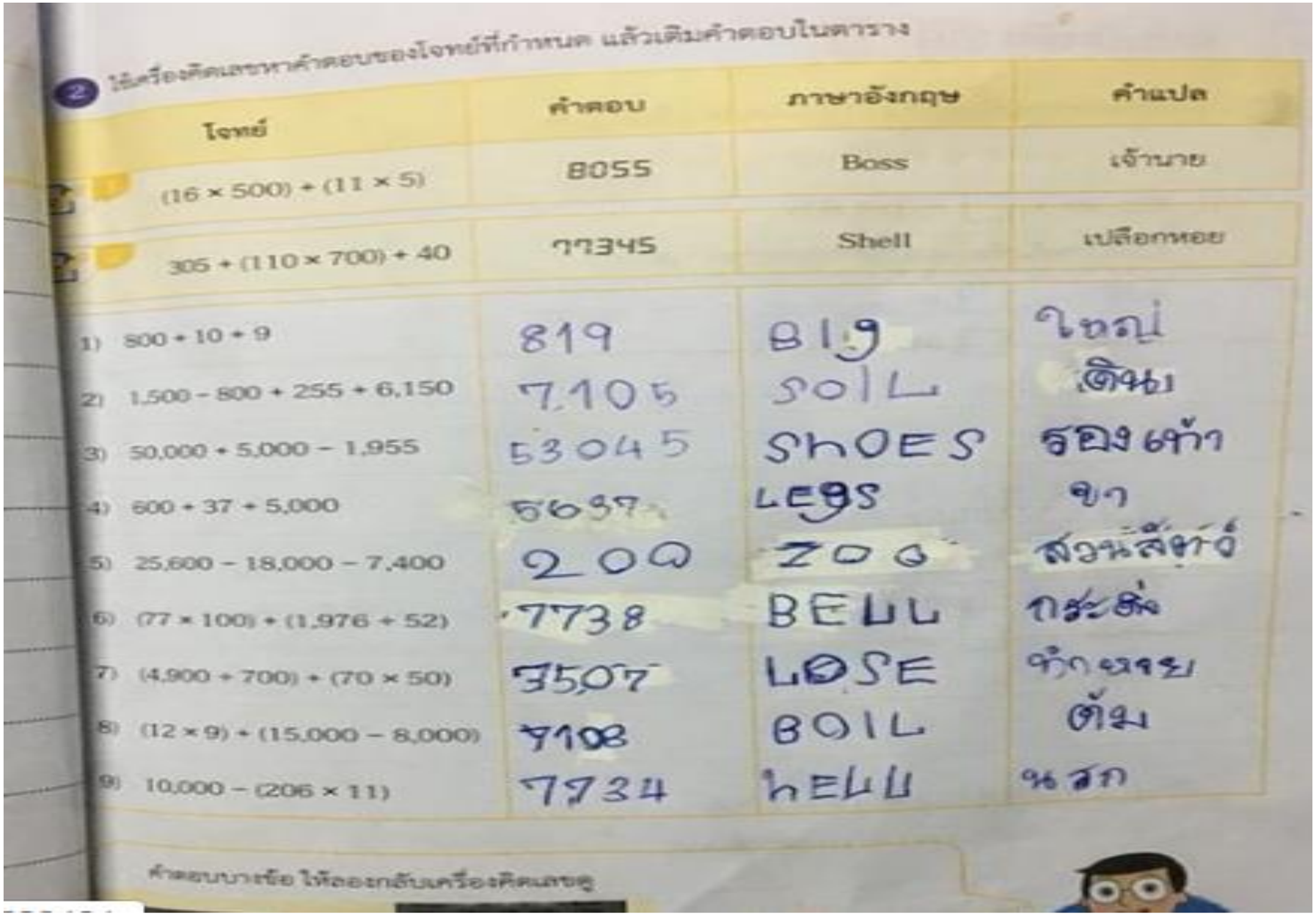
- At least 8 characters long
- Include numbers, symbol, capital and non-capital letters
  - บางระบบไม่ให้ใส่ symbol ทำไม? ดีหรือไม่?
  - บางระบบไม่สน Capital หรือ Non-capital letters
    บางระบบสนใจ เป็น Case Sensitive และบังคับให้ผสมตัวเล็กใหญ่ อะไรดีกว่ากัน?
- Varying to systems (ไม่ใช้รหัสซ้ำกันระหว่างระบบ)
  - Ref system ที่ใช้ reset รหัสระบบอื่น เช่น รหัส e-mail จะต้อง
    - ตั้งให้ดี + 2FA
- Password that you can remember

ตัวอย่าง Good Password

- Thai over English keyboard
- ใช้ Leet
  - 3^07
  - B4
  - แต่บางตัวก็ไม่ดี เช่น P@55w0rd แม้ดูเนียน

บางตัวเหมือนดีแต่ไม่ดี

- P@55w0rd แม้ดูเนียน
  - แต่เป็นรูปแบบที่ Hacker รู้
- **ji32k7au4a83 ดูเหมือนจะเป็นรหัสที่ดี**
  - **เพราะมี** ตัวอักษรผสมกับตัวเลขและอักขระพิเศษ
  - **แพร่หลายในจีน ไต้หวัน ฮ่องกง สิงค์โปร์**
  - **แต่จริง ๆ แล้วเป็นรหัสที่ไม่ดี Hacker เดารหัสนี้ได้ !**
  - **เพราะ**
    ji32k7au4a83 ในแป้นพิมพ์ภาษาอังกฤษ
    ตรงกับ 我的密碼 ในแป้นภาษาจีน (Zhuyin keyboard)
    ซึ่งแปลว่า “รหัสผ่านของฉัน”



2 ใช้เครื่องคิดเลขหาคำตอบของโจทย์ที่กำหนด แล้วเติมคำตอบในตาราง

โจทย์	คำตอบ	ภาษาอังกฤษ	คำแปล
(16 × 500) + (11 × 5)	8055	Boss	เจ้านาย
305 + (110 × 700) + 40	77345	Shell	เปลือกหอย
1) 800 + 10 + 9	819	BIG	ใหญ่
2) 1,500 − 800 + 255 + 6,150	7,105	SOIL	ดิน
3) 50,000 + 5,000 − 1,955	53045	SHOES	รองเท้า
4) 600 + 37 + 5,000	5637	LEGS	ขา
5) 25,600 − 18,000 − 7,400	200	ZOO	สวนสัตว์
6) (77 × 100) + (1,976 ÷ 52)	7738	BELL	กระดิ่ง
7) (4,900 ÷ 700) + (70 × 50)	3507	LOSE	ทำแพ้
8) (12 × 9) + (15,000 − 8,000)	7108	BOIL	ต้ม
9) 10,000 − (206 × 11)	7734	HELL	นรก

คำตอบบางข้อ ให้ลองกลับเครื่องคิดเลขดู

หัวใจหลักของ Good Password

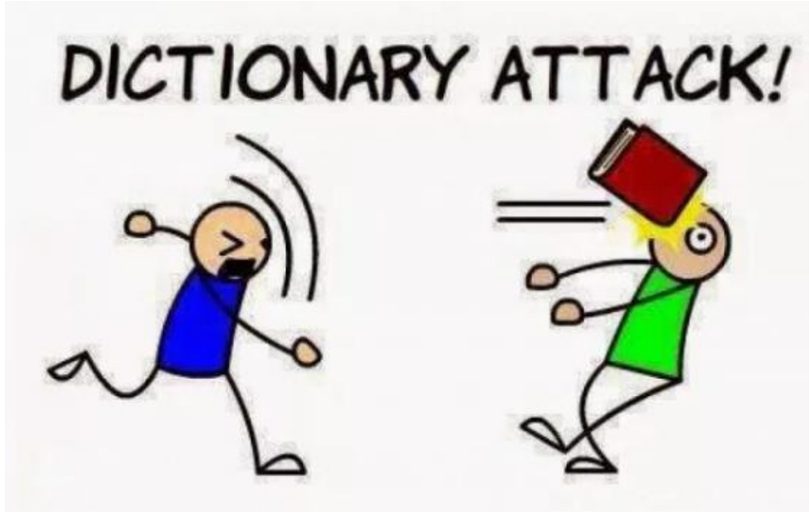
- กำหนด รูปแบบ เฉพาะที่ตนจะจำได้
- ไม่ใช้รูปแบบ ที่ Hacker รู้แล้ว หรือจะเดาได้

พวกเราคิดว่าอะไรคือหลักการตั้งรหัสที่ดี
ที่อยากแนะนำเพิ่มเติม?

Password Practices

- Use good password.
  - Check รหัสผ่านที่ Hacker ได้ของคนอื่นมา หากซ้ำไม่ใช้
  - ไม่งั้น โดน dictionary attack
- Never give password to anyone.
- Don’t just use one password for all systems.
- Don’t post it in plaintext.
  - Master key and password safer
  - ใช้ Words/Excels ช่วยเก็บ รหัสแบบปลอดภัย ทำไง? จดยังไง?
- Change it when not sure
  - Iphone ตกส้วม ส่งซ่อม
  - ใช้ WiFi นอกสถานที่

Dictionary attack



- a type of Brute-Force attack
- ใช่การเดารหัสจาก dictionary ที่ใช้เรียนภาษาอังกฤษไม๊?

- 10 million password list

  https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt

- 14 million password list

  https://sinister.ly/Thread-14-Million-Password-List

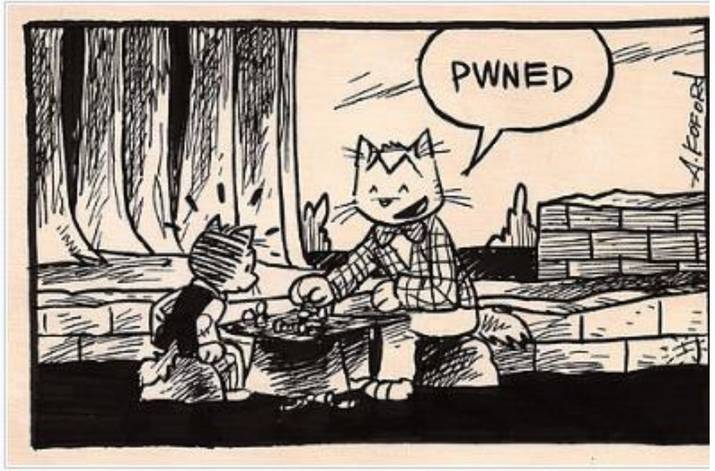
pwned

- เป็น Slang และเป็น leet (หรือ leetspeak)
- Pwn เป็น Verb
  - Be Pwned (passive voice)
  - To Pwn (active voice)
  - Pwnage เป็น Noun
- ที่มา
  - มาจาก “Owned”
  - Slang จาก Keyboarding Error หรือ typo error
  - เหมือน “เมพขิงๆ” มาจาก “เทพจิงๆ”
  - จุดเริ่ม “Warcraft” online game คำว่า owned ถูกสะกดผิดใน map นึง

ความหมายของ Pwned

- แปลตรงๆ
  - **Pwned** หรือ **Owned** แปลว่า **defeated** พ่ายแพ้ปราชัย
  - **Pwn** ก็คือ ชนะ ยึดได้
  - **Pwnage** ชัยชนะ การเข้ายึดสำเร็จ

ความหมายของ Pwned (2)



An example of the term in a *Laugh-Out-Loud Cats* comic strip

- ถูกใช้บ่อยใน
  - Online games และเกมหมากรุก
    - เวลาถูกยึดป้อม (pwned) หรือตีป้อมได้ (pwn)
    - "That was total pwnage! We crushed that boss monster!“
  - IT Security เวลาถูกยึดฐานข้อมูลผู้ใช้ หรือยึดฐานข้อมูลผู้ใช้ได้
    - If you're a victim of a data breach, you've been pwned.

เวลาจะบอกว่าระบบโดนแฮก

- The system has been compromised.
- The system has been pwned.
- The system has been controlled by a hacker.
- The system has been hacked.

ระบบถูก pwned และเสีย database ของรหัสผ่าน

- ระบบถูก Pwned
  - ระบบถูกยึดครอง ฐานข้อมูลผู้ใช้และรหัสผ่าน
- Cases
  - linkedIn (2012) – 6.5 million (2012) – 117 million (2016) user accounts
  - Dropbox (2012, 2016) – 68 million user accounts, leaked 2012, confirmed in 2016
  - Yahoo (2014, 2016) – 500 million user accounts (leaked since 2014)
  - Quora (2018) – 100 million user accounts

LinedIn (hacked 2012, selling 2016)

Dropbox (leaked 2012, confirmed 2016)

The Dropbox hack is real

31 AUGUST 2016

Earlier today, Motherboard reported on what had been rumoured for some time, namely that Dropbox had been hacked. Not just a little bit hacked and not in that "someone has cobbled together a list of credentials that work on Dropbox" hacked either, but *proper* hacked to the tune of 68 million records.

Very shortly after, a supporter of Have I been pwned (HIBP) sent over the data which once unzipped, looked like this:

https://www.facebook.com/174246142644437/photos/a.398675263534856/1112557505479958/?type=3&theater

1) คนที่ใช้ password dropbox ตัวเอง เหมือนระบบอื่นๆ ที่ใช้อยู่
ก็เปลี่ยนระบบอื่นๆ ซะครับ

2) หากโดน 1) ก็จำไว้ว่า
คราวหลัง อย่า set password แต่ละระบบเหมือนกัน ....
แต่ ... ต้องมี trick ในการ set ให้ต่าง
และที่สำคัญ ... มี trick ที่จะจำให้ได้ด้วยนะครับ

3) คนไม่ยอม set Two-Step Verification ให้ใช้ OTP อีกชั้น
กับระบบที่ set ได้อย่าง dropbox, gmail, facebook และอื่นๆ
.... นี่ ก็ควร set ซะนะครับ

ข้อสังเกตทางเทคนิค จากข่าวคือ
Salted Hash Password ที่ salt อยู่ในกองเดียวกับ password database (dump) นี่ไม่มีประโยชน์อะไร โดน crack ออกมาได้เหมือนเดิม แม้มีการเข้ารหัสซ้ำด้วย bcrypt

เหอะๆ ....คนออกแบบวิธีการ salted hash password ต้องทบทวน และคิดอะไรดีๆ ลึกๆ กว่าเดิมซะแล้ว หากจะสะกัดพวก password cracker เวลามันล้วงเอา user profile database เราไปได้

อ่านรายละเอียดเพิ่มเติม ที่ http://www.theregister.co.uk/2016/08/31/dropbox_2012_credentials_file_is_real/

Write a comment...

CNN Money International + Markets Economy Companies Tech Autos Video stock

Yahoo says 500 million accounts stolen

by Seth Fiegerman @sfiegerman

September 22, 2016: 11:30 PM ET

Recommend 13K

Social Surge - What's T


Disr
Moa
racis

Mas
glob
emp


Forg
mov
big

ISAN FANPAGE

Published by Somnuk Puangpronpitag [?]
· September 23, 2016 · Edited ·

Yahoo โดน pwned (โดนยึดฐานข้อมูลผู้ใช้และรหัสผ่าน) ไปเรียบร้อยครับ
อีกราย ตาม linkedIn, dropbox และเจ้าอื่นๆ ไปติดๆ

แต่งานนี้สาหัส เพราะ
500 million user accounts โดน ...มหาศาลมาก
งานนี้ ได้ฐาน password สำหรับทดลองเดาอีกมหาศาล
เชื่อว่า น่าจะมีปัญหา รั่วมาตั้งแต่ ค.ศ. 2014
ข้อสังเกตคือ บริษัท Verizon ตกลงจะซื้อ Yahoo ด้วยราคา $4.83 พันล้านเมื่อ เดือน กรกฎาคม ไม่กี่วันก่อน ข่าวการโดน pwned ครั้งนี้ จะถูกเปิดเผย
มีการสงสัยกันว่า yahoo พยายามจะปิดบังปัญหานี้ เพื่อไม่ให้เสียราคา

ข้อมูลที่รั่วไปคือ names, email addresses, telephone numbers, dates of birth, hashed passwords (ส่วนใหญ่โดน bcrypt ไว้) และ คำถามและคำตอบกันลืม

ข้อแนะนำ และบทเรียน สำหรับ ผู้ใช้ทั่วไป
1) ผู้ใช้ yahoo mail ให้เปลี่ยนรหัสผ่าน และคำถามคำตอบกันลืม

2) คนที่ ทะลึ่ง ตั้ง password ระบบอื่น เหมือน yahoo mail ของตน ก็ต้องเปลี่ยนซะนะครับ ให้ดี อย่าตั้ง password ระบบสำคัญๆ ซ้ำกัน เหมือนกัน

3) ระบบพวกนี้ มันท่า การยืนยันตัวตนสองชั้นได้ ผู้ใช้ควร set ด้วยครับ เผื่อ password รั่ว ก็ยังมีอีกด่าน นอกจาก yahoo mail คนที่ใช้ gmail และ facebook แนะนำว่า

Write a comment...

Quora Gets Hacked – 100 Million Users Data Stolen

December 03, 2018 Swati Khandelwal

The World's most popular question-and-answer website **Quora** has suffered a massive data breach with unknown hackers gaining unauthorized access to potentially sensitive personal information of about 100 million of its users.

ISAN FANPAGE
Published by Somnuk Puangpronpitag [?]
· December 4, 2018 ·

อีกแล้ว โดน pwned เรียบร้อย
งานนี้ Quora ฐานข้อมูล username/password
โดนไปอีก 100 ล้าน users
รู้ว่าโดนไปเมื่อ ศุกร์ 30 Nov 2018
ประกาศยอมรับเป็นทางการ เมื่อ 3 Dec 2018

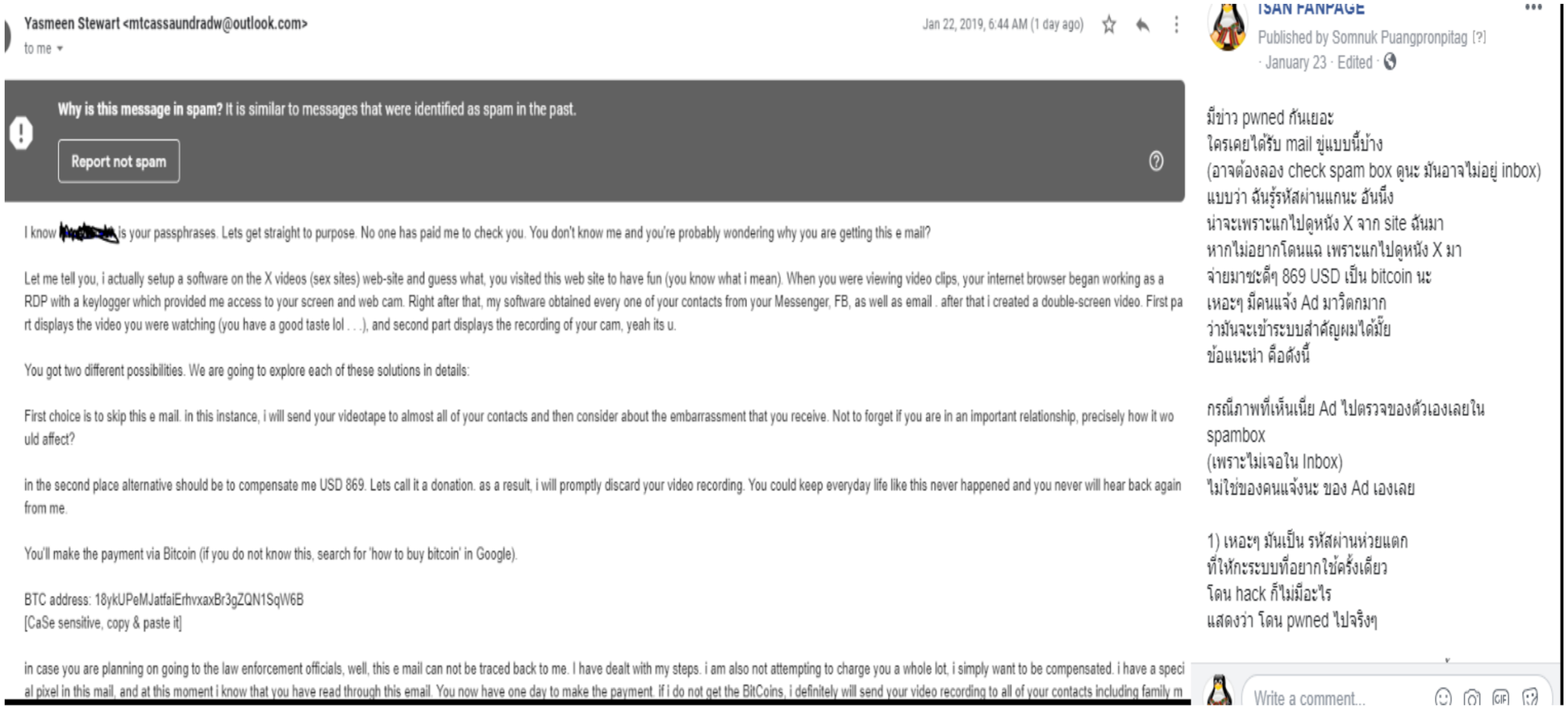
Hacker เอาไปแกะ
ก็มีรหัส 100 ล้าน พวกนี้ไว้ใช้ ประกอบ dictionary attack
เหมือน linkedIn, yahoo และอื่นๆ โดน

*** บทเรียนสำคัญ อีกที ***
อย่าตั้งรหัสผ่านระบบต่างๆ ซ้ำกัน
เพราะหากระบบหนึ่งโดนเจาะเข้า
รหัสผ่านอาจตกในมือ Hacker
แม้ระบบจะเก็บข้อมูลในรูปแบบ Hash
ก็มีทาง brute-force หาจนเจอ

จากกรณี รหัสผ่านว่า "dadada"
ของเฮีย Mark Zuckerberg ใช่ไหม
ที่หลุดจากการที่รหัสผ่าน 170 ล้าน username
ของ linkedIn โดน pwned
แม้ รหัสจะถูกเก็บเป็น SHA-1 hashed password
ก็โดน chosen-plain-text attack สำเร็จ
และรู้รหัสผ่าน

Write a comment...

Pay me! I Know your PASSWORD! (2019)



Yasmeen Stewart <mtcassaundradw@outlook.com>
to me

Jan 22, 2019, 6:44 AM (1 day ago)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

I know [redacted] is your passphrases. Lets get straight to purpose. No one has paid me to check you. You don't know me and you're probably wondering why you are getting this e mail?

Let me tell you, i actually setup a software on the X videos (sex sites) web-site and guess what, you visited this web site to have fun (you know what i mean). When you were viewing video clips, your internet browser began working as a RDP with a keylogger which provided me access to your screen and web cam. Right after that, my software obtained every one of your contacts from your Messenger, FB, as well as email . after that i created a double-screen video. First pa rt displays the video you were watching (you have a good taste lol . . .), and second part displays the recording of your cam, yeah its u.

You got two different possibilities. We are going to explore each of these solutions in details:

First choice is to skip this e mail. in this instance, i will send your videotape to almost all of your contacts and then consider about the embarrassment that you receive. Not to forget if you are in an important relationship, precisely how it wo uld affect?

in the second place alternative should be to compensate me USD 869. Lets call it a donation. as a result, i will promptly discard your video recording. You could keep everyday life like this never happened and you never will hear back again from me.

You'll make the payment via Bitcoin (if you do not know this, search for 'how to buy bitcoin' in Google).

BTC address: 18ykUPeMJatfaiErhvxaxBr3gZQN1SqW6B
[CaSe sensitive, copy & paste it]

in case you are planning on going to the law enforcement officials, well, this e mail can not be traced back to me. I have dealt with my steps. i am also not attempting to charge you a whole lot, i simply want to be compensated. i have a speci al pixel in this mail, and at this moment i know that you have read through this email. You now have one day to make the payment. if i do not get the BitCoins, i definitely will send your video recording to all of your contacts including family m

ISAN FANPAGE
Published by Somnuk Puangpronpitag [?]
· January 23 · Edited ·

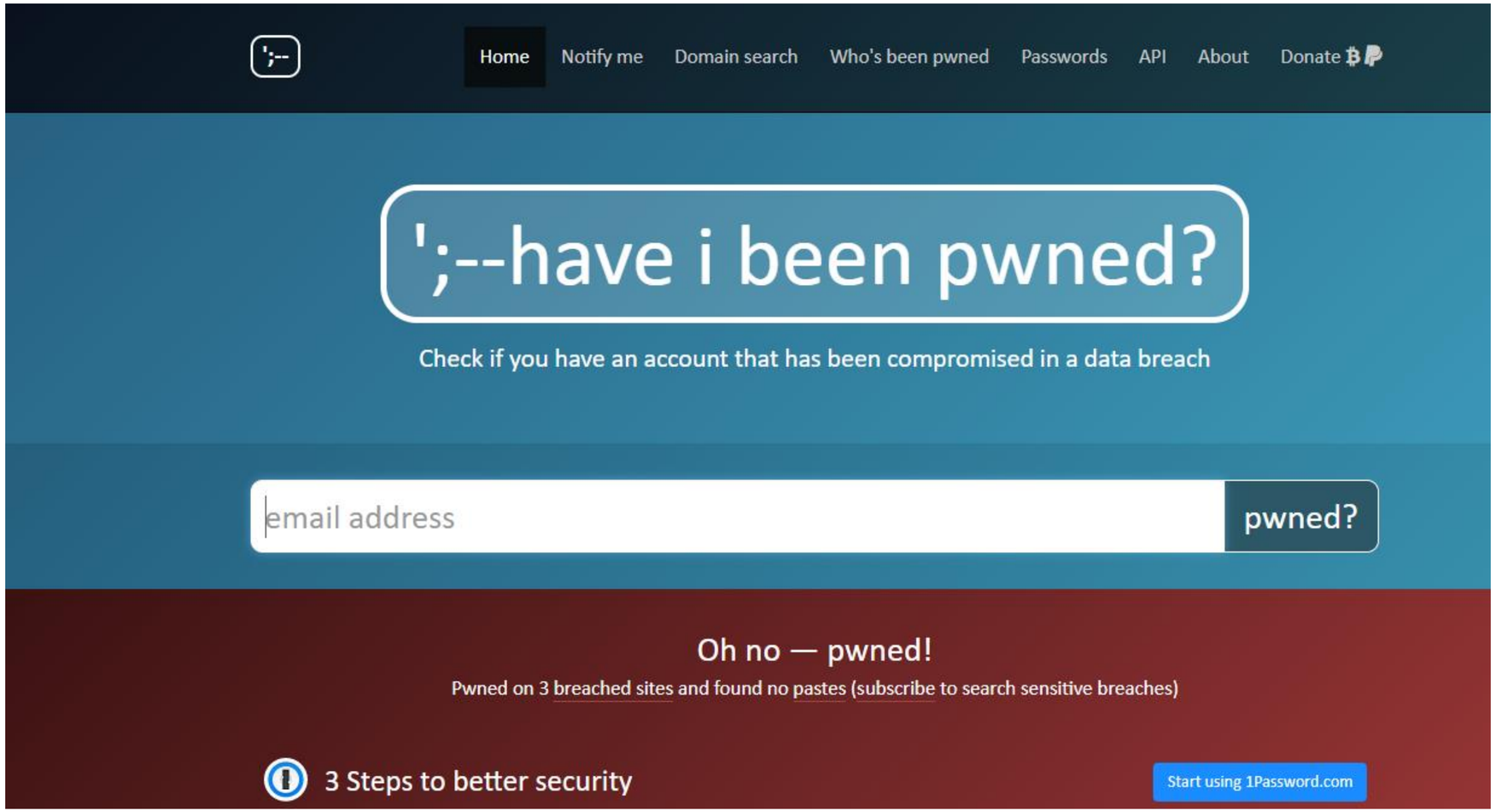
มีข่าว pwned กันเยอะ
ใครเคยได้รับ mail ขู่แบบนี้บ้าง
(อาจต้องลอง check spam box ดูนะ มันอาจไม่อยู่ inbox)
แบบว่า ฉันรู้รหัสผ่านแกนะ อันนึง
น่าจะเพราะแกไปดูหนัง X จาก site ฉันมา
หากไม่อยากโดนแฉ เพราะแกไปดูหนัง X มา
จ่ายมาซะดีๆ 869 USD เป็น bitcoin นะ
เหอะๆ มีคนแจ้ง Ad มาวิตกมาก
ว่ามันจะเข้าระบบสำคัญผมได้มั้ย
ข้อแนะนำ คือดังนี้

กรณีภาพที่เห็นเนี่ย Ad ไปตรวจของตัวเองเลยใน spambox
(เพราะไม่เจอใน Inbox)
ไม่ใช่ของคนแจ้งนะ ของ Ad เองเลย

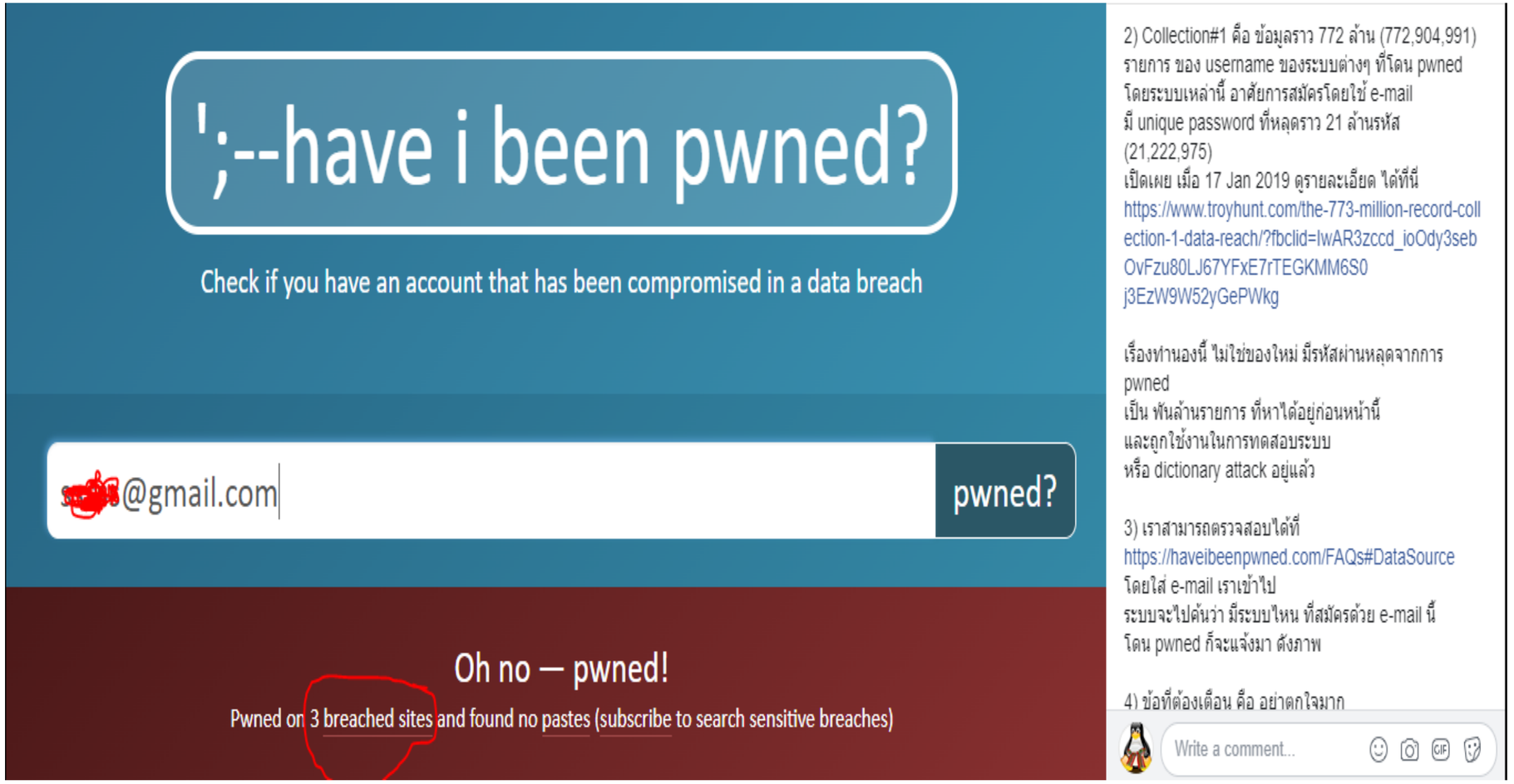
1) เหอะๆ มันเป็น รหัสผ่านห่วยแตก
ที่ให้กะระบบที่อยากใช้ครั้งเดียว
โดน hack ก็ไม่มีอะไร
แสดงว่า โดน pwned ไปจริงๆ

Write a comment...

HIBP (2019)


Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Oh no — pwned!
Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)
3 Steps to better security
Start using 1Password.com

https://www.facebook.com/174246142644437/photos/a.398675263534856/2038853169517049/?type=3&theater



Hacker tools to brute-force password

- John the ripper
- Hashcat
- Other tools

June 2016 - dadada

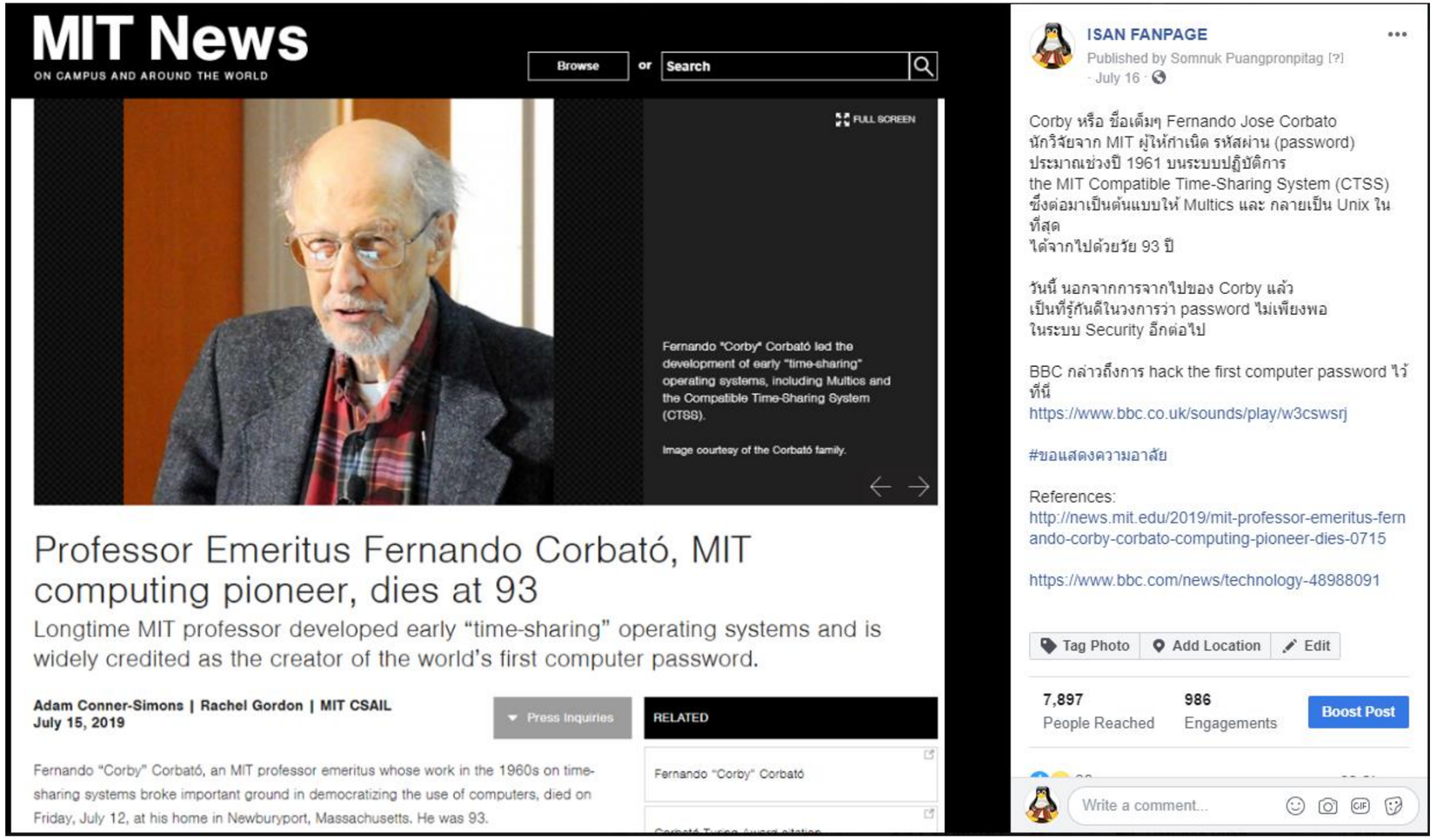
ปัญหา:
การตั้ง password ซ้ำกัน ระหว่างระบบ !!

Multiple Factor Authentication

ยุคที่คนเริ่มไม่เชื่อใน password

Password was created in 1961 by
Fernando Corbato
from MIT

การจากไปของผู้สร้างรหัสผ่าน



Multiple Factor Authentication

- Multiple Factor Authentication (MFA)
- Two Factor Authentication (2FA)
- Two-step Verifycation
- How to:
  - Using One Time Password (OTP)
    - SMS OTP, Token OTP, Mobile OTP, Paper OTP (Backup Code)
- Google, Facebook, Online Bank
  - SMS OTP
  - Mobile OTP: Google Authenticator, Facebook Code Generator

- In 2007, Bank of Thailand suggests all online banking to use Two Factor Authentication before allowing money to be transferred!

- *So, are we now secured?*

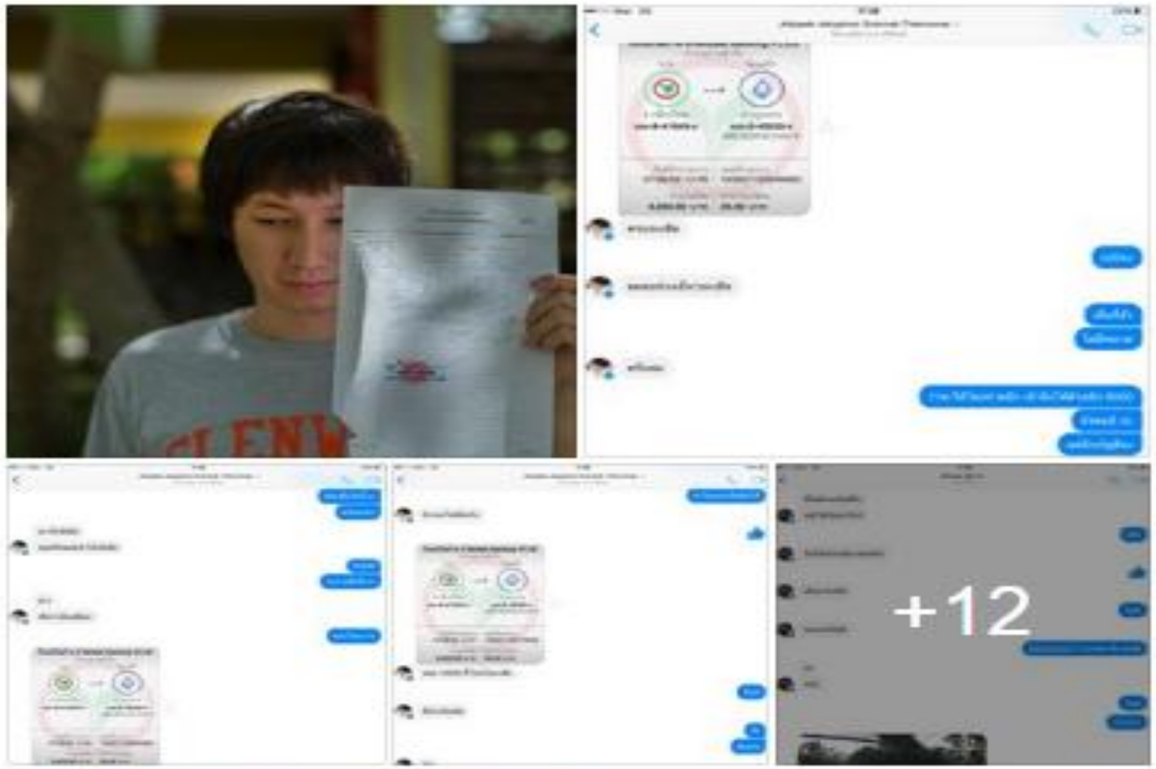
On Multiple Factor Authentication

Eg.., Facebook?, Gmail?

7 Jun 2016

Facebook Hack + Social Engineering

เหตุเกิด 7 June 2016
หลัก Social Engineer
Hack facebook เหยื่อ เพื่อขอยืมเงินเพื่อน เหยื่อ
ได้เงินไปเยอะเชียว ...
*** บทเรียน ยุค digital 2016 ***
อยู่ดีๆ เพื่อนยืมเงินทาง facebook messenger หรือทาง online
ต้องคิดใหม่ว่า ไม่แน่ ... เพื่อนหรือโจร
หาทาง ยืนยันตัวตน ดีๆ ก่อนนะครับ
https://www.facebook.com/noppadol.soisakun/posts/10156895520380618



Noppadol Soisakun added 16 new photos.
June 10 · Chiang Mai

NOPPADOL SOISAKUL โดนแฮ็ค Facebook เมื่อวันที่ 7 มิถุนายน 2559 เมื่อเวลา 12.30 ภายในเวลา 1 ชั่วโมง คนร้ายหลอกเงินของคนรู้จักไปเกือบ 70,000 บาท

Turn on 2FA on Facebook

Setting > Security and Login> Use Two-factor authentication