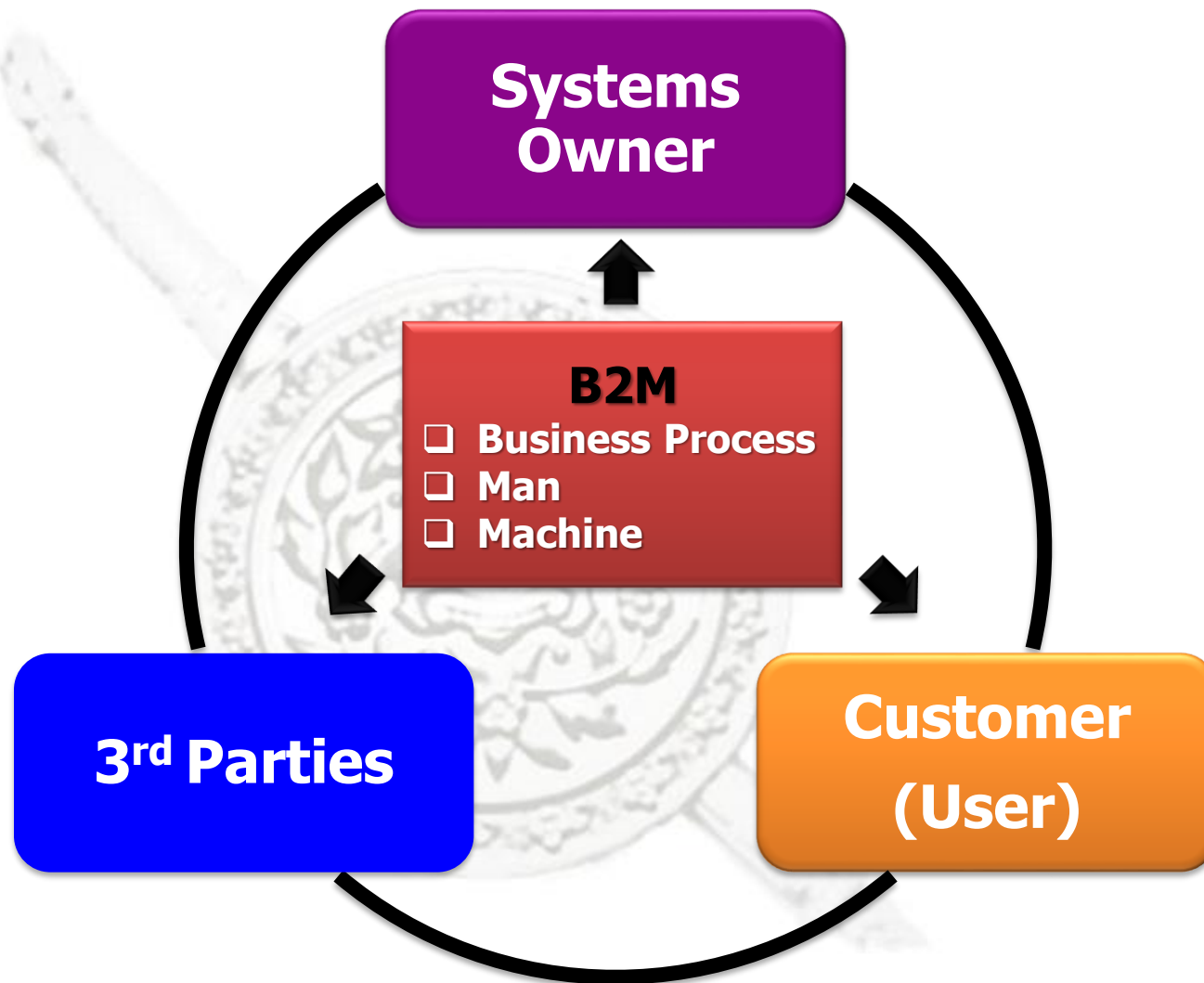




Hacking Systems Model





Thanachart IT Security Awareness 2016

พล.ต.ต ศิริพงษ์ ติมุลา

ผู้บัญชาการ กองบังคับการสนับสนุนทางเทคโนโลยี
สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ

พันตำรวจโท นันทวุฒิ รอดมณี

สารวัตรฝ่ายอำนวยการ 9 กองบังคับการอำนวยการ
ตำรวจภูธรภาค 9 สำนักงานตำรวจแห่งชาติ



อาชญากรรมคอมพิวเตอร์

© Cartoonbank.com



"You know, you can do this just as easily online."



ภัยคุกคาม

ระดับโลกหรือระดับประเทศ

- ❑ **นายกรัฐมนตรี** ใต้หวันส่งเสียงเตือนจีนที่โหมโจมตีเว็บไซต์รัฐบาลและเอกชนอย่างหนัก เพื่อหวังขโมยความลับ
- ❑ **"บ.โรงไฟฟ้านิวเคลียร์"** เกาหลีใต้โดนแฮก ไม่พ่นธงฝีมือนิยมแดง
- ❑ อินเทอร์เน็ตประเทศเกาหลีเหนือล่มทั้งระบบ
- ❑ เว็บไซต์กว่า **19,000** แห่งในฝรั่งเศสโดนโจมตีหลังเหตุการณ์ยิงถล่ม **Charlie Hebdo**
- ❑ **Anonymous** กลุ่มแฮกเกอร์ระดับเทพ ประกาศเตรียมถล่มกลุ่ม **ISIS** บนโลกออนไลน์ให้เหี้ยน
- ❑ ดำรวจยันเว็บหน่วยงานราชการถูกแฮก ไม่มีเอี่ยวระเบิดราชประสงค์



ภัยคุกคาม

ระดับองค์กร

- ❑ **Sony อ้วม!! โดน Hack ข้อมูลครั้งใหญ่**
- ❑ **บริษัทประกันฯ "Anthem" ถูกแฮกเกอร์ฉกข้อมูลลูกค้าและพนักงานไปกว่า 10 ล้านรายการ**
- ❑ **ทำไปซ้ำๆ? แฮกเกอร์อ้าง ฉกข้อมูลผู้ใช้ PlayStation, Xbox และ Amazon รวมๆกว่า 13,000 user**
- ❑ **Skype โดนแฮกบัญชี Twitter, Facebook และ Blog โดยฝีมือของกลุ่มแฮกเกอร์ชาวซีเรีย**
- ❑ **"Heartbleed" ยังป่วนไม่เลิก ล่าสุด แฮคเกอร์ใช้มันเป็นเครื่องมือในการฉกข้อมูลคนไข้กว่า 4.5 ล้านรายจากเครือข่ายโรงพยาบาลในอเมริกา**
- ❑ **ซีอีโอเว็บหาคู่ Ashley Madison ประกาศลาออกแล้วหลังถูกแฮกข้อมูลส่วนตัวลูกค้า**



ภัยคุกคาม

ระดับบุคคล

- ❑ **Twitter** นายกรัฐมนตรีถูกแฮก พร้อม **tweet** ว่าจะลาออกจากตำแหน่งแล้ว มาเป็นช่างภาพอิสระ !!!
- ❑ เตือนผู้ใช้ **LINE** ระวังโดนแฮกและโดนหลอกซื้อบัตร **iTunes**
- ❑ เตือนภัย มิจฉาชีพแฮกเฟซบุ๊ก สวมรอยหลอกให้คนโอนเงินให้
- ❑ **Scam Mail** วิธีการล่อลวงการหลอกลวงบนโลกอินเทอร์เน็ต
- ❑ แก๊งเฟชบุคต่างชาติหลอกสาวไทยโอนเงิน
- ❑ โดนแฮกเฟสบุค!! โปสเป็นมือระเบิดราชประสงค์ เครียดหนักผูกคอตาย!!
- ❑ รวบรวมโพสต์เฟซบุ๊กขู่ วางบึ้มป่วนเมืองขุนแผน
- ❑ สาวคลั่งพยายามฆ่าตัวตาย รับไม่ได้แฟนที่คบผ่านเน็ตไม่หล่ออย่างที่คิด
- ❑ หึงเมียเล่นเฟสบุคคุยกับหนุ่ม - สามีคว่ำซากดีหัวดับ

แผนประทุษกรรม E-Banking Fraud

และกรอบแนวคิดการป้องกัน



พัฒนาการของแผนปฏิบัติการ นับตั้งแต่มี E-banking service

- From 1 factor authentication > 2 factors authentication (OTP, Token)





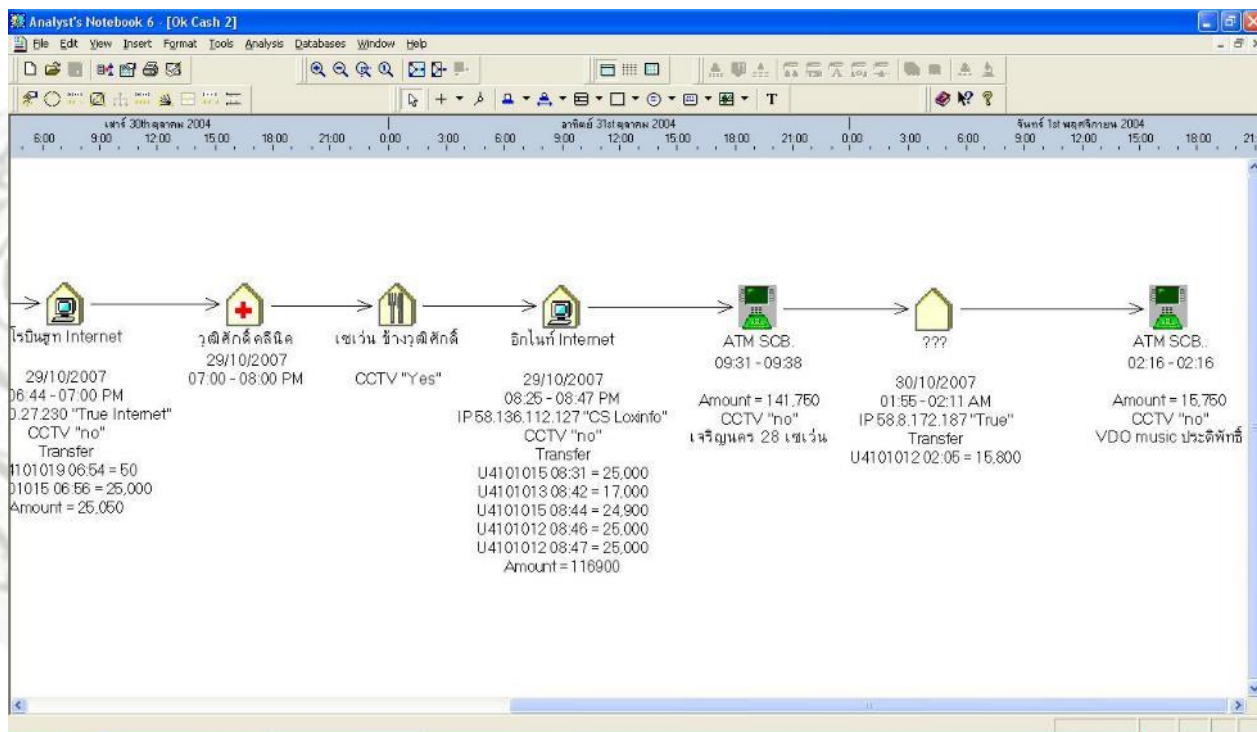
1 factor authentication

- **Phishing**
- **Next ATM card no.**
- **Call center social engineering**
- **Trojan Hack & Keylogger**
- **Trojan Hack & Remote access**





Next ATM card no.



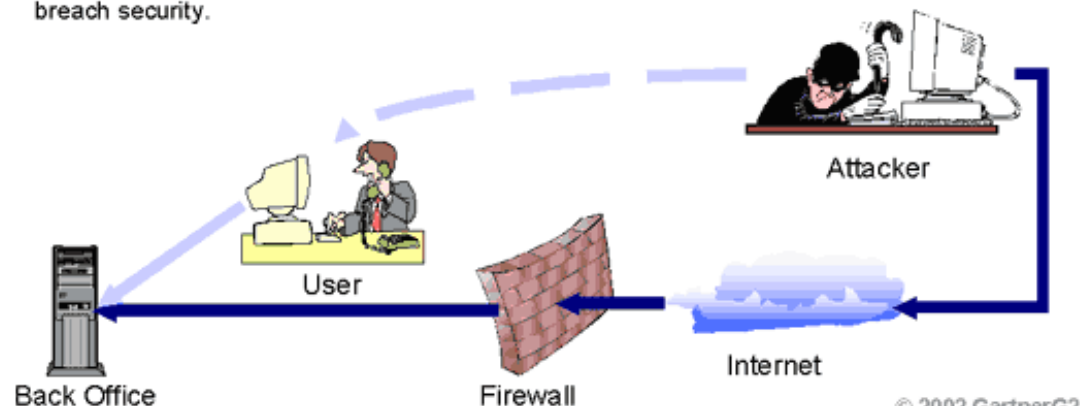


Call center social engineering



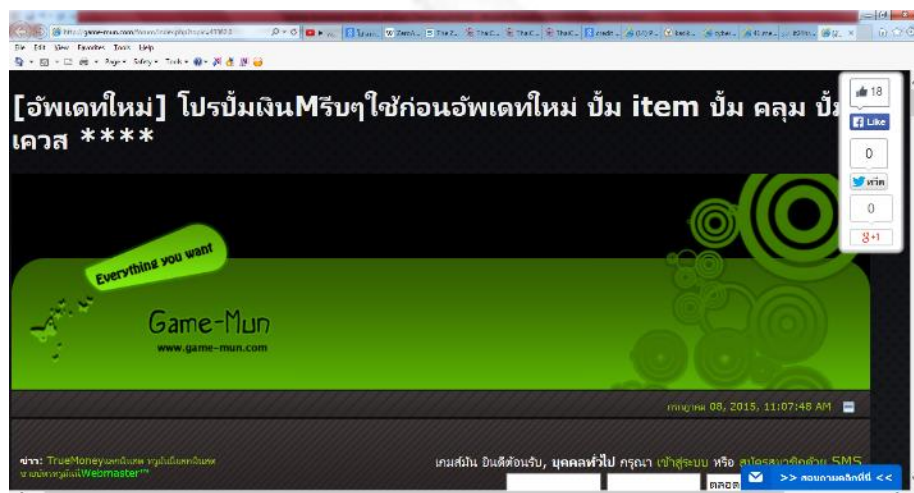
Social Engineering

- Includes extensive research information (legal and illicit) about an enterprise, which is gathered and used to exploit people.
- Successful social engineering results in partial or complete circumvention of an enterprise's security systems. The best firewall is useless if the person behind it gives away either the access codes or the information it is installed to protect.
- Social engineering *principally* involves the manipulation of people rather than technology to breach security.





Trojan Hack & Keylogger





Trojan Hack & Remote access



https://www.thaicert.or.th/papers/general/2011/pa2011g004.htm

Zeus Trojan (Zbot) ม้าโทรจันปล้นธนาคารทั่วโลก

ผู้เขียน: ศุภกร อุภะสิทธิ์พร
วันที่เผยแพร่: 5 พ.ย. 2554
ปรับปรุงล่าสุด: 5 พ.ย. 2554

Zeus (ซุส) หรือที่รู้จักในอีกชื่อหนึ่งคือ Zbot เป็นมัลแวร์ที่โด่งดังในปี 2006 มีแหล่งกำเนิดจากยุโรปตะวันออก ถูกสร้างขึ้นเพื่อใช้เป็นเครื่องมือสำหรับอาชญากรในการขโมยข้อมูลสำคัญของผู้ใช้งานบริการสถาบันการเงินออนไลน์ ดังแสดงในรูปที่ 1 และ 2 ซุสสามารถแพร่กระจายได้หลายวิธี เช่น แนบไฟล์หรือลิงค์มากับอีเมล ฝังตัวอยู่ในช่องโหว่ของเอกสารประเภท PDF แฝงมากับอุปกรณ์บันทึกข้อมูลภายนอก (External drive) ติดมากับซอฟต์แวร์ละเมิดลิขสิทธิ์ หรือส่งต่อลิงค์ผ่านเครือข่ายสังคมออนไลน์ (Social network) เป็นต้น เมื่อซุสได้ติดตั้งตัวเองลงบนเครื่องคอมพิวเตอร์ของเหยื่อ เครื่องนั้นก็จะกลายเป็น Botnet ของซุสในทันที [1] ทำให้ผู้โจมตีสามารถเข้าโจมตีระบบข้อมูลสำคัญภายในเครื่องคอมพิวเตอร์ของเหยื่อได้ ไม่ว่าจะเป็นหมายเลขบัญชีธนาคาร รหัสผ่าน หรือข้อมูลอื่นๆ [2] นอกจากนี้ ซุสยังพยายามรวบรวมข้อมูลของผู้ใช้งานที่ขโมยมาได้แล้วส่งมาเก็บไว้ที่เซิร์ฟเวอร์ของผู้โจมตี ซุสถูกขายเป็นเครื่องมือในตลาดมืด โดยมีราคาประมาณ 3000-4000 ดอลลาร์สหรัฐ [3]

ซุสมีกระบวนการในการสั่งการและควบคุมระบบ คือ

1. รอเวลาที่เหยื่อเข้าทำรายการธุรกรรมออนไลน์ตามช่องทางของธนาคาร
2. รายงานการดำเนินการต่างๆ ของเหยื่อไปยังหน่วยสั่งการและควบคุมเซิร์ฟเวอร์ในระบบธนาคาร
3. หน่วยสั่งการและควบคุมระบบ สั่งการให้ซุสเปลี่ยนแปลงการโอนเงินจากธนาคารของเหยื่อ
4. ดำเนินการเปลี่ยนแปลงการโอนเงินจากธนาคารของเหยื่อโดยตรวจสอบยอดเงินในบัญชี กำหนดวงเงินใหม่ให้มากที่สุดที่จะขโมยได้โดยไม่เกินวงเงินที่ธนาคารกำหนด จากนั้นจึงโอนเงินไปยังบัญชีเป้าหมายแล้วส่งต่อไปยังบัญชีต่างประเทศของผู้ขโมย
5. รายงานผลการดำเนินการให้หน่วยสั่งการและควบคุมระบบธนาคารเพื่อให้ทราบความสำเร็จหรือล้มเหลว



Any Account Hacking

- Password Cracking
- Systems Hacking/Reset Password
- Malware
- Social Engineering





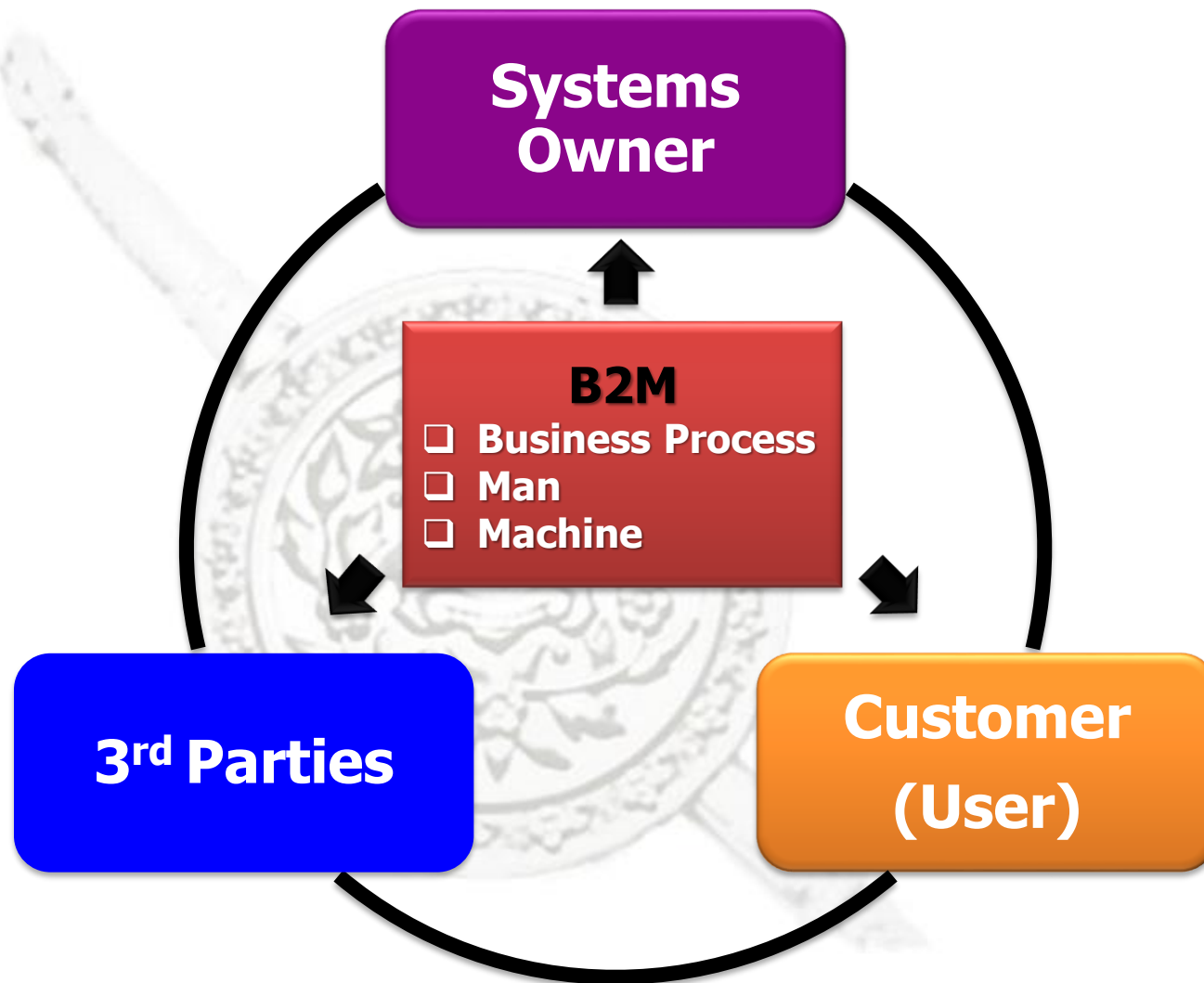
2 factors authentication (OTP, Token)

- ❑ SMS social engineering
- ❑ Mobile App./Malware
- ❑ SIM card changed
- ❑ Token hacked/Man in the Middle



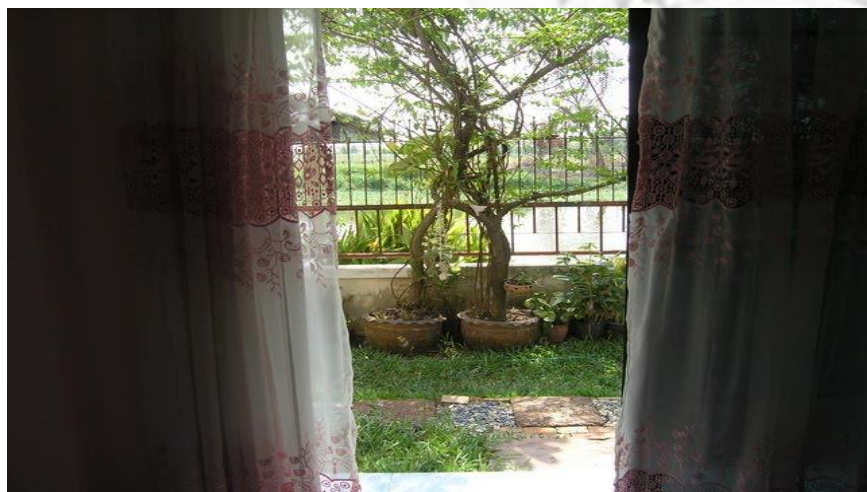


Hacking Systems Model





Inside out vs. outside in





Berlin wall & different questions



คำถาม: จะสร้างกำแพงเพื่อป้องกันการหลบหนีได้อย่างไร ?



คำถาม: จะหนีโดยข้ามกำแพงได้อย่างไร ?



Achilles' *heel* – *paradox*

- Sweep under the carpet
- Image – steak holder
- Marketing competition
- System relation
- Knowledge gab
- Separate function



Prevention measure (bank perspective)

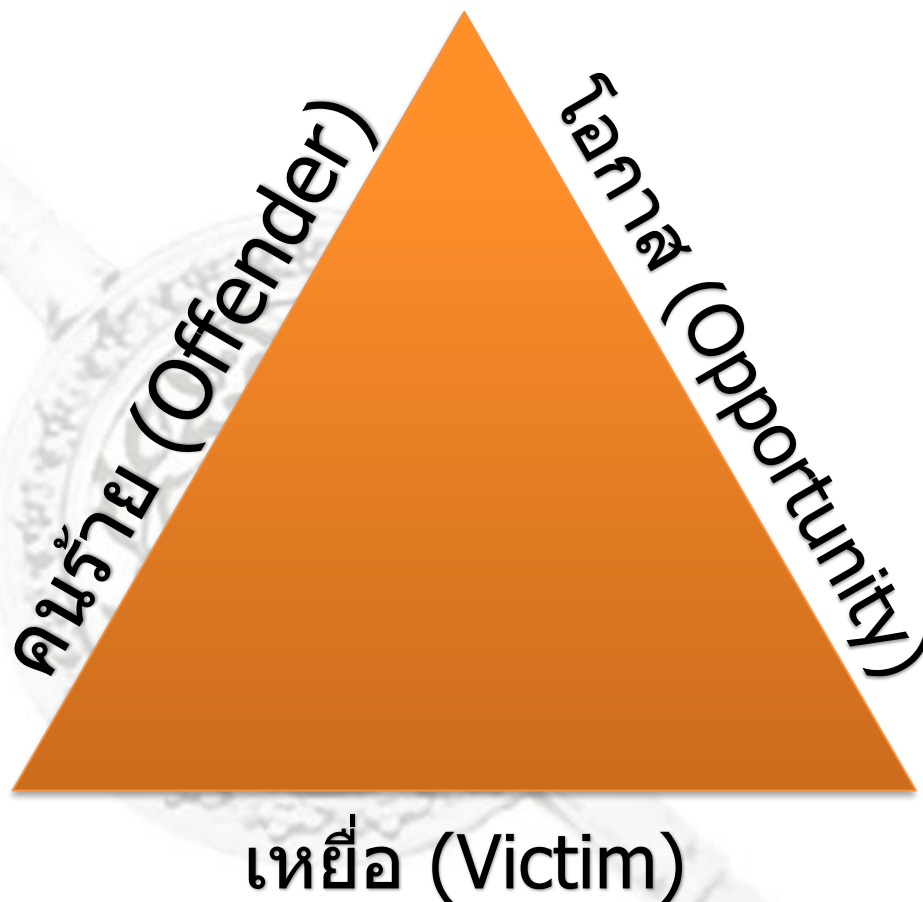
- **Fraud detection system (alert)**
- **Suspected transaction**
- **Error by intention/unintention**
- **Guess**
- **Trying**
- **Proxy**
- **Place /time**
- **System review/assessment**
- **Keeps your customers Aware. (KYCA)**

- **Contingency plan**
- **War room**
- **Response team**
- **Investigation team**
- **Scenario simulation**
- **Thinking like a thief**
- **CCTV**
- **Synergy with another**
- **Data sharing**
- **Connection**





ทฤษฎี 3 เหลี่ยมอาชญากรรม





แรงขับที่ส่งผลต่อพฤติกรรมมนุษย์

แรงขับทางเพศ

แรงขับของการต้องการเป็นคนสำคัญ



“กฎหมายที่เกี่ยวข้องกับ อาชญากรรมทางเทคโนโลยี”



พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา	ใคร	กระทำ	สิ่งที่ถูกกระทำ	เงื่อนไข	ผลลัพธ์	ผลที่ตามมา/เหตุอุกฉกรรจ์
5	ผู้ใด	เข้าถึงโดยมิชอบ	ระบบคอมพิวเตอร์	มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน		
6	ผู้ใด	ล่วงรู้ไปเปิดเผย	มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ	โดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น		
7	ผู้ใด	เข้าถึงโดยมิชอบ	ข้อมูลคอมพิวเตอร์	มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน		

Hacking/Cracking



ป.อาญา หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

มาตรา 3 ให้เพิ่มความต่อไปนี้เป็น (14) ของ มาตรา 1 แห่งประมวลกฎหมายอาญา

(14) "บัตรอิเล็กทรอนิกส์ หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใดทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมีได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในการทำงานเดียวกับ (ก) หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ



ป.อาญา หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

มาตรา 269/4 ผู้ใดใช้หรือมีไว้เพื่อใช้ซึ่งสิ่งใดๆ ตามมาตรา 269/1 อันได้มาโดยรู้ว่าเป็นของที่ทำปลอมหรือแปลงขึ้น ต้องระวางโทษ จำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี หรือปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งสิ่งใดๆ ที่ทำปลอมหรือแปลงขึ้นตามมาตรา 269/1 ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ

ถ้าผู้กระทำความผิดตามวรรคแรกหรือวรรคสองเป็นผู้ปลอมซึ่งบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 ให้ลงโทษตามมาตรานี้แต่กระหนเดียว

มาตรา 269/5 ผู้ใด**ใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ** ในประการที่น่าจะ**ก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน** ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ



พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา	ใคร	กระทำ	สิ่งที่ถูกกระทำ	เงื่อนไข	ผลลัพธ์	ผลที่ตามมา/เหตุอุกฉกรรจ์
8	ผู้ใด	ดักจับไว้	ข้อมูลคอมพิวเตอร์	-โดยมิชอบด้วย วิธีการทาง อิเล็กทรอนิกส์ -อยู่ระหว่างการส่ง ในระบบ คอมพิวเตอร์ -ข้อมูลคอมพิวเตอร์ นั้น มิได้มีไว้เพื่อ ประโยชน์สาธารณะ หรือเพื่อให้บุคคล ทั่วไปใช้ประโยชน์ ได้		

Sniffing



พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา	ใคร	กระทำ	สิ่งที่ถูกกระทำ	เจตนา	ผลลัพธ์	ผลที่ตามมา/เหตุฉุกเฉิน
9	ผู้ใด	ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือ เพิ่มเติมไม่ว่าทั้งหมด หรือ บางส่วน	ข้อมูลคอมพิวเตอร์	โดยมิชอบ		- ก่อให้เกิดความเสียหายแก่ประชาชน - เสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ -ผู้อื่นถึงแก่ความตาย (ม.12)

Data didling
Logic bomb
Cyber war



พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา	ใคร	กระทำ	สิ่งที่ถูกกระทำ	เงื่อนไข	ผลลัพธ์	ผลที่ตามมา/เหตุอุกฉกรรจ์
10	ผู้ใด	ระงับ ชะลอ ขัดขวาง หรือรบกวน	ระบบคอมพิวเตอร์	โดยมิชอบ DOS : Denial Of Service	ไม่สามารถทำงานตามปกติได้	“-----”
11	ผู้ใด	ส่ง ข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์	บุคคลอื่น	ปกปิด หรือปลอมแปลง แหล่งที่มาของการส่งข้อมูล Spamming	รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข	
13	ผู้ใด	จำหน่ายหรือ เผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕-มาตรา ๑๑	บุคคลอื่น	Hack Tools		



พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑)(๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔



พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็น**ภาพของผู้อื่น** และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะ**ทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย** ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย



กฎหมายอื่น ๆ ที่น่าสนใจ

“มาตรา 287/1 ผู้ใด**ครอบครองสื่อลามกอนาจารเด็กเพื่อแสวงหาประโยชน์ในทางเพศสำหรับตนเองหรือผู้อื่น** ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับถ้าผู้กระทำความผิดตามวรรคหนึ่งส่งต่อซึ่งสื่อลามกอนาจารเด็กแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินเจ็ดปี หรือปรับไม่เกินหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 287/2 ผู้ใด

(1) เพื่อความประสงค์แห่งการค้า หรือโดยการค้า เพื่อการแจกจ่ายหรือเพื่อการแสดงอวดแก่ประชาชน ทำ ผลิต มีไว้ นำเข้าหรือยังให้นำเข้าในราชอาณาจักร ส่งออกหรือยังให้ส่งออกไปนอกราชอาณาจักร พาไปหรือยังให้พาไปหรือทำให้แพร่หลายโดยประการใดๆ ซึ่งสื่อลามกอนาจารเด็ก

(2) ประกอบการค้า หรือมีส่วนหรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับสื่อลามกอนาจารเด็ก แจกจ่ายหรือแสดงอวดแก่ประชาชนหรือให้เข้าสื่อลามกอนาจารเด็ก

(3) เพื่อจะช่วยให้แพร่หลาย หรือการค้าสื่อลามกอนาจารเด็กแล้วโฆษณาหรือโฆษณาโดยประการใดๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรานี้ หรือโฆษณาหรือโฆษณาว่าสื่อลามกอนาจารเด็กดังกล่าวแล้วจะหาได้จากบุคคลใด หรือโดยวิธีใด ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบปี และปรับตั้งแต่หกหมื่นบาทถึงสองแสนบาท”



กฎหมายอื่น ๆ ที่น่าสนใจ

หมิ่นประมาท

1 กระทำต่อบุคคลธรรมดา

- 1.1 หมิ่นประมาท (ประมวลกฎหมายอาญา มาตรา 326) , (1 ปี 20,000)
- 1.2 หมิ่นประมาทโดยการโฆษณา (ประมวลกฎหมายอาญา มาตรา 328) , (2 ปี 200,000)
- 1.3 ดูหมิ่นซึ่งหน้า (ประมวลกฎหมายอาญา มาตรา 393) , (1 เดือน 1,000)

2 กระทำต่อเจ้าหน้าที่รัฐ

- 2.1 การหมิ่นประมาทเจ้าพนักงาน (1 ปี 200,000)
- 2.2 การหมิ่นประมาทศาล (1-7 ปี 2,000-14,000)

3 การหมิ่นประมาทบุคคลสำคัญระดับชาติ

- 3.1 หมิ่นพระบรมเดชานุภาพ (3-15 ปี)
- 3.2 การหมิ่นประมาทบุคคลสำคัญของรัฐต่างชาติ



กฎหมายอื่น ๆ ที่น่าสนใจ

ฉ้อโกง

มาตรา 341 ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังวานั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

มาตรา 342 ถ้าในการกระทำความผิดฐานฉ้อโกง ผู้กระทำ

(1) แสดงตนเป็นคนอื่น หรือ

(2) อาศัยความเบาปัญญาของผู้ถูกหลอกลวงซึ่งเป็นเด็ก หรืออาศัยความอ่อนแอแห่งจิตของผู้ถูกหลอกลวง

ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 343 ถ้าการกระทำความผิดตามมาตรา 341 ได้กระทำด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดดังกล่าวในวรรคแรก ต้องด้วยลักษณะดังกล่าวในมาตรา 342 อนุมาตราหนึ่งอนุมาตราใดด้วย ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงเจ็ดปี และปรับตั้งแต่หนึ่งพันบาทถึงหนึ่งหมื่นสี่พันบาท



กฎหมายอื่น ๆ ที่น่าสนใจ

มาตรา 344 ผู้ใดโดยทุจริต หลอกลวงบุคคลตั้งแต่สิบคนขึ้นไปให้ประกอบการงานอย่างใดๆ ให้แก่ตนหรือให้แก่บุคคลที่สาม โดยจะไม่ใช่ค่าแรงงานหรือค่าจ้างแก่บุคคลเหล่านั้น หรือโดยจะใช้ค่าแรงงานหรือค่าจ้างแก่บุคคลเหล่านั้นต่ำกว่าที่ตกลงกัน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

มาตรา 345 ผู้ใดสั่งซื้อและบริโภคอาหารหรือเครื่องดื่ม หรือเข้าพักในโรงแรม โดยรู้ว่าตนไม่สามารถชำระเงินค่าอาหาร ค่าเครื่องดื่ม หรือค่าอยู่ในโรงแรมนั้น ต้องระวางโทษจำคุกไม่เกินสามเดือน หรือปรับไม่เกินห้าร้อยบาท หรือทั้งจำทั้งปรับ

มาตรา 346 ผู้ใดเพื่อเอาทรัพย์สินของผู้อื่นเป็นของตนหรือของบุคคลที่สาม ชักจูงผู้หนึ่งผู้ใดให้จำหน่ายโดยเสียเปรียบซึ่งทรัพย์สิน โดยอาศัยเหตุที่ผู้ถูกชักจูงมีจิตอ่อนแอ หรือเป็นเด็กเบาปัญญา และไม่สามารถเข้าใจตามควรซึ่งสาระสำคัญแห่งการกระทำของตน จนผู้ถูกชักจูงจำหน่ายซึ่งทรัพย์สินนั้น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่พันบาท หรือทั้งจำทั้งปรับ

มาตรา 347 ผู้ใดเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์จากการประกันวินาศภัย แกล้งทำให้เกิดเสียหายแก่ทรัพย์สินอันเป็นวัตถุที่เอาประกันภัย ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ



แนวโน้มภัยคุกคามของประเทศไทย





แนวโน้มภัยคุกคามของประเทศไทย

แบ่งตามความเสียหาย

- ☐ ทำให้เสียชื่อ
- ☐ ทำให้เสียทรัพย์

แบ่งตามวิธีการ (B2M)

- ☐ Business Process
- ☐ Machine
- ☐ Man





แนวโน้มนักคุกคามของประเทศไทย

เป้าหมายการเจาะระบบ (Hacking)

- Website
- Email
- Any Account
- Systems

วิธีการ

1. Password Cracking
2. Systems Hacking
3. Malware
4. Social Engineering

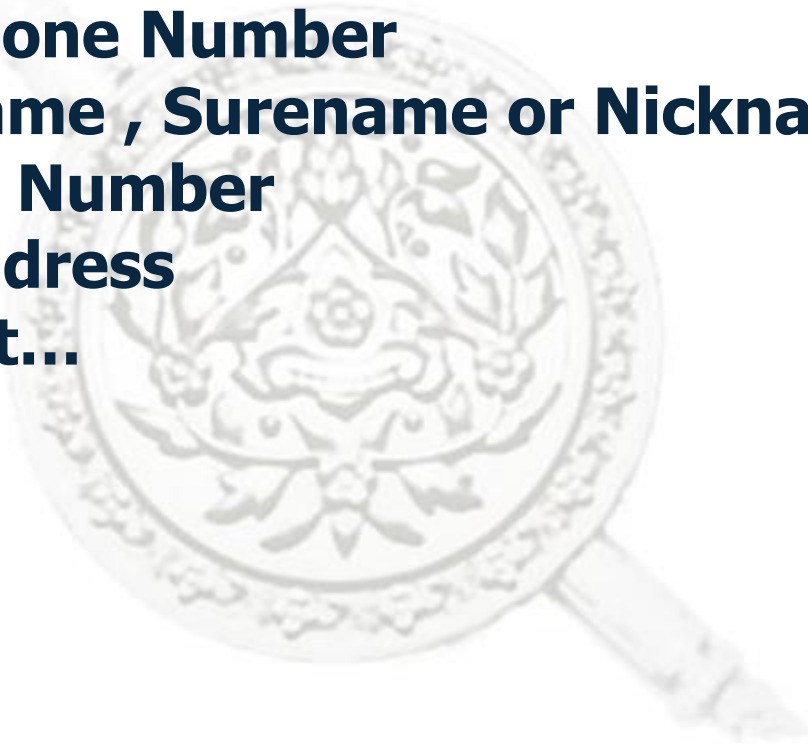




การเจาะระบบ (Hacking)

1.Password Cracking

- ☐ Don't use for Password
 - ☐ Birth Date
 - ☐ Phone Number
 - ☐ Name , Surname or Nickname
 - ☐ ID Number
 - ☐ Address
 - ☐ Ect...





การเจาะระบบ (Hacking)

2.Systems Hacking / Account Reset

- ☐ Systems
- ☐ Email
- ☐ Bank Account
- ☐ Social Media Account





การเจาะระบบ (Hacking)

3. Malware

- ☐ Virus
- ☐ Worm
- ☐ Trojan
- ☐ Spyware
- ☐ Hybrid Malware



**Payload
Malware**

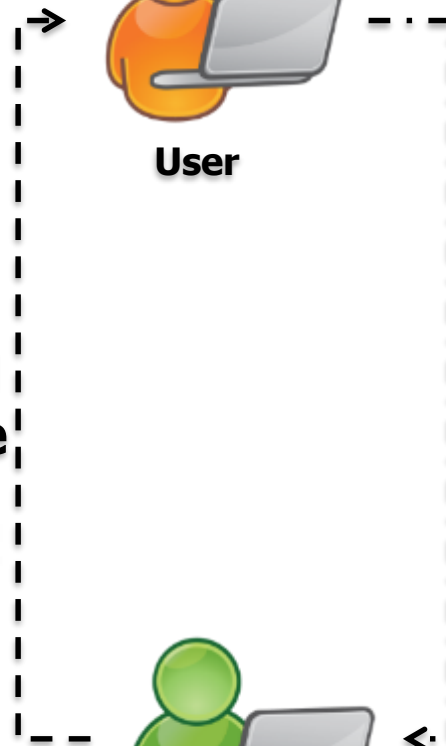


User

**Username
Password**



**Malware
Owner**





การเจาะระบบ (Hacking)

4.Social Engineering

4.1 Human Based

- ☐Telephone , Online
- ☐Dumpster Diving
- ☐Shoulder Surfing
- ☐Reverse Social Engineering

4.2 Computer Based

- ☐File Attachment
- ☐Phishing

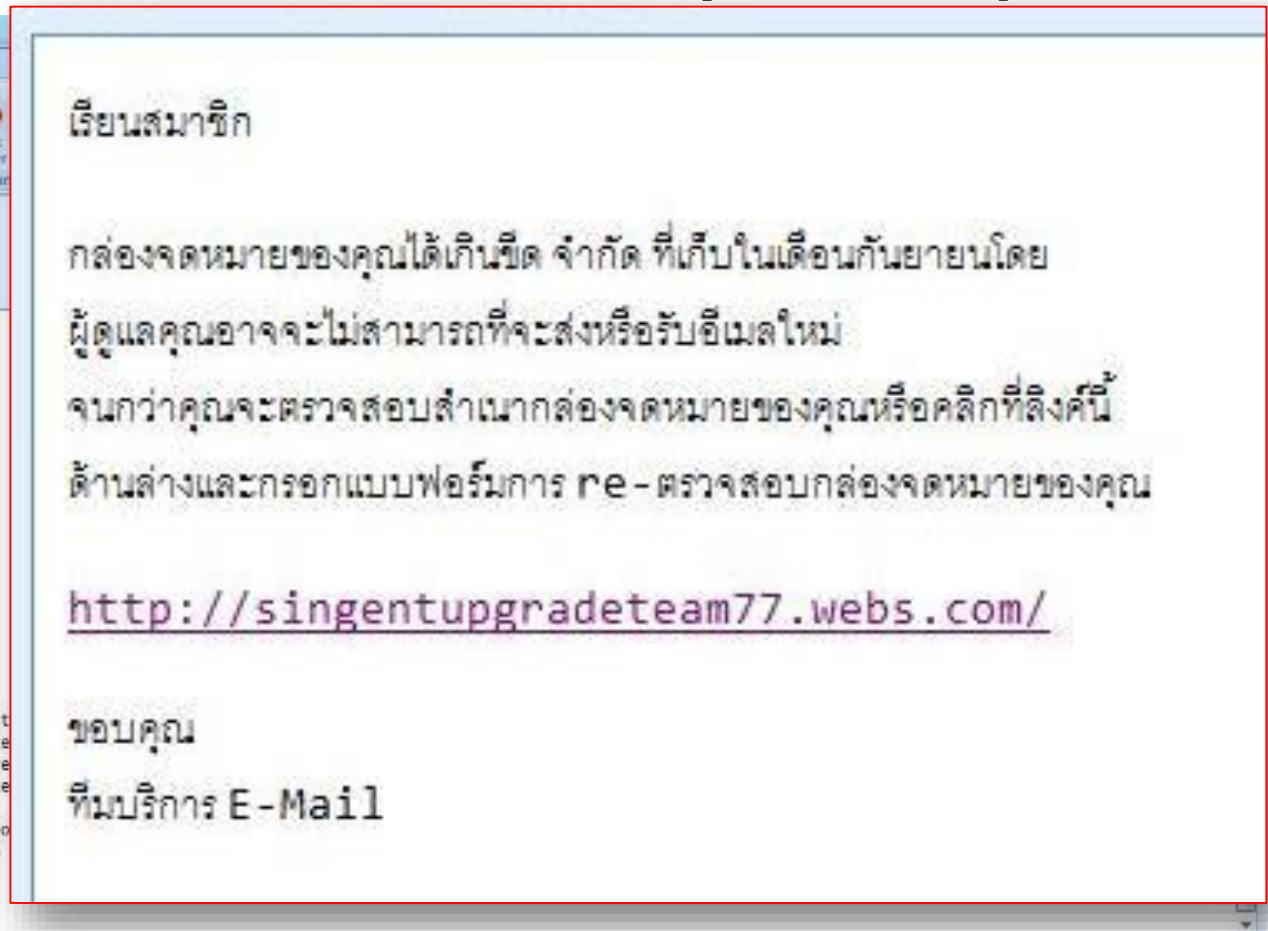
**SOCIAL ENGINEERING
SPECIALIST**

Because there is no patch
for human stupidity



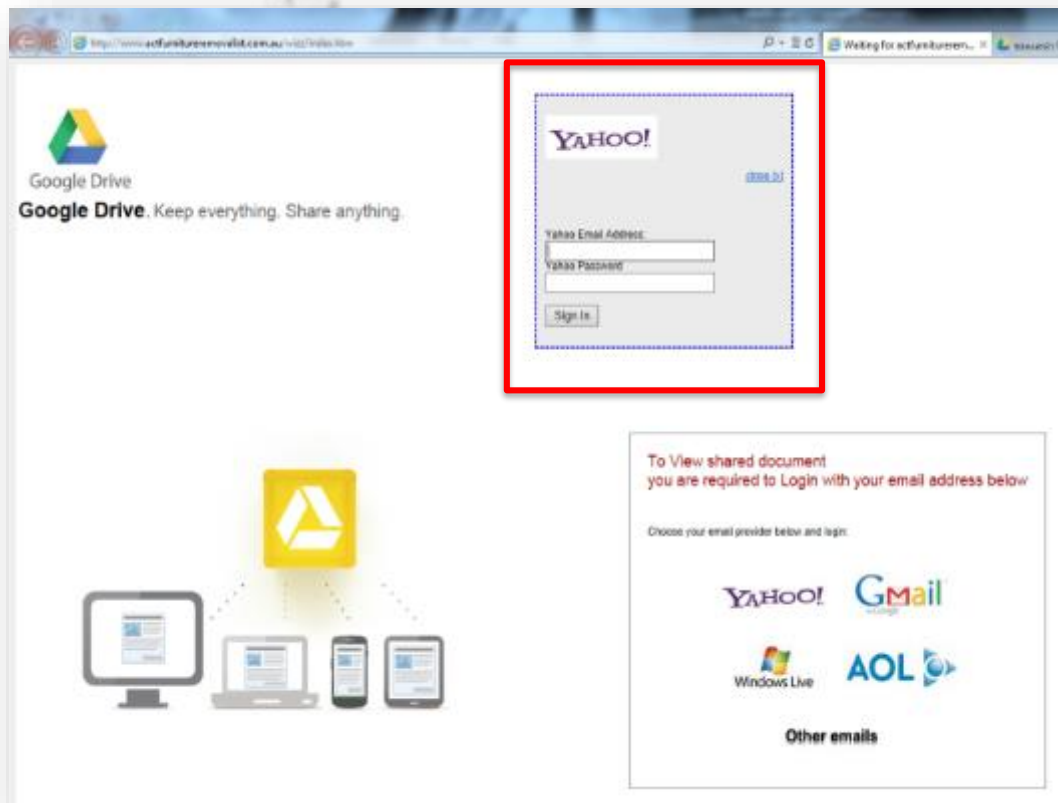
Phishing

❑ ส่ง e-mail มาแจ้งว่ากล่องจดหมายของเราเต็ม (mailbox full)





Phishing





แนวโน้มภัยคุกคามของประเทศไทย

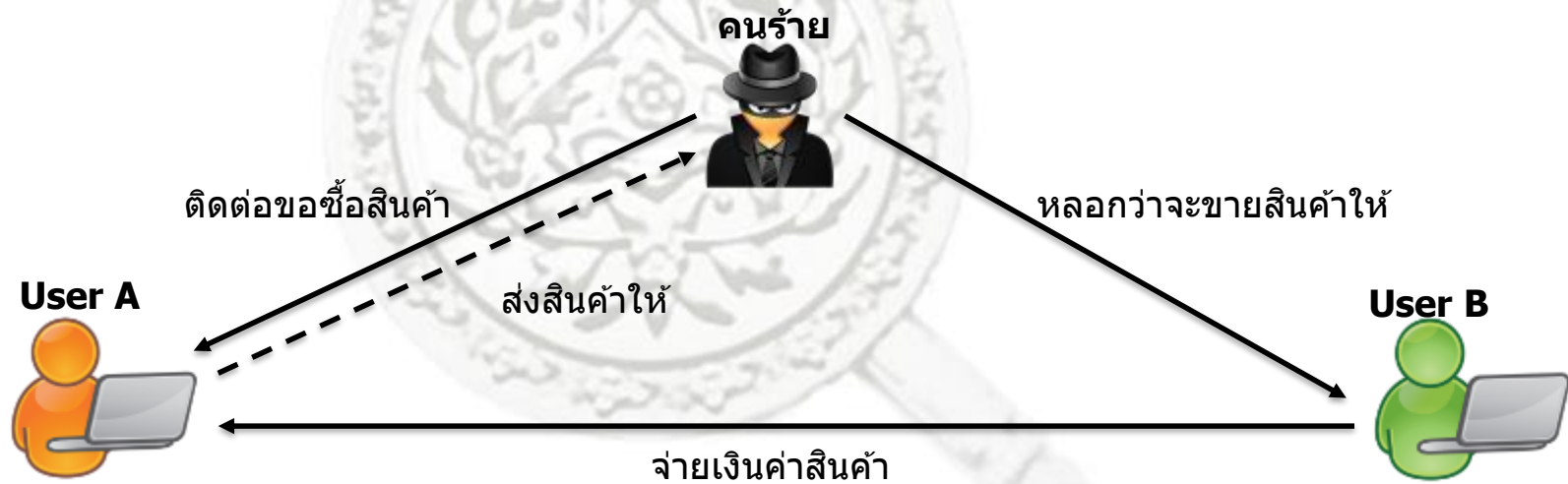
1. การหลอกลขายสินค้าในอินเทอร์เน็ต

➤ ฝั่งผู้ซื้อ

- ชื่อของไม่ได้ของ
- ได้ของไม่ตรงกับที่โฆษณา
- ได้ของไม่มีคุณภาพหรือหมดอายุ

➤ ฝั่งผู้ขาย

- หลอกให้ผู้อื่นจ่ายเงินค่าสินค้าให้





แนวโน้มนักภัยคุกคามของประเทศไทย

2. Romance Scam

- International Scam
- Local Scam



แนวโน้มนภัยคุกคามของประเทศไทย

3. Email Scam

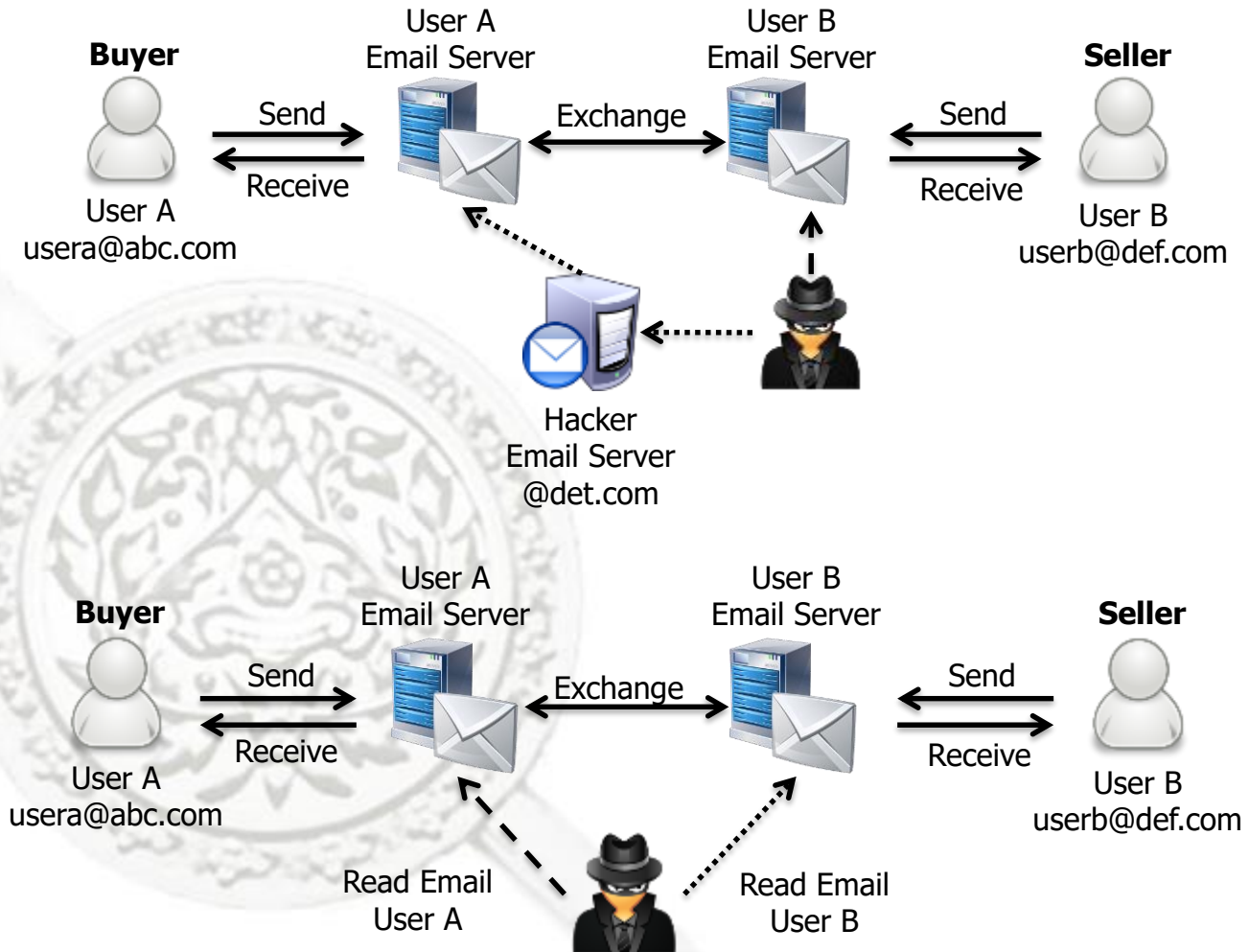
ท้ออีเมลเป้าหมาย

ศึกษาขั้นตอนทาง
ธุรกรรม

ส่งอีเมลเปลี่ยนบัญชี
การโอนเงิน

Phishing Email ต่อ
(ถ้าทำได้)

ถอนเงินจากบัญชีและ
มองหาเหยื่อต่อ





แนวโน้มนักควบคุมคามของประเทศไทย

4. ภัยและการกระทำความผิดทางโซเชียลมีเดีย (Social Media)

4.1 การหลอกลวง

4.2 ล่อลวง

4.3 การโฆษณาชวนเชื่อ และทำให้เสียชื่อเสียง

4.4 โพสต์หรือแชร์ข้อมูลที่ไม่เหมาะสม





แนวโน้มนักคอมพิวเตอร์ของประเทศไทย



5. การเรียกค่าไถ่ และการแบล็คเมลล์

❖ Ransomware

❖ ขโมยตัวตนและเรียกค่าไถ่

❖ การแบล็คเมลล์



Blue Lace.16.bmp.EnCiPhErEd	2 KB	CRYPTED!
clock.avi.EnCiPhErEd	81 KB	CRYPTED!
Coffee Bean.bmp.EnCiPhErEd	17 KB	CRYPTED!
FeatherTexture.bmp.EnCiPhErEd	17 KB	CRYPTED!
Gone Fishing.bmp.EnCiPhErEd	17 KB	CRYPTED!
Greenstone.bmp.EnCiPhErEd	26 KB	CRYPTED!
OEWABLog.txt.EnCiPhErEd	2 KB	CRYPTED!
Prairie Wind.bmp.EnCiPhErEd	65 KB	CRYPTED!
Rhododendron.bmp.EnCiPhErEd	17 KB	CRYPTED!
River Sumida.bmp.EnCiPhErEd	27 KB	CRYPTED!
Santa Fe Stucco.bmp.EnCiPhErEd	65 KB	CRYPTED!
setuplog.txt.EnCiPhErEd	21 KB	CRYPTED!
Soap Bubbles.bmp.EnCiPhErEd	65 KB	CRYPTED!
winnt256.bmp.EnCiPhErEd	48 KB	CRYPTED!
winnt.bmp.EnCiPhErEd	48 KB	CRYPTED!



แนวโน้มภัยคุกคามของประเทศไทย

6. ภัยคุกคามจากระบบทางการเงิน

❖ **Bank , E-Banking**

❖ **Non-Bank**

- True Money
- mPay
- Rabbit
- Paypal , Paysbuy
- Apple Gift Card
- Apple Pay

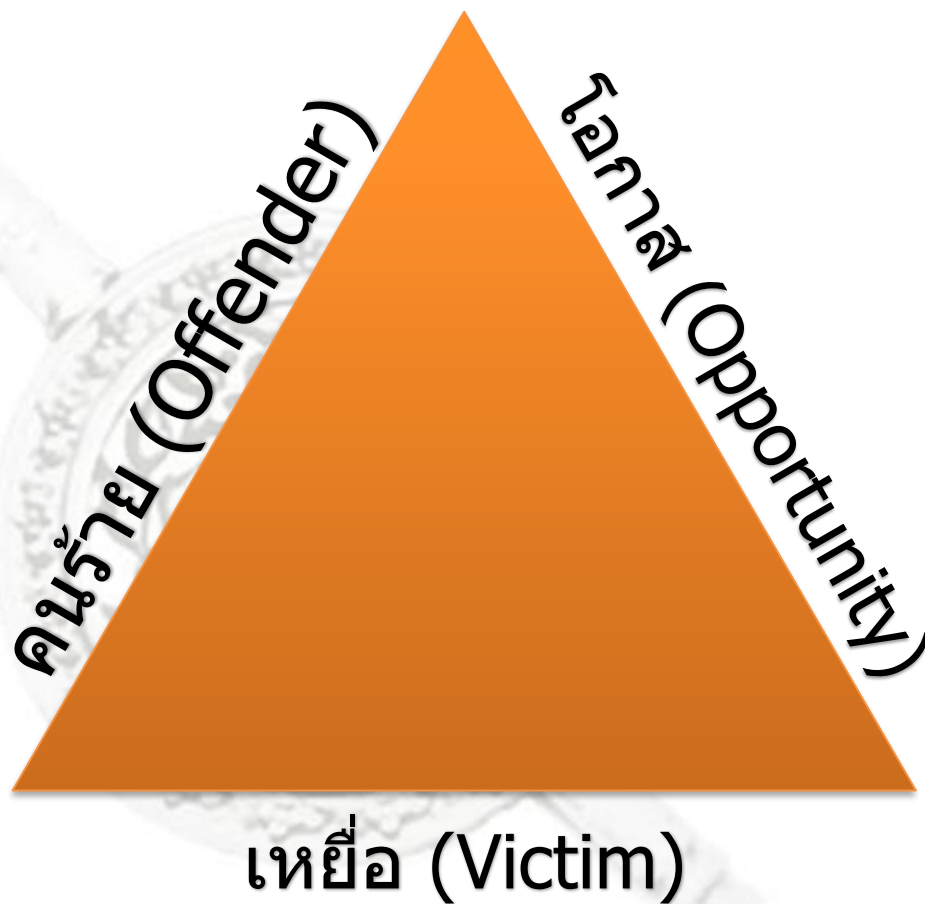


เครื่องมือ Spy , anti spy



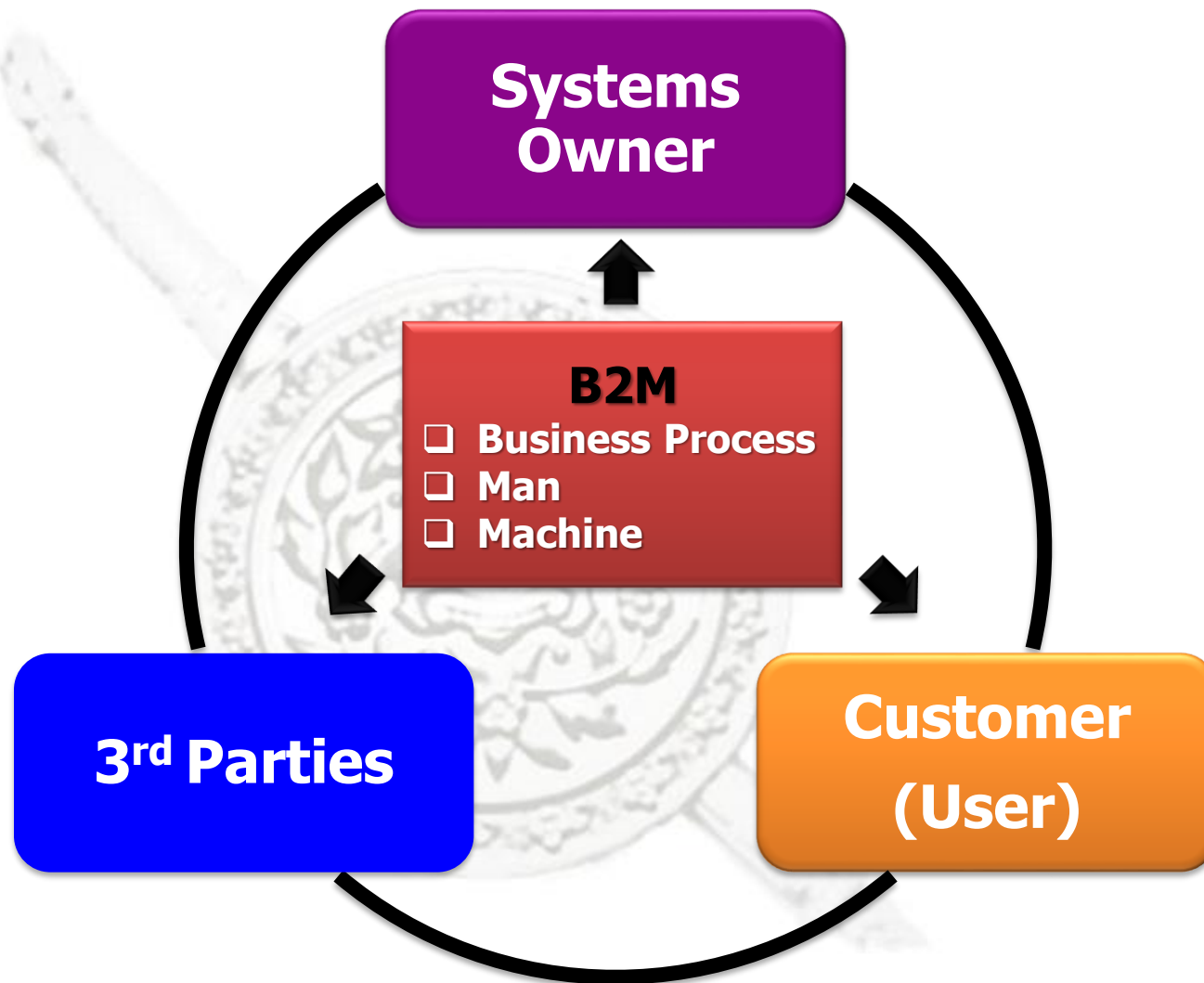


ทฤษฎี 3 เหลี่ยมอาชญากรรม





Hacking Systems Model





คาถากันภัย

❑ 5 อย่า

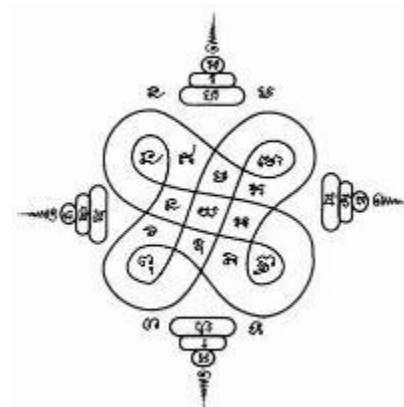
- ❑ อย่าตั้งพาสเวิร์ดง่าย ๆ จากข้อมูลส่วนตัว
- ❑ อย่าเซฟพาสเวิร์ดไว้ในเครื่อง
- ❑ อย่าคลิกอะไรที่ไม่คุ้นเคยหรือติดตั้งโปรแกรมอะไรที่ไม่รู้จัก
- ❑ อย่าใช้ Wifi ที่ไม่รู้จัก
- ❑ อย่าโลภหรือเชื่อว่าสามารถทำอะไรได้ง่าย

❑ 4 ตรวจ

- ❑ ตรวจสอบข้อมูลให้ดีก่อนซื้อ
- ❑ ตรวจสอบ URL ให้ดีก่อนทำธุรกรรม
- ❑ ตรวจสอบเจ้าของโปรแกรมให้ดีก่อนติดตั้ง
- ❑ ตรวจสอบข้อมูลและคิดให้ดีก่อนไลต์ โพสท์ แชร์ คอมเมนต์

❑ 3 ต้อง

- ❑ ต้องล็อกหน้าจอทุกครั้งที่ไม่ได้ใช้เครื่อง
- ❑ ต้องทำ 2 step login (ทำมากกว่า 1 Factor Authen)
- ❑ ต้องใช้โปรแกรม Private Gallery สำหรับเก็บรูปส่วนตัว





Awareness

Personal Computer Security Awareness



Question





คู่มือการใช้ Email

1-3 จาก 3 แถว

หลัก	โซเชี่ยล	โปรโมชัน
☐ ☆ ☐ ☐ ทีมงาน Gmail	คุณลักษณะที่ดีที่สุดของ Gmail จากทุกที่ - สวัสดิ์ Boring โหลดแอปทางการของ Gmail คุณลักษณะที่ดีที่สุดของ	30 ต.ค.
☐ ☆ ☐ ☐ ทีมงาน Gmail	จัดระเบียบได้ดียิ่งขึ้นด้วยกล่องจดหมายของ Gmail - สวัสดิ์ Boring กล่องจดหมายของ Gmail ช่วยให้คุณเป็นผู้	30 ต.ค.
☐ ☆ ☐ ☐ ทีมงาน Gmail	เคล็ดลับสามข้อในการใช้ประโยชน์สูงสุดจาก Gmail - สวัสดิ์ Boring เคล็ดลับในการใช้ประโยชน์สูงสุดจาก Gm	30 ต.ค.

ใช้ไป 0 GB (0%) จาก 15 GB

จัดการ

ข้อกำหนด - ความปลอดภัย

กิจกรรมล่าสุดของบัญชี: 11 วันที่ผ่านมา

รายละเอียด

กิจกรรมในบัญชีนี้

คุณลักษณะนี้ให้ข้อมูลเกี่ยวกับกิจกรรมล่าสุดทำในบัญชีนี้และกิจกรรมอื่นที่เกี่ยวข้องพร้อมกัน [เรียนรู้เพิ่มเติม](#)

ดูเพื่อหาบัญชีที่ไม่ได้เปิดในตำแหน่งอื่น แต่อาจมีเซสชันที่ยังไม่ได้จากระบบ

เลือกจากเซสชันเว็บอื่นๆ ที่มองเห็น

กิจกรรมล่าสุด:

ประเภทการเข้าถึง [2] (เบราว์เซอร์ มีชื่อ POP3 เป็นต้น)	ตำแหน่ง (ที่อยู่ IP) [2]	วันที่/เวลา (แสดงตามเขตเวลาของคุณ)
เบราว์เซอร์ (Chrome) แสดงรายละเอียด	* ไทย (125.24.30.53)	22:32 (0 นาทีที่แล้ว)
เบราว์เซอร์ (Chrome) แสดงรายละเอียด	ไทย (125.24.72.10)	2 พ.ย.
เบราว์เซอร์ (Chrome) แสดงรายละเอียด	ไทย (125.24.72.10)	2 พ.ย.
เบราว์เซอร์ (Chrome) แสดงรายละเอียด	ไทย (1.1.178.3)	30 ต.ค.

การจัดการแจ้งเตือน: แสดงการแจ้งเตือนสำหรับกิจกรรมที่ผิดปกติ [เปลี่ยน](#)

* หมายถึงกิจกรรมจากเซสชันปัจจุบัน

คอมพิวเตอร์เครื่องนี้กำลังใช้ที่อยู่ IP 125.24.30.53 (ไทย)

คู่มือการใช้ Facebook

🏠 ทั่วไป

🔒 ความปลอดภัย

👤 ความเป็นส่วนตัว

📧 โหมดและแท็ก

🛑 การล็อก

🌐 ภาษา

🌐 การแจ้งเตือน

📱 โทรศัพท์มือถือ

📡 ผู้ติดตาม

📱 แอป

📄 โฆษณา

💰 การชำระเงิน

🛑 กล้องข้อความการสนทนา...

📺 วิดีโอ

การตั้งค่าความปลอดภัย

เดือนการเข้าสู่ระบบ	รับการเตือนเมื่อมีผู้เข้าสู่ระบบบัญชีผู้ใช้ของคุณจากอุปกรณ์หรือเบราว์เซอร์ใหม่	แก้ไข
การอนุมัติการเข้าสู่ระบบ	ใช้โทรศัพท์ของคุณเป็นการรักษาความปลอดภัยอีกระดับเพื่อป้องกันไม่ให้ผู้อื่นเข้าสู่ระบบบัญชีผู้ใช้ของคุณ	แก้ไข
ตัวสำรองรหัส	ใช้แอป Facebook ของคุณเพื่อรับรหัสรักษาความปลอดภัยเมื่อคุณต้องการ	แก้ไข
รหัสผ่านแอป	ใช้รหัสผ่านพิเศษเพื่อเข้าสู่ระบบแอปของคุณแทนการใช้รหัสผ่าน Facebook หรือรหัสการอนุมัติการเข้าสู่ระบบ	แก้ไข
ผู้ติดต่อที่ไว้วางใจ	เลือกเพื่อนที่คุณสามารถร้องขอให้ช่วยหาคุณกลับเข้าสู่บัญชีผู้ใช้ของคุณได้หากมีการปิดกั้นไม่ให้คุณเข้าถึง	แก้ไข
เบราว์เซอร์และแอปของคุณ	ตรวจสอบว่าเบราว์เซอร์ใดเป็นเบราว์เซอร์ที่คุณบันทึกไว้ว่าเป็นเบราว์เซอร์ที่คุณใช้บ่อย	แก้ไข

สถานที่ที่คุณเข้าสู่ระบบ

เซสชันปัจจุบัน

สิ้นสุดกิจกรรมทั้งหมด

สถานที่ Bangkok, Thailand (โดยประมาณ)

ประเภทอุปกรณ์ Chrome บน Mac OS X 10.11

หากคุณสังเกตเห็นอุปกรณ์หรือสถานที่ที่ไม่คุ้นเคย คลิก 'หยุดกิจกรรม' เพื่อจบเซสชันดังกล่าว

เดสก์ท็อป (7) ▾

ใช้งานล่าสุด 11 พฤศจิกายน เวลา 23:26 น.

หยุดกิจกรรม

สถานที่ Amphoe Sai Noi, Thailand (โดยประมาณ)

ประเภทอุปกรณ์ Chrome บน Mac OS X 10.11

ใช้งานล่าสุด 2 พฤศจิกายน เวลา 14:54 น.

www.facebook.com/settings?tab=security§ion=devices

สำนักงานตำรวจแห่งชาติ : Royal Thai Police

<http://www.royalthaipolice.go.th/>



การตั้งค่า 2 Step Login Gmail

บัญชีของฉัน

ควบคุม ปกป้อง และรักษาบัญชีของคุณ ให้ปลอดภัย ทั้งหมดนี้ในที่เดียว

บัญชีของฉันช่วยให้คุณสามารถตั้งค่าได้อย่างรวดเร็ว รวมถึงเครื่องมือที่ช่วยให้คุณปกป้องข้อมูล ปกป้องความเป็นส่วนตัว และเลือกที่จะให้ข้อมูลของคุณทำให้นักการต่างๆ ของ Google ทำงานให้คุณดีขึ้นได้อย่างไร



การลงชื่อเข้าใช้และการรักษาความปลอดภัย

ควบคุมรหัสผ่านและการตั้งค่าการเข้าถึงบัญชี

การลงชื่อเข้าใช้ Google

กิจกรรมบนอุปกรณ์และการแจ้งเตือน
เว็บไซต์และแอปที่เชื่อมต่อ



การตรวจสอบความปลอดภัย

ปกป้องบัญชีของคุณในเวลาเพียงไม่กี่นาที
โดยการตรวจสอบการตั้งค่าความปลอดภัย
และกิจกรรมของคุณ

เริ่มต้นใช้งาน



ข้อมูลส่วนบุคคลและความเป็นส่วนตัว

จัดการการตั้งค่าการเปิดเผยข้อมูลของคุณและข้อมูลที่เรา
ใช้ในการปรับเปลี่ยนประสบการณ์ในแบบของคุณ

ข้อมูลส่วนตัว

ส่วนควบคุมกิจกรรม

การตั้งค่าโฆษณา

ภาพรวม

บัญชีของฉัน

ควบคุม

ติดต่อ

การลงชื่อเข้าใช้และการรักษาความปลอดภัย

กิจกรรมบนอุปกรณ์และการแจ้งเตือน

เว็บไซต์และแอปที่เชื่อมต่อ

ข้อมูลส่วนบุคคลและความเป็นส่วนตัว

ข้อมูลส่วนตัว

ส่วนควบคุมกิจกรรม

การตั้งค่าโฆษณา

ภาพรวมของบัญชี



การตั้งค่าบัญชี

ตั้งค่าภาษา การเข้าถึง และการตั้งค่าอื่นๆ ที่ช่วยคุณใน
การใช้งาน Google

ภาษาและเครื่องมือป้องกันข้อมูล

การเข้าถึง

พื้นที่เก็บข้อมูล Google ไดรฟ์โฟลเดอร์

การลงชื่อเข้าใช้และการรักษาความปลอดภัย

การลงชื่อเข้าใช้ Google

ควบคุมรหัสผ่านและการเข้าถึงบัญชี พร้อมตัวเลือก
การสำรองข้อมูลหากบัญชี ใดสูญหาย

ตรวจสอบให้แน่ใจว่าคุณเลือกที่ผ่านที่ปลอดภัย

รหัสผ่านที่ปลอดภัยควรมีตัวเลข ตัวอักษร และสัญลักษณ์ผสมกัน
เพื่อให้ปลอดภัย ไม่เหมือนกับคำที่ใช้โดยปกติ และจะใช้
สำหรับบัญชีเท่านั้น

รหัสผ่านและวิธีการลงชื่อเข้าใช้

รหัสผ่านช่วยปกป้องบัญชีของคุณ คุณสามารถเพิ่มการป้องกันขั้นที่ 2 ด้วยการ
ยืนยันแบบ 2 ขั้นตอนได้อีกด้วย ซึ่งจะส่งรหัสแบบ ใช้ครั้งเดียวไปยังโทรศัพท์
ของคุณ เพื่อให้คุณผ่านขั้นตอนการลงชื่อเข้าใช้ ดังนั้น แม้จะมีผู้ขโมยรหัสผ่านไป
ก็ยังไม่สามารถเข้าถึงบัญชีของคุณได้

หมายเหตุ: หากต้องการเปลี่ยนการตั้งค่าเหล่านี้ คุณจะต้องยืนยันขั้นผ่าน

รหัสผ่าน

เปลี่ยนแปลงล่าสุด: 30 ตุลาคม 14:48

การยืนยันแบบสองขั้นตอน

ปิด



การตั้งค่า 2 Step Login Facebook

๑๑ ทวีป

ความปลอดภัย

ความเป็นส่วนตัว

โหมไล่และกัก

การเลือก

ภาษา

การแจ้งเตือน

โทรศัพท์มือถือ

ผู้ติดตาม

แอป

โฆษณา

การชำระเงิน

กล่องข้อความการสนทนา...

วิธีใช้

การตั้งค่าความปลอดภัย

เตือนการเข้าสู่ระบบ

การอนุมัติการเข้าสู่ระบบ

ตัวสร้างรหัส

รหัสผ่านแอป

ผู้ติดต่อไวใจ

เบราว์เซอร์และแอปของคุณ

สถานที่ที่คุณเข้าสู่ระบบ

ผู้สืบทอดบัญชี

ปิดใช้งานบัญชีผู้ใช้ของคุณ

รับการเตือนเมื่อมีผู้เข้าสู่ระบบบัญชีผู้ใช้ของคุณจากอุปกรณ์หรือเบราว์เซอร์ใหม่

ไม่ต้องใช้รหัสรักษาความปลอดภัยในการเข้าถึงบัญชีผู้ใช้ของคุณจากเบราว์เซอร์ที่ไม่รู้จัก

บันทึกการเปลี่ยนแปลง

ยกเลิก

ตัวสร้างรหัส

ใช้แอป Facebook ของคุณเพื่อรับรหัสรักษาความปลอดภัยเมื่อคุณต้องการ

รหัสผ่านแอป

ใช้รหัสผ่านพิเศษเพื่อเข้าสู่ระบบแอปของคุณแทนการป้อนรหัสผ่าน Facebook หรือรหัสผ่าน

การอนุมัติการเข้าสู่ระบบคืออะไร

การอนุมัติการเข้าสู่ระบบเป็นการรักษาความปลอดภัยอีกระดับหนึ่งที่ใช้โทรศัพท์ของคุณในการป้องกันบัญชีผู้ใช้ของคุณ

วิธีการทำงาน



เมื่อคุณเข้าสู่ระบบจากเบราว์เซอร์ที่ไม่รู้จัก คุณจะต้องใช้รหัสรักษาความปลอดภัย



คุณจะได้รับรหัสรักษาความปลอดภัยจากโทรศัพท์ของคุณเท่านั้น



การป้อนรหัสนี้เป็น การแสดงว่าคุณสามารถพิสูจน์ได้ว่าผู้กำลังเข้าสู่ระบบคือตัวคุณจริงๆ

เริ่มต้นใช้งาน

ยกเลิก

กับคุณ

เลือกว่าคุณต้องการให้บัญชีผู้ใช้ของคุณพร้อมทำงานอยู่เสมอหรือปิดใช้งานบัญชีผู้ใช้ของคุณ



การตั้งค่า 2 Step Login Facebook

การตั้งค่าความปลอดภัย

เตือนการเข้าสู่ระบบ รับการเตือนเมื่อมีผู้เข้าสู่ระบบบัญชีผู้ใช้ของคุณจากอุปกรณ์หรือเบราว์เซอร์ใหม่ แก้ไข

การอนุมัติการเข้าสู่ระบบ ☐ ต้องใช้รหัสรักษาความปลอดภัยในการเข้าถึงบัญชีผู้ใช้ของฉันจากเบราว์เซอร์ที่ไม่รู้จัก [?] แก้ไข

การส่งรหัสรักษาความปลอดภัยสำรอง

หากคุณไม่สามารถใช้ตัวสร้างรหัสได้ เราสามารถส่งรหัสรักษาความปลอดภัยไปให้คุณทางข้อความในโทรศัพท์ของคุณได้

ดำเนินการต่อ ยกเลิก

การอนุมัติการเข้าสู่ระบบ

ตัวสร้างรหัส

รหัสผ่านแอป

ผู้ติดต่อที่ไว้วางใจ

เบอร์โทรศัพท์และแอปของคุณ

สถานที่ที่คุณเข้าสู่ระบบ

ผู้สืบทอดบัญชี

ตั้งค่าการส่งรหัสรักษาความปลอดภัย

เพื่อให้เราสามารถส่งรหัสรักษาความปลอดภัยไปยังคุณ คุณต้องเพิ่มโทรศัพท์มือถือไปยังไทม์ไลน์ของคุณ

รหัสประเทศ ไทย (+66) ▼

หมายเลขโทรศัพท์ ป้อนหมายเลขของคุณ

ยืนยันหมายเลขโทรศัพท์ ☒ ส่งข้อความ SMS มาให้อิน ☐ โดย

โปรดจำไว้ว่า หากคุณต้องการเปลี่ยนผู้ที่คุณต้องการรับหมายเลขโทรศัพท์ด้วย ให้ไปที่ไทม์ไลน์ของคุณ หากต้องการเปลี่ยนว่าใครสามารถค้นหาคุณได้โดยใช้หมายเลขโทรศัพท์ได้บ้าง ไปที่การตั้งค่าความเป็นส่วนตัวของคุณ ในการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ข้อมูลบนไทม์ไลน์ของคุณ ไปที่นโยบายความเป็นส่วนตัวของเรา

ดำเนินการต่อ ยกเลิก



Question

