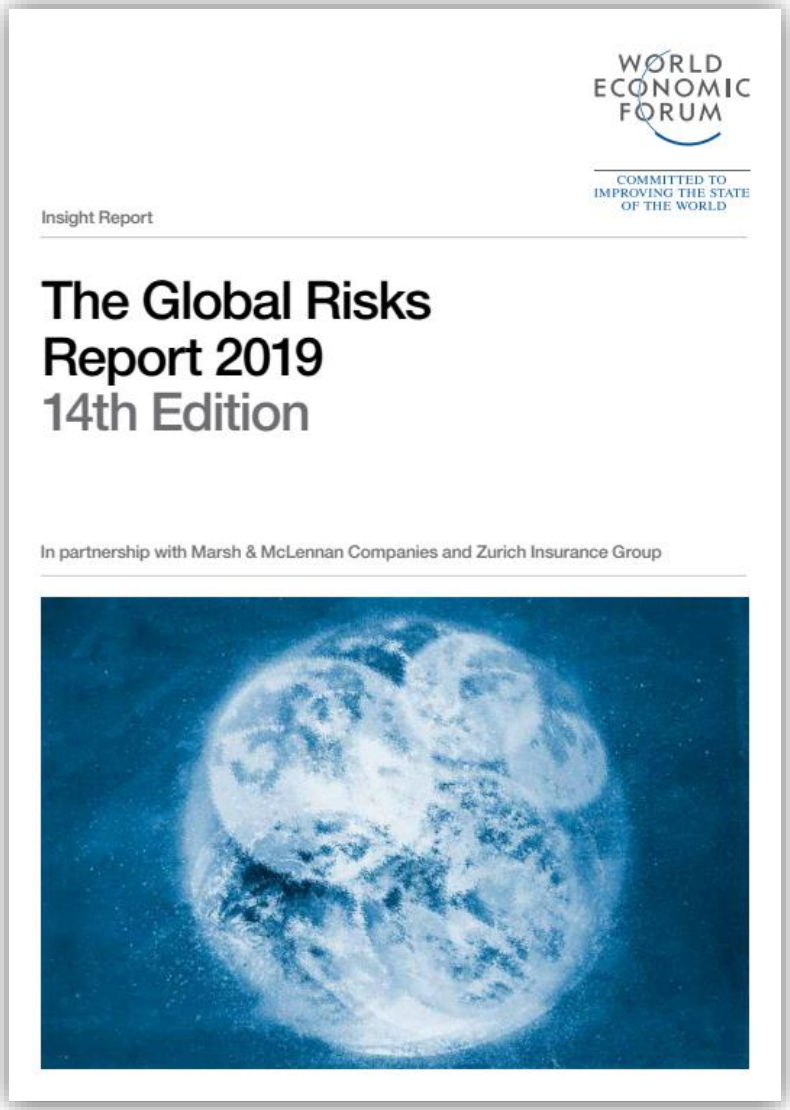
25th ANNIVERSARY
COLLEGE OF MUSIC
MAHIDOL UNIVERSITY
1994-2019

Technological Risk Management



Top 10 risks in terms of **Likelihood**

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

TIMELINE การโจมตีทางไซเบอร์เพื่อ**เรียกค่าไถ**ในประเทศไทย

พ.ย. 2556 — 01 CRYPTOLOCKER

เรียกค่าไถ่ประมาณ
4,000-10,000 บาท

เป็นมัลแวร์เรียกค่าไถ่ที่ระบาดหนักทั่วโลกในช่วงแรกของการแพร่ระบาด จน FBI ออกมาแจ้งเตือน

แพร่กระจาย ผ่านไฟล์แนบอีเมล และ คลิกลิงก์อันตราย

มิ.ย. 2557 — 02 GAMEOVER

สามารถดาวน์โหลด Cryptolocker ลงมาติดตั้งในเครื่อง

พบเหยื่อ **3,400 ราย**

ส.ค. 2557 — 03 SYNOLOCKER

เรียกค่าไถ่ประมาณ
40,000 บาท

สามารถแพร่ระบาดไปยัง NAS และเข้ารหัสลับข้อมูลที่เก็บอยู่บน NAS

ม.ค. 2558 — 04 CTB LOCKER

เรียกค่าไถ่ประมาณ
20,000 บาท

ระบาดในหน่วยงานภาครัฐไทยที่สำคัญหลายแห่ง

ต.ค. 2558 — 05 ARMADA COLLECTIVE

กลุ่มแฮกเกอร์ Armada Collective ข่มขู่ธนาคารทั่วโลกและ **ธนาคารไทย 4 แห่ง** หากไม่จ่ายเงินจะโจมตีเพื่อทำให้ระบบล่ม

เม.ย. 2559 — 06 LOCKY

สามารถเข้ารหัสลับข้อมูลบนเครื่องและอุปกรณ์เก็บข้อมูลแบบพกพา เช่น external harddisk ที่เข้ามาเชื่อมต่อ

เรียกค่าไถ่ประมาณ
30,000-60,000 บาท

พ.ค. 2560 — 07 WANNACRY

ปัจจุบันพบว่ามีเครื่องคอมพิวเตอร์ **มากกว่า 236,902 เครื่องติด WannaCry** ในวันที่ 14 พ.ค. 60 **และลดลงเหลือ 187,635 เครื่อง** ในกว่า 150 ประเทศ ในวันที่ 15 พ.ค. 60 และมีแนวโน้มว่า จะลดลงเรื่อยๆ

เวอร์ชั่น 01
15 พ.ค.2560
เวลา 20.30 น.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ThaiCERT
ETDA
ThaiCERT
ThaiCERT
thaicert.or.th

The Geography of financial attacks by Lazarus group

The malware by Lazarus group, infamous for its theft of $81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.

ภัยคุกคามทางไซเบอร์กับองค์กรธุรกิจไทย

ไทยมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ลำดับที่ 15 ของโลก จาก 165 ประเทศ

41% ขององค์กรธุรกิจไทยได้รับการแจ้งเตือนมากกว่า 5 หมื่น-1.5 แสนรายการ/วัน

60% ของรายการแจ้งเตือนไม่ได้รับการดำเนินการตรวจสอบว่าเป็นภัยคุกคามจริงหรือไม่

54% ขององค์กรธุรกิจไทยได้รับความเสียหายทางการเงินต่อภัยคุกคามไซเบอร์กว่า 16-165 ล้านบาท

36% ขององค์กรธุรกิจไทยได้รับการโจมตีผ่านทางโครงสร้างพื้นฐานในการดำเนินงานมากขึ้น

ที่มา : ซิสโก้ ประเทศไทย

บางกอกโพสต์ กราฟฟิก

เล่น Social Network ให้ปลอดภัย "รู้" ไว้เลี่ยงอันตราย

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

ETDA สพธอ www.etda.or.th

ICT Ministry of Smart Thailand

etda.thailand ThaiCERT thaicert.or.th

1 คิดให้รอบ

สักนิดก่อนโพสต์

เพราะมันเปิดเผยและทุกคนเข้าถึงได้ง่าย
การโพสต์ข้อมูลที่สุ่มเสี่ยงจึงอาจเป็นภัยต่อตัวเอง

2 ระมัดระวัง

ในการคลิกลิงก์

ที่มากับการแชร์ เพราะอาจนำไปสู่ไวรัส
หรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์

3 เข้าโซเชียลเน็ตเวิร์ก พิมพ์ URL โดยตรง

เลี่ยงคลิกลิงก์ เพราะอาจเป็น URL ปลอมหลอกเอาบัญชีใช้งานของเรา
เช่น facebook.com อาจมี URL หลอกเป็น faeebook.com

4 รอบคอบ

ก่อนตอบรับเป็นเพื่อน

คัดกรองคนที่ขอเป็นเพื่อนโดยเข้าไปดูโปรไฟล์ก่อนทุกครั้ง
เพราะอาจมีผู้ไม่หวังดีแฝงมาด้วย

5 ตั้งค่า

ความเป็นส่วนตัว

หลีกเลี่ยงตั้งค่าแบบสาธารณะ
และอนุญาตให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเราได้

6 ไม่แสดงข้อมูล

ส่วนตัวที่เป็นความลับ

เช่น บัตรประชาชน บัตรเครดิต
ไม่ว่าจะอยู่ในรูปแบบข้อความหรือรูปภาพก็ตาม

7 เปิดใช้งาน Do Not Track

ป้องกันการติดตามและเก็บข้อมูลจากผู้ให้บริการโซเชียลเน็ตเวิร์ก
รวมถึงผู้ไม่หวังดีที่เข้ามาขโมยข้อมูล

8 ใช้วิจารณญาณ

ในการรับข่าวสาร

อย่าปักใจเชื่อทันที อาจมีการสร้างกระแส สวมรอย สมอ้างจากผู้ไม่หวังดี

9 ควบคุมการใช้งาน

ของบุตรหลาน

ลองหาเครื่องมือมาเป็นตัวช่วย เช่น Windows Live Family Safety

10 ตระหนักว่าเป็น สังคมเสรี

แม้ทุกคนมีสิทธิ์ในการแสดงความเห็น
แต่การกระทำที่ไม่เหมาะสมก็เป็นเหตุให้ถูกฟ้องร้อง
และศาลก็อาจรับฟังคำร้องด้วย

สถิติภัยคุกคามไซเบอร์ครึ่งปี'62

แจ้งเหตุ **1,083** กรณี

- หลอกลวงออนไลน์ 389 กรณี
- พยายามจะบุกรุกเข้าระบบ 330 กรณี
- เนื้อหาที่เป็นภัยต่อระบบ 112 กรณี
- เจาะระบบได้สำเร็จ 105 กรณี
- เข้าถึง/แก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต 83 กรณี
- โจมตีด้วยมัลแวร์ 61 กรณี

ที่มา : ไทยเซิร์ต (ThaiCERT) สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประชาชาติกราฟิก

Phishing (ฟิชชิง) คือ

การปลอมแปลงอีเมลให้เหมือนว่าส่งมาจากหน่วยงาน องค์กร หรือสถาบันที่มีชื่อเสียง เพื่อหลอกให้เหยื่อหลงกลใส่ข้อมูลสำคัญส่วนตัว จากนั้น ก็จะนำข้อมูลที่ได้จากเราไปสวมรอยสร้างความเสียหายที่เกี่ยวข้องกับเรื่องเงิน

ลักษณะที่น่าสงสัยของฟิชชิงอีเมล

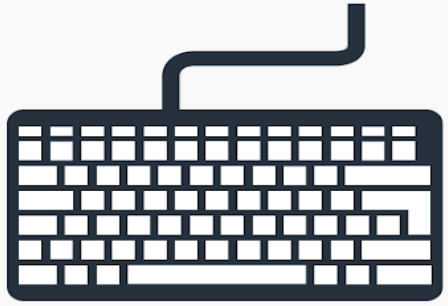
1. อีเมลที่ไม่น่าเชื่อถือ
2. มีไฟล์แนบมาด้วยเช่น .zip
3. ไม่มีการระบุชื่อ-นามสกุล หรือข้อมูลสำคัญ
4. มีคำสะกดผิด
5. มีลิงก์น่าสงสัย
6. มีข้อความแจ้งเตือนว่า ด่วน หรือสำคัญมาก

บัญชีเมลแบบไหนคือเป้าหมาย?

- บัญชีเมลที่ไม่มีการเคลื่อนไหวเกิน 6 เดือน
- บัญชีที่ใช้ล็อกอินหลาย ๆ แอคเคาท์
- บัญชีธุรกิจติดต่องานสำคัญ
- บัญชีที่ไม่เคยเปลี่ยนรหัสผ่าน

Types of Spyware

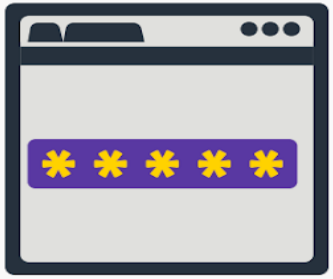
Adware



Keyloggers

Trojans

Mobile Spyware

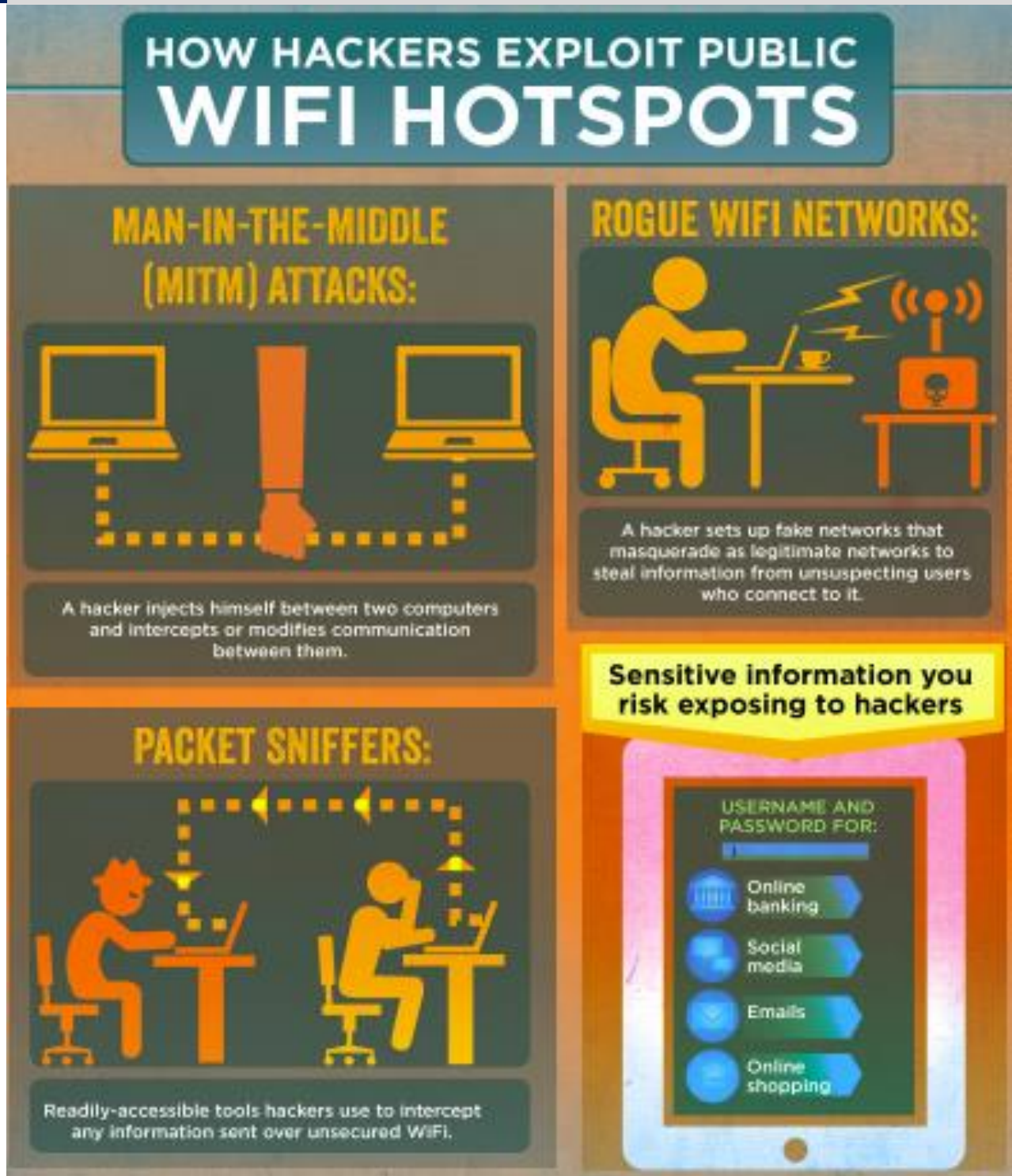


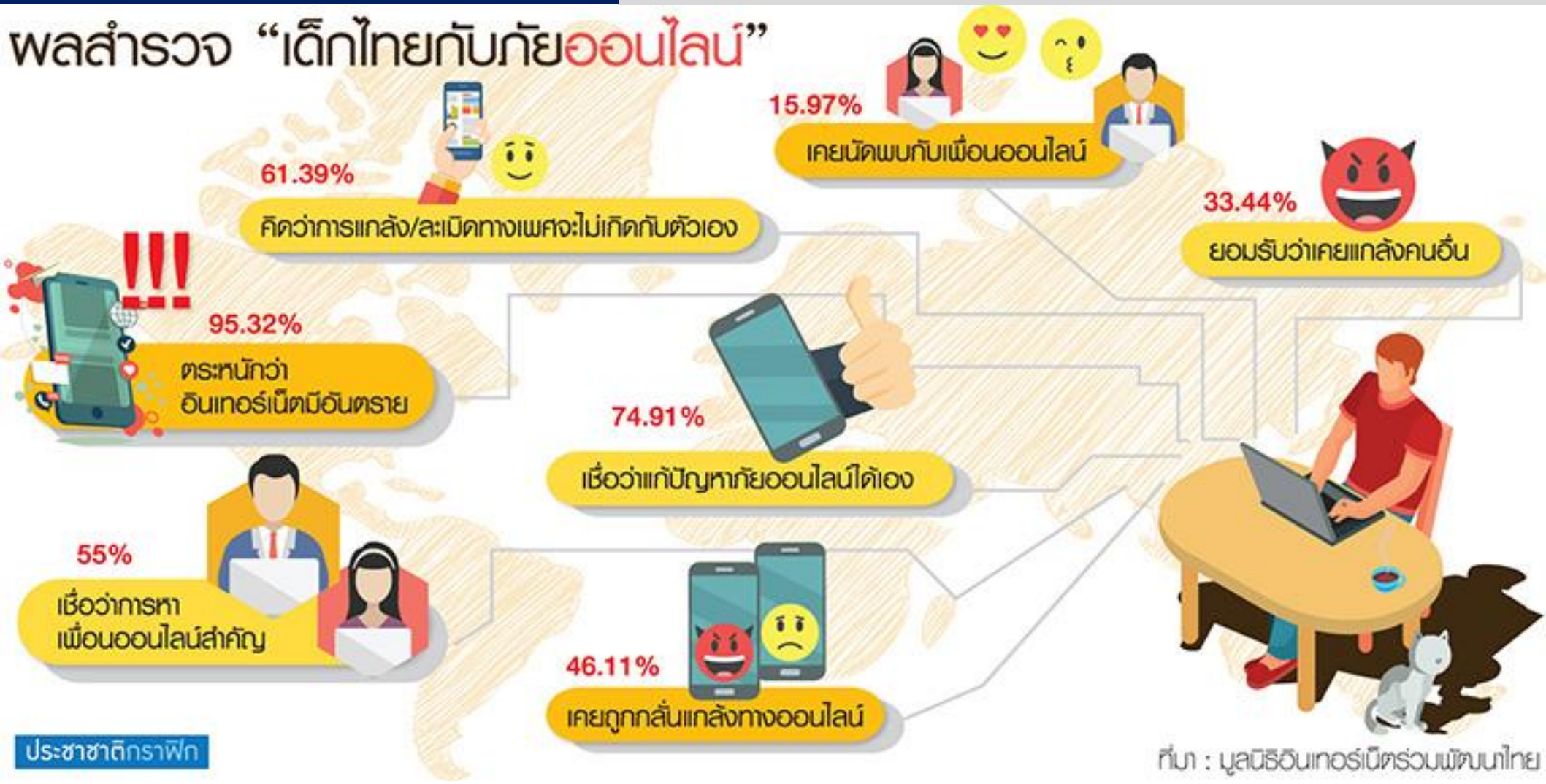
Password Stealers

Technological Risk Management

Case Study : Free Public Wifi Risk

STOP, think twice!




ผลสำรวจ "เด็กไทยกับภัยออนไลน์"
15.97%
เคยนัดพบกับเพื่อนออนไลน์
61.39%
คิดว่าการแกล้ง/ละเมิดทางเพศจะไม่เกิดกับตัวเอง
33.44%
ยอมรับว่าเคยแกล้งคนอื่น
95.32%
ตระหนักว่า
อินเทอร์เน็ตมีอันตราย
74.91%
เชื่อว่าแก้ปัญหาภัยออนไลน์ได้เอง
55%
เชื่อว่าการหา
เพื่อนออนไลน์สำคัญ
46.11%
เคยถูกกลั่นแกล้งทางออนไลน์
ประชาชาติกราฟิก
ที่มา : มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย

นุ๊ก สุทธิดา แจ้งความ ปอท.ถูกคนปลอมเฟซบุ๊ก ไปหลอกคนให้โอนเงินร่วมทำบุญ

ข่าว อาชญากรรม

ไทยรัฐออนไลน์
16 ธ.ค. 2562 15:05 น.

SHARE

โพสต์ แชร์ ไม่คิด ชีวิตใกล้คุก

มาตรา 14 แห่ง พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

ใครโพสต์ข้อมูลอันเป็นเท็จ หรือเรื่องไม่จริงที่ทำให้เกิดความเสียหายทั้งต่อบุคคล ธุรกิจ หรือความมั่นคงของชาติ

ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

ด้วยความปรารถนาดีจากกองบังคับการปราบปราม


FAKE
NEWS


ระวัง!! โพสต์ แชร์ ข่าวปลอม
"เสี่ยงคุก"
1 นำเข้าข้อมูลปลอม
ข่าวปลอม หรือข้อมูลเท็จ
2 เผยแพร่ ส่งต่อ
ข้อมูลเท็จ
ผิด พ.ร.บ.คอมพิวเตอร์
ม.14(1)
ผิด พ.ร.บ.คอมพิวเตอร์
ม.14 (5)
ข่าวปลอม
ข่าวมั่ว
โทษจำคุก 5 ปี
ปรับไม่เกิน 1 แสนบาท
หรือทั้งจำทั้งปรับ
โทษจำคุก 5 ปี
ปรับไม่เกิน 1 แสนบาท
หรือทั้งจำทั้งปรับ
ผิดกฎหมายอาญา ม.328
ฐานหมิ่นประมาทด้วยการโฆษณา
กองปราบปราม
POLICE
3 ร่วมแชร์ ร่วมด่า แสดงความคิดเห็น
ด้วยภาษาที่หยาบคาย
โทษจำคุก 2 ปี
ปรับไม่เกิน 2 แสนบาท

แนวทาง
การรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับบุคคลทั่วไป

1

หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม
ไม่คลิกไฟล์แนบที่ไม่มั่นใจ

2

ไม่ใช้รหัสผ่านชุดเดียวกัน
กับทุกระบบ

3

พิจารณาข้อมูลก่อนการแชร์ต่อ
ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยัน
จากผู้เกี่ยวข้อง

หากต้องการความช่วยเหลือเพิ่มเติม สามารถแจ้งมายัง ThaiCERT
เพื่อประสานการรับมือได้ที่ โทร. 02-123-1212 หรือ อีเมล report@thaicert.or.th

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

ICT
Smart Thailand