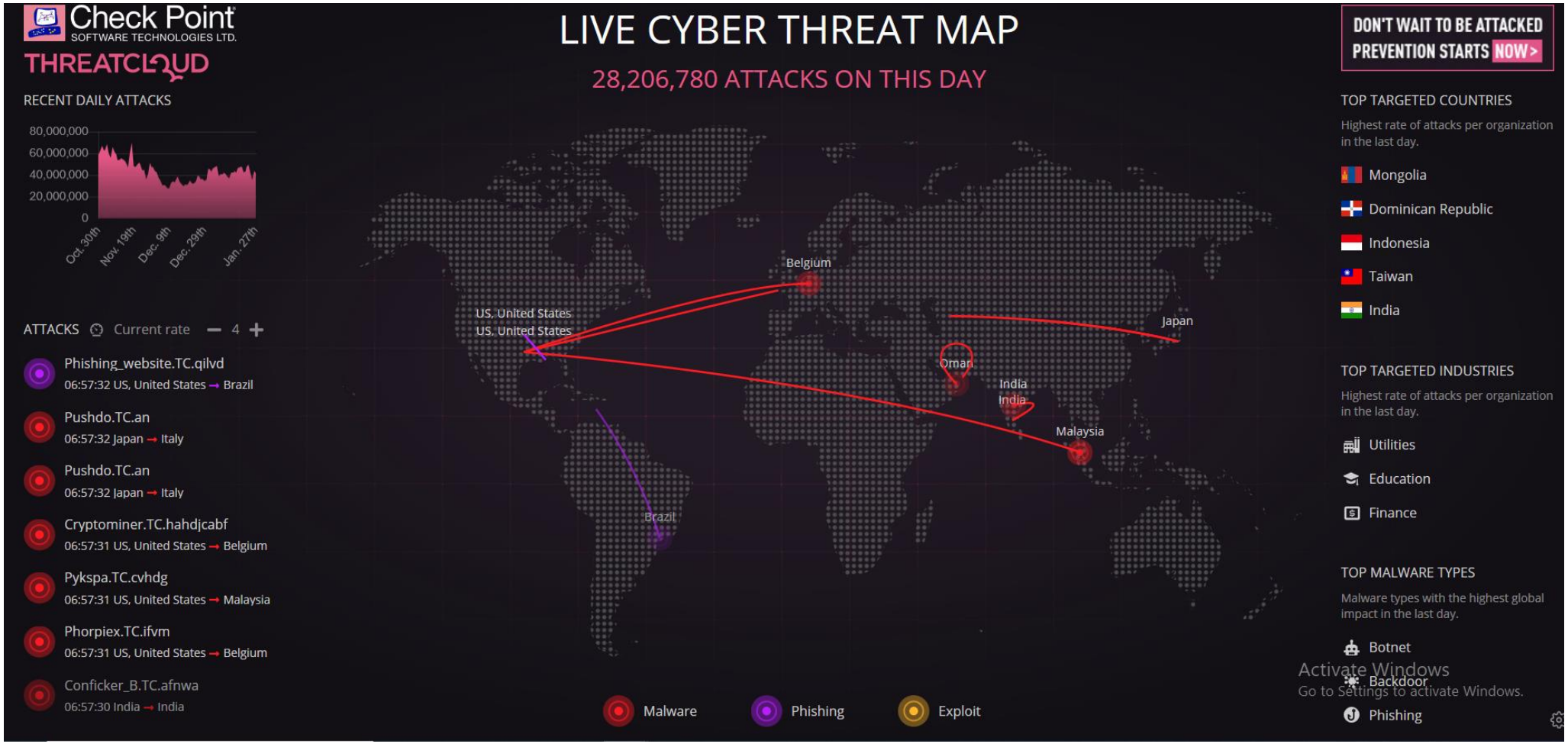
ภัยคุกคามและการป้องกันทางไซเบอร์

- ทุก ๆวินาทีบนโลกออนไลน์
มีผู้ไม่หวังดีคอย Scan ระบบต่าง ๆ อยู่ตลอดเวลาเพื่อหาช่องทางสำหรับทำการโจมตี

Cyber Attack Map



ภัยคุกคามและการป้องกันทางไซเบอร์

แจ้งเหตุภัยคุกคามและ
ช่องทางติดต่อ

สถิติภัยคุกคาม

เอกสารเผยแพร่

สถิติภัยคุกคาม ประจำปี พ.ศ. 2565

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	7	0	1	0	0	0	0	0	0	0	0	0	**8**
Availability	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Fraud	6	9	10	0	0	0	0	0	0	0	0	0	**25**
Information Gathering	0	9	4	0	0	0	0	0	0	0	0	0	**13**
Information Security	1	6	1	0	0	0	0	0	0	0	0	0	**8**
Intrusion Attempts	17	7	6	0	0	0	0	0	0	0	0	0	**30**
Intrusions	23	4	13	0	0	0	0	0	0	0	0	0	**40**
Malicious Code	111	66	201	0	0	0	0	0	0	0	0	0	**378**
Vulnerability	55	52	106	0	0	0	0	0	0	0	0	0	**213**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**220**	**153**	**342**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**715**

ที่มา : thaicert ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย

ภัยคุกคามและการป้องกันทางไซเบอร์

สถิติภัยคุกคาม ประจำปี พ.ศ. 2565

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	7	0	1	0	0	0	0	0	0	0	0	0	**8**
Availability	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Fraud	6	9	10	0	0	0	0	0	0	0	0	0	**25**
Information Gathering	0	9	4	0	0	0	0	0	0	0	0	0	**13**
Information Security	1	6	1	0	0	0	0	0	0	0	0	0	**8**
Intrusion Attempts	17	7	6	0	0	0	0	0	0	0	0	0	**30**
Intrusions	23	4	13	0	0	0	0	0	0	0	0	0	**40**
Malicious Code	111	66	201	0	0	0	0	0	0	0	0	0	**378**
Vulnerability	55	52	106	0	0	0	0	0	0	0	0	0	**213**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**220**	**153**	**342**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**715**

Intrusions = การบุกรุก

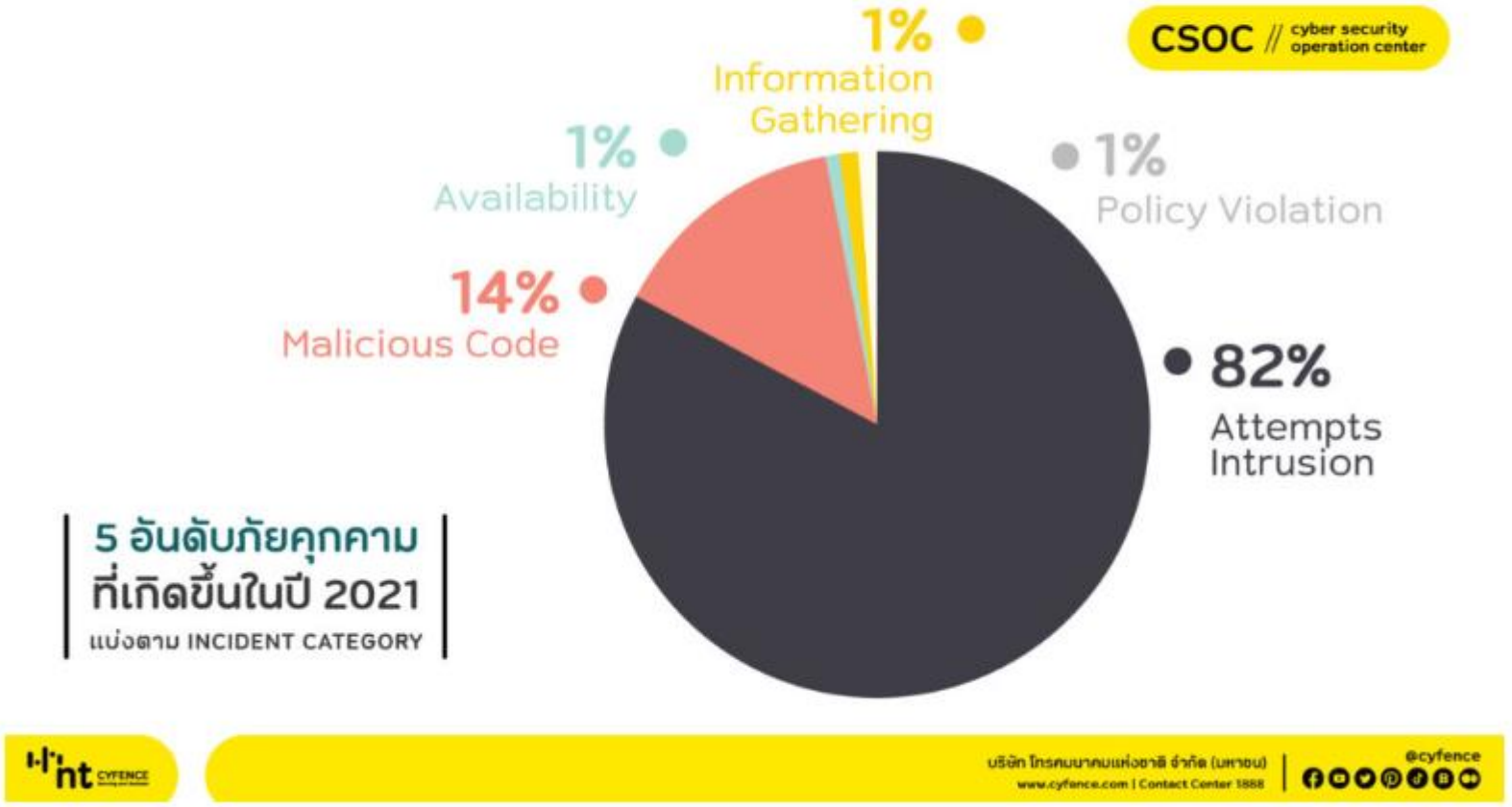
Malicious Code = โค้ดอันตราย คือโปรแกรมที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ ใช้งานหรือระบบโดยปกติภัยคุกคามประเภทนี้ ต้องอาศัยการหลอกลวงให้ผู้ใช้งานเรียกใช้งานโปรแกรมก่อนจึงจะสามารถทำการ โจมตีได้

Vulnerability = การโจมตีช่องโหว่ เช่น ระบบปฏิบัติการ,โปรแกรมต่าง ๆ

ภัยคุกคามและการป้องกันทางไซเบอร์

NT cyfence ผู้ให้บริการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้รวบรวมข้อมูลสถิติภัยคุกคามที่อาจส่งผลกระทบกับระบบ IT จากศูนย์ปฏิบัติการ Cyber Security Operation Center (CSOC) ของ NT cyfence ในปี 2021 ที่ผ่านมา โดยสรุปได้ดังต่อไปนี้

5 อันดับภัยคุกคามแบ่งตามประเภท incident



ประเภทภัยคุกคาม อ้างอิงตามเอกสาร ECSIRT.net project on cooperation and common statics.

ที่มา : NT cyfence

ภัยคุกคามและการป้องกันทางไซเบอร์

รูปแบบการโจมตี

- **Malware หรือ Malicious Software** เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (Virus), วอร์ม (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware)

ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท ตัวอย่างเช่น

Virus: มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

Worm: สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

ที่มา : https://www.it.chula.ac.th/

ภัยคุกคามและการป้องกันทางไซเบอร์

รูปแบบการโจมตี

ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

- **Trojan:** หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย เช่นหลอกว่าเครื่องติดไวรัส ให้ดาวน์โหลดโปรแกรมเพื่อกำจัด

- **Backdoor:** เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว

- **Rootkit:** เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่องพร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

- **Spyware:** แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย

ภัยคุกคามและการป้องกันทางไซเบอร์

รูปแบบการโจมตี

ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

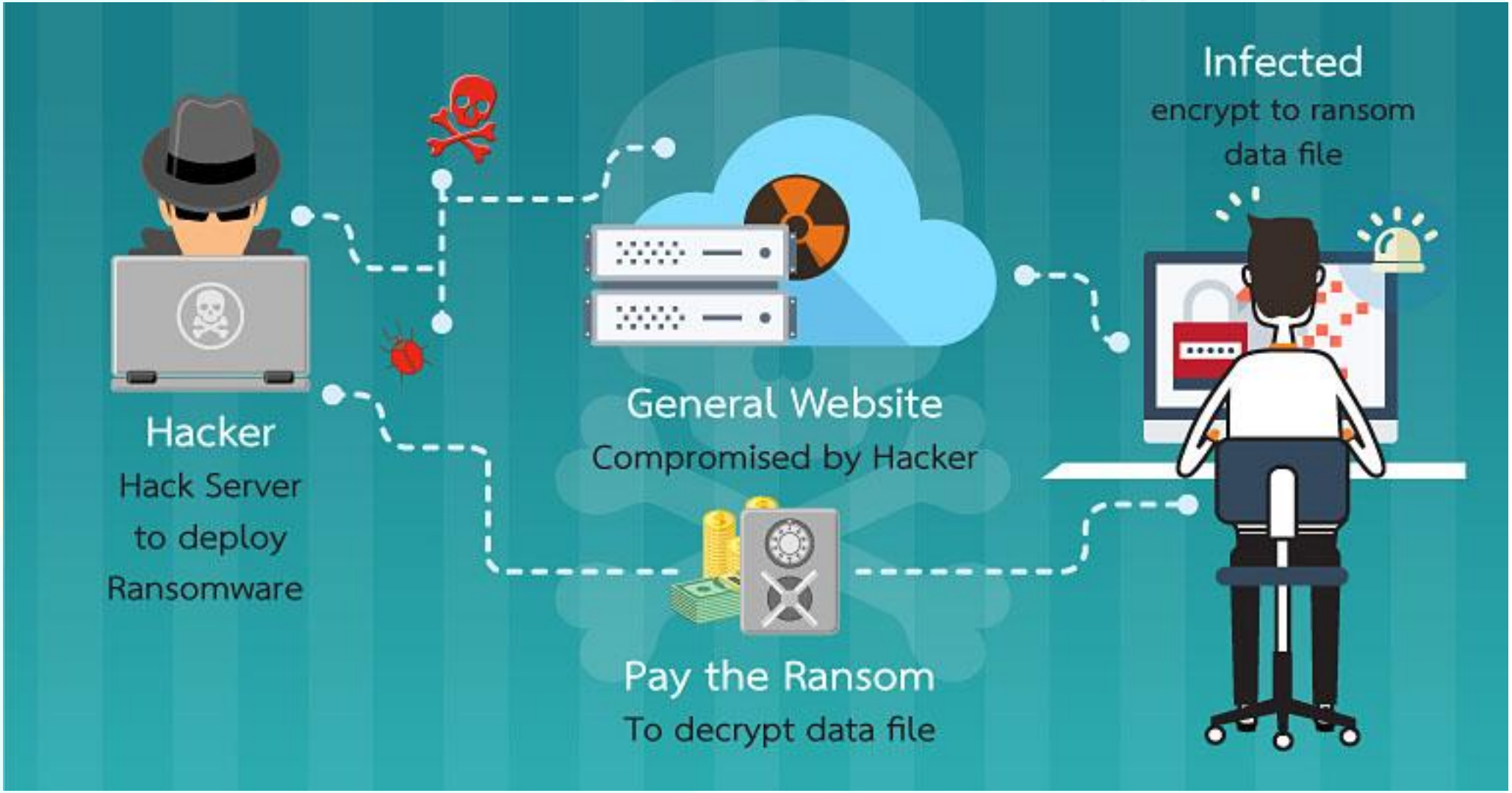
- **Ransomware:** ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

***รูปแบบการโจมตีด้วย **Ransomware เพิ่มสูงขึ้นตลอดเวลา และมีเป้าหมายเป็น**

โรงพยาบาลรัฐฯ เป็นอันดับต้น ๆ

ภัยคุกคามและการป้องกันทางไซเบอร์

รูปแบบการโจมตี



ที่มา : NT cyfence, แค่เข้าเว็บไซต์ อาจจะติด Ransomware

ภัยคุกคามและการป้องกันทางไซเบอร์

ความเสียหาย

แนวโน้มมูลค่าความเสียหายและความเสี่ยงของสถานพยาบาลสูงสุด ซึ่งสูงกว่าสถาบันการเงิน เนื่องจาก

- งบประมาณ
- การให้ความรู้แก่บุคลากร ให้เกิดความตระหนัก

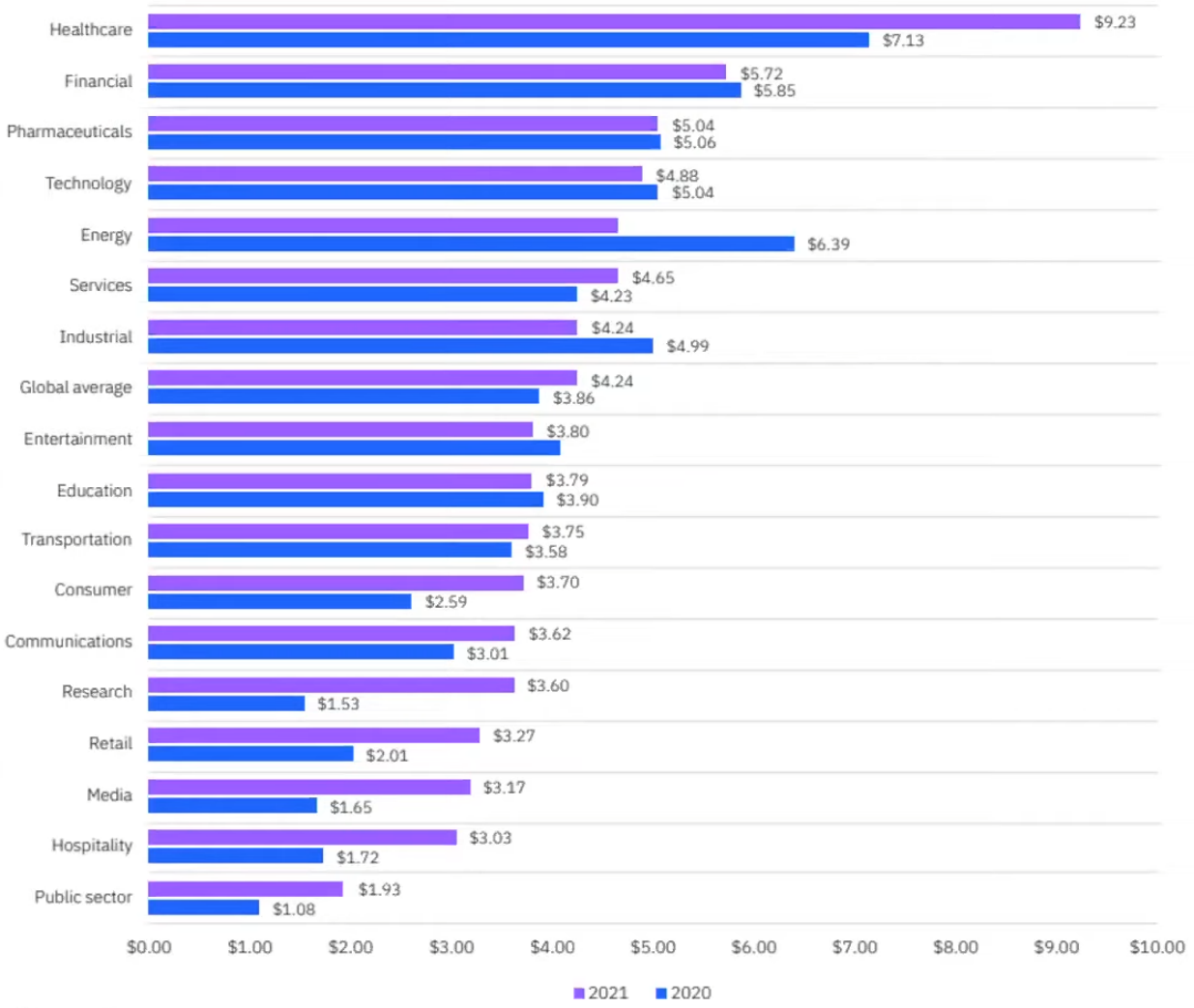
*** หน่วยที่ต้องระวังเป็นพิเศษฯ เช่นการเงิน ,ลิ้งค์ลวง, อีเมล์ลวง

ตัวอย่างความเสี่ยง

- แปะรหัสผ่านไว้หน้าเครื่อง
- ล็อกอินค้างไว้
- การตั้งค่าโปรแกรมให้จำรหัสผ่าน
- การกดลิ้งอันตราย

Average total cost of a data breach by industry

Measured in US$ millions



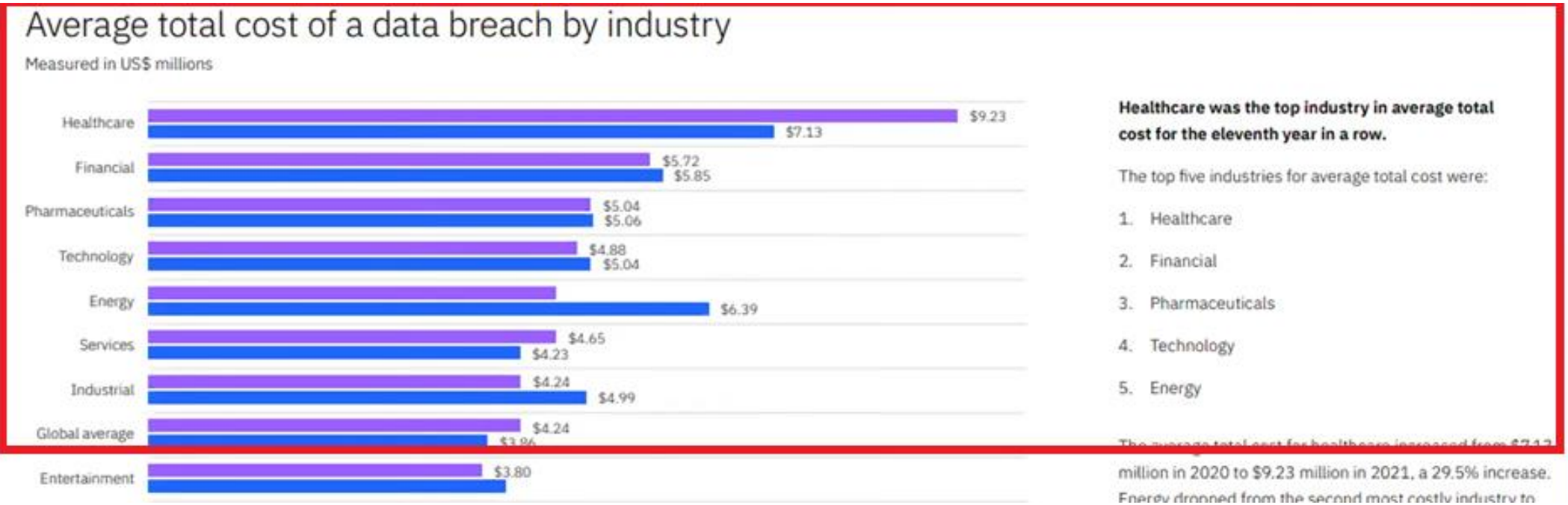
Healthcare was the top industry in average total cost for the eleventh year in a row.

The top five industries for average total cost were:

1. Healthcare
2. Financial
3. Pharmaceuticals
4. Technology
5. Energy

The average total cost for healthcare increased from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Energy dropped from the second most costly industry to fifth place, decreasing in cost from $6.39 million in 2020 to $4.65 million in 2021 (27.2% decrease).

Other industries that saw large cost increases included services (7.8% increase), communications (20.3% increase), consumer (42.9% increase), retail (62.7% increase), media (92.1% increase), hospitality (76.2% increase), and public sector (78.7% increase).


Average total cost of a data breach by industry
Measured in US$ millions
Healthcare
$9.23
$7.13
Financial
$5.72
$5.85
Pharmaceuticals
$5.04
$5.06
Technology
$4.88
$5.04
Energy
$6.39
Services
$4.65
$4.23
Industrial
$4.24
$4.99
Global average
$4.24
Entertainment
$3.80
Healthcare was the top industry in average total cost for the eleventh year in a row.
The top five industries for average total cost were:
1. Healthcare
2. Financial
3. Pharmaceuticals
4. Technology
5. Energy
million in 2020 to $9.23 million in 2021, a 29.5% increase.

ภัยคุกคามและการป้องกันทางไซเบอร์

- ข้อแนะนำในการป้องกันการโจมตีมัลแวร์

1. อัพเดทคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
2. ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
3. ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดร์ฟ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน, ปิดการใช้งาน AutoPlay
4. ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ
5. ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่
6. หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิด

ภัยคุกคามและการป้องกันทางไซเบอร์

- ข้อแนะนำในการป้องกันการติดมัลแวร์
- ติดตามข่าวสารเกี่ยวกับภัยคุกคาม
- ภัยคุกคามอื่น ๆ

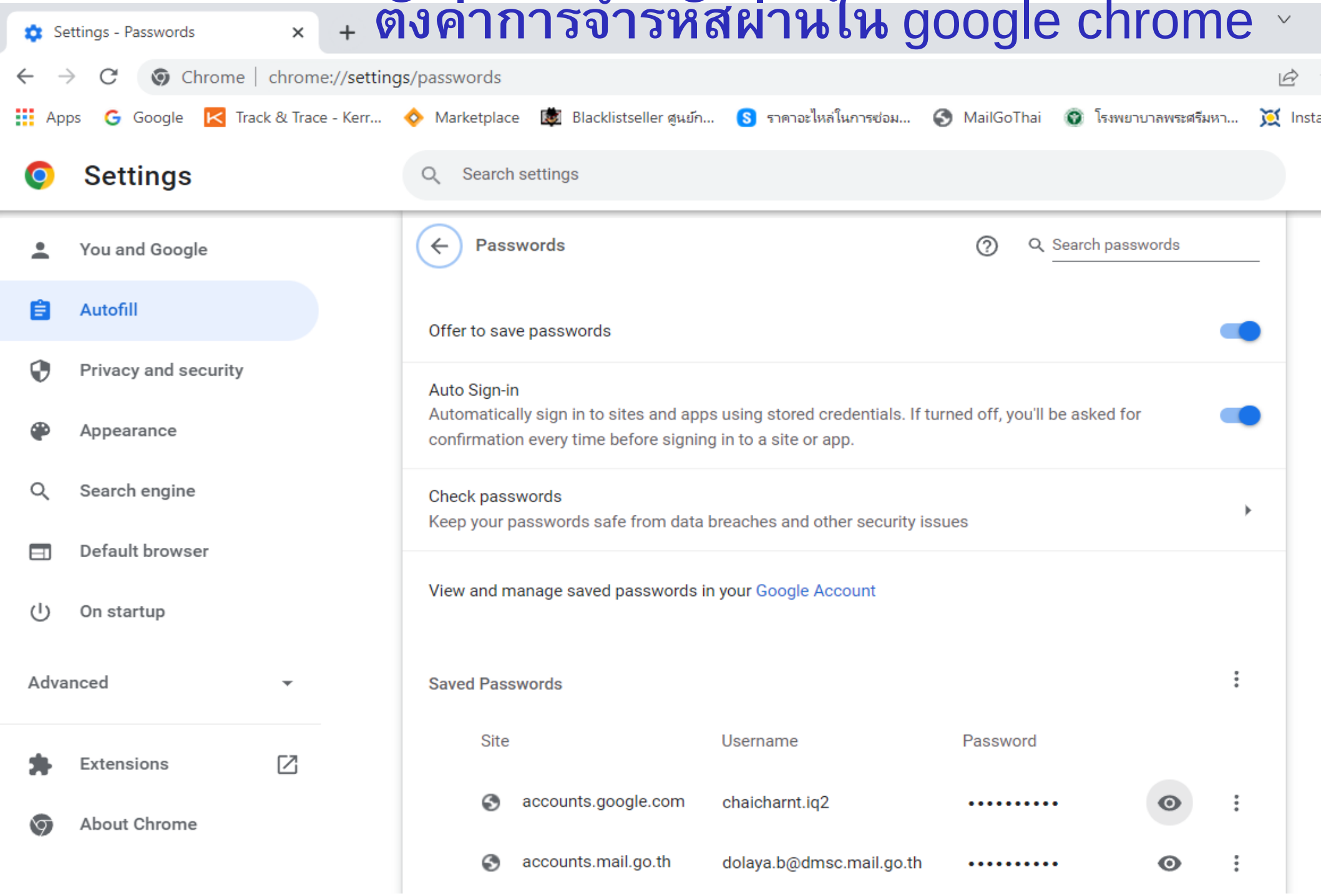
SMS หลอกลวง (มีใครยังไม่เจอบ้าง), ทำ phishing หลอกให้ดาวน์โหลดแอปฯ

แท้จริงเป็นมัลแวร์ขโมยข้อมูลทางการเงิน, Call Center, โฆษณาแฝง ฯลฯ

- สไลด์ CyberSecurity-Awareness.pdf (TDGA)

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล : Thailand Digital Government Academy หรือ TDGA

ตั้งค่าการจำรหัสผ่านใน google chrome



ภัยคุกคามและการป้องกันทางไซเบอร์

ปราการสุดท้าย
(เพื่อป้องกันและแก้ไขเมื่อเกิดเหตุ)

backup (สำรองข้อมูลอยู่เสมอ)ครับสำคัญมาก

Link ข้อมูลน่าสนใจ

ชัวร์ก่อนแชร์ ภัยไซเบอร์ : เทรนด์ 2022 แนวโน้มภัยไซเบอร์ (ตอนที่ 1) กับ อ.ปริญญา หอมเอนก
https://www.youtube.com/watch?v=yne0SOP9XH4

ชัวร์ก่อนแชร์ ภัยไซเบอร์ : เทรนด์ 2022 แนวโน้มภัยไซเบอร์ (ตอนที่ 2) กับ อ.ปริญญา หอมเอนก
https://www.youtube.com/watch?v=GNiUDwaW6P4

4 Cybersecurity Trends 2022 ในภาคธุรกิจ ที่น่าจับตามอง
https://www.youtube.com/watch?v=2HR-wEJWHZw

TechTalk x ACIS Webinar: Cybersecurity & Privacy Threats and Trends 2022 - YouTube

บทความ IT Security (cyfence.com)

https://www.beartai.com/article/tech-article/1014091
ระวังตัว!! กลลวงเว็บปลอมใหม่เช็กแค่ลิงก์คงไม่พอ เนียนยันช่อง URL

https://blog.cloudhm.co.th/what-is-malware/
Malware คืออะไร? ป้องกันยังไงไม่ให้ถูกโจมตี?


ถาม-ตอบ
ขอบคุณครับ

PASSWORD
พาสเวิร์ด
รหัสผ่าน

ตั้งให้ยาก
จำให้ได้
ไม่แชร์กับใคร
อย่าใช้ซ้ำทุกบัญชี

••••••••••

อย่างน้อย
ควรมี ***8 ตัวอักษร***

เดายาก
ไม่เป็นคำจากพจนานุกรม

ไม่ใช้ซ้ำกัน
ในบัญชีต่าง ๆ

112233

ไม่เป็นตัวเลข
หรือตัวอักษร***เรียงกัน***
หรือซ้ำกัน เช่น abcd1111

ใช้การ***ยืนยัน 2 ขั้นตอน***
หรือหลายขั้นตอน

ไม่ใช้พาสเวิร์ดหรือ
default password
ที่ตั้งค่ามาตั้งแต่แรก

ระวังอีเมลฟิชชิง
หลอกให้เปลี่ยนพาสเวิร์ด
โดยให้คลิกลิงก์

ไม่ใช้ข้อมูลส่วนตัว
เช่น วันเดือนปีเกิด
เบอร์โทร.

พิจารณา***ใช้งาน***
ซอฟต์แวร์ช่วยจัดการ
พาสเวิร์ด

ThaiCERT ETDA

เวอร์ชัน 01
22 มิ.ย. 2561

แบ็กอัปข้อมูลไว้ก่อน
เพราะถ้าหายไป เสียเงินเท่าไร... ก็อาจไม่ได้คืนมา

รู้มั้ย? **34%** (1)
ของคนทั่วโลกเคยสูญเสียข้อมูล

ในปี 2560
กว่าล้านคนถูกโจมตี ด้วยมัลแวร์เรียกค่าไถ่ (2)

ซึ่งจะล็อกข้อมูลในเครื่อง เช่น เอกสาร รูปภาพ ทำให้เปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่
และแม้จ่ายค่าไถ่ไปแล้วก็**ไม่ได้รับประกัน**ว่าจะได้ข้อมูลนั้นคืนมา

แบ็กอัปแบบไหน...ถามใจเธอดู?

วิธีเก็บ	ข้อดี	ข้อเสีย
บริการ Cloud เช่น Google Drive, Dropbox, OneDrive	ใช้ง่าย ฟรี เข้าถึงได้ทุกที่ แบ็กอัปอัตโนมัติได้	ต้องมีอินเทอร์เน็ต มีความเสี่ยงนโยบายบริการ
อุปกรณ์เก็บข้อมูลแบบพกพา เช่น DVD, ฮาร์ดดิสก์, Flash Drive	ใช้ง่าย เก็บรักษาในที่ปลอดภัย พกติดตัวได้	มีโอกาสสูญหายหรือเสียหาย
พิมพ์เป็นกระดาษ	ไม่ขึ้นกับฮาร์ดแวร์ ป้องกันการถูกเจาะข้อมูล	จัดการยาก ไม่ดีต่อสิ่งแวดล้อม
NAS (Network Attach Storage)	เก็บข้อมูลจากคอมพิวเตอร์หลายเครื่อง พร้อมกันได้ แบ็กอัปอัตโนมัติได้	ต้องติดตั้งและดูแลระบบ ราคาสูง มีโอกาสเสียหาย

(1) : https://www.acronis.com/en-us/blog/posts/acronis-world-backup-day-survey-results
(2) : https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf

NAS (Network Attach Storage)
* คือ อุปกรณ์ที่ให้บริการกันและแชร์ข้อมูลแก่เครื่องลูกข่ายในเครือข่ายเดียวกัน

ข้อมูลเพิ่มเติม ศึกษาได้ที่
www.thaicert.or.th / www.etda.or.th

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ThaiCERT ETDA

ThaiCERT ThaiCERT thaicert.or.th