
การสร้างความตระหนักรู้
ด้านความมั่นคงทางไซเบอร์
CyberSecurity
Awareness
ศูนย์เทคโนโลยีดิจิทัล
IT DTAM

หัวข้อการนำเสนอเพื่อการป้องกันและเรียนรู้

1. CyberSecurity คืออะไร ?
2. ความรู้พื้นฐานของ CyberSecurity
3. รูปแบบภัยคุกคามของ CyberSecurity
4. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
Department of Thai Traditional and Alternative Medicine

ศูนย์เทคโนโลยีดิจิทัล
IT DTAM

CyberSecurity

CyberSecurity

หรือ ความมั่นคงปลอดภัยทางไซเบอร์คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึง วิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจาก เป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้าง ความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

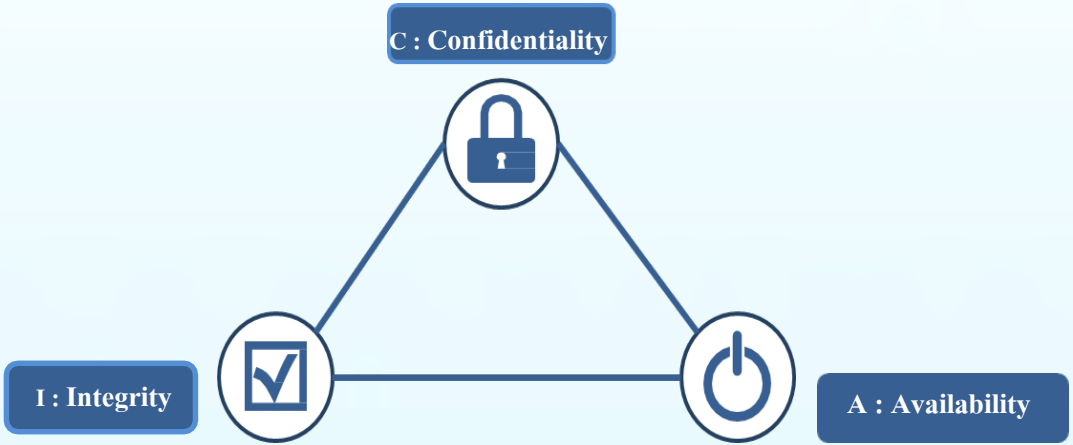
ให้ไว้ ณ วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

1. พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. พ.ร.บ ว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
3. พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
4. มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
Department of Thai Traditional and Alternative Medicine
ศูนย์เทคโนโลยีดิจิทัล
IT DTAM

ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



ประกอบด้วย 3 ส่วน คือ

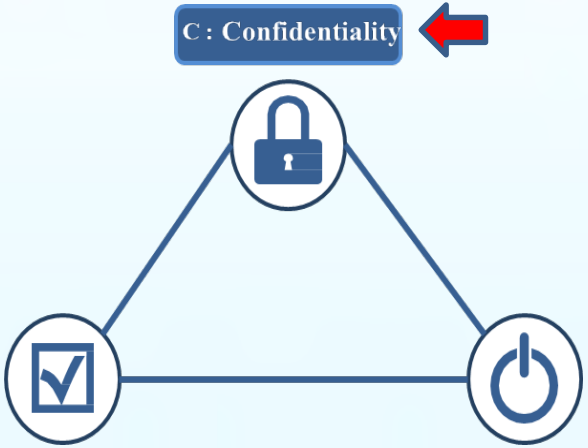
1. Confidentiality
2. Integrity
3. Availability

ส่วนที่ 1 Confidentiality

Confidentiality หรือ การรักษาความลับของข้อมูล

คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

ตัวอย่างเช่น



- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น

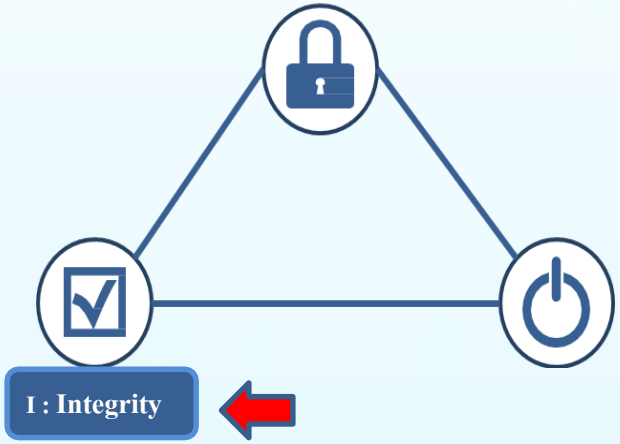
  ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

ส่วนที่ 2 Integrity

Integrity หรือ การรักษาความถูกต้องของข้อมูล

คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มี ความถูกต้องอย่างต่อเนื่อง เช่น

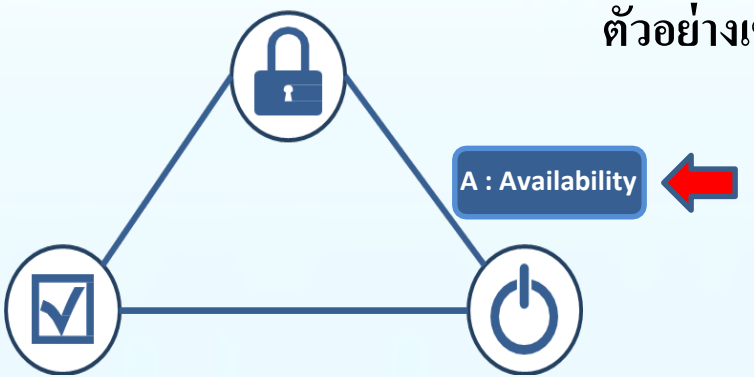
- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



ส่วนที่ 3 Availability

Availability หรือ ความพร้อมใช้งานของข้อมูล

คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา
รักษาความต่อเนื่องในการ ให้บริการข้อมูล
ตัวอย่างเช่น



- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ CyberSecurity

ภัยคุกคาม สามารถแบ่งออกได้หลายรูปแบบ แต่ละประเภทของภัยคุกคามก็จะแตกต่างกัน ศูนย์เทคโนโลยีดิจิทัล กรมการแพทย์แผนไทยและการแพทย์ทางเลือก จึงได้รวบรวมภัยคุกคามทางไซเบอร์ที่พบบ่อย ได้ดังต่อไปนี้

ศูนย์เทคโนโลยีดิจิทัล
IT DTAM
กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
Department of Thai Traditional and Alternative Medicine

รูปแบบภัยคุกคามประเภทที่ 1

Malware

Malware มาจากคำว่า “**Malicious**” ผสมกับ “**Software**”

หรือที่คนส่วนใหญ่จะเรียกกันว่า “ไวรัส” นั่นเอง ภัยคุกคามประเภทนี้ มักแฝงตัวมากับไฟล์ที่เราดาวน์โหลดจากเว็บไซต์ อีเมล หรือจากอุปกรณ์เสริมที่เชื่อมต่อเข้ากับคอมพิวเตอร์ **Ransomware** เองก็ถือว่าเป็นหนึ่งในประเภทของ **Malware** ด้วย ซึ่งหากมี **Malware** อยู่ในคอมพิวเตอร์แล้ว ก็จะสามารถสร้างความเสียหายได้มากเลยทีเดียว ไม่ว่าจะเป็นการทำลายข้อมูล หรือแม้แต่การเข้าควบคุมระบบของคุณ

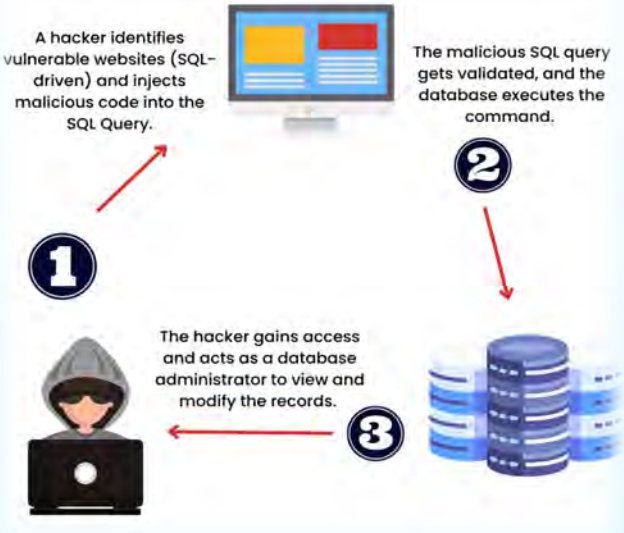
รูปแบบภัยคุกคามประเภทที่ 2

Phishing

Phishing คือ ภัยคุกคามทางอีเมล แน่นอนว่าคนส่วนหนึ่งจะเรียนรู้ความอันตรายของ Malware กันไปแล้ว ก็จะมีความระมัดระวังตัวมากขึ้นในเกิดเปิดไฟล์แปลกปลอม ดังนั้นอาชญากรไซเบอร์ จึงพัฒนารูปแบบไปอีกขั้น รูปแบบการโจมตีนี้ จะแสร้งมาในรูปแบบของอีเมลจากบุคคลที่สามารถไว้วางใจหรือสั่งการได้ เช่น ผู้บริหาร หรือองค์กรที่น่าเชื่อถือ ทั้งรูปแบบของภาครัฐ หรือเอกชน พร้อมแนบไฟล์ที่ฝัง Malware ไว้ อาจมีข้อความแจ้งคุณว่า พบการฉ้อโกงเกิดขึ้นกับบัญชีของคุณ แนะนำให้กรอกข้อมูล หรือเปิดไฟล์บางอย่าง เพื่อให้คุณติดกับและติดตั้ง Malware นั่นเอง

รูปแบบภัยคุกคามประเภทที่ 3

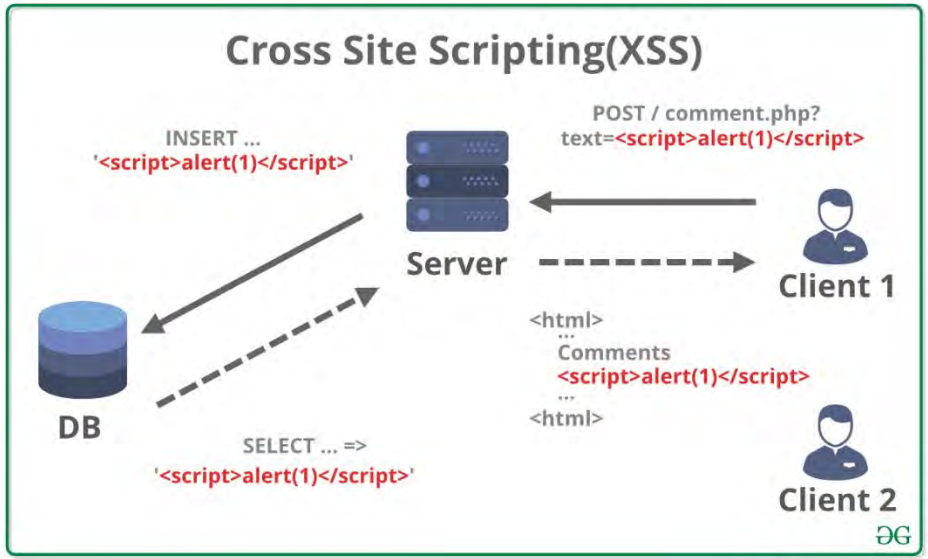
SQL Injection Attacks



ระบบ SQL นั้นถูกสร้างมาเพื่อจัดระบบฐานข้อมูลขององค์กร ซึ่งหากอาชญากรไซเบอร์โจมตีไปยังระบบนี้ผ่านเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ จะส่งผลกระทบที่มีความเสียหายมากกับระบบเซิร์ฟเวอร์โดยตรง ซึ่งภัยคุกคามประเภทนี้ ถือว่าเป็นปัญหาที่ส่งผลกระทบร้ายแรงกับองค์กร เนื่องจากภายในเซิร์ฟเวอร์ของแต่ละองค์กร มักจะมี “ฐานข้อมูลส่วนบุคคลของลูกค้า” “หมายเลขบัตรเครดิตและระบบการเงิน” ซึ่งการโจมตีแบบนี้อาจส่งผลระยะยาวได้ หากไม่มีการรับมือที่ทันท่วงที

รูปแบบภัยคุกคามประเภทที่ 4

Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS)

คือ เป็นการโจมตีผู้เข้าใช้บริการเว็บไซต์ โดยอาชญากรไซเบอร์จะใช้วิธีใส่โค้ดที่เป็นอันตรายลงในช่องทางที่ผู้ใช้งานเว็บไซต์จะต้องเปิด หรือฝังลิงก์ไปยัง JavaScript ภายในเว็บไซต์ ซึ่งถึงแม้ว่าการโจมตีรูปแบบนี้ จะไม่สร้างความเสียหายให้กับเว็บไซต์และเซิร์ฟเวอร์ แต่กลับมีผลต่อชื่อเสียงและความน่าเชื่อถือของเว็บไซต์และองค์กรเป็นอย่างมาก

รูปแบบภัยคุกคามประเภทที่ 5

Web application attacks

Web application attacks

คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น • Code ของเว็บไซต์ เช่น CMS • Web Server หรือ DatabaseServer วิธีการโจมตีที่นิยมใช้ •Cross-Site Scripting • SQL Injection • Path Traversal สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten. Spam.

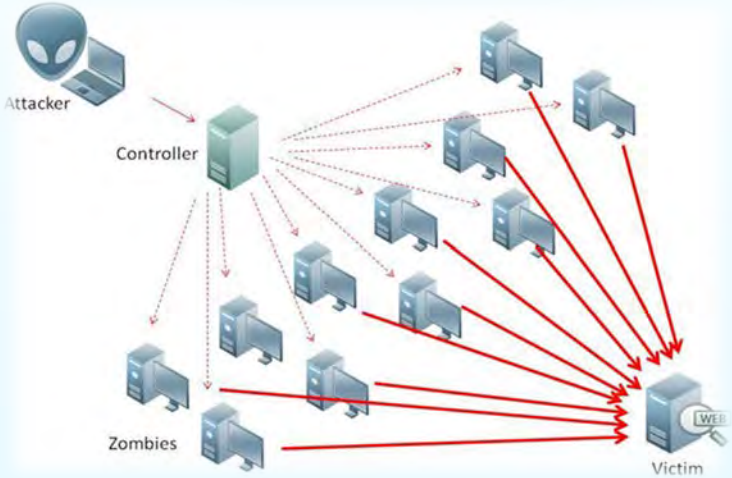
รูปแบบภัยคุกคามประเภทที่ 6

Spam

สแปม (Spam) คือ การส่งอีเมลที่มีข้อความโฆษณาไปให้โดยไม่ได้รับอนุญาตจากผู้รับ การสแปมส่วนใหญ่ทำเพื่อการโฆษณาเชิงพาณิชย์ มักจะเป็นสินค้าที่น่าสงสัย หรือการเสนองานที่ทำให้รายได้อย่างรวดเร็ว หรือบริการที่ก้ำกึ่งผิดกฎหมาย ผู้ส่งจะเสียค่าใช้จ่ายในการส่งไม่มากนัก แต่ค่าใช้จ่ายส่วนใหญ่จะตกอยู่กับผู้รับอีเมลนั้น

รูปแบบภัยคุกคามประเภทที่ 7

DDoS



Distributed Denial of Service หรือ DDoS

คือ การโจมตีทางไซเบอร์รูปแบบหนึ่ง โดยมีรูปแบบการโจมตี คือ แฮกเกอร์จะทำการส่ง Traffic หรือคำขอเข้าถึงข้อมูลจากหลากหลายที่ไปยังเว็บไซต์ที่ต้องการโจมตีพร้อม ๆ กัน ทำให้เว็บไซต์นั้นมีปริมาณ Traffic มากเกินกว่าที่ Server จะสามารถรองรับได้ ส่งผลให้เว็บไซต์ไม่สามารถใช้งานได้ หรือที่นิยมเรียกกันว่าเว็บไซต์ล่มนั่นเอง

รูปแบบภัยคุกคามประเภทที่ 8

Data Breach

Data Breach คือ การละเมิดข้อมูล การที่ข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต โดยสามารถทำลายธุรกิจและผู้บริโภคได้หลายวิธี อีกทั้งยังมีค่าใช้จ่ายราคาแพงในการกู้ข้อมูลกลับคืนมา ซึ่งอาจทำลายชีวิตและชื่อเสียงของบริษัทนั้นหรือของบุคคลนั้นได้ หลายคนอาจจะเคยได้ยินเรื่องการละเมิดข้อมูล ในข่าวโดยเฉพาะในต่างประเทศ แต่ก็ไม่ใช่เรื่องที่น่าแปลกใจอะไร เพราะเมื่อเทคโนโลยีก้าวหน้ามากขึ้น ข้อมูลของเราก็ได้เคลื่อนไปสู่โลกของดิจิทัลมากขึ้นทำให้การโจมตีทางไซเบอร์เป็นเรื่องที่ใกล้ตัว และต้องเตรียมการถูกโจรกรรมข้อมูลให้มีความปลอดภัยสูง

รูปแบบภัยคุกคามประเภทที่ 9

Insider Threat

Insider Threat เป็น ภัยคุกคามทางไซเบอร์ ที่เกิดจากบุคคลภายในองค์กร ที่แบ่งออกได้เป็น 3 ประเภท คือ

-ภัยที่เกิดจากการประมาทโดยไม่ได้ตั้งใจของพนักงาน

-ภัยที่เกิดจากการขโมยตัวตนหรือข้อมูลพนักงานที่ทำให้แฮกเกอร์เจาะเข้าระบบได้

-ภัยจากตัวบุคคลที่ต้องการจะบ่อนทำลายองค์กรจากภายใน

รูปแบบภัยคุกคามประเภทที่ 10

Botnet

Botnet คือ กลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ ในบ้านของเรา เพื่อรอรับคำสั่งจากแฮ็กเกอร์ โดยแฮ็กเกอร์จะนำ Botnetที่มีไปใช้ในแคมเปญการโจมตีขนาดใหญ่ เช่น DDoS อย่างกรณีของ MiraiBotnet ที่โด่งดังเมื่อ 2 ปีก่อน ซึ่งใช้ Botnet กว่า 300,000 เครื่องในการถล่มระบบของ Netflix, Twitter หรือ Reddit

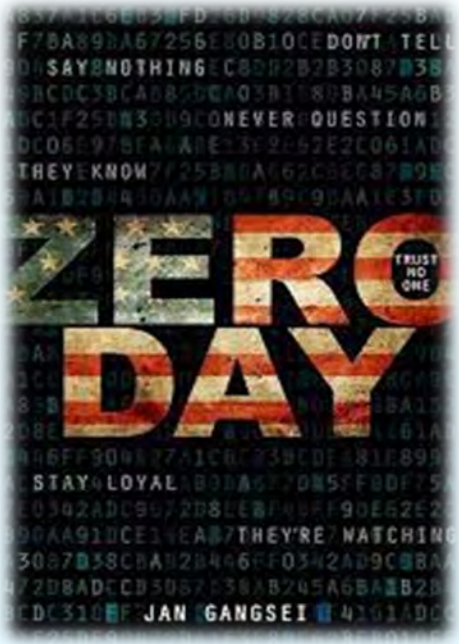
รูปแบบภัยคุกคามประเภทที่ 10

Ransomware

Ransomware เป็น มัลแวร์ (Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

รูปแบบภัยคุกคามประเภทที่ 11

Zero-Day



Zero-Day หรือ 0-Day คือชื่อเรียกช่องโหว่หรือจุดอ่อนในระบบคอมพิวเตอร์ประเภทหนึ่ง ซึ่งเกิดขึ้นจากความผิดพลาดในขั้นตอนการออกแบบและพัฒนาระบบ ที่ผู้พัฒนาไม่สามารถตรวจสอบพบก่อนนำระบบนั้นมาใช้งานจริง เมื่อมีผู้พบช่องโหว่ในขณะที่ระบบถูกนำไปใช้งานแล้ว ผู้พัฒนาระบบจึงมีเวลาน้อยมากในการสร้างส่วนแก้ไขมาเพื่อปิดช่องโหว่ จึงถูกเรียกว่า Zero-Day **(ศูนย์วัน)**

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

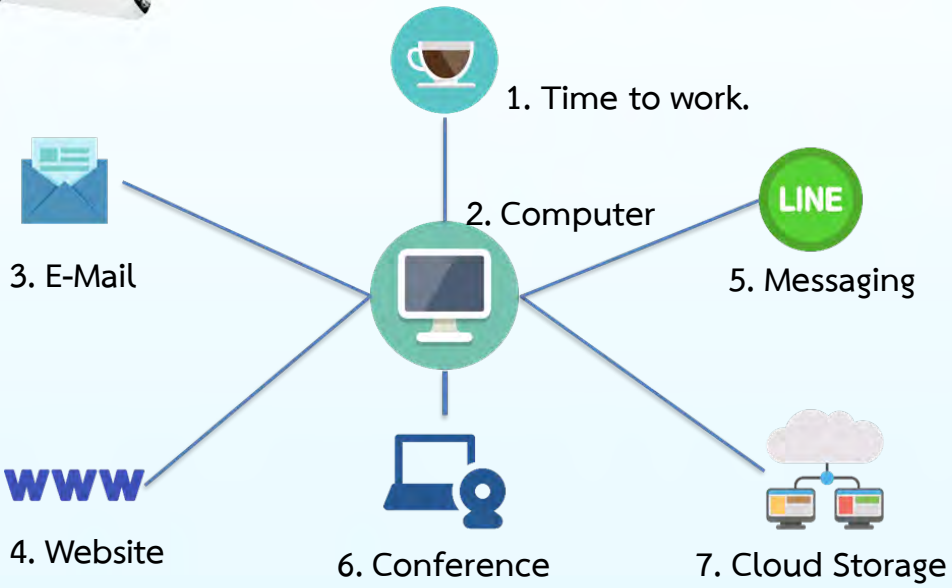
วันทำงาน (Workday)

วันพักผ่อน (Rest day)

กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
Department of Thai Traditional and Alternative Medicine

ศูนย์เทคโนโลยีดิจิทัล
IT DTAM

วันทำงาน (Workday)



Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Password

การใช้ Password ที่ดี คือ

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ
2. มีความยาวของ Password อย่างน้อย 8-10 ตัวอักษร
3. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดา ได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์
4. มีการเปลี่ยน Password อย่างสม่ำเสมอ อย่างน้อย 3 เดือน/ครั้ง
5. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
6. ไม่ควรบอก Password แก่ผู้อื่น

Password

ควรหลีกเลี่ยงการใช้ Common password หรือ Defaultpassword หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์

Source : https://www.springnews.co.th/news/infographic/833905

Password

กราฟแสดงระยะเวลาในการถอดรหัสผ่าน

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS > Learn how we made this table at hivesystems.io/password

Source : https://www.netsec.news/how-long-does-it-take-a-hacker-to-brute-force-a-password-in-2023/

เหตุผลที่ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด,หมายเลขโทรศัพท์

E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
3. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

ตัวอย่าง E-mail ปลอม

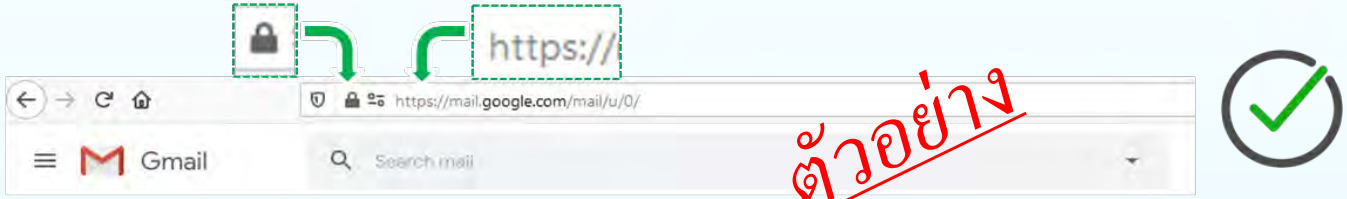
Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่าง ๆ
2. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser
3. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome firefox เป็นต้น
5. ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ
6. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing
7. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

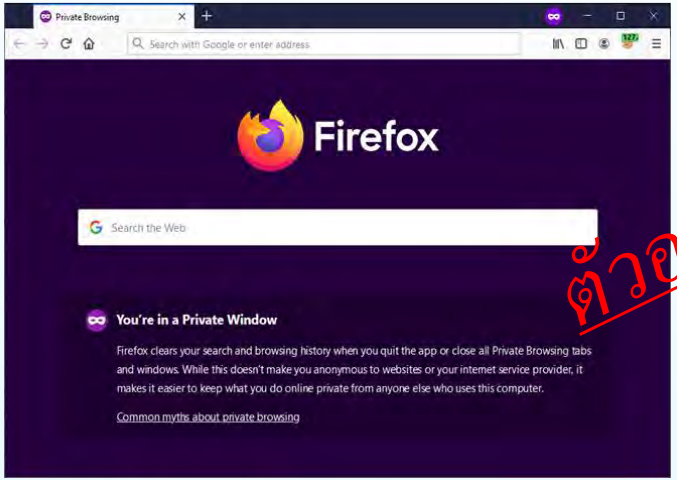
Website

เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญ
ต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

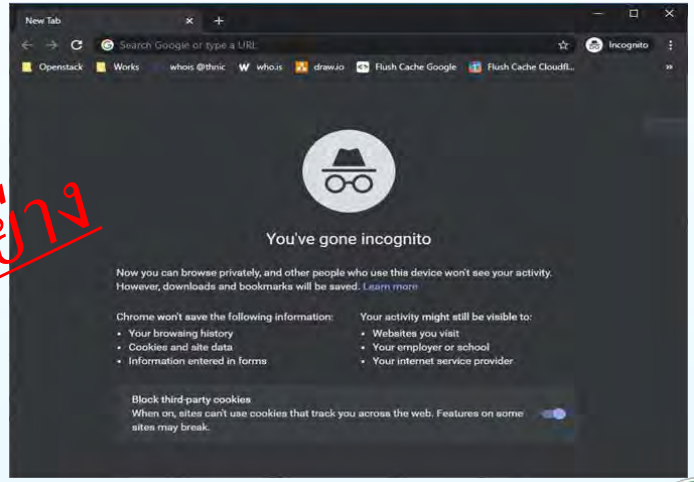


Website

ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing



ตัวอย่าง



Firefox คือ Private Windows

Google Chrome คือ Incognito mode หรือ โหมดแบบไม่ระบุตัวตน

Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

ห้ามบันทึกรหัสผ่านไว้

1.ไม่ควรบันทึก Password ไว้ที่โปรแกรม

2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

3. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

4. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

5. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

Fake News หรือ ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจาก ข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้ อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการ กระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตุข่าวปลอม

- มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
- ระบุที่มาของข่าวไม่ได้
- มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
- สำนวนการเขียนออกแนวการโฆษณา

Fake News

ตัวอย่าง

Source :https://www.antifakenewscenter.com/

Line Official Account

ชนิดของบัญชี LINE Official Account

บัญชี LINE เพื่อธุรกิจมีทั้งหมด 3 แบบโดยสามารถดูได้จากสีที่แตกต่างของสีโล่

บัญชีทั่วไป

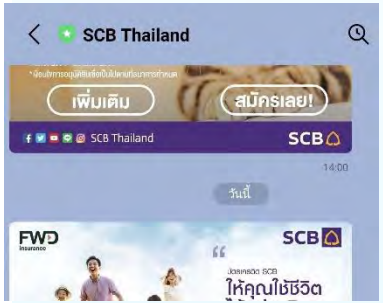
บัญชีโล่สีเทา ที่ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มต้นใช้งาน ซึ่งสามารถอัปเกรดบัญชี เป็นบัญชีรับรองหรือบัญชีพรีเมียมได้ในภายหลัง

บัญชีรับรอง

บัญชีโล่สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหาธุรกิจได้ง่ายขึ้นทั้งบน LINE และ Search engine ต่างๆ โดยมีค่าใช้จ่ายในการดำเนินการ 888 บาท ตลอดอายุการใช้งาน

บัญชีพรีเมียม

บัญชีโล่สีเขียว ที่เหมาะสำหรับธุรกิจหรือองค์กร ขนาดใหญ่ ที่ต้องการสร้างฐานผู้ติดตามเป็นหลักล้าน สามารถค้นหาเจอได้ง่าย
และใช้งานสปอนเซอร์สติกเกอร์ และจะต้องมีใช้จ่ายขั้นต่ำตามที่กำหนด



ที่มา https://lineforbusiness.com/th/service/line-oa-features

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ในการใช้งาน

1. ใช้สถานที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชร์เอกสารต่าง ๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น ZOOM, Microsoft Teams, Google Meet, Webex เป็นต้น
5. มีการอัพเดทเวอร์ชั่นของโปรแกรม Conference อย่างสม่ำเสมอ

เพิ่มเติม : ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการ ประชุม

Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. แยก User ในการใช้งานของแต่ละบุคคล
2. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
5. มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

วันพักผ่อน (Rest day)

1. Computer

2. Internet Connection

2. Mobile

4. IoT Devices

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Internet Connection

FREE WIFI

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

IoT Devices

IoT Devices คือ

อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สรุป

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

ในปัจจุบันเทคโนโลยีถูกพัฒนาให้ทันสมัย สะดวกสบายในการใช้งาน จนบางครั้งลืมคิดถึงเรื่องความปลอดภัยในชีวิตและทรัพย์สินของผู้บริโภค ดังนั้นหากจะกล่าวให้ถูกต้องควรมีความปลอดภัยที่มากขึ้นมาพร้อมกับความสดวกสบายที่ตามมา