บันทึกข้อความ

ส่วนราชการ กลุ่มวางโครงการ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร. ๑๓๘๓

ที่ กษ ๐๘๐๔.๐๕/๒๓ **วันที่** ๓๐ สิงหาคม ๒๕๖๗

เรื่อง ขอรายงานผลการพัฒนาความรู้จำนวน ๒ เรื่อง

เรียน ผอ.สวพ. ผ่าน ผอ.กวค.

ตามแบบกำหนดและประเมินผลสัมฤทธิ์ของงาน ปีงบประมาณ ๒๕๖๗ รอบการประเมินครั้งที่ ๒ ได้กำหนดให้ระดับความสำเร็จของการพัฒนาความรู้ เป็นหนึ่งในตัวชี้วัดผลงาน โดยมีค่าเป้าหมายให้มีการพัฒนาทักษะด้านดิจิทัล ๑ เรื่อง ครบถ้วนตามเงื่อนไขของหลักสูตร และพัฒนาความรู้ ๑ เรื่อง นั้น

บัดนี้ กระผมได้ดำเนินการพัฒนาความรู้ครบถ้วนตามเงื่อนไขหลักสูตรแล้ว จำนวน ๒ เรื่อง โดยได้ฝึกอบรมในหลักสูตร “การสร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ CyberSecurity Awareness” จัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และ การพัฒนาความรู้ในงานวันสถาปนากรมพัฒนาที่ดิน ๒๕๖๗

ในการนี้กระผมจึงขอส่งหลักฐานการผ่านการฝึกอบรมดังกล่าว ตามเอกสารที่ได้แนบมาพร้อมนี้

๑. สรุปบทเรียนจากการฝึกอบรมหลักสูตร “การสร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ CyberSecurity Awareness”
๒. ประกาศนียบัตรผ่านการฝึกอบรมด้วยระบบบการเรียนออนไลน์ในบทเรียน “การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ CyberSecurity Awareness“
๓. หนังสือขอแจ้งรายชื่อผู้ที่ผ่านการพัฒนาความรู้ในงานวันสถาปนากรมพัฒนาที่ดิน ๒๕๖๗

จึงเรียนมาเพื่อโปรดทราบและพิจารณา

ธนภัทร งามดี
(นายธนภัทร งามดี)
วิศวกรโยธาชำนาญการ

- ทราบ
- ดำเนินการตามเสนอ (ลงชื่อ)

(นายวีระพงษ์ พิกุลประยงค์)
ผู้อำนวยการกลุ่มวางโครงการ

(นายธนากร นาเชียงใต้)
ผู้อำนวยการสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล TDGA THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ธนภัทร งามดี

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 29 ส.ค. 2567

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

74d0e32e

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2024-08-29T18:56:23.429+07:00
Reason: Confirm Certificate

บันทึกข้อความ

ส่วนราชการ กองการเจ้าหน้าที่ กลุ่มพัฒนาบุคคล โทร. ๑๒๑๓

ที่ กษ ๐๘๐๒/๒๒๙๕ **วันที่** ๒๙ พฤษภาคม ๒๕๖๗

เรื่อง ขอแจ้งรายชื่อผู้ที่ผ่านการพัฒนาความรู้ในงานวันสถาปนากรมพัฒนาที่ดิน ๒๕๖๗

เรียน ผอ.กอง/ผอ.สำนัก/ผอ.สพข. ๑-๑๒/ศูนย์

ตามที่กรมฯ เห็นชอบในกิจกรรม KPI ตามตัวชี้วัด “ระดับความสำเร็จของการพัฒนาความรู้” ของข้าราชการ โดยสามารถนำการชมนิทรรศการภายในงานวันสถาปนากรมพัฒนาที่ดิน วันที่ ๒๓ พฤษภาคม ๒๕๖๗ มาใช้เป็นการรายงานผลการพัฒนาความรู้ได้ ๑ เรื่อง นั้น

กองการเจ้าหน้าที่ จึงขอแจ้งรายชื่อผู้ที่ผ่านการพัฒนาความรู้ในงานวันสถาปนากรมพัฒนาที่ดิน เมื่อวันที่ ๒๓ พฤษภาคม ๒๕๖๗ เพื่อใช้เป็นข้อมูลประกอบการพิจารณาการรายงานผลตามตัวชี้วัด “ระดับความสำเร็จของการพัฒนาความรู้” ของข้าราชการรายบุคคล ในรอบการประเมินที่ ๒/๒๕๖๗ ตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ และแจ้งข้าราชการในสังกัดท่านทราบ

(นางกิติยา มงคลเกตุ)
ผู้อำนวยการกองการเจ้าหน้าที่

ลำดับที่	ชื่อ-นามสกุล	ประเภท
205	สุจิตรา ไทยเทศ	ข้าราชการ
206	อรอนงค์ โฉมศิริ	ข้าราชการ
207	อลีนา รัตนไพโรจน์	ข้าราชการ
208	อัจจิมา พงษ์จินดา	ข้าราชการ
209	ตวงทิพย์ หอมวิวรรธน์	พนักงานราชการ
210	นันทิกานต์ แก้วมา	พนักงานราชการ
211	พรรณนิชชา น้อยเจริญ	พนักงานราชการ
212	พัฒนาวดี บุญชื่น	พนักงานราชการ
	สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน	
213	ชานนท์ ทับสุข	ข้าราชการ
214	ไชยยุทธ ลียะวณิช	ข้าราชการ
215	ณฐพล ลิ้มสกุล	ข้าราชการ
216	ดนุ เนียมฤทธิ์	ข้าราชการ
217	ธนภัทร งามดี	ข้าราชการ
218	ธีศิษฏ์ ฐิติโชติรัตนา	ข้าราชการ
219	พงศกร สุวรรณวิโก	ข้าราชการ
220	พรรณี พะโยม	ข้าราชการ
221	ศรวิทย์ วรรธนะสาร	ข้าราชการ
222	ศิลปทัต โอพิทักษ์ชีวัน	ข้าราชการ
223	สุรินทร์ พันธ์สิงห์	ข้าราชการ
224	อรอุมา แสงรอดรัตน์	ข้าราชการ
225	กัลยรัตน์ โรจนโพธิ์	พนักงานราชการ
226	จุฬาลักษณ์ สุขแต้ม	พนักงานราชการ
	กองสำรวจดินและวิจัยทรัพยากรดิน	
227	กรรณิการ์ หอมยามเย็น	ข้าราชการ
228	จารุณี หนูมาก	ข้าราชการ
229	เฉลิมชัย แสงทองพินิจ	ข้าราชการ
230	ชญาดา วงศ์พรประทีป	ข้าราชการ
231	ซิตีฮาวา นุวันนา	ข้าราชการ
232	ดนัย แสนจันทอง	ข้าราชการ
233	ธนากร บั้งเงิน	ข้าราชการ
234	ธมลวรรณ คงไชย	ข้าราชการ
235	ธีรนุช โอภาชาติ	ข้าราชการ
236	นฤกมล จันทร์จิราวุฒิกุล	ข้าราชการ
237	ปภาวี สุขพิทักษ์	ข้าราชการ
238	ปิยภัทร นิ่มสนิท	ข้าราชการ

สรุปบทเรียนเรื่อง "การสร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ CyberSecurity Awareness"

ชื่อ - นามสกุล : นายธนภัทร งามดี ตำแหน่ง วิศวกรโยธาชำนาญการ

หน่วยงาน : กลุ่มวางโครงการ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

หัวข้อการพัฒนา : การสร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ CyberSecurity Awareness

ผู้บรรยาย : คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้าสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิธีการพัฒนา : พัฒนาความรู้ผ่านระบบออนไลน์ (TDGA E-learning) ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy หรือ TDGA

1.เนื้อหาโดยสังเขป

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (CyberSecurity Awareness)

1.1 Cybersecurity คืออะไร

1.2 ความรู้พื้นฐานของ Cybersecurity

1.3 รูปแบบภัยคุกคามของ Cybersecurity

1.4 ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

1.1 Cybersecurity คืออะไร

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาตในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

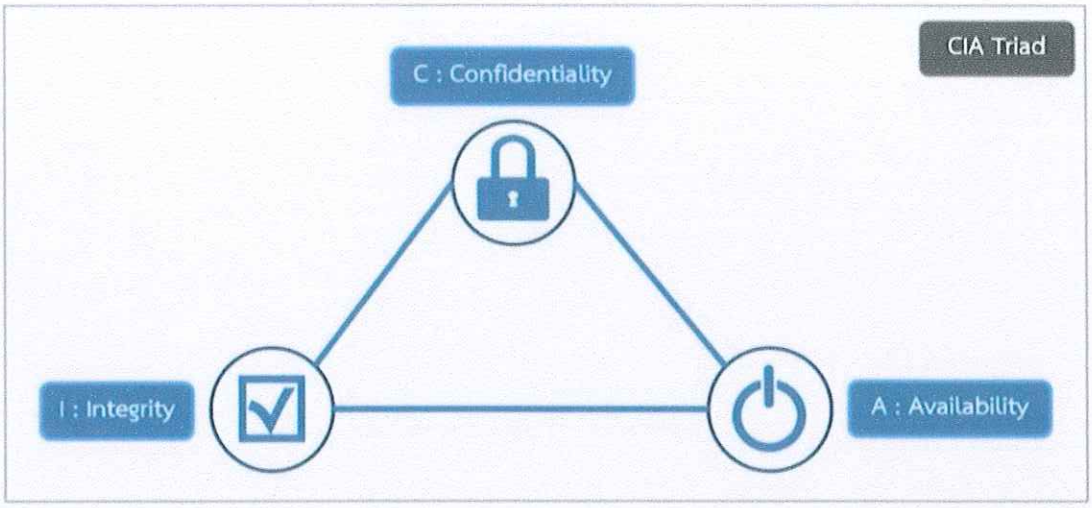
กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.บ ว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

1.2 ความรู้พื้นฐานของ Cybersecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (CIA Triad)



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

1.3 รูปแบบภัยคุกคามของ CyberSecurity

ตัวอย่างภัยคุกคามของ CyberSecurity เช่น

- Malware
- Web-based attacks
- Phishing
- Web application attacks

- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

1) Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส(Virus) เวิร์ม (Worms) และ โทรจัน (Trojans)

2) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

3) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทางSocial โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

4) Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL Injection
- Path Traversal

5) Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน

6) DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการหรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

7) Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

<u>ผลกระทบ</u>

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

8) Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

<u>วิธีการป้อง</u>

นำหลักการ Zero Trust มาใช้งานภายในองค์กร

9) Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

10) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่องรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

<u>วิธีการป้องกัน</u>

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

11) Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacke

1.4. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1) การใช้งานคอมพิวเตอร์

- ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
- ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

2) การใช้ Password ที่ดี

- มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
- มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
- ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password 123456 วันเกิด หมายเลขโทรศัพท์
- มีการเปลี่ยน Password อย่างสม่ำเสมอ
- ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก Password แก่ผู้อื่น

3) การใช้ E-mail

- ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
- เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

4) การใช้ Website

- ไม่เข้าเว็บไซที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
- ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
- เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน

HTTPS เท่านั้น

- ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
- ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
- ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
- ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

5) **การใช้ Messaging**

- ไม่ควรบันทึก Password ไว้ที่โปรแกรม
- กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
- มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
- มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

6) **Fake News หรือ ข่าวปลอม** เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตุข่าวปลอม

- มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
- ระบุที่มาของข่าวไม่ได้
- มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
- สำนวนการเขียนออกแนวการโฆษณา

7) **การใช้ Conference**

- ใช้สถานที่เหมาะสมกับการ Conference
- ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
- แชร์เอกสารต่างๆ อย่างระมัดระวัง
- ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
- มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ
- ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

8) **การใช้ Cloud Storage**

- แยก User ในการใช้งานของแต่ละบุคคล
- ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

- ปิดการเข้าถึงไฟล์ หรือปิดการแชไฟล์เมื่อไม่มีความจำเป็น
- ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

9) การใช้ WIFI

- ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
- หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

10) การใช้ Mobile

- เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
- ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- กำหนด Application permission ให้เหมาะสม
- มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

11) การใช้ Internet Connection

- เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
- เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
- กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

2. ประโยชน์ที่ได้รับ

มีความรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน และมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่างๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

3. แนวคิดในการนำไปใช้การพัฒนางานของตนเอง และหน่วยงาน

นำความรู้ที่ได้รับไปถ่ายทอดให้บุคลากรในหน่วยงานให้ตระหนักและรับรู้ถึงความสำคัญ CyberSecurity Awareness นำวิธีการใช้งาน และวิธีป้องกันไปใช้งาน เพื่อลดความเสี่ยงต่อภัยคุกคามหรือข้อผิดพลาดที่อาจเกิดขึ้นในการทำงานของพนักงาน เพิ่มความปลอดภัย สร้างความมั่นใจให้กับผู้ใช้บริการ และหน่วยงานที่ทำงานร่วมกัน