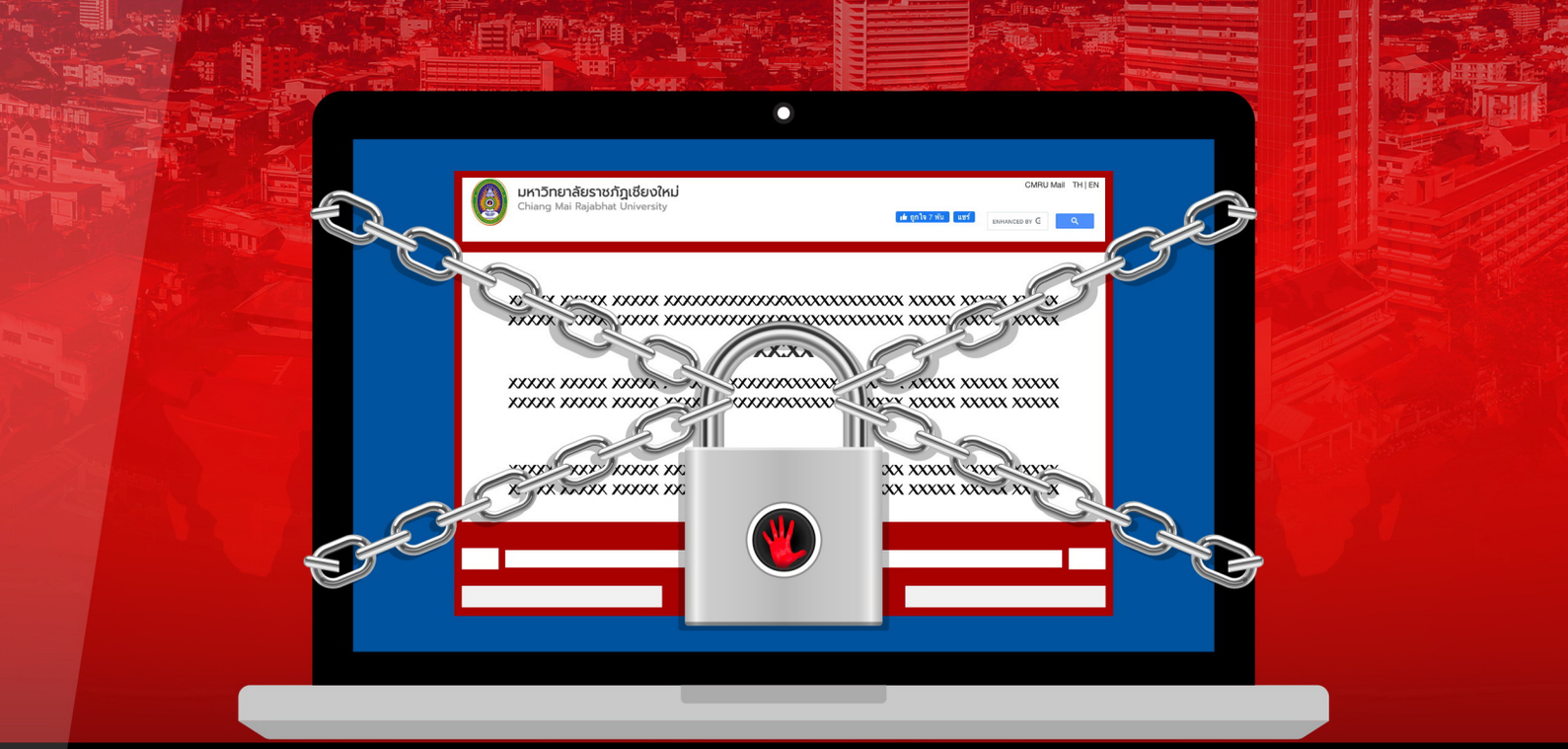


รายงาน

สรุปผลการดำเนินงาน การจัดการความรู้ (KM)

ประจำปีงบประมาณ พ.ศ. 2564

DIGITAL EDUCATION

สำนักดิจิทัลเพื่อการศึกษา
มหาวิทยาลัยราชภัฏเชียงใหม่

www.digital.cmru.ac.th

รายงานสรุปผลการดำเนินงาน

การจัดการความรู้ ประจำปีงบประมาณ พ.ศ. 2564

สำนักดิจิทัลเพื่อการศึกษา

โดย

คณะกรรมการจัดการความรู้

สำนักดิจิทัลเพื่อการศึกษา

มหาวิทยาลัยราชภัฏเชียงใหม่

คำนำ

สำนักดิจิทัลเพื่อการศึกษา จัดทำแผนการจัดการความรู้ (KM Action Plan) ปีงบประมาณ พ.ศ. 2564 ฉบับนี้ โดยคำนึงถึงภารกิจหลักของสำนักดิจิทัลเพื่อการศึกษา ตามยุทธศาสตร์ที่ 2 : พัฒนาระบบสารสนเทศเพื่อการบริหารจัดการ (MIS) และระบบสนับสนุนผู้บริหาร (ESS) เพื่อการบริหารงานอย่างมีประสิทธิภาพและยั่งยืน (Sustainable MIS) โดยสำนักฯ ได้มองเห็นเหตุการณ์ที่อาจจะเกิดขึ้นเกี่ยวกับการเรียกค่าไถ่ข้อมูลจากผู้ไม่หวังดี ซึ่งอาจส่งผลให้ข้อมูลที่จัดเก็บบนระบบเครือข่ายไม่สามารถใช้งานได้ หากมีเหตุการณ์เหล่านั้นเกิดขึ้นอาจส่งผลกระทบกับมหาวิทยาลัยในระดับสูง ทางสำนักดิจิทัลเพื่อการศึกษาจึงได้ร่วมกันวิเคราะห์ปัญหารวมถึงแลกเปลี่ยนสิ่งที่ได้รับรู้มาและนำมาสรุปเป็นแนวทางปฏิบัติที่ดี จึงได้จัดกิจกรรมการจัดการความรู้ในหัวข้อ ***"การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่"*** ขึ้น ซึ่งผลลัพธ์ในวันนี้นอกจากได้แนวปฏิบัติที่ดีจากทีมงานแล้ว ยังได้ผลลัพธ์ที่ดีคือข้อมูลที่อยู่ในระบบเครือข่ายขององค์กรมีความปลอดภัยในระดับสูง และไม่มีเหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยเกิดขึ้น ซึ่งทุก ๆ หน่วยงานสามารถนำไปใช้เป็นแนวปฏิบัติในองค์กรได้

สำนักดิจิทัลเพื่อการศึกษา หวังเป็นอย่างยิ่งว่า รายงานสรุปผลการดำเนินงานการจัดการความรู้ประจำปีงบประมาณ พ.ศ. 2564 จะเป็นประโยชน์ในการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ได้ ตลอดจนหน่วยงานอื่น ๆ ที่สนใจสามารถนำไปใช้เป็นแนวปฏิบัติได้อย่างมีประสิทธิภาพ และประสิทธิผลต่อไป

คณะกรรมการจัดการความรู้
สำนักดิจิทัลเพื่อการศึกษา
มิถุนายน 2564

สารบัญ

หน้า

บทสรุปผู้บริหาร

การจัดการความรู้ตามแผนการจัดการความรู้ ประจำปีงบประมาณ พ.ศ. 2564 สำนักดิจิทัลเพื่อการศึกษา ได้ร่วมกันหาแนวปฏิบัติที่ดี ซึ่งใช้กระบวนการจัดการความรู้เข้ามาเป็นกลไก และได้เกิดการจัดการความรู้ในหัวข้อ “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่” โดยมุ่งเน้นการวิเคราะห์เหตุการณ์ที่อาจจะเกิดขึ้นเกี่ยวกับการเรียกค่าไถ่ข้อมูลจากผู้ไม่หวังดี และร่วมกันหาแนวทางปฏิบัติที่ดีเพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งผลลัพธ์ที่ได้คือแนวปฏิบัติที่ดีในการป้องกันการเรียกค่าไถ่ฐานข้อมูล ข้อมูลที่อยู่ในระบบเครือข่ายขององค์กรมีความปลอดภัยในระดับสูง และไม่มีเหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยเกิดขึ้น ซึ่งทุก ๆ หน่วยงานสามารถนำไปปฏิบัติใช้ในองค์กรได้

ขอบเขต KM : “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่”

ผลผลิต : 1. แนวปฏิบัติที่ดีในการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

2. ข้อมูลที่อยู่ในระบบเครือข่ายขององค์กรมีความปลอดภัยในระดับสูง

องค์ความรู้ที่เกิดขึ้น :

การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ มีจำนวน 6 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 ศึกษาเหตุการณ์ที่อาจจะเกิดขึ้นจากการเรียกค่าไถ่ข้อมูล และกำหนดขอบเขตงาน

ขั้นตอนที่ 2 จัดประชุมผู้ที่เกี่ยวข้องร่วมกันวิเคราะห์ปัญหา และหาแนวปฏิบัติร่วมกัน

ขั้นตอนที่ 3 ได้แนวปฏิบัติที่ดีตามขอบเขตงานที่กำหนดขึ้น

ขั้นตอนที่ 4 นำแนวปฏิบัติในการป้องกันการเรียกค่าไถ่ฐานข้อมูลไปปฏิบัติใช้

ขั้นตอนที่ 5 ประเมินความพึงพอใจการใช้แนวปฏิบัติ และการให้ข้อเสนอแนะเพิ่มเติมในการปรับปรุงแนวปฏิบัติให้มีประสิทธิภาพมากยิ่งขึ้น

ขั้นตอนที่ 6 การปรับปรุงแนวปฏิบัติตามข้อเสนอแนะ เพื่อให้เป็นแนวปฏิบัติที่ดีและมีประสิทธิภาพมากยิ่งขึ้น

รายงานผลการดำเนินงานการจัดการความรู้
สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่ ประจำปีงบประมาณ พ.ศ. 2564

หัวข้อการจัดการความรู้ ประจำปีงบประมาณ พ.ศ. 2564

การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

หลักการและเหตุผล

สำนักดิจิทัลเพื่อการศึกษา เป็นหน่วยงานที่ส่งเสริม สนับสนุนเพิ่มความรู้และทักษะในด้าน ICT รวมทั้งเป็นหน่วยบริการระบบเครือข่ายคอมพิวเตอร์หลักของมหาวิทยาลัยและพื้นที่จัดการศึกษาทั้งทางด้านระบบเครือข่ายแบบมีสายและไร้สายรวมถึงการบริการทางด้านระบบงานเครือข่ายจากเครื่องคอมพิวเตอร์แม่ข่ายหลักของมหาวิทยาลัย ให้แก่นักศึกษา และบุคลากรของมหาวิทยาลัย อีกทั้งให้บริการด้านระบบสารสนเทศเพื่อการบริหารจัดการ โดยพัฒนาและให้บริการระบบสารสนเทศด้านต่างๆ เพื่อสนับสนุนและให้บริการระบบสารสนเทศด้านต่าง ๆ ตามภารกิจของมหาวิทยาลัย และที่ผ่านมาสำนักฯ ได้มองเห็นเหตุการณ์ร้ายที่อาจจะเกิดขึ้น ไม่ว่าจะเป็นการหลอกเอาข้อมูล การโจรกรรมข้อมูล หรือการเรียกค่าไถ่ข้อมูล ซึ่งเหตุการณ์เหล่านี้ล้วนเป็นปัญหาที่ร้ายแรงและส่งผลกระทบต่อข้อมูลที่จัดเก็บบนระบบเครือข่ายไม่สามารถใช้งานได้หากมีเหตุการณ์เหล่านี้เกิดขึ้น และยังอาจส่งผลกระทบกับมหาวิทยาลัยในระดับสูง ทางสำนักฯ จึงได้วิเคราะห์เหตุการณ์ที่เคยรับรู้ และร่วมกันหาแนวปฏิบัติที่ดี ซึ่งใช้กระบวนจัดการความรู้เข้ามาเป็นกลไก และได้เกิดการจัดการความรู้ในหัวข้อ “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่” ขึ้น เพื่อร่วมกันวิเคราะห์ปัญหาอันอาจจะเกิดขึ้นและหาแนวปฏิบัติร่วมกัน ซึ่งผลลัพธ์นอกจากได้แนวปฏิบัติที่ดีแล้ว ข้อมูลที่อยู่ในระบบเครือข่ายขององค์กรจะมีความปลอดภัยในระดับสูงขึ้น และไม่มีเหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยเกิดขึ้น ซึ่งทุก ๆ หน่วยงานสามารถนำไปใช้เป็นแนวปฏิบัติในองค์กรได้

วัตถุประสงค์

1. เพื่อจัดทำแนวปฏิบัติที่ดีในการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์
2. เพื่อให้ข้อมูลที่อยู่บนระบบเครือข่ายขององค์กรมีความปลอดภัยในระดับสูง
3. เพื่อไม่ให้มีเหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยเกิดขึ้น

แนวทางการดำเนินงาน

จากแผนการจัดการความรู้ ได้กำหนดกระบวนการสกัดความรู้จากการทำกิจกรรม จำนวน 7 ขั้นตอน รายละเอียดดังนี้

1) **การกำหนดเป้าหมายของการจัดการความรู้**

ศึกษาเหตุการณ์ที่อาจจะเกิดการเรียกค่าไถ่ข้อมูล และกำหนดขอบเขตงาน

2) **การสร้างและแสวงหาความรู้**

จัดกิจกรรมการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ โดยการประชุมวางแผน ร่วมกันหาแนวปฏิบัติที่ดีร่วมกัน สรุปแนวทางการปฏิบัติ ประเมินผลการปฏิบัติงานจากแนวทางใหม่ และระบุปัญหาที่พบ

3) **การสร้างความรู้ หรือแนวปฏิบัติ**

นำข้อมูลจากการประชุมมาจัดกิจกรรม “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่” มาเป็นแนวปฏิบัติ และเป็นมาตรฐานซึ่งสำนักดิจิทัลเพื่อการศึกษา และหน่วยงานอื่นสามารถนำไปใช้ในองค์กรได้

4) **การประยุกต์ใช้ความรู้**

จัดประชุมเพื่อแจ้งแนวปฏิบัติภายในสำนักฯ โดยแจ้งให้บุคลากรที่เกี่ยวข้องให้ร่วมกันปฏิบัติให้มีประสิทธิภาพมากยิ่งขึ้น

5) **การแบ่งปันแลกเปลี่ยนเรียนรู้**

จัดกิจกรรมแลกเปลี่ยนเรียนรู้ภายในองค์กรในหัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ ให้หน่วยงานที่เกี่ยวข้องและสนใจเข้าร่วมแบ่งปันความรู้ ประสบการณ์ และรับฟังข้อเสนอแนะจากหน่วยงานที่เข้าร่วม

6) **การปรับปรุงเป็นชุดความรู้**

นำข้อเสนอแนะจากการจัดกิจกรรม การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ มาปรับปรุงเพื่อให้ได้แนวปฏิบัติที่ดีในการนำไปใช้ต่อไป

7) การประเมินผลการดำเนินงาน

กำหนดตัวชี้วัดเชิงปริมาณ และตัวชี้วัดเชิงคุณภาพ ดังนี้

ตัวชี้วัดเชิงปริมาณ

1. เหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยมีค่าเท่ากับ ศูนย์

ตัวชี้วัดเชิงคุณภาพ

1. ผู้บริหารหน่วยงานมีความพึงพอใจแนวทางในการจัดเก็บข้อมูลที่ปลอดภัย

ผลการดำเนินงาน

ตามแผนการจัดการความรู้ “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่” ได้ดำเนินงานตามกระบวนการจัดการความรู้ 7 ขั้นตอน ดังนี้

1) การกำหนดเป้าหมายของการจัดการความรู้

วิธีการสู่ความสำเร็จ

ทำการวิเคราะห์สถานการณ์ที่เสี่ยงต่อการเรียกค่าไถ่ข้อมูล ซึ่งปัจจุบันการทำงานโดยการใช้อินเทอร์เน็ตเข้ามาช่วยงานเป็นสิ่งจำเป็น ไม่ว่าจะเป็นการค้นหาข้อมูล การดาวน์โหลดงานต่าง ๆ แม้กระทั่งการใช้อีเมล์ในการรับข้อมูล และอื่น ๆ ด้วยเหตุนี้จึงจำเป็นที่ควรมีมาตรการที่เหมาะสมเพื่อป้องกันภัยคุกคามจากการโจรกรรมหรือเรียกค่าไถ่ข้อมูลจากอาชญากรไซเบอร์

2) การสร้างและแสวงหาความรู้

วิธีการสู่ความสำเร็จ

จัดประชุมผู้ที่เกี่ยวข้องในวันที่ 28 เมษายน 2564 ในรูปแบบออนไลน์ ผ่านระบบ zoom meeting เพื่อร่วมกันหารือแนวปฏิบัติที่ดีในการป้องกันการเรียกค่าไถ่ข้อมูลจากอาชญากรไซเบอร์

3) การสร้างความรู้ หรือแนวปฏิบัติ

วิธีการสู่ความสำเร็จ

จากการที่ได้ประชุมหารือเพื่อหาแนวปฏิบัติที่ดีในการป้องกันการเรียกค่าไถ่ข้อมูลผู้ที่เกี่ยวข้องได้รวบรวมข้อมูลทั้งหมดมาจัดทำแนวปฏิบัติในการป้องกันการเรียกค่าไถ่ข้อมูลระหว่างเดือนพฤษภาคม – มิถุนายน 2564 และจัดทำให้เป็นแนวปฏิบัติที่ดีในการปฏิบัติงานให้มีประสิทธิภาพ และปลอดภัยยิ่งขึ้น

4) การประยุกต์ใช้ความรู้

วิธีการสู่ความสำเร็จ

จัดประชุมหน่วยพัฒนาระบบสารสนเทศ หน่วยบริหารและจัดการระบบเครือข่ายคอมพิวเตอร์ และหน่วยดูแลและบำรุงระบบคอมพิวเตอร์ ร่วมกันปรับปรุงและหาแนวทางที่ดีจากข้อเสนอแนะ และทดลองปฏิบัติใช้งานระหว่างเดือนพฤษภาคม 2564

5) การแบ่งปันแลกเปลี่ยนเรียนรู้

วิธีการสู่ความสำเร็จ

จัดกิจกรรมแลกเปลี่ยนเรียนรู้ เรื่อง การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ ในวันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 09.00 – 12.00 น. ในรูปแบบออนไลน์ ผ่านระบบ Zoom meeting เพื่อร่วมกันแบ่งปันความรู้ ประสบการณ์ และหาแนวปฏิบัติที่ดีร่วมกัน สรุปแนวทางปฏิบัติลงสู่การปฏิบัติจริง ประเมินผลการปฏิบัติจากแนวทางใหม่ และระบุปัญหาที่พบ และรับฟังข้อเสนอแนะเพิ่มเติมในการปรับปรุงแนวปฏิบัติต่อไป

6) การปรับปรุงเป็นชุดความรู้

วิธีการสู่ความสำเร็จ

จากการจัดกิจกรรมแลกเปลี่ยนเรียนรู้ ได้นำข้อเสนอแนะจากผู้เข้าร่วมกิจกรรมมาปรับปรุงแนวปฏิบัติการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ขององค์กรให้มีประสิทธิภาพ และปลอดภัยมากยิ่งขึ้น

7) การประเมินผลการดำเนินงาน

วิธีการสู่ความสำเร็จ

ทำการประเมินผลแนวปฏิบัติการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ได้ดังนี้

<u>ตัวชี้วัดเชิงปริมาณ</u>

1. เหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยมีค่าเท่ากับ ศูนย์

<u>ตัวชี้วัดเชิงคุณภาพ</u>

1. ผู้บริหารหน่วยงานมีความพึงพอใจแนวทางในการจัดเก็บข้อมูลที่ปลอดภัย

องค์ความรู้ที่เกิดขึ้น

จากขั้นตอนตามแผนการจัดการความรู้ ประจำปีงบประมาณ พ.ศ. 2564 ซึ่งมีเป้าหมายให้เกิดการแลกเปลี่ยนเรียนรู้ และมีแนวปฏิบัติเกี่ยวกับการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ จึงมีองค์ความรู้ที่เกิดขึ้น ดังนี้

ขอบเขต KM

การแลกเปลี่ยนเรียนรู้แนวปฏิบัติที่ดี ประเด็นความรู้เรื่อง “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่”

ผลผลิต : แนวทางและการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

องค์ความรู้ที่เกิดขึ้น

การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ มีจำนวน 6 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 ศึกษาเหตุการณ์ที่อาจจะเกิดขึ้นจากการเรียกค่าไถ่ข้อมูล วิเคราะห์ปัญหาเพื่อหาแนวทางแก้ไข และกำหนดแนวทางในการป้องกันการเรียกค่าไถ่ข้อมูลจากอาชญากรไซเบอร์

ขั้นตอนที่ 2 จัดประชุมผู้ที่เกี่ยวข้องร่วมกันวิเคราะห์ปัญหา และหาแนวทางร่วมกันภายในหน่วยงาน และจัดทำแนวปฏิบัติที่ดีในการป้องกันเหตุการณ์ที่อาจจะเกิดขึ้นในการเรียกค่าไถ่ข้อมูล

ขั้นตอนที่ 3 ได้แนวปฏิบัติที่ดีตามขอบเขตงานที่กำหนดขึ้น

ขั้นตอนที่ 4 นำแนวปฏิบัติในการป้องกันการเรียกค่าไถ่ฐานข้อมูลไปปฏิบัติใช้

ขั้นตอนที่ 5 ประเมินความพึงพอใจการใช้แนวปฏิบัติ และการให้ข้อเสนอแนะเพิ่มเติมในการปรับปรุงแนวปฏิบัติให้มีประสิทธิภาพมากยิ่งขึ้น

ขั้นตอนที่ 6 การปรับปรุงแนวปฏิบัติตามข้อเสนอแนะ เพื่อให้เป็นแนวปฏิบัติที่ดีและมีประสิทธิภาพมากยิ่งขึ้น และนำไปใช้เป็นแนวปฏิบัติภายในองค์กรและหน่วยงานอื่น ๆ ต่อไป

ภาคผนวก

แผนการจัดการความรู้ (KM Action Plan)

ประจำปีงบประมาณ พ.ศ. 2564

แผนการจัดการความรู้
KM Action Plan

การป้องกัน การเรียกค่าไถ่ฐานข้อมูล จากอาชญากรไซเบอร์

ประจำปีงบประมาณ 2564

DIGITAL EDUCATION

สำนักดิจิทัลเพื่อการศึกษา
มหาวิทยาลัยราชภัฏเชียงใหม่

www.digital.cmru.ac.th

คำนำ

แผนการจัดการความรู้ (KM Action Plan) สำนักดิจิทัลเพื่อการศึกษา ปีงบประมาณ 2564 ฉบับนี้จัดทำขึ้นโดยคำนึงถึงภารกิจหลักของสำนักดิจิทัลเพื่อการศึกษา ตามยุทธศาสตร์ที่ 2 : พัฒนาระบบสารสนเทศเพื่อการบริหารจัดการ (MIS) และระบบสนับสนุนผู้บริหาร (ESS) เพื่อการบริหารงานอย่างมีประสิทธิภาพและยั่งยืน (Sustainable MIS) โดยมีการแลกเปลี่ยนเรียนรู้ภายในองค์กรในการบริหารจัดการเว็บไซต์เพื่อหาแนวทางการแก้ปัญหาร่วมกัน ตามกระบวนการจัดการความรู้ ของสำนักดิจิทัลเพื่อการศึกษา (Knowledge Management Process) เพื่อให้การจัดเก็บข้อมูลของมหาวิทยาลัยมีประสิทธิภาพ และปลอดภัย โดยจัดกิจกรรมในหัวข้อ ***"การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์"*** ซึ่งได้ร่วมกันวิเคราะห์ปัญหาภัยคุกคามที่อาจจะเกิดขึ้นสูง และมีผลกระทบสูงหากเหตุการณ์ดังกล่าวเกิดขึ้น และนำมาพัฒนาแนวการจัดเก็บข้อมูลที่ปลอดภัยให้เป็นแนวปฏิบัติที่ดีในการใช้งานบริหารจัดการของสำนักดิจิทัลเพื่อการศึกษา และหน่วยงานภายในมหาวิทยาลัย

สำนักดิจิทัลเพื่อการศึกษา หวังเป็นอย่างยิ่งว่า แผนการจัดการความรู้ฉบับนี้จะเป็นประโยชน์ต่อการดำเนินงานด้านการพัฒนาการบริหารจัดการของสำนักดิจิทัลเพื่อการศึกษาได้อย่างมีประสิทธิภาพและประสิทธิผลต่อไป

(อาจารย์อำนาจ โกวรรณ)
ผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา

สารบัญ

หน้า

องค์ความรู้ที่จำเป็น

วิสัยทัศน์ (Vision)

"เป็นองค์กรที่เป็นเลิศด้านเทคโนโลยีดิจิทัลเพื่อสนับสนุนคุณภาพการศึกษาอย่างยั่งยืน"

พันธกิจ (Mission)

1. พัฒนาการบริการด้านเทคโนโลยีดิจิทัลเพื่อให้ได้ตามมาตรฐานระดับสากล
2. พัฒนามหาวิทยาลัยให้ก้าวสู่องค์กรดิจิทัลอย่างเต็มรูปแบบ
3. ส่งเสริมศักยภาพด้านการใช้เทคโนโลยีดิจิทัล เพื่อยกระดับความสามารถในการดำเนินงานให้มีประสิทธิภาพอย่างเต็มศักยภาพแก่บุคลากร นักศึกษา และท้องถิ่น
4. พัฒนาองค์กรให้เป็นองค์กรแห่งการเรียนรู้ โดยเชื่อมโยงองค์ความรู้กับบุคลากรทั้งภายในและภายนอกองค์กรเพื่อสร้างความร่วมมือที่เข้มแข็ง ด้านเทคโนโลยีดิจิทัล
5. ส่งเสริม สนับสนุนองค์กรให้มีการใช้เทคโนโลยีดิจิทัลที่เป็นมิตรกับสิ่งแวดล้อม

วัตถุประสงค์ (Objective)

1. เพื่อพัฒนาระบบดิจิทัลให้ตอบสนองนโยบายและสนับสนุนการบริหารงานของมหาวิทยาลัยตามภารกิจทั้ง 4 ด้าน คือ การผลิตบัณฑิต การวิจัย การบริการวิชาการแก่สังคมการทำนุบำรุงศิลปะและวัฒนธรรม
2. เพื่อพัฒนาสารสนเทศของมหาวิทยาลัย เพื่อการบริหารจัดการและเพื่อการเรียนรู้
3. เพื่อสร้างองค์ความรู้ด้านเทคโนโลยีดิจิทัล และให้บริการวิชาการแก่สังคม ตลอดจนสร้างเครือข่ายดิจิทัลทั้งในประเทศและต่างประเทศ

องค์ความรู้ที่จำเป็นต่อการปฏิบัติราชการตามประเด็นยุทธศาสตร์ที่เลือกมาทำแผนการจัดการความรู้ คือ
ประเด็นยุทธศาสตร์ : ประเด็นยุทธศาสตร์ที่ 2 พัฒนาระบบสารสนเทศเพื่อการบริหารจัดการ (MIS) และระบบสนับสนุนผู้บริหาร (ESS) เพื่อการบริหารงานอย่างมีประสิทธิภาพและยั่งยืน (Sustainable MIS)
องค์ความรู้ที่จำเป็น (K) : “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์”
เหตุผลที่เลือกองค์ความรู้ : 1. ข้อมูลที่จัดเก็บบนระบบเครือข่าย อาจมีการโจมตีจากผู้ไม่หวังดีทำให้ไม่สามารถใช้งานได้ 2. การเรียกค่าไถ่ข้อมูลส่งผลกระทบกับมหาวิทยาลัยในระดับสูง
ตัวชี้วัด (KPI) ตามคำรับรอง : เหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยมีค่าเท่ากับ 0
เป้าหมายตามคำรับรอง : 1. ข้อมูลที่อยู่บนระบบเครือข่ายขององค์กรมีความปลอดภัยในระดับสูง 2. ไม่มีเหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยเกิดขึ้น

กระบวนการสกัดความรู้จากการทำกิจกรรม

กระบวนการจัดการความรู้ (KM Process)	กระบวนการสกัดความรู้	ประเด็น/วิธีการ
1.การกำหนดเป้าหมายของการจัดการความรู้	ศึกษาเหตุการณ์ที่อาจจะเกิดการเรียกค่าไถ่ข้อมูล และกำหนดขอบเขตงาน	ศึกษาเหตุการณ์ที่เคยเกิดขึ้นของการเรียกค่าไถ่ข้อมูล - ปัจจุบันอินเตอร์เนตเป็นสิ่งจำเป็นในการดำเนินงานไม่ว่าจะเป็น การค้นหาข้อมูลผ่านอินเตอร์เนต การดาวน์โหลดไฟล์ต่างๆ แม้กระทั่งการใช้อีเมลในการรับข้อมูล และอื่นๆ เพื่อป้องกันเหตุการณ์ร้ายที่อาจจะเกิดขึ้น ไม่ว่าจะเป็นการหลอกเอาข้อมูล การโจรกรรมข้อมูล หรือการเรียกค่าไถ่ข้อมูล จึงควรมีมาตรการที่เหมาะสมเพื่อป้องกันคอมพิวเตอร์จากภัยคุกคามออนไลน์
2.การสร้างและแสวงหาความรู้	จัดกิจกรรม การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์	- ประชุมวางแผนทบทวนกระบวนการทำงาน - หาแนวทางการแก้ไขปัญหาร่วมกัน - สรุปแนวทางปฏิบัติ ลงสู่การปฏิบัติ - ประเมินผลการปฏิบัติงานจากแนวทางใหม่ - ระบุปัญหาที่พบ
3.การสร้างความรู้ หรือแนวปฏิบัติ	การบันทึกการเล่าเรื่องจากการจัดกิจกรรม การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์	- ออกแบบและพัฒนาแนวทางการจัดเก็บข้อมูลที่ปลอดภัย
4. การประยุกต์ใช้ความรู้	จัดประชุมเพื่อแจ้งแนวปฏิบัติภายในองค์กร	- ประชุมแจ้งทุกฝ่ายที่เกี่ยวข้องให้ทดลองใช้แนวทางการจัดเก็บข้อมูลที่ปลอดภัย

กระบวนการจัดการความรู้ (KM Process)	กระบวนการสกัดความรู้	ประเด็น/วิธีการ
5. การแบ่งปันแลกเปลี่ยนเรียนรู้	จัดกิจกรรมแลกเปลี่ยนเรียนรู้ภายในองค์กรเพื่อหาแนวทางการจัดเก็บข้อมูลที่ปลอดภัย	- แลกเปลี่ยนเรียนรู้ภายในหน่วยงานถึงวิธีการและการป้องกันฐานข้อมูลให้ปลอดภัยจากการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์
6.การปรับปรุงเป็นชุดความรู้	การบันทึกการเล่าเรื่องจากการจัดกิจกรรม การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์	- นำข้อเสนอแนะมาเป็นแนวทางในการจัดเก็บข้อมูลให้ปลอดภัยยิ่งขึ้น
7.การประเมินผลการดำเนินงาน	ตัวชี้วัด เชิงปริมาณ ตัวชี้วัด เชิงคุณภาพ	- เหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยมีค่าเท่ากับ ศูนย์ 1. ผู้บริหารหน่วยงานมีความพึงพอใจแนวทางในการจัดเก็บข้อมูลที่ปลอดภัย

แผนการจัดการความรู้ (KM Action Plan) ปีงบประมาณ 2564

ชื่อหน่วยงาน : สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่

ประเด็นยุทธศาสตร์ : ประเด็นยุทธศาสตร์ที่ 2 : พัฒนาระบบสารสนเทศเพื่อการบริหารจัดการ (MIS) และระบบสนับสนุนผู้บริหาร (ESS) เพื่อการบริหารงานอย่างมีประสิทธิภาพและยั่งยืน (Sustainable MIS)

องค์ความรู้ที่จำเป็น (K) : “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์”

ตัวชี้วัด (KPI) ตามคำรับรอง : เหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัยเท่ากับ ศูนย์

กลุ่มเป้าหมายตามคำรับรอง : ผู้บริหาร บุคลากร ผู้ใช้งาน สำนักดิจิทัลเพื่อการศึกษา

ลำดับ	กิจกรรม	ระยะเวลา	ตัวชี้วัด	กลุ่มเป้าหมาย	ผู้รับผิดชอบ/หมายเหตุ
1	การแลกเปลี่ยนเรียนรู้ “การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์”	กุมภาพันธ์ 2564	บันทึกการเล่าเรื่อง เรื่อง การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ จำนวน 1 ฉบับ	บุคลากร สำนักดิจิทัลเพื่อการศึกษา	ผศ. ดร.กัลยา ใจรักษ์
2	ออกแบบและพัฒนาแนวทางการจัดเก็บข้อมูลที่ปลอดภัย	มีนาคม 2564	แนวทางการจัดเก็บข้อมูลที่ปลอดภัย จำนวน 1 ฉบับ	บุคลากร สำนักดิจิทัลเพื่อการศึกษา	1. นายธีระพงษ์ ใจคำมา 2. นายวิวัฒน์ชัย ขำประไพ
3	จัดประชุมบุคลากรภายในหน่วยงาน เพื่อแจ้งให้ทุกฝ่ายที่เกี่ยวข้องทดลองแนวทางการจัดเก็บข้อมูลที่ปลอดภัย	มีนาคม 2564	รายการประชุม เรื่อง การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ จำนวน 1 ฉบับ	บุคลากร สำนักดิจิทัลเพื่อการศึกษา	นางสาวจริยา หมื่นแก้ว
4	แลกเปลี่ยนเรียนรู้เกี่ยวกับแนวทางในการจัดเก็บข้อมูลที่ปลอดภัย และให้ข้อเสนอแนะในการปรับปรุง	เมษายน 2564	บันทึกการเล่าเรื่อง เรื่อง การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ จำนวน 1 ฉบับ	บุคลากร สำนักดิจิทัลเพื่อการศึกษาและบุคลากรที่ดูแลเว็บไซต์ของหน่วยงานภายนอก	นางสาวจริยา หมื่นแก้ว

ลำดับ	กิจกรรม	ระยะเวลา	ตัวชี้วัด	กลุ่มเป้าหมาย	ผู้รับผิดชอบ/ หมายเหตุ
5	ปรับปรุงแนวทาง และประเมินผลความพึงพอใจผู้ใช้งาน	พฤษภาคม 2564	ผลการประเมินเหตุการณ์เรียกค่าไถ่ข้อมูลของมหาวิทยาลัย เท่ากับ ศูนย์	บุคลากรสำนักดิจิทัลเพื่อการศึกษา	1. นายธีระพงษ์ ใจคำมา 2. นายวิวัฒน์ชัย ขำประไพ

วงจรการเรียนรู้ (Learning Cycle)

วงจรการเรียนรู้	การประยุกใช้
1. การมีคลังความรู้	1. ศึกษาเหตุการณ์ที่ผ่านมา 2. วิเคราะห์ปัญหาเพื่อหาแนวทางแก้ไข 3. กำหนดขอบเขตแนวทางการจัดการข้อมูลที่ปลอดภัย
2. การผลักดันให้นำความรู้ไปใช้	จัดกิจกรรมแลกเปลี่ยนเรียนรู้ระหว่างบุคลากรที่เกี่ยวข้อง
3. การนำความรู้ไปใช้	ผู้ที่เกี่ยวข้องนำแนวทางการจัดเก็บข้อมูลที่ปลอดภัยไปใช้เป็นแนวปฏิบัติ
4. การสรุปความรู้ที่ได้จากการทำกิจกรรม ปัญหา/อุปสรรค ในการใช้งานระบบ เก็บเข้าคลังความรู้	จัดประชุมแลกเปลี่ยนเรียนรู้ภายในหน่วยงาน ถึงประสิทธิภาพของการใช้งานและให้ข้อเสนอแนะในการปรับปรุงเพิ่มเติม
5. การนำความรู้มาปรับเป็นแนวปฏิบัติในการดำเนินงาน	นำข้อเสนอแนะที่ได้มาปรับปรุงเพื่อให้มีประสิทธิภาพสมบูรณ์มากยิ่งขึ้น และนำไปใช้เป็นแนวปฏิบัติภายในองค์กรและหน่วยงานอื่นๆ ต่อไป

ทีมงานการจัดการองค์ความรู้ (KM : Knowledge Management)

คณะกรรมการอำนวยการและคณะทำงาน บริหารจัดการความรู้ สำนักดิจิทัลเพื่อการศึกษา ประกอบด้วย

ผู้บริหารสูงสุด (CEO)	
อาจารย์อำนาจ โกวรรณ	ผู้บริหารสูงสุด เป็นผู้ริเริ่มกิจกรรมจัดการความรู้โดยกำหนดตัวบุคคลที่จะทำหน้าที่ “คุณเอื้อ (ระบบ)” ของ KM
คุณเอื้อ (Chief Knowledge Officer , CKO)	
อาจารย์ ดร.ทิวาวัลย์ ต๊ะการ ผศ. ดร.กัลยา ใจรักษ์	จัดการระบบของการจัดการความรู้ขององค์กร มีบทบาท คือ กำหนดเป้าหมายของการจัดการความรู้ของหน่วยงานเชื่อมโยงเป้าหมายของการจัดการความรู้ของหน่วยงานเข้ากับวิสัยทัศน์ พันธกิจ และยุทธศาสตร์ขององค์กร
คุณอำนวย (Knowledge Facilitator , KF)	
นายมารุต เปี่ยมเกตุ	ผู้อำนวยความสะดวกในการจัดการความรู้ มีบทบาทหรือมีหน้าที่หลัก คือ ส่งเสริมให้เกิดการเปลี่ยนแปลงเรียนรู้ และอำนวยความสะดวกต่อการแลกเปลี่ยนเรียนรู้
คุณกิจ (Knowledge Practitioner ,KP)	
นางสาวนันทาวดี คุณศิลป์ นายธีระพงษ์ ใจคำ นายวิวัฒน์ชัย ขำประไพ นายกุลชาติ ปัญญาดี นายบัณฑิต นันทะเทศ	ผู้ดำเนินกิจกรรมจัดการความรู้ มีบทบาทหรือมีหน้าที่หลัก คือ ผู้จัดการความรู้ตัวจริง เป็นผู้มีความรู้ (Explicit Knowledge) และเป็นผู้ต้องมาแลกเปลี่ยนเรียนรู้ เพื่อการปฏิบัติให้บรรลุถึง “เป้าหมาย” ที่ตั้งไว้
คุณลิขิต (Note Taker)	
นางสาวจริยา หมื่นแก้ว	ผู้ทำหน้าที่จดบันทึกในกิจกรรมการจัดการความรู้จากกิจกรรมเพื่อบรรลุเป้าหมายของงานแต่ละกิจกรรม บันทึกการประชุม หรือบันทึกอื่นๆ เพื่อให้การดำเนินการจัดการความรู้มีความต่อเนื่อง การจดบันทึกอาจเป็นการจดในกระดาษ บันทึกในรูปแบบอิเล็กทรอนิกส์ไฟล์
คุณประสาน (Network Manager)	
นางสาวรุ่งทิวา กิตติยังกุล	ประสานเชื่อมโยงเครือข่ายการจัดการความรู้ระหว่างหน่วยงานให้เกิดการแลกเปลี่ยนเรียนรู้ในวงที่กว้างขึ้นเกิดพลังร่วมมือทางเครือข่ายในการเรียนรู้

คุณวิศาสตร์ (IT Wizard)	
นายธีระพงษ์ ใจคำ นายวิวัฒน์ชัย ขำประไพ	พัฒนาแนวทางการจัดเก็บข้อมูลที่ปลอดภัยตามขอบเขตงานที่กำหนด เพื่อให้ตรงกับความต้องการของผู้ใช้งานระบบ

กลุ่มเป้าหมาย
กิจกรรม การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

ลำดับ	ชื่อ-นามสกุล		ตำแหน่ง
1	นายมารุต	เปี่ยมเกตุ	หัวหน้าสำนักงานผู้อำนวยการ
2	นางสาวนันทาวดี	คุณศิลป์	หัวหน้างานบริหารงานทั่วไป
3	นายธีระพงษ์	ใจคำมา	หัวหน้างานเทคโนโลยีสารสนเทศ
4	นายชลิต	โปธา	นักวิชาการคอมพิวเตอร์
5	นายวิวัฒน์ชัย	ขำประไพ	นักวิชาการคอมพิวเตอร์
6	นายอานนท์	มะโนเมือง	นักวิชาการคอมพิวเตอร์
7	นายกฤษณ์	ขาวศรี	นักวิชาการคอมพิวเตอร์
8	นายจรูญ	บุตรแก้ว	นักวิชาการคอมพิวเตอร์
9	นายวิทูร	อุ่นแสน	นักวิชาการคอมพิวเตอร์
10	นายบัณฑิต	นันทะเทศ	นักวิชาการคอมพิวเตอร์
11	นายกุลชาติ	ปัญญาดี	นักวิชาการคอมพิวเตอร์
12	นายเจษฎา	ยาวุฑฒิ	นักวิชาการคอมพิวเตอร์
13	นางสาวรุ่งทิวา	กิตติยังกุล	นักวิชาการคอมพิวเตอร์
14	นางพรพิมล	แก้วฟุ้งรังสี	นักวิชาการคอมพิวเตอร์
15	นายณัฐพงษ์	วงศ์จันทร์ตา	นักวิชาการศึกษา
16	นายปิยะพงษ์	หินเกย	นักวิชาการศึกษา
17	นางสาวจริยา	หมื่นแก้ว	นักวิชาการเงินและบัญชี
18	นางสาวเสฎฐพร	เสทธะยะ	นักวิเคราะห์นโยบายและแผน

ภาคผนวก

คำสั่งสำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่
ที่ ๑๐๙/๒๕๖๓
เรื่อง แต่งตั้งคณะกรรมการดำเนินงานการจัดการความรู้ สำนักดิจิทัลเพื่อการศึกษา
ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

เพื่อให้การจัดการความรู้ สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่ ดำเนินงานไปอย่างต่อเนื่องมีประสิทธิภาพเกิดประสิทธิผล ส่งผลต่อการจัดการศึกษาให้มีคุณภาพเป็นไปตามมาตรฐาน ตลอดจนการดำเนินงานสำเร็จบรรลุตามวัตถุประสงค์ที่มหาวิทยาลัยราชภัฏเชียงใหม่กำหนด สำนักดิจิทัลเพื่อการศึกษา จึงขอยกเลิกคำสั่งสำนักดิจิทัลเพื่อการศึกษา ที่ ๑๑๔/๒๕๖๒ เรื่อง แต่งตั้งคณะกรรมการดำเนินงานการจัดการความรู้ สำนักดิจิทัลเพื่อการศึกษา และขอแต่งตั้งคณะกรรมการดำเนินการจัดการความรู้ สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ดังต่อไปนี้

๑. ผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา (อาจารย์อำนาจ โกวรรณ)		ประธานกรรมการ
๒. รองผู้อำนวยการ (อาจารย์ ดร.ทิวาวัลย์ ต๊ะการ)		รองประธานกรรมการ
๓. รองผู้อำนวยการ (ผศ. ดร.กัลยา ใจรักษ์)		รองประธานกรรมการ
๔. หัวหน้าสำนักงานผู้อำนวยการ (นายมารุต เปี่ยมเกตุ)		กรรมการ
๕. หัวหน้างานบริหารงานทั่วไป (นางสาวนันทาวดี คุณศิลป์)		กรรมการ
๖. หัวหน้างานเทคโนโลยีสารสนเทศ (นายธีระพงษ์ ใจคำมา)		กรรมการ
๗. นายชลิต	โปธา	กรรมการ
๘. นายเจษฎา	ยาวุฑฒิ	กรรมการ
๙. ว่าที่ร้อยตรีอานนท์	มะโนเมือง	กรรมการ
๑๐. นายกุลชาติ	ปัญญาดี	กรรมการ
๑๑. นายบัณฑิต	นันทะเทศ	กรรมการ
๑๒. นายกฤษณ์	ขาวศรี	กรรมการ
๑๓. นายณัฐพงษ์	วงค์จันทร์ตา	กรรมการ
๑๔. นายจรูญ	บุตรแก้ว	กรรมการ
๑๕. นายวิทูร	อุ่นแสน	กรรมการ
๑๖. นายปิยะพงษ์	หินเกย	กรรมการ

๑๗. นางพรพิมล	แก้วฟุ้งรังษี	กรรมการ
๑๘. นางสาวรุ่งทิวา	กิตติยังกุล	กรรมการ
๑๙. นางสาวเสฏฐพร	เสทธะยะ	กรรมการ
๒๐. นางสาวจริยา	หมื่นแก้ว	กรรมการและเลขานุการ
๒๑. นายวิวัฒน์ชัย	ขำประไพ	กรรมการและผู้ช่วยเลขานุการ

มีหน้าที่

๑. ดำเนินการวางแผน รวบรวม วิเคราะห์ข้อมูลประกอบเพื่อกำหนดแนวทาง และทิศทางการจัดทำแผนการจัดการความรู้ (KM) สำนักดิจิทัลเพื่อการศึกษา

๒. กำหนดกิจกรรม และดำเนินการการจัดการความรู้ (KM)

๓. ดำเนินการเผยแพร่ประชาสัมพันธ์แนวทาง และทิศทางการจัดการความรู้ (KM) ให้บุคลากรได้รับทราบและเข้าใจตรงกันอย่างทั่วถึง

๔. ประเมินผลการดำเนินกิจกรรมตามแผนการจัดการความรู้ (KM)

๕. ดำเนินการติดตามและสรุปรายงานผลการดำเนินงานการจัดการความรู้ (KM)

สั่ง ณ วันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๓

(อาจารย์อำนาจ โกวรรณ)
ผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา

DIGITAL
EDUCATION

Digital Education is an organization to support knowledge and ICT skills for Chiang Mai Rajabhat University students, lecturers, staffs and interested people. We provide ICT training program from basic to advance level. We attempt to create ICT competency to reach international standard.

202 Chang Puak road., Tambon Chang Puak
Maung, Chiangmai 50300
Tel 0-5388-5924 | Fax 0-5388-5924

www.digital.cmru.ac.th

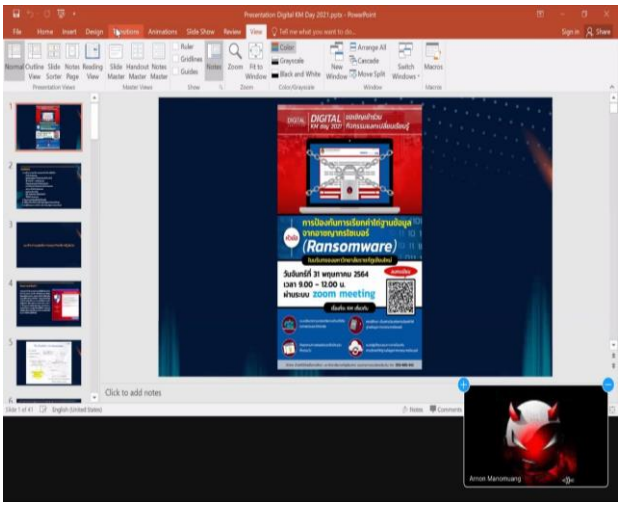
ภาพบรรยากาศวันกิจกรรมแลกเปลี่ยนเรียนรู้

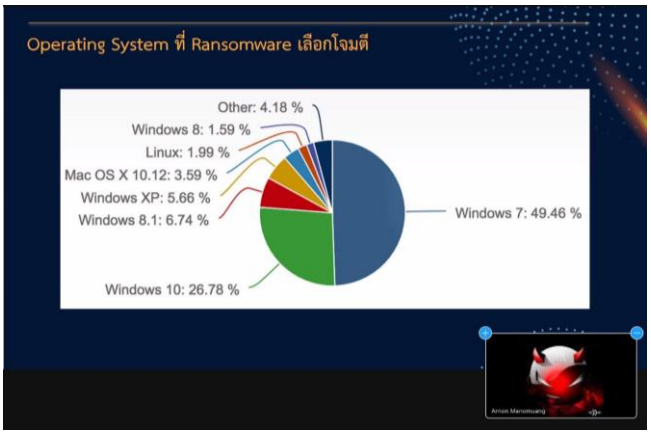
Digital KM Day 2021

ผ่านรูปแบบออนไลน์ ระบบ zoom meeting

หัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูล จากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

ภาพบรรยากาศวันกิจกรรมแลกเปลี่ยนเรียนรู้ Digital KM Day 2021
ผ่านรูปแบบออนไลน์ ระบบ zoom meeting
หัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)
ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่
วันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 09.00 – 12.00 น.





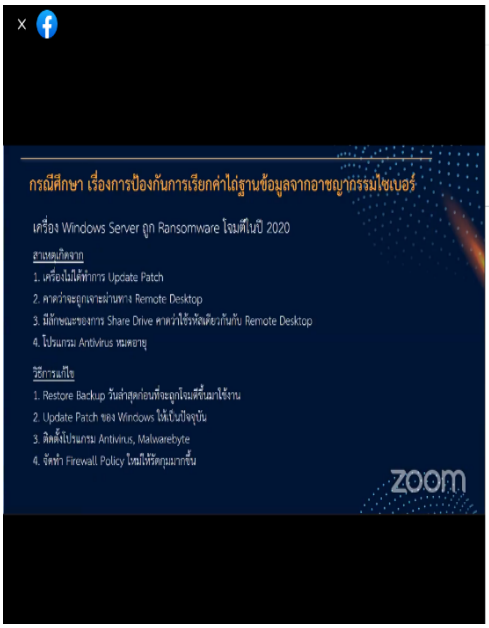
ภาพบรรยากาศวันกิจกรรมแลกเปลี่ยนเรียนรู้ Digital KM Day 2021

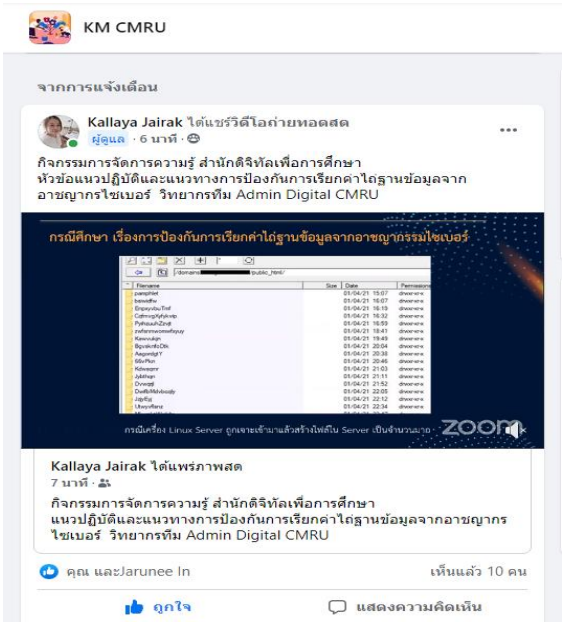
ผ่านรูปแบบออนไลน์ ระบบ zoom meeting

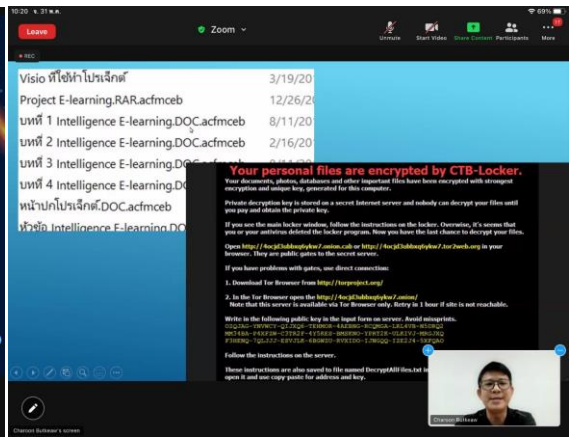
หัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)

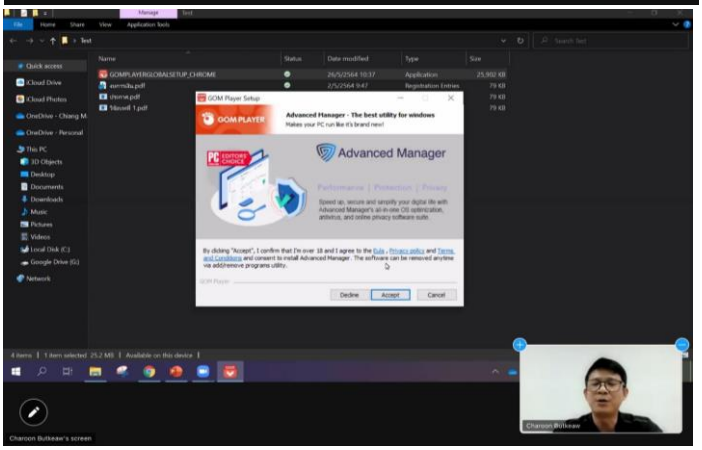
ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

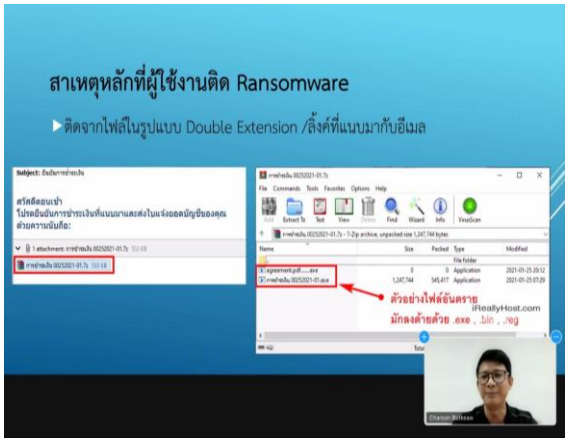
วันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 09.00 – 12.00 น.











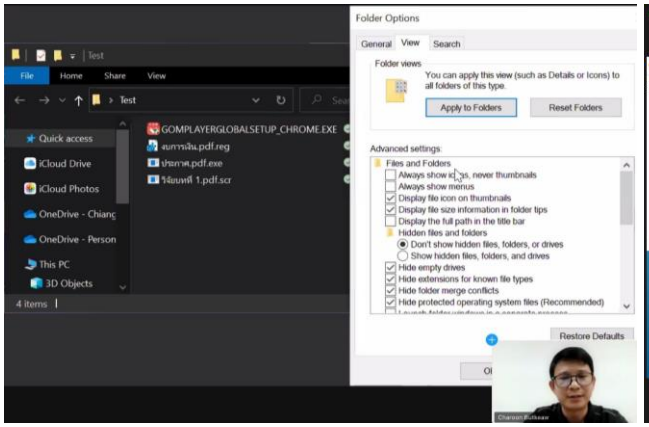
ภาพบรรยากาศวันกิจกรรมแลกเปลี่ยนเรียนรู้ Digital KM Day 2021

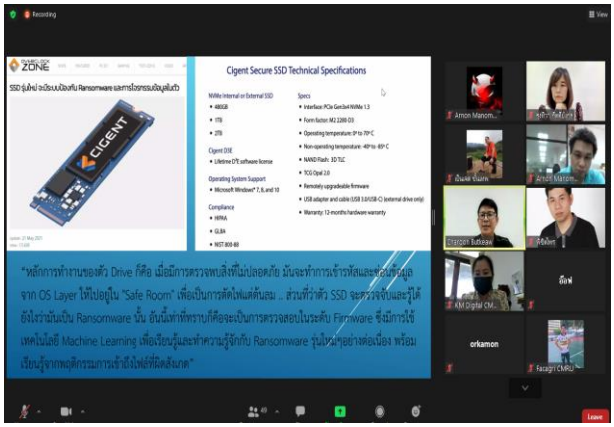
ผ่านรูปแบบออนไลน์ ระบบ zoom meeting

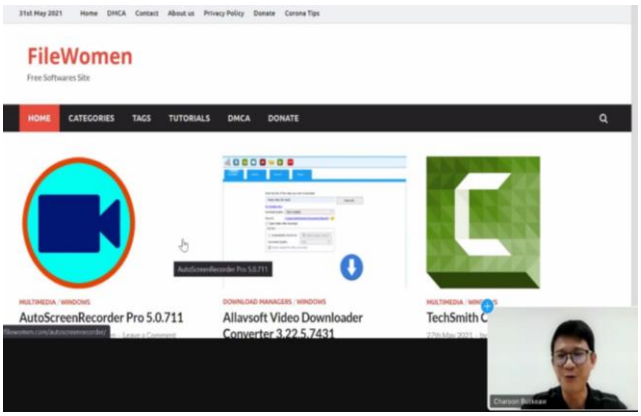
หัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)

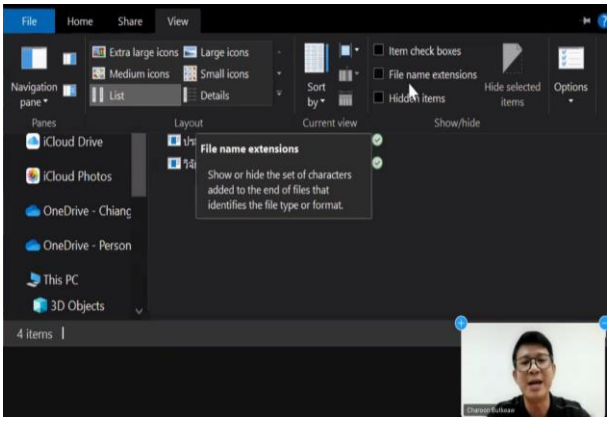
ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

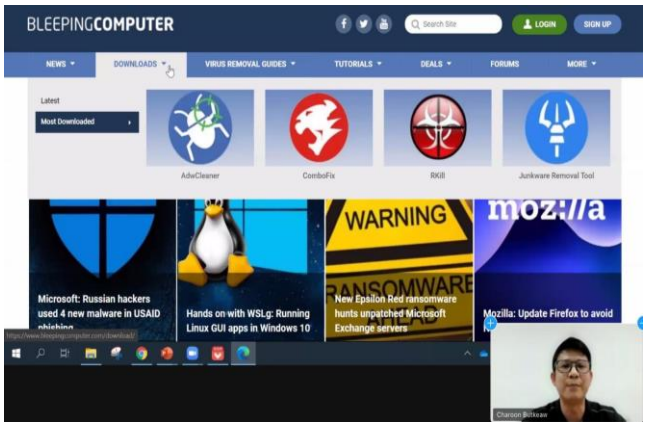
วันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 09.00 – 12.00 น.

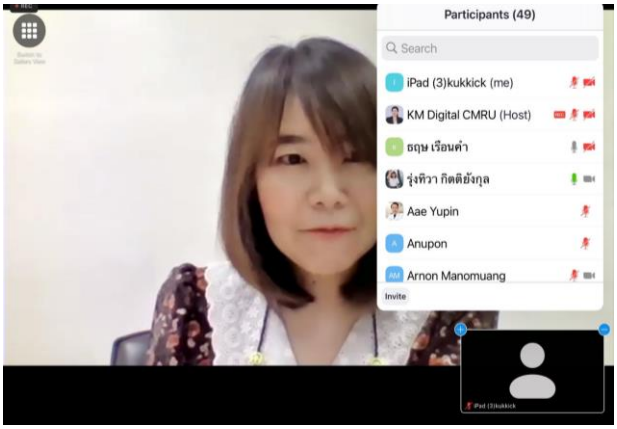












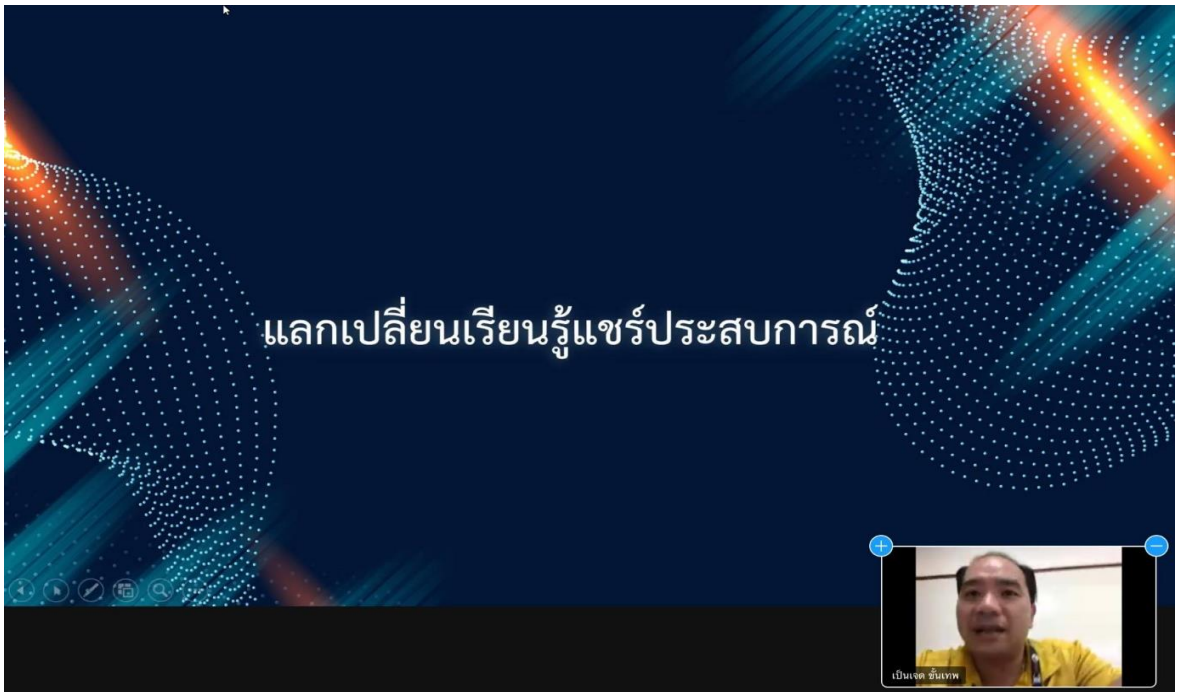
ภาพบรรยากาศวันกิจกรรมแลกเปลี่ยนเรียนรู้ Digital KM Day 2021

ผ่านรูปแบบออนไลน์ ระบบ zoom meeting

หัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)

ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

วันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 09.00 – 12.00 น.



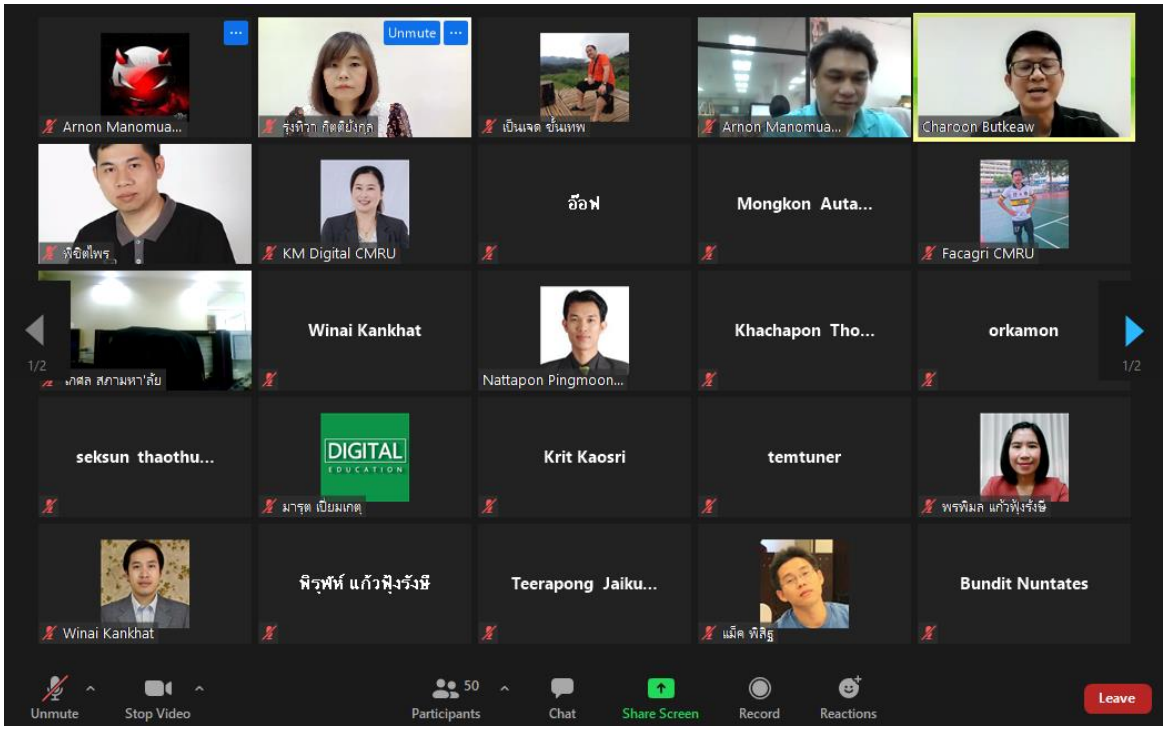
ภาพบรรยากาศวันกิจกรรมแลกเปลี่ยนเรียนรู้ Digital KM Day 2021

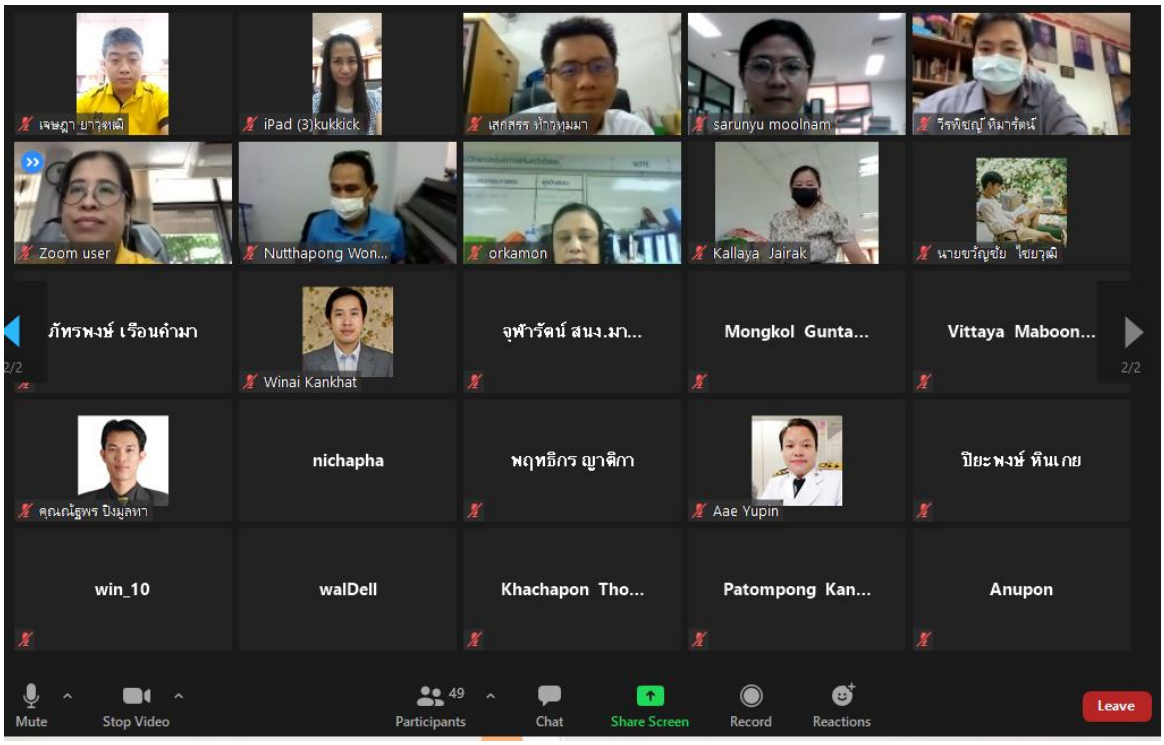
ผ่านรูปแบบออนไลน์ ระบบ zoom meeting

หัวข้อ การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)

ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

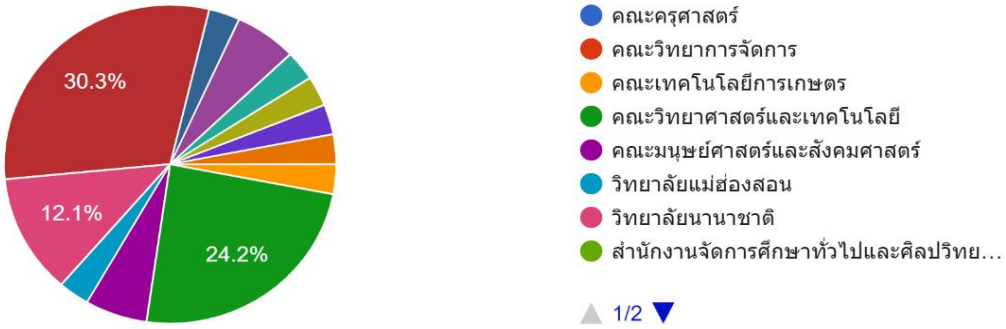
วันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 09.00 – 12.00 น.



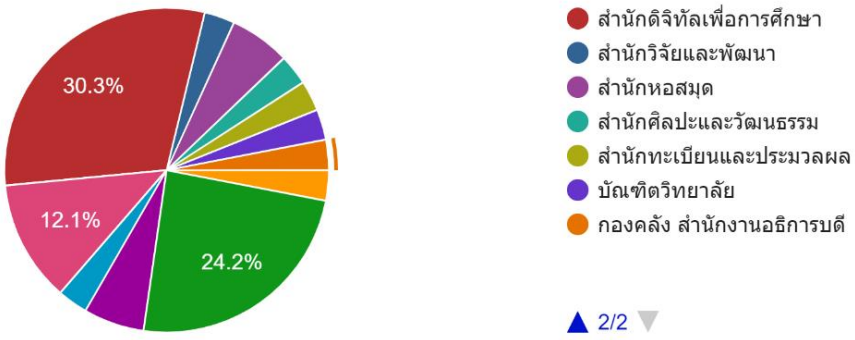


แบบประเมินความพึงพอใจโครงการแลกเปลี่ยนเรียนรู้
หัวข้อเรื่อง การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)
ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ ประจำปีงบประมาณ 2564

หน่วยงาน
คำตอบ 33 ข้อ

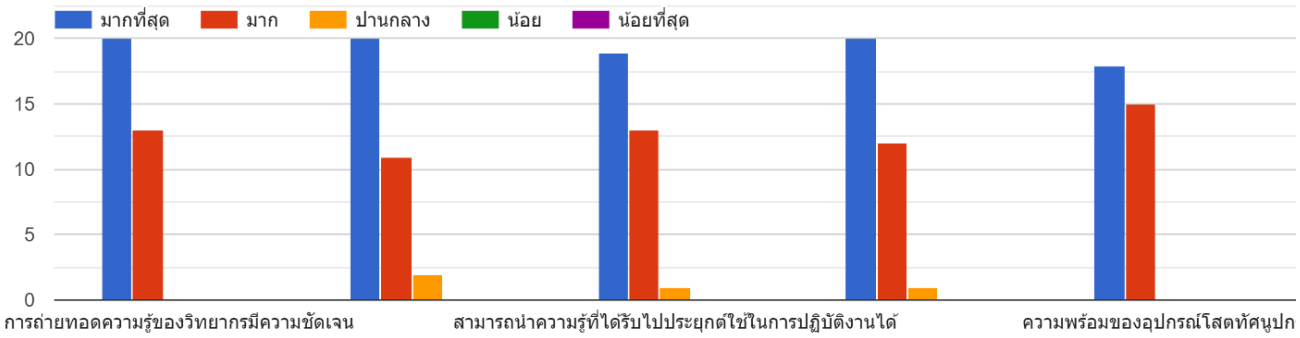


หน่วยงาน
คำตอบ 33 ข้อ

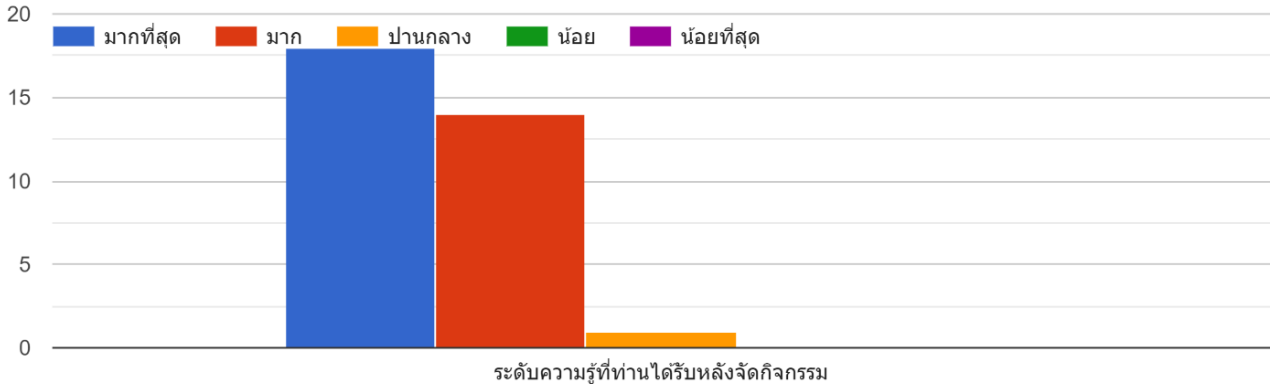


แบบประเมินความพึงพอใจโครงการแลกเปลี่ยนเรียนรู้
หัวข้อเรื่อง การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware)
ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่ ประจำปีงบประมาณ 2564

ระดับความพึงพอใจต่อการจัดกิจกรรมในภาพรวม



ระดับความรู้ที่ท่านได้รับหลังจัดกิจกรรม (เมื่อ 5 หมายถึง มากที่สุด และ 1 หมายถึงน้อยที่สุด)



ข้อเสนอแนะเพื่อปรับปรุงการจัดกิจกรรมครั้งต่อไปคำตอบ 5 ข้อ

1. จัดกิจกรรมบ่อย ๆ ครับ
2. ควรจัดกิจกรรมลักษณะเดียวกันนี้อีก
3. อยากให้มีการจัดอบรมแนวทางการรับมือกับ PDPA ครับ
4. น่าจะ download เอกสารประกอบการบรรยายได้
5. มีเวลาในการจัดกิจกรรมเพิ่มมากขึ้น (อาจจะจัดทั้งวัน)

คู่มือ

การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

สำนักดิจิทัลเพื่อการศึกษา

CONTENTS

1. ระบบรักษาความปลอดภัยภาพรวมของมหาวิทยาลัยราชภัฏเชียงใหม่
   - เกี่ยวกับ Ransomware
   - Operating System ที่ Ransomware เลือกในการโจมตี
   - วิธีการโจมตีหลัก ๆ ของ Ransomware
   - เมื่อถูก Ransomware โจมตีแล้วจะเป็นอย่างไร ?
   - อาการที่บ่งบอกว่าเครื่องของคุณอาจจะติด Ransomware
   - ช่องทางการโจมตีของ Ransomware
   - กลุ่มเป้าหมายในการโจมตี
   - ถ้าติด Ransomware แล้วต้องทำอย่างไร ?
   - วิธีรับมือกับ Ransomware
2. ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง
3. กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์
4. แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

ระบบรักษาความปลอดภัยภาพรวมของมหาวิทยาลัยราชภัฏเชียงใหม่

Ransomware คืออะไร ?

Ransomware จัดว่าเป็น Malware ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับ Malware ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัส หรือล็อกไฟล์ทุกประเภท ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ ส่วนมากจะต้องชำระด้วย Bitcoin แต่อย่างไรก็ตามการชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อคไฟล์ให้กับผู้ใช้งานเมื่อชำระแล้วจะได้รับ Key สำหรับการถอดรหัสไฟล์ ซึ่งก็ไม่สามารถการันตีได้ว่าจะกู้ได้จริงหรือไม่

วิธีการโจมตีหลัก ๆ ของ Ransomeware

- แฮกเกอร์ส่ง Spam Mail
- จาก Flash Drive ที่มี Malware
- จาก Website ที่เป็นอันตราย

→ ผ่านตัวกรอง Spam เข้ามาใน Inbox ของผู้ใช้คอมพิวเตอร์ → ผู้ใช้กดลิ้งค์ในเมลล์ที่แฮกเกอร์ส่งมา

แอนตี้ไวรัสตรวจจับไม่เจอไฟล์ Malware ฝังตัวลงในเครื่องของผู้ใช้

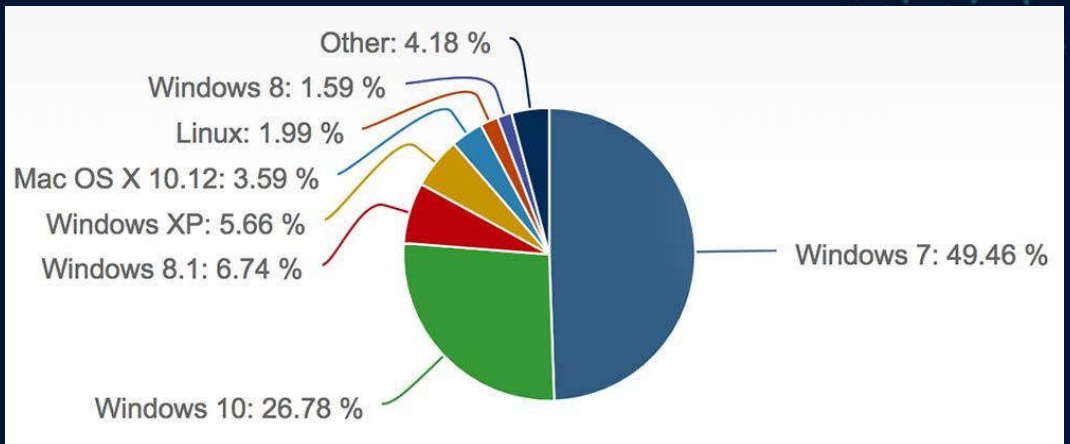
เข้ารหัสไฟล์ในเครื่องของผู้ใช้ หรือเข้าไปยังเซิฟเวอร์ส่วนกลางขององค์กร เพื่อเข้ารหัสข้อมูลสำคัญในเซิฟเวอร์

แฝงตัวเข้าไปยังคอมพิวเตอร์เครื่องอื่นๆ ที่มีการเชื่อมต่อกับเซิฟเวอร์ส่วนกลางขององค์กร

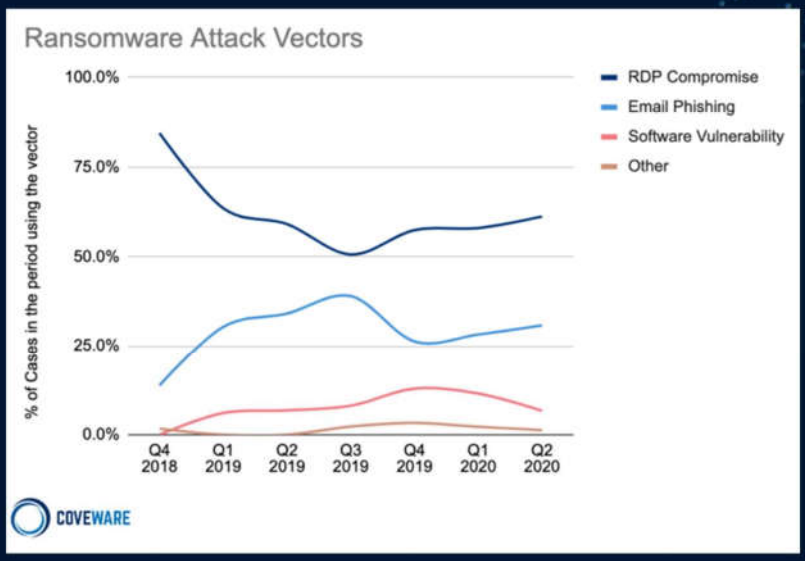
ส่งแจ้งเตือนเรียกค่าไถ่

แม้จะมีการจ่ายค่าไถ่ แต่ไฟล์ Malware ยังสามารถทิ้งซากไฟล์ที่ตรวจจับได้ยากไว้ในเครื่องหรือเซิฟเวอร์ เพื่อรอวันถูกกระตุ้นให้กลับมาทำงานอีกครั้ง

Operating System ที่ Ransomware เลือกโจมตี



การโจมตีผ่าน Service ต่าง ๆ



ตัวอย่าง Windows ขึ้นหน้าจอ Lock Screen

เมื่อ Ransomware เข้ารหัสไฟล์ของเครื่องเป้าหมายเป็นที่เรียบร้อยแล้วจะสร้างหน้าจอขึ้นมาเพื่อแจ้งรายละเอียดต่าง ๆ ตามที่ต้องการ บางกรณีจะไม่สามารถปิดหน้าจอนี้ได้เลย เนื่องจากถูกฝังลงไปใน Startup และแก้ไขค่า Registry ของ Windows ไปเป็นที่เรียบร้อยแล้ว

ตัวอย่าง Android Phone ขึ้น Pop Up ให้ชำระเงิน

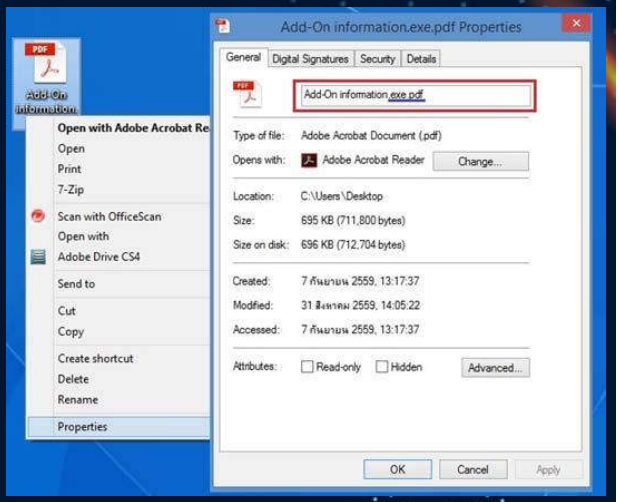
หน้าจอขึ้นมาเพื่อหลอกล่อเหยื่อ เพื่อให้ชำระเงิน หากต้องการได้ไฟล์กลับคืนมา บางกรณีเป็นแค่หน้าจอที่ทำมาหลอก ๆ เท่านั้น ซึ่งไฟล์นั้นอาจได้ถูกเข้ารหัสจริง ๆ ก็ได้

อาการที่บ่งบอกว่าคุณเครื่องของคุณอาจจะติด Ransomware

1. เครื่องทำงานช้าลงอย่างเห็นได้ชัด ทั้ง ๆ ที่ไม่ได้ใช้งานอะไรเลย
2. ไฟแสดงการทำงานของฮาร์ดดิสก์ กระพริบตลอดเวลา
3. การใช้อินเทอร์เน็ตช้าลง
4. มี Message ขึ้นหน้าจอ หรือ Popup แปลกๆ แจ้งเตือนเป็นจำนวนมาก
5. ใช้โปรแกรม Antivirus Scan ทั้งเครื่องก็ยังไม่หาย บางครั้งตรวจไม่พบ
6. มีไฟล์แปลก ๆ เพิ่มขึ้นมาใน Drive ต่าง ๆ โดยที่ไม่ได้มีการบันทึกอะไรลงไป
7. พื้นว่างที่ของฮาร์ดดิสก์ลดลง

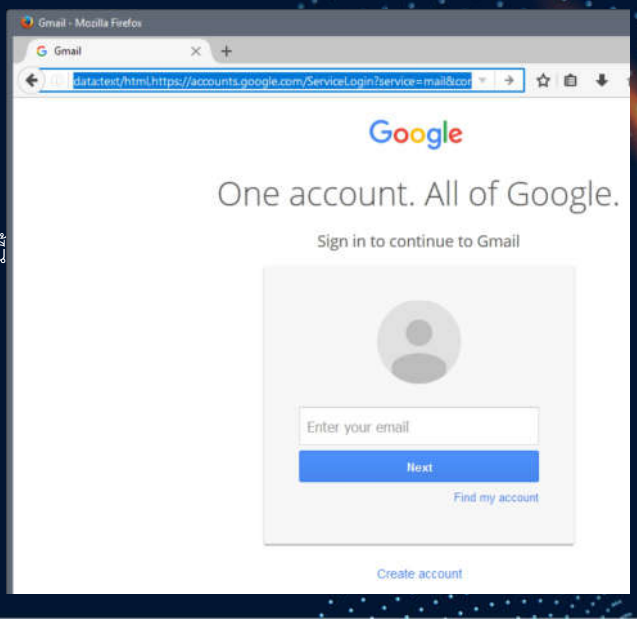
ช่องทางการโจมตีของ Ransomware

1. การโจมตีส่วนใหญ่จะมาทางอีเมล์หลอกลวงที่แนบไฟล์ Ransomware ไว้ โดยเนื้อหาในอีเมล์จะดึงดูดให้ผู้อ่านอยากคลิกเข้าไปอ่าน เช่น อีเมล์แจ้งเลขที่ใบสั่งซื้อสินค้า (OrderID) หากผู้ใช้ไม่คลิกไปเปิดไฟล์แนบ ก็อาจจะทำให้สูญเสียโอกาสทางการค้าได้ ซึ่งถ้าผู้ใช้คลิกเปิดไฟล์โดยไม่ระมัดระวังก็จะตกเป็นเหยื่อของ Ransomware ทันที ไฟล์แนบที่มากับอีเมล์จะเป็น zip file หากแตกไฟล์ออกมาก็จะพบไฟล์นามสกุล .doc, .xls หรือไฟล์อื่น ๆ ที่เราคุ้นเคย แต่ถ้าสังเกตดี ๆ จะพบว่านามสกุลของไฟล์จริง ๆ แล้วเป็น .exe เรียกเทคนิคการตั้งชื่อไฟล์แบบนี้ว่า Double Extensions



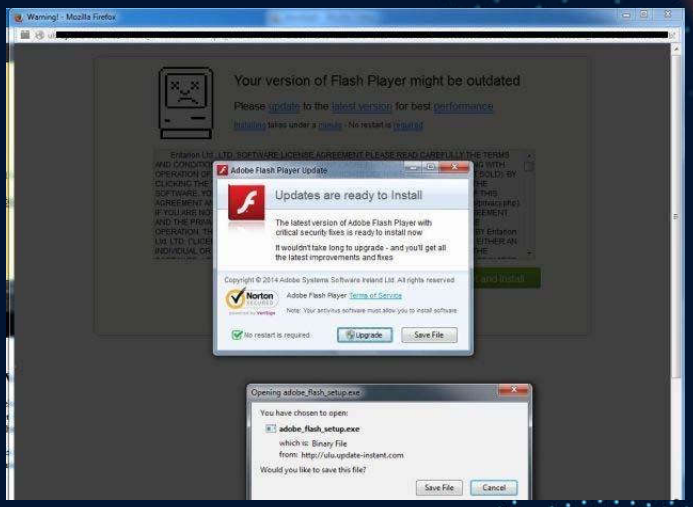
ช่องทางการโจมตีของ Ransomware

2. โจมตีด้วยวิธี Social Engineering เป็นการหลอกผู้ใช้งานให้ดาวน์โหลดโปรแกรมมาติดตั้งในเครื่อง เช่น ในขณะที่ใช้งานระบบลงทะเบียนเรียนออนไลน์ของมหาวิทยาลัย พบว่ามี Pop-up ขึ้นมาบอกว่า ให้ดาวน์โหลดโปรแกรมเสริมมาติดตั้งเพื่อให้สามารถลงทะเบียนได้สะดวก และรวดเร็วขึ้น ทั้ง ๆ ที่โปรแกรมนี้ไม่มีอยู่จริง หากผู้ใช้งานหลงเชื่อและทำการดาวน์โหลดมาติดตั้งไฟล์ต่าง ๆ ก็จะโดนจับเป็นตัวประกันทันที



ช่องทางการโจมตีของ Ransomware

3. โจมตีทางช่องโหว่ของ Browser รวมถึง Add-on, Plug-in ต่าง ๆ เช่น Java, Flash และ Acrobat Reader เป็นต้น



กลุ่มเป้าหมายของการโจมตี

1. กลุ่มคน ทั่วไปผู้ใช้งานตามบ้าน และในกลุ่มธุรกิจ หรือองค์กรที่ไม่มีหรือมีระบบรักษาความปลอดภัยทางไซเบอร์ โดยเฉพาะกลุ่มคนในแวดวงการศึกษา หรือมหาวิทยาลัย ที่มักตกเป็นเหยื่อบ่อยครั้ง เพราะจะต้องรับ –ส่ง ไฟล์หรือแชร์ไฟล์บ่อย ๆ โอกาสที่จะแพร่กระจายในระบบ Network เป็นไปได้ง่าย

2. ธุรกิจ หรือองค์กรต่าง ๆ ที่มีโอกาสในการจ่ายเงินสูง เช่น องค์กรภาครัฐ โรงพยาบาลธนาคาร องค์กรสาธารณสุข กองสลาก หรือองค์กรอื่น ๆ ที่มีความคล้ายคลึงกัน

3. ธุรกิจหรือองค์กรที่ถือข้อมูลสำคัญ เช่น องค์กรที่เกี่ยวกับกฎหมาย ข้อมูลประชากร กรมการขนส่ง ข้อมูลบัตรเครดิต สินเชื่อ

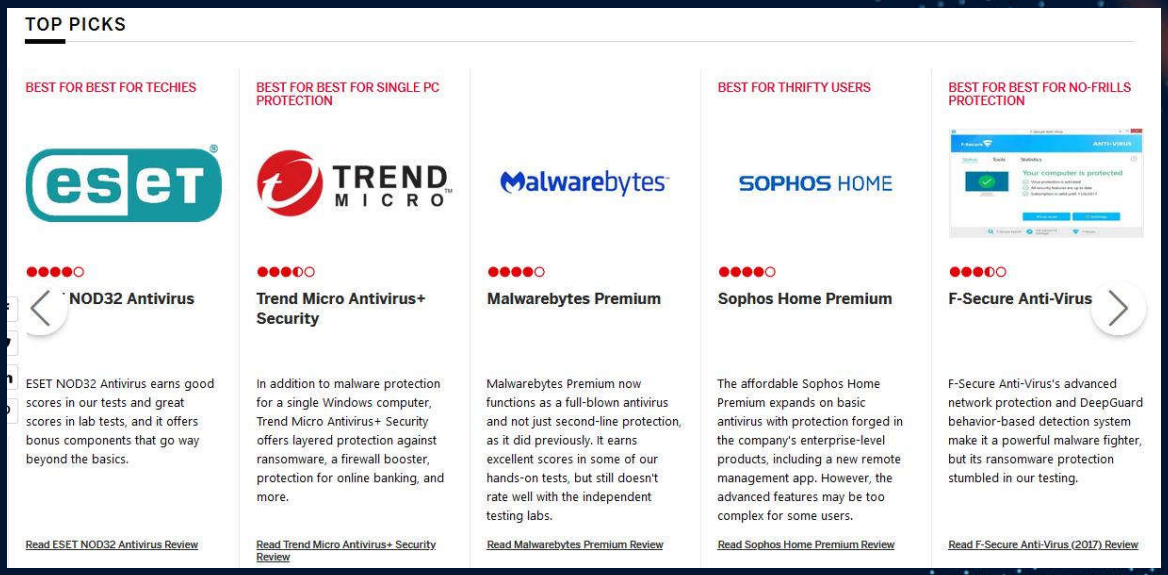
ถ้าติด Ransomware ต้องทำอย่างไร ?

1. ตัดการเชื่อมต่อเครือข่ายออกเพื่อป้องกันการลุกลามไปยังเครื่องอื่น
2. หาโปรแกรมที่สามารถยับยั้งการทำงานของ Ransomeware ได้ เช่น Malwarebyte, Kaspersky, Mcafee
3. ไม่ควรจ่ายเงินให้โจร เพราะโอกาสที่จะได้ไฟล์กลับคืนมานั้นน้อยมาก
4. ปรึกษาผู้เชี่ยวชาญเพื่อขอคำแนะนำเพิ่มเติม
5. เครื่องมือถอดรหัสออนไลน์อาจช่วยได้ : โดยมีเครื่องมือที่เรียกว่า “Crypto Sheriff” ที่ใช้ในการระบุว่า Malware หรือไวรัสที่ติดคอมพิวเตอร์ของคุณนั้นเป็นชนิดใด จากนั้นระบบจะค้นหาแหล่งทรัพยากรอย่าง No More Ransom เพื่อดูว่ามีคีย์ถอดรหัสสำหรับสายพันธุ์นั้น ๆ หรือไม่ หากเป็น Ransomware สายพันธุ์ธรรมดา ก็มีโอกาสสูงที่คุณอาจสามารถกู้ไฟล์คืนได้

วิธีรับมือกับ Ransomware

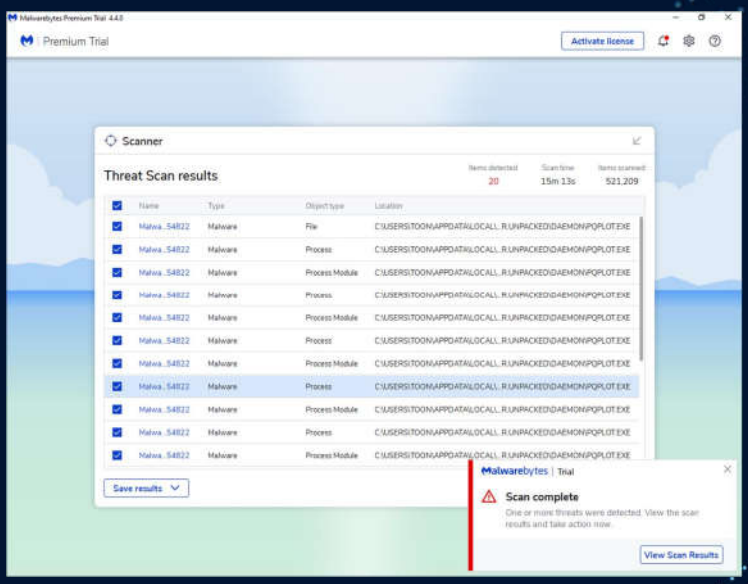
1. อัพเดตระบบปฏิบัติการ (Operating System) และโปรแกรมอื่น ๆ บ่อย ๆ
2. ติดตั้งโปรแกรมแอนตี้ไวรัสที่มีการป้องกัน Ransomware เช่น Malwarebyte
3. ไม่คลิกลิงก์แปลก ๆ หรือดาวน์โหลดไฟล์ที่ไม่มี Crack หรือนามสกุลแปลกๆ
4. สำรองข้อมูลไว้หลายที่ เช่น เก็บบน Cloud หรือ External Harddisk
5. กรณีที่ต้องแชร์ไฟล์กันในเครือข่าย ควรกำหนดสิทธิ์ในการเข้าถึง ป้องกันไฟล์สำคัญด้วย Read-Only
6. ปิดการเข้าถึงข้อมูลจากระยะไกล Remote Desktop และโปรแกรมรีโมทต่างๆ
7. กรณีที่ใช้ระบบ Virtual Machine ควรมีการสำรองข้อมูล ตรวจสอบไฟล์ Snap Shot
8. ใช้ซอฟต์แวร์ลิขสิทธิ์แท้

ตัวอย่างโปรแกรม Antivirus ที่นิยมใช้กันในปัจจุบัน



https://www.pcmag.com

ตัวอย่างโปรแกรม Malwarebyte



ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง

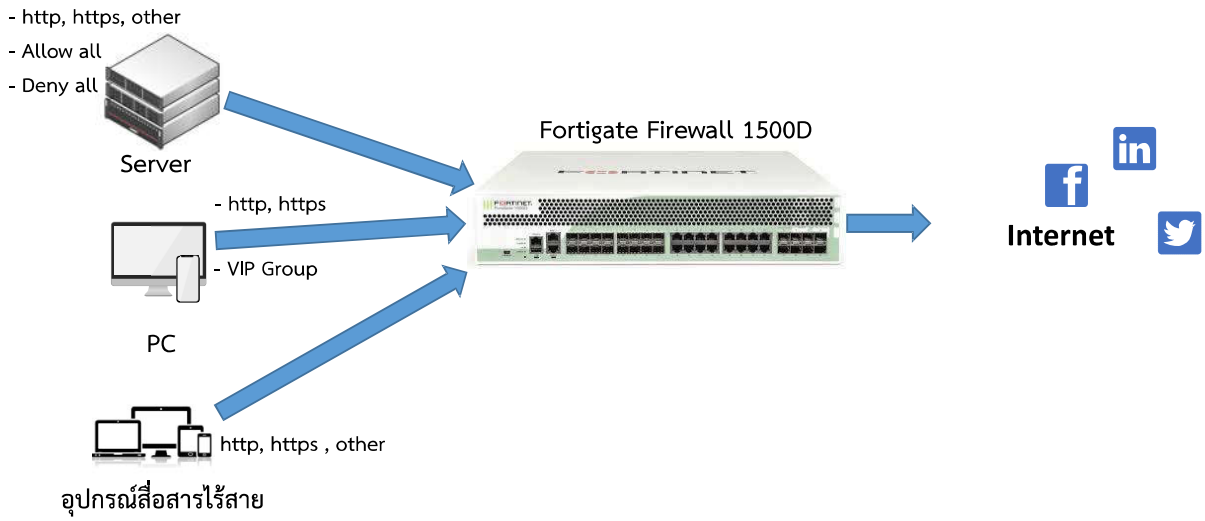
ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง

1. ภัยคุกคามทางระบบฮาร์ดแวร์ (Physical)
   - กระแสไฟฟ้าดับ
   - ไฟไหม้
   - การถูกขโมยเครื่อง และอุปกรณ์คอมพิวเตอร์
   - อุปกรณ์ถูกทำลายเสียหาย

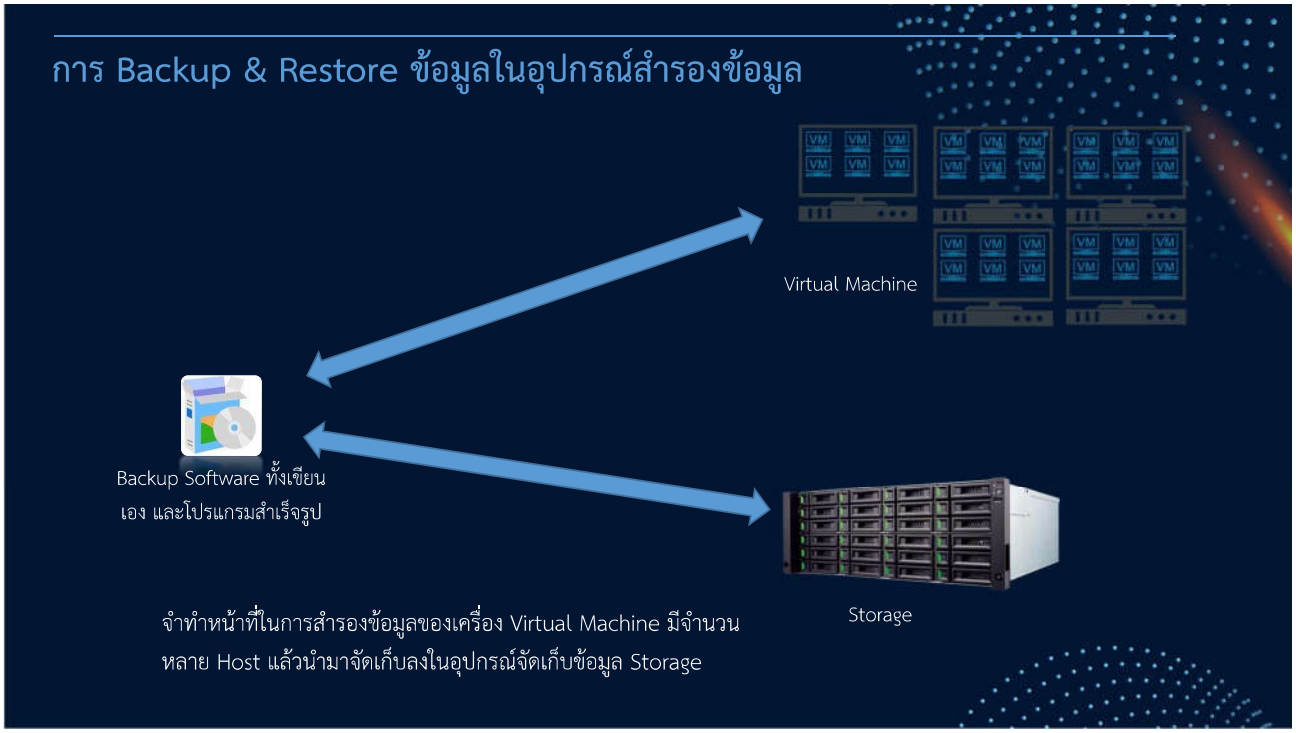
2. ภัยคุกคามทางซอฟต์แวร์ (Logical)
   - ถูก Hacker โจมตีด้วยวิธีการต่าง ๆ
   - ติดไวรัส Worm, Malware, Trojan, Spyware, Backdoor, DDOS .....
   - Phishing ขโมยข้อมูลสำคัญส่วนตัว โดยหลอกให้กรอกข้อมูลคล้ายกับเว็บไซต์ของจริง
   - Spam Mail ส่งข่าวสารเชิญชวน โฆษณาสินค้าและบริการ ทำให้เกิดความรำคาน
   - Sniffing การดักจับข้อมูล

การเตรียมความพร้อมในการรับมือภัยคุกคามคอมพิวเตอร์
ของมหาวิทยาลัยราชภัฏเชียงใหม่

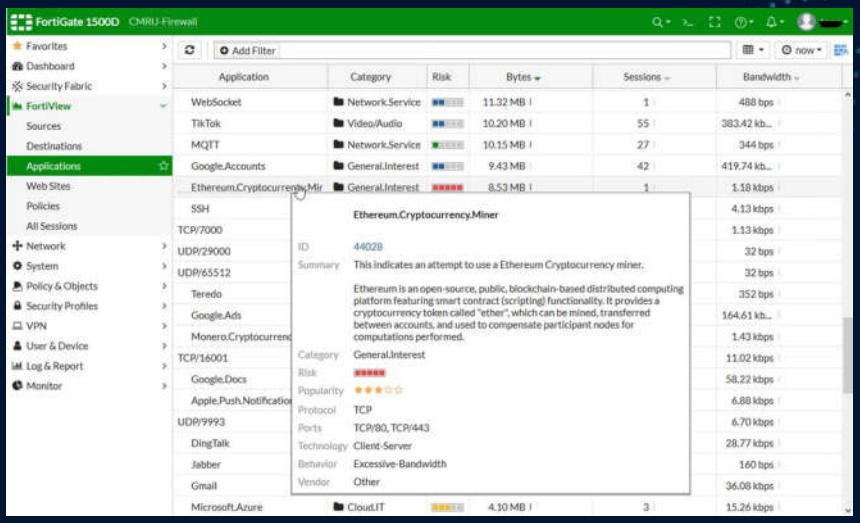
เข้มงวดการเข้าถึงอินเทอร์เน็ตของผู้ใช้งานภายในองค์กรด้วย Firewall Policy



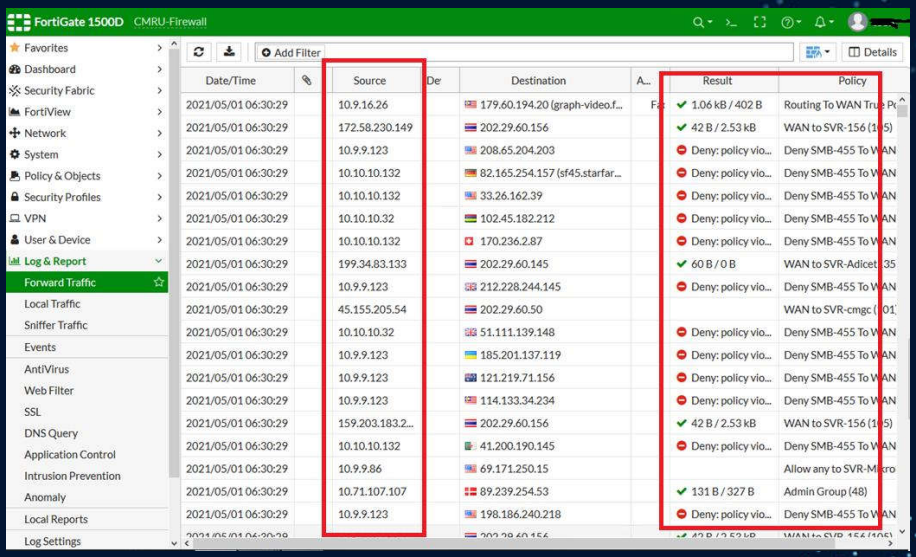
เข้มงวดการ Access เข้ามาจากภายนอก โดยจัดทำ Policy ให้เหมาะสมกับการใช้งาน



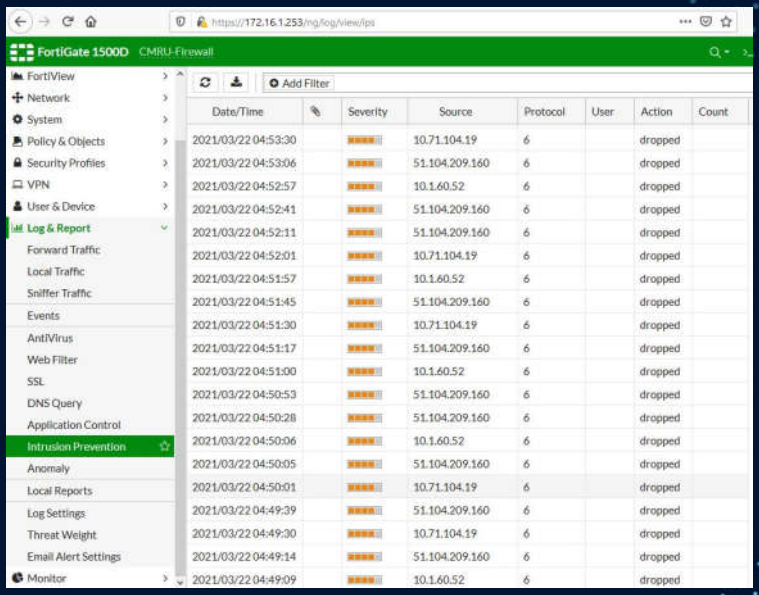
ตรวจสอบ Firewall Log เพื่อแก้ไขจุดบกพร่องต่าง ๆ



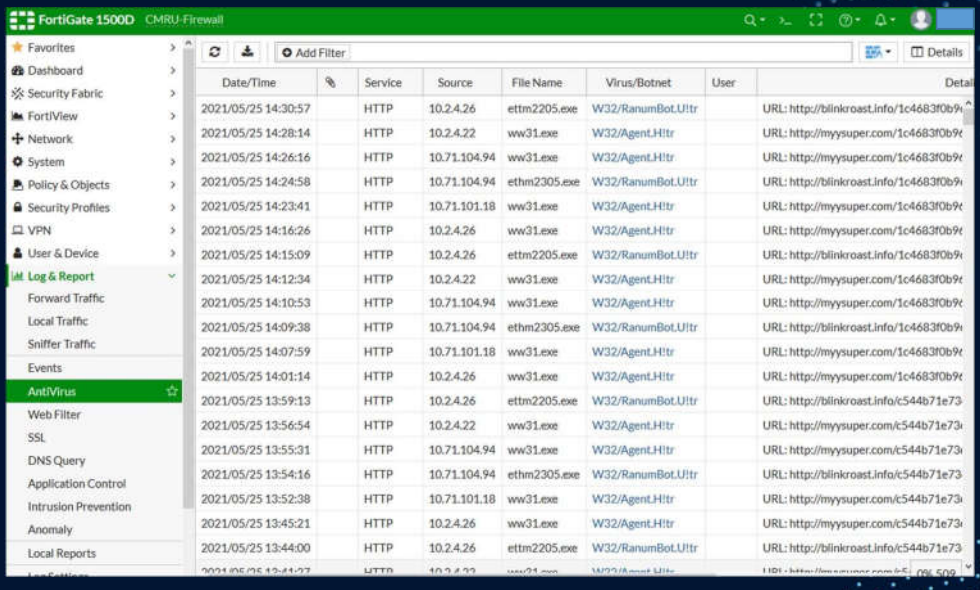
ตรวจสอบเครื่องที่ติด Ransomware



ตรวจสอบการทำงานของ IPS บน Firewall

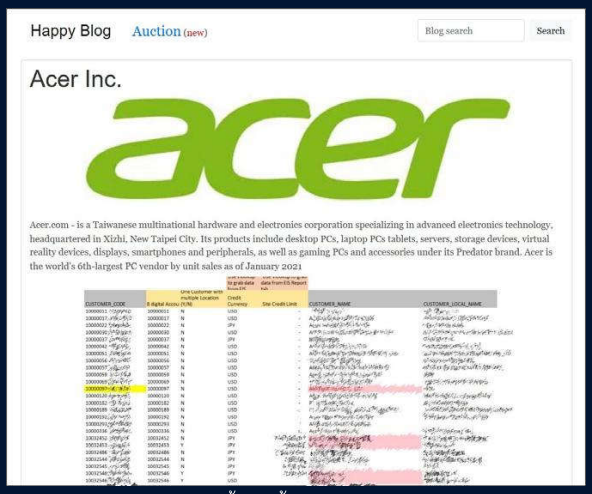


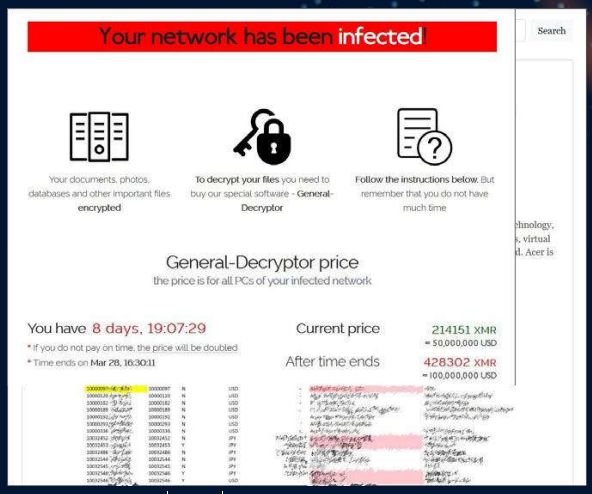
การตรวจสอบ Antivirus บนอุปกรณ์ Firewall



กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์ (หน่วยงานภาครัฐ และเอกชนภายนอก)

Acer บริษัทยักษ์ใหญ่แห่งวงการคอมพิวเตอร์ถูกโจมตีด้วย REvil ransomware โดยมีการเรียกค่าไถ่เป็นจำนวนสูงที่สุดเท่าที่เคยมีมา ที่ 50 ล้านดอลลาร์

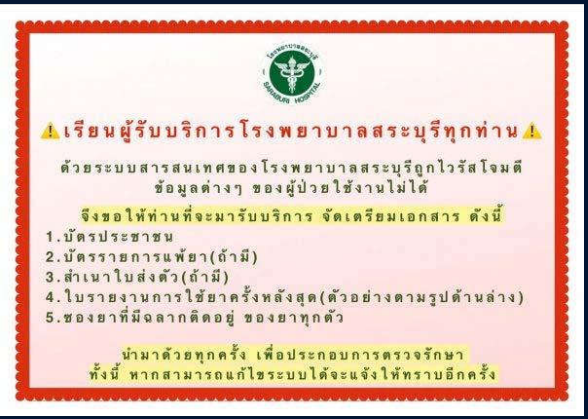




หลักฐานว่าการโจมตี Acer นั้นเกิดขึ้นจริง เช่น ข้อมูลทางการเงิน ยอดคงเหลือในธนาคาร และข้อมูลที่ติดต่อสื่อสารกับธนาคาร เป็นต้น ผู้โจมตีเสนอส่วนลดให้ 20% หากชำระเงินภายในวัน เวลา ที่กำหนด และจะจัดหาตัวถอดรหัส รายงานเรื่องช่องโหว่ และลบไฟล์ที่ขโมยมาทั้งหมดเป็นการตอบแทน

https://www.beartai.com/news/itnews/576375

แฮกเกอร์ส่ง'มัลแวร์'เรียกค่าไถ่ รพ.สระบุรี เป็นเงินทั้งสิ้น 200,000 Bitcoin หรือราว ๆ 63,000 ล้านบาท



เนื่องด้วย เมื่อวันที่ ๕ กันยายน ๒๕๖๓ โรงพยาบาลสระบุรี ได้รับการโจมตีจากไวรัสเรียกค่าไถ่ชื่อ Ransomware ทำให้ข้อมูลการบริการรวมถึงระบบสนับสนุนทั้งหมดได้รับความเสียหาย และโรงพยาบาลไม่สามารถเข้าถึงข้อมูลได้ ซึ่งส่งผลกระทบกับประชาชนทำให้ได้รับบริการล่าช้าและไม่มีข้อมูลการรักษาพยาบาลเดิม โรงพยาบาลสระบุรีได้ดำเนินการแก้ไขโดยเริ่มระบบการทำงานด้วยมือทั้งหมดโดยทันที และกู้คืนฐานข้อมูลจากแหล่งอื่น ๆ ทำให้กู้คืนข้อมูลบางส่วนกลับมาได้ได้แก่ ผล LAB ผล X-Ray และประวัติยาเดิมบางส่วน เหตุการณ์ดังกล่าว แม้ทางโรงพยาบาลสระบุรีจะมีการสำรองข้อมูลสม่ำเสมอทุกวันและเก็บสำรองไว้ ๓ วัน แต่เนื่องจากการโจมตีฐานข้อมูลได้กระทำอย่างรวดเร็วและการกระทำระหว่างสำรองข้อมูล จึงไม่สามารถป้องกันฐานข้อมูลไว้ได้ ฐานข้อมูลที่ยังรักษาไว้ได้มีเพียงฐานข้อมูลก่อน ๓๑ มกราคม ๒๕๖๐ โรงพยาบาดสระบุรีจะเร่งดำเนินการแก้ไขโดยการถอดรหัส และวางระบบปฏิบัติการทางคอมพิวเตอร์ใหม่

https://www.dailynews.co.th/regional/794273

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์ (ของมหาวิทยาลัยราชภัฏเชียงใหม่)

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์

เครื่อง Windows Server ถูก Ransomware โจมตีในปี 2020

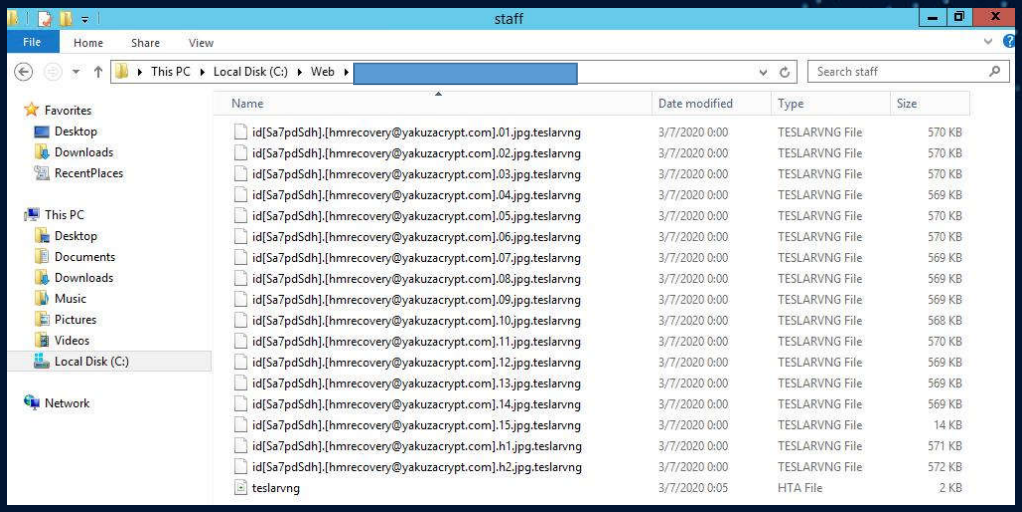
<u>สาเหตุเกิดจาก</u>

1. เครื่องไม่ได้ทำการ Update Patch
2. คาดว่าจะถูกเจาะผ่านทาง Remote Desktop
3. มีลักษณะของการ Share Drive คาดว่าใช้รหัสเดียวกันกับ Remote Desktop
4. โปรแกรม Antivirus หมดอายุ

<u>วิธีการแก้ไข</u>

1. Restore Backup วันล่าสุดก่อนที่จะถูกโจมตีขึ้นมาใช้งาน
2. Update Patch ของ Windows ให้เป็นปัจจุบัน
3. ติดตั้งโปรแกรม Antivirus, Malwarebyte
4. จัดทำ Firewall Policy ใหม่ให้รัดกุมมากขึ้น

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์



กรณีเครื่อง Windows Server ถูก Ransomware โจมตีในปี 2020

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์

กรณีเครื่อง Linux Server ถูกเจาะเข้ามาแล้วสร้างไฟล์ใน Server เป็นจำนวนมาก

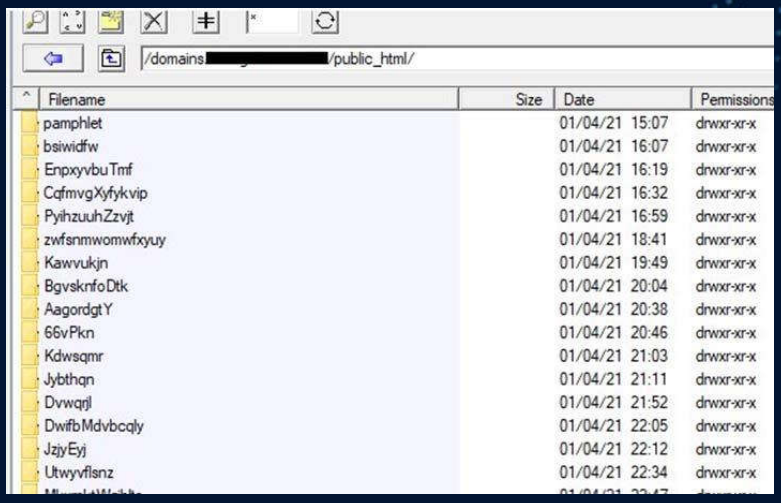
<u>สาเหตุเกิดจาก</u>

1. เครื่อง Server ไม่ได้ทำการ Update Patch
2. เจาะเข้ามาผ่านช่องโหว่ของ PHP Version เก่า และ Server มีการเปิดให้รัน CGI ผ่านทาง PHP Script
3. รหัสของเว็บไซต์สามารถคาดเดาได้ง่ายมากเกินไป เช่น “cmru1234”, “tak1234”, “aaaabbbb”
4. โปรแกรมภาษา PHP ยังคงเป็น Version เก่า 5.xx
5. เว็บไซต์ไม่มี SSL เนื่องจากไม่รองรับ

<u>วิธีการแก้ไข</u>

1. Update Patch ของ OS ให้ใหม่ล่าสุด
2. ลบไฟล์ที่น่าสงสัยทิ้ง
3. กำหนดสิทธิ์การเข้าถึงในแต่ละ Folder ให้เหมาะสม
4. เปลี่ยนรหัสผ่านทุกอย่าง รหัสผ่าน Root, MySQL, FTP โดยเพิ่มความยากของตัวอักษรเข้าไป
5. แนะนำให้ admin ที่ดูแลเว็บไซต์นั้นย้ายไปใช้บริการ Server ที่มี PHP Version ใหม่ และรองรับ SSL

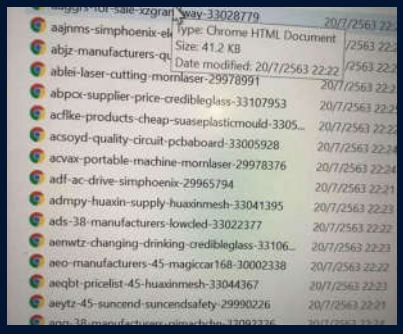
กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์



กรณีเครื่อง Linux Server ถูกเจาะเข้ามาแล้วสร้างไฟล์ใน Server เป็นจำนวนมาก

สั่ง Run Command เพื่อใช้เครื่อง Server ในการขุด Bitcoin

```
Apr28   0:00 sh -c ./xmrig -a cryptonight -o stratum+tcp://xmr.pool.minergate.com:45700 -u castorforelli42@gmail.com -p x 2>&1
Apr28 167726:32 ./xmrig -a cryptonight -o stratum+tcp://xmr.pool.minergate.com:45700 -u castorforelli42@gmail.com -p x
```



กรณีเครื่อง Linux Server ถูกเจาะเข้ามาเพื่อใช้เป็นเครื่องขุด Bitcoin

แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

1. หมั่นตรวจสอบการ Update ของ OS รวมไปถึงโปรแกรม Antivirus, Spyware, Malware ต่าง ๆ
2. การตั้งรหัสผ่านจะต้องตั้งค่าให้มีความยากต่อการคาดเดา
3. มีการสำรองข้อมูลอย่างสม่ำเสมอ มีตารางการสำรองข้อมูลที่แน่นอน และจัดเก็บข้อมูลไว้มากกว่า 1 แหล่งเสมอ
4. ทดสอบการกู้คืนข้อมูล เพื่อให้แน่ใจว่าข้อมูลที่สำรองไว้นั้นสามารถนำมาใช้งานได้จริง
4. ควบคุมการเข้าถึงเครือข่าย และระบบสารสนเทศ จำกัดสิทธิ์ในการเข้าถึงทรัพยากรในระบบเครือข่ายให้สามารถเข้าถึงได้เฉพาะเครื่องที่จำเป็นเท่านั้น
5. ไม่ควรเปิดไฟล์ที่ถูกส่งมาทาง E-mail หรือ กด Link ที่ไม่รู้จัก
6. กรณีที่จำเป็นต้องทำการ Remote มายังเครื่อง Server จากภายนอกมหาวิทยาลัย ต้องใช้งานผ่าน VPN เท่านั้น

แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (ต่อ)

7. ใช้ Software ที่ถูกต้องตามลิขสิทธิ์เท่านั้น หลีกเลี่ยงการใช้ Software เถื่อนที่มี Crack
8. ผู้ดูละระบบต้องตรวจสอบความผิดปกติของเครื่อง Server และข้อมูลบันทึกกิจกรรม (log) อย่างสม่ำเสมอ
9. ตรวจสอบช่องโหว่ ของระบบสารสนเทศ หรือซอฟต์แวร์ที่ให้บริการ อย่างสม่ำเสมอ และให้รีบแก้ไขช่องโหว่ทันทีหากพบว่าเป็นความเสี่ยงที่รุนแรง
10. ประเมินความเสี่ยงทางด้านระบบสารสนเทศอย่างสม่ำเสมอ มีการประชุมเพื่อสรุปปัญหาที่ได้พบจากการปฏิบัติงาน
11. ลดการใช้ Flash Drive ในการโอนถ่ายข้อมูล เพราะปัจจุบัน Cloud Services อย่าง Google Drive, OneDrive
12. อย่าเปิดเผยข้อมูลส่วนตัวเช่น E-mail หรือเบอร์โทรศัพท์โดยไม่จำเป็น

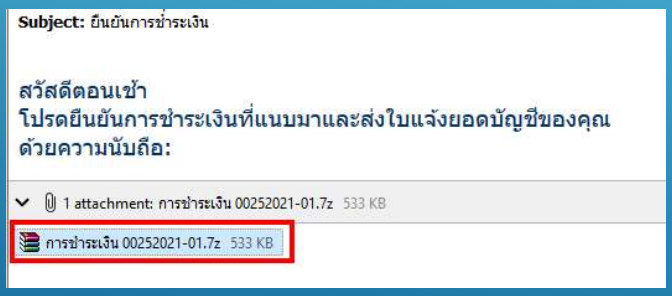
กรณีศึกษาเกี่ยวกับ RANSOMWARE ที่ฝ่ายซ่อมบำรุงคอมพิวเตอร์พบเจอในฝั่งของผู้ใช้ทั่วไป (END-USER)

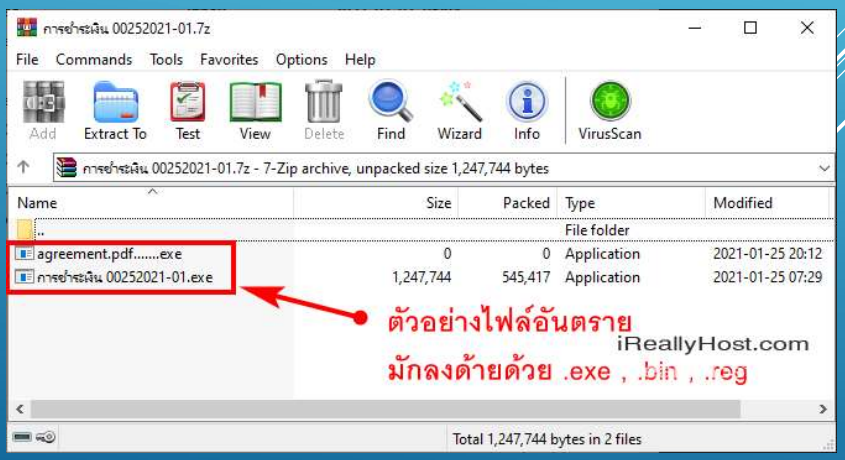
หน้าที่ของฝ่ายซ่อมบำรุงคอมพิวเตอร์

- ติดตั้งซอฟต์แวร์ให้แก่ผู้ใช้บริการ
- แก้ไขปัญหาเกี่ยวกับการใช้งานคอมพิวเตอร์
- แก้ไขปัญหาไวรัสคอมพิวเตอร์และการกู้ข้อมูล
- ให้คำปรึกษาเกี่ยวกับการใช้งานคอมพิวเตอร์

สาเหตุหลักที่ผู้ใช้งานติด Ransomware

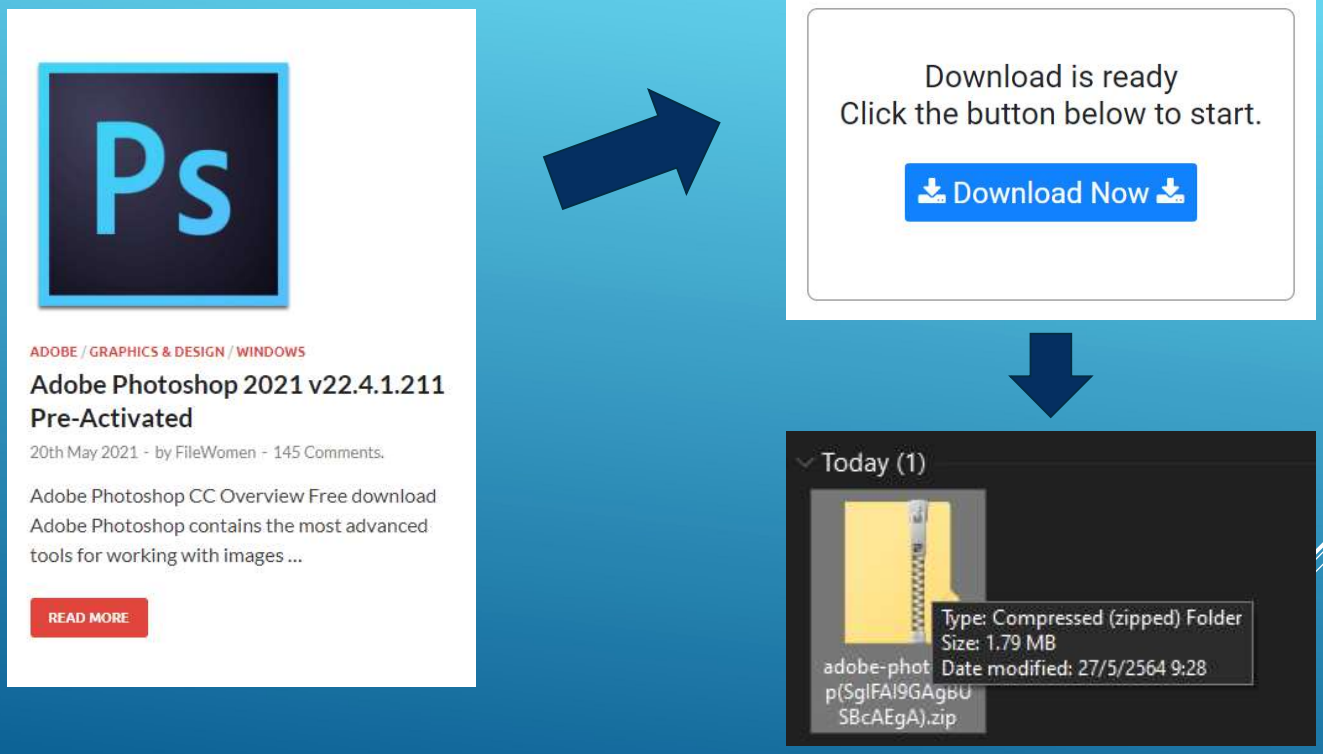
- ติดจากไฟล์ในรูปแบบ Double Extension /ลิ้งค์ที่แนบมากับอีเมล





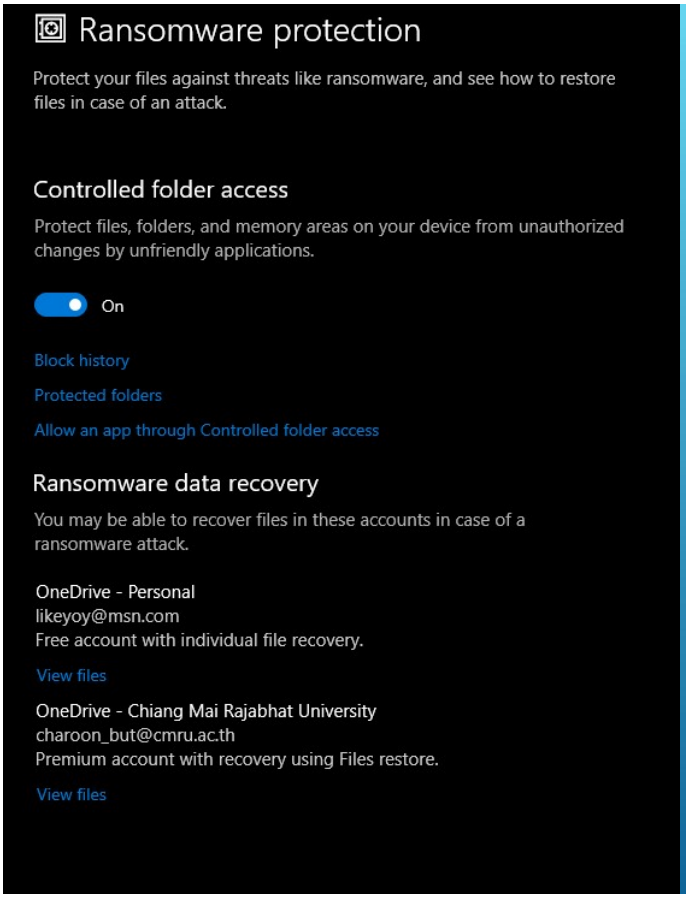
สาเหตุหลักที่ผู้ใช้งานติด Ransomware

- ติดจากการดาวน์โหลดไฟล์ในอินเทอร์เน็ต
- ติดจากการดาวน์โหลดโปรแกรมในอินเทอร์เน็ต



การป้องกัน Ransomware

1. อัพเดทระบบปฏิบัติการและโปรแกรมแอนตี้ไวรัสอย่างสม่ำเสมอ
2. ดาวน์โหลดไฟล์ต่าง ๆ จากแหล่งที่น่าเชื่อถือเท่านั้น
3. หาความรู้และอัพเดทข่าวสารเกี่ยวกับการรักษาความปลอดภัยเพิ่มเติม
   - https://www.thaicert.or.th/index.html
   - https://www.bleepingcomputer.com/
   - เว็บไซต์เกี่ยวกับข่าวสารไอทีต่าง ๆ



การป้องกัน Ransomware

3. วิธีป้องกัน Ransomware ของ Windows 10 ด้วยการเปิดฟังก์ชั่นป้องกันไวรัสเรียกค่าไถ่

Windows Security > Virus & threat protection > Ransomware protection

การแก้ไข Ransomware

1. ตัดการเชื่อมต่อกับเครือข่ายทันที
2. ค้นหาข้อมูลของ Ransomware เพื่อหาวิธีแก้ไข
3. Format Hard disk ทิ้งทั้งหมดแล้วติดตั้งระบบปฏิบัติการและโปรแกรมใหม่

Visio ที่ใช้ทำโปรเจ็กต์ 3/19/20
Project E-learning.RAR.acfmceb 12/26/2
บทที่ 1 Intelligence E-learning.DOC.acfmceb 8/11/20
บทที่ 2 Intelligence E-learning.DOC.acfmceb 2/16/20
บทที่ 3 Intelligence E-learning.DO
บทที่ 4 Intelligence E-learning.DO
หน้าปกโปรเจ็กต์.DOC.acfmceb
หัวข้อ Intelligence E-learning DO

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Overwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open http://4ocjd3ubbxq6ykw7.onion.cab or http://4ocjd3ubbxq6ykw7.tor2web.org in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from http://torproject.org/

2. In the Tor Browser open the http://4ocjd3ubbxq6ykw7.onion/
   Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

Write in the following public key in the input form on server. Avoid missprints.

```
OZQJAG-YNVWCY-QIJXQ6-TEHMOR-4AEBNG-RCQMGA-LRL4VB-N5DRQ2
MM34BA-P4XFZW-C3TR2F-4Y5KES-BMSKNO-YPRT2K-ULKIVJ-MRGJXQ
F3HENQ-7QLJJJ-ESVJLK-6BGWZU-RVXIDO-IJNGQQ-IZE2J4-5XFQAO
```

Follow the instructions on the server.

These instructions are also saved to file named DecryptAllFiles.txt in Documents folder. You can open it and use copy-paste for address and key.

Google CTB-Locker

https://www.pcrisk.com › removal-guides ▾ แปลหน้านี้

How to remove CTB-Locker Ransomware [Updated] - virus ...

6 ส.ค. 2563 — What is 'Your personal files are encrypted by CTB-Locker'? CTB-Locker ransomware virus infiltrates operating systems via infected email ...

Threat Type: Ransomware, Crypto Virus, File... **Malware Removal (Windows):** To eliminat...
Name: CTB-Locker virus

Description · Removal · Isolating the infected device. · Identifying the ransomware...

https://news.sophos.com › 2015/12/31 › t... ▾ แปลห

The current state of ransomware: CT

31 ธ.ค. 2558 — CTB-Locker is a ransomware variar
before demanding a ransom be paid to decrypt the f

https://th.k2rx.com › how-remove-ctb-locker-encrypt

วิธีการ: ลบไวรัสการเข้ารหัสลับของ CTE

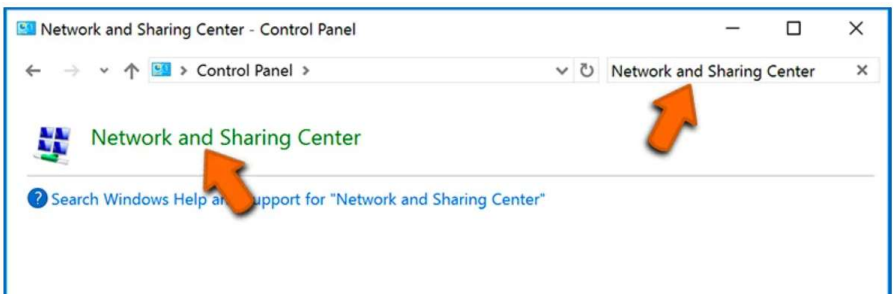
CTB-Locker เป็น ransomware ที่ออกแบบมาเพื่อสแกน

spread throughout the entire local network. For this reason, it is very important to isolate the infected device (computer) as soon as possible.

Step 1: Disconnect from the internet.

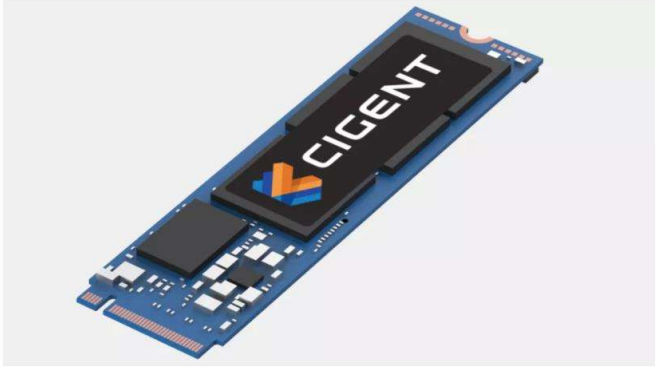
The easiest way to disconnect a computer from the internet is to unplug the Ethernet cable from the motherboard, however, some devices are connected via a wireless network and for some users (especially those who are not particularly tech-savvy), disconnecting cables may seem troublesome. Therefore, you can also disconnect the system manually via Control Panel:

Navigate to the "**Control Panel**", click the search bar in the upper-right corner of the screen, enter "**Network and Sharing Center**" and select search result:



OVERCLOCK ZONE NEWS FEATURED PC DIY GAMING TECH ZONE VIDEO AR

SSD รุ่นใหม่ จะมีระบบป้องกัน Ransomware และการโจรกรรมข้อมูลในตัว



Update : 21 May 2021
View : 17,436

Cigent Secure SSD Technical Specifications

NVMe Internal or External SSD
- 480GB
- 1TB
- 2TB

Cigent D3E
- Lifetime D^{3}E software license

Operating System Support
- Microsoft Windows® 7, 8, and 10

Compliance
- HIPAA
- GLBA
- NIST 800-88

Specs
- Interface: PCIe Gen3x4 NVMe 1.3
- Form factor: M2 2280-D3
- Operating temperature: 0° to 70° C
- Non-operating temperature: -40° to -85° C
- NAND Flash: 3D TLC
- TCG Opal 2.0
- Remotely upgradeable firmware
- USB adapter and cable (USB 3.0/USB-C) (external drive only)
- Warranty: 12-months hardware warranty

“หลักการทำงานของตัว Drive ก็คือ เมื่อมีการตรวจพบสิ่งที่ไม่ปลอดภัย มันจะทำการเข้ารหัสและซ่อนข้อมูลจาก OS Layer ให้ไปอยู่ใน "Safe Room" เพื่อเป็นการตัดไฟแต่ต้นลม .. ส่วนที่ว่าตัว SSD จะตรวจจับและรู้ได้ยังไงว่ามันเป็น Ransomware นั้น อันนี้เท่าที่ทราบก็คือจะเป็นการตรวจสอบในระดับ Firmware ซึ่งมีการใช้เทคโนโลยี Machine Learning เพื่อเรียนรู้และทำความรู้จักกับ Ransomware รุ่นใหม่ๆอย่างต่อเนื่อง พร้อมเรียนรู้จากพฤติกรรมการเข้าถึงไฟล์ที่ผิดสังเกต”

ภาพบรรยากาศวันกิจกรรม CMRU KM Day ประจำปี 2564 :

การจัดการความรู้กับการพัฒนาคนและองค์กร

วันที่ 2 มิถุนายน 2564 เวลา 13.00 – 16.00 น.

ณ ห้องประชุมเอื้องสายส่องแสง สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่

DIGITAL
EDUCATION

สำนักดิจิทัลเพื่อการศึกษา
มหาวิทยาลัยราชภัฏเชียงใหม่

202 ถ.ช้างเผือก ต.ช้างเผือก อ.เมือง จ.เชียงใหม่
โทร. 0-5388-5924, โทรสาร. 0-5388-5924

www.digital.cmru.ac.th