หลักสูตร
ความมั่นคงปลอดภัยไซเบอร์พื้นฐาน

CYBERSECURITY FUNDAMENTALS

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา เชียงใหม่

สารบัญ

โครงการฝึกอบรมหลักสูตรความมั่นคงปลอดภัยไซเบอร์พื้นฐาน

(Cybersecurity Fundamentals)

จัดโดย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา เชียงใหม่

หลักการและเหตุผล

ในการใช้ชีวิตในปัจจุบัน เราใช้ชีวิตเชื่อมโยงกับอินเทอร์เน็ตมากมายในหลากหลายมิติมาก เช่น การทำธุรกรรมผ่านระบบออนไลน์ การทำงานหรือการจัดประชุมผ่านระบบอิเล็กทรอนิกส์ หรือแม้กระทั้งการสืบค้น การส่งต่อข้อมูลสารสนเทศที่เกิดขึ้นอย่างรวดเร็ว ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทยในปี พ.ศ. 2563 ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ ETDA กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม นั้น พบว่า คนไทยใช้อินเทอร์เน็ตในการทำกิจกรรมมากมาย ตั้งแต่การทำธุรกรรมออนไลน์ (56.5%) การซื้อของ (67.3%) การหาข้อมูล (82.2%) การติดต่อสื่อสาร (77.8%) ความบันเทิง (ดูหนัง/คลิป/โทรทัศน์/ฟังเพลง ที่ 85%) และอื่น ๆ อีกมากมาย ทั้งหมดนี้ หากการรักษาความมั่นคงปลอดภัยไซเบอร์อ่อนแอ ก็อาจทำให้ผู้ประสงค์ร้ายเข้ามาทำอันตรายต่อเราและข้อมูลส่วนบุคคลของเราได้ ตั้งแต่การเข้าถึงข้อมูลส่วนบุคคลของเราที่เราไม่ได้ตั้งใจจะเปิดเผย เช่น เพศวิถี อายุ สัญชาติ ศาสนา จนอาจนำไปสู่การขโมยข้อมูลของเราไปใช้ อาทิ รหัสบัตร ATM ข้อมูลบัตรเครดิต การสวมรอยเป็นเรา ไปจนถึงการเรียกค่าไถ่เพื่อแลกกับการไม่เปิดเผยข้อมูลของเรา

จากความรวดเร็วในการประมวลผลและการใช้งานข้อมูลผ่านระบบสารสนเทศซึ่งเป็นของได้เปรียบทางการแข่งขั้นแล้ว ย่อมเกิดปัญหาและผลกระทบจากการสะดวกรวดเร็วดังกล่าว ภัยคุกคามทางไซเบอร์ที่สามารถเข้าถึงข้อมูลของเราสามารถทำให้เกิดอันตรายได้หลายรูปแบบมาก อาทิเช่น

- Malware มาจากคำว่า Malicious + Software ที่แปลว่า ที่ประสงค์ร้าย + ซอฟต์แวร์ (ซอฟต์แวร์ที่ประสงค์ร้าย) ซึ่งเป็นซอฟต์แวร์ที่สร้างขึ้นเพื่อรบกวนหรือทำให้เกิดความเสียหาย เช่น ไวรัสคอมพิวเตอร์ (Virus) ที่สามารถคัดลอกโปรแกรมของตัวเองให้ไปติดกับไฟล์อื่น ๆ ในเครื่องคอมพิวเตอร์ได้ Trojans (โทรจัน) ที่สามารถสร้างความเสียหายหรือเก็บข้อมูลของเรา Spyware ที่แอบเก็บข้อมูลสำคัญของเรา Ransomware หรือมัลแวร์เรียกค่าไถ่ ที่จะปิดกั้นไม่ให้เราเข้าไปใช้งานไฟล์หรือข้อมูลจนกว่าจะจ่ายค่าไถ่ เป็นต้น
- Phishing เป็นการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายด้านอื่น ๆ
- การโจมตีด้วยการแทรกกลาง (Man-in-the-middle attack) เป็นการจู่โจมระหว่างโหนด (Node) การสื่อสารของอุปกรณ์ เพื่อดักจับข้อความหรือข้อมูลระหว่างผู้ส่งและผู้รับข้อมูล ลองนึกภาพว่าเรากำลังส่งน้ำไหลไปตามท่อ แต่มีคนมาดักตรงกลางเพื่อเอาน้ำไป

- การโจมตีด้วยการปฏิเสธการให้บริการ (Denial-of-service attack) เป็นการจู่โจมที่ผู้ประสงค์ร้ายเข้าควบคุมอุปกรณ์เครือข่าย หรือเซิร์ฟเวอร์ไม่ให้ทำงาน ซึ่งหากเป็นระบบโรงพยาบาลหรือหน่วยงานด้านพลังงานก็จะก่อให้เกิดความเสียหายต่อชีวิตและทรัพย์สินมหาศาล

หลักสูตรการฝึกอบรมความมั่นคงปลอดภัยไซเบอร์พื้นฐาน (Cybersecurity Fundamentals) มุ่งเน้นให้ผู้เข้าอบรมได้ตระหนักรู้ความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งมีความรู้และความเข้าใจในภัยคุกคามไซเบอร์รูปแบบต่าง ๆ โดยเฉพาะที่กำลังเป็นประเด็นสำคัญในปัจจุบันนอกจากนี้ยังส่งเสริมให้ผู้เข้ารับการอบรมมีความรู้เบื้องต้นในวิธีการป้องกันภัยคุกคามไซเบอร์ที่จะเกิดขึ้นในอนาคตได้อย่างถูกต้องและทันท่วงที รวมทั้งมีความเข้าใจเบื้องต้นเกี่ยวกับการบริหารความเสี่ยง (Risk Management) และการประเมินความเสี่ยง (Risk Assessment) ระบบสารสนเทศให้มีความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพ

วัตถุประสงค์

1. เพื่อให้มีความตระหนักรู้ในความมั่นคงปลอดภัยไซเบอร์
2. เพื่อให้สามารถใช้เทคโนโลยีคอมพิวเตอร์ได้อย่างปลอดภัยและแก้ปัญหาเบื้องต้นได้เมื่อต้องพบกับภัยคุกคาม
3. เพื่อให้การประเมินความเสี่ยงด้านไซเบอร์โดยมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสม
4. เพื่อศึกษากรณีตัวอย่างแนวทางการพัฒนาระบบความความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

รูปแบบการฝึกอบรม

หลักสูตรการฝึกอบรมความมั่นคงปลอดภัยไซเบอร์พื้นฐาน (Cybersecurity Fundamentals) เปนการผสมผสานหลายวิธี ได้แก่ การบรรยาย การอภิปราย และการฝกปฏิบัติการ และกรณีศึกษาในแนวทางการวางแผนพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

การผสมผสานรูปแบบการฝกอบรมดังกล่าวข้างต้นจะทำให้ผู้เรียนมีกระบวนการเรียนรู้ และเกิดความคิดและสามารถวิเคราะหซึ่งจะสามารถทำให้บรรลุตามวัตถุประสงคของหลักสูตรที่ได้กำหนดไว้ กรอบเนื้อหาของความรู้ที่จะได้รับ ประกอบด้วย

1. กฎหมายและประเภทของภัยคุกคามทางไซเบอร์
2. ข้อควรปฏิบัติ/วิธีการป้องกันภัยคุกคามทางไซเบอร์
3. รูปแบบและวิธีการแก้ไขปัญหาเมื่อถูกโจมตีทางไซเบอร์
4. การประเมินความเสี่ยงด้านไซเบอร์โดยมีแนวทางการดำเนินงานที่ถูกต้อง
5. กรณีศึกษาในแนวทางการวางแผนพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

ระยะเวลาการฝึกอบรม

การจัดอบรมจำนวน 1 รุ่น รุ่นละไม่เกิน 30 คน จำนวน 2 วัน (วันละ 6 ชั่วโมง รวม 12 ชั่วโมง)
กำหนดจัดอบรมระหว่างวันที่ 17 – 18 พฤศจิกายน 2565

ตารางการฝึกอบรม

วิทยากรฝึกอบรม

1. อาจารย์ภาณุเดช ทิพย์อักษร
   รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
   มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา
2. อาจารย์ ดร.ปรัชญ์ ปิยะวงศ์วิศาล
   (M.S. in Computer Science Carnegie Mellon University, Pittsburgh, PA, USA)

เวลา	หัวข้อ	เนื้อหา
	วันที่ 17 พฤศจิกายน 2565	
09.00 – 12.00	**ความรู้เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศขององค์กรและกฎหมายที่เกี่ยวข้องในหน่วยงาน**	▪ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ▪ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ▪ พื้นฐานการป้องกันภัยคุกคามไซเบอร์
	การวิเคราะห์กระบวนการทำวานขององค์กร	▪ แนวคิดความมั่นคงปลอดภัยแบบ Zero Trust
13.00 – 16.00	**เทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์**	▪ การตระหนักรู้รูปแบบภัยคุมคามไซเบอร์(Cyber Security Awareness) ▪ รูปแบบการโจมตีทางไซเบอร์และการป้องกัน ▪ การรักษาความปลอดภัยไซเบอร์กับระบบเครือข่ายไร้สาย (Wireless LAN Security)
	การปรับแต่งเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย โทรศัพท์มือถือด้านการรักษาความปลอดภัยทางไซเบอร์พื้นฐาน และกิจกรรม Workshop	▪ การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล ▪ การรักษาความปลอดภัยของเว็บบราวเซอร์ ▪ การรักษาความปลอดภัยการใช้สื่อสังคมออนไลน์

เวลา	หัวข้อ	เนื้อหา
	วันที่ 18 พฤศจิกายน 2565	
09.00 -12.00	**แนวทางการประเมินความเสี่ยงในการเตรียมความพร้อมวางแผนและรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์**	▪ ความรู้เบื้องต้นเกี่ยวกับการบริหารความเสี่ยง (Introduction to Risk Management) ▪ การประเมินความเสี่ยง (Risk Assessment) ระบบสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ ▪ ตัวอย่างการประเมิน- การประเมินตนเองตามมาตรฐานสากล ISO/IEC 27001:2013
13.00 – 16.00	**กรณีศึกษาในแนวทางการวางแผนพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน**	▪ กรณีศึกษาภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา แผนความเสี่ยง แนวทางป้องกันและการแก้ไขปัญหาที่เกิดขึ้น ▪ กรณีศึกษาภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานพันธมิตรด้านเครือข่ายยการศึกษา (กรณีศึกษาบริษัทเอกชนแห่งหนึ่งด้านเครือข่ายเทคโนโลยีสารสนเทศในจังหวัดเชียงใหม่)
	Workshop การประเมินตนเองตามมาตรฐานสากล ISO/IEC 27001:2013	▪ กิจกรรมฝึกปฏิบัติ การประเมินตนเองตามมาตรฐานสากล ISO/IEC 27001:2013

หมายเหตุ

1. พักรับประทานอาหารว่าง ช่วงเช้าเวลา 10.30 – 10.45 น. ช่วงบ่ายเวลา 14.30 – 14.45 น.
2. พักรับประทานอาหารกลางวัน เวลา 12.00 – 13.00 น.
3. กำหนดการอาจจะมีการเปลี่ยนแปลงตามความเหมาะสม

ค่าธรรมเนียมการฝึกอบรมของหลักสูตร

ค่าลงทะเบียนฝึกอบรมท่านละ 6,900 **บาท (หกพันเก้าร้อยบาทถ้วน)** (รวมภาษีมูลค่าเพิ่มแล้ว)

ค่าลงทะเบียนข้างต้น **<u>รวม</u>** ค่าอาหารกลางวัน และอาหารว่างแล้ว

หมายเหตุ กรณีผู้เข้าอบรมมีจำนวนไม่ถึงตามที่กำหนด ผู้จัดอบรมจะดำเนินการแจ้งให้ผู้สมัครเข้าร่วมอบรมทราบล่วงหน้า

เงื่อนไขการผ่านการอบรมและได้รับประกาศนียบัตร

1. ผู้เข้ารับการฝึกอบรมจะต้องเข้าร่วมการฝึกอบรมไม่น้อยกว่าน้อยละ 80 ของระยะเวลาการฝึกอบรมฯ
2. ผู้เข้ารับการฝึกอบรมจะต้องเข้ารับการทดสอบประเมินความรู้ภาคทฤษฎีด้วยแบบประเมินผลหลังการฝึกอบรม (Post-Test) โดยเกณฑ์การผ่านไม่น้อยกว่าร้อยละ 75
3. ผู้เข้ารับการอบรมจะต้องนำเสนอผลการฝึกปฏิบัติจากกรณีศึกษากิจกรรมกลุ่มในวันสุดท้ายของการฝึกอบรม

สถานที่ฝึกอบรม

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา
128 ถนนห้วยแก้ว ตำบลช้างเผือก อำเภอเมือง จังหวัดเชียงใหม่ 50300
โทรศัพท์ 0 5392 1444 ต่อ 1630 (งานบริการการศึกษา)

สอบถามรายละเอียด

หากท่านมีข้อสงสัย และ/หรือต้องการทราบรายละเอียดเพิ่มเติม สามารถติดต่อสอบถามได้ที่ นายออมทรัพย์ อินกองงาม สำนักวิทยบริการและเทคโนโลยีสารสนเทศ หมายเลขโทรศัพท์ 081 5544691

ดำเนินการฝึกอบรมโดย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา
(Office of Academic Resource and Information Technology, RMUTL)
128 ถ.ห้วยแก้ว ต.ช้างเผือก อ.เมือง จ.เชียงใหม่ 50300
โทรศัพท์ : 0 5392 1444 ต่อ 1619 , โทรสาร : 0 53921 444 ต่อ 1630
https://arit.rmutl.ac.th/