ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารทางการศึกษา

Information and Communication Technology Security in Education

ดร.จิระ จิตสุภา

บทนำ

ปัจจุบันเป็นที่ยอมรับกันโดยทั่วไปแล้วว่าเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทต่อการดำรงชีวิตประจำวันของประชากรทุกสังคมในโลก และยังเป็นกลไกสำคัญในการแข่งขันเพื่อความอยู่รอดขององค์กรทั้งหลายทั้งรัฐและเอกชน ประเทศไทยยอมรับว่าเทคโนโลยีสารสนเทศเป็นยุทธศาสตร์การพัฒนาประเทศที่สำคัญประการหนึ่งที่สามารถเสริมสร้างความแข็งแกร่งต่อธุรกิจ อุตสาหกรรม การค้า ตลอดจนเป็นเครื่องมือที่ใช้ในการพัฒนามนุษย์และสังคมได้อย่างมีประสิทธิภาพ [1]

การพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย มุ่งพัฒนาสู่สังคมแห่งภูมิปัญญาและการเรียนรู้ 5 ด้านได้แก่ e-Industrial, e-Commerce, e-Government, e-Society และ e-Education [2] ส่งผลให้ประเทศไทยมีอัตราการใช้เทคโนโลยีสารสนเทศที่เพิ่มมากขึ้นอย่างรวดเร็วทั้ง Hardware, Software, Network System และInformation รวมถึงการเพิ่มขึ้นของภัยคุกคาม การเจาะระบบคอมพิวเตอร์โดยผู้ไม่ประสงค์ดี และอาชญากรรมทางคอมพิวเตอร์ ดังข่าวที่ปรากฏผ่านสื่อสารมวลชนอยู่เป็นระยะๆ อีกด้วย จากผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย พบว่าภัยคุกคาม และอาชญากรรมทางคอมพิวเตอร์ เช่น ไวรัสและผู้ไม่ประสงค์ดี ยังคงเป็นปัญหาอันดับหนึ่ง [3]

ความสนใจเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารและความเป็นส่วนตัวในระบบการศึกษาไม่ใช่เรื่องใหม่ ประกอบกับเทคโนโลยีสารสนเทศและนวัตกรรมที่ถูกสร้างขึ้นอยู่ตลอดเวลา รวมทั้งเทคโนโลยีที่เพิ่มประสิทธิภาพและช่องทางในการเรียนรู้มีมากขึ้น ทั้งแบบไร้สายสัญญาณ (Wireless) เช่น โทรศัพท์มือถือ คอมพิวเตอร์และอุปกรณ์จัดเก็บข้อมูลแบบพกพา และชนิดมีสายสัญญาณ (Wired) เว็บ 2.0 หรือสังคมออนไลน์ (Social Network) ที่กำลังได้รับความนิยม เช่น Facebook รวมถึงระบบการเรียนการสอนผ่านเครือข่ายคอมพิวเตอร์ (e-Learning) เทคโนโลยีและนวัตกรรมเหล่านี้เป็นฐานในการใช้เพื่อการศึกษาและการเรียนรู้ได้เป็นอย่างดี แต่เทคโนโลยีและนวัตกรรมที่กล่าวมานั้นมีส่วนในการนำพาและเพิ่มปัญหาเกี่ยวกับความเป็นส่วนตัวและความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศทั้งสิ้น เนื่องจากอุปกรณ์ต่างๆ เหล่านี้ส่วนใหญ่ถูกใช้ในชีวิตประจำวัน และมีขนาดเล็กพกพาสะดวกและมักจะสูญหายเป็นประจำ ที่สำคัญเกือบร้อยละ 60 ของผู้ใช้อุปกรณ์เหล่านี้ไม่มีการป้องกันด้วยรหัสผ่านหรือการป้องกันด้วยการเข้ารหัสแต่อย่างใด ผู้ใช้คอมพิวเตอร์ส่วนใหญ่มีความรู้ที่น้อยมากเกี่ยวกับไวรัส เช่น วิธีการทำงาน แหล่งที่มาและความเสียหายที่เกิดจากไวรัส การขาดซึ่งความเข้าใจเหล่านี้เพิ่มความเสี่ยงมากขึ้น นักเขียนโปรแกรมไวรัสและหนอนอินเทอร์เน็ตมีวิธีและรูปแบบการเขียนโปรแกรมที่สร้างสรรค์มากขึ้นเพื่อดึงดูดผู้ใช้และหาทางเข้าระบบเทคโนโลยีสารสนเทศที่มีช่องโหว่ ทำให้เทคโนโลยีสารสนเทศเป็นทั้งเพื่อนและศัตรูเกี่ยวกับความมั่นคงปลอดภัย [4]

การวิจัยในสหรัฐอเมริกาเผยให้เห็นความสำคัญของความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร และการจัดการหลักฐาน สถาบันการศึกษาจำนวนมากล้วนให้ความสำคัญกับประเด็นที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต้องลงมือกระทำอย่างจริงจัง เนื่องจากปัญหาความเป็นส่วนตัวและความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารมีผลกับผู้สอน ผู้จัดเตรียม

อาจารย์ประจำคณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสวนดุสิต email : jirajitsupa@gmail.com

เทคโนโลยีสำหรับการเรียนรู้ ผู้ให้บริการการเรียนรู้ ผู้จัดเตรียมเนื้อหาการเรียนรู้ และผู้เรียน [5]

เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษารูปแบบใหม่

การศึกษาในปัจจุบันมีหลักสูตรการเรียนรู้มากมายให้ผู้เรียนได้ตัดสินใจเลือกตามความสามารถ ความสนใจ และความเหมาะสมของผู้เรียน ทั้งหลักสูตรแบบปกติ (Classroom Learning) และหลักสูตรทางไกล หรือการเรียนออนไลน์ (Distance Learning)

การเรียนรู้โดยใช้อินเทอร์เน็ตเป็นฐานช่วยเพิ่มประสิทธิภาพในการเรียนรู้ผ่านเครื่องมือที่เกี่ยวข้องกับคอมพิวเตอร์และเทคโนโลยีโทรคมนาคม [6] เป็นลักษณะการเรียนรู้ที่มีความยืดหยุ่น และมีความอิสระจากเวลาและสถานที่อย่างมาก แต่ก็ขึ้นอยู่กับการทำงานและความน่าเชื่อถือของโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศและการสื่อสารเนื่องจากผู้เรียนจะต้องเรียนรู้ด้วยตนเองและถูกคาดหมายว่าจะมีความรับผิดชอบอย่างดีในการเรียนรู้ ผู้เรียนเหล่านั้นยังจะต้องสามารถใช้ทรัพยากรทางเทคโนโลยีสารสนเทศและการสื่อสาร ได้อย่างมีประสิทธิภาพ เพื่อจัดการกับข้อมูลและสารสนเทศจำนวนมาก รวมทั้งการสื่อสารกับผู้สอนและเพื่อนผู้เรียนคนอื่นๆ [7]

สถาบันการศึกษาในยุโรปและสหรัฐอเมริกาให้ความสนใจที่จะเปลี่ยนแปลงและปฏิรูปการศึกษามานานนับทศวรรษ คอมพิวเตอร์และอุปกรณ์ต่อพ่วงมีราคาที่ถูกลง เทคโนโลยีมัลติมีเดียและอินเตอร์เน็ตมีการทำงานที่รวดเร็วมากขึ้น เป็นเงื่อนไขสำคัญในการเพิ่มจำนวนของผู้เรียนการเรียนรู้ผ่านการศึกษาทางไกลหรือการศึกษาออนไลน์เปิดโอกาสสำหรับการเรียนรู้ตลอดชีวิต เป็นรูปแบบที่เหมาะสำหรับการเรียนการสอนที่มีผู้สอนเป็นเพียงผู้คอยชี้แนะ แนะนำและช่วยเหลือผู้เรียน แทนการที่ผู้สอนจะเป็นผู้นำและผู้เรียนเป็นเพียงผู้ตาม แต่เมื่อความต้องการเรียนรู้ผ่านการศึกษาทางไกลหรือออนไลน์มีมากขึ้น ความต้องการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารสำหรับการเรียนรู้ก็เติบโตตามไปด้วยเช่นกัน [7] เนื่องจากความมั่นคงปลอดภัยเป็นองค์ประกอบที่สำคัญที่สุดในการจัดการเรียนการสอน ทางไกลผ่านอุปกรณ์อิเล็กทรอนิกส์ [6]

ความสำคัญของความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการศึกษา

โลกกำลังอยู่ในยุคอิเล็กทรอนิกส์ยุคที่มีการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลกันผ่านทางจดหมายอิเล็กทรอนิกส์ ธนาคารอิเล็กทรอนิกส์ การพานิชอิเล็กทรอนิกส์ และการจัดการเรียนการสอนทางไกลผ่านอุปกรณ์อิเล็กทรอนิกส์อย่างชัดเจน [8]

สถาบันการศึกษามีผู้ใช้คอมพิวเตอร์ ประกอบด้วยผู้บริหาร ผู้สอน เจ้าหน้าที่ และผู้เรียน บุคคลกลุ่มนี้ล้วนเป็นองค์ประกอบสำคัญของทรัพยากรสารสนเทศของสถาบันการศึกษาที่มีการเรียนรู้ผ่านเทคโนโลยีสารสนเทศและยังเป็นผู้รักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการเรียนรู้อีกด้วย เนื่องจากสามารถเข้าถึงข้อมูลที่สำคัญที่สถาบันการศึกษาพึงมี และในบางครั้งยังมีความรู้ ความสามารถในการหลบหลีกระบบที่มีการป้องกันข้อมูล หรือขาดความรู้ที่จำเป็นในการปกป้องข้อมูลและเทคโนโลยีสารสนเทศของสถาบันการศึกษา คำถามที่ต้องถามว่าทำไมผู้ใช้คอมพิวเตอร์กลุ่มนี้จึงเป็นส่วนสำคัญของโครงสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการเรียนรู้ของสถาบันการศึกษา เนื่องจากผู้ใช้ปลายทางเหล่านี้ เป็นคนหนึ่งที่จะเห็นข้อมูลและเป็นภัยคุกคามต่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของสถาบันการศึกษา และได้ประโยชน์จากภัยคุกคามเหล่านี้

การเกิดขึ้นลักษณะเหล่านี้เนื่องจากการขาดความรู้ในการใช้งานเทคโนโลยีสารสนเทศ [4] เช่น การทำให้ระบบเครือข่ายคอมพิวเตอร์ล่ม หรือการเปิดเผยข้อมูลส่วนบุคคลที่เป็นความลับ เช่น Login และ Password ภัยคุกคามที่พบมากที่สุดในการดำเนินงานเกี่ยวกับเทคโนโลยีสารสนเทศที่เกิดขึ้น ได้แก่ การบกพร่องในการจัดการกับงานประจำและกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น การลืมสำรองข้อมูล การเปิดเครื่องคอมพิวเตอร์ทิ้งไว้โดยไม่มีการ Logoff หรือ การส่งข้อมูลสำคัญผ่านเมลไปหาผิดคน เรียกภัยคุกคามประเภทนี้ว่าภัยคุกคามแบบไม่ตั้งใจทำให้เกิดขึ้นซึ่งมักจะเกิดขึ้นจากคนภายในองค์กร ส่วนภัยคุกคามแบบ

ตั้งใจทำให้เกิดขึ้น มักจะเกิดขึ้นจากคนภายนอกองค์กร ได้แก่ การเข้าดูข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตผ่านช่องทางใดช่องทางหนึ่ง การโจรกรรมข้อมูล การแก้ไขเปลี่ยนแปลงข้อมูลให้บิดเบือนไปจากความเป็นจริง เป็นต้น เป็นที่น่าสังเกตว่าภัยคุกคามที่เกิดขึ้นนั้นเกิดจากบุคคลภายนอกองค์กรเพียงแค่ 3% เท่านั้น [7]

รูปที่ 1 ส่วนหนึ่งของภัยคุกคามจากภายในและภายนอกสถานศึกษา [7]

การแนบไฟล์ไปกับเมลและการดาวน์โหลดโปรแกรมและไฟล์ อาจทำให้คอมพิวเตอร์ติดโค้ดซึ่งเป็นอันตราย เช่น โปรแกรมไวรัส หนอนอินเตอร์เน็ต และม้าโทรจัน นอกจากนี้ความเสี่ยงที่เกิดจากการล่วงล้ำหรือการบุกรุกที่ไม่ได้รับอนุญาตโดยแฮกเกอร์ ที่สามารถเข้าถึงทรัพยากรเทคโนโลยีสารสนเทศ และนำทรัพยากรเหล่านี้ไปใช้ในทางไม่เหมาะสม หรือทางที่อันตราย ปัญหาเกี่ยวกับความมั่นคงปลอดภัยเหล่านี้อาจจะเป็นกรณีที่เลวร้ายที่สุดที่นำไปสู่การเกิดการสูญเสียของข้อมูล และระบบเครือข่ายคอมพิวเตอร์

ปัญหาการเข้าถึงและการสูญเสียข้อมูลที่มีค่าอาจเกิดขึ้น เมื่อผู้เรียนต้องจัดการกับไฟล์เอกสารที่มีจำนวนมาก หรือไฟล์ที่มีขนาดยาวๆ เช่น การบ้าน รายงาน หรือวิทยานิพนธ์ หากผู้เรียนไม่ปฏิบัติตามขั้นตอนที่ถูกต้องเมื่อต้องใช้งานกับโปรแกรมคอมพิวเตอร์ที่มีเวอร์ชันที่แตกต่างกัน หรือไม่ได้มีสำรองไฟล์

นอกจากนี้จำนวนที่เพิ่มขึ้นของหลักสูตรการเรียนรู้ทางไกลหรือการเรียนรู้ออนไลน์ ทำให้การรักษาความมั่นคงปลอดภัยของข้อมูลการศึกษาสูงตามไปด้วย เพื่อสร้างความไว้วางใจระหว่างผู้สอนและผู้เรียนซึ่งมีความสำคัญอย่างยิ่ง ข้อมูลที่ถูกนำเสนอผ่านการเรียนรู้ออนไลน์จะต้องมีความถูกต้อง สะดวกในการเข้าถึง สามารถติดตามแหล่งที่มาของข้อมูล โดยเฉพาะเมื่อผู้สอนต้องการวัดผลการเรียนรู้ของผู้เรียนด้วยการทดสอบผ่านระบบเครือข่ายคอมพิวเตอร์ ถ้าทุกคนตระหนักและสนับสนุนเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ จะช่วยให้การออกแบบโครงสร้างพื้นฐานและการใช้เทคโนโลยีสารสนเทศลดความเสี่ยงที่อาจเกิดขึ้นกับการศึกษา รวมถึงเศรษฐกิจและสังคมลง [7]

ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการศึกษา

ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสามารถแบ่งออกเป็นความมั่นคง (Integrity), ความพร้อมใช้ (Availability), ความลับ (Confidentially), การห้ามปฏิเสธความรับผิดชอบ (Accountability), และการควบคุมการเข้าถึง (Access control) [9]

1. ความมั่นคง คือการป้องกันจากบุคคล หรือสิ่งที่ไม่ได้รับอนุญาต เป็นความต้องการขั้นพื้นฐานของข้อมูลที่มีคุณภาพ ประกอบด้วย ความมั่นคงปลอดภัยส่วนบุคคล ระบบ และคุณภาพของสารสนเทศ ความมั่นคงเป็นเป้าหมายของการป้องกันการเปลี่ยนแปลงข้อมูลที่ไม่ได้รับอนุญาต การขาดความมั่นคงปลอดภัยส่งผลต่อความเสียหายของข้อมูลที่ใช้งานอยู่ หรืออาจจะเกิดความเสียหายต่อทรัพยากรทางด้านเทคโนโลยีสารสนเทศ เช่น ระบบเซิร์ฟเวอร์ โปรแกรม และระบบเครือข่าย คุณภาพของสารสนเทศ เช่น เมื่อผู้เรียนวางแผนสำหรับการศึกษา พวกเขาจะค้นหาข้อมูลเกี่ยวกับเนื้อหาของหลักสูตร ตารางและเวลาเรียน รูปแบบการสอบ เป็นต้น หากสารสนเทศเหล่านั้นทำให้เกิดการเข้าใจผิด ไม่เป็นปัจจุบัน หรือถูกนำเสนอให้ยากต่อการทำความเข้าใจ คุณภาพของสารสนเทศเหล่านั้นจะถูกลดคุณค่าลง เนื่องจากข้อมูลเกี่ยวกับหลักสูตรจะมีผลต่อการเลือกเรียนของผู้เรียน อีกปัญหาที่ร้ายแรง คือ คำอธิบายที่ไม่ชัดเจน หรือไม่ถูกต้องของเนื้อหาของหลักสูตร อาจทำให้เกิดความเสี่ยงในการล้มเหลวของผู้เรียน

2. ความพร้อมใช้ คือความเป็นไปได้ในการอนุญาตให้ผู้เรียนใช้ทรัพยากรตามที่ผู้เรียนต้องการภายในระยะเวลาที่กำหนด การหยุดชะงักของระบบเทคโนโลยีสารสนเทศและการถูกรบกวนจะต้องได้รับการป้องกัน เช่น การที่ผู้เรียนจะต้องใช้สื่อและทรัพยากรการเรียนของหลักสูตรและระบบอย่างต่อเนื่อง หากเกิดปัญหาทางเทคนิคที่ผู้เรียนไม่สามารถแก้ไขปัญหาได้ขึ้นมา มันเป็นความจำเป็นที่ผู้เรียนจะสามารถเข้าถึงการช่วยเหลือแก้ไขปัญหาเหล่านี้ในเบื้องต้น ทั้งโดยทางตรง และทางอ้อม เช่น e - mail หรือโทรศัพท์ เพื่อให้สามารถสื่อสารกับผู้สอนในหลักสูตรได้ เปรียบเสมือนเงื่อนไขสำคัญในการศึกษาให้ประสบความสำเร็จ

3. ความลับ คือการที่ข้อมูลสำคัญไม่ถูกเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต หรือการไม่เปิดเผยข้อมูลที่สำคัญให้คนที่ไม่ได้รับอนุญาต ข้อมูลทั้งหมดควรจะมี กฎ ระเบียบ หรือนโยบายในการเข้าถึงและการอนุมัติการใช้ข้อมูล การสูญเสียความลับจะเกิดขึ้นเมื่อผู้ที่ได้รับอนุญาต และไม่ได้รับอนุญาตเข้าถึงข้อมูล เช่น บางครั้งผู้สอนส่งข้อมูลที่เป็นสื่อการเรียนทั้งข้อความ และรูปภาพไปยังผู้เรียนสื่อการสอนดังกล่าวอาจมีความสำคัญไม่มากนักที่จะถูกคุกคามจากผู้ไม่หวังดี แต่ความลับเป็นสิ่งสำคัญเมื่อผู้เรียนต้องการการติดต่อสื่อสารที่ไว้วางใจได้กับผู้สอนในเรื่องที่เกี่ยวกับการเรียน

4. การห้ามปฏิเสธความรับผิดชอบ คือการที่ผู้ใช้คอมพิวเตอร์จะไม่สามารถปฏิเสธได้ว่าได้ส่ง หรือได้รับข้อความ หรือเข้าร่วม หรือดำเนินการอย่างใดอย่างหนึ่งกับเทคโนโลยีสารสนเทศ ผ่านการตรวจสอบการเข้าถึงและเข้าใช้งานของผู้ใช้ ความรับผิดชอบทำให้เกิดการป้องกันจากการเสียหาย การสูญเสียข้อมูลและความมั่นคงปลอดภัยจากอาชญากรรมคอมพิวเตอร์ ในขณะเดียวกันถ้าผู้ใช้ไม่รับผิดชอบต่อการกระทำเหล่านั้น การระบุตัวตนของผู้ใช้มีความเป็นไปได้ในการสร้างความรับผิดชอบ เช่น การระบุตัวตนในการศึกษาออนไลน์สามารถอธิบายได้ในสามระดับ

1. ระดับที่หนึ่งทางกายภาพ ผ่านทางหมายเลข IP Address หรือ MAC Address ที่ถูกระบุอยู่ในคอมพิวเตอร์ทุกเครื่องที่ถูกใช้งานออกไป

2. ระดับที่สองทางกฎหมาย เป็นการระบุการตอบสนองอย่างหนึ่งของผู้ใช้ อาจจะเป็นชื่อ และรหัสผ่านที่ใช้ในการเข้าสู่ระบบ รวมถึงลายเซ็นดิจิตอลด้วย

3. ระดับที่สามทางบุคคล คือการสร้างความมั่นใจว่าสิ่งที่ถูกเขียนหรือสร้างขึ้นขึ้นและถูกส่งส่งออกไปได้ถูกสร้างขึ้นมาโดยบุคคลผู้เป็นเจ้าของชื่อผู้ใช้จริงๆ ซึ่งเป็นการตรวจสอบที่ยากที่สุด

ความรับผิดชอบที่มีต่อการเข้าถึงข้อมูลและการสื่อสารผ่านการ Login เข้าระบบด้วยชื่อและรหัสผ่านกับการเรียนออนไลน์สามารถติดตามร่องรอย การร่วมกิจกรรมของผู้เรียนได้ว่าผู้เรียนมีการตอบสนองต่อบทเรียนหรือต่อการเรียนมากน้อยแค่ไหน เช่น ผู้เรียนใช้เวลาในการอยู่ในบทเรียนนานแค่ไหน และทำกิจรรมอะไรบ้างในขณะอยู่ในบทเรียน เป็นต้น ผู้เรียนทุกคนจะมีการตอบสนองชัดเจนต่อการกระทำของตน ถ้าผู้เรียนสามารถระบุชื่อและรหัสผ่านได้อย่างชัดเจน ความเสี่ยงต่อพฤติกรรมที่ไม่

เหมาะสมจะลดลงเมื่อมีการติดต่อสื่อสารกับผู้สอนและผู้เรียนคนอื่นๆ [7]

5. การควบคุมการเข้าถึง คือการที่ผู้ใช้ระบบคอมพิวเตอร์ไม่สามารถส่งผ่านหรือเพิ่มสิทธิ์ในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต [10] การเข้าถึงข้อมูลจำเป็นต้องมีการควบคุมบนพื้นฐานของการรักษาความปลอดภัย การกำหนดสิทธิการทำงานและเข้าถึงข้อมูลของผู้ใช้จะต้องมีการกำหนดที่ชัดเจนบนนโยบายของหน่วยงาน ผู้ใช้ควรจะได้รับการกำหนดสิทธิให้เข้าถึงข้อมูลหรือระบบเฉพาะส่วนที่จำเป็นและอนุญาตให้ใช้เท่านั้น [11] การควบคุมการเข้าถึงเป็นการทำให้มั่นใจได้ว่าทรัพยากรต่างๆ ของระบบเครือข่ายจะได้รับอนุญาตให้ถูกใช้โดยผู้ที่มีสิทธิ์ในการเข้าถึงหรือในการใช้ข้อมูลเท่านั้น ประกอบด้วย

- ความเป็นส่วนตัว (Privacy) ข้อมูลรวบรวม จัดเก็บและใช้งานนั้นควรถูกใช้เพื่อจุดประสงค์ที่เจ้าของข้อมูลระบุตอนที่เก็บรวบรวมเท่านั้น ถ้าถูกใช้เพื่อจุดประสงค์อื่นก็แสดงว่าเป็นการละเมิดสิทธิ์ส่วนบุคคลของเจ้าของข้อมูลนั้น

- การระบุตัวตน (Identification) เป็นกลไกที่จัดเตรียมสารสนเทศของบุคคลที่จะเข้าใช้ระบบ หรือเรียกว่า Identifier ซึ่งผู้ใช้แต่ละคนจะต้องมีค่าที่ไม่เหมือน หรือไม่ซ้ำกัน

- การพิสูจน์ทราบตัวตน (Authentication) เป็นกลไกการตรวจสอบว่าผู้ใช้เป็นใคร และเป็นผู้ที่ได้รับอนุญาตหรือไม่ผ่านทางการล็อกอิน และรหัสผ่าน (Password)

- การกำหนดสิทธิ์ (Authorization) เป็นกลไกการอนุญาต หรือให้สิทธิ์ในการเข้าถึงระบบและเข้าใช้ข้อมูลในระบบของผู้ที่ผ่านการพิสูจน์ตัวตนมาแล้ว โดยกลไกจะพิจารณาว่าผู้ใช้แต่ละคนได้รับอนุญาตให้เข้าถึงระบบในระดับใดบ้าง

- การจัดทำประวัติการเข้าใช้ระบบ (Accountability) เป็นการบันทึกการเข้าใช้ระบบของผู้ใช้ เพื่อจัดทำเป็นหลักฐานการตรวจสอบที่จะเป็นประโยชน์ต่อการติดตามพฤติกรรมที่น่าสงสัยได้

องค์ประกอบของความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการศึกษา [9]

1. ซอฟแวร์ (Software) ในการพัฒนาซอฟแวร์ต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ เช่น เวลา ต้นทุน และกำลังคน ดังนั้น จะพบว่าการเพิ่มความมั่นคงปลอดภัยให้กับซอฟแวร์มักจะทำภายหลังจากพัฒนาซอฟแวร์เสร็จแล้วไม่ได้ทำในตอนต้นของการพัฒนา

2. ฮาร์ดแวร์ (Hardware) ความมั่นคงปลอดภัยที่มีต่อฮาร์ดแวร์นั้น นั้นคือการป้องกันฮาร์ดแวร์จากการลักขโมย เช่น การใส่กุญแจ การจำกัดการใช้งานอุปกรณ์เหล่านั้น หรือการจัดสถานที่ที่ปลอดภัยให้กับฮาร์ดแวร์ การป้องกันการเข้าถึงอุปกรณ์หรือฮาร์ดแวร์ต่างๆ ช่วยลดโอกาสในการเข้าถึงหรือสร้างความเสียหายให้กับข้อมูลได้ระดับหนึ่ง

3. ข้อมูล (Data) ข้อมูลหรือสารสนเทศเป็นทรัพยากรที่มีค่ามาก และเป็นเป้าหมายหลักของการโจมตี หรือการคุกคาม

4. บุคลากร (People) เป็นภัยคุกคามต่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ถูกมองข้ามมากที่สุด ถึงแม้จะมีระบบรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่มีประสิทธิภาพมากเพียงใด แต่หากบุคลากรที่เกี่ยวข้องไม่มีจิตสำนึก หรือไม่มีความตระหนักถึงความมั่นคงปลอดภัยก็จะเป็นจุดอ่อนที่ดีที่สุดของการโจมตีระบบได้

5. ขั้นตอนการทำงาน (Procedure) เป็นอีกองค์กระกอบหนึ่งด้านความมั่นคงปลอดภัยที่ถูกมองข้าม โดยหากผู้ไม่ประสงค์ดีทราบถึงขั้นตอนการทำงานอย่างใดอย่างหนึ่งครบถ้วนแล้ว ก็จะสามารถค้นหาจุดอ่อนเพื่อกระทำการอันก่อให้เกิดความเสียหายต่อข้อมูลได้

6. เครือข่ายคอมพิวเตอร์ (Network) การเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันผ่านระบบเครือข่าย ทำให้เกิดผู้ไม่ประสงค์ดี และภัยคุกคามทางคอมพิวเตอร์ชนิดใหม่จำนวนมาก โดยเฉพาะภัยคุกคามต่อข้อมูลหรือสารสนเทศที่ต้องส่งผ่านระหว่างเครือข่ายต้นทางไปยังปลายทางหรือส่งผ่านไปทางอินเทอร์เน็ต

การโจมตี ช่องโหว่ และภัยคุกคามต่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการศึกษา

ภารกิจหลักของการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีเพื่อการเรียนรู้ คือการทำให้มั่นใจว่าข้อมูลจะไม่ถูกเปลี่ยนแปลง หรือแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต สามารถใช้งานได้อย่างมีประสิทธิภาพ เข้าถึงข้อมูลได้เฉพาะผู้ที่มีส่วนเกี่ยวข้องเท่านั้น และหากเกิดความไม่มั่นคงปลอดภัยของระบบขึ้นมาก็สามารถแก้ไขปัญหาได้ทันทีเพื่อไม่ให้เกิดความเสียหาย หรือเป็นช่องทางในการทำลายความมั่นคงปลอดภัยของข้อมูล ตัวอย่างที่อาจสร้างความเสียหายต่อระบบสารสนเทศเพื่อการเรียนรู้ ได้แก่

1. การโจมตี (Attack) เป็นการกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ เพื่อเข้าควบคุมการทำงานทำให้ระบบเกิดความเสียหาย หรือเพื่อโจรกรรมข้อมูล เช่น การโจมตีที่สร้างความเสียหายต่อเทคโนโลยีสารสนเทศเพื่อการเรียนรู้ อย่าง Malicious หรือ Malware โปรแกรมคอมพิวเตอร์ที่ถูกเขียนขึ้นมาเพื่อมุ่งร้ายหรือเป็นอันตรายต่อระบบสารสนเทศของผู้ใช้ ที่รู้จักกันเป็นอย่างดี ได้แก่ ไวรัส เวอร์ม ม้าโทรจัน การทำงานของ Malicious Code เหล่านี้จะโจมตีในหลายรูปแบบ เช่น การสแกนหมายเลข IP Address เพื่อหาช่องโหว่และเปิดทางลับให้กับแฮกเกอร์ (Hacker) เข้ามาโจรกรรมข้อมูล หรือเจาะรหัสผ่าน (Cracking) ของผู้ใช้งาน เป็นต้น

2. ช่องโหว่ หรือความล่อแหลม (Vulnerabilities) เป็นความอ่อนแอของระบบคอมพิวเตอร์ หรือระบบเครือข่ายที่เปิดโอกาสภัยคุกคาม หรือผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลของได้ อันจะนำไปสู่ความเสียหายของสารสนเทศหรือการทำงานของระบบเครือข่ายที่ไม่มีกลไกในการกำหนดระบบล็อกอินเพื่อตรวจสอบชื่อผู้ใช้และรหัสผ่านที่ดีทำให้ผู้ไม่ประสงค์ดีสามารถคาดเดารหัสผ่านและลักลอบเข้าสู่ระบบโดยไม่ได้รับอนุญาตได้อย่างง่ายดาย เช่น การจัดทำบัญชีรายชื่อผู้ใช้ที่ไม่มีประสิทธิภาพ หละหลวมในการจัดทำบัญชีรายชื่อผู้ใช้ที่ลาออกจากองค์กรแล้ว ไม่มีการกำหนดหรือเปลี่ยนแปลงสิทธิ์ในการเข้าใช้งานกรณีที่ผู้ใช้มีการเปลี่ยนแหลงตำแหน่งงานหรือมีการ โยกย้ายหน่วยงาน และการกระทำที่ผู้ใช้งานระบบคอมพิวเตอร์ทั่วไปสามารถกระทำได้โดยง่ายแต่มักจะละเลยการปฏิบัติ ได้แก่ การไม่อัพเดทโปรแกรม Anti virus อันเป็นการเพิ่มข้อมูลคุณลักษณะของไวรัสใหม่ๆ ลงไปในฐานข้อมูลของโปรแกรมป้องกันไวรัสในเครื่องขอผู้ใช้ ซึ่งสามารถช่วยให้โปรแกรมป้องกันไวรัสสามารถตรวจจับไวรัสใหม่ๆ ได้แต่หากไม่มีการอัพเดทจะส่งผลให้โปรแกรมป้องกันไวรัสไม่รู้จักไวรัสตัวใหม่ๆ ส่งผลให้ระบบคอมพิวเตอร์มีความเสี่ยงต่อการติดไวรัสมากยิ่งขึ้น

3. ภัยคุกคาม (Threat) ภัยคุกคามมีด้วยกันหลายประเภท บางประเภทเป็นภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยเจตนาหรือ โดยความตั้งใจทำให้เกิดขึ้น ในขณะที่บางประเภทอาจจะเกิดขึ้นจากความไม่เจตนาทำให้เกิดขึ้นโดยผู้ใช้ภายในหรือภายนอกองค์กร เช่น อุบัติเหตุ ความเข้าใจผิดของผู้ใช้ ความไม่รู้ไม่เข้าใจในระบบ หรือ อาจจะเกิดขึ้นจากภัยธรรมชาติอย่างน้ำท่วม ไฟไหม้ แผ่นดินไหว แม้แต่ไฟฟ้าดับ รวมทั้งการก่อการร้าย การก่อจลาจล เป็นต้น

การรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการศึกษา

เทคโนโลยีสารสนเทศช่วยส่งเสริมศักยภาพให้แก่ผู้เรียนได้เรียนรู้อย่างเต็มประสิทธิภาพส่งผลให้ผู้เรียนมีคุณภาพต่อไป แต่ไม่มีสิ่งที่ทำให้คอมพิวเตอร์มีความมั่นคงปลอดภัย การทำให้ระบบคอมพิวเตอร์มีความมั่นคงปลอดภัยต้องการการลงมือทำและมีเหตุผลที่แตกต่างกัน [12] ดังนั้นการรักษาการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการเรียนรู้ จึงมีความจำเป็นเพื่อทำให้ระบบการเรียนรู้มีความน่าเชื่อถือ และสร้างความเชื่อมั่นให้แก่ผู้เรียน ดังนี้

1. การสำรองข้อมูล (Backup) การสำรองข้อมูลเป็นขั้นตอนแรกที่มีความสำคัญที่สุดในการป้องกันการสูญหายของข้อมูล หน่วยงานหลายแห่งหายไปวงการธุรกิจ หรือหยุดกิจการไป ส่วนหนึ่งเนื่องมาจากการสูญเสียข้อมูลที่มีค่า [12] การสำรองข้อมูลสามารถทำได้ในดิสก์ เทป งาน

พิมพ์กระดาษ หรือ ระบบคอมพิวเตอร์อื่นๆ และเป็นสิ่งสำคัญที่จะเก็บสำเนาข้อมูลเหล่านี้ไว้ในสถานที่ไกลจากที่เดิม

2. การเข้ารหัสข้อมูล (Encryptions) การเข้ารหัสข้อมูลเป็นขั้นที่สองของการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เนื่องจากเมื่อผู้ไม่ประสงค์ดีพยายามที่จะเข้าถึงข้อมูลใดๆ ข้อมูลเหล่านั้นก็จะไร้ประโยชน์ผู้ไม่ประสงค์ดีไม่สามารถนำข้อมูลเหล่านั้นไปใช้งานได้ เนื่องจากถูกเข้ารหัสเอาไว้

3. การติดตั้ง firewall ซึ่งเป็นองค์ประกอบหนึ่งของระบบเครือข่าย มีหน้าที่ในตรวจสอบข้อมูลที่ผ่านเข้าออกระหว่างระบบเครือข่ายภายในองค์กรและภายนอกองค์กรที่ไม่น่าไว้วางใจหรือที่ไม่ได้รับอนุญาต รวมทั้งการป้องการการโจมตีในรูปแบบ เช่น virus หรือ Spyware อีกด้วย firewall ถูกออกแบบมาทั้งชนิดที่เป็น Hardware และ Software ให้เลือกใช้งานโดยผู้ใช้งานทั่วไปควรจะให้ผู้ดูแลระบบ หรือผู้ที่มีความรู้ทางเทคนิคคอมพิวเตอร์เป็นผู้ติดตั้งให้

4. ตัวกรองเนื้อหา (Content Filter) เป็นซอฟต์แวร์กรองเนื้อหาที่จะช่วยให้ผู้ดูแลระบบสามารถจำกัดการเข้าถึงเว็บไซต์ต่างๆ ที่ไม่เหมาะสมของผู้ใช้ภายในเครือข่ายได้ เช่น การจำกัดการเข้าถึงเว็บไซต์ลามก อนาจาร ซึ่งมีความเหมาะสมอย่างยิ่งที่จะใช้ในสถาบันการศึกษาทั้งหลายที่มีการเชื่อมต่อเข้าสู่อินเตอร์เน็ตเพื่อป้องกันการค้นหาข้อมูลที่ไม่เหมาะสมของผู้เรียน

5. การตรวจจับการบุกรุก (Intrusion Detection System) เป็นระบบซอฟต์แวร์ หรือฮาร์ดแวร์ที่ติดตามการจราจรและพฤติกรรมที่น่าสงสัยบนรบเครือข่าย ทำหน้าที่แจ้งเตือนไปยังผู้ดูแลระบบทันทีที่พบการบุกรุก เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้น

กฎทอง [13] ของการตระหนักเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศทางการศึกษาได้แก่

- ยึดมั่นต่อนโยบายความมั่นคงปลอดภัยที่ถูกกำหนดขึ้นมาอย่างสม่ำเสมอ

- เก็บรหัสประจำตัวที่ใช้เกี่ยวกับระบบคอมพิวเตอร์และเครือข่ายเป็นความลับ

- ใช้เมล และอินเทอร์เน็ตอย่างระมัดระวัง

- ระมัดระวังและรอบคอบเมื่อใช้อุปกรณ์พกพาที่เกี่ยวกับระบบคอมพิวเตอร์

- รายงานข้อมูลเกี่ยวกับไวรัส การขโมย และการสูญเสียให้ผู้ที่เกี่ยวข้องได้รับทราบ

การสร้างความตระหนักและการฝึกอบรมด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อการศึกษา

ประเทศไทยมีผู้มีความรู้ด้านเทคโนโลยีสารสนเทศมากขึ้นทั้งภาครัฐและเอกชน และมีผู้จบการศึกษาในสาขาที่เกี่ยวข้องจำนวนไม่น้อย แต่ยังขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศอีกมาก [2] เนื่องจากคนคือส่วนที่อ่อนแอที่สุดของความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ [11], [14]

การฝึกอบรมด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเป็นกลไกหลักในการพัฒนาบุคลากรด้านการศึกษาให้มีความรู้ ทักษะ และความสามารถในการบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ [10] สร้างความตื่นตัวเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้เห็นว่าเป็นเรื่องใกล้ตัวที่ทุกคนต้องช่วยกัน โปรแกรมการฝึกอบรมนั้นอาจแตกต่างกันไป ซึ่งต้องปรับให้เข้ากับกับลักษณะขององค์กรหรือสถานศึกษานั้นๆ มีการแบ่งระดับการฝึกอบรมบุคลากรด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ออกเป็น 5 ระดับ [11], [15], [16] ดังนี้

ระดับ 1: ผู้บริหารระดับสูง ผู้บริหารระดับนโยบายและวิสัยทัศน์ การฝึกอบรม ควรกล่าวถึงภาพรวมของความสำคัญด้านความมั่นคงปลอดภัย ผลกระทบที่จะเกิดขึ้นหากถูกบุกรุก ด้วยผู้ไม่ประสงค์ดี หรือมีการติดไวรัสในระบบ รวมทั้งควรจะกล่าวถึงภาระหน้าที่ที่ต้องรับผิดชอบทั้งก่อนเกิดปัญหาและหลังจากเกิดปัญหา

ระดับ 2: ผู้บริหารระดับกลาง การฝึกอบรมด้านความมั่นคงปลอดภัยให้กับผู้บริหารระดับกลาง ควรจะมีความแตกต่างจากผู้บริหารระดับสูง เนื้อหาการอบรมจะต้องพูดถึงรายละเอียดมากขึ้น ในส่วนของนโยบายความมั่นคงปลอดภัย กระบวนการทำงาน มาตรฐานและแนวทางที่สอดคล้องกับงานที่ผิดชอบดูแลอยู่

ระดับ 3: บุคลากรระบบเครือข่าย การฝึกอบรมจะมีความแตกต่างจากผู้บริหารทั้ง 2 ระดับโดยจะมีรายละเอียดลงลึกที่งานที่ต้องทำประจำวันและเจาะลึกในด้านเทคนิคกับระบบที่ดูแลอยู่ เช่น ระบบปฏิบัติการด้านระบบเครือข่ายที่แสดงให้เห็นว่า Hacker สามารถเข้าสู่ระบบที่ไม่ปลอดภัยได้อย่างไร เพื่อให้มีความเข้าใจและมีความตระหนักว่าเรื่องความปลอดภัยว่าเป็นเรื่องที่ต้องดูแลกันแทบทุกวันเลยทีเดียว

ระดับ 4: ผู้ดูแลระบบความปลอดภัยคอมพิวเตอร์จำเป็นที่จะต้องมีความรู้ในขั้นสูง และมีเวลามากพอที่จะดูแลเรื่องของความมั่นคงปลอดภัยอย่างเพียงพอ เช่น มีเวลาดูเรื่องช่องโหว่ใหม่ ๆ ของระบบปฏิบัติการเป็นประจำ รวมทั้งทราบถึงวิธีการแก้ปัญหาที่ถูกต้อง เพื่อจะได้แนะนำการทำงานให้กับระดับที่เกี่ยวข้องต่อไป

ระดับ 5: ระดับปฏิบัติการ หรือผู้ใช้ทั่วไป เป็นผู้ที่มีความรู้ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศน้อยมาก เช่น เจ้าหน้าที่คีย์ข้อมูล เจ้าหน้าที่ธุรการ เจ้าหน้าที่บัญชี ฯลฯ ที่ต้องใช้คอมพิวเตอร์และระบบเครือข่ายในการทำงานประจำวัน ควรจะเรียนรู้วิธีการใช้งานคอมพิวเตอร์และอินเทอร์เน็ต วิธีการป้องกันไวรัสและการแก้ไขปัญหาที่ถูกต้องเป็นการเบื้องต้น รู้วิธีการป้องกันด้วยการใช้โปรแกรมสำหรับการป้องกัน การใช้งานเมลที่ถูกต้อง เป็นต้น

บทสรุป

ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเป็นปัญหาที่สำคัญระดับชาติ รัฐบาลให้ความสำคัญและสนใจกำกับดูแลอย่างใกล้ชิด มีการแต่งตั้งองค์กร และหน่วยงานเข้ามาดูแล กำหนดข้อบังคับ กฎหมายและพระราชบัญญัติที่เกี่ยวข้องออกมาบังคับใช้ สถาบันการศึกษาต่างเปิดสอนหลักสูตรที่เกี่ยวข้องทั้งระดับปริญญาตรี และปริญญาโท เมื่อพิจารณาการให้ความสำคัญเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของต่างประเทศ เช่น ประเทศออสเตรเลียมีการเปิดสอนสาขาทางด้านความมั่นคงปลอดภัย เช่น การจัดการความมั่นคงปลอดภัยทางอินเทอร์เน็ต, ความปลอดภัยและอาชญากรรมคอมพิวเตอร์, ความมั่นคงทางเทคโนโลยีสารสนเทศ, การบริหารความเสี่ยงด้านความมั่นคงปลอดภัย, นิติคอมพิวเตอร์ [17] สร้างความตื่นตัวในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กรและหน่วยงานที่เห็นความสำคัญเป็นอย่างดี

แต่อย่างไรก็ตามเทคโนโลยีสารสนเทศและนวัตกรรมที่เกี่ยวข้องคอมพิวเตอร์มีการเปลี่ยนแปลงอย่างรวดเร็วอยู่ตลอดเวลา ส่งผลให้ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศต้องมีการปรับตัวให้ทันตามไปด้วย เพื่อสร้างความมั่นใจและความเชื่อถือให้กับผู้ใช้งาน เช่นเดียวกับสถาบันการศึกษาที่ดำเนินกิจกรรมเกี่ยวกับการจัดการเรียนรู้เป็นหลัก มีข้อมูลปริมาณมหาศาลที่ต้องบริหารจัดการ เนื่องจากมีผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องจำนวนมาก ทั้งคณาจารย์ เจ้าหน้าที่ นักศึกษา และประชาชนทั่วไป ซึ่งกลุ่มคนเหล่านี้มีความสำคัญอย่างยิ่งต่อระบบการเรียนรู้ แต่ส่วนมากยังขาดทักษะที่ดีเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ประกอบกับเทคโนโลยีและนวัตกรรมที่ใช้ในการจัดการเรียนการสอนมีจำนวนมากขึ้นและมีหลายชนิดที่ต้องการการรักษาข้อมูลให้มีความมั่นคงปลอดภัยเป็นอย่างดี

ดังนั้นการสร้างความตระหนัก ความรู้ ความเข้าใจ เจตคติ และทักษะที่ดีเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศผ่านการเรียนการสอนและการฝึกอบรมยังคงต้องดำเนินการต่อไปด้วยความเอาใจใส่อย่างใกล้ชิดจากทุกฝ่าย และต้องดำเนินการอย่างเร่งด่วนเพื่อตามให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศและนวัตกรรมที่เปลี่ยนแปลงไปอย่างไม่หยุดยั้ง

เอกสารอ้างอิง

[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. 2543. แผนแม่บทเชิงกลยุทธ์เทคโนโลยีอิเล็กทรอนิกส์ คอมพิวเตอร์ โทรคมนาคม และสารสนเทศ พ.ศ. 2543-2552.

[2] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. 2552. แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) พ.ศ. 2552-2556.

[3] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. 2552. รายงานการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2551.

[4] Stephanie D. Hight. (2005). The importance of a security, education, training and awareness program. [Online]. [cite 2010 August 10] Available From: http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf

[5] Tomaž KLOBUČAR, Mahsa JENABI, and other. Security and Privacy Issues in_Technology-Enhanced Learning. [Online]. [cite 2010 August 10] Available From: http://www.mendeley.com/research/security-and-privacy-issues-in-technologyenhanced learning/#.

[6] A. Jalal, Mian Ahmad Zeb. (2008). Security Enhancement for E-Learning Portal. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March.

[7] Jokela P and Karlsudd P. (2007). Learning with Security. Journal of Information Technology Education,V.6

[8] E. Kritzinger and S.H von Solms. (2006). E-learning: Incorporating Information Security Governance. Informing Science and Information Technology. Vol. 3

[9] พนิดา พานิชกุล. 2553. ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ. กรุงเทพ:เคทีพี.

[10] Eibl C. and Schubert S. (2008) Development of E-Learning Design Criteria with Secure Realization Concepts. Springer-Verlag Berlin Heidelberg.

[11] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. 2550. แผนแม่บท ICT Security แห่งชาติ.

[12] Young D. Computer Security Basics [Online]. [cite 2010 August 10] Available From: http://www.ccl.net/cca/documents/dyoung/topics-orig/security1.html

[13] H.A. Krugera and W.D. Kearneyb. (2006). A prototype for assessing information security awareness. Elsevier Computer & Security.

[14] AT Stephanou and R Dagada. (2008. The impact of information security awareness training on information security behavior: The case for further research for Further Research. [Online]. [cite 2010 August 10] Available From: http://icsa.cs.up.ac.za/issa/2008/Proceedings/ISSA2008Proceedings.pdf

[15] ปริญญา หอมเอนก. 2549. Information Security Awareness Program เรื่องสำคัญขององค์กรที่ถูกมองข้าม?. eWeek Thailand ปักษ์แรก สิงหาคม.

[16] สานนท์ ฉิมพลี และ ภส จันทรศิริ. 2553. เอกสารประกอบการฝึกอบรมโครงการเสริมสร้างศักยภาพบุคลากร ICT ไทย หลักสูตรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ระดับที่ 3. กรุงเทพ: สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศ.

[17] Hentea M and Dhillon H. (2006) Towards Changes in Information Security Education. Journal of Information Technology Education,V.5