รายงานการเข้าร่วมสัมมนา

Promoting Cybersecurity Awareness:

Research on Communication Campaign to Promote Safe Online Behavior

จัดโดย

สาขาวิชานิเทศศาสตร์

มหาวิทยาลัยสุโขทัยธรรมาธิราช

ณ ห้องประชุม 1514 ชั้น 5 อาคารบริหาร

มหาวิทยาลัยสุโขทัยธรรมาธิราช

วันที่ 8 กรกฎาคม 2557

ผู้จัดทำ

อาจารย์ ดร.ขจิตพรรณ กฤตพลวิมาน

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

1. ชื่อ นางขจิตพรรณ **นามสกุล** กฤตพลวิมาน **อายุ** 37 **ปี**

ตำแหน่ง อาจารย์ **ระดับ** 6 **สังกัด** สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ไปเข้าร่วมสัมมนา การนำเทคโนโลยีสมัยใหม่มาใช้กับการเรียนการสอนทางไกล

วันที่ 8 กรกฎาคม 2557 **รวมระยะเวลา** 9.30-12.00 น.

จัดโดย สาขาวิชานิเทศศาสตร์ ม.สุโขทัยธรรมาธิราช ณ ห้องประชุม 1514 ชั้น 5 อาคารบริหาร

2. รายงานการสัมมนา

(1) หัวข้อเรื่อง Promoting Cybersecurity Awareness: Research on Communication Campaign to Promote Safe Online Behavior

(2) ผู้เข้าร่วมประชุมสัมมนา ประมาณ 30 คน เป็นคณาจารย์ประจำสาขาวิชานิเทศศาสตร์ และนักศึกษาระดับบัณฑิตศึกษา สาขาวิชานิเทศศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

(3) วิธีการประชุม/สัมมนา

หัวข้อปาฐกถาพิเศษในงานสัมมนา โดย Prof. Dr. Stephen D. McDowell จาก Florida State University

(4) วัตถุประสงค์ของการประชุมสัมมนา

1) เพื่อสร้างความเข้าใจในความสำคัญของการสนับสนุนและรณรงค์การรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ในองค์กร
2) เพื่อสร้างแนวทางในการทำวิจัยที่สนับสนุนการตระหนักรู้ถึงการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

(5) สรุปเนื้อหาจากการสัมมนา

ความสำคัญและความเป็นมาของกิจกรรมนี้คือ เพื่อนำเสนองานวิจัยที่เกี่ยวของกับธรรมาภิบาลด้านต่างๆ บนเครือข่ายอินเทอร์เน็ต และผู้ที่เกี่ยวข้องต่างๆ โดยอ้างอิงความร่วมมือด้าน Cybersecurity ระดับนานาชาติ เช่น องค์กร OECD (Organization for Economic Co-Operational Development) และ ITU (International Telecommunication Union)

อินเทอร์เน็ตเป็นส่วนหนึ่งของชีวิตของทุกคนในปัจจุบัน มีการใช้อินเทอร์เน็ตในที่ทำงานที่บ้านเพื่อความบันเทิงและการเชื่อมต่อกับผู้ที่ใกล้ชิด แต่การเชื่อมต่อบนระบบอินเทอร์เน็ตทำให้เกิดความเสี่ยงเพิ่มขึ้นจากการโจรกรรม การทุจริตและการละเมิด ผู้ใช้งานทั่วไปต้องเผชิญกับภัยคุกคามในโลกไซเบอร์อยู่ตลอดเวลา ซึ่งส่งผลกระทบต่อโครงสร้างพื้นฐานและเศรษฐกิจ ดังนั้นโลกไซเบอร์จึงเป็นหนึ่งในสิ่งที่สำคัญที่สุดของการรักษาความปลอดภัยแห่งชาติของประเทศ โดยที่ผู้ใช้งานแต่ละคนมีบทบาทความรับผิดชอบร่วมกันในการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์

1. **ความท้าทายของระบบเครือข่ายคอมพิวเตอร์ที่มีลักษณะเปิด** มีหลากหลายประเด็นที่ทำให้เกิดภัยคุกคามต่างๆ หรือช่องโหว่ต่อความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ ดังนี้
    - ระบบเครือข่ายคอมพิวเตอร์เป็นการเชื่อมต่อระหว่างโหนดเครือข่าย หรือเครื่องคอมพิวเตอร์ ซึ่งเป็นระบบเปิด
    - มีการเชื่อมต่อระหว่างโหนดเครือข่ายหรือเครื่องคอมพิวเตอร์ในจุดเชื่อมต่อหนึ่งๆ หลากหลายการเชื่อมต่อ
    - ระบบเครือข่ายคอมพิวเตอร์มีการเชื่อมโยงระหว่างเครือข่ายภายในและการเชื่อมโยงระหว่างเครือข่ายภายนอก
    - ลักษณะการใช้งานที่มีการใช้งานซ้ำๆ หรือประยุกต์ใช้โดยทั่วไปในสเกลขนาดใหญ่ จำเป็นต้องอาศัยโครงสร้างพื้นฐานเครือข่าย เช่น เครือข่ายทางการค้า เครือข่ายการจราจร
    - ระบบเครือข่ายคอมพิวเตอร์จำเป็นต้องมีมาตรฐานและโพรโทคอลกลางในการสนับสนุนการใช้งานร่วมกันระหว่างอุปกรณ์ต่างๆ หรือโปรแกรมประยุกต์ต่างๆ
    - ระบบเครือข่ายคอมพิวเตอร์ระบบเปิดจะมีการเชื่อมต่อกันระหว่างผู้ใช้งานอย่างไร้พรมแดน
    - ผู้ใช้งานมีหลากหลายประเภท หลากหลายจุดประสงค์และเจตนา
    - ผู้ใช้งานมีความรู้ ความพร้อม และความต้องการในการใช้คอมพิวเตอร์และระบบเครือข่ายแตกต่างกันหลายระดับ
    - การรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์มีหลายระดับจาก ระบบเครือข่ายส่วนบุคคล ระบบเครือข่ายองค์กรขนาดเล็ก ขนาดใหญ่ ระบบเครือข่ายระดับภูมิภาค และระบบเครือข่ายสาธารณะ
    - การประสบปัญหาเกี่ยวกับการขาดแคลนทรัพยากรเครือข่ายคอมพิวเตอร์ โครงสร้างการสื่อสารพื้นฐาน

2. **การควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศ**

การควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศ (access control) เป็นความสามารถในการจำกัดและการควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศต่างๆ เช่น เครื่องโฮสต์ เครื่องแม่ข่าย ระบบงานประยุกต์ และเครือข่ายคอมพิวตอร์ ผ่านการเชื่อมต่อสื่อสารหรือระบบเครือข่าย ดังนั้นเพื่อให้สามารถควบคุมการเข้าถึงได้จึงควรมีวิธีในการระบุตัวตนว่าเป็นใคร สามารถพิสูจน์ตัวจริงของผู้ที่ต้องการเข้าถึงสารสนเทศได้ ซึ่งผู้ใช้งานแต่ละคนมีสิทธิ์ในการเข้าถึงสารสนเทศ หรือใช้งานสารสนเทศแตกต่างกันไปตามแต่ที่ได้รับอนุญาต

การควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศส่วนใหญ่พิจารณาตามมาตรฐาน ISO 17799 โดยมาตรฐาน ISO 17799 ซึ่งเป็นมาตรฐานการบริหารการรักษาความมั่นคงปลอดภัย ได้ระบุถึงความสำคัญของการควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศ โดยมีจุดมุ่งหมายคือ

- เพื่อควบคุมการเข้าถึงสารสนเทศ
- เพื่อป้องกันการเข้าถึงสารสนเทศต่างๆ โดยไม่ได้รับอนุญาต
- เพื่อป้องกันการให้บริการเครือข่ายคอมพิวเตอร์
- เพื่อตรวจจับการเข้าถึงสารสนเทศที่ผิดปกติ หรือการเข้าถึงที่ไม่ได้รับอนุญาต

การควบคุมการเข้าถึงตามมาตรฐาน ISO 17799 หรือ BS 7799 (ต่อมาเปลี่ยนเป็น ISO/IEC 27002) สามารถตอบสนองต่อการดำเนินการด้านต่างๆ รวมถึงการรักษาความมั่นคงปลอดภัยในการใช้งานสารสนเทศ โดยมีมาตรการควบคุมด้านต่างๆ ดังนี้

- ข้อกำหนดทางธุรกิจสำหรับควบคุมการเข้าถึง (business requirement for access control)
- การจัดการการเข้าถึงของผู้ใช้งาน (user access management)
- การกำหนดหน้าที่ความรับผิดชอบผู้ใช้งาน (user responsibility)
- การควบคุมการเข้าถึงเครือข่าย (network access control)
- การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)
- การควบคุมการเข้าถึงโปรแกรมประยุกต์ (application access control)
- การควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศ (Information access control)
- การควบคุมอุปกรณ์สื่อสารแบบพกพา (mobile computing access control)
- การควบคุมการเข้าถึงความมั่นคงปลอดภัยสารสนเทศจากภายนอกองค์กร (teleworking access control)

3. แนวทางการส่งเสริมการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

ในประเทศสหรัฐอเมริกาได้มีการรณรงค์ให้ผู้ใช้งานทราบขั้นตอนง่ายๆ ในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลออนไลน์ของตนเอง ซึ่งผู้ใช้อินเทอร์เน็ตทุกคนสามารถเรียนรู้ได้เอง ในระหว่างช่วงเวลาการจัดกิจกรรมการเรียนรู้ Cyber Security แห่งชาติ โดยมีการรณรงค์ด้านต่างๆ รวมถึงธรรมาภิบาลการใช้งานอินเทอร์เน็ตได้อย่างปลอดภัย ให้แก่กลุ่มผู้ใช้งานหลายกลุ่ม ได้แก่ นักเรียนระดับประถมศึกษา มัธยมศึกษา ผู้ปกครอง อาจารย์ ผู้สูงอายุ หน่วยงานรัฐบาล อุตสาหกรรม ธุรกิจขนาดเล็ก และผู้เกี่ยวข้องกับการบังคับใช้กฎหมาย โดยมีการส่งเสริม รณรงค์ให้ผู้ใช้งานเกี่ยวกับประเด็นต่างๆ ดังต่อไปนี้

- ตั้งรหัสผ่านที่รัดกุมและไม่แบ่งปันให้บุคคลอื่น

- ติดตั้งระบบปฏิบัติการ เบราว์เซอร์และซอฟต์แวร์ที่สำคัญอื่น ๆ
- ประกาศ แจ้งข่าว เตือนผู้ใช้งานอินเทอร์เน็ตในครอบครัว เพื่อน และชุมชนเกี่ยวกับความปลอดภัยทางอินเทอร์เน็ต
- จำกัดจำนวนของข้อมูลส่วนบุคคลที่โพสต์ออนไลน์และใช้การตั้งค่าความเป็นส่วนตัวเพื่อหลีกเลี่ยงการใช้ข้อมูลร่วมกันอย่างกว้างขวาง

นอกจากนี้ยังมีตัวอย่างการรณรงค์การสร้างความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์และโลกไซเบอร์ของประเทศสหรัฐอเมริกา โดยมีการแบ่งกิจกรรมส่งเสริมในแต่ละสัปดาห์ในเดือนตุลาคมของทุกปี (ดังรายละเอียดใน http://staysafeonline.org/ncsam/get-involved/promote-NCSAM) เช่น

สัปดาห์ที่ 1: 1-3 ตุลาคม 2014: หยุดการเชื่อมต่อ

มีจุดมุ่งหมายเพื่อสร้างความตระหนักด้านความปลอดภัยทางออนไลน์ในหมู่ชาวอเมริกันทุกคนและเสริมสร้าง แนวความคิดว่า การหยุดการเชื่อมต่อ เป็นมาตรการที่ง่ายที่ทุกคนควรนำไปใช้ เพื่อสร้างความปลอดภัยการใช้งานออนไลน์ต่างๆ

สัปดาห์ที่ 2: 6-10 ตุลาคม 2014 : รูปแบบการพัฒนาระบบรักษาความปลอดภัยของผลิตภัณฑ์ไอที

การรักษาความมั่นคงปลอดภัยเป็นผลิตภัณฑ์เทคโนโลยีสารสนเทศที่เป็นกุญแจสำคัญในโลกไซเบอร์ เป็นองค์ประกอบสำคัญในการออกแบบซอฟแวร์ การพัฒนาทดสอบและบำรุงรักษา ซอฟแวร์ที่ใช้ในชีวิตประจำวัน เช่น ซอฟต์แวร์บนโทรศัพท์ แท็บเล็ตและคอมพิวเตอร์ ซึ่งยังคงมีช่องโหว่ของข้อมูลส่วนบุคคลและความเป็นส่วนตัว ในสัปดาห์นี้จะกำหนดเป้าหมายให้ความรู้แก่ผู้มีส่วนได้ส่วนเสียเหล่านี้และให้ความรู้ผู้อื่นเกี่ยวกับสิ่งที่ต้องดำเนินการและการเลือกใช้ผลิตภัณฑ์ไอทีที่ปลอดภัย

สัปดาห์ที่ 3: 13-17 ตุลาคม 2014: โครงสร้างพื้นฐาน

อินเทอร์เน็ตมีความเกี่ยวข้องเกือบทุกด้านในชีวิตประจำวันของทุกคนและเป็นรากฐานสำคัญสำหรับโครงสร้างพื้นฐานที่ช่วยในกระบวนการทำงานต่างๆ ระบบสนับสนุนการผลิตไฟฟ้า การให้บริการทางการเงิน การขนส่งและการสื่อสารต่างๆ มีความเชื่อมโยงกันมากขึ้นผ่านอินเทอร์เน็ต สัปดาห์ที่ 3 นี้ให้ความสำคัญต่อการปกป้องโครงสร้างพื้นฐานที่สำคัญและการรักษาความมั่นคงปลอดภัยอุปกรณ์ทั้งหมดที่เชื่อมต่อกับอินเทอร์เน็ต

สัปดาห์ที่ 4: 20-24 ตุลาคม 2014 : Cybersecurity สำหรับธุรกิจขนาดเล็กและขนาดกลางและผู้ประกอบการ

ธุรกิจขนาดเล็กและขนาดกลางเป็นส่วนขับเคลื่อนสำคัญของเศรษฐกิจ แต่ส่วนใหญ่ผู้ประกอบการเหล่านี้มักไม่เห็นว่าตนเองเป็นเป้าหมายสำหรับการโจมตีในโลกไซเบอร์ ในสัปดาห์นี้จะมุ่งเน้นในการเพิ่มโอกาสทางธุรกิจและสร้างความน่าเชื่อถือทางธุรกิจต่อการรักษาความมั่นคงปลอดภัยขององค์กรที่ต้องติดต่อสื่อสารผ่านโลกไซเบอร์

สัปดาห์ที่ 5: 27-31 ตุลาคม 2014: อาชญากรรมในโลกไซเบอร์และการบังคับใช้กฎหมาย

สัปดาห์นี้จะเน้นเรื่องความตระหนักถึงและให้ความรู้เจ้าหน้าที่ที่บังคับใช้กฎหมายเกี่ยวกับวิธีการที่จะช่วยประชาสัมพันธ์แก่ประชาชนในการป้องกันอาชญากรรมและให้ความรู้ประชาชนทั่วไปเกี่ยวกับวิธีป้องกันตัวเองจากการเป็นเหยื่อของการโจรกรรมหลอกลวงฟิชชิ่งและอาชญากรรมอื่น ๆ ทางออนไลน์

(6) ประโยชน์ที่ได้รับ

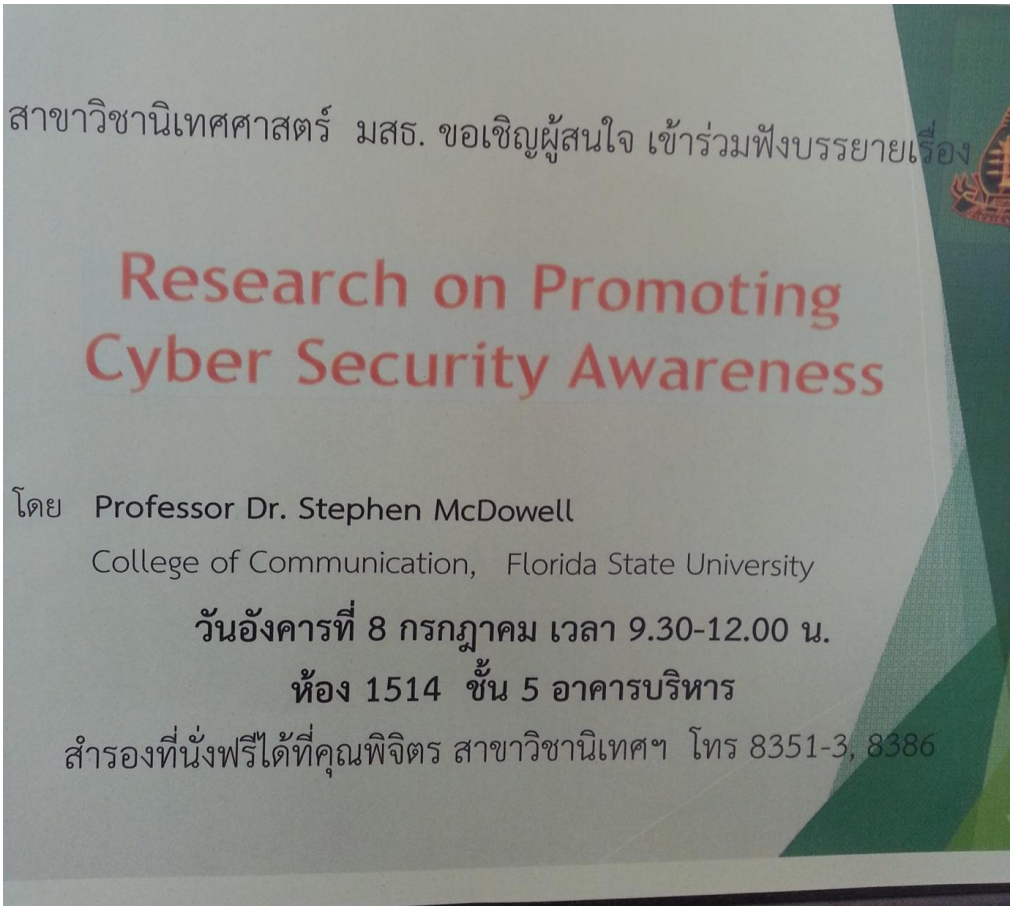
(6.1) ประโยชน์ที่ผู้เข้าร่วมสัมมนาได้รับ

1) ทราบแนวทางการสร้างโครงการต่างๆ และการวิจัยที่สนับสนุนการรักษาความมั่นคงปลอดภัย
2) เพิ่มแนวคิดในการจัดกิจกรรมโครงการบริการสังคมหรือบริการวิชาการต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบเครือข่ายเบื้องต้น

(6.2) ประโยชน์ที่มหาวิทยาลัยได้รับ

1) ทราบแนวทางการจัดกิจกรรมรณรงค์ความรู้ด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารสำหรับมหาวิทยาลัย
2) แนวทางการให้คำปรึกษาวิทยานิพนธ์ การค้นคว้าอิสระ ด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารในระดับองค์กร

(7) ภาพกิจกรรมการสัมมนา


สาขาวิชานิเทศศาสตร์ มสธ. ขอเชิญผู้สนใจ เข้าร่วมฟังบรรยายเรื่อง
Research on Promoting Cyber Security Awareness
โดย Professor Dr. Stephen McDowell
College of Communication, Florida State University
วันอังคารที่ 8 กรกฎาคม เวลา 9.30-12.00 น.
ห้อง 1514 ชั้น 5 อาคารบริหาร
สำรองที่นั่งฟรีได้ที่คุณพิจิตร สาขาวิชานิเทศฯ โทร 8351-3, 8386


Promoting Cybersecurity Awareness:
Research on Communication Campaigns to
Promote Safe Online Behavior
Stephen D. McDowell
(with Judd Butler, Xiuwen Liu)
Florida State University
for
School of Communication Arts
Sukhothai Thammatirat University
July 8, 2014