สรุปบทเรียน งานพัฒนาความรู้ครั้งที่ ๒/๒๕๕๖

หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล DS๐๓
ชื่อ-สกุล ว่าที่ ร.ต.ธเนศ แซวหลี ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

กลุ่ม/ฝ่าย บริหารทั่วไป

วันที่อบรม วันที่ ๖ สิงหาคม ๒๕๖๖ ถึง วันที่ ๗ สิงหาคม ๒๕๖๖

วัตถุประสงค์

๑.เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเตอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในยุคดิจิทัล

๒.เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง เพื่อให้ปลอดภัยจากภัยคุกคาม

๓.เพื่อให้สามารถยกตัวอย่างภัยคุกคามต่างๆ ได้

๔.เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

สรุปบทเรียน

ในปัจจุบันเทคโนโลยีและอินเทอร์เน็ตถือเป็นปัจจัยที่สำคัญในการดำรงชีวิตของมนุษย์ จนอาจจะเป็นปัจจัยที่ ๕ ซึ่งภัยคุกคามทางไซเบอร์เป็นภัยคุกคามทางเศรษฐกิจสังคมและความมั่นคงของประเทศ การรักษาความมั่นคงปลอดภัยเป็นการสร้างภูมิคุ้มกันเบื้องต้นและการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศและอินเทอร์เน็ต ดังนั้นจึงต้องเรียนรู้ถึงการมีวิธีปกป้องตนเองรวมทั้งข้อกฎหมายที่เกี่ยวข้องตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย

ในช่วงระยะเวลา ๑๐ ปี (ปี ๒๐๐๐ - ปี ๒๐๑๐) ปริมาณผู้ใช้งานอินเทอร์เน็ตมีแนวโน้มการใช้งานสูงขึ้น ถึงกว่า ๙ เท่า แบบก้าวกระโดด การใช้งานอินเทอร์เน็ตสามารถเข้าถึงได้เกือบ ๕๐% ของประชากรทั่วโลก ทำให้อินเทอร์เน็ตนั้นค่อนข้างมีบทบาทสำคัญต่อการดำเนินชีวิตประจำวัน ปัจจุบันแนวโน้มการใช้งานอินเทอร์เน็ตจะเป็นในรูปแบบที่เรียกว่าสื่อสังคมออนไลน์หรือ Social Media ทุกคนมีโอกาสร่วมกันสร้างสรรค์อินเทอร์เน็ตทำให้เกิดการใช้งานในรูปแบบต่าง ๆ จากปัจจัยเบื้องต้น เมื่ออินเทอร์เน็ตเป็นส่วนหนึ่งของชีวิตย่อมมีผลกระทบทั้งด้านดีและไม่ดีผู้ไม่ประสงค์ดีหรืออาชญากรมีแนวโน้มที่จะเปลี่ยนแปลงรูปแบบให้เข้ากับสถานการณ์หรือการใช้งานอินเทอร์เน็ตที่เป็นปัจจุบันนั่นหมายถึง สิ่งที่เกิดขึ้นกับโลกปัจจุบันที่ไม่ได้เกิดขึ้นบนอินเทอร์เน็ตมีแนวโน้มที่จะเปลี่ยนรูปแบบให้มาเกิดขึ้นบน อินเทอร์เน็ต

สถิติการใช้งานของประเทศไทย

สังคมไทยผู้ที่มีอายุระหว่าง ๒๐-๓๐ ปีเป็นกลุ่มที่ใช้งานอินเทอร์เน็ตสูง จากสถิติหลายช่วงปีที่ผ่านมา มีปริมาณเกือบ ๖๐-๗๐ เปอร์เซ็นต์ดังนั้นคนกลุ่มนี้มีโอกาสมีความเสี่ยงที่จะเผชิญโลกของอาชญากรรม ค่อนข้างสูง รวมทั้งกลุ่มผู้สูงวัยหรือวัยหลังเกษียณที่เพิ่งเริ่มต้นการใช้งาน โดยประชาชนคนไทยส่วนมากใช้ อินเทอร์เน็ตในช่วงเวลางาน

ความสัมพันธ์และการกระจายตัวของข้อมูล

โลกของ Social Media ข้อมูลเดิม ๆ ซ้ำ ๆ ที่เคยรับ ซึ่งถ้าเป็นข้อมูลที่ไม่เหมาะสมหรือข้อมูลเท็จหลอกลวงก็อาจจะวนเวียนกลับมาให้รับรู้ การได้รับทราบข้อมูลเดิม ๆ ทำให้อาจจะตกเป็นเหยื่อกับข้อมูลลักษณะดังกล่าว เช่น หลอกรับบริจาคให้โอนเงินช่วยเหลือผู้ป่วย ทั้งที่ผู้ขอรับบริจาคได้รับการรักษาแล้ว เป็นต้น ปัจจุบันแนวโน้มที่โลกออนไลน์ จะมีระบบการใช้จ่ายเป็น Digital currency ระบบ payment Gateway มีการใช้จ่ายเงินรูปแบบสกุลอื่น ๆ นอกจากนี้คอมพิวเตอร์โน้ตบุ๊ค คอมพิวเตอร์ตั้งโต๊ะก็มีแนวโน้มที่จะเปลี่ยนแปลงไปใช้งานสมาร์ทโฟน

วิวัฒนาการของเว็บไซต์

ยุค Web ๑.๐ เป็นเว็บไซต์ที่สร้างขึ้นมาเพื่อให้ผู้ที่พัฒนาหรือสร้างเว็บไซต์นั้นติดต่อสื่อสารกับบุคคลอื่นอย่างเดียว (one way Communication)

ยุค Web ๒.๐ เป็นการใช้อินเทอร์เน็ตลักษณะที่เรียกว่า Two Way Communication เปิดโอกาสให้ผู้ใช้งานสามารถที่จะโต้ตอบกับบุคคลอื่นสนทนากับบุคคลอื่น ๆ ได้ web ๒.๐ ในยุคแรกเลย คือ เว็บบอร์ด และเป็นยุคของที่เรียกว่าเป็น Web Platform

ยุค Web ๓.๐ เป็นยุคปัจจุบัน ช่วงรอยต่อระหว่าง Web ๒.๐ และ Web ๓.๐ ความแตกต่าง คือ platform ต่าง ๆ มีความฉลาดมากขึ้น เนื่องจากมีข้อมูลมหาศาล (Big Data) สามารถนำข้อมูลมาวิเคราะห์ ให้เข้าถึงผู้ใช้งาน สร้างสิ่งที่ต้องการให้ผู้ใช้งาน มีการเชื่อมโยงเนื้อหาสัมพันธ์ที่มีความสัมพันธ์กันกับ แหล่งข้อมูลอื่น ๆ เป็นเครือข่ายเดียวทั่วโลก

รูปแบบการกระทำผิดทางอินเทอร์เน็ต (Social Engineering)

คือ ปฏิบัติการทางจิตวิทยาหลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญ เกี่ยวกับคอมพิวเตอร์ เช่น ส่งอีเมล์หลอกลวงให้โอนเงิน

Password Guessing คือ การเดา Password เพื่อเข้าสู่ระบบ

Denial of Service คือ การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

Decryption คือ การถอดรหัสข้อมูล

Birthday Attacks คือ การสุ่มคีย์ขึ้นมา และตรงกับที่กำหนดไว้

Man In the middle Attacks คือ การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

ประเภทการกระทำผิดทางคอมพิวเตอร์

Hacker คือ บุคคลที่ศึกษาค้นคว้าเรื่องเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ มีความสามารถในการเข้าถึงโปรแกรมหรือระบบต่าง ๆ แล้วนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker คือผู้ที่มีความรู้ความเข้าใจในระบบคล้าย Hackerแต่ Cracker มีเจตนาที่จะทำลายก่อความเสียหาย

Script kiddy คือ บุคคลที่ยังไม่ค่อยมีความชำนาญในการแฮ็กมากนัก ไม่สามารถเขียนโปรแกรมในการ เจาะระบบได้เอง ส่วนใหญ่เป็นมือใหม่ที่อยากทดลองเป็นแฮ็กเกอร์

Spy คือ บุคคลที่ถูกจ้างเพื่อเจาะระบบและขโมยข้อมูล

Employee คือ พนักงานในองค์กรที่นำความลับขององค์การไปเผยแพร่โดยไม่เจตนา แล้วทำให้ระบบขององค์กรถูกโจมตี

Terrorist คือ บุคคลที่ก่อความไม่สงบบนเว็บไซต์หรือเครือข่ายอินเทอร์เน็ต ทำให้ไม่สามารถใช้งานได้

สิ่งที่ต้องฟังระวังในการใช้งานบนอินเตอร์เน็ต

การโจมตีของ Malware and Virus Threat รูปแบบของไฟล์ที่ส่งต่อผ่านอีเมล์หรืออาจจะส่งผ่านสื่อสังคมออนไลน์หรือ Social Media

การโจมตีของ Zombie attack เป็นรูปแบบแนวโน้มที่จะมีมากในปัจจุบัน โดยปล่อยไวรัสไปยังคอมพิวเตอร์ เครือข่ายของอุปกรณ์คอมพิวเตอร์ที่ติดมัลแวร์กลายเป็น Zombie ถูกแฮกเกอร์ควบคุม

การหลอกลวงเชิงจิตวิทยา (Social Engineering) เพื่อให้เปิดเผยข้อมูล Phishing เป็นรูปแบบหนึ่งของการทำ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ส่วนใหญ่จะมา ในรูปแบบอีเมล์ เว็บไซต์ และสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ ที่จะให้ผู้ใช้กรอกข้อมูลส่วนบุคคลที่เป็นความลับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) และได้ประกาศในราชกิจจานุเบกษา เมื่อ ๒๕ มกราคม ๒๕๖๐

คำศัพท์เกี่ยวกับคอมพิวเตอร์ในมาตรา ๓

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดสิ่งใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูลข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในคอมพิวเตอร์ ในสภาพที่ระบบอาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ผู้ให้บริการ" หมายความว่า (๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่าน ทางระบบคอมพิวเตอร์ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของ บุคคลอื่น (๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตราพระราชบัญญัตินี้

สิ่งที่สำคัญที่เป็นจุดเด่นของ พ.ร.บ. ฉบับนี้ คือ ข้อมูลจราจรทางคอมพิวเตอร์ โดยถ้ามีการทำผิดทางเครือข่ายอินเตอร์เน็ตหรือเครือข่ายคอมพิวเตอร์ จะสามารถนำข้อมูลจราจรทางคอมพิวเตอร์มาทำการตรวจสอบเพื่อให้ทราบว่าผู้กระทำความผิดนั้น เป็นใคร อย่างไร ในเวลานั้น ๆ

ตัวอย่าง การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรานี้เป็นการป้องกันบุคคลที่นำข้อมูลที่เป็นความลับเกี่ยวกับมาตรการการป้องกันระบบฐานข้อมูลไปเปิดเผยโดยมิชอบ แล้วทำให้เกิดความเสียหายเกิดขึ้น เช่น นำรุ่น เวอร์ชั่นระบบรักษาความปลอดภัยขององค์กรไปเปิดเผย และมีผู้นำข้อมูลเหล่านั้นไปใช้ในการโจมตีระบบและเป็นผลสำเร็จทำให้เกิดความเสียหาย ถ้ามีการนำไปพูดและพิสูจน์ทราบ บุคคลนั้นจะมีความผิดตามมาตรานี้

ประโยชน์ที่ได้รับ

มีความรู้ที่จะป้องกัน รักษาความมั่นคง ปลอดภัย บนอินเทอร์เน็ตและการปฏิบัติตนที่ถูกต้อง ทั้งต่อตนเอง และหน่วยงาน