# ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

นางสาวอาภัสนันท์ สุดเจริญ ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ กองเทคโนโลยีชีวภาพทางดิน
ที่มา : อบรมวันที่ 16 พฤศจิกายน 2568 ฝึกอบรมผ่านระบบ OCSC Learning Portal ศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ สำนักงาน ก.พ. โดย อาจารย์ณัฐ พยงค์ศรี นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

อินเทอร์เน็ตมีความสำคัญกับชีวิตมนุษย์ และมีบทบาทสำคัญกับการดำเนินชีวิตในปัจจุบัน อำนวยความสะดวกให้กับมนุษย์สามารถสื่อสารผ่านทางข้อความ รูปภาพ วิดีโอต่างๆ มีการโต้ตอบและทำกิจกรรมร่วมกันบนอินเทอร์เน็ตอีกด้วย แต่สิ่งที่ต้องพึงระวังนั้นคืออาชญากรออนไลน์ ที่มีการปรับตัวให้ทันสมัย โดยใช้อินเทอร์เน็ตช่วยในการหลอกลวง ทำให้เกิดการสูญเสียทรัพย์สินได้อย่างง่ายดาย ดังนั้นจึงต้องมีความรู้ ความเข้าใจ และสามารถป้องกัน ตรวจสอบความปลอดภัย เพื่อป้องกันความเสียหายทางด้านข้อมูลและทรัพย์สินต่างๆ โดยมีรายละเอียด ดังนี้

**1. สถิติการใช้งานอินเทอร์เน็ตของประเทศไทย** คนไทย อายุ 20 – 30 ปี ใช้งานอินเทอร์เน็ตค่อนข้างสูง ประมาณ 60 – 70 เปอร์เซ็นต์ โดยส่วนใหญ่คนไทยจะใช้อินเทอร์เน็ตสูงสุดในช่วงเวลาการทำงาน มีโอกาสเผชิญกับภัยคุกคามบนโลกอินเทอร์เน็ตสูง อีกทั้งสังคมผู้สูงอายุบางท่านที่เพิ่งเริ่มใช้งานอินเทอร์เน็ตนั้นมีความเสี่ยงสูงเช่นกัน โดยอาจถูกหลอกลวงผ่าน Call center เป็นต้น

**2. วิวัฒนาการของเว็บไซต์** หรือยุคของอินเทอร์เน็ต แบ่งเป็น 4 ยุค ได้แก่

2.1 Web 1.0 การให้บริการเว็บไซต์ในรูปแบบสื่อสารทางเดียว (One way communication) เป็นยุคที่ผู้พัฒนาเว็บไซต์หรือผู้ดูแลระบบจะเป็นผู้สร้างเนื้อหาเว็บไซต์ แล้วให้ผู้ใช้เข้ามาดูเนื้อหาอย่างเดียว ไม่มีโอกาสตอบโต้กับผู้อื่น นอกจากติดต่อผ่านอีเมลหรือโทรศัพท์ เท่านั้น

2.2 Web 2.0 การใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบสื่อสารสองทาง (Two way communication) เป็นยุคที่ให้ผู้ใช้งานสามารถโต้ตอบหรือแสดงความคิดเห็นต่างๆ ได้ และในยุค Web 2.0 นั้น มีการพัฒนาที่เรียกว่า เว็บแพลตฟอร์ม ซึ่งเป็นรูปแบบที่เจ้าของเว็บไซต์ไม่นิยมสร้างเนื้อหา แต่จะเปิด โอกาสให้ผู้ใช้งานเข้ามาสร้างเนื้อหาและเผยแพร่ให้ผู้ใช้อื่นๆ เข้ามาตอบโต้ระหว่างกันได้มากขึ้น เช่น Wikipedia Facebook และ YouTube เป็นต้น นับเป็นยุคทองของผู้พัฒนาเว็บไซต์ และมีการพัฒนาเป็น Web Marketing

2.3 ยุค Web 3.0 เป็นการนำข้อมูล Big Data มาวิเคราะห์ประมวลผลผ่านแพลตฟอร์มต่างๆ เช่น ภาพ วิดีโอ ต่างๆ โดยมีการอัปโหลดผ่านสมาร์ทโฟนเป็นหลัก ในอนาคตอาชีพที่น่าสนใจ คืออาชีพ Big Data Analysis เป็นการวิเคราะห์ข้อมูลทางด้านเศรษฐกิจ สังคมฯลฯ

**3 ประเภทของผู้กระทำผิดทางคอมพิวเตอร์**

3.1 Hacker คือ บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ แต่นำความรู้ไปใช้ในทางที่ผิด

3.2 Cracker คือ บุคคลที่คล้ายกับ Hacker แต่จะนำช่องโหว่ทางคอมพิวเตอร์มาโจมตีให้เกิดความเสียหายในระบบคอมพิวเตอร์

3.3 Script Kiddy คือ บุคคลที่ได้รับทราบข้อมูลใดๆ ที่เจาะช่องโหว่ของเว็บไซต์ สามารถสร้างความเสียหายกับระบบปฏิบัติการได้

3.4 Spy คือ บุคคลที่แอบเข้ามาในระบบปฏิบัติการคอมพิวเตอร์เพื่อสืบข้อมูลต่างๆ แ ล ะ น ำ ความลับออกไปเผยแพร่สู่บุคคลภายนอกโดยไม่ได้รับอนุญาต

3.5 Employee คือ บุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่ได้ตั้งใจ ทำให้ผู้ที่ไม่ประสงค์ดีที่ได้รับข้อมูล สามารถโจมตีระบบปฏิบัติการได้

3.6 Terrorist คือ บุคคลที่ก่อความไม่สงบในเครือข่ายอินเทอร์เน็ต เจาะระบบข้อมูลที่เป็นความลับนำมาเผยแพร่

**4 รูปแบบของการกระทำความผิด**

4.1 Social Engineering หมายถึง การปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับ โดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

4.2 Password Guessing หมายถึง การเดา Password เพื่อเข้าสู่ระบบ

4.3 Denial of Service (DOS) หมายถึง การโจมตีลักษณะหนึ่ง ที่อาศัยการส่งคำสั่งลวง ไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมากๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

4.4 Man in the Middle Attacks หมายถึง การพยายามที่จะทำตัวเป็นคนกลาง เพื่อคอยดักเปลี่ยนแปลงข้อมูล โดยที่คู่สนทนาไม่รู้ตัว

**5 สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต**

5.1 การโจมตีแบบ Zombie attack ผู้ไม่ประสงค์ดีที่ต้องการโจมตีเครือข่ายหรือระบบใดๆ จะทำการปล่อยไวรัสไปยังเครื่องคอมพิวเตอร์ของเหยื่อ เมื่อถูกสั่งการจะทำตามคำสั่ง เกิดการโจมตีอย่างรุนแรงที่เป้าหมาย ทำให้การติดตามผลค่อนข้างยาก เกิดความเสียหายเป็นอย่างมาก

5.2 กลลวงทางสังคม Social Engineering หรือ Phishing เช่น การปลอมตัวจากผู้ชายเป็นผู้หญิง ทำการโชว์ภาพอนาจารแล้วเรียกเก็บเงิน และการปลอมแปลงเว็บไซต์ โปรแกรมต่างๆ เพื่อหลอกลวงให้โอนเงิน

5.3 การละเมิดข้อมูลส่วนบุคคล เช่น การใช้งาน Facebook แล้วทำการเช็คอินโดยตั้งค่าเป็นสาธารณะ อาจทำให้มีคนติดตาม ทำให้เกิดการโจรกรรมเกิดขึ้นได้

5.4 การละเมิดความเป็นส่วนตัว เช่น Google map ได้บังเอิญทำการถ่ายภาพที่ไม่เหมาะสมแล้วอัปโหลดสู่โลกอินเทอร์เน็ต เกิดการละเมิดความเป็นส่วนตัว ซึ่งผู้ก่อการร้ายสามารถเข้ามาเช็คใน Google map ได้ เพื่อดูว่าพื้นที่เป้าหมายนั้น มีระบบรักษาความปลอดภัยอย่างไร เพื่อหาวิธีที่จะหลบเลี่ยงระบบรักษาความปลอดภัย

5.5 การใช้งานบนสื่ออินเทอร์เน็ต ต้องพึงระมัดระวังการบริโภคข้อมูลข่าวสาร เนื่องจากอาจเกิดการปั่นกระแสข้อมูล ทำให้เกิดการหลงเชื่อข้อมูลแบบผิดๆ ที่เรียกว่า Search Engine Optimizer (SEO) ได้