# ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตน สำหรับข้าราชการยุคดิจิทัล

โดย นางสาววิภารัตน์ นิลสนธิ
นักวิชาการแผนที่ภาพถ่ายปฏิบัติการ

## วัตถุประสงค์

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในยุคดิจิทัล

๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง เพื่อให้ปลอดภัยจากภัยคุกคาม

๓. เพื่อให้สามารถยกตัวอย่างภัยคุกคามต่าง ๆ ได้

๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

## สรุปเนื้อหา

### แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย

การเติบโตของอินเทอร์เน็ตในประเทศไทยมีเปอร์เซ็นต์ค่อนข้างสูง ปี ๒๐๐๐ จากที่ใช้งานอยู่ที่ ๓.๗% แต่ปี ๒๐๑๐ ได้เพิ่มเป็น ๒๖.๓๐% โดยเพิ่มเกือบประมาณ ๙ เท่า ทำให้เห็นได้ว่าการเติบโตการใช้อินเทอร์เน็ตเพิ่มขึ้น ผู้ใช้งานอินเทอร์เน็ต คือ ๑/๓ ของคนทั้งประเทศ โดยปัจจุบันแนวโน้มการใช้งานจะเป็นในรูปแบบสื่อสังคมออนไลน์ หรือโซเชียลมีเดีย ทำให้ความสัมพันธ์และการกระจายตัวของข้อมูลเป็นไปอย่างรวดเร็วและรุนแรง รวมทั้งรูปแบบของเว็บไซต์ก็มีการเปลี่ยนแปลงไปตามวิวัฒนาการของเว็บไซต์ จึงจำเป็นต้องออกแบบให้สามารถรองรับการแสดงผลผ่านหน้าจอของ Smart Phone หรือ Tablet แต่ละรุ่น รวมไปถึงระบบปฏิบัติการ และแอปพลิเคชันต่าง ๆ อีกด้วย

### วิวัฒนาการของเว็บไซต์

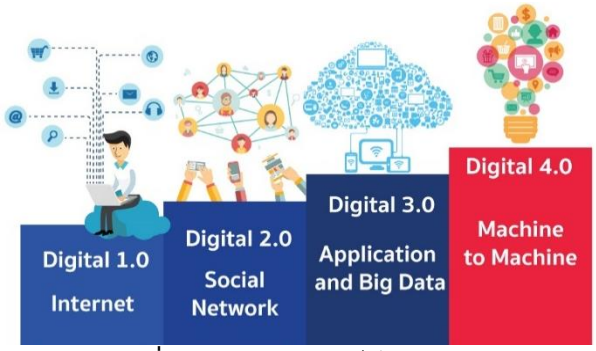
วิวัฒนาการของเว็บไซต์ แบ่งเป็น ๔ ยุค ได้แก่

ยุค Web ๑.๐ การให้บริการเว็บไซต์ในรูปแบบการสื่อสารทางเดียว (One Way Communication) โดยให้ผู้พัฒนา หรือผู้ที่สร้างเว็บไซต์นั้น ติดต่อสื่อสาร สร้างเนื้อหาได้เพียงคนเดียว ผู้เข้าถึงเว็บไซต์สามารถเข้าไปรับชมเนื้อหาได้เพียงอย่างเดียวเท่านั้น

ยุค Web ๒.๐ การใช้งานเครือข่ายอินเทอร์เน็ตในรูปแบบสองทาง (Two Way Communication) เปิดโอกาสให้ผู้ใช้งานสามารถโต้ตอบกันได้ จำพวก Webboard หรือ Platform เช่น Facebook Youtube Wikipedia ที่เปิดโอกาสให้ผู้ใช้งานเข้ามาสร้างเนื้อหาและทำให้เกิด Big Data

ยุค Web ๓.๐ เป็นช่วงรอยต่อจาก Web ๒.๐ ที่นำข้อมูล Big Data มาวิเคราะห์และให้คำแนะนำกับผู้ใช้งานได้ มีการเชื่อมโยงข้อมูลที่หลากหลาย

ยุค Web ๔.๐ Symbiotic Web เป็นยุคของเว็บไซต์ที่มีลักษณะการเรียนรู้พฤติกรรมของมนุษย์ สามารถให้คำแนะนำผู้ใช้งานได้ดีกว่ายุค Web ๓.๐ และระบบมีแนวโน้มสามารถชักจูงให้คล้อยตามได้




**รูปที่ ๑** วิวัฒนาการของเว็บไซต์ ๔ ยุค
ที่มา : https://www.wice.co.th/๒๐๑๘/๐๑/๑๑/digital-๔-๐-technology/

## รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

**ประเภทของผู้กระทำความผิด**

Hacker คือ คนที่มีความสนใจจะศึกษาระบบเครือข่ายคอมพิวเตอร์ เพื่อนำมาแชร์ต่อ

Cracker คือ Hacker ที่มีความรู้ ความสามารถ ที่นำความรู้ไปใช้ในทางที่ผิด

Script Kiddy คือ คนที่นำเครื่องมือ โปรแกรม หรือช่องโหว่ มาทดลองให้เกิดความเสียหายบนเครือข่ายอินเทอร์เน็ต

Spy คือ สายลับ ที่อาจจะนำข้อมูลหรือความลับของระบบออกไปเผยแพร่ให้เกิดความเสียหาย

Employee คือ เจ้าหน้าที่ในองค์กรที่เข้าสู่ระบบได้ทำการเผยแพร่ระบบรักษาความปลอดภัยออกไป

Terrorist คือ กลุ่มก่อการร้าย มีจุดมุ่งหมายก่อความไม่สงบบนเครือข่ายอินเทอร์เน็ต

**รูปแบบของการกระทำความผิด**

Social Engineering เป็นปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

Password Guessing การเดา Password เพื่อเข้าสู่ระบบ

Denial of Service (DOS) การโจมตีที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบ และการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

Decryption การถอดข้อมูลที่มีการเข้ารหัสอยู่

Man in the middle Attacks การพยายามที่จะทำตัวเป็นกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

Phishing การปลอมแปลงเว็บไซต์ทำให้ผู้เข้าใช้งานเข้าใจว่าเป็นเว็บไซต์จริง

## พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับเดิม คือ พ.ศ. ๒๕๕๐ ปัจจุบันได้มีการแก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐ และได้ประกาศใช้แล้ว

ตัวอย่างการใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิดที่มีความผิดทางกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การใช้โปรแกรมในการแก้ไขค่าในเกม เพื่ออำนวยความสะดวกในการเล่นเกม แต่การกระทำเช่นนี้เป็นการรบกวนการประมวลผลของเครือข่ายคอมพิวเตอร์ หรือการโพสต์ การแชร์ข้อมูลหรือรูปภาพ เช่น การใช้สารเสพติด การทำร้ายร่างกายผ่านทางอินเทอร์เน็ต ทำให้เกิดพฤติกรรมเลียนแบบ และเกิดความเสียหายต่อสังคมเป็นวงกว้าง

**การตั้งค่าความปลอดภัยสำหรับ Social Media**

การตั้งค่าความปลอดภัยสำหรับ Social Media เช่น Facebook Line หรือ Gmail สิ่งแรกที่ควรทำก็คือ การตั้งค่ารหัสผ่าน ซึ่งกฎเพื่อความปลอดภัยในการตั้งรหัสผ่าน คือ

๑. ไม่ควรตั้งเป็นหมายเลขโทรศัพท์

๒. ไม่ควรตั้งเป็นวันเกิดตัวเองหรือคนใกล้ชิด

๓. ไม่ควรตั้งเป็นชื่อตัวเอง ชื่อเล่น หรือชื่อที่ใช้ในการตั้ง User

๔. ไม่ควรตั้งเป็นชุดตัวเลข หรืออักษรที่เดาได้ง่าย เช่น ๑๒๓๔ abcd

**การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน**

ทำให้เกิดความรู้ ความเข้าใจ และระมัดระวังการใช้งานคอมพิวเตอร์ของหน่วยงาน ในเรื่องการเข้าถึงเว็บไซต์ ให้สังเกต URL หรือความผิดปกติของเว็บไซต์ก่อนการคลิกลิงก์ หรือไฟล์ เพื่อป้องกันการโจมตีจากไวรัสหรือ Hacker ที่แฝงมาในรูปแบบต่าง ๆ และการกระทำที่สุ่มเสี่ยงต่อความผิด พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมไปถึงการตั้งค่ารหัสผ่าน เพื่อความปลอดภัยของข้อมูลภายในหน่วยงาน

**ประโยชน์ที่ได้รับ**

- ต่อตนเอง สามารถตั้งรหัสผ่าน Social Media ของตัวเองได้อย่างปลอดภัย และระมัดระวังในการเข้าใช้งานเว็บไซต์ เพื่อป้องกันการโจมตีของไวรัส รวมทั้งไม่แชร์หรือโพสต์ข้อมูลที่ไม่ถูกต้องที่จะทำให้เกิดความเข้าใจผิด

- ต่อองค์กร มีความระมัดระวังการเข้าถึงเว็บไซต์ต่าง ๆ ด้วยคอมพิวเตอร์ของหน่วยงาน ทำให้คอมพิวเตอร์ไม่ถูกโจมตีด้วยไวรัส และข้อมูลภายในหน่วยงานมีความปลอดภัย

- ต่อสาธารณะ ไม่แชร์หรือโพสต์ข้อมูลที่จะทำให้เกิดความเข้าใจผิด หรือเสียหายเป็นวงกว้างในสังคม

**แหล่งที่มา**

**หลักสูตร :** ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตน สำหรับข้าราชการยุคดิจิทัล
**บรรยายโดย :** อาจารย์ณัฐ พยงค์ศรี นักวิชาการคอมพิวเตอร์
**สถาบัน/หน่วยงาน/ระบบ :** สำนักงาน ก.พ.
**รูปแบบหลักสูตร :** e-Learning
**ช่วงเวลาการฝึกอบรม :** สิงหาคม ๒๕๖๗