**<u>การอบรมทางไกลด้วยระบบอิเล็กทรอนิกส์ (HRD:e-learning) ของ ก.พ.</u>**

**<u>วิชาความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล</u>**

ปัจจุบันหน่วยงานราชการทั่วโลก กำลังเผชิญกับภัยไซเบอร์ในรูปแบบต่างๆ ซึ่งเป็นภัยคุกคามอันใหญ่หลวง ทั้งทางเศรษฐกิจ สังคม และความมั่นคงของประเทศ ข้าราชการและบุคลากรภาครัฐจะต้องเรียนรู้เรื่องความมั่นคง ปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล ซึ่งการรักษาความมั่นคงปลอดภัยบนอินเทอร์เน็ตเป็นการสร้างภูมิคุ้มกันเบื้องต้น และการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นกับการใช้งานเทคโนโลยีสารสนเทศและอินเทอร์เน็ต ซึ่งข้าราชการในยุคดิจิทัลควรมีความรู้ความเข้าใจเกี่ยวกับเรื่องความปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนได้อย่างถูกต้อง

**แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัย**

๑. เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกัน หรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมต่างๆ หรือช่องทางสังคมออนไลน์ (Social Media) เพื่อหลีกเลี่ยงการติดซอฟต์แวร์ที่เป็นอันตราย (Malware)

๒. การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ หรือตั้งรหัสที่ง่ายต่อการคาดเดา เช่น วัน เดือน ปี เกิด ตัวเลขที่เรียงกัน ตัวพยัญชนะเรียงกัน เป็นต้น เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่นๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

๓. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อ ตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

**กฎหมายที่ใช้กับการกระทำความผิดทางคอมพิวเตอร์**

การที่เจาะเข้าระบบคอมพิวเตอร์ของผู้อื่น การแอบดูข้อมูลอื่น การลบ แก้ไข เพิ่มเติมข้อมูลส่วนตัวของผู้อื่นนั้น เป็นสิ่งผิดกฎหมายทั้งสิ้น ความรับผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ พ.ศ.๒๕๕๐ และ พ.ศ.๒๕๖๐ ที่แก้ไขเพิ่มเติม ดังนี้

๑. เป็นการกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์ ได้แก่

- การกระทำความผิดตามมาตรา ๕ คือ การเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันโดยมิชอบ การเข้าถึงนั้นไม่จำกัดว่าเข้าถึงในระดับใด ทั้งระดับกายภาพ หรือผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมา และสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

- การกระทำความผิดตามมาตรา ๖ คือ การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไม่ว่าการรู้ถึงมาตรการป้องกันนั้นจะได้มาโดยมิชอบหรือไม่ก็ตาม และนำมาตรการดังกล่าวไปเปิดเผยทำให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

/การกระทำ...

- การกระทำความผิดตามมาตรา ๑๐ คือ การขัดขวางการทำงานของระบบคอมพิวเตอร์จนไม่สามารถทำงานได้ตามปกติต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

๒. เป็นการกระทำความผิดที่มีวัตถุประสงค์ต่อข้อมูลของคอมพิวเตอร์ ได้แก่

- การกระทำความผิดตามมาตรา ๗ คือ การเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการป้องกันไว้เป็นพิเศษโดยมิชอบ ซึ่งการเข้าถึง วิธีการเข้าถึง ตลอดจนช่องทางในการเข้าถึงนั้นมีส่วนคล้ายกับความผิดตามมาตรา ๕ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

- การกระทำความผิดตามมาตรา ๘ คือ การดักรับข้อมูลที่อยู่ระหว่างการรับส่งในระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

- การกระทำความผิดตามมาตรา ๙ คือ การแก้ไข เปลี่ยนแปลง หรือเพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ไม่ว่าจะเป็นการแก้ไข เปลี่ยนแปลง หรือเพิ่มเติมทั้งหมด หรือบางส่วนก็ตาม และผู้แก้ไขนั้นไม่มีสิทธิ์แก้ไข ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

- การกระทำความผิดตามมาตรา ๑๑ คือ การส่งข้อมูล หรืออีเมลให้ผู้อื่นโดยไม่เปิดเผยแหล่งที่มาของข้อมูล โดยทำให้ผู้ที่รับข้อมูลนั้นเกิดความรำคาญ หรือรบกวนผู้อื่น การกระทำนี้ในปัจจุบันเราเรียกการกระทำนี้ว่า Spam Mail (อีเมลขยะ) ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

๓. เป็นการกระทำความผิดที่มีวัตถุประสงค์ต่อบุคคล ได้แก่

- การกระทำความผิดตามมาตรา ๑๒ คือ เป็นลักษณะกฎหมายที่มุ่งคุ้มครองผู้ที่ถูกรบกวนตามมาตรา ๙ หรือมาตรา ๑๐ โดยมีลักษณะเป็นการเพิ่มโทษ ถ้าเป็นความเสียหายเกิดขึ้นกับบุคคล จะเพิ่มโทษเป็นโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท และถ้าเป็นความเสียหายที่เกิดขึ้นต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในการเศรษฐกิจของประเทศ หรือการบริการสาธารณะ จะเพิ่มโทษเป็นจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

- การกระทำความผิดตามมาตรา ๑๔ คือ เป็นการนำข้อมูลปลอม หรือข้อมูลอันเป็นเท็จ หรือข้อมูลที่มีลักษณะเป็นอันลามก เข้าสู่ระบบ แล้วทำให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (ประเทศไทยมีผู้กระทำความผิดมากที่สุด)

- การกระทำความผิดตามมาตรา ๑๖ คือ การนำภาพของผู้อื่น และภาพที่เกิดจากการสร้างขึ้นเข้าสู่ระบบคอมพิวเตอร์ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ แต่ถ้าเป็นการนำเข้าโดยสุจริต ผู้กระทำไม่มีความผิด และความผิดตามมาตรานี้ยอมความได้ (เป็นมาตราเดียวที่ยอมความได้)

**ประโยชน์ที่ได้รับจากการศึกษาหลักสูตรนี้**

๑. สามารถนำเทคโนโลยีดิจิทัลที่ทันสมัยมาใช้ประโยชน์ได้อย่างถูกต้อง เหมาะสม และปลอดภัยในการปฏิบัติงาน

๒. เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่ได้ตกลงกันหรือไม่รู้จักกันมาก่อน เพื่อหลีกเลี่ยงการติดซอฟต์แวร์ที่เป็นอันตราย (Malware)

/๓.ทำให้รู้...

๓. ทำให้รู้ว่าการใช้บริการอินเทอร์เน็ตไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือง่ายต่อการคาดเดา เช่น รหัสที่เป็น วัน เดือน ปีเกิด รหัสตัวเลขที่เรียงลำดับ หรือรหัสตัวอักษรที่เรียงกัน เพื่อป้องกันการเจาะระบบ เช่น การตั้งรหัสผ่านในการเข้าระบบสารสนเทศทรัพยากรส่วนบุคคล (DPIS) ไม่ควรตั้งค่าให้โปรแกรมที่ใช้ในการเข้าถึงข้อมูลและติดต่อสื่อสาร (Web Browser) จำรหัสผ่าน ควรใส่รหัสเองของทุกครั้ง เป็นต้น

๔. ทำให้รู้ว่าไม่ควรใช้อินเทอร์เน็ตสาธารณะ เช่น ร้านค้า หรือโรงแรม เพราะจะทำให้เสี่ยงต่อการแฮกเกอร์เจาะระบบสำเร็จได้ง่าย

---

นางธรณ์ธันย์ บุญแก้ว
นักทรัพยากรบุคคลชำนาญการ
กลุ่มทะเบียนประวัติและบำเหน็จความชอบ
กองการเจ้าหน้าที่
มีนาคม ๒๕๖๔