แบบรายงานผลการพัฒนาความรู้ของข้าราชการ
สถานีพัฒนาที่ดินปราจีนบุรี สำนักงานพัฒนาที่ดินเขต ๒ กรมพัฒนาที่ดิน
รอบการประเมินที่ ๑/๒๕๖๙ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ ถึงวันที่ ๓๑ มีนาคม ๒๕๖๙
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ - นามสกุล นางสาวปติมา คำกองแก้ว **ตำแหน่ง** เจ้าพนักงานธุรการชำนาญงาน
หน่วยงาน ฝ่ายบริหารทั่วไป สถานีพัฒนาที่ดินปราจีนบุรี สำนักงานพัฒนาที่ดินเขต ๒ กรมพัฒนาที่ดิน
หัวข้อการพัฒนา "ความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน"
วิธีการพัฒนา การฝึกอบรมพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์ (HRD e – Learning)
วันที่ ๓๑ มกราคม ๒๕๖๙
หน่วยงานที่จัดอบรม สำนักงานข้าราชการพลเรือน (ก.พ.)
วัตถุประสงค์

๑. บุคลากรมีความเข้าใจและตระหนักรู้ถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์
๒. บุคลากรมีการเตรียมความพร้อมในปฏิบัติงานทางด้านความปลอดภัยทางไซเบอร์
๓. สามารถประยุกต์ใช้เทคโนโลยีในกระบวนการทางาน เพื่อลดขั้นตอนและเพิ่มประสิทธิภาพในการทำงาน

สรุปสาระสำคัญ

ความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน (Basic Cybersecurity) คือแนวปฏิบัติเพื่อปกป้องอุปกรณ์ ข้อมูล และเครือข่ายจากการโจมตีทางดิจิทัล โดยเน้นการสร้างรหัสผ่านที่แข็งแกร่งและไม่ซ้ำกันการอัปเดตซอฟต์แวร์สม่ำเสมอ การใช้ การยืนยันตัวตนแบบหลายปัจจัย (MFA) และความระมัดระวังในการใช้งานอินเทอร์เน็ต เพื่อป้องกันภัยคุกคาม เช่น แรนซัมแวร์และการตกเป็นเหยื่อของการหลอกลวง

ความหมายความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน

National Cyber Security Centre (NCSC หรือศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร) ให้ความหมายของความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ไว้กว้าง ๆ ว่าคือ "วิธีที่บุคคลหรือหน่วยงานทำเพื่อลดความเสียงต่อการถูกโจมตีทางไซเบอร์" ในขณะที่ Cybersecurity & Infrastructure Security Agency (หน่วยงานความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของสหรัฐอเมริกา) ให้คำนิยามไว้ว่า "ศิลปะในการป้องกันเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ทางอาชญากรรม และการทำให้มั่นใจว่าข้อมูล (information) ได้รับการรักษาความลับ (confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)"

สำหรับประเทศไทย เรามีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่ให้ความหมาย "การรักษาความมั่นคงปลอดภัยไซเบอร์" ไว้หมายความว่า "มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ"

ทำไมต้องมีความมั่นคงปลอดภัยไซเบอร์ ปัจจุบันเราใช้ชีวิตเชื่อมโยงกับอินเทอร์เน็ตในหลากหลายมิติมาก โดยจากผลสำรวจพฤติกรรมการใช้อินเทอร์เน็ตของประเทศไทยในปี ๒๕๖๓ ของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมคนไทยใช้อินเทอร์เน็ตในการทำกิจกรรมมากมาย ตั้งแต่การทำธุรกรรมออนไลน์ (๕๖.๕%) การซื้อของ (๖๗.๓%) การหาข้อมูล (๘๒.๒%) การติดต่อสื่อสาร (๗๗.๘%) ความบันเทิง (ดูหนัง/คลิป/โทรทัศน์/ฟังเพลง ที่ ๘๕%)

ทั้งหมดนี้ หากการรักษาความมั่นคงปลอดภัยไซเบอร์อ่อนแอก็อาจทำให้ผู้ประสงค์ร้ายเข้ามาทำอันตรายต่อเราและข้อมูลส่วนบุคคลของเราได้ ตั้งแต่การเข้าถึงข้อมูลส่วนบุคคลของเราที่เราไม่ได้ตั้งใจจะเปิดเผย เช่น เพศวิถี อายุ สัญชาติ ศาสนา จนอาจนำไปสู่การขโมยข้อมูลของเราไปใช้ อาทิ รหัสบัตร ATM ข้อมูลบัตรเครดิต การสวมรอยเป็นเรา ไปจนถึงการเรียกค่าไถ่เพื่อแลกกับการไม่เปิดเผยข้อมูลของเรา

ประเภทของภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ที่สามารถเข้าถึงข้อมูลของเราสามารถทำให้เกิดอันตรายได้หลายรูปแบบมาก โดยสามารถแบ่งออกได้ดังนี้

๑. Malware มาจากคำว่า Malicious + Software ที่แปลว่า ที่ประสงค์ร้าย + ซอฟต์แวร์ (ซอฟต์แวร์ที่ประสงค์ร้าย) ซึ่งเป็นซอฟต์แวร์ที่สร้างขึ้นเพื่อรบกวนหรือทำให้เกิดความเสียหาย เช่น ไวรัสคอมพิวเตอร์ (Virus) ที่สามารถคัดลอกโปรแกรมของตัวเองให้ไปติดกับไฟล์อื่น ๆ ในเครื่องคอมพิวเตอร์ได้ Trojans (โทรจัน) ที่สามารถสร้างความเสียหายหรือเก็บข้อมูลของเรา Spyware ที่แอบเก็บข้อมูลสำคัญของเรา Ransomware หรือมัลแวร์เรียกค่าไถ่ ที่จะปิดกั้นไม่ให้เราเข้าไปใช้งานไฟล์หรือข้อมูลจนกว่าจะจ่ายค่าไถ่ เป็นต้น

๒. Phishing เป็นการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายด้านอื่น ๆ

๓. การโจมตีด้วยการแทรกกลาง (Man-in-the-middle attack) เป็นการจู่โจมระหว่างโหนด (Node) การสื่อสารของอุปกรณ์ เพื่อดักจับข้อความหรือข้อมูลระหว่างผู้ส่งและผู้รับข้อมูล ลองนึกภาพว่าเรากำลังส่งน้ำไหลไปตามท่อ แต่มีคนมาดักตรงกลางเพื่อเอาน้ำไป

๔. การโจมตีด้วยการปฏิเสธการให้บริการ (Denial-of-service attack) เป็นการจู่โจมที่ผู้ประสงค์ร้ายเข้าควบคุมอุปกรณ์เครือข่าย หรือเซิร์ฟเวอร์ไม่ให้ทำงาน ซึ่งหากเป็นระบบโรงพยาบาลหรือหน่วยงานด้านพลังงานก็จะก่อให้เกิดความเสียหายต่อชีวิตและทรัพย์สินมหาศาล

หลักปฏิบัติพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

๑. การจัดการรหัสผ่าน (Password Management) ใช้รหัสผ่านที่ซับซ้อน (ตัวอักษรเล็ก-ใหญ่, ตัวเลข, อักขระพิเศษ) ยาวไม่น้อยกว่า ๘ ตัวอักษร และไม่ใช้รหัสผ่านเดียวกันในทุกบัญชี

๒. การยืนยันตัวตนแบบหลายปัจจัย (MFA/๒FA) เปิดใช้งานการยืนยันตัวตนหลายชั้น เช่น รหัสผ่านร่วมกับ OTP เพื่อเพิ่มความปลอดภัย

๓. อัปเดตระบบและซอฟต์แวร์ (Patch Update) อัปเดตระบบปฏิบัติการ (OS), แอปพลิเคชัน, และโปรแกรมแอนตี้ไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ความปลอดภัย

๔. การสำรองข้อมูล (Data Backup) สำรองข้อมูลสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการสูญหายจากแรนซัมแวร์หรืออุปกรณ์เสียหาย

๕. ความตระหนักรู้ (Security Awareness) ระวังการคลิกลิงก์หรือเปิดไฟล์แนบที่ไม่รู้จัก ป้องกันการตกเป็นเหยื่อของ Phishing (การปลอมแปลงอีเมล/SMS)

๖. การรักษาความปลอดภัยเครือข่าย (Network Security) เปลี่ยนรหัสผ่านเริ่มต้น (Default Password) ของ Router และระมัดระวังการใช้ Free Wi-Fi

วิธีการป้องกันพื้นฐาน

Cybersecurity & Infrastructure Security Agency ได้ให้คำแนะนำพื้นฐานเอาไว้ ดังนี้

๑. อัปเดตซอฟต์แวร์อย่างสม่ำเสมอ ซึ่งในหลายโปรแกรมอาจมีช่องโหว่หรือถูกค้นพบช่องโหว่ในภายหลังจากที่เราซื้อมา เมื่อผู้ผลิตและพัฒนาค้นพบก็จะออกตัวอัปเดตออกมาให้เราทำให้โปรแกรมสามารถปิดช่องโหว่ดังกล่าวได้

๒. ใช้งานโปรแกรม Antivirus ที่ได้รับการอัปเดตอย่างสม่ำเสมอ เพราะเวอร์ชันเดิมอาจจะไม่รู้จักกับ Malware ใหม่ ๆ

๓. สร้างรหัสผ่านที่เข้มแข็ง โดย ETDA ได้เคยจัดทำและให้คำแนะนำเอาไว้คือ ไม่ใช่ซ้ำกันทุกบัญชี ความยาวไม่น้อยกว่า ๘ ตัวอักษรและทำให้ซับซ้อนด้วยเลขหรืออักขระพิเศษ

๔. เปลี่ยนรหัสผ่านเริ่มต้น เมื่อเราสมัครบัญชีใช้งานในแพลตฟอร์มหรือบริการต่าง ๆ เราอาจจะได้รับรหัสผ่านเริ่มต้นมา ซึ่งเราควรเปลี่ยนรหัสผ่านนั้น โดยใช้วิธีการในข้อข้างบน

๕. ใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication หรือ MFA) ซึ่งนอกจากการแนะนำการสร้างรหัสผ่านที่เข้มแข็งแล้ว เรายังควรเปิดใช้งานการยืนยันตัวตนหลากหลายวิธี เช่น ใช้การใส่รหัสผ่านร่วมกับ OTP (One Time Password หรือรหัสผ่านแบบใช้ครั้งเดียว โดยมากจะเห็นจากการส่งรหัสตัวเลขใช้ครั้งเดียวและมีจำกัดเวลาไปทางข้อความสั้น (Short Message Service) ทางโทรศัพท์มือถือ)

๖. ติดตั้ง Firewall ในอุปกรณ์ ซึ่งจะเป็นกำแพงกั้นไม่ให้โปรแกรมหรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตเข้ามาหรือทำงานในอุปกรณ์ของเรา

๗. คิดก่อนเปิด (Be suspicious of unexpected emails) เมื่อได้รับ Email เราควรคิดก่อนจะกดลิงก์ (Link) ที่ส่งมาด้วย เพราะอาจทำให้เราดาวน์โหลด Malware เข้ามาในเครื่องโดยไม่รู้ตัว ซึ่งรวมถึงข้อความสั้นทางโทรศัพท์ และข้อความจากโปรแกรมแชทด้วย

ประโยชน์ที่ได้รับ

๑. การป้องกันตนเองและข้อมูล เข้าใจวิธีการป้องกันการถูกโจรกรรมข้อมูลส่วนบุคคล ข้อมูลทางการเงิน และบัญชีออนไลน์จากการใช้งานโซเชียลแอปพลิเคชันอย่างปลอดภัย

๒. ลดความเสี่ยงต่อองค์กร มีความเข้าใจสามารถสังเกตและรายงานกิจกรรมที่น่าสงสัยได้อย่างทันท่วงที ช่วยลดโอกาสที่องค์กรจะถูกโจมตีทางไซเบอร์

๓. สร้างความตระหนักรู้ (Cybersecurity Awareness) ตระหนักถึงความเสี่ยง เข้าใจรูปแบบภัยคุกคามและรู้วิธีป้องกันตัวเอง

๔. ลดค่าใช้จ่ายจากการถูกโจมตี ลดความเสี่ยงในการสูญเสียทรัพย์สิน การกู้คืนข้อมูล และความเสียหายต่อชื่อเสียง ทั้งต่อตนเองและองค์กร

๕. เข้าใจกฎหมาย มีความเข้าใจเบื้องต้นเกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ และข้อบังคับการคุ้มครองข้อมูลส่วนบุคคล (PDPA/GDPR)

(ลงนาม).....

(นางสาวปติมา คำกองแก้ว)

ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน

(ลงนาม).....

(นางสาววรารัตน์ ลิ่วรางกุล)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินปราจีนบุรี

ความมั่นคงปลอดภัยไซเบอร์ ระดับพื้นฐาน

(Basic Cybersecurity)

ความหมาย

แนวปฏิบัติเพื่อปกป้องอุปกรณ์ ข้อมูล และเครือข่าย จากการโจมตีทางดิจิทัล สร้างเกราะป้องกันภัยคุกคาม เช่น แรนซัมแวร์, การหลอกลวง (Phishing)

- รหัสผ่านแข็งแกร่ง ไม่ซ้ำกัน
- อัปเดตซอฟต์แวร์ สม่ำเสมอ
- ยืนยันตัวตน หลายปัจจัย (MFA)
- ใช้งานอินเทอร์เน็ต อย่างระมัดระวัง

ประเภทภัยคุกคามทางไซเบอร์

Malware
- ไวรัส, โทรจัน, สปายแวร์, แรนซัมแวร์

Phishing
- อีเมล/เว็บไซต์ปลอม หลอกเอาข้อมูล

Man-in-the-Middle
- ดักจับข้อมูลระหว่างการสื่อสาร

Denial-of-Service (DoS)
- โจมตีจนระบบล่ม ไม่สามารถใช้งานได้

หลักปฏิบัติพื้นฐานด้านความปลอดภัย

- **การจัดการรหัสผ่าน** ใช้รหัสผ่านที่ยากและไม่ซ้ำ
- **การยืนยันตัวตน** แบบหลายปัจจัย (MFA/2FA)
- **อัปเดตระบบ และซอฟต์แวร์**
- **การสำรองข้อมูล** (Data Backup)
- **ความตระหนักรู้** ระวังลิงก์ & ไฟล์แนบ
- **การรักษาความปลอดภัย เครือข่าย** (Network Security)

วิธีการป้องกันพื้นฐาน

- อัปเดตซอฟต์แวร์อย่างสม่ำเสมอ
- ใช้โปรแกรม Antivirus ให้เป็นปัจจุบัน
- สร้างรหัสผ่านที่เข้มแข็ง (≥ 8 ตัวอักษร)
- เปลี่ยนรหัสผ่านเริ่มต้น (Default Password)
- เปิดใช้งาน MFA / OTP
- ติดตั้ง Firewall ในอุปกรณ์
- คิดก่อนคลิก ลิงก์หรือไฟล์แนบที่ไม่รู้จัก

ประโยชน์ที่ได้รับ

- **ป้องกันตนเอง** และข้อมูลสำคัญ
- **ลดความเสี่ยง** ต่อองค์กร
- **สร้างความ ตระหนักรู้**
- **ลดความเสียหาย** ทางการเงิน | พ.ร.บ.คอมพิวเตอร์

สรุปโดย: นางสาวปติมา คำกองแก้ว

เจ้าพนักงานธุรการชำนาญงาน | สถานีพัฒนาที่ดินปราจีนบุรี