บันทึกข้อความ

ส่วนราชการ ฝ่ายบริหารทั่วไป กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๑๘๘

ที่ กษ ๐๘๓๗.๐๑ / ๘๒ **วันที่** ๙ กุมภาพันธ์ ๒๕๖๖

เรื่อง รายงานการพัฒนาความรู้ข้าราชการ จำนวน ๒ เรื่อง

เรียน ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

ตามที่ กองนโยบายและแผนการใช้ที่ดิน ได้กำหนดตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร การประเมินรอบที่ ๑ (ตุลาคม ๒๕๖๕ - มีนาคม ๒๕๖๖) ในมิติพัฒนาองค์การ ให้ข้าราชการพัฒนาทักษะด้านดิจิทัล ๑ หลักสูตร และหลักสูตรอื่นๆ อย่างน้อย ๑ หลักสูตร พร้อมทั้งสรุปบทเรียนมาอย่างน้อย ๑ หลักสูตร นั้น

บัดนี้ ข้าพเจ้า ได้เข้ารับการพัฒนาการเรียนรู้ ๒ หลักสูตร เรียบร้อยแล้ว ประกอบด้วย

๑. หลักสูตร “การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” รุ่นที่ ๒
หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

๒. หลักสูตร “STRONG : จิตพอเพียงต้านทุจริต”
หน่วยงาน กองการเจ้าหน้าที่ กรมพัฒนาที่ดิน

ทั้งนี้ได้จัดทำรายงานสรุปบทเรียน รายละเอียดตามเอกสารแนบ

จึงเรียนมาเพื่อโปรดทราบ

(นางลักษิกา ไชยศิลป์)
เจ้าพนักงานธุรการปฏิบัติงาน

(นางสาวจตุพร เพชรนุ้ย)
เจ้าพนักงานธุรการอาวุโส
หัวหน้าฝ่ายบริหารทั่วไป

ลงนามแล้ว
- ๗ ก.พ. ๒๕๖๖

(นางสาวพิมพิลัย นวลละออง)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร
รักษาราชการแทน ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
- ๙ ก.พ. ๒๕๖๖

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร

กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ-นามสกุล นางลักษิกา ไชยศิลป์
ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน **ฝ่าย** บริหารทั่วไป

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ :
หลักสูตร การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รุ่นที่ 2

สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ :
ห้องปฏิบัติการฝึกอบรมคอมพิวเตอร์และภูมิสารสนเทศ กรมพัฒนาที่ดิน

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ :
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ตั้งแต่วันที่ 2 เดือน กุมภาพันธ์ พ.ศ. 2566 **ถึงวันที่** 2 เดือน กุมภาพันธ์ พ.ศ. 2566

เพื่อ ☑ **อบรม** ☐ **สัมมนา** ☐ **อื่นๆ ระบุ**.....

ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

ความปลอดภัยทางไซเบอร์ หมายถึง วิธีลดความเสี่ยงจากการโจมตีทางอินเทอร์เน็ตสำหรับองค์กร ผลกระทบที่เกิดขึ้นอาจส่งผลต่อการปฏิบัติงาน การปกป้องอุปกรณ์ และบริการที่ใช้ การโจมตีทางไซเบอร์นี้ไม่คำนึงถึงขนาดขององค์กร ความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์จึงเป็นสิ่งสำคัญอย่างยิ่งในการปกป้ององค์กร เนื่องจากมีความเสี่ยงที่จะถูกแฮกข้อมูล

ประเภทของการโจมตีด้วยการแฮกข้อมูล

การโจมตีทางไซเบอร์มีประเภทที่เป็นทั้งแบบเปิดเผยและแบบแอบแฝง ซึ่งทั้งสองแบบนี้ออกแบบมาเพื่อขัดขวางธุรกิจของบริษัทหรือองค์กรในรูปแบบอื่น ๆ เมื่อบริษัทหรือองค์กรต่าง ๆ เริ่มตระหนักถึงความสำคัญของการปกป้องทรัพยากร และการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ แฮกเกอร์และอาชญากรไซเบอร์ก็กำลังพัฒนารูปแบบการโจมตีที่ซับซ้อนมากขึ้นเรื่อย ๆ

การโจมตีทางไซเบอร์ที่พบบ่อยที่สุดมีอยู่ 5 ประเภท:

1. **มัลแวร์ (Malware)** เป็นช่องโหว่ที่สามารถทะลุการปกป้องเครือข่ายของคุณเช่น สปายแวร์ (spyware) ไวรรักเรียกค่าไถ่ (ransomware) และไวรัสคอมพิวเตอร์ (viruses)
2. **ฟิชชิ่ง (Phishing)** ข้อความเหล่านี้เป็นข้อความที่เป็นอันตราย (โดยส่วนมากที่พบคืออีเมล) ที่มีลิงก์ที่เป็นอันตราย ซึ่งเมื่อได้คลิกเข้าไปแล้ว จะทำการหลอกล่อให้คุณส่งข้อมูลที่ละเอียดอ่อนไปยังเป้าหมาย
3. **การปฏิเสธการให้บริการ (Denial of Service (DoS))** แฮกเกอร์มักทำการโจมตีเพื่อทำให้เครือข่าย หรือระบบของคุณ ที่มีข้อมูลส่วนเกิน จนล้นเครือข่าย และบังคับให้ระบบหยุดทำงาน
4. **เทคนิคคนกลาง (Man in the middle (MitM))** อาชญากรไซเบอร์ที่เข้ามาอยู่ระหว่างการเชื่อมต่อของคุณ ซึ่งมักจะกระทำผ่านเครือข่าย Wi-Fi สาธารณะที่ไม่ปลอดภัย และขโมยข้อมูลที่ละเอียดอ่อนของคุณไป
5. **การโจมตีแบบซีโร่เดย์ (Zero-day attack)** พบได้น้อย แต่มากขึ้นเรื่อย ๆ การโจมตีทั่วไปที่เกิดขึ้นระหว่างรอการประกาศการอัปเดตความปลอดภัย หรือโปรแกรมแก้ไข และการติดตั้งดังกล่าว

การโจมตีทางไซเบอร์เหล่านี้อาจส่งผลกระทบต่อองค์กรจำนวนมาก เช่น คาเฟ่ที่มีเครือข่าย Wi-Fi ที่ไม่ปลอดภัย หรือร้านค้าออนไลน์ที่เสี่ยงต่อการถูกโจมตีแบบ Zero-day เป็นต้น

การตรวจสอบอีเมลล์ที่เป็น Phishing Mail

การโจมตีด้วย Phishing email กระจายไปทั่วโลกทั้งแนบไฟล์อันตรายเพื่อหวังควบคุมระบบเครือข่ายหรือหลอกเอาข้อมูลส่วนตัวของผู้ใช้งาน ซึ่งไม่ว่ารูปแบบใดหากผู้ใช้งานมีความระมัดระวังและหมั่นสังเกตความแตกต่างระหว่างอีเมลหลอกลวงกับอีเมลจริงก็จะช่วยลดความเสี่ยงในการตกเป็นเหยื่อภัยคุกคามต่างๆ ได้ โดยวิธีสังเกต10 ข้อ ที่จะช่วยตรวจสอบอีเมลว่าเป็น Phishing email หรือไม่

1. มั่นใจว่าไม่เคยมีบัญชีออนไลน์ของเจ้านั้น ๆ ที่ส่งเมลล์มากรณีนี้ส่วนใหญ่ Phishing email จะแอบอ้างว่าบัญชีของเรามีปัญหาและเกิดข้อผิดพลาดจนไม่สามารถใช้งานกับเว็บไซต์ของบริษัท เช่น " โปรดอัปเดตบัญชี PayPal ของคุณ! ก่อนที่จะไม่สามารถใช้งานได้อีกต่อไป " หากเราไม่มีบัญชีดังกล่าวก็มั่นใจได้ว่านี่คือ Phishing email แน่นอน
2. อีเมลล์ที่ได้รับข้อความ ไม่ได้ใช้เป็นอีเมลที่เคยใช้ติดต่อกับบริษัทที่ส่งมา บางครั้งเราอาจจะได้รับอีเมลล์จากเว็บไซต์ที่เราสมัครใช้งาน ขอให้พิจารณาและตรวจสอบก่อนว่าอีเมลล์ที่รับเชื่อมโยงกับบริษัทนั้นหรือไม่ เราใช้อีเมลล์อื่นในการติดต่อหรือเปล่า เช่น ได้รับข้อความจาก PayPal ส่งเข้าอีเมลล์ abc1122@gmail.com แต่ที่จริงใช้ อีเมลล์ abc2222@gmail.com ในการสมัครใช้งาน PayPal นั่นแสดงว่าเป็น Phishing email แล้วแน่นอน
3. ที่อยู่อีเมลล์สำหรับตอบกลับดูผิดปกติ ข้อนี้มักจะถูกมองข้ามเสมอ ซึ่งหากตรวจสอบอย่างรอบคอบจะพบว่าสิ่งสำคัญที่จะบอกได้ว่าเมลล์นั้นเป็น Phishing email โดยให้สังเกตจากที่อยู่อีเมลล์ที่ได้รับหากเป็น PayPal จริงจะต้องเป็น @mail.paypal.com
4. อีเมลล์ที่ส่งมาเพื่อขอให้ยืนยัน Account หรือ ข้อมูลส่วนตัว ข้อความใน Phishing email มักจะหนีไม่พ้นเรื่องการให้อัปเดตข้อมูลหรือยืนยันข้อมูลส่วนตัว แม้จะดูน่าเชื่อถือแต่ถ้าทบทวนดีๆ จะพบว่าหลายหน่วยงานประกาศเตือนว่าไม่มีนโยบายขอข้อมูลส่วนตัวผ่านอีเมลอยู่เสมอ
5. เนื้อความอีเมลล์มีภาษาผิดหลักไวยากรณ์ เนื้อความใน Phishing email มักจะมีคำที่พิมพ์ผิดออกมาให้เห็น เช่น ใช้ภาษาไม่เป็นทางการ เลือกใช้คำไม่เหมาะสมมีรูปประโยคแปลก ๆ จนคาดเดาได้ว่าไม่ใช่อีเมลจากหน่วยงานอย่างแน่นอน เพราะองค์กรที่มีชื่อเสียงจะไม่ปล่อยอีเมลล์แบบนี้ออกมาแน่นอน
6. มีไฟล์แนบน่าสงสัย อีเมลล์ส่วนใหญ่จะมีไฟล์แนบเป็นลิงก์ให้กดเข้าไปอ่าน เมื่อกดแล้วจะเข้าสู่การดาวน์โหลดไฟล์อันตรายหรือเข้าไปที่เว็บไซต์ Phishing ซึ่งวิธีสังเกตคือให้ลองเอาเม้าส์ไปวางที่ลิงก์นั้นโดยไม่ต้องกด จะเห็นข้อความขึ้นเป็นเส้นทางลิงก์ปลายทาง
7. มีข้อความที่เขียนว่า "ด่วนมาก" เทคนิคที่แฮกเกอร์หลอกลวงคือการสร้างแรงกดดันให้ต้องจัดการอย่างใดอย่างหนึ่งในทันที เช่น อ้างว่าคุณไม่ได้ชำระเงินตามกำหนด, อ้างว่าคุณเป็นหนี้กับภาครัฐ, หรืออ้างว่าคุณถูกบันทึกภาพผ่านกล้องแล็ปท็อปของคุณ เป็นต้น
8. อีเมลล์ที่ไม่ได้ระบุชื่อผู้ใช้งาน ตอนทักทายประโยคแรก ลักษณะ Phishing email ทั่วไป ที่ไม่ได้เจาะจงโจมตีหน่วยงานใดหน่วยงานหนึ่งมักจะส่งอีเมลล์กระจายไปทั่ว โดยรอให้เหยื่อมากดคลิกลิงก์ซึ่งมักจะใช้คำขึ้นต้นประโยคทักทายเพื่อทักทายเป็นคำกว้าง ๆ เช่น Dear valued customer ถ้าเจอคำนี้แปลว่าเป็นอีเมลที่ไม่ได้จากต้นทางที่รู้จักเราหรือทำงานร่วมกับเรา จึงคาดเดาได้ว่าเป็น Phishing email
9. อีเมลล์ที่ส่งมาแค่ลิงค์อย่างเดียว ถ้าข้อความในอีเมลล์มาเป็นลิงค์หรือภาพใหญ่ ๆ ที่ลากเมาส์ไปตรงไหนก็เป็นไอคอนนิ้วมือกดแบบนี้เป็นสัญญาณว่าอีเมลล์อันตรายพยายามหลอกให้คลิกเมาส์สุ่มๆ ไปก็สามารถโหลดไวรัส หรือ มัลแวร์ได้แล้ว
10. เป็นอีเมลล์จากโดเมนสาธารณะ ถ้าได้รับอีเมลล์ที่อ้างว่ามาจากธุรกิจที่รู้จักแต่ที่อยู่อีเมลล์ใช้โดเมนสาธารณะ เช่น @gmail.com หรือ @outlook.com ให้สันนิษฐานว่าเป็นเมลล์อันตราย เพราะบริษัท ธุรกิจขนาดใหญ่หรือองค์กรที่มีชื่อเสียง จะต้องมีโดเมนเนมขององค์กรเสมอเพื่อความน่าเชื่อถือ

Cyber Security

Cyber Security เป็นเพียงกลยุทธ์ที่องค์กรใช้ในการปกป้องสินทรัพย์ดิจิทัลจากการแฮก การโจมตี การใช้งานกลยุทธ์ อาจรวมถึงเทคโนโลยี ขั้นตอนและมาตรการรักษาความปลอดภัยอื่น ๆ สำหรับระบบอุปกรณ์และข้อมูลได้รับการออกแบบมา เพื่อป้องกันการเข้าถึงข้อมูลที่เก็บไว้ในสื่อทางกายภาพหรือสื่อออนไลน์ โดยไม่ได้รับอนุญาต Cyber Security ไม่เหมือนกับการรักษาความปลอดภัยของข้อมูลซึ่งครอบคลุมพื้นที่ที่กว้างขึ้น รวมถึงทรัพย์สินข้อมูลทั้งหมด เช่น สำเนาเอกสารที่เป็นกระดาษ เป็นต้น

การรักษาความปลอดภัยทางไซเบอร์มีความสำคัญมากขึ้นเรื่อย ๆ เนื่องจากสมาร์ทโฟน คอมพิวเตอร์ และอุปกรณ์แท็บเล็ตนั้นล้วนเป็นส่วนสำคัญของงานและชีวิตส่วนตัวในแต่ละวัน ระดับของการพึ่งพาเครื่องมือออนไลน์ในแง่มุมต่างๆ ของการทำธุรกิจ ตั้งแต่โซเชียลมีเดีย และการตลาดผ่านอีเมลล์ ไปจนถึงองค์กรต่างๆที่ต้องการจัดเก็บข้อมูลพนักงาน และรายละเอียดต่างๆ

การพึ่งพาเครื่องมือดิจิทัล ทำให้หลายองค์กรมีความเสี่ยงจากการโจมตีทางไซเบอร์ ความรู้ที่มั่นคงเกี่ยวกับความปลอดภัยทางไซเบอร์เป็นสิ่งสำคัญ เนื่องจากการโจมตีดังกล่าวมีการพัฒนาอย่างต่อเนื่อง และมีความซับซ้อนมากขึ้น ผู้ที่ตกเป็นเหยื่อของการโจมตีทางไซเบอร์อาจเสี่ยงต่อการสูญเสีย ดังนี้

1.การสูญเสียข้อมูลที่ละเอียดอ่อน (Sensitive Data)

2.ความสูญเสียทางการเงิน อันเป็นผลพวงมาจากการโจรกรรม

3.ค่าใช้จ่ายที่สูงขึ้นในการกู้คืนข้อมูลที่ถูกขโมยไป

4.การสูญเสียชื่อเสียงที่ดี ขาดความเชื่อมั่น

5.การปิดกิจการ (ในกรณีร้ายแรง)

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

ลงชื่อ.....

(นางสาวพิมพิลัย นวลละออง)

ตำแหน่ง ผู้อำนวยการกลุ่มวางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร

รักษาราชการแทนผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ ๙ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๖