Received: May 21, 2020 **Revised:** Oct 26, 2020 **Accepted:** Nov 05, 2020

การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลองการโจมตีด้วยฟิชชิ่ง

CYBERSECURITY AWARENESS LEVEL IMPROVEMENT FOR EMPLOYEES IN AN ORGANIZATION : A CASE OF PHISHING ATTACK SIMULATION

สุรชัย ฉัตรเฉลิมพันธุ์[1], เทอดพงษ์ แดงสี[2]
[1]สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเอเชียอาคเนย์
[2]สาขาวิชาวิศวกรรมการจัดการอุตสาหกรรมเพื่อความยั่งยืน คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
Surachai Chatchalermpun[1] Therdpong Daengsi[2]
[1]Computer Engineering, Faculty of Engineering, Southeast Asia University
[2]Sustainable Industrial Management Engineer Faculty of Engineering
Rajamangala University of Technology Phra Nakhon
E-mail: therdpong.d@rmutp.ac.th

บทคัดย่อ

บทความนี้นำเสนอการศึกษาเพื่อยกระดับความตระหนักรู้ของบุคลากรภายในองค์กรแห่งหนึ่งเกี่ยวกับภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์โดยใช้การจำลองการโจมตีด้วยอีเมลฟิชชิ่ง หลังจากที่ได้มีรวบรวมข้อมูลจากบุคลากรจำนวน 482 คน แล้วทำการวิเคราะห์ด้วยสถิติพื้นฐาน พบว่า มีบุคลากรมากกว่า 22.41 % ที่เปิดอ่านอีเมลดังกล่าวและทำการคลิกลิงก์ที่อยู่ในอีเมล เพื่อยกระดับความตระหนักรู้เกี่ยวกับภัยทางไซเบอร์ซึ่งเป็นเรื่องที่สำคัญ จึงมีการจัดกระบวนการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากร หลังจากนั้นได้มีการจำลองการโจมตีด้วยฟิชชิ่งอีกครั้งด้วยเนื้อหาในอีเมลที่แตกต่างจากเดิม เมื่อได้รวบรวมข้อมูลจากบุคลากรกลุ่มเดิม แล้วทำการวิเคราะห์อีกครั้ง พบว่า มีบุคลากรน้อยกว่า 7.88 % ที่เปิดอ่านอีเมลดังกล่าวและทำการคลิกลิงก์ที่อยู่ในอีเมล ซึ่งลดลงประมาณ 64.81 % เมื่อเทียบกับผลการศึกษาในครั้งที่ 1 ทำให้ค่าระดับความความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ของบุคลากรในองค์กรเพิ่มสูงขึ้นเป็น 88.80 % นั่นแสดงว่ากระบวนการถ่ายทอดความรู้ที่ดำเนินการไปสามารถให้ผลลัพธ์ที่ดี ฉะนั้นการศึกษานี้จึงมีคุณค่าสำหรับนำไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ในองค์การอื่นและกับการโจมตีรูปแบบอื่นได้

คำสำคัญ: ฟิชชิ่ง ความตระหนักรู้ ความมั่นคงปลอดภัยทางไซเบอร์ การจำลองการโจมตี

Abstract

This article presents the study for enhancing cybersecurity awareness of the employees within an organization by using phishing attack simulation. After gathering data from 482 employees, the data were analyzed using descriptive statistics and it was found that 22.41 % opened a phishing email message and clicked on the link. In order to gain their cyber threat awareness, therefore, the knowledge transfer processes based on cybersecurity awareness for employees have been conducted. Then, the attack simulation with different content compared to the first round was conducted again. After gathering and analyzing the data from the same employees, it has been found that only 7.88 % opened the email and clicked on the link. The number has been reduced by 64.81 % compared to the first phase. Also, the cybersecurity awareness level has been increased to 88.80 %. That means the knowledge transfer processes that have been conducted works well. Therefore, this study has a contribution to the concept application for the cybersecurity awareness in other organizations and other forms of attacks.

Keywords: phishing, awareness, cybersecurity, attack simulation

บทนำ

ปัจจุบันมีการใช้งานเทคโนโลยีอินเทอร์เน็ตอย่างกว้างขวาง ไม่ว่าจะเป็นการใช้ในการศึกษาหาความรู้ผ่านการเรียนออนไลน์ การใช้เพื่อความบันเทิง (เช่น ดูละครย้อนหลัง ดูหนัง หรือฟังเพลง) การเรียน การค้นคว้าหาความรู้หรือพัฒนาตนเอง (เช่น การเรียนภาษาอังกฤษออนไลน์) และการใช้เพื่อทำธุรกรรมทางการเงิน (เช่น การโอนหรือชำระเงินค่าสินค้าที่สั่งซื้อออนไลน์ผ่านอินเทอร์เน็ต) เนื่องจากมีการใช้งานอินเทอร์เน็ตอย่างกว้างขวาง ปัญหาด้านความมั่นคงปลอดภัยเกี่ยวกับการใช้งานอินเทอร์เน็ตหรือที่เรียกอีกอย่างว่าความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นสิ่งที่สิ่งที่หลีกเลี่ยงได้ค่อนข้างยาก ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (Thailand Computer Emergency Response Team: ThaiCERT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการรวบรวมสถิติภัยคุกคามทางไซเบอร์ (เช่น เนื้อหาที่ไม่เหมาะสม ปัญหาความพร้อมใช้งาน ปัญหาการฉ้อโกงออนไลน์ ปัญหาความปลอดภัยของข้อมูล ความพยายามในการบุกรุกและการบุกรุก และไวรัสคอมพิวเตอร์หรือรหัสที่เป็นอันตรายอื่น ๆ เป็นต้น) ที่เกิดขึ้นปี พ.ศ. 2562 พบว่ามีผู้แจ้งรวมกันทั้งสิ้น 2,470 ครั้ง (ไทยเซิร์ต, 2563)

อย่างไรก็ดี หนึ่งในภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ค่อนข้างสำคัญและมีความน่าสนใจก็คือ ฟิชชิ่ง (Phishing) ซึ่งเป็นวิธีการหรือสิ่งที่ผู้ไม่ประสงค์ดีพยายามที่จะใช้เพื่อขโมยข้อมูลที่สำคัญของผู้ใช้งานอินเทอร์เน็ต เช่น ชื่อผู้ใช้ (User name) รหัสผ่าน (Password) เป็นต้น ด้วยการส่งอีเมลหรือลิงก์ของเว็บไซต์ปลอม แล้วนำชื่อผู้ใช้และรหัสผ่านของพนักงานไปสวมรอยเข้าระบบการเงินที่สำคัญของบริษัทซึ่งเคยเกิดขึ้นมาแล้ว เช่น กรณีของธนาคารกลางประเทศบังคลาเทศที่ถูกโจมตีระบบ SWIFT (Society for Worldwide Interbank Financial Telecommunication) ผ่านเทคนิคฟิชชิ่งจนเกิดความเสียหายมากกว่า 80 ล้านดอลล่าร์สหรัฐหรือกว่า 2,800 ล้านบาท เมื่อปี พ.ศ. 2559 (Zetter, 2016) และกรณีของ บมจ. สตาร์ ปิโตรเลียม รีไฟน์นิ่ง ในประเทศไทยที่ถูกโจมตีฟิชชิ่งจนเกิดความเสียหายไปมากกว่า 700 ล้านบาท ซึ่งกลายเป็นปัจจัยลบสำคัญปัจจัยหนึ่งที่ทำให้ผลประกอบการของบริษัทอยู่ในสถานะขาดทุนเป็นครั้งแรก นับตั้งแต่เข้าจดทะเบียนในตลาดหลักทรัพย์ฯ ในปี พ.ศ. 2558 (กรุงเทพธุรกิจ, 2563)

ทั้งนี้ ได้มีการประมาณการว่า ภายใน พ.ศ. 2570 ทั่วโลกจะมีค่าใช้จ่ายในการอบรมพนักงานเพื่อให้มีความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์สูงถึง 300,000 ล้านบาท ซึ่งเพิ่มขึ้นเป็น 10 เท่าเมื่อเทียบกับตัวเลขประมาณการเมื่อ พ.ศ. 2557 (Morgan, 2019) และมีรายงานฉบับหนึ่งระบุเอาไว้ว่า ในปี 2561 มีรายงานพบการฟิชชิ่งเกิดขึ้นประมาณ 22% ของรายงานการเกิดภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ที่เกิดขึ้นทั้งหมดในอเมริกา (Slye, 2019) นอกจากนี้ ได้มีข้อมูลที่ระบุว่า 30% ของอีเมลฟิชชิ่งถูกเปิดอ่านโดยผู้ที่เป็นเป้าหมายของผู้ไม่ประสงค์ดี และรายงานด้วยว่า มี 12% คลิกบนลิงก์ที่ส่งมากับในอีเมล (Cranor, 2018) นอกจากประเด็นดังกล่าว ยังมีรายงานที่แสดงให้เห็นว่า อุตสาหกรรมการเงินเป็นหนึ่งในเป้าหมายในการโจมตีของผู้ไม่ประสงค์ดี โดยพบว่า มีความพยายามที่จะเข้าถึงข้อมูลสำคัญโดยการล่วงละ เมิดด้วยวิธีการต่าง ๆ ซึ่งครอบคลุมถึงการฟิชชิ่ง ที่คิดเป็นสัดส่วนประมาณ 10% ด้วย (Zaw, 2019)

จากที่กล่าวมาข้างต้นจะเห็นได้ว่า ภัยทางไซเบอร์ถือเป็นปัญหาใหม่และส่งผลกระทบค่อนข้างมาก โดยเฉพาะอย่างยิ่งภัยจากการโจมตีด้วยฟิชชิ่ง ซึ่งสามารถสร้างความเสียหายทางการเงินให้กับบุคลากรในองค์กรได้โดยตรง นอกจากนี้ยังอาจส่งผลให้เกิดความเสียหายทางการเงินให้กับองค์กรได้อย่างมหาศาล ผู้วิจัยจึงได้ทำการศึกษาเกี่ยวกับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในบริษัทแห่งหนึ่ง โดยมีขั้นตอนคือ 1) จำลองการโจมตีด้วยอีเมลฟิชชิ่ง 2) จัดกระบวนการถ่ายทอดความรู้ให้บุคลากรเหล่านั้นเพื่อให้รู้เท่าทันภัยทางไซเบอร์ 3) ทำการจำลองการโจมตีซ้ำด้วยรูปแบบการโจมตีเดิม แล้วทำการวิเคราะห์และเปรียบเทียบผลจากการจำลองการโจมตีทั้ง 2 ครั้ง โดยมีสมมุติฐานว่า กระบวนการถ่ายทอดความรู้ที่ดำเนินการไปสามารถให้ผลลัพธ์ที่ดี และสามารถนำไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ ในองค์การอื่น ๆ ได้

ทฤษฎีที่เกี่ยวข้อง

1. การฟิชชิ่ง

ภัยทางไซเบอร์ในปัจจุบันมีหลากหลายรูปแบบ ไม่ว่าจะเป็นภัยในรูปแบบของมัลแวร์ (Malware) ซึ่งเป็นซอฟต์แวร์ประสงค์ร้ายที่สามารถสร้างความเดือนร้อนให้กับผู้ใช้งานได้ เช่น ไวรัสคอมพิวเตอร์ (Virus) หนอนคอมพิวเตอร์ (Worms) ม้าโทรจัน (Trojan horse) สปายแวร์ (Spyware) บ็อต (Bot) แอดแวร์ (Adware) และมัลแวร์เรียกค่าไถ่ (Ransomware) เป็น

ต้น ตลอดจนการโจมตีจนระบบสารสนเทศทางธุรกิจจนเกิดการปฏิเสธการให้บริการ (Denial-of-Service: DoS) อย่างไรก็ดี ฟิชชิ่ง (Phishing) ก็เป็นภัยทางไซเบอร์อีกรูปแบบที่สามารถสร้างความเสียหายได้ทั้งในระดับบุคคลและระดับองค์กร โดยเริ่มมีการรายงานเกี่ยวกับการฟิชชิ่ง (Phishing) ครั้งแรกเมื่อช่วงทศวรรษ 1990 ซึ่งระบุว่า แฮกเกอร์ (Hacker) ได้พยายามที่จะขโมยข้อมูลบัญชีผู้ใช้อเมริกันออนไลน์หรือ AOL โดยการหลอกเหยื่อว่าเป็นเจ้าหน้าที่ของ AOL แล้วส่งอีเมล (Email) เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลชื่อผู้ใช้และรหัสผ่าน ซึ่งเป็นข้อมูลที่ผูกกับข้อมูลบัตรเครดิตของเหยื่อ (Chaudhry et al., 2016; Jain & Gupta, 2017)

การฟิชชิ่งถือเป็นภัยคุกคามทางไซเบอร์ประเภทหนึ่ง ซึ่งคล้ายกับการจับปลาในบึงหรือทะเลสาบ ที่แม้จะมีโอกาสตกปลาได้จำนวนไม่มาก แต่ถ้าตกได้ปลาตัวใหญ่ก็ถือว่าคุ้มค่า ภัยคุกคามประเภทนี้อาจมาในรูปแบบของการหลอกล่อให้เหยื่อเปิดเผยข้อมูลส่วนตัวที่สำคัญ เช่น ชื่อผู้ใช้และรหัสผ่าน วันเดือนปีเกิด เลขบัตรประจำตัวประชาชน และข้อมูลทางการเงิน เป็นต้น หรืออาจจะแอบทำการติดตั้งสปายแวร์ (Spyware) หรือมัลแวร์ (Malware) อื่น ๆ บนเครื่องคอมพิวเตอร์ของเหยื่อก็ได้ (Jain & Gupta, 2017; Bahnsen et al., 2017; Peng et al., 2018)

ปกติการโจมตีประเภทนี้จะเกี่ยวข้องกับการส่งข้อความหรืออีเมล (อีเมลประเภทนี้บางครั้งจึงถูกเรียกว่าอีเมลฟิชชิ่ง) ที่มาพร้อมกับลิงก์ (Link) ที่ดูผิวเผินอาจเป็นเหมือนลิงก์ของเว็บไซต์ปกติทั่วไป แต่ในความเป็นจริงคือเป็นลิงก์ของเว็บไซต์ที่ควบคุมโดยฟิชเชอร์ (Phisher) นอกจากนี้ การฟิชชิ่งถือเป็นอาชญากรรมรูปแบบหนึ่งซึ่งไม่ได้ใช้เพียงเทคนิคที่ต้องอาศัยเทคโนโลยีเท่านั้น แต่ยังใช้เทคนิคที่เรียกว่าวิศวกรรมเชิงสังคม (Social Engineering) ด้วย (Jain & Gupta, 2017; Bahnsen et al., 2017; Peng et al., 2018) อย่างไรก็ดี แม้ว่าการหลีกเลี่ยงการโจมตีด้วยการฟิชชิ่งจะดูเหมือนง่าย แต่ปัจจุบันรูปแบบการฟิชชิ่งได้รับการพัฒนาให้มีความซับซ้อนขึ้นกว่าเมื่อก่อนมาก จนทำให้ผู้ใช้งานเครือข่ายอินเทอร์เน็ตและคอมพิวเตอร์หลงเชื่อและตกเป็นเหยื่อ

ในบรรดาเทคนิคการฟิชชิ่งที่มีหลากหลายรูปแบบ มีวิธีหนึ่งซึ่งฟิชเชอร์ (Phisher) หรือผู้โจมตี (Attacker) หรือแฮกเกอร์ นิยมใช้เรียกว่า Spear Phishing (ล้อกันกับคำว่า Spear Fishing ที่หมายถึงการจับปลาด้วยฉมวก) ซึ่งเป็นรูปแบบการฟิชชิ่งแบบมุ่งเป้า ซึ่งใช้แทนการส่งอีเมลแบบสุ่มไปหาผู้ใช้งานคอมพิวเตอร์ทั่วไป (Anstett, 2020) การฟิชชิ่งแบบมุ่งเป้า อาจทำได้โดยการส่งอีเมลไปยังกลุ่มเป้าหมายที่คาดว่าจะตกเป็นเหยื่อ โดยที่เนื้อหาในอีเมลเป็นเรื่องที่คาดว่ากลุ่มเป้าหมายจะให้ความสนใจ

2. การฝึกฝนบุคลากร: ด้านความมั่นคงปลอดภัยทางไซเบอร์

การฝึกฝนพนักงานหรือบุคลากรในองค์กรให้มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ตระหนักถึงความเสี่ยงและรู้เท่าทันภัยคุกคามกลายเป็นเรื่องที่จำเป็นและมีความสำคัญ การฝึกฝนดังกล่าว สามารถทำได้ในหลายรูปแบบ ทั้งนี้ก็เพื่อโอกาสในการปรับปรุงและพัฒนาศักยภาพและความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรในองค์กร

สำหรับภาคการเงินการธนาคารซึ่งเป็นภาคธุรกิจที่มีโอกาสสูงที่จะถูกคุกคามหรือโจมตีจากผู้ไม่ประสงค์ดี ธนาคารแห่งประเทศไทยซึ่งทำหน้าที่เป็นผู้กำกับดูแลภาคธุรกิจดังกล่าวในประเทศไทย ได้จัดทำกรอบการประเมินความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นกรอบที่อยู่ภายใต้หลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) สำหรับสถาบันการเงิน โดยที่ในกรอบดังกล่าว ได้มีการกล่าวถึงการฝึกฝนและทดสอบด้านความมั่นคงปลอดภัยทางไซเบอร์ด้วยการจำลองสถานการณ์การโจมตีด้วยรูปแบบภัยคุกคามและเทคนิควิธีการต่าง ๆ เพื่อให้ผู้ใช้งานคุ้นเคยและรู้วิธีการป้องกัน รับมือภัยคุกคาม และรวมไปถึงการทดสอบการตอบสนองต่อเหตุการณ์ภัยคุกคามของฝ่ายเทคโนโลยีสารสนเทศขององค์กรเอาไว้ด้วย นอกจากนี้ ยังสามารถใช้วัดระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของผู้ใช้งานและช่วยลดจำนวนปัญหาด้านความมั่นคงปลอดภัยขององค์กรได้เป็นอย่างดีด้วย (ธปท., 2562; Nachin et al., 2019)

3.งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า มีงานวิจัยหลายงานที่ได้มีการศึกษาในประเด็นคล้ายกัน ดังนี้

1) Greene et al. (2018) ได้ทำการศึกษาและวิเคราะห์ที่ได้จากการรวมรวมข้อมูลเกี่ยวกับการฟิชชิ่งนานมากกว่า 4 ปีครึ่ง พบว่า ผู้ที่คลิกอีเมลฟิชชิ่งให้เหตุผลว่า คลิกเปิดอีเมลดังกล่าวเนื่องจากกังวลว่าอาจจะเกิดผลเสียหายตามมาหากไม่เปิดอ่าน ในการศึกษาดังกล่าวได้สรุปว่า การอบรมให้รู้เท่าทันภัยจากการฟิชชิ่งอย่างเดียวไม่เพียงพอ จำเป็นหาแนวทางการอบรมให้ความรู้ที่เหมาะสมกับแต่ละองค์กร

2) Nachin et al. (2019) ได้ทำการศึกษาจากบุคลากรมากกว่า 4,500 คน ใน 20 องค์กร พบว่า การสร้างสถานการณ์จำลอง สามารถเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ได้และดีกว่าการอบรมโดยวิธีใช้ผู้ฝึกอบรมหรือวิทยากร แต่มีข้อเสนอแนะว่า ควรประยุกต์ใช้ทั้ง 2 วิธีการร่วมกันเพื่อผลลัพธ์ที่ดี

3) Carella et al. (2017) ได้ทำการศึกษาผลการจากการฝึกอบรมให้ผู้ใช้งานที่มีการคลิกลิงก์ที่ส่งกับอีเมลมาจากผู้ไม่ประสงค์ดี โดยมีการอบรมให้ผู้ใช้งานมีความรู้เท่าทันภัยทางไซเบอร์ด้วยวิธีการอบรมในห้อง และอบรมผ่านเอกสารเพียงอย่างเดียว และพบว่า การอบรมด้วยเอกสารให้ผลลัพธ์ที่ดีกว่าการจัดอบรมในห้อง

4) Diaz et al. (2019) ทำการศึกษาด้วยการจำลองการโจมตีด้วยฟิชชิ่ง ในมหาวิทยาลัยแห่งหนึ่งในมลรัฐแมรี่แลนด์ สหรัฐอเมริกา พบว่า กลุ่มตัวอย่างที่เข้าร่วมโครงการศึกษาซึ่งมีพื้นฐานความรู้ที่แตกต่างกัน มีการตอบสนองต่อการโจมตีด้วยฟิชชิ่งอีเมลในรูปแบบที่แตกต่างกัน โดยเฉพาะอย่างยิ่งกลุ่มตัวอย่างที่เรียนด้านศิลปศาสตร์ และสังคมศาสตร์ จะตอบสนองแตกต่างจากกลุ่มตัวอย่างที่เรียนด้านคณิตศาสตร์และวิทยาศาสตร์

5) Filippidis et al. (2018) ได้ทำการวัดเกี่ยวกับสิ่งที่มีผลกับความตระหนักรู้เท่าทันภัยทางไซเบอร์ ซึ่งได้มีการศึกษาถึงปัจจัยด้าน เพศ ระดับการศึกษา และโปรแกรมที่ศึกษา โดยทำการศึกษาในประเทศกรีซแห่งหนึ่ง พบว่า เพศไม่มีผลต่อความตระหนักรู้เท่าทันภัยทางไซเบอร์ ในขณะที่ระดับการศึกษาและโปรแกรมที่ศึกษามีผล โดยเฉพาะอย่างยิ่งระดับการศึกษาปริญญาโทมีผลมากกว่าปริญญาตรี

6) Abdullah & Mohd (2019) ได้ทำการศึกษาโดยใช้การจำลองโจมตีด้วยฟิชชิ่งในหน่วยงานหนึ่งกับกลุ่มตัวอย่างจำนวน 39 คน ในไตรมาสที่ 2 พ.ศ. 2561 พบว่ากลุ่มตัวอย่างสามารถระบุจุดต่าง ๆ ที่ผิดปกติในฟิชชิ่งอีเมลได้อย่างง่ายดาย อย่างไรก็ดี ผู้วิจัยและคณะได้ทำการศึกษาครั้งที่ 2 ในไตรมาสที่ 4 พ.ศ. 2561 กลับพบว่า มี 31% หรือ 12 คน ที่คลิกลิงก์ที่ส่งมากับอีเมล ซึ่งแสดงว่า การปรับเปลี่ยนแนวทางบางอย่างมีผลต่อความสำเร็จในการโจมตี แม้ผู้ใช้งานจะรู้เท่าทันภัยทางไซเบอร์อยู่บ้างก็ตาม

7) Ikhsan & Ramli (2019) ได้ทำการศึกษาด้วยแบบสอบถามเกี่ยวกับพฤติกรรมเพื่อวัดระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของเจ้าพนักงานในหน่วยงานรัฐในประเทศอินโดนีเซียจำนวนมากกว่า 7,300 คนทั่วประเทศ จากการศึกษาพบว่า เจ้าพนักงานในหน่วยงานรัฐในหน่วยงานดังกล่าวซึ่งตอบแบบสอบถาม 736 คนมีความตระหนักรู้เท่าทันภัยทางไซเบอร์ในระดับ 79.32 % เมื่อ 60 % - 79 % คือ ปานกลาง และ 80 % - 100 % คือ ดี

8) Mustafa et al. (2019) ได้นำเสนอแบบจำลองที่เรียกว่า แบบจำลอง ความรู้-ทัศนคติ-พฤติกรรม เพื่อเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์จากการโจมตีด้วยฟิชชิ่งในทั้ง 3 ด้าน โดยในครั้งแรกคณะผู้วิจัยดังกล่าวได้ทำการศึกษาเบื้องต้นกับกลุ่มตัวอย่างจำนวน 67 คน เพื่อวัดระดับความตระหนักรู้เท่าทันภัยทางไซบอร์และวิเคราะห์แล้วทำการนำเสนอแบบจำลอง KAB แบบเพิ่มสมรถนะ (KAB ย่อมาจาก Knowledge-Attitude-Behavior) หลังจากที่นำแบบจำลองไปใช้ในการศึกษาในครั้งที่สอง พบว่า ระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์เพิ่มขึ้นทั้ง 3 ด้าน

9) Moore & Clayton (2007) ได้ทำการประเมินมูลค่าความเสียหายจากการตกเป็นเหยื่อของการฟิชชิ่งในสหรัฐอเมริกาเมื่อปี พ.ศ. 2550 โดยรวบรวมข้อมูลเป็นเวลาประมาณ 2 เดือนจากเว็บไซต์ฟิชชิ่งธนาคาร (หรือเว็บไซต์ธนาคารปลอม) 1,438 แห่ง แล้วทำการคำนวณพบว่า มีมูลค่าความเสียหายไม่น้อยกว่า 320 ล้านดอลลาร์ (ประมาณ 9.99 พันล้านบาท) ซึ่งถือว่าสร้างความเสียหายให้สังคมค่อนข้างมากเพราะกระทบโดยตรงต่อเหยื่อจำนวนมาก

10) Davis (2020) ได้รายงานสถิติจากสำนักงานสอบสวนกลางของสหรัฐอเมริกา หรือเอฟบีไอ (Federal Bureau of Investigation: FBI) อาชญากรรมทางไซเบอร์ ได้สร้างความเสียหายให้กับเหยื่อทั้งในระดับบุคคลและองค์กรธุรกิจ รวมกันประมาณ 3.5 พันล้านดอลลาร์ (ประมาณ 1.09 แสนล้านบาท) ซึ่งเป็นมูลค่าความเสียหายทางธุรกิจที่สูงมาก

การจำลองการโจมตีด้วยอีเมลฟิชชิ่งและผลการศึกษา

ผู้วิจัยได้ดำเนินการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในบริษัทแห่งหนึ่งในกรุงเทพมหานคร ในช่วงต้นไตรมาสที่ 4 พ.ศ. 2562 โดยได้มีการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในบริษัทแห่งหนึ่งในกรุงเทพมหานคร ซึ่งเป็นบริษัทในเครือของสถาบันการเงินแห่งหนึ่งและเป็นผู้ให้บริการหลักในการดูแลระบบสารสนเทศให้กับสถาบันการเงินดังกล่าวซึ่งอยู่ภายใต้การกำกับดูแล

ของธนาคารแห่งประเทศไทย บริษัทนี้มีพนักงานรวมกันมากกว่า 500 คน ในการทดสอบดังกล่าว ผู้ที่ดำเนินการทดสอบไม่ใช่บุคลากรขององค์กร แต่เป็นการว่าจ้างบริษัทผู้เชี่ยวชาญจากภายนอกให้เป็นผู้ดำเนินการทดสอบ ซึ่งผู้ทดสอบได้ดำเนินการทดสอบในรูปแบบที่เรียกว่าไซเบอร์ดริลล์โดยใช้เทคนิคการจำลองการโจมตีด้วยอีเมลฟิชชิ่ง ซึ่งแบ่งการจำลองการโจมตีออกเป็น 2 ครั้ง โดยมีกระบวนการถ่ายทอดความรู้ระหว่างการจำลองการโจมตีทั้ง 2 ครั้งด้วย (ดังภาพที่ 1) ดังนี้

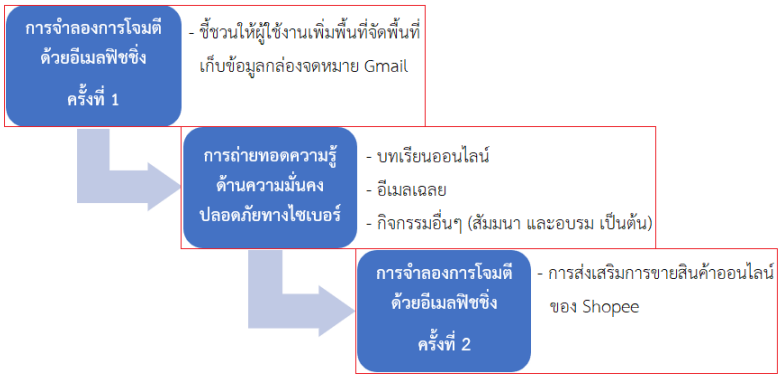
1) จำลองการโจมตีครั้งที่ 1 ดำเนินการขึ้นเมื่อเดือนตุลาคม พ.ศ. 2562 เป็นการโจมตีด้วยฟิชชิ่งโดยส่งอีเมลที่มีเนื้อหาชี้ชวนให้ผู้ใช้งานเพิ่มพื้นที่จัดพื้นที่เก็บข้อมูลกล่องจดหมาย Gmail (ดังภาพที่ 2) ไปยังพนักงานของบริษัท จำนวน 546 คน ซึ่งมีทั้งพนักงานหญิงและชาย ที่มีอายุระหว่าง 23-60 ปี อย่างไรก็ดีที่ มีเพียง 482 เท่านั้น จากนั้นจึงนำผลการศึกษาที่ได้ (ดังภาพที่ 3) ไปวิเคราะห์หาบุคลากรที่เข้าข่ายเหยื่อฟิชชิ่ง

2) ดำเนินการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากร ซึ่งประกอบด้วย

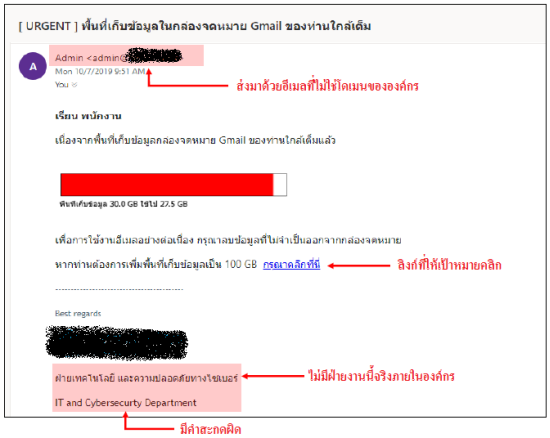
- การให้ความรู้ผ่านบทเรียนออนไลน์ (E-leaning) เรื่องความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งไม่ได้มีเนื้อหาเฉพาะเรื่องฟิชชิ่งเท่านั้นแต่ยังรวมถึงภัยคุมคามรูปแบบอื่น ๆ ด้วย พร้อมทั้งมีแบบทดสอบ (เกณฑ์สอบผ่านคือ 80%) (ดังภาพที่ 4)
- การส่งอีเมลเฉลยซึ่งเป็นการแจ้งด้วยอีเมลว่ามีการจำลองการโจมตีด้วยเทคนิคฟิชชิ่ง โดยมีการเฉลยให้ทราบถึงสิ่งผิดปกติหรือข้อควรสังเกตต่าง ๆ ที่มักพบในอีเมลฟิชชิ่ง
- การจัดกิจกรรมเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีกิจกรรมหลายอย่าง เช่น การสัมมนาให้ความรู้ในหัวข้อต่าง ๆ จากผู้เชี่ยวชาญ และการจัด Workshop เพื่อให้ผู้เข้าร่วมกิจกรรมได้ฝึกทักษะและซักถามข้อสงสัยกับผู้เชี่ยวชาญได้อย่างใกล้ชิด (ดังภาพที่ 5)

3) จำลองการโจมตีครั้งที่ 2 ดำเนินการเมื่อเดือนกุมภาพันธ์ พ.ศ. 2563 เป็นการจำลองการโจมตีด้วยฟิชชิ่งโดยส่งอีเมลที่มีเนื้อหาแตกต่างจากครั้งที่ 1 โดยครั้งที่ 2 เกี่ยวข้องกับการส่งเสริมการขายสินค้าออนไลน์ของ Shopee (ดังภาพที่ 6) ซึ่งเป็นหนึ่งในแพล็ตฟอร์มซื้อขายสินค้าออนไลน์ยอดนิยมในประเทศไทยไปยังพนักงานของบริษัทกลุ่มเดียวกันกับครั้งที่ 1 เมื่อได้ผลการศึกษาจากครั้งที่ 2 (ดังภาพที่ 7) แล้วจึงทำการวิเคราะห์เปรียบเทียบกับผลที่ได้จากการศึกษาครั้งแรก

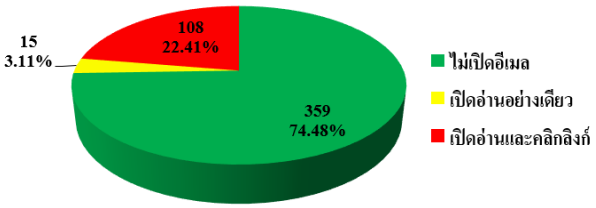
ในการจำลองการโจมตีด้วยฟิชชิ่งทั้ง 2 ครั้ง คณะผู้วิจัยเลือกใช้เนื้อหาในอีเมลที่ชี้ชวนให้ผู้ใช้งานเพิ่มพื้นที่จัดพื้นที่เก็บข้อมูลกล่องจดหมาย Gmail และการส่งเสริมการขายสินค้าออนไลน์ของ Shopee เพราะเป็นประเด็นที่ถือว่าน่าสนใจสำหรับผู้ใช้งานทั่วไป อย่างไรก็ดี เหตุที่คณะผู้วิจัยจำเป็นต้องใช้รูปแบบเนื้อหาในอีเมลที่แตกต่างกันในการจำลองการโจมตีครั้งแรกและครั้งที่ 2 ก็เพื่อหลีกเลี่ยงไม่ให้พนักงานทราบว่าเป็นการจำลองการโจมตีซ้ำในครั้งที่ 2 ซึ่งอาจเป็นปัจจัยหนึ่งที่ส่งผลกระทบต่อผลการศึกษา



ภาพที่ 1 ภาพรวมการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในการศึกษานี้

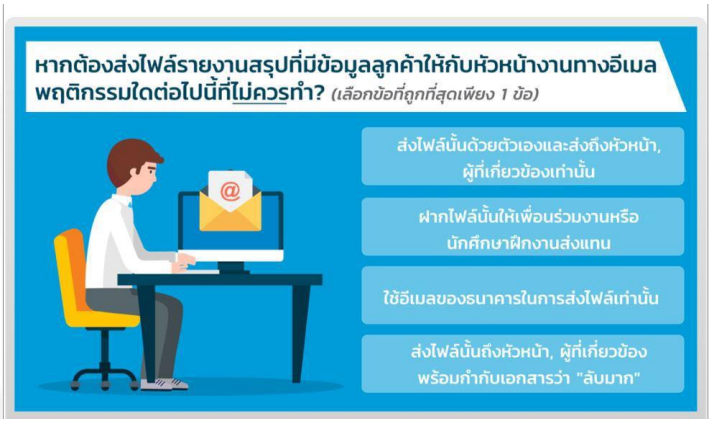


ภาพที่ 2 หน้าจออีเมลฟิชชิ่งที่ใช้ในการศึกษาครั้งที่ 1



ภาพที่ 3 ผลการศึกษาครั้งที่ 1

(ก)



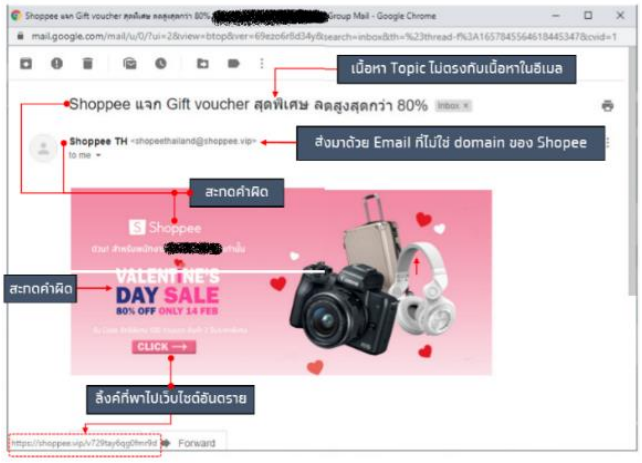
(ข)

ภาพที่ 4 บทเรียนออนไลน์เกี่ยวกับภัยคุกคามทางไซบอร์ (ก) คำชี้แจง (ข) ตัวอย่างคำถามในแบบทดสอบ

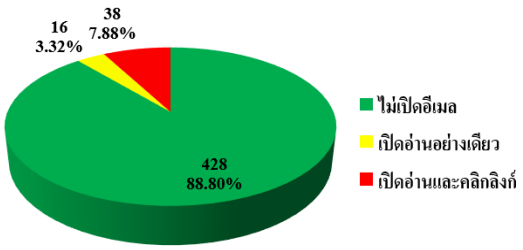
(ก)

(ข)

ภาพที่ 5 ภาพกิจกรรม (ก) การบรรยายบนเวทีในงานวันรู้เท่าทันภัยทางไซเบอร์
(ข) สัมมนาความปลอดภัยทางไซเบอร์ให้กับผู้บริหาร



ภาพที่ 6 หน้าจออีเมลฟิชชิ่งที่ใช้ในการศึกษาครั้งที่ 2



ภาพที่ 7 ผลการศึกษาครั้งที่ 2

การวิเคราะห์และอภิปรายผล

จากวิเคราะห์ผลการศึกษาในครั้งที่ 1 ด้วยสถิติพื้นฐาน ซึ่งผลดังกล่าวได้มาจากการจำลองการโจมตีทางไซเบอร์ด้วยอีเมลฟิชชิ่งที่มีเนื้อหาเกี่ยวกับกล่องจดหมาย Gmail พบว่า บุคลากร 359 คน หรือ 74.48 % ไม่มีการตอบสนองต่ออีเมลดังกล่าว ในขณะที่มี 108 คน หรือ 22.41 % ที่เปิดอีเมลและคลิกลิงก์ที่อยู่ในอีเมล และมี 15 คน หรือ 3.11 % ที่เปิดอีเมลเพียงอย่างเดียว จึงอนุมานได้ว่า บุคลากรในองค์กรรู้เท่าทันภัยทางไซเบอร์ในเกณฑ์ปานกลาง (60 %-79 % = ปานกลาง) (Ikhsan & Ramli, 2019)

อย่างไรก็ดีหลังจากที่มีการได้มีการถ่ายทอดความรู้ให้กับบุคลากรด้วยวิธีการต่าง ๆ เช่น การให้ความรู้ผ่านออนไลน์ซึ่งเป็นกระบวนการเรียนรู้ที่บุคลกรสามารถเรียนรู้ได้ด้วยตนเองผ่านหลักสูตรและแบบทดสอบที่ทางบริษัทได้จัดเตรียม โดยสามารถเลือกเวลาเรียนและทำแบบทดสอบได้ทั้งในและนอกเวลางาน ตลอดจนกิจกรรมต่าง ๆ เช่น สัมมนาและการอบรม แล้วทำการจำลองการโจมตีอีกครั้งโดยมีการปรับเปลี่ยนเนื้อหาในอีเมลฟิชชิ่งเป็นเรื่องการส่งเสริมการขายสินค้าออนไลน์พบว่า บุคลากร 428 คน หรือประมาณ 88.80 % ไม่มีการตอบสนองต่ออีเมลดังกล่าว ในขณะที่มี 38 คน หรือ 7.88 % ที่เปิดอีเมลและคลิกลิงก์ที่อยู่ในอีเมล และมี 16 คน หรือ 3.32 % ที่เปิดอีเมลเพียงอย่างเดียว จึงอนุมานได้ว่า บุคลากรในองค์กรรู้เท่าทันภัยทางไซเบอร์ในเกณฑ์ดี (80 %-100 % = ดี) (Ikhsan & Ramli, 2019)

เมื่อวิเคราะห์เปรียบเทียบผลการศึกษาจากทั้งสองครั้งจากภาพที่ 2 และรูปที่ 5 แล้วแสดงในตารางที่ 1 จะเห็นได้ชัดเจนว่า ภายหลังการจำลองการโจมตีด้วยฟิชชิ่งในครั้งที่ 1 แล้วทำการถ่ายทอดองค์ความรู้ให้บุคลากรในรูปแบบต่าง ๆ แล้วทำการจำลองการโจมตีด้วยฟิชชิ่งในครั้งที่ 2 พบว่า บุคลากรในองค์กรที่ไม่เปิดอีเมลฟิชชิ่งมีจำนวนเพิ่มขึ้นจาก 359 คน หรือประมาณ 74.48 % เป็น 428 คน หรือ 88.80 % ซึ่งคิดเป็น 19.22 % (ดูตารางที่ 1) ในขณะที่มีจำนวนบุคลากรที่เปิดอ่านอีเมลและคลิก

ลิงก์ลดลงจาก 108 คน เป็น 38 คน หรือจาก 22.41 % เป็น 7.88 % โดยประมาณ ซึ่งคิดเป็น 64.81 % (ดูตารางที่ 1) ถึงแม้ว่าจะมีจำนวนบุคลากรที่เปิดอ่านอีเมลเพียงอย่างเดียวแต่ไม่ได้คลิกลิงก์เพิ่มขึ้น แต่ก็เพิ่มขึ้นเพียงคนเดียวเท่านั้น จึงสามารถกล่าวได้ว่า วิธีดำเนินการที่ใช้ในการศึกษานี้ สามารถเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรได้เป็นอย่างดี โดยเฉพาะอย่างยิ่งกรณีการโจมตีด้วยอีเมลฟิชชิ่ง

นอกจากนี้ เมื่อเปรียบเทียบกับข้อมูลที่มาจากการศึกษาก่อนหน้านี้ที่ระบุว่ามีการเปิดอีเมลฟิชชิ่งถึง 30% (Cranor, 2018) จะเห็นได้ว่า ผลการศึกษาที่ได้จากการศึกษานี้ทั้งในครั้งที่ 1 (รวม 25.52 %) และครั้งที่ 2 (11.20 %) มีจำนวนน้อยกว่าผลการศึกษาดังกล่าว ยิ่งไปกว่านั้น เมื่อเปรียบเทียบกับผลการศึกษาเดียวกันที่ระบุว่ามีการเปิดอีเมลฟิชชิ่งและคลิกลิงก์ 12 % จะเห็นได้ว่า ผลที่ได้จากการศึกษานี้ในครั้งที่ 1 (22.41 %) มีจำนวนสูงกว่า อย่างไรก็ดีหลังจากที่มีการถ่ายทอดความรู้เกี่ยวกับภัยทางไซเบอร์พบว่า ผลที่ได้จากการศึกษานี้ในครั้งที่ 2 (7.88 %) ลดลงอย่างเห็นได้ชัดและมีจำนวนน้อยกว่าผลการศึกษาดังกล่าว นั่นแสดงว่า ผลการศึกษานี้เป็นไปตามสมมุติฐานที่ระบุไว้ในบทนำ

ตารางที่ 1 ผลการวิเคราะห์เปรียบเทียบผลการศึกษาครั้งที่ 1 กับ 2 คิดเป็นร้อยละ

การตอบสนอง	ครั้งที่	จำนวนคน	ความเปลี่ยนแปลง	หมายเหตุ
ไม่เปิดอีเมล	1	74.48 %	19.22 %	เพิ่มขึ้น
	2	88.80 %		
เปิดอ่านอย่างเดียว	1	3.11 %	6.67 %	เพิ่มขึ้น
	2	3.32 %		
เปิดอ่านและคลิกลิงก์	1	22.41 %	64.81 %	ลดลง
	2	7.88 %		

อย่างไรก็ตาม ถึงแม้ตัวเลขดังกล่าวนี้จะน้อยกว่าตัวเลขที่ได้มีการศึกษาก่อนหน้านี้ แต่ก็ยังถือว่ามีช่องโหว่ให้ถูกโจมตีได้ ดังนั้นจึงจำเป็นที่จะต้องมีการดำเนินการผ่านกิจกรรมต่าง ๆ เพื่อรักษาและเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร นอกจากนี้ เมื่อพิจารณาถึงเนื้อหาในอีเมลฟิชชิ่ง ซึ่งเกี่ยวกับพื้นที่เก็บข้อมูลกล่องจดหมาย Gmail และการส่งเสริมการขายสินค้าออนไลน์ของ Shopee อาจเป็นไปได้ว่า เนื้อหาไม่จูงใจบุคลากรบางส่วนเท่าที่ควร หากมีการเปลี่ยนเนื้อหาในอีเมลฟิชชิ่ง เช่น การส่งเสริมการขายโทรศัพท์รุ่นใหม่ หรือร้านกาแฟชื่อดัง อาจทำให้ได้ผลการทดสอบที่แตกต่างไปจากผลการทดสอบในครั้งนี้ก็เป็นได้ จึงควรมีการพิจารณาการศึกษาเพิ่มเติมประเด็นนี้ในอนาคต

สรุปผลการวิจัย

จากผลการศึกษาด้วยการจำลองการโจมตีโดยใช้อีเมลฟิชชิ่งในบริษัทแห่งหนึ่งเกี่ยวกับประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ในครั้งนี้ สามารถสรุปจากผลการศึกษาในครั้งที่ 1 ได้ว่า บุคลากรในองค์กรมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ยังไม่จัดได้ว่าอยู่ในเกณฑ์ดี (74.48 %) เพราะยังมีพนักงานหรือบุคลากรขององค์กรจำนวนหนึ่งที่ยังขาดความตระหนักถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดีเมื่อมีการดำเนินการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากร แล้วทำการศึกษาซ้ำในครั้งที่ 2 พบว่า บุคลากรในองค์กรมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ดีขึ้นอย่างชัดเจน คืออยู่ในเกณฑ์ดี (88.80 %) แสดงว่าการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากรที่ดำเนินการไปให้ผลลัพธ์ที่ดี และสามารถนำรูปแบบการดำเนินการที่ได้บรรยายไว้ในบทความนี้ไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ในองค์กรอื่น ๆ ได้ เพื่อเพิ่มความมั่นคงปลอดภัยทางไซเบอร์และของบุคลากรในองค์กร

อย่างไรก็ตามการยกระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ด้วยการจำลองการโจมตีด้วยอีเมลฟิชชิ่งเพียงอย่างเดียวอาจไม่เพียงพอ ผู้บริหารจำเป็นที่จะต้องดำเนินการอย่างต่อเนื่องและครอบคลุมภัยทางไซเบอร์รูปแบบอื่น ๆ ด้วย เช่น การโจมตีด้วยไวรัสเรียกค่าไถ่ (Ransomware) ตลอดจนการโจมตีด้วยมัลแวร์ (Malware) ทุกรูปแบบ

กิตติกรรมประกาศ

ขอขอบคุณคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเอเชียอาคเนย์ และคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครที่ให้การสนับสนุนการเขียนบทความวิจัยนี้

เอกสารอ้างอิง

[1] กรุงเทพธุรกิจ (2563). SPRC เสียเหลี่ยม ถูก'อีเมล์ลวง'หลอกโอนเงินสูญหลักร้อยล้าน [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://www.bangkokbiznews.com/news/detail/867528

[2] ไทยเซิร์ต (2563). สถิติภัยคุกคาม ประจำปี พ.ศ. 2562 [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://www.thaicert.or.th/statistics/statistics2019.html

[3] ธปท. (2562). กรอบการประเมินความพร้อมด้าน Cyber Resilience [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/FSINotifications/Cyber%2_0_resilience%20framework%202019.pdf.

[4] Abdullah, A. S., & Mohd, M. (2019). Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. Proc. of ICoCSec 2019, Negeri Sembilan, Malaysia, 26-31. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1109/ICoCSec47621.2019.8970803.

[5] Anstett, A. (2019). What is spear phishing? [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://www.wandera.com/what-is-spear-phishing/.

[6] Bahnsen, A. C., Bohorquez, E. C., Villegasy, S., Vargasy, J., & Gonz´alez, F. A. (2017). Classifying Phishing URLs Using Recurrent Neural Networks. Proc. of eCrime 2017, Scottsdale, AZ, 1-8. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1109/ECRIME.2017.7945048.

[7] Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. Proc. of Big Data 2017, Boston, MA, 4458-4466. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org /10.1109/BigData.2017.8258485.

[8] Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. International Journal of Security and Its Applications, 10(1), 247-256. ค้นเมื่อ 25 ตุลาคม 2563, จาก http://dx.doi.org/ 10.14257 /ijsia.2016.10.1.23.

[9] Cranor, L. (2018). 25 Security awareness training and phishing prevention [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://canvas.cmu.edu/files/965667/download?download_frd=1.

[10] Davis, J. (2020). FBI: $3.5B Lost to Cybercrime in 2019, Led by Business Email Compromise [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก. https://healthitsecurity.com/news/fbi-3.5b-lost-to-cybercrime-in-2019-led-by-business-email-compromise#:~:text=February%2012%2C%202020%20%2D%20The%20FBI,caused%20by%20business%20email%20compromise.

[11] Diaz, A., Sherman, A. T., & Joshi, A. (2019). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1), 53-67. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1080/01611194.2019.1623343.

[12] Filippidis, A. P., Hilas, C. S., Filippidis, G., & Politis, A. (2018). Information Security Awareness of Greek Higher Education Students - Preliminary Findings. Proc. of MOCAST 2018, Thessaloniki, Greece, 1-4. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1109/MOCAST.2018.8376578.

[13] Greene, K.K., Steves, M., & Theofanos, M. (2018). No Phishing beyond This Point. Computer, 51(6), 86–89. ค้นเมื่อ 25 ตุลาคม 2563, จาก http://doi.ieeecomputersociety.org/10.1109/MC.2018.2701632.

[14] Ikhsan, M. G., & Ramli, K. (2019). Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment. Proc. of ITC-CSCC 2019, JeJu, Korea (South), 1-4. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1109/ITC-CSCC.2019.8793292.

[15] Jain, A. K., & Gupta, B. B. (2017). Phishing Detection: Analysis of Visual Similarity Based Approaches. Security and Communication Networks, 2017, 5421046. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1155/2017/5421046.

[16] Moore, T. & Clayton, R. (2007). Examining the Impact of Website Take-down on Phishing. Proc. of eCrime '07, Pittsburgh, PA, 1-13. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://dl.acm.org/doi/pdf/10.1145/1299015.1299016.

[17] Morgan, S. (2019). Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021 [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://cybersecurityventures.com/cybersecurity-market-report/.

[18] Mustafa, M. S. b. O., Kabir, Ernawan, F., & Jing, W. (2019). An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks. Proc. of I2CACIS, Selangor, Malaysia, 10-14. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1109/I2CACIS.2019.8825070.

[19] Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). How to Increase Cybersecurity Awareness. ISACA Journal, 2, 45-50. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://next.isaca.org/resources/isaca-journal/issues/2019/volume-2/how-to-increase-cybersecurity-awareness.

[20] Peng, T., Harris, I. G., & Sawa, Y. (2018). Detecting Phishing Attacks Using Natural Language Processing and Machine Learning. Proc. of ICSC 2018, Laguna Hills, CA, 300-301, ค้นเมื่อ 25 ตุลาคม 2563, จาก https://doi.org/10.1109/ICSC.2018.00056.

[21] Slye, J. (2019). End-User Cybersecurity Violations Continue to Plague Federal Agencies [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://iq.govwin.com/neo/marketAnalysis/view/End-User-Cybersecurity-Violations-Continue-to-Plague-Federal-Agencies/3716?researchTypeId=1.

[22] Zaw, T. (2019). 2019 Verizon Data Breach Investigations Report: First impressions from the perimeter [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://www.verizondigitalmedia.com/blog/2019-verizon-data-breach-investigations-report-first-impressions/.

[23] Zetter, K. (2016). That Insane, $81M Bangladesh Bank Heist? Here's What We Know. [เว็บไซต์]. ค้นเมื่อ 25 ตุลาคม 2563, จาก https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.