`{link_th_title_1}`

นายณภัทร ทารมย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวงและการพัฒนาโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทเอกชน

นายณภัทร ทารมย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ใบรับรองโครงร่างวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง

โดย นายณภัทร ทารมย์

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

คณะกรรมการสอบวิทยานิพนธ์

.....

อาจารย์ที่ปรึกษา

(นวพร วิสิฐพงศ์พันธ์)

ชื่อ : นายณภัทร ทารมย์
ชื่อวิทยานิพนธ์ : การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวงและการพัฒนาโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทเอกชน
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : นวพร วิสิฐพงศ์พันธ์
ปีการศึกษา : 2567

บทคัดย่อ

ปัญหาการโจมตีแบบฟิชชิง (Phishing) บนไซเบอร์มีรากฐานมาตั้งแต่ปลายทศวรรษ 1990 ซึ่งผู้โจมตีมักใช้รูปแบบของอีเมลปลอมแปลงที่อ้างว่ามาจากแหล่งที่น่าเชื่อถือ เช่น ธนาคารหรือบริษัทที่ผู้ใช้คุ้นเคย อีเมลเหล่านี้มักจะออกแบบมาเพื่อหลอกล่อผู้ใช้ให้คลิกลิงก์หรือเปิดไฟล์แนบที่ติดไวรัส เมื่อผู้ใช้คลิกลิงก์หรือเปิดไฟล์แนบ ผู้โจมตีจะสามารถเข้าถึงข้อมูลส่วนตัวของผู้ใช้ เช่น รหัสผ่าน ข้อมูลบัญชีธนาคาร หรือข้อมูลทางการเงิน ผู้วิจัยจึงเล็งเห็นถึงความสำคัญในการหามาตรการป้องกันและจัดการกับภัยคุกคามด้านความปลอดภัยทางไซเบอร์ ดังนั้น จึงได้เลือกบริษัทเอกชนแห่งหนึ่งมาเป็นกรณีศึกษาเพื่อดำเนินการประเมินระดับความเสี่ยงและพัฒนาหลักสูตรการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ โดยมีวัตถุประสงค์เพื่อลดความเสี่ยงในการถูกโจมตีในรูปแบบฟิชชิง การศึกษานี้จะมีผลช่วยให้บริษัทมีความพร้อมในการป้องกันและการจัดการกับภัยคุกคามด้านความปลอดภัยทางไซเบอร์ในองค์กรและสังคมออนไลน์อย่างมีประสิทธิภาพในอนาคต

(มีจำนวนทั้งสิ้น xx หน้า)

คำสำคัญ : คำสำคัญ1, คำสำคัญ2, คำสำคัญ3

_____ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Name : Mr. Napat Tarom
Thesis Title : Assessing Phishing Vulnerabilities and Developing Cybersecurity Training Program for Private Company
Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Thesis Advisor : Nawaporn Wisitpongphan
Academic Year : 2024

ABSTRACT

Since the late 1990s, phishing attacks has become a big problem in the online environment. These tricky attacks often pretend to be emails from trusted sources, such as banks or big companies. They try to fool people into clicking on bad links or opening harmful attachments, which can give hackers access to important information such as passwords or financial data. To tackle this issue and find measures to prevent and manage cyber security threats, we chose to perform a risk assessment and develop cybersecurity training program using one particular private company as a case study. The goal is to reduce the risk of victims falling for phishing attacks. The ultimate outcome is to help the company prepared for sneaky cyber-attacks, and be able to manage cyber security threats in organization or online community contexts effectively in the future.

(Total xx Pages)

Keywords: Keyword1, Keyword2, Keyword 3

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระอีเมลนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ อาจารย์ที่ปรึกษาการค้นคว้าอิสระที่ได้ให้ข้อคิดเห็นต่าง ๆ และให้ความช่วยเหลือชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิจัยนี้มาโดยตลอด ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณผู้บริหาร ผู้บังคับบัญชา และบุคลากรทุกท่านขององค์กร ที่ให้การสนับสนุนและให้ความร่วมมือ พร้อมทั้งสละเวลาอันมีค่าเพื่อให้ได้มาซึ่งข้อมูลประกอบการวิจัยในครั้งนี้

ท้ายที่สุดนี้ ผู้วิจัยขอกราบขอบพระคุณบิดา มารดา ซึ่งสนับสนุนในด้านการเงินและให้กำลังใจแก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

ณภัทร ทารมย์

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง (ถ้ามี) ..... ซ

สารบัญรูปภาพ (ถ้ามี) ..... ฌ

บรรณานุกรม 2

ภาคผนวก 3

ประวัติผู้เขียน 4

สารบัญตาราง (ถ้ามี)

หน้า

No table of figures entries found.

สารบัญรูปภาพ (ถ้ามี)

หน้า

No table of figures entries found.

“เริ่มเขียนบทที่ 1 ที่นี่”

บรรณานุกรม

พิมพ์รายการอ้างอิงลงในนี้ หรือทำการย้ายรายการอ้างอิงที่สร้างจาก Endnote หรือ Zotero ท้ายเล่มมายังบริเวณนี้

ภาคผนวก

หากมีภาคผนวกให้จัดทำเนื้อหาบริเวณนี้ หากไม่มีสามารถลบหน้านี้ทิ้งได้เลย

ประวัติผู้เขียน

ชื่อ ณภัทร ทารมย์

ชื่อวิทยานิพนธ์ การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวงและการพัฒนาโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทเอกชน

สาขาวิชา การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประวัติ

อนุปริญญา : สาขาอิเล็กทรอนิกส์การบิน
คณะเทคโนโลยีอากาศยาน
สถาบันการบินพลเรือน

ปริญญาตรี : สาขาการจัดการการขนส่งสินค้าทางอากาศ
คณะการจัดการเทคโนโลยีการบิน
สถาบันการบินพลเรือน

การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวงและการพัฒนาโปรแกรมฝึกอบรม
ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทเอกชน

นายณภัทร ทารมย์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตร์มหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2566

ชื่อ : นายณภัทร ทารมย์
ชื่อการค้นคว้าอิสระ : การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวงและการพัฒนาโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทเอกชน
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์
ปีการศึกษา : 2566

บทคัดย่อ

ปัญหาการโจมตีแบบฟิชชิง (Phishing) บนไซเบอร์มีรากฐานมาตั้งแต่ปลายทศวรรษ 1990 ซึ่งผู้โจมตีมักใช้รูปแบบของอีเมลปลอมแปลงที่อ้างว่ามาจากแหล่งที่น่าเชื่อถือ เช่น ธนาคารหรือบริษัทที่ผู้ใช้คุ้นเคย อีเมลเหล่านี้มักจะออกแบบมาเพื่อหลอกล่อผู้ใช้ให้คลิกลิงก์หรือเปิดไฟล์แนบที่ติดไวรัส เมื่อผู้ใช้คลิกลิงก์หรือเปิดไฟล์แนบ ผู้โจมตีจะสามารถเข้าถึงข้อมูลส่วนตัวของผู้ใช้ เช่น รหัสผ่าน ข้อมูลบัญชีธนาคาร หรือข้อมูลทางการเงิน ผู้วิจัยจึงเล็งเห็นถึงความสำคัญในการหามาตรการป้องกันและจัดการกับภัยคุกคามด้านความปลอดภัยทางไซเบอร์ ดังนั้น จึงได้เลือกบริษัทเอกชนแห่งหนึ่งมาเป็นกรณีศึกษาเพื่อดำเนินการประเมินระดับความเสี่ยงและพัฒนาหลักสูตรการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ โดยมีวัตถุประสงค์เพื่อลดความเสี่ยงในการถูกโจมตีในรูปแบบฟิชชิง การศึกษานี้จะมีผลช่วยให้บริษัทมีความพร้อมในการป้องกันและการจัดการกับภัยคุกคามด้านความปลอดภัยทางไซเบอร์ในองค์กรและสังคมออนไลน์อย่างมีประสิทธิภาพในอนาคต

(การค้นคว้าอิสระนี้มีจำนวนทั้งสิ้น 55 หน้า)

คำสำคัญ : การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวง, การพัฒนาโปรแกรมฝึกอบรมด้านความปลอดภัยทางไซเบอร์

_____อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr.Napat Tarom
Independent Study Title : Assessing Phishing Vulnerabilities and Developing Cybersecurity Training Program for Private Company
Major Field : Network and Information Security Management
: King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Assistant Professor Dr.Nawaporn Wisitpongphan
Academic Year : 2023

Abstract

Since the late 1990s, phishing attacks has become a big problem in the online environment. These tricky attacks often pretend to be emails from trusted sources, such as banks or big companies. They try to fool people into clicking on bad links or opening harmful attachments, which can give hackers access to important information such as passwords or financial data. To tackle this issue and find measures to prevent and manage cyber security threats, we chose to perform a risk assessment and develop cybersecurity training program using one particular private company as a case study. The goal is to reduce the risk of victims falling for phishing attacks. The ultimate outcome is to help the company prepared for sneaky cyber-attacks, and be able to manage cyber security threats in organization or online community contexts effectively in the future.

(Total 55 pages)

Keywords : Assessing Phishing Vulnerabilities, Developing Cybersecurity Training Program

_____Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระอีเมลนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ อาจารย์ที่ปรึกษาการค้นคว้าอิสระที่ได้ให้ข้อคิดเห็นต่าง ๆ และให้ความช่วยเหลือชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิจัยนี้มาโดยตลอด ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณผู้บริหาร ผู้บังคับบัญชา และบุคลากรทุกท่านขององค์กร ที่ให้การสนับสนุนและให้ความร่วมมือ พร้อมทั้งสละเวลาอันมีค่าเพื่อให้ได้มาซึ่งข้อมูลประกอบการวิจัยในครั้งนี้

ท้ายที่สุดนี้ ผู้วิจัยขอกราบขอบพระคุณบิดา มารดา ซึ่งสนับสนุนในด้านการเงินและให้กำลังใจแก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

ณภัทร ทารมย์

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ข
บทคัดย่อภาษาอังกฤษ	ค
กิตติกรรมประกาศ	ง
สารบัญตาราง	ฉ
สารบัญภาพ	ช
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	2
1.3 ขอบเขตของการวิจัย	2
1.4 ประโยชน์ที่คาดว่าจะได้รับ	2
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง	4
2.1 ทฤษฎีที่เกี่ยวข้อง	4
2.2 งานวิจัยที่เกี่ยวข้อง	6
บทที่ 3 วิธีดำเนินการวิจัย	10
3.1 วิธีดำเนินการวิจัย	10
บทที่ 4 ผลการวิจัย	20
4.1 ผลการจำลองการโจมตีด้วยอีเมลฟิชชิง	20
บทที่ 5 อภิปรายสรุปผลและข้อเสนอแนะ	33
5.1 ปัญหาและข้อจำกัด	33
5.2 สรุปผล	34
5.3 ข้อเสนอแนะและแนวทางการปฏิบัติ	34
เอกสารอ้างอิง	35
ภาคผนวก	37
ประวัติผู้วิจัย	55

สารบัญตาราง

ตารางที่	หน้า
ผลการจำลองการโจมตีครั้งที่ 1	26
ผลการจำลองการโจมตีครั้งที่ 2	32

สารบัญรูปภาพ

ภาพที่ หน้า

3-1 วิธีการดำเนินการวิจัย 10

3-2 CanIPhish 11

3-2 CanIPhish (2) 11

3-3 ฟังก์ชั่นการฝึกอบรมและสร้างความตระหนัก 12

3-4 เครื่องมือที่ใช้มีการประเมินความเสี่ยง 12

3-5 เครื่องมือที่ใช้มีมีนโยบายและการปฏิบัติตาม 13

3-6 การติด QR Code หน้าบริษัท 14

3-7 รูปแบบอีเมลปลอม 14

3-8 การเลือกหัวข้อที่มีความน่าสนใจ 15

3-9 การออกแบบเนื้อหาที่มีการนำเสนอสิทธิประโยชน์ 15

3-10 การออกแบบเนื้อหาให้เสมือนเป็นการมอบหมายงานจากหัวหน้างาน 16

3-11 การสร้างปุ่มเชื่อมโยงไปหน้าเว็บไซต์ปลอม 16

3-11 การสร้างปุ่มเชื่อมโยงไปหน้าเว็บไซต์ปลอม (ต่อ) 16

3-12 การทดสอบการส่งอีเมล 17

3-13 ตัวอย่างหลักสูตรที่ใช้อบรม 18

3-13 ตัวอย่างหลักสูตรที่ใช้อบรม (ต่อ) 18

3-13 ตัวอย่างหลักสูตรที่ใช้อบรม (ต่อ) 18

4-1 รูปแบบอีเมลฟิชชิง ครั้งที่ 1 21

4-2 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Office of Managing Director ครั้งที่ 1 22

4-3 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Back Office ครั้งที่ 1 22

4-4 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Technical Support ครั้งที่ 1 23

4-5 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Channel Sales ครั้งที่ 1 23

4-6 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Project Sales ครั้งที่ 1 24

4-7 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม Project Management ครั้งที่ 1 24

4-8 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม NVK48 และNVK AI ครั้งที่ 1 25

4-9 รูปแบบQR Code ครั้งที่ 1 25

4-10 แผนภูมิแสดงผลการทดสอบ ครั้งที่ 1 26

4-11 รูปแบบอีเมลฟิชชิง ครั้งที่ 2 27

สารบัญรูปภาพ (ต่อ)

ภาพที่ หน้า

4-12 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Office of Managing Director ครั้งที่ 2 28

4-13 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Back Office ครั้งที่ 2 28

4-14 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Technical Support ครั้งที่ 2 29

4-15 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Channel Sales ครั้งที่ 2 29

4-16 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Project Sales ครั้งที่ 2 30

4-17 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม Project Management ครั้งที่ 2 30

4-18 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม NVK48 และNVK AI ครั้งที่ 2 31

4-19 รูปแบบQR Code ครั้งที่ 2 31

4-20 แผนภูมิแสดงผลการทดสอบ ครั้งที่ 2 32

5-1 การรับรองการปฏิบัติตามของผู้ให้บริการ 33

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในโลกอินเทอร์เน็ตที่กว้างใหญ่ที่ข้อมูลไหลเวียนอิสระ และการเชื่อมต่อเกิดขึ้นในเสี้ยววินาที มีการโจมตีที่เรียกว่า ฟิชชิง (Phishing) ซึ่งเริ่มต้นในช่วงทศวรรษ 1990 จากการใช้งานอีเมลที่แพร่หลาย ฟิชชิงเป็นการโจมตีที่ถูกพัฒนาขึ้นมาโดยผู้ไม่ประสงค์ดีโดยอาศัยการส่งข้อมูลหลอกลวงโดยอ้างเป็นองค์กรที่เชื่อถือได้เพื่อหลอกล่อผู้ใช้ที่ไม่สงสัยให้เปิดเผยข้อมูลสำคัญ เช่น ข้อมูลการเข้าสู่ระบบ หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ ปรากฏการณ์ของฟิชชิงได้เติบโตขึ้นพร้อม ๆ กับการปฏิวัติดิจิทัล อีเมลที่อ้างว่ามาจากสถาบันที่ถูกต้อง เช่น ธนาคารหรือบริษัทที่มีชื่อเสียง ถูกออกแบบมาเพื่อกระตุ้นให้เกิดความตกใจและความกลัว กระตุ้นให้เกิดการกระทำที่สูญเสียความปลอดภัยส่วนบุคคลและองค์กร การโจมตีเหล่านี้ไม่เพียงแต่ทำให้เกิดการสูญเสียทางการเงินเท่านั้น แต่ยังสร้างความเสื่อมเสียในความเชื่อมั่นในช่องทางการสื่อสารดิจิทัล และมีผลกระทบอย่างมากต่อความเป็นส่วนตัวและความปลอดภัยของข้อมูลส่วนตัว

ด้วยเหตุนี้ การค้นคว้าอิสระครั้งนี้จึงมีสองเป้าหมาย คือ (1) ประเมินความเสี่ยงและวิเคราะห์หามาตรการเพื่อป้องกันไม่ให้เกิดความเสี่ยงจากการถูกโจมตีโดยการฟิชชิงโดยใช้วิธีการทดลองฟิชชิงผ่านมุมมองหลายด้าน โดยมุ่งหวังที่จะเปิดเผยลักษณะที่ทำให้การหลอกลวงเหล่านี้ให้ไม่ประสบความสำเร็จ นอกจากนี้ ผลจากการทดสอบฟิชชิงในองค์กรนี้จะช่วยเสริมสร้างความตระหนักรู้ในการป้องกันภัยคุกคามทางไซเบอร์ (2) กำหนดหลักสูตรการฝึกอบรมด้านไซเบอร์ที่เหมาะสมสำหรับผู้ใช้อินเทอร์เน็ตทุกระดับ วัตถุประสงค์สูงสุด คือ การสร้างความตระหนักรู้ให้กับชุมชนดิจิทัล เพื่อป้องกันภัยคุกคามด้วยความรู้และเครื่องมือเพื่อให้มีความรู้และสามารถป้องกันตัวจากการล่อลวงของการหลอกลวงแบบฟิชชิง

ในการดำเนินการค้นคว้าอิสระนี้ ผู้วิจัยสำรวจการหลอกลวงแบบฟิชชิง แนวคิดการโจมตีแบบต่าง ๆ และกลยุทธ์ทางจิตวิทยา เพื่อนำมาใช้ทดสอบการโจมตีในบริษัทเอกชนแห่งหนึ่งเป็นกรณีศึกษา และประเมินความเสี่ยงที่เกิดจากการโจมตีเหล่านี้เพื่อนำมาออกแบบหลักสูตรและทำการฝึกอบรมผ่านการวิเคราะห์ข้อมูลและการทบทวนอย่างละเอียด โดยการศึกษานี้จะนำทางไปสู่อนาคตที่ปลอดภัยในโลกดิจิทัลที่บุคลากรในองค์กรจะมีการใช้งานในโลกออนไลน์แบบรู้เท่าทันและมีความมั่นใจ และสามารถที่จะหลีกเลี่ยงกับดักที่กำหนดโดยอาชญากรไซเบอร์ได้อย่างชาญฉลาด

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อประเมินระดับความเสี่ยงของภัยคุกคามฟิชชิงในบริษัทขนาดเล็ก

1.2.2 เพื่อพัฒนาหลักสูตรการฝึกอบรมด้านความปลอดภัยไซเบอร์สำหรับพนักงาน เพื่อลดความเสี่ยงในการถูกโจมตีในรูปแบบฟิชชิง

1.3 ขอบเขตของการวิจัย

1.3.1 กลุ่มตัวอย่างจำนวน 46 คน ซึ่งเป็นพนักงานของบริษัทเอกชนแห่งหนึ่ง

1.3.2 ขอบเขตของรูปแบบการทดสอบการโจมตีด้วยวิธีฟิชชิง

1.3.2.1 การทดสอบฟิชชิงแบบทั่วไปทำการทดสอบโดยการส่งอีเมลปลอมที่มีลักษณะของการหลอกลวงฟิชชิงแบบทั่วไป ซึ่งไม่ได้เจาะจงเป้าหมายเฉพาะ แต่มุ่งหวังที่จะหลอกล่อให้ผู้รับอีเมลปลอมเปิดลิงค์หรือแนบไฟล์ที่อาจนำไปสู่การขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางธุรกิจ

1.3.2.2 การทดสอบฟิชชิงแบบเจาะจง (Spear phishing) ทำการทดสอบการหลอกลวงด้วยอีเมลที่ออกแบบมาเพื่อเป็นเป้าหมายเฉพาะตามแผนกต่าง ๆ ได้แก่ แผนกบัญชี, พนักงานขาย, พนักงานขายแบบโครงการ, ทีมบริหาร, ทีมสนับสนุน, และทีมบริหารโครงการ เพื่อศึกษาว่าการทำการฟิชชิงที่เจาะจงมากขึ้นจะมีประสิทธิภาพและมีการตอบสนองอย่างไรจากพนักงานในแต่ละส่วน

1.3.2.3 การทดสอบโดยใช้ QR Code ทดสอบการหลอกลวงด้วยการใช้ QR Code ที่ติดตั้งที่หน้าตึกของบริษัท เพื่อดูว่าพนักงานจะมีการตอบสนองอย่างไรต่อวิธีการหลอกลวงที่ไม่ใช่ดิจิทัลโดยตรง แต่เป็นการใช้เทคโนโลยีในการเชื่อมต่อไปยังเนื้อหาหรือแอปพลิเคชันที่อาจเป็นอันตราย

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 การตระหนักถึงความเสี่ยง : บริษัทจะได้รับความรู้เกี่ยวกับความเสี่ยงที่เกี่ยวข้องกับการถูกโจมตีด้วยภัยคุกคามแบบฟิชชิงทำให้บริษัทสามารถรับรู้และเข้าใจถึงวิธีการที่อาชญากรไซเบอร์อาจใช้เพื่อหลอกลวงพนักงานให้เปิดเผยข้อมูลสำคัญ ความรู้นี้จะช่วยให้บริษัทสามารถปรับปรุงแผนการป้องกันและความพร้อมในการรับมือกับภัยคุกคามเหล่านี้ได้ดียิ่งขึ้น

1.4.2 การเพิ่มความรู้และความเข้าใจของพนักงาน : พนักงานจะได้รับความรู้และความเข้าใจเกี่ยวกับการหลอกลวงแบบฟิชชิงรวมถึงวิธีการต่าง ๆ ที่ใช้ในการดำเนินการโจมตี การเรียนรู้เหล่านี้จะทำให้พวกเขาสามารถระบุและหลีกเลี่ยงการหลอกลวงได้อย่างมีประสิทธิภาพ เพิ่มความสามารถในการป้องกันตนเองและบริษัทจากความเสียหายที่อาจเกิดขึ้น

1.4.3 การลดความเสี่ยงจากการโจมตี : ด้วยความรู้และความเข้าใจที่เพิ่มขึ้นของทั้งบริษัทและพนักงาน ความเสี่ยงในการถูกโจมตีด้วยภัยคุกคามแบบฟิชชิงจะลดลงอย่างมีนัยสำคัญ การฝึกอบรม

และการตระหนักเกี่ยวกับภัยคุกคามนี้จะช่วยสร้างวัฒนธรรมความปลอดภัยที่แข็งแกร่งภายในองค์กร ลดโอกาสที่พนักงานจะตกเป็นเหยื่อของการหลอกลวงและป้องกันความเสียหายต่อข้อมูลและทรัพย์สินทางปัญญา

1.4.4 การประยุกต์ใช้เอกสารการอบรมเพื่อการพัฒนาต่อเนื่อง : เอกสารและคู่มือที่ใช้ในการอบรมเป็นเครื่องมือสำหรับการสอนหลังจากการทดสอบครั้งแรก และทางผู้วิจัยหวังว่าสามารถนำไปใช้การอบรมพนักงานใหม่ รวมทั้งเป็นแหล่งข้อมูลที่สำคัญสำหรับการทบทวนความรู้อย่างสม่ำเสมออย่างสม่ำเสมอ โดยที่สามารถย้อนกลับมาศึกษาและทบทวนข้อมูลที่ได้รับจากการอบรมเพื่อรักษาความเข้มแข็งของมาตรฐานการปฏิบัติงาน และยังช่วยให้สามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างต่อเนื่องและมีประสิทธิภาพ

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

ในโลกยุคดิจิทัลที่สังคมออนไลน์เป็นส่วนหนึ่งของชีวิต การฟิชชิงเป็นหนึ่งในภัยคุกคามทางไซเบอร์ที่ผู้ใช้งานต้องมีความตระหนักรู้เพื่อปกป้องข้อมูลส่วนตัว การฟิชชิงคือวิธีการหลอกลวงที่มิจฉาชีพจะสร้างข้อความหรืออีเมลที่ดูเหมือนมาจากหน่วยงานที่น่าเชื่อถือ เช่น ธนาคารหรือหน่วยงานรัฐโดยมีวัตถุประสงค์เพื่อหลอกลวงให้เชื่อและทำการกรอกข้อมูลสำคัญ เช่น หมายเลขบัตรเครดิตหรือรหัสผ่าน ซึ่งสามารถนำไปสู่การสูญเสียทางการเงินหรือการละเมิดข้อมูลส่วนบุคคลได้

งานวิจัยของ Al-Qahtani และ Cresci (2022) ได้เปิดเผยว่า สถานการณ์การระบาดของโควิด-19 ได้ทำให้การโจมตีแบบฟิชชิงเพิ่มขึ้น เนื่องจากผู้คนหันมาทำงานและใช้ชีวิตออนไลน์มากขึ้น ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) การระบุและเข้าใจภัยคุกคามทางไซเบอร์ (Cyber Threat) รวมถึงการมีความตระหนักรู้ทางไซเบอร์ (Cybersecurity Awareness) จึงเป็นเครื่องมือที่จำเป็นในการเสริมความเข้าใจและเตรียมความพร้อมในการป้องกันตนเองจากการโจมตี ไม่ว่าจะเป็นการตรวจสอบอีเมลอย่างระมัดระวัง การไม่เปิดลิงก์ที่ไม่เชื่อถือได้ หรือการใช้มาตรการด้านความปลอดภัยที่เข้มข้น ผู้ใช้งานจึงสามารถใช้งานออนไลน์อย่างมั่นใจและปลอดภัยท่ามกลางการกระทำของตนเองในทุก ๆ ด้าน

2.1.1 ฟิชชิง (Phishing) หมายถึง เทคนิคที่ผู้ไม่ประสงค์ดีใช้เพื่อหลอกลวงและขโมยข้อมูลส่วนตัวจากผู้ใช้ โดยใช้วิธีการปลอมแปลงเว็บไซต์ อีเมล หรือข้อความทางสังคมออนไลน์ โดยมีเป้าหมายเพื่อล่อเอาข้อมูลที่มักเป็นข้อมูลส่วนตัว เช่น ชื่อผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลการเข้าสู่ระบบอื่น ๆ ตัวอย่างการล่อเอาข้อมูล เช่น ผู้ไม่ประสงค์ดีอาจสร้างเว็บไซต์ปลอมที่มีลักษณะคล้ายกับเว็บไซต์ธนาคารเป้าหมาย และส่งอีเมลหรือข้อความให้กับผู้ใช้โดยแสดงเหตุผล เช่น การตรวจสอบบัญชี การปรับปรุงระบบ หรือโปรโมชันพิเศษ และให้ผู้ใช้คลิกลิงก์เข้าสู่เว็บไซต์ปลอมเพื่อทำให้ผู้ไม่ประสงค์ดีสามารถเอาข้อมูลส่วนตัวของผู้ใช้ได้โดยไม่รู้ตัว มาตรการป้องกันของการล่อเอาข้อมูลที่นิยม คือ การอบรมและเสริมสร้างการรับรู้ทางไซเบอร์ให้กับผู้ใช้ โดยการเรียนรู้เกี่ยวกับเทคนิคที่ใช้ในการล่อเอาข้อมูลและระวังการแชร์ข้อมูลส่วนตัวผ่านทางอินเทอร์เน็ต โดยไม่ระมัดระวัง

2.1.2 ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) เป็นการป้องกันและรักษาความปลอดภัยของข้อมูล ระบบ และเครือข่ายคอมพิวเตอร์ การโจมตีด้านเทคโนโลยีสารสนเทศ เช่น ไวรัสคอมพิวเตอร์ จากการโจมตีด้านความมั่นคงปลอดภัยทางเครือข่าย เช่น การบุกรุกเข้าสู่ระบบหรือกระทำให้ระบบหยุดทำงานชั่วขณะ โดยไม่ได้รับอนุญาต มีแนวทางดังนี้

2.1.2.1 การประสานงานกับผู้ให้บริการระบบคอมพิวเตอร์ : การใช้บริการระบบคอมพิวเตอร์ที่มีความมั่นคงปลอดภัยสูง เช่น การเก็บข้อมูลในคลังข้อมูลบนคลาวด์ที่มีการเข้ารหัสข้อมูลอย่างเข้มงวด

2.1.2.2 การอัปเดตระบบปฏิบัติการและโปรแกรม : การอัปเดตระบบปฏิบัติการและโปรแกรมอย่างสม่ำเสมอช่วยให้ระบบคอมพิวเตอร์มีความปลอดภัยมากขึ้น และป้องกันการโจมตีที่เกิดขึ้นจากช่องโหว่ในระบบ

2.1.3 ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง สิ่งที่ผู้ไม่ประสงค์ดีสร้างขึ้นมาเพื่อทำให้ระบบคอมพิวเตอร์หรือเครือข่ายทางไซเบอร์เสียหายหรือทำลายข้อมูล มักจะมีจุดประสงค์หลายประการ เช่น การขโมยข้อมูลส่วนตัว เพื่อเจาะระบบ เพื่อขโมยเงินหรือข้อมูลการเงิน หรือเพื่อก่อกวนการใช้งานของระบบคอมพิวเตอร์ โดยส่วนใหญ่เป้าหมายที่ถูกโจมตีมักเป็นบุคคล องค์กร หรือระบบคอมพิวเตอร์ที่มีข้อมูลสำคัญ ตัวอย่างของภัยคุกคามทางไซเบอร์ เช่น

2.1.3.1 ไวรัสคอมพิวเตอร์ : โปรแกรมคอมพิวเตอร์ที่ถูกสร้างขึ้นเพื่อทำความเสียหายหรือขโมยข้อมูลจากเครื่องคอมพิวเตอร์ที่ติดเชื้อ

2.1.3.2 การเข้าถึงไม่รับอนุญาต : การใช้เทคนิคต่าง ๆ เช่น การเดารหัสผ่าน การโจมตีช่องโหว่ในระบบ เพื่อเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาต

2.1.3.3 การปลอมแปลงเว็บไซต์ : การสร้างเว็บไซต์ปลอมที่มีลักษณะคล้ายกับเว็บไซต์จริงเพื่อล่อให้ผู้ใช้ป้อนข้อมูลส่วนตัว เช่น ชื่อผู้ใช้และรหัสผ่าน

2.1.3.4 การเป็นเจ้าของบัญชีผู้ใช้ : โจมตีเพื่อครอบครองบัญชีผู้ใช้ และใช้บัญชีนั้น เพื่อประโยชน์ต่าง ๆ อย่างไม่ถูกต้อง เช่น การส่งข้อความสแปม การโพสต์ข้อความเจาะข้อมูล หรือการขายบัญชีผู้ใช้ให้ผู้อื่น

2.1.4 ความตระหนักรู้ทางไซเบอร์ (Cybersecurity Awareness) หมายถึง การเข้าใจและตระหนักถึงความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและการใช้เทคโนโลยี การเสริมสร้างความตระหนักรู้ทางไซเบอร์เป็นส่วนสำคัญในการป้องกันการโจมตีทางไซเบอร์และการรักษาความปลอดภัยในระบบคอมพิวเตอร์ ความตระหนักรู้ทางไซเบอร์มีความสำคัญอย่างมาก เพราะเป็นปัจจัยช่วยให้ผู้ใช้เข้าใจถึงอันตรายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีอย่างไม่ระมัดระวัง นอกจากนี้การเสริมสร้างความตระหนักรู้ทางไซเบอร์ยังช่วยให้คนมีความรอบคอบและรู้จักป้องกันตัวเองและองค์กร ตัวอย่างของวิธีการเสริมสร้างความตระหนักรู้ทางไซเบอร์ เช่น

2.1.4.1 การอบรมและการฝึกปฏิบัติ : การจัดอบรมและการฝึกปฏิบัติให้กับพนักงานและผู้ใช้ทั่วไปเกี่ยวกับเรื่องความมั่นคงปลอดภัยทางไซเบอร์ เช่น วิธีการรู้เหตุการณ์ของการโจมตี วิธีการระบุและป้องกันการล่อเอาข้อมูล เป็นต้น

2.1.4.2 การแจ้งเตือนและการแชร์ข้อมูล : การแจ้งเตือนผู้ใช้เกี่ยวกับอันตรายทางไซเบอร์และการแชร์ข้อมูลเกี่ยวกับวิธีการป้องกันและการระบุการโจมตีที่เกี่ยวข้อง

2.1.4.3 การใช้เทคโนโลยีสนับสนุนการสร้างความตระหนักรู้ : การใช้เทคโนโลยีเพื่อส่งเสริมการรับรู้ทางไซเบอร์ รวมถึงการใช้โปรแกรมคอมพิวเตอร์ แอปพลิเคชันมือถือ หรือระบบการเรียนการสอนออนไลน์เพื่อสร้างความเข้าใจเกี่ยวกับความปลอดภัยทางไซเบอร์และเทคนิคที่ใช้ในการป้องกันการโจมตี

2.2 งานวิจัยที่เกี่ยวข้อง

Al-Qahtani และ Cresci (2022) ได้ศึกษาและชี้ให้เห็นว่าการระบาดของโควิด-19 ส่งผลให้เกิดการโจมตีด้วยฟิชชิงมากขึ้น ฟิชชิงคือ กลวิธีหลอกลวงทางออนไลน์เพื่อขโมยข้อมูลส่วนตัว เช่น บัตรเครดิตหรือรหัสผ่าน มิจฉาชีพมักส่งอีเมลหรือข้อความปลอม โดยแอบอ้างเป็นหน่วยงานน่าเชื่อถือ เช่น ธนาคารหรือหน่วยงานรัฐ บทความยังแนะนำวิธีป้องกันฟิชชิง เช่น การระมัดระวังอีเมลที่เปิดและลิงก์ที่คลิก สรุปคือ โควิด-19 ทำให้ฟิชชิงเพิ่มขึ้น ผู้ใช้งานควรตระหนักและป้องกันตัวเองด้วยการใช้อินเทอร์เน็ตอย่างปลอดภัย

ภัยคุกคามจากการโจมตีแบบฟิชชิงเพิ่มขึ้นบนแพลตฟอร์มมือถือ ซึ่งมีความเปราะบางเป็นพิเศษเนื่องจากข้อจำกัดของอุปกรณ์และพฤติกรรมการใช้งานของผู้ใช้ การโจมตีแบบฟิชชิงมีเป้าหมายเพื่อขโมยข้อมูลสำคัญโดยปลอมตัวเป็นหน่วยงานที่เชื่อถือได้ วิธีการตรวจจับแบบดั้งเดิม เช่น การกำหนดรายชื่อไม่ได้รับอนุญาตและรายชื่อที่ได้รับอนุญาต การเรียนรู้ของเครื่อง และภาพที่มีความคล้ายคลึงแต่มีข้อจำกัด คือ ข้อมูลที่ล้าสมัย จำนวนชุดข้อมูลที่จำกัด ส่งผลให้ไม่สามารถตรวจจับภัยคุกคามได้และต้นทุนที่สูง เพื่อเอาชนะความท้าทายเหล่านี้ Zakarya และคณะ (2020) นำเสนอกลยุทธ์ต่อต้านฟิชชิงใหม่ที่เน้นการตรวจจับลิงก์ฟิชชิงที่นำไปสู่หน้าล็อกอินที่ไม่สมบูรณ์ วิธีการผสมผสานนี้รวมข้อดีของวิธีการรายชื่อที่ไม่ได้รับอนุญาตกับเทคนิคใหม่สองวิธี คือการตรวจจับหน้าเว็บและการใช้ข้อมูลปลอม กระบวนการตรวจจับประกอบด้วยสามขั้นตอน เพื่อระบุภัยคุกคามฟิชชิงใหม่ ผลการทดลองแสดงให้เห็นว่าวิธีการนี้มีประสิทธิภาพเหนือกว่าเครื่องมือต่อต้านฟิชชิงอื่นในท้องตลาด

Chen และคณะ (2020) นำเสนอวิธีการตรวจจับเว็บไซต์ฟิชชิงโดยการวิเคราะห์ลักษณะทางภาพโดยจัดหมวดหมู่เว็บไซต์ตามระดับความคล้ายคลึงกับเว็บไซต์ที่ถูกต้อง และการวิเคราะห์แฮชวอล์เล็ต (wHash) ร่วมกับการวิเคราะห์ฮิสโตแกรมสี เพื่อประเมินความคล้ายคลึงกัน สำหรับเว็บไซต์คล้ายกันพอสมควรใช้เทคนิค Scale-Invariant Feature Transform (SIFT) โดยเน้นหลักในการตรวจจับ

เว็บไซต์ฟิชชิงที่คล้ายกันมาก และคล้ายกันพอสมควร ผลการทดลองแสดงให้เห็นว่าวิธีการ wHash ร่วมกับการวิเคราะห์ฮิสโตแกรมสีมีประสิทธิภาพเหนือกว่าการแฮชที่สัมพันธ์กับการรับรู้ (pHash) ในด้านความแม่นยำโดยเฉพาะอย่างยิ่ง เทคนิค SIFT บรรลุความแม่นยำ 97.93%, 98.61%, และ 99.95% สำหรับเว็บไซต์ฟิชชิงที่เลียนแบบ Microsoft, Dropbox และ Bank of America ตามลำดับ

Huynh และคณะ (2017) ได้ศึกษาและเสนอแนวทางใหม่ในการประเมินความเสี่ยงที่ผู้ใช้จะตกเป็นเหยื่อของการโจมตีแบบฟิชชิงซึ่งต่างจากการฝึกอบรมแบบเดิมที่อาศัยความสมัครใจ บทความนี้นำเสนอวิธีการทดสอบโดยส่งอีเมลปลอมที่ดูเหมือนจริงและบันทึกการตอบกลับของผู้ใช้ วิธีการนี้มีจุดประสงค์เพื่อประเมินพฤติกรรมของผู้ใช้จริงและวัดประสิทธิภาพของโปรแกรมการศึกษาการประกันข้อมูลสารสนเทศขององค์กร บทความนี้เน้นข้อควรคำนึงและกระบวนการในการสร้างและการใช้อุปกรณ์ประเมินพิเศษนี้ โดยนำเสนอข้อมูลเชิงลึกสำหรับองค์กรที่ต้องการเสริมสร้างความแข็งแกร่งด้านไซเบอร์ผ่านการให้ความรู้แก่ผู้ใช้

Hota และคณะ (2018) นำเสนอวิธีการที่ในการตรวจจับอีเมลฟิชชิงโดยใช้โมเดลการเรียนรู้ของเครื่องแบบผสม ซึ่งรวมเทคนิคการเลือกคุณลักษณะที่ถูกลบและแทนที่ Remove-Replace Feature Selection Technique (RRFST) โดยเทคนิค RRFST ทำงานโดยการเลือกคุณสมบัติแบบสุ่มและจะลบออกหากการลบไม่มีการเปลี่ยนแปลงหรือปรับปรุงความแม่นยำของโมเดล มิฉะนั้นคุณสมบัตินั้นจะถูกเก็บไว้ นอกจากนี้ยังได้พัฒนาตัวจำแนกประเภทโดยอิงจากอัลกอริทึมต้นไม้การตัดสินใจสองแบบ คือ C4.5 และ CART ซึ่งผลแสดงให้เห็นว่าสามารถลดชุดคุณลักษณะได้อย่างมีประสิทธิภาพโดยยังคงรักษาความแม่นยำสูง

Brij และคณะ (2021) ได้ศึกษาเกี่ยวกับการจัดการกับปัญหาการปลอมแปลง URL ในการโจมตีแบบฟิชชิงที่ยังคงมีอยู่อย่างต่อเนื่อง โดยเสนอโมเดลการเรียนรู้เชิงลึกแบบผสมที่รวมเครือข่ายประสาทเทียมแบบคอนโวลูชันนัล (CNN) และเครือข่าย Long Short-Term Memory (LSTM) ด้วยข้อจำกัดของรายชื่อที่ไม่ได้รับอนุญาตแบบดั้งเดิมและความท้าทายเฉพาะในการตรวจจับ URL ที่เป็นอันตรายที่ซับซ้อน การวิจัยนี้สำรวจศักยภาพของการทำงานร่วมกันระหว่าง CNN สำหรับการเรียนรู้คุณลักษณะและ LSTM สำหรับการเข้าใจความสัมพันธ์บริบทในข้อความ URL โมเดลผสมนี้ได้รับการทดสอบบนชุดข้อมูลสาธารณะสองชุด ได้แก่ UCL spoofing Website และ PhishTank โดยได้ความแม่นยำที่ 98.9% และ 96.8% ตามลำดับ ซึ่งโดดเด่นกว่าประสิทธิภาพของโมเดล CNN และ LSTM ที่ทำงานเดี่ยว ๆ ผลลัพธ์เหล่านี้สนับสนุนการใช้งานวิธีการผสมผสานระหว่าง CNN และ LSTM เพื่อต่อสู้กับการปลอมแปลง URL และเสริมสร้างมาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่อการโจมตีแบบฟิชชิ่ง (Phishing)

Aldawood และ Skinner (2019) ได้ศึกษาและทำให้เห็นว่า แม้จะมีการลงทุนด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้น แต่พนักงานหลายคนยังขาดความรู้ในการป้องกันตัวเองจากกลอุบายทางสังคม

แฮ็กเกอร์ยังคงสามารถขโมยข้อมูลสำคัญจากองค์กรได้ แม้จะมีมาตรการป้องกันไซเบอร์ขั้นสูง ปัจจัยหลายอย่างส่งผลต่อความสามารถของผู้ใช้ในการตรวจจับและลดภัยคุกคามทางไซเบอร์ เช่น สภาพแวดล้อมทางธุรกิจ ปัจจัยทางสังคม และปัจจัยส่วนบุคคล เครื่องมือป้องกันไซเบอร์แบบดั้งเดิมและแบบใหม่มีข้อจำกัด องค์กรจำเป็นต้องพัฒนาวิธีการฝึกอบรมพนักงานและป้องกันตัวเองจากการโจมตีทางไซเบอร์ที่มีประสิทธิภาพมากขึ้น งานวิจัยเน้นย้ำถึงความสำคัญของทรัพยากรบุคคลด้านความปลอดภัยทางไซเบอร์และความจำเป็นที่องค์กรต้องลงทุนด้านการฝึกอบรมและการศึกษาเพื่อปกป้องตัวเองจากการโจมตีทางไซเบอร์

Hijji และ Alam (2022) ได้ศึกษาเกี่ยวกับกรอบการสร้างความตระหนักและการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Awareness Training: CAT) สำหรับพนักงานที่ทำงานทางไกล บทความนี้กล่าวถึงความสำคัญของการสร้างความตระหนักและการฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับองค์กรต่าง ๆ ระหว่างการแพร่ระบาดของโควิด-19 และยังให้รายละเอียดเกี่ยวกับการพัฒนาและประเมินกรอบงาน CAT ซึ่งครอบคลุมสามตัวชี้วัด ได้แก่ ปัญญาประดิษฐ์ การวัดความรู้เชิงปรับตัว และระดับความสามารถ ผลการศึกษาแสดงให้เห็นว่ากรอบงาน CAT มีประสิทธิภาพในการปรับปรุงการสร้างความตระหนักและการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ของพนักงาน

Rendall และคณะ (2020) เสนอกรอบการตรวจจับหลายชั้นที่ทำการจำแนกประเภทต่อโดเมนที่น่าสงสัยโดยใช้ชุดคุณสมบัติที่หลากหลาย การจำแนกประเภทเพิ่มเติมนี้จะเกิดขึ้นหากความมั่นใจของการประเมินเบื้องต้นอยู่ต่ำกว่าเกณฑ์ที่ผู้ดูแลระบบตั้งไว้ ผู้เขียนได้นำเสนอและทดสอบระบบการตรวจจับสองชั้นโดยใช้การเรียนรู้ของเครื่องแบบมีผู้ดูแลระบบและได้ประเมินผลด้วยชุดข้อมูลของการโจมตีแบบฟิชชิงที่กำลังใช้งาน ผลลัพธ์แสดงให้เห็นว่าประสิทธิภาพของระบบนี้เทียบเท่ากับโซลูชันชั้นนำในปัจจุบัน

Al-Ahmadi และคณะ (2022) เสนอโมเดลการตรวจจับฟิชชิงที่เรียกว่า PDGAN ซึ่งขึ้นอยู่กับ Uniform Resource Locator (URL) ของเว็บไซต์โดยใช้เครือข่าย Long Short-Term Memory (LSTM) เป็นตัวสร้าง URL ฟิชชิงเทียมและใช้เครือข่าย Convolutional Neural Network (CNN) เป็นตัวตัดสินว่า URL นั้นเป็นฟิชชิงหรือไม่ โดยใช้ชุดข้อมูลที่มี URL เกือบสองล้านรายการจาก PhishTank และ DomCop ผลการทดลองแสดงให้เห็นว่า PDGAN มีความแม่นยำในการตรวจจับได้ถึง 97.58% และความแม่นยำ 98.02% โดยไม่ต้องพึ่งพาบริการจากบุคคลที่สามและมีความแม่นยำมากกว่าโมเดลอื่น ๆ

Sadiq และ คณะ (2021) ได้ศึกษาว่าความก้าวหน้าในอุตสาหกรรม 4.0 อาชญากรรมไซเบอร์ในแอปพลิเคชันธุรกิจที่ใช้อินเทอร์เน็ตกำลังเพิ่มขึ้นอย่างรวดเร็ว เพื่อรับมือกับการโจมตีเหล่านี้ ผู้รุกรานใช้เครื่องมือและเทคนิคต่าง ๆ เช่น ฟิชชิง, มัลแวร์, SQL Injection, Ransomware, Cross-Site Scripting (XSS), Denial of Service (DoS), การแฮ็กเซสชัน (Session Hijacking) และการใช้ข้อมูล

รับรองซ้ำ (Credential Reuse) ฟิชชิงเป็นวิธีที่พบมากที่สุดในยุคดิจิทัลปัจจุบัน ประเภทของการโจมตีไซเบอร์เหล่านี้ใช้เพื่อทำร้ายบุคคลหรือธุรกิจทั้งหมดขึ้นอยู่กับวัตถุประสงค์ที่ต้องการของผู้โจมตี เพื่อต่อสู้กับการโจมตีเหล่านี้ ชุมชนการวิจัยได้ให้เทคนิคการตรวจจับฟิชชิงไว้หลายวิธี

Alharbi และ Tassaddi (2021) ได้ศึกษาเกี่ยวกับความตระหนักด้านความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัยมัจมาห์ ผลการศึกษาพบว่า นักศึกษามีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับปานกลาง แต่ยังขาดความตระหนักและพฤติกรรมในการป้องกันตัวเอง ดังนั้น ผู้วิจัยเสนอแนะให้มีการส่งเสริมการเรียนรู้ด้านความปลอดภัยทางไซเบอร์ในหลักสูตรการศึกษาและรณรงค์สร้างความตระหนักให้กับนักศึกษาอย่างต่อเนื่อง

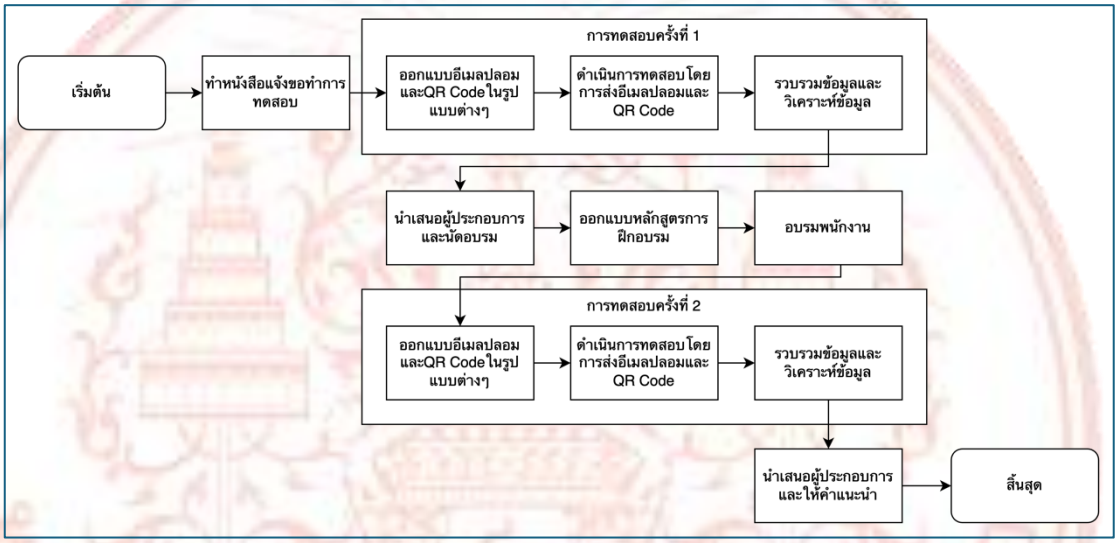
Dong และคณะ (2008) นำเสนอการตรวจจับเว็บไซต์ฟิชชิงซึ่งพิจารณาจากพฤติกรรมออนไลน์ของผู้ใช้งาน นั่นคือ เว็บไซต์ที่ผู้ใช้เยี่ยมชมและข้อมูลที่ผู้ใช้ส่งไปยังเว็บไซต์เหล่านั้น พฤติกรรมของผู้ใช้เหล่านี้ไม่สามารถถูกควบคุมหรือแก้ไขได้อย่างอิสระโดยผู้โจมตี การตรวจจับที่อิงจากข้อมูลเหล่านี้ไม่เพียงแต่สามารถบรรลุความแม่นยำสูงได้ แต่ยังมีความยืดหยุ่นพื้นฐานในการต่อสู้กับวิธีการหลอกลวงที่เปลี่ยนแปลงไป

สรุปผลการวิจัยและการศึกษาหลากหลายที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เรียกว่า “ฟิชชิง” ซึ่งเป็นวิธีการหลอกลวงเพื่อขโมยข้อมูลสำคัญผ่านทางอินเทอร์เน็ต เช่น ข้อมูลการเข้าสู่ระบบ หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ โดยทั่วไป การโจมตีแบบฟิชชิงมักเกิดจากการส่งอีเมลหลอกลวงที่ดูเหมือนมาจากแหล่งที่เชื่อถือได้ และบางครั้งก็รวมไปถึงการสร้างเว็บไซต์ปลอมที่ลอกเลียนแบบเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้ใส่ข้อมูลส่วนบุคคล ความสำคัญของการวิจัยเหล่านี้อยู่ที่การพัฒนาเทคนิคและเครื่องมือใหม่ ๆ เพื่อต่อสู้กับการโจมตีที่มีความซับซ้อนมากขึ้น การสร้างความตระหนักและฝึกอบรมผู้ใช้อินเทอร์เน็ตให้รู้จักป้องกันตัวเองจากภัยคุกคามเหล่านี้จากการพึ่งพาเทคโนโลยีเพิ่มมากขึ้น อีเมลและเว็บไซต์เป็นช่องทางหลักที่ผู้ใช้จะติดต่อสื่อสารและดำเนินการทางธุรกิจ การทำให้มั่นใจว่าข้อมูลของพวกเขาปลอดภัยจึงเป็นเรื่องสำคัญ ผลการวิจัยที่ถูกสรุปในวิจัยนี้ยังชี้ไปที่การพัฒนาวิธีการที่ซับซ้อนมากขึ้น เช่น การใช้เครื่องมือทางคณิตศาสตร์และปัญญาประดิษฐ์ (AI) เพื่อตรวจจับและป้องกันภัยคุกคามที่เกี่ยวข้องกับฟิชชิง นอกจากนี้ยังรวมถึงการสร้างและการประเมินโปรแกรมการศึกษาเพื่อสร้างความตระหนักในเรื่องความปลอดภัยทางไซเบอร์ให้กับพนักงาน โดยเฉพาะในช่วงที่การทำงานทางไกลกลายเป็นเรื่องปกติในหลายองค์กรจากการแพร่ระบาดของ COVID-19

บทที่ 3
วิธีดำเนินการวิจัย

3.1 วิธีดำเนินการวิจัย

ในการดำเนินการวิจัย ขั้นตอนการออกแบบ และวิธีการ ประกอบด้วยรายละเอียดดังต่อไปนี้ ดังภาพที่ 3-1

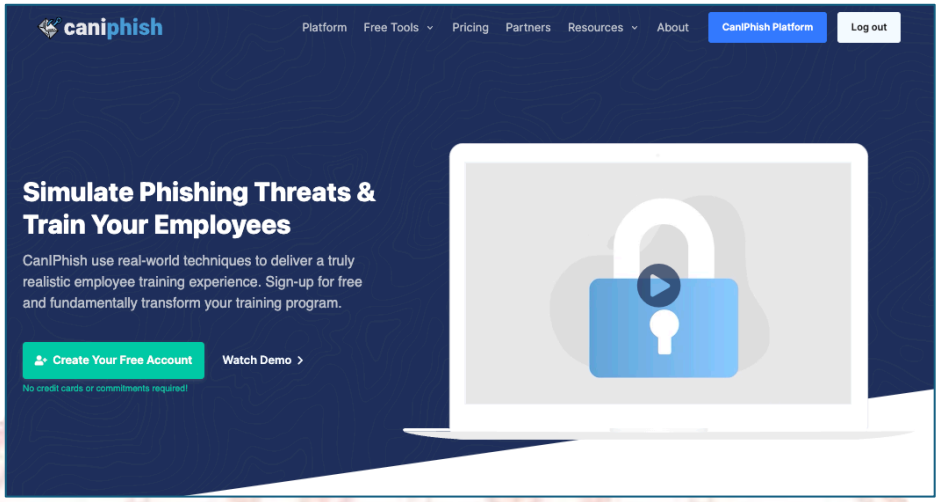


ภาพที่ 3-1 วิธีการดำเนินการวิจัย

3.1.1 การประสานงานกับบริษัทเป้าหมาย : ขั้นแรก คือ การติดต่อและประสานงานกับบริษัทเป้าหมายเพื่อขออนุญาตในการทำการทดสอบฟิชชิง ซึ่งจำเป็นต้องได้รับความยินยอมและความเข้าใจเกี่ยวกับวัตถุประสงค์ของการทดสอบ

3.1.2 การรวบรวมข้อมูลเบื้องต้น : รวบรวมข้อมูลเกี่ยวกับบริษัทเป้าหมาย ซึ่งรวมถึงรายชื่อพนักงาน, ที่อยู่อีเมล, แผนก ฯลฯ เพื่อใช้ในการออกแบบอีเมลปลอมและเลือกกลุ่มเป้าหมายที่เหมาะสมสำหรับการทดสอบ

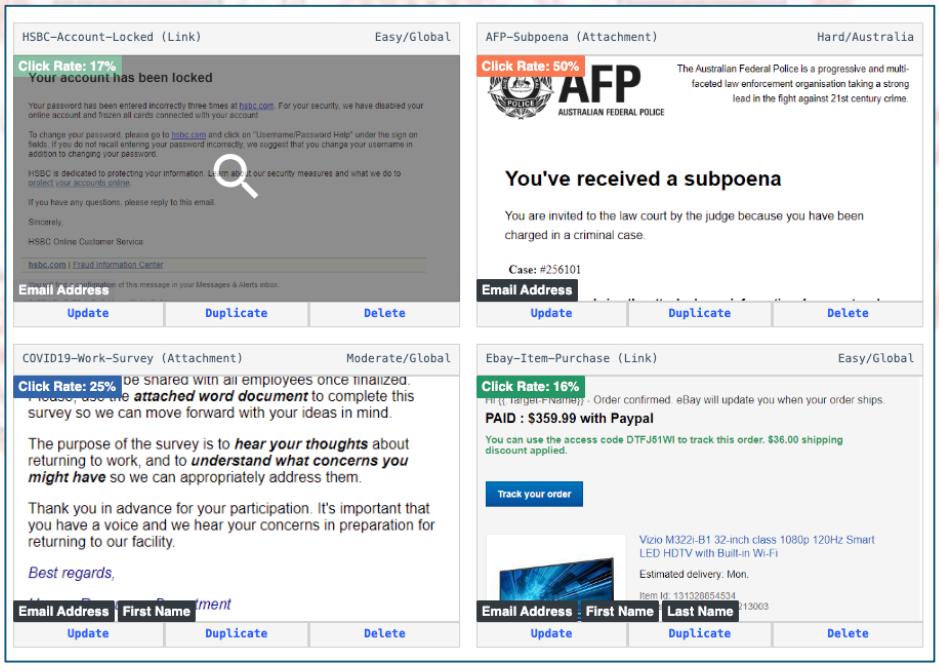
3.1.3 เลือกเครื่องมือที่เหมาะสม : ในการใช้ทดสอบโดยวิจัยนี้เลือกเป็นแพลตฟอร์มของ CanIPhish ดังภาพที่ 3-2 เนื่องจาก CanIPhish เป็นแพลตฟอร์มที่ถูกสร้างมาเพื่อจำลองการโจมตีแบบฟิชชิง ซึ่งมีข้อดีหลายด้าน ได้แก่



ภาพที่ 3-2 CanIPhish

ที่มา : https://caniphish.com/

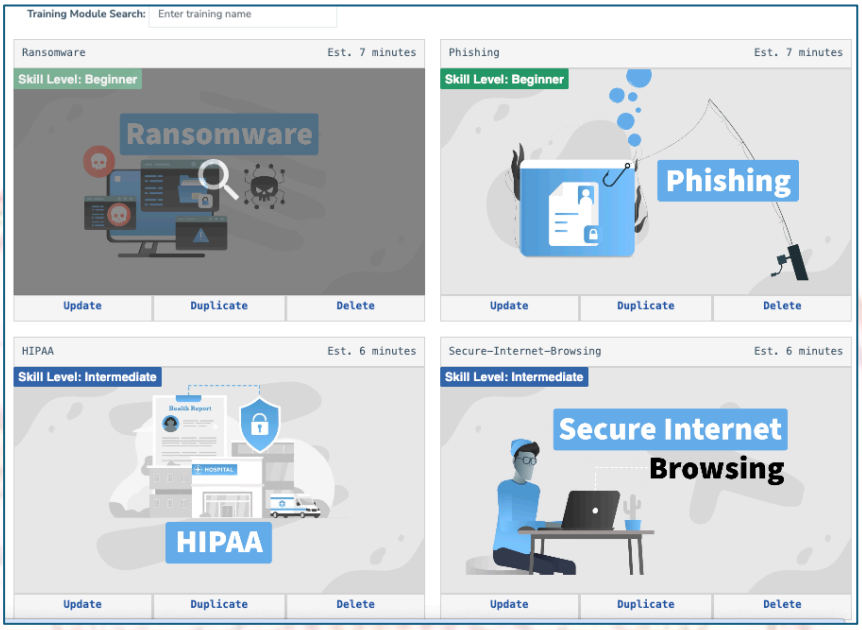
3.1.3.1 มีความเสมือนจริง: เครื่องมือมีการออกแบบรูปแบบอีเมลให้มีความสมจริง จึงทำให้การทดสอบดูเสมือนจริง ดังภาพที่ 3-2



ภาพที่ 3-2 CanIPhish (ต่อ)

ที่มา : https://caniphish.com/User/EmailPhishing

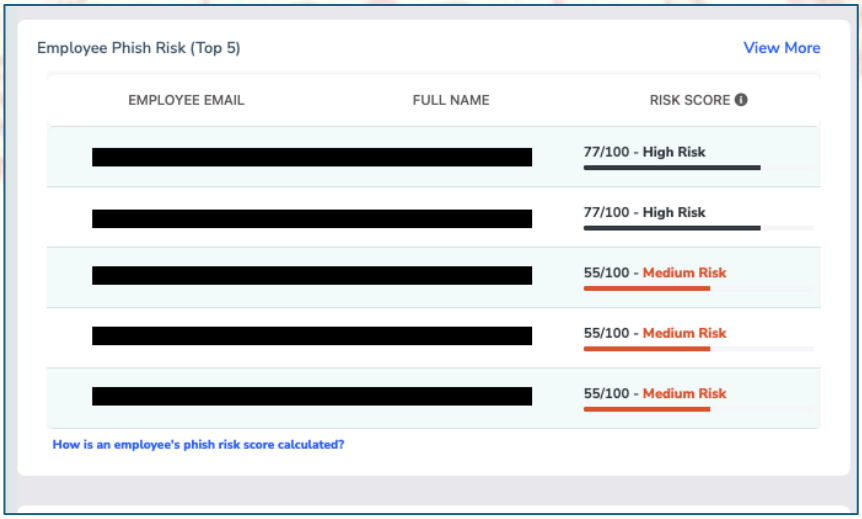
3.1.3.2 ฟังก์ชันฝึกอบรมและสร้างการตระหนัก : การฝึกอบรมและการสร้างความตระหนักอย่างต่อเนื่องเป็นสิ่งสำคัญในการป้องกันการโจมตีแบบฟิชชิงเพราะการจำลองเหล่านี้เป็นประจำสามารถรับมือต่อกลยุทธ์ที่เปลี่ยนแปลงอยู่ตลอดเวลาของผู้โจมตีได้ ดังภาพที่ 3-3



ภาพที่ 3-3 ฟังก์ชั่นการฝึกอบรบและสร้างความตระหนัก

ที่มา : https://caniphish.com/User/TrainingModules

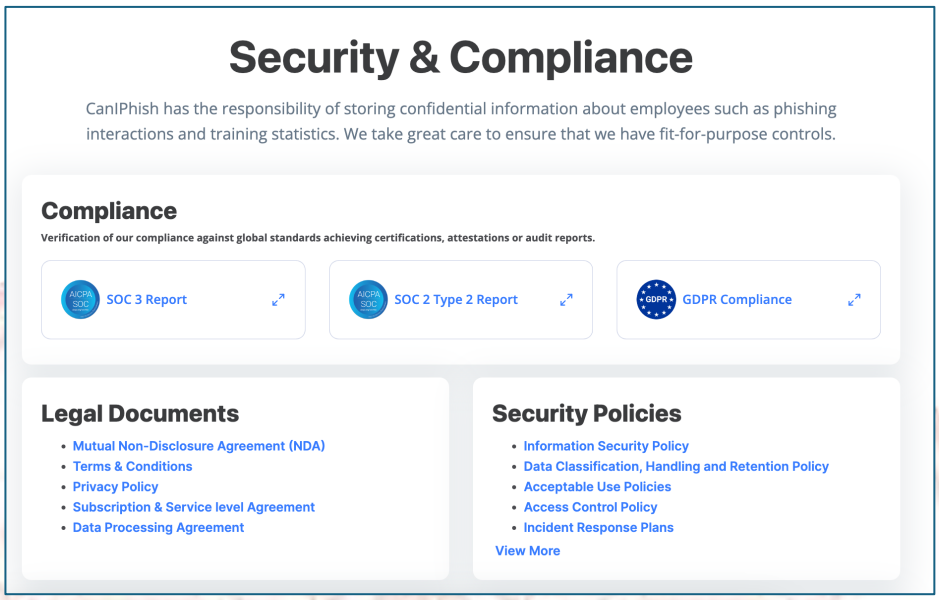
3.1.3.3 ฟังก์ชันการประเมินความเสี่ยง : ทางแพลตฟอร์มมีการประเมินความเสี่ยงของพนักงานที่มีแนวโน้มจะถูกหลอกได้ง่าย ดังภาพที่ 3-4



ภาพที่ 3-4 เครื่องมือที่ใช้มีการประเมินความเสี่ยง

ที่มา : https://caniphish.com/User

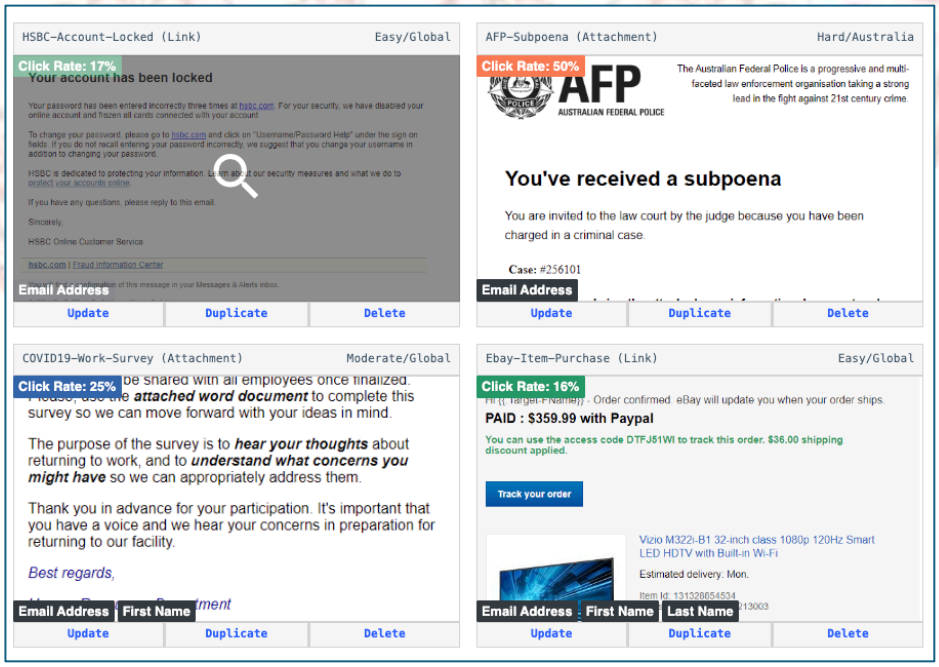
3.1.3.4 มีโมดูลนโยบายและการปฏิบัติตาม : แพลตฟอร์มมีการดำเนินงานตามมาตรฐานการรักษาความปลอดภัยและข้อมูลส่วนบุคคลดังภาพที่ 3-5



ภาพที่ 3-5 เครื่องมือที่ใช้มีมีนโยบายและการปฏิบัติตาม
ที่มา : https://caniphish.com/security

3.1.3.5 อีเมลปลอมและ QR Code: สนับสนุนการสร้างอีเมลปลอมหลายรูปแบบที่มีลักษณะเช่นเดียวกับอีเมลฟิชชิงจริง และQR Code ที่จะติดบริเวณที่ต้องการโจมตี ดังรูปที่ 3-6 เพื่อหลอกล่อให้พนักงานคลิกลิงก์หรือดำเนินการอัพเดทข้อมูลต่าง ๆ โดยแบ่งให้มีความหลากหลาย เช่น สิทธิประโยชน์ใหม่ของบริษัท การขอเข้าถึงไฟล์ การส่งไฟล์ให้อ่าน หรือการมีทีมใหม่ให้เข้าร่วม เป็นต้น ดังภาพที่ 3-7

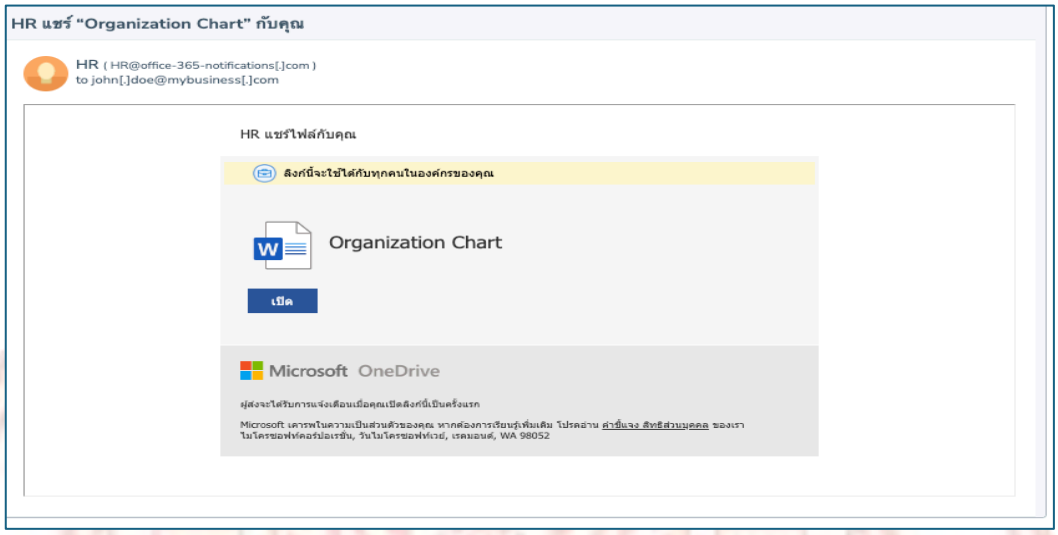
ภาพที่ 3-6 การติด QR Code หน้าบริษัท



ภาพที่ 3-7 รูปแบบอีเมลปลอม

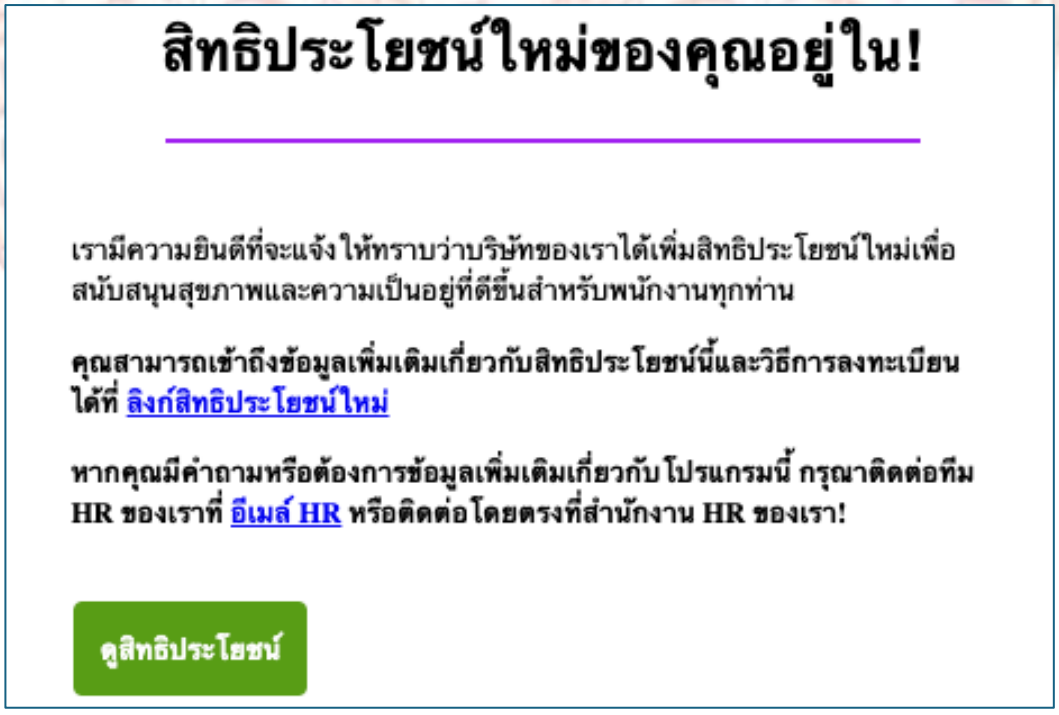
ที่มา : https://caniphish.com/User/EmailPhishing

3.1.3.6 เลือกหัวข้อหรือเรื่องที่มีความน่าสนใจและต้องการให้ผู้รับอีเมลตอบสนอง ดังภาพที่ 3-8



ภาพที่ 3-8 การเลือกหัวข้อที่มีความน่าสนใจ

3.1.3.7 ออกแบบเนื้อหาของอีเมลโดยใช้ภาษาที่สร้างความเชื่อมั่นและเตรียมความพร้อมให้กับการกระทำตามคำแนะนำ ดังภาพที่ 3-9

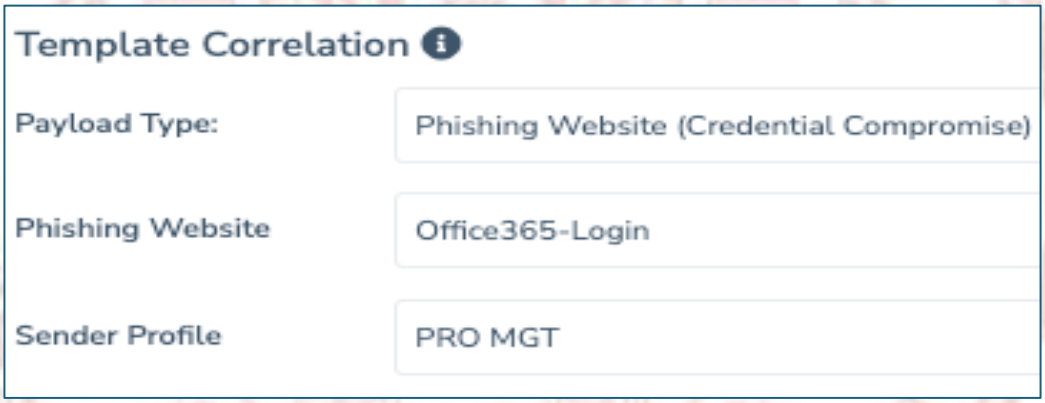


ภาพที่ 3-9 การออกแบบเนื้อหาที่มีการนำเสนอสิทธิประโยชน์

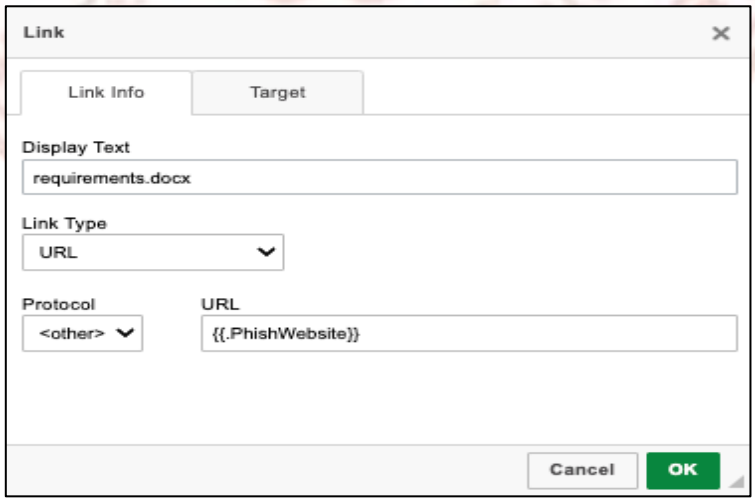
3.1.3.8 เลือกรูปแบบอีเมลที่มีลักษณะเช่นเดียวกับอีเมลฟิชชิงจริง เช่น การปลอมเป็นอีเมลจากบริษัทที่รู้จัก หรือจากบัญชีบุคคลที่น่าเชื่อถือ ดังภาพที่ 3-10

ภาพที่ 3-10 การออกแบบเนื้อหาให้เสมือนเป็นการมอบหมายงานจากหัวหน้างาน

3.1.3.9 ใส่ลิงก์หรือปุ่มที่เชื่อมโยงไปยังเว็บไซต์ปลอมหรือหน้าเว็บที่ต้องการให้ผู้รับอีเมลเข้าไป ดังภาพที่ 3-11

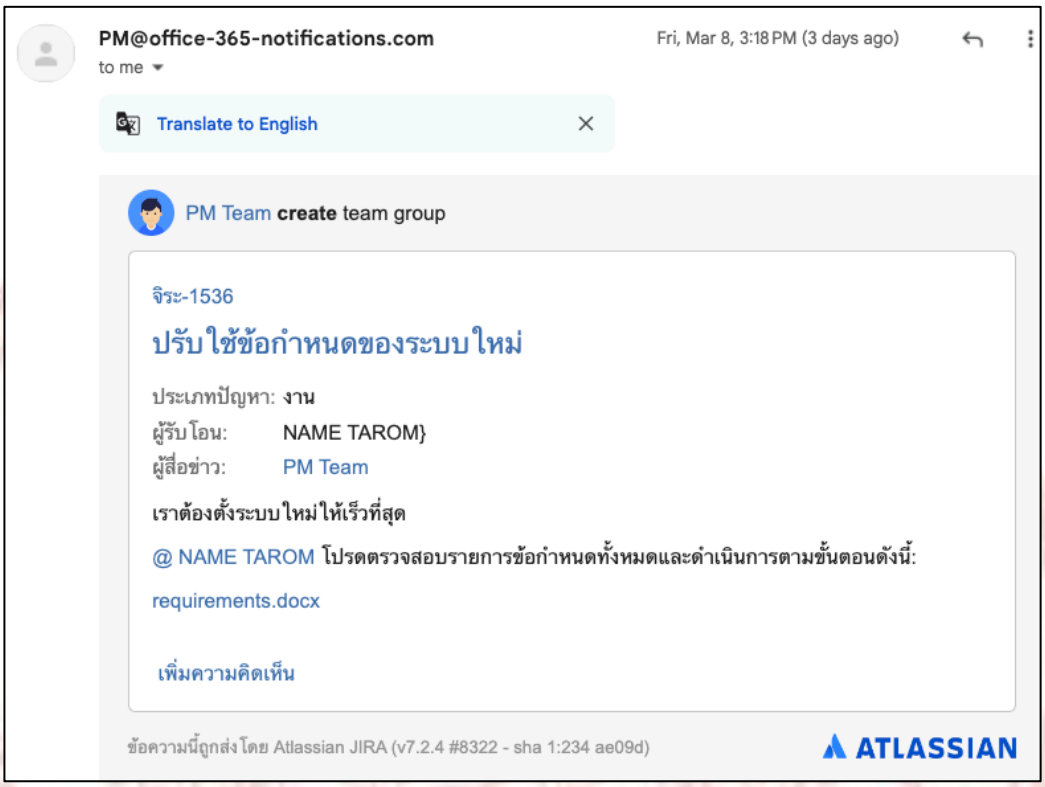


ภาพที่ 3-11 การสร้างปุ่มเชื่อมโยงไปหน้าเว็บไซต์ปลอม



ภาพที่ 3-11 การสร้างปุ่มเชื่อมโยงไปหน้าเว็บไซต์ปลอม (ต่อ)

3.1.3.10 ตรวจสอบให้แน่ใจว่ารูปแบบและเนื้อหาของอีเมลปลอมดูเชื่อถือได้และเหมือนจริงมากที่สุด ทดสอบการส่งอีเมลปลอมโดยส่งไปยังตัวเองหรือผู้รับทดสอบเพื่อดูว่าอีเมลมีลักษณะเช่นเดียวกับอีเมลฟิชชิงจริงหรือไม่ ดังภาพที่ 3-12



ภาพที่ 3-12 การทดสอบการส่งอีเมล

3.1.4 การส่งอีเมลปลอม : ดำเนินการส่งอีเมลปลอมไปยังพนักงานเป้าหมายที่ได้ระบุไว้จากข้อมูลที่รวบรวมมา

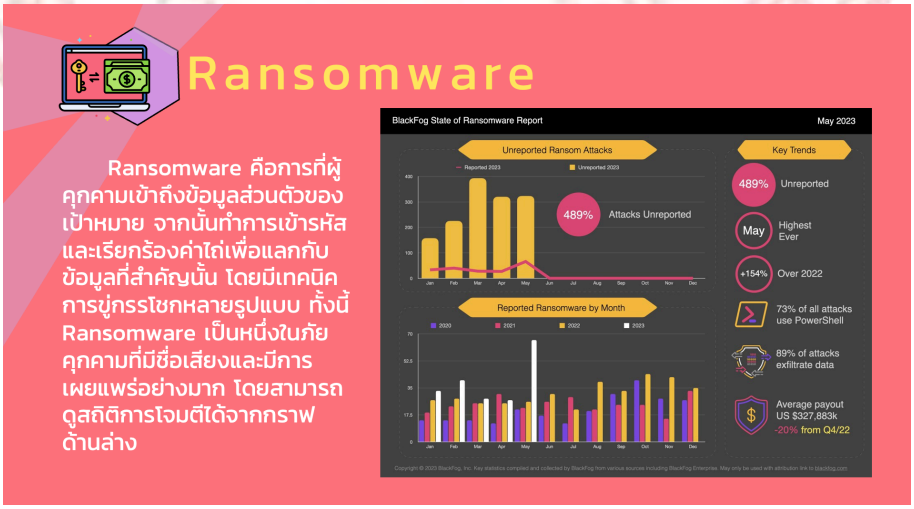
3.1.5 การรวบรวมและวิเคราะห์ผลลัพธ์ : รวบรวมข้อมูลจากการทดสอบ และวิเคราะห์ผลลัพธ์เพื่อดูว่ามีการตอบสนองอย่างไรต่ออีเมลฟิชชิง

3.1.6 การออกแบบหลักสูตรการฝึกอบรม : จากผลลัพธ์ที่ได้ ออกแบบหลักสูตรการฝึกอบรมด้านความปลอดภัยไซเบอร์ที่ครอบคลุมหัวข้อสำคัญ เช่น ความรู้เกี่ยวกับภัยคุกคามฟิชชิง

3.1.7 กลอุบายที่ใช้หลอกลวง, วิธีสังเกตและป้องกันตนเองจากภัยคุกคาม ดังภาพที่ 3-13

ภาพที่ 3-13 ตัวอย่างหลักสูตรที่ใช้อบรม

ภาพที่ 3-13 ตัวอย่างหลักสูตรที่ใช้อบรม (ต่อ)



ภาพที่ 3-13 ตัวอย่างหลักสูตรที่ใช้อบรม (ต่อ)

3.1.8 การทำการทดสอบซ้ำ : หลังจากการฝึกอบรม ทำการทดสอบซ้ำกับกลุ่มเดียวกันโดยใช้วิธีการคล้ายคลึงกันเพื่อเปรียบเทียบผลลัพธ์ก่อนและหลังการฝึกอบรม จากนั้นรวบรวมข้อมูลและวิเคราะห์ผลลัพธ์อีกครั้ง เพื่อนำเสนอแนวทางและแนะนำให้กับผู้ประกอบการในการพัฒนามาตรการป้องกันและแก้ไขปัญหาภัยคุกคามฟิชชิง ในองค์กร

3.1.9 รายงานผลการทดสอบและคำแนะนำให้กับผู้ประกอบการ : หลังจากทำการทดสอบในแต่ละครั้งจะทำการรายงานผลแต่ละครั้งไปให้ผู้ประกอบการและเมื่อเสร็จสิ้นโครงการจะมีการแนะนำกับทางผู้ประกอบการให้เห็นถึงความสำคัญในการสร้างความตระหนักเกี่ยวกับความปลอดภัยไซเบอร์เพิ่มเติม

บทที่ 4
ผลการวิจัย

งานวิจัยนี้ได้ศึกษาและวิเคราะห์ความตระหนักรู้ในเรื่องของความมั่นคงปลอดภัยด้านสารสนเทศในกลุ่มบุคลากรของบริษัทไอที โดยได้ดำเนินการจำลองสถานการณ์การโจมตีด้วยอีเมลฟิชชิงทั้งหมดจำนวน 2 ครั้ง และได้จัดการฝึกอบรมในหัวข้อเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์ 1 ครั้ง กลุ่มตัวอย่างในการศึกษานี้ประกอบด้วยพนักงานจำนวน 46 คนจากบริษัทไอทีแห่งหนึ่ง โดยเน้นการวัดและเปรียบเทียบผลลัพธ์ก่อนและหลังการเข้ารับการฝึกอบรมเพื่อตรวจสอบการเปลี่ยนแปลงในพฤติกรรมเมื่อเผชิญกับอีเมลที่มีลักษณะเป็นภัยคุกคาม

นอกจากนี้งานวิจัยยังเน้นการศึกษาความตระหนักรู้และความเข้าใจเกี่ยวกับมาตรการป้องกันและวิธีการตอบสนองต่อภัยคุกคามทางไซเบอร์ของพนักงานด้วยวัตถุประสงค์หลัก 2 ประการ คือ 1. พัฒนาความรู้และเสริมสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศให้กับพนักงานบริษัทไอทีแห่งหนึ่ง 2. ประเมินและวิเคราะห์ระดับความตระหนักรู้และประสิทธิภาพของพนักงานในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ ผลลัพธ์จากการดำเนินงาน มีดังนี้

4.1 ผลการจำลองการโจมตีด้วยอีเมลฟิชชิง

ผู้วิจัยได้ศึกษาและเก็บผลจากการใช้เครื่องมือ CanIPhish เพื่อจำลองการโจมตีด้วยอีเมลฟิชชิงต่อพนักงานในบริษัทไอทีแห่งหนึ่งมีพนักงานทั้งหมด 46 คน โดยเก็บข้อมูล และนำมาวิเคราะห์ สรุปผลได้ดังนี้ การทดสอบครั้งที่ 1 มีการส่งอีเมลจำนวน 92 อีเมล ประกอบด้วยอีเมล 6 รูปแบบ ดังนี้

4.1.1 รูปแบบเป็นการทดสอบการหลอกลวง โดยการนำเสนอเกี่ยวกับสิทธิประโยชน์ของบริษัทโดยทำการหลอกลวงให้เป้าหมายคลิกไปที่เว็บไซต์หลอกลวง ดังภาพที่ 4-1

4.1.2 ฟิชชิง 5 รูปแบบ โดยแบ่งเป็นแต่ละแผนก

4.1.2.1 แผนก Office of Managing Director หลอกลวงโดยการมีแชร์ไฟล์เกี่ยวกับ Organization Chart ดังภาพที่ 4-2

4.1.2.2 Back Officeและ Technical Support หลอกลวงโดยแจ้งว่ามีอีเมลอยู่ใน Quarantine ดังภาพที่ 4-3 และ 4-4

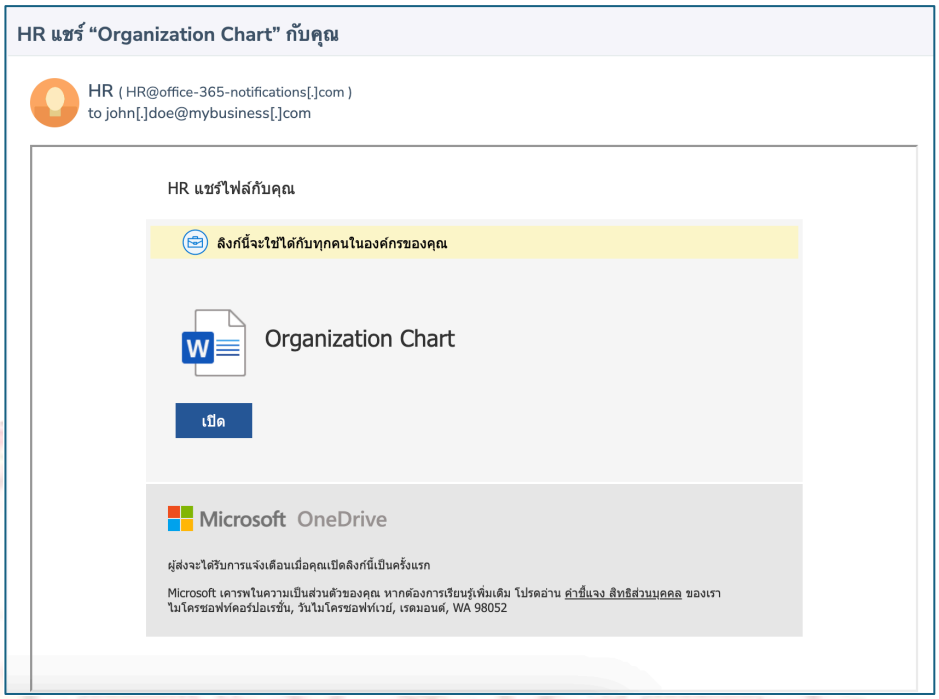
4.1.2.3 Channel Sales เป็นการหลอกลวงโดยการมีแชร์ไฟล์เกี่ยวกับ Product Pricelist Update ดังภาพที่ 4-5

4.1.2.4 Project Sales เป็นการหลอกลวงโดยการแชร์ไฟล์ Project List FY24 ดังภาพที่ 4-6

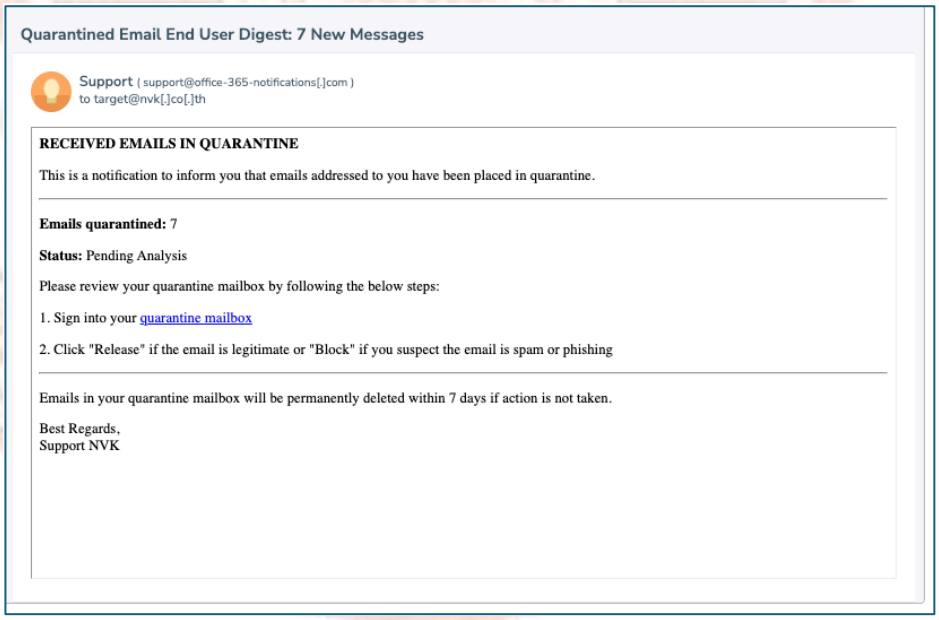
4.1.2.5 Project Management NVK48 และNVK AI เป็นการหลอกลวงโดยการเชิญเข้าร่วมโครงการ ดังภาพที่ 4-7 และ 4-8

อีเมลดังกล่าวจะหลอกลวงให้คลิกไปที่เว็บไซต์หลอกและอีเมลดังกล่าวถูกเปิดอ่าน 41 ครั้ง โดยมีการคลิกเว็บไซต์หลอกลวง 20 ครั้ง มีคนกรอกข้อมูลผ่านเว็บไซต์น่าสงสัย 10 คน และกรอกข้อมูลผ่าน QR Code ที่มีการหลอกลวงโดยการเชิญให้ลงทะเบียน 1 คน ดังภาพที่ 4-9 จึงสรุปได้ว่า มีพนักงานทั้งหมด 11 คนที่เปิดเผยข้อมูลผ่านการทดสอบ โดยมีรายละเอียดดังตารางที่ 4-1 และภาพที่ 4-10

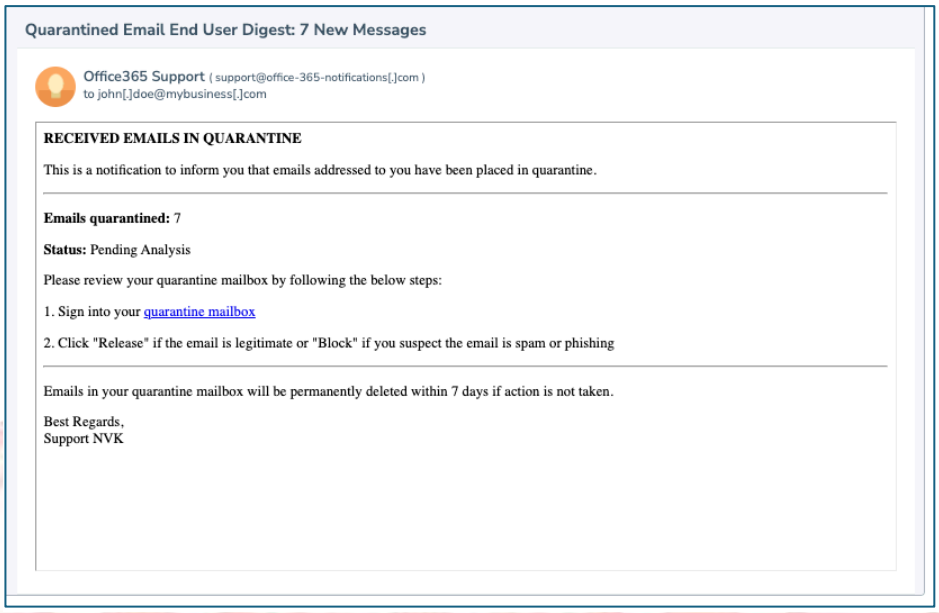
ภาพที่ 4-1 รูปแบบอีเมลฟิชชิง ครั้งที่ 1



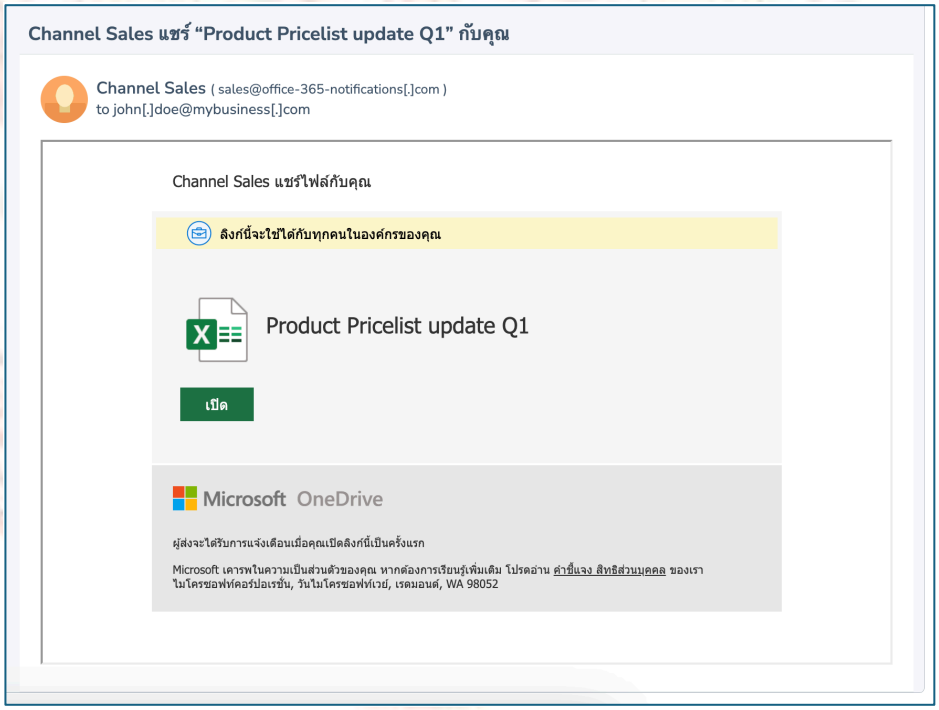
ภาพที่ 4-2 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Office of Managing Director ครั้งที่ 1



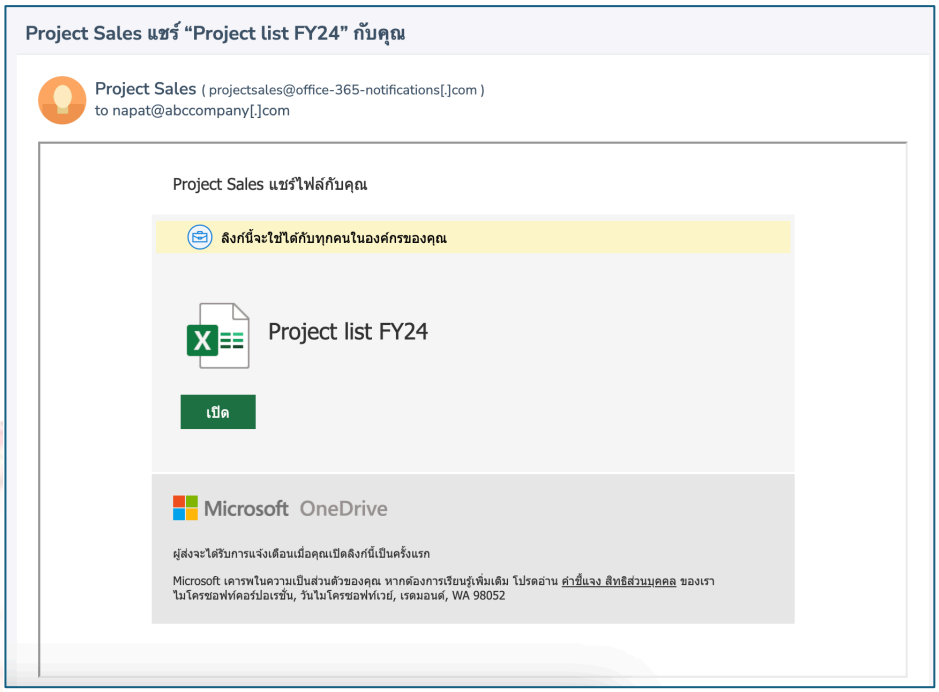
ภาพที่ 4-3 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Back Office ครั้งที่ 1



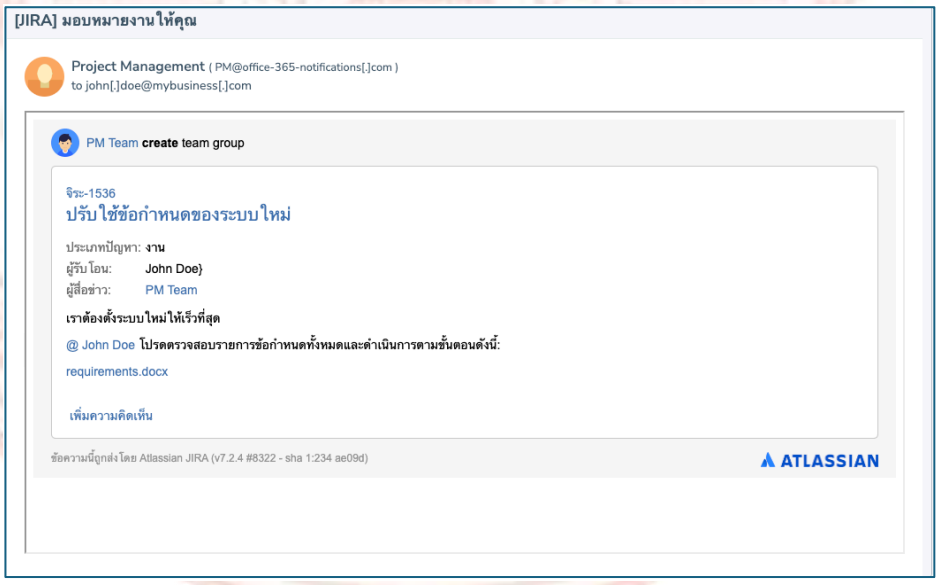
ภาพที่ 4-4 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Technical Support ครั้งที่ 1



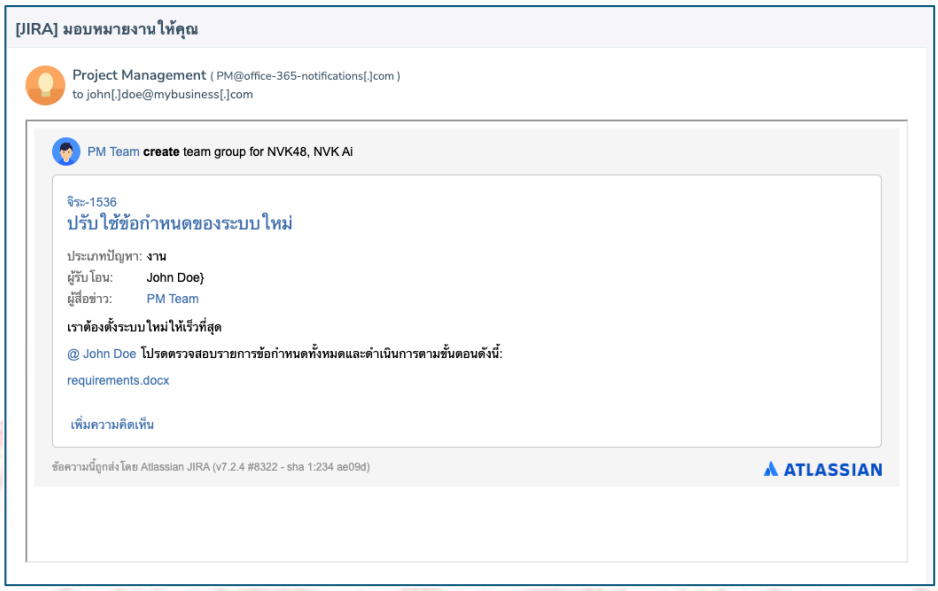
ภาพที่ 4-5 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Channel Sales ครั้งที่ 1



ภาพที่ 4-6 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Project Sales ครั้งที่ 1



ภาพที่ 4-7 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม Project Management ครั้งที่ 1

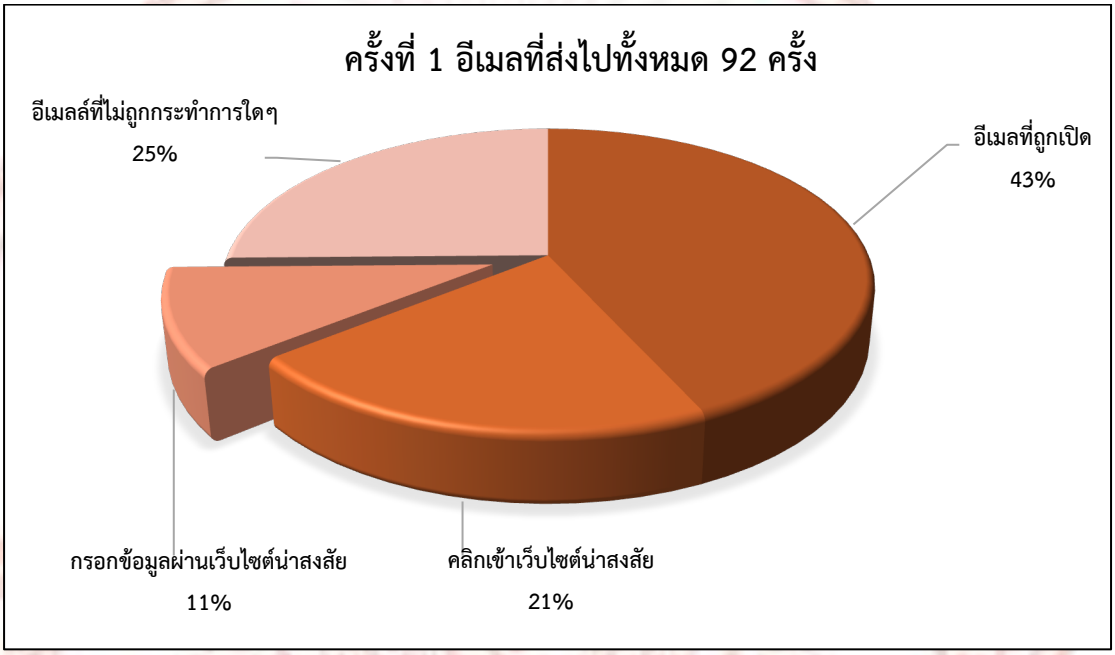


ภาพที่ 4-8 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม NVK48 และNVK AI ครั้งที่ 1

ภาพที่ 4-9 รูปแบบQR Code ครั้งที่ 1

ตารางที่ 4-1 ผลการจำลองการโจมตีครั้งที่ 1

ผลการจำลองการโจมตีครั้งที่ 1		
สถานะ	**จำนวนพนักงานในบริษัท**	
	(คน)	**(%)**
ป้อนข้อมูลกลับ	10	21.74%
กรอกข้อมูลผ่าน QR Code	1	2.17%



ภาพที่ 4-10 แผนภูมิแสดงผลการทดสอบ ครั้งที่ 1

การทดสอบครั้งที่ 2 มีการส่งอีเมลทั้งหมด 92 อีเมล มี 5 รูปแบบ

4.1.3 ฟิชชิง 1 รูปแบบเป็นการทดสอบทำการหลอกลวงโดยการแจ้งเตือนเกี่ยวกับการลงทะเบียนทำการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) ดังภาพที่ 4-11

4.1.4 ฟิชชิง 4 รูปแบบ โดยแบ่งเป็นแต่ละแผนก

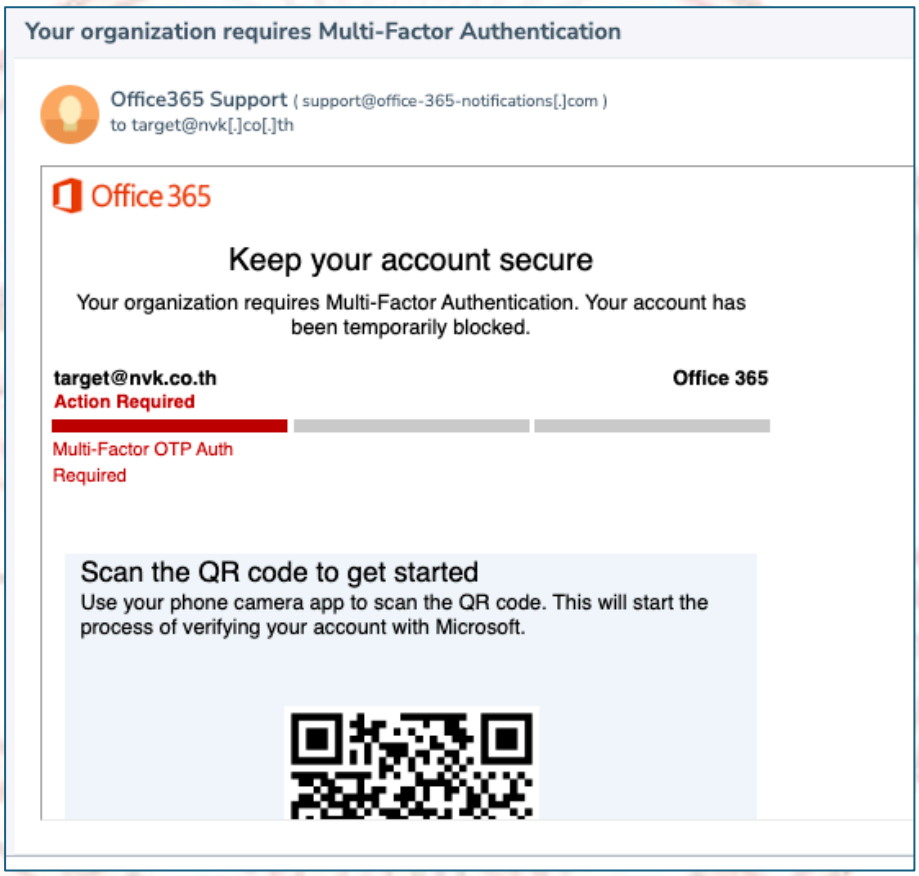
4.1.4.1 Office of Managing Director เป็นการหลอกลวงโดยการขออนุญาตเข้าถึงไฟล์ ดังภาพที่ 4-12

4.1.4.2 Back Office มีการทดสอบการหลอกลวงโดยการแชร์หลักฐานการบันทึกข้อมูล ดังภาพที่ 4-13

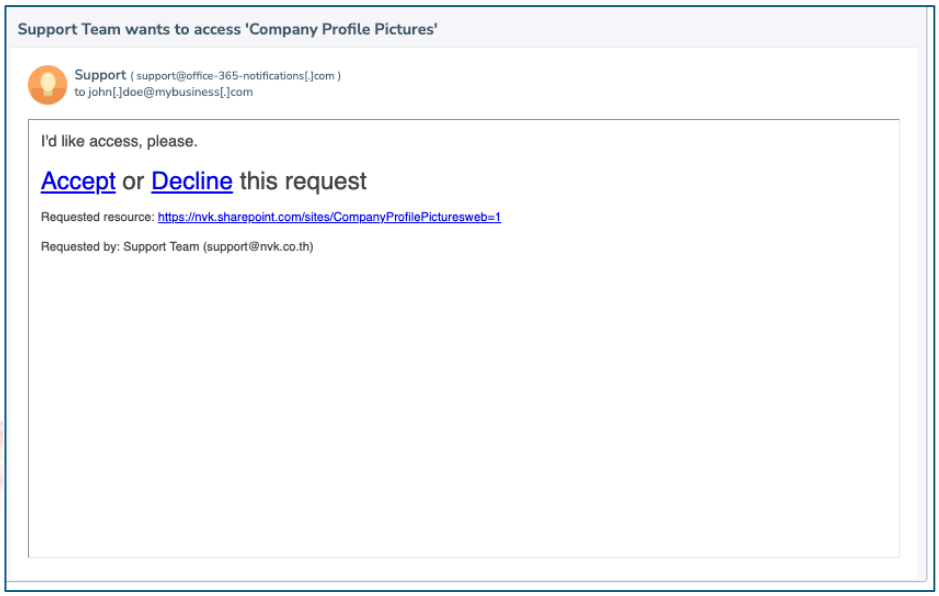
4.1.4.3 Technical Support เป็นการทดสอบการหลอกลวงโดยแจ้งว่ามีอีเมลอยู่ใน Quarantine ดังภาพที่ 4-14

4.1.4.4 Channel Sales, Project Sales, Project Management, NVK48 และNVK AI เป็นการทดสอบการหลอกลวงโดยการขออนุญาตเข้าถึงไฟล์ ดังภาพที่ 4-15, 4-16, 4-17, 4-18 และ4-19

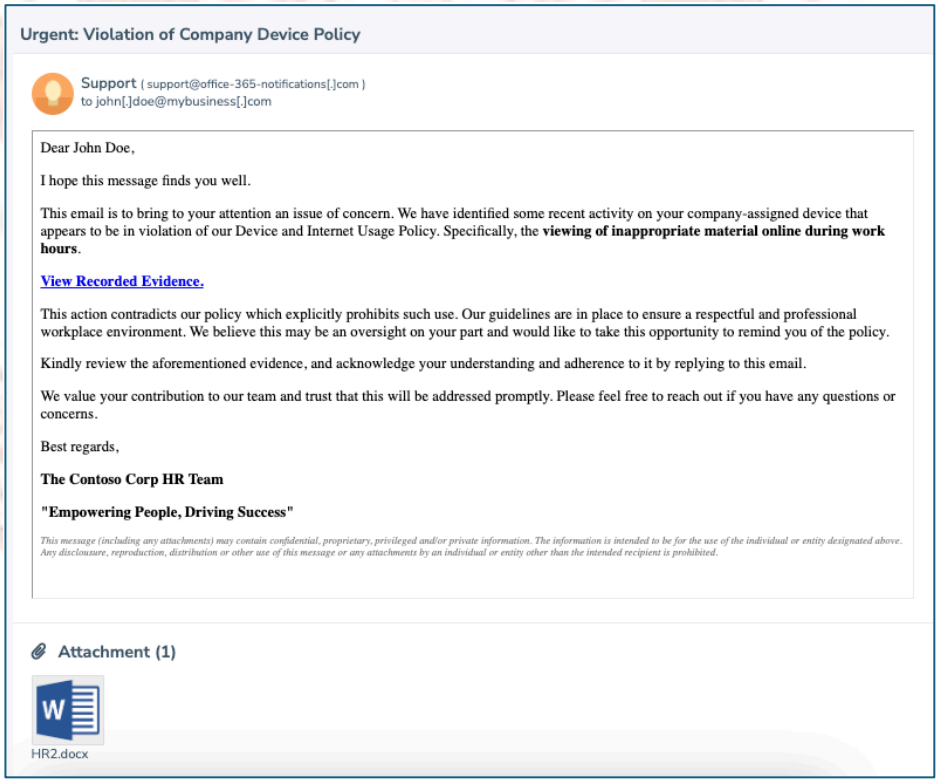
อีเมลดังกล่าวจะหลอกลวงให้คลิกไปที่เว็บไซต์หลอกและและอีเมลดังกล่าวถูกเปิดอ่าน 35 ครั้ง โดยมีการคลิกเว็บไซต์หลอกลวง 4 ครั้ง กรอกข้อมูลผ่านเว็บไซต์น่าสงสัย 2 คน และกรอกข้อมูลผ่าน QR Code ที่มีการหลอกลวงโดยการเชิญให้ลงทะเบียน 0 คน จึงสรุปได้ว่า มีพนักงานทั้งหมด 2 คนที่เปิดเผยข้อมูลผ่านการทดสอบ โดยมีรายละเอียดดังตารางที่ 4-2 และภาพที่ 4-20



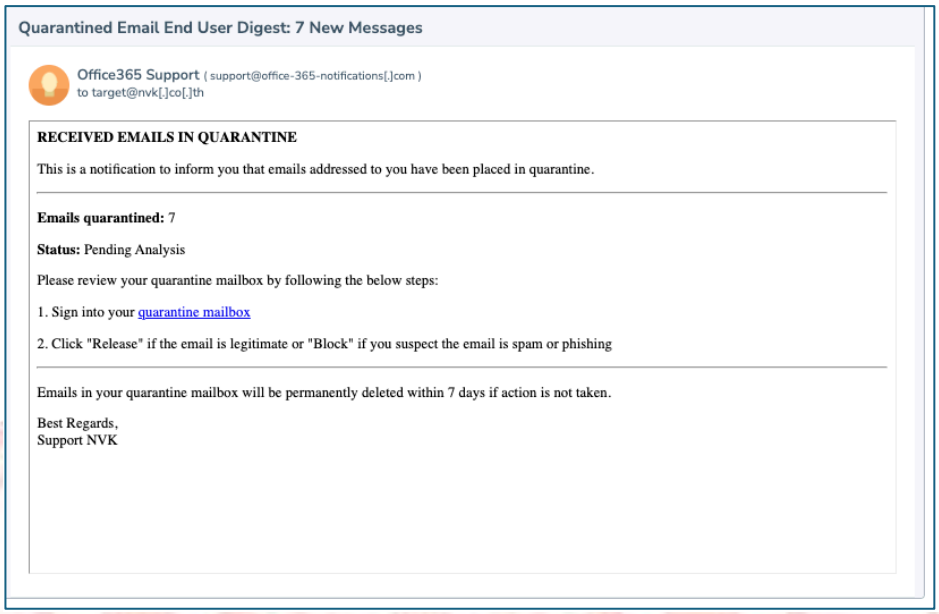
ภาพที่ 4-11 รูปแบบอีเมลฟิชชิง ครั้งที่ 2



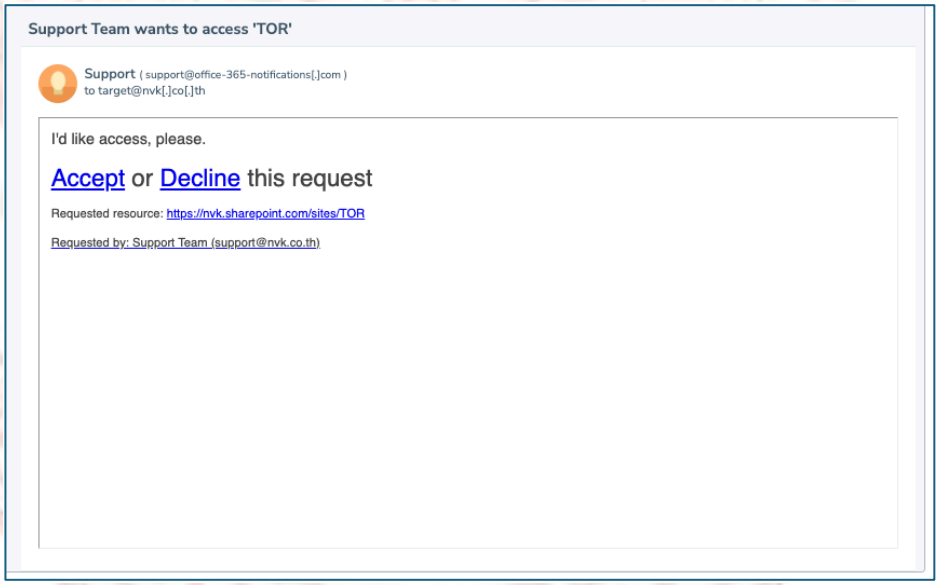
ภาพที่ 4-12 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Office of Managing Director ครั้งที่ 2



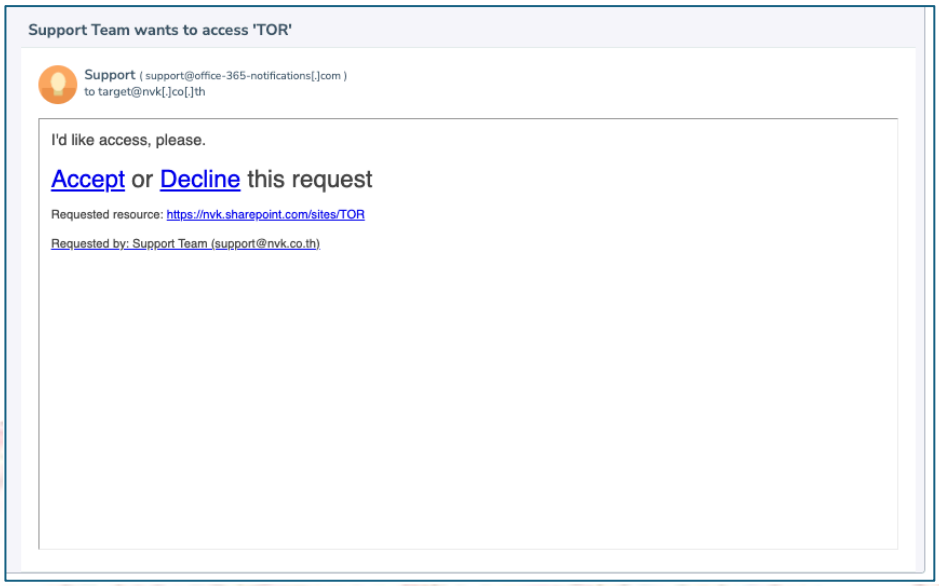
ภาพที่ 4-13 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Back Office ครั้งที่ 2



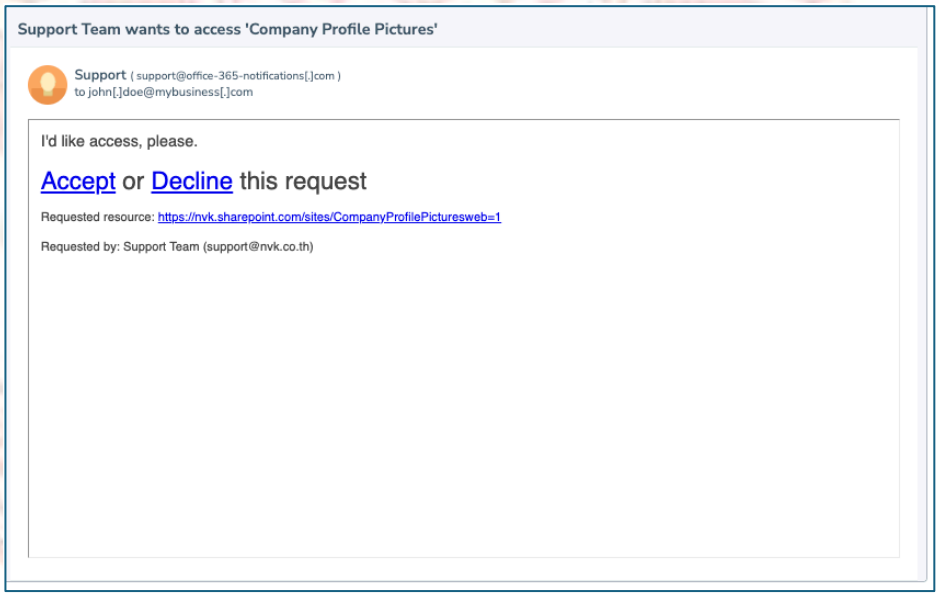
ภาพที่ 4-14 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Technical Support ครั้งที่ 2



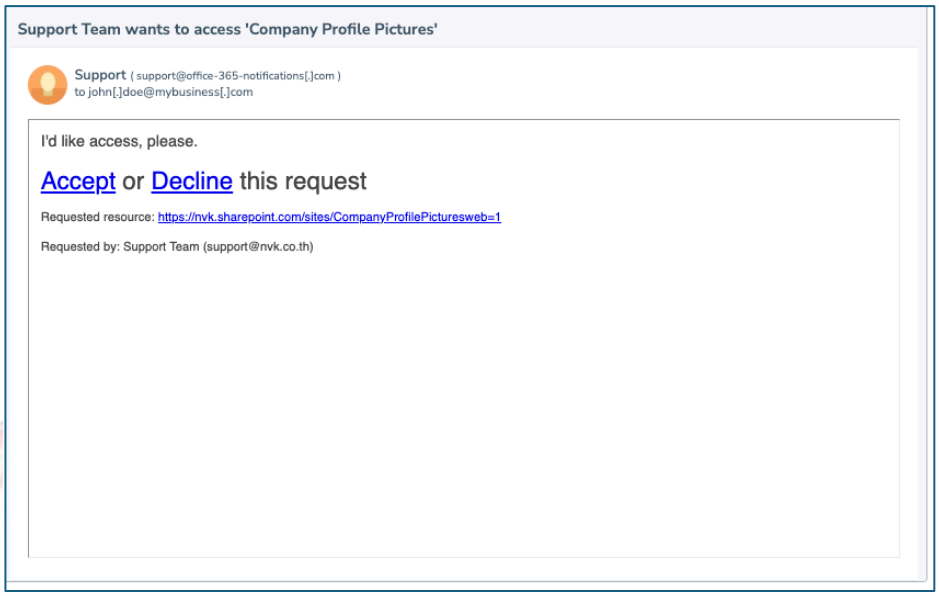
ภาพที่ 4-15 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Channel Sales ครั้งที่ 2



ภาพที่ 4-16 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับแผนก Project Sales ครั้งที่ 2



ภาพที่ 4-17 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม Project Management ครั้งที่ 2

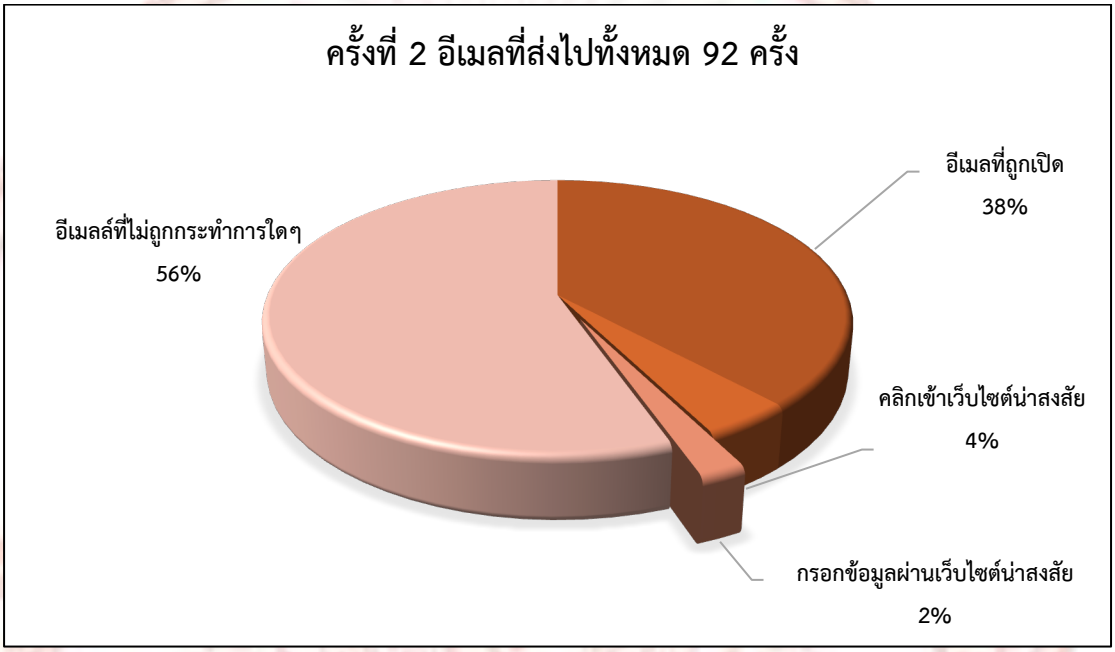


ภาพที่ 4-18 รูปแบบอีเมลฟิชชิงแบบเจาะจงกับทีม NVK48 และNVK AI ครั้งที่ 2

ภาพที่ 4-19 รูปแบบQR Code ครั้งที่ 2

ตารางที่ 4-2 ผลการจำลองการโจมตีครั้งที่ 2

ผลการจำลองการโจมตีครั้งที่ 2		
สถานะ	**จำนวนพนักงานในบริษัท**	
	(คน)	**(%)**
ป้อนข้อมูลกลับ	2	4.35%
กรอกข้อมูลผ่าน QR Code	0	0%



ภาพที่ 4-20 แผนภูมิแสดงผลการทดสอบ ครั้งที่ 2

บทที่ 5
อภิปราย สรุป และข้อเสนอแนะ

5.1 สรุปผล

การศึกษานี้ แสดงให้เห็นภัยคุกคามที่เกิดขึ้นจากการโจมตีโดยวิธีการฟิชชิงนี้มีความรุนแรงและมีผลกระทบที่หลากหลายต่อบุคคลและองค์กรทั้งในระดับบุคคลและองค์กร จากผลการทดสอบโจมตีทั้งสองครั้ง สามารถสังเกตได้ว่า การทดสอบครั้งแรกมีการเปิดอ่านอีเมลและมีการตอบสนองที่สูงกว่าการทดสอบครั้งที่สอง ซึ่งแสดงถึงการลดลงของการตอบสนองต่ออีเมลที่มีลักษณะเป็นการหลอกลวงในครั้งที่สอง และจำนวนพนักงานที่กรอกข้อมูลผ่านช่องทางต่าง ๆ ลดลงอย่างเห็นได้ชัด โดยเฉพาะการกรอกข้อมูลผ่านเว็บไซต์หลอกลวงและ QR Code ที่มีจำนวนลดลงจาก 10 คน และ 1 คน ในการทดสอบครั้งแรกเหลือเพียง 2 คน และ 0 คน ในการทดสอบครั้งที่สองตามลำดับ นอกจากนี้ จำนวนอีเมลที่ถูกเปิดอ่านก็มีจำนวนลดลงจาก 41 ครั้งเป็น 35 ครั้งเมื่อเปรียบเทียบระหว่างการทดสอบครั้งแรกและครั้งที่สอง ซึ่งทำให้เห็นว่าการฝึกอบรมและการเพิ่มความตระหนักรู้เป็นสิ่งสำคัญในการป้องกันตัวเองและองค์กรจากการโจมตีแบบฟิชชิง

5.2 อภิปรายผล

การศึกษานี้มีข้อจำกัดสำคัญที่ควรจะตระหนักและควรทำความเข้าใจปัจจัยที่อาจมีผลต่อการวิเคราะห์และการสรุปผลของการทดสอบ ข้อจำกัดเหล่านี้มีผลโดยตรงต่อความน่าเชื่อถือของข้อมูลที่ได้รวมถึงอาจเป็นตัวกำหนดความสำเร็จของการทดสอบ ซึ่งมีรายละเอียด 3 ประการมีดังนี้

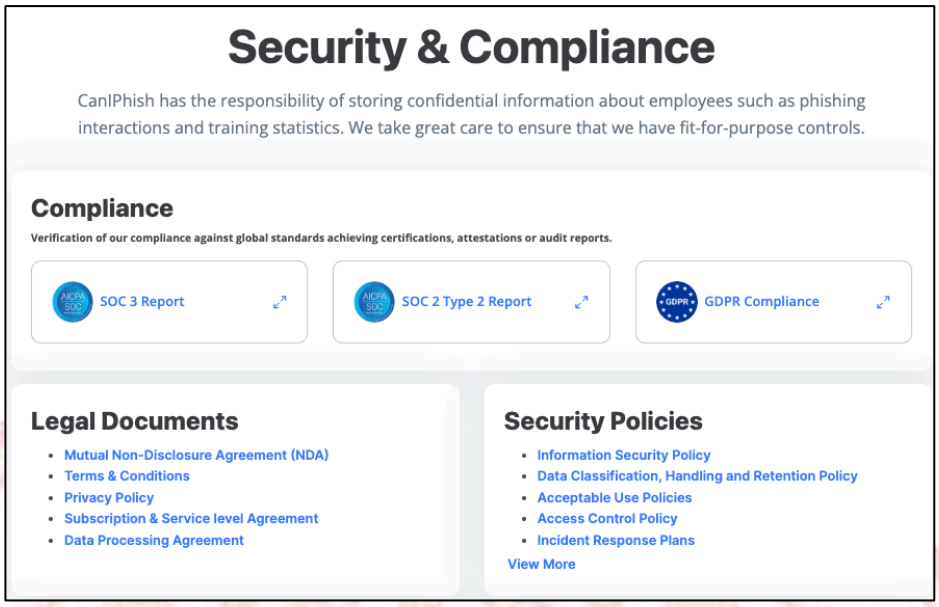
5.2.1 ข้อจำกัดของวิธีการ

5.2.1.1 การส่งอีเมลทดสอบจะต้องมีการเพิ่ม domain ของอีเมลผู้ส่งไปในระบบอีเมลเซิฟเวอร์ของเป้าหมายก่อน

5.2.1.2 ในการติด QR Code จะต้องดำเนินการตอนที่ไม่มีบุคคลอื่นเห็น

5.1.2 ข้อจำกัดของเครื่องมือ

5.2.2.1 เครื่องมือมีการเก็บข้อมูลกับทางผู้ให้บริการ ทำให้ข้อมูลอาจรั่วไหลได้ ทั้งนี้ทางผู้ให้บริการมีการรับรองในด้านการปฏิบัติตามกฎระเบียบ ดังภาพที่ 5-1



ภาพที่ 5-1 การรับรองการปฏิบัติตามของผู้ให้บริการ

ที่มา : https://caniphish.com/security

5.1.3 ข้อจำกัดของกลุ่มเป้าหมาย

5.1.3.1 ในการทดสอบฟิชชิงพนักงานอาจจะบอกต่อกันทำให้ผลที่ได้จากการทดสอบมีความแม่นยำลดน้อยลง

5.3 ข้อเสนอและแนวทางการปฏิบัติ

5.3.1 การฝึกอบรมและเพิ่มความตระหนักรู้ : ผู้ประกอบการควรลงทุนในการฝึกอบรมพนักงานเพื่อเพิ่มความเข้าใจในภัยคุกคาม และวิธีป้องกันตัวจากการโจมตีแบบฟิชชิง การเรียนรู้ว่าอย่างไรที่จะระวังและระวังเท่าที่จะทำให้สามารถลดความเสี่ยงจากการโจมตีแบบนี้ได้อย่างมีประสิทธิภาพ

5.3.2 การปรับปรุงนโยบายและมาตรการ : องค์กรควรพิจารณาการปรับปรุงนโยบายและมาตรการเพื่อเสริมสร้างความคล่องตัวต่อการโจมตีแบบฟิชชิง การใช้เทคโนโลยีป้องกันที่ทันสมัยและการสร้างการตรวจจับที่มีประสิทธิภาพสามารถช่วยให้องค์กรมีความปลอดภัยมากขึ้น

5.3.3 การสร้างวินัยและการรายงาน : ผู้บริหารควรสร้างวินัยและกระบวนการที่ชัดเจนในการรายงานข้อสงสัยเกี่ยวกับฟิชชิง การสร้างบรรยากาศที่เชื่อถือได้และการสนับสนุนในการรายงานจะช่วยให้ประเทศมีการตอบสนองที่รวดเร็วต่อภัยคุกคาม

5.3.4 การเปลี่ยนแปลงพฤติกรรม : การสร้างการตระหนักในพนักงานให้เข้าใจถึงพฤติกรรมที่เพิ่มความเสี่ยงต่อการโจมตีแบบฟิชชิงและสร้างบรรยากาศที่สนับสนุนการรายงานและความรับผิดชอบต่อการป้องกันก่อนที่จะเกิดความเสียหาย

5.3.5 การรักษาความต่อเนื่อง : ควรมีการรักษาความต่อเนื่องในการฝึกอบรมและการส่งเสริมความตระหนักรู้เกี่ยวกับฟิชชิง เนื่องจากผู้โจมตีอาจปรับปรุงวิธีการของพวกเขาเสมอ

ดังนั้นการป้องกันตนเองและองค์กรจากการโจมตีแบบฟิชชิงนั้นมีความสำคัญอย่างยิ่ง ควรเริ่มต้นดำเนินการในขั้นตอนที่เหมาะสมเพื่อให้ผู้ใช้งานมีความคล่องตัวและปลอดภัยในโลกออนไลน์ที่เต็มไปด้วยภัยคุกคามนี้ และสำหรับการศึกษาในอนาคตควรคำนึงถึงข้อจำกัดดังกล่าว เพื่อประสิทธิผลที่ดีขึ้น

เอกสารอ้างอิง

Ali F. Al-Qahtani, Stefano Cresci. The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET Inf Secur*. 2022;16(5):324-345

Alzamil Zakarya, Aljurayyad Abdulmalik, Almajally Mohammed, Abuhemid Mohammed, Alsharafi Abdulmajeed, Alfreddi Bader. A HYBRID PHISHING DETECTION APPROACH FOR MOBILE APPLICATION. International Journal of Security and its Applications. 2020; 14. 15-28

Ashina Sadiq, Muhammad Anwar, Rizwan Asiam Butt, Farhan Masud. Internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies, 3(5), 854–864

B.B. Gupta, Nalin Asanka Gamagedara Arachchilage, Kostas E. Psannis. Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 67, 247–267 (2018)

Dhiman Sarma, Sohrab Hossain, Rana Joyti Chakma, Tanni Mittra. "Phishing Attacks Detection using Deep Learning Approach". 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 1180-1185

Duy Huynh, Phuc Luong, Hiroyuki Iida, Razvan Beuran. Design and Evaluation of a Cybersecurity Awareness Training Game. In: Munekata, N., Kunita, I., Hoshino, J. (eds) Entertainment Computing - ICEC 2017. ICEC 2017. Lecture Notes in Computer Science, vol 10507. Springer, Cham.

Gupta Brij, Yadav Krishna, Razzak Imran, Psannis Kostas, Castiglione Arcangelo, Chang Xiaojun. (2021). A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment. Computer Communications. 175. 47-57

H.S. Hota, A.K. Shrivas, Rahul Hota. An Ensemble Model for Detecting Phishing Attack with Proposed Remove-Replace Feature Selection Technique. Procedia Computer Science. Volume 132, 2018, Pages 900-907

Hussain Aldawood, Geoffrey Skinner. Reviewing Cyber Security Social Engineering Training and Awareness Programs, Skinner G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet. 2019; 11(3):73.

Jiann-Liang Chen, Yi-Wei Ma, Kuan-Lung Huang. Intelligent Visual Similarity-Based Phishing Websites Detection. Symmetry. 2020; 12(10):1681

Kieran Rendall, Antonia Nisioti, Alexios Mylonas. Towards a Multi-Layered Phishing Detection. Sensors. 2020; 20(16):4540

Mohammad Hijji, Gulzar Alam. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors. 2022; 22(22):8663.

Saad Al-Ahmadi, Afran Alotaibi, Omar Alsaleh. "PDGAN: Phishing Detection With Generative Adversarial Networks". in IEEE Access, vol. 10, pp. 42459-42468, 2022

Sadiq Ashina, Anwar Muhammad, Butt Rizwan, Masud Farhan, Shahzad Muhammad Kashif, Naseem, Younas Muhammad. A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies. 2021; 3. 10.1002/hbe2.301

Talal Alharbi, Asifa Tassaddiq. Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data and Cognitive Computing. 2021; 5(2):23.

Xun Dong, J. A. Clark and J. L. Jacob. "User behaviour based phishing websites detection". 2008 International Multiconference on Computer Science and Information Technology, Wisla, Poland, 2008, pp. 783-790

ภาคผนวก

1. หลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

เอกสารประกอบการอบรม

หลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

กำหนดการ :
วันที่ 22 มีนาคม 2567
ระยะเวลา:
30 นาที

วัตถุประสงค์
หลักสูตรนี้มีวัตถุประสงค์พนักงานขององค์กรได้ตระหนักถึงความเสี่ยงและภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศรวมไปถึงแนวทาง วิธีการในการควบคุมเพื่อให้องค์กรสามารถลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม

หัวข้อบรรยาย

- Cyber-attack. You are the target!!
- Phishing
- Social engineering
- Working Remote
- Mobile Security

INSTRUCTOR

ณภัทร ทารมย์
Napat Tarom

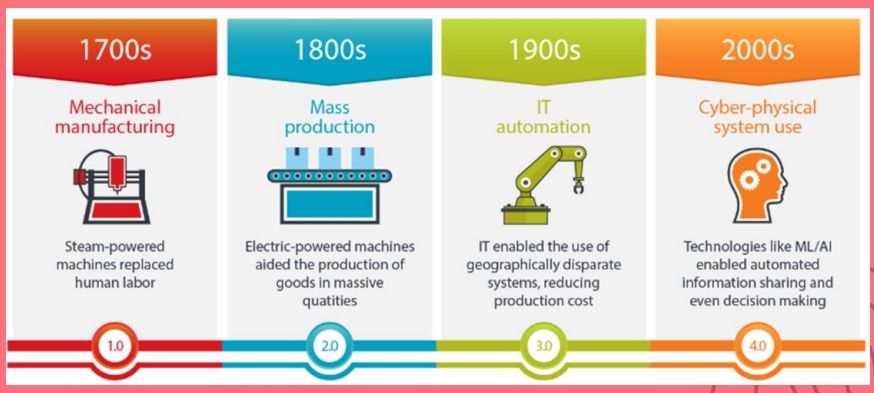
Cybersecurity and Privacy Consultant

E-mail: aud.napat@Hotmail.com
Mobile. 080-4959965

AGENDA

1. Cyber-attack. You are the target!!
2. Phishing
3. Social engineering
4. Working Remote
5. Mobile Security

The Evolution



CYBER ATTACK YOU ARE TARGET

THE PROBLEM?

การโจมตีทางไซเบอร์เป็นการที่คุณเป็นเป้าหมายของผู้โจมตีทางไซเบอร์ ซึ่งอาจทำให้ข้อมูลสำคัญของคุณถูกเข้าถึงและถูกนำไปใช้ในทางที่ไม่เหมาะสม ดังนั้นควรรักษาความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลของคุณอย่างเคร่งครัดเสมอ และไม่ควรเผชิญกับความเสี่ยงโดยไม่มีการป้องกันอย่างเหมาะสม

WHAT ARE THE COMMON WAYS THAT CYBER CRIMINALS ATTACK?

- การส่งลิงก์ผ่านอีเมลที่เปิดเว็บไซต์ที่เป็น malicious website.
- การใส่โทรจันในคอมพิวเตอร์ของเป้าหมายผ่านการแนบไฟล์ในอีเมล
- การสร้างอีเมลปลอมเพื่อดูเหมือนว่ามาจากแหล่งที่มีความน่าเชื่อถือสูงเพื่อหลอกลวงผู้รับ
- การปลอมตัวเป็นผู้ขายหรือแผนกไอทีและและมีการโทรติดต่อผ่านโทรศัพท์
- แฮกเป็นตัวกลางระหว่างบริษัทและลูกค้าของพวกเขาเพื่อดักจับข้อมูลที่ถูกส่งผ่านระหว่างบริษัทและลูกค้าของพวกเขาทั้งหมด

WHAT IS A PHISHING ATTACK?

Phishing attack เป็นการโจมตีด้านความปลอดภัยของข้อมูลออนไลน์ที่เป้าหมายเป็นผู้ใช้งานอินเทอร์เน็ต โดยการโจมตีนี้จะใช้เทคนิคการปลอมแอปพลิเคชันหรือเว็บไซต์ขององค์กรที่เป็นเป้าหมาย แล้วก็สร้างลิงค์หรือส่งอีเมล์เพื่อเชิญผู้ใช้งานคลิกเข้าไปยังเว็บไซต์ปลอมที่จะขโมยข้อมูลส่วนบุคคลหรือข้อมูลเชิงลึกของผู้ใช้งานออนไลน์ หรืออาจเกิดขึ้นได้จากผู้ไม่หวังดีที่ต้องการขโมยข้อมูลส่วนตัว เช่น หมายเลขบัตรเครดิต ชื่อผู้ใช้งานและรหัสผ่าน หรืออาจเป็นการติดตั้งโปรแกรมอันตรายลงในเครื่องคอมพิวเตอร์ของผู้ใช้งาน

PHISHING EMAIL

- Phishing accounts for 90% of data breaches
- Phishing attempts have grown 65% in the last year
- 30% of phishing messages get opened by targeted users (Verizon)
- Around 1.5m new phishing sites are created each month (Webroot)
- The average financial cost of a data breach is $3.86 Million (IBM)

Ransomware Attacks

เรียกค่าไถ่เพื่อ
ปลดล็อคข้อมูล

Ransomware

Ransomware คือการที่ผู้คุกคามเข้าถึงข้อมูลส่วนตัวของเป้าหมาย จากนั้นทำการเข้ารหัสและเรียกร้องค่าไถ่เพื่อแลกกับข้อมูลที่สำคัญนั้น โดยมีเทคนิคการขู่กรรโชกหลายรูปแบบ ทั้งนี้ Ransomware เป็นหนึ่งในภัยคุกคามที่มีชื่อเสียงและมีการเผยแพร่อย่างมาก โดยสามารถดูสถิติการโจมตีได้จากกราฟด้านล่าง

How ransomware work?

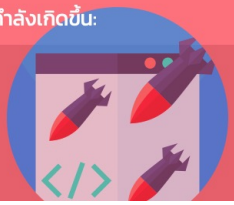
1. ผู้ไม่ประสงค์ดีส่งข้อความที่มี ransomware
2. เหยื่อเปิดข้อความดังกล่าวและเปิดไฟล์ที่มีมัลแวร์อยู่
3. Ransomware ทำงานและติดตั้งบนเครื่องเหยื่อ
4. ไฟล์ในคอมพิวเตอร์ของเครื่องเหยื่อถูกเข้ารหัส
5. มีข้อความแจ้งให้จ่ายเงินค่าไถ่ก่อนถึงกำหนดเวลา
6. การจ่ายค่าไถ่สามารถจ่ายเป็นเหรียญ bitcoin
7. การจ่ายเงินอาจได้รับไฟล์คืน หรือไม่ได้รับ
   หากได้รับไฟล์คืนหมายถึงผู้ไม่ประสงค์ดีได้ทำการปลดล็อคไฟล์ผ่าน Key ที่ทำการเข้ารหัสไฟล์ไว้

วิธีการสังเกตุเหตกาณ์ด้าน CYBER ATTACK

โดยการตรวจสอบสัญญาณเหล่านี้ องค์กรจะมีอุปกรณ์เครื่องมือที่ดีกว่าในการตรวจจับและตอบสนองต่อการโจมตีด้านความปลอดภัยดิจิทัลก่อนที่จะก่อให้เกิดความเสียหายที่สำคัญ

วิธีการสังเกตุเหตกาณ์ด้าน CYBER ATTACK

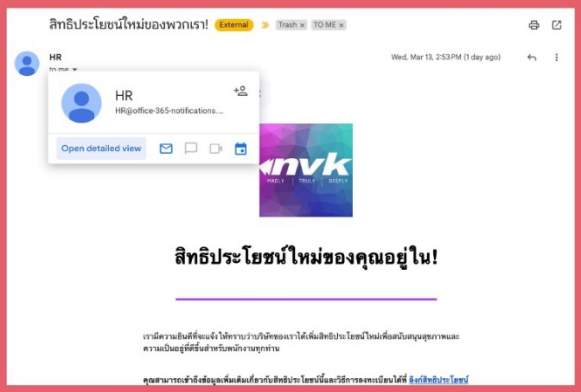
การตรวจจับการโจมตีไซเบอร์อาจเป็นเรื่องยาก เนื่องจากผู้โจมตีมักใช้เทคนิคที่ซับซ้อนเพื่อหลีกเลี่ยงการตรวจจับ อย่างไรก็ตาม นี่คือสัญญาณที่มักจะเป็นตัวบ่งชี้ว่ามีการโจมตีไซเบอร์กำลังเกิดขึ้น:

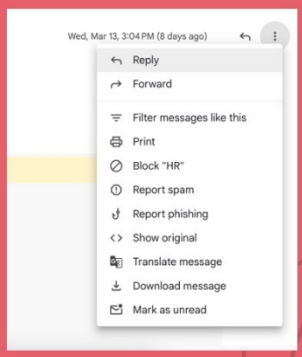


DETECTING AND DEFENDING AGAINST PHISHING ATTACKS

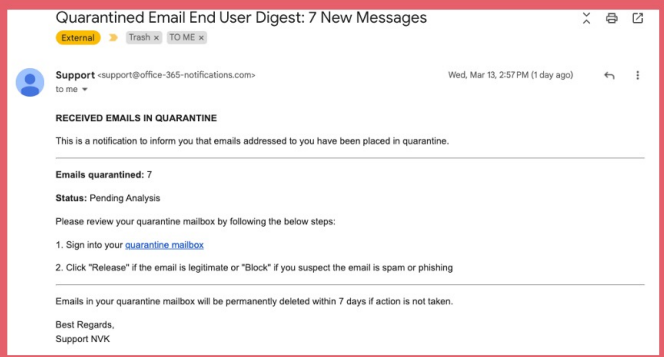
- Be cautious of unsolicited emails
- Use two-factor authentication
- Check for spelling and grammar mistakes:
- Keep your software up to date
- Look for HTTPS
- Use antivirus software

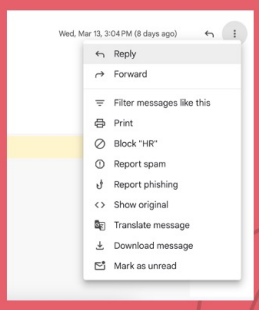
วิธีการสังเกตุเหตกาณ์ด้าน CYBER ATTACK



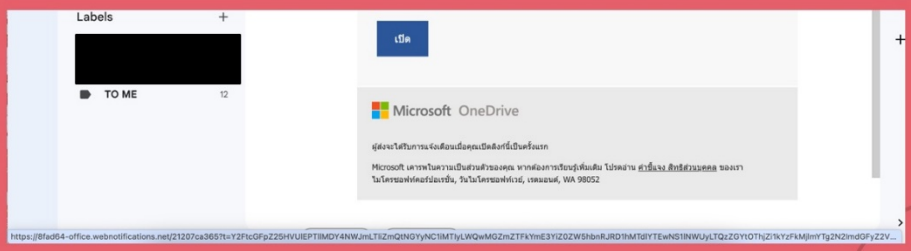


วิธีการสังเกตุเหตกาณ์ด้าน CYBER ATTACK



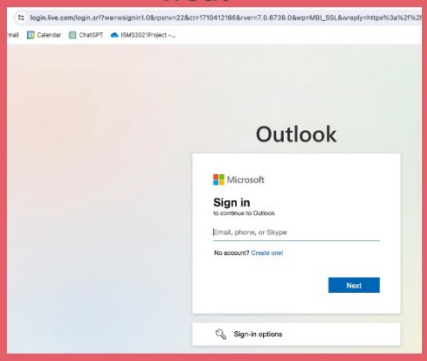


วิธีการสังเกตุเหตกาณ์ด้าน CYBER ATTACK

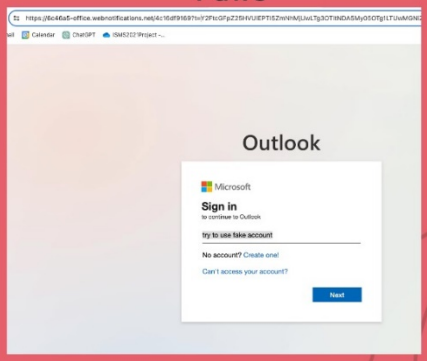


วิธีการสังเกตุเหตกาณ์ด้าน CYBER ATTACK

Real



Fake



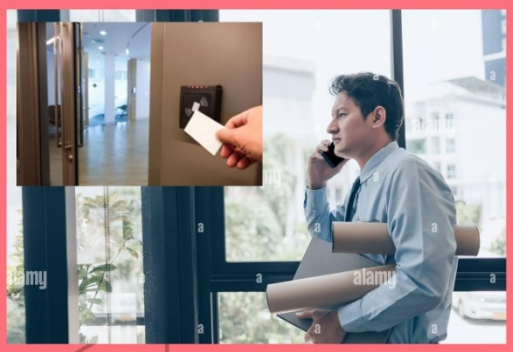
SOCIAL ENGINEERING

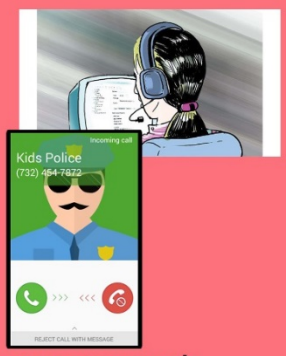

INTRODUCTION
TO SOCIAL
ENGINEERING
สร้างความน่าเชื่อถือให้เหยื่อ
หลงเชื่อใจแล้วตกหลุมพลาง
ขอตรวจดูรหัสผ่านที่ใช้งาน ณ ปัจจุบัน ว่าถูกหลักการและปลอดภัยหรือไม่


INTRODUCTION
TO SOCIAL
ENGINEERING
ปีเกิดของคุณ... ใช่วันที่นี้หรือไม่
ถ้าไม่ใช่กรุณาแก้ไขให้ให้ถูกต้อง
ด้วย
HR ตัวปลอมที่แกล้งโทรมาเพื่อหลอกถามถึงข้อมูลส่วนบุคคล


INTRODUCTION
TO SOCIAL
ENGINEERING
ผมต้องการที่จะให้คุณ
เปลี่ยนรหัสผ่านให้ผมโดย
ด่วน ผมไม่มีเวลาแล้ว ถ้า
หากไม่ทำตาม ผมแจ้ง
เรื่องต่อหัวหน้าฝ่ายแน่
แล้วเราจะได้เห็นดีกัน
ตัวปลอมโทรมากดดัน IT เพื่อให้เปลี่ยนรหัสผ่าน โดยไม่ตามขั้นตอนปฏิบัติขององค์กร

INTRODUCTION TO SOCIAL ENGINEERING





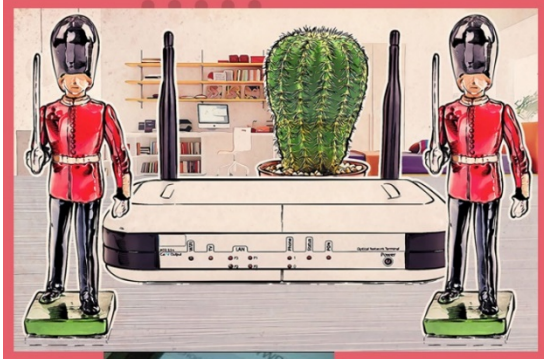
ตระหนักรู้และมีสติ สามารถลดความเสี่ยงที่จะโดน Social Engineering ได้

การป้องกันตัวจาก SOCIAL ENGINEERING

การป้องกันจากศิลปะการหลอกลวงผู้คนเพื่อผลประโยชน์ตามที่แฮกเกอร์ต้องการ

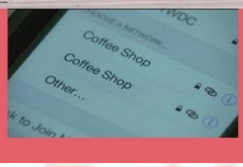
SAFE FROM WORKING REMOTE

ในยุคปัจจุบันการทำงานระยะไกล (WORKING REMOTELY) เป็นสิ่งที่มีความจำเป็นมากขึ้น ซึ่งทำให้ความปลอดภัยในการเชื่อมต่อเครือข่ายสำคัญมากยิ่งขึ้น การตรวจสอบความปลอดภัยของอุปกรณ์ที่ใช้งานระยะไกลเช่น โน๊ตบุ๊ค แท็บเล็ต และสมาร์ทโฟน เป็นสิ่งจำเป็น

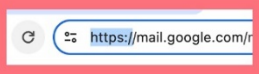


SAFE BROWSING ON PUBLIC WI-FI

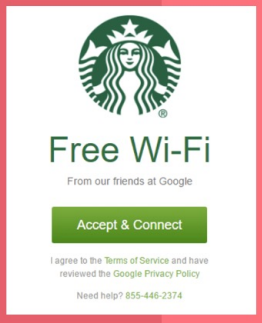
การใช้อินเทอร์เน็ตอย่างมั่นคง ปลอดภัยภายใต้เครือข่ายสาธารณะ

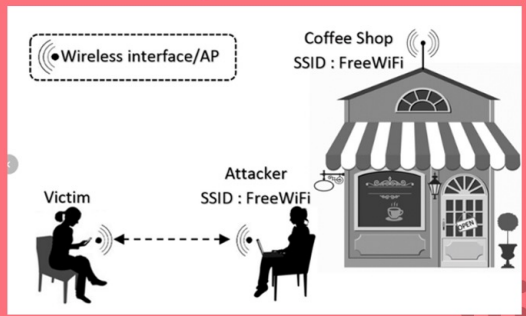


FREE WIFI ที่สนามบิน ปลอดภัยจริงไหม

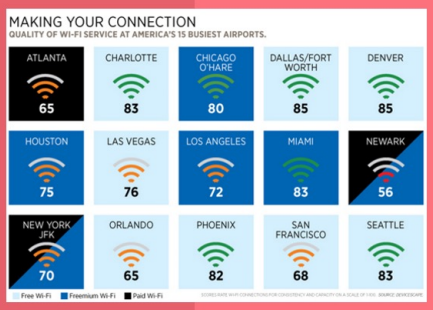


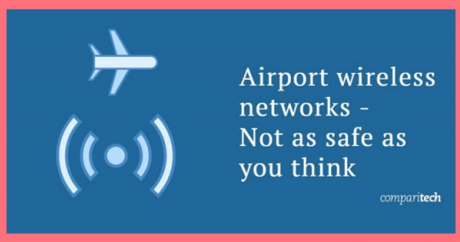
แน่ใจได้อย่างไรว่า SSID ที่เชื่อมต่ออยู่นั้นปลอดภัย





FREE WIFI ที่สนามบิน ปลอดภัยจริงไหม





การป้องกันภัยที่อาจเกิดจาก WORING REMOTE

การเพิ่มความปลอดภัยในการทำงานระยะไกล

- ควรให้การฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
- กำหนดขอบเขตการทำงานชัดเจน
- ใช้อุปกรณ์ที่มีความปลอดภัย

การทำงานแบบ WORKING REMOTE

- ตั้งรหัสผ่านที่เข้มงวด
- ใช้โปรแกรมปลอดภัย
- ไม่เผยแพร่ข้อมูลส่วนตัว
- ใช้เครือข่ายคอมพิวเตอร์ที่ปลอดภัย
- ติดตั้งซอฟต์แวร์ป้องกันไวรัส
- อัปเดตซอฟต์แวร์

PASSWORD

รหัสผ่านที่ดีควรมีความซับซ้อนเพียงพอที่จะยากต่อการคาดเดา และควรจะมีความยาวไม่น้อยกว่า 12 ตัวอักษร โดยรหัสผ่านที่ดีควรประกอบไปด้วยตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก ตัวเลข และอักขระพิเศษ เพื่อเพิ่มความปลอดภัยให้กับบัญชีของคุณ

P@SSWORD
การตั้งพาสเวิร์ด

ควรเปลี่ยนรหัสผ่านของคุณอย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาตหรือการแฮกบัญชี นอกจากนี้ คุณควรหลีกเลี่ยงการใช้รหัสผ่านที่ซ้ำกันในบัญชีอื่น ๆ ของคุณ และหลีกเลี่ยงการใช้รหัสผ่านที่เหมือนหรือคล้ายกันกับข้อมูลส่วนตัวของคุณ เช่น วันเกิด ชื่อสัตว์เลี้ยง หรือที่อยู่บ้าน

THE TOP (WORST) PASSWORDS

RANK	PASSWORD	RANK	PASSWORD	RANK	PASSWORD
1	123456	11	1234567	21	SUPERMAN
2	PASSWORD	12	MONKEY	22	696969
3	12345	13	LETMEIN	23	123123
4	12345678	14	ABC123	24	BATMAN
5	QWERTY	15	111111	25	TRUSTNO1
6	123456789	16	MUSTANG		
7	1234	17	ACCESS		
8	BASEBALL	18	SHADOW		
9	DRAGON	19	MASTER		
10	FOOTBALL	20	MICHAEL		

Credit: SplashData

P@SSWORD

Create Strong Passwords

1. เทคนิค : ตั้งพาสเวิร์ดที่จำได้ 1 ชุด แต่ต่อท้ายด้วยคำที่หมายถึงโซเชียลมีเดียต่าง ๆลงไป สมมติว่าฉันมีแมวที่ชื่อเพนกวิน และ Penguin เกิดในปี 2015 รหัสผ่านของฉันเป็นไปได้

penguin2015

FB: penguin2015!FB

TW: penguin2015!TW

Create Strong Passwords

2. เทคนิค : สุ่มสี่คำ (Four random common words)
ตัวอย่างเช่น olivia-mimigumo-waikiki-yesterday
แปลงเป็นพาสเวิร์ดได้ว่า 0li1v1a-m1m1gum0-wa1k1k1-y3st3rday เท่านี้ก็จะได้รหัสที่เดายากขึ้นแล้ว

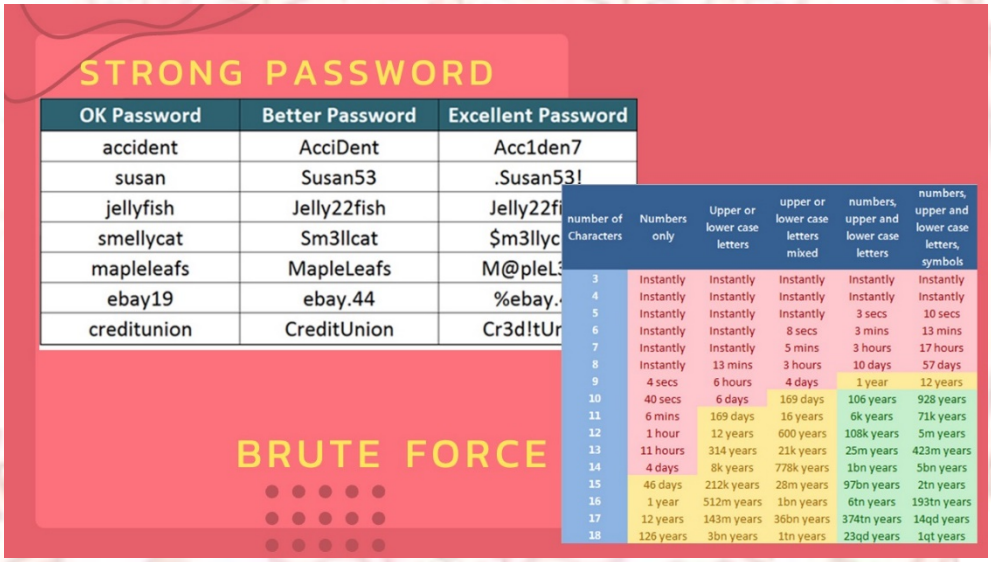
Create Strong Passwords

3. เทคนิค : PAO method
ตัวอย่างเช่น "Monkey D. Luffy jumping on a bouncy castle in Osaka"
เราก็จะได้รหัสที่มีแค่เราที่จำได้คือ MKDLFjmp1ng@bc@0saka แล้ว

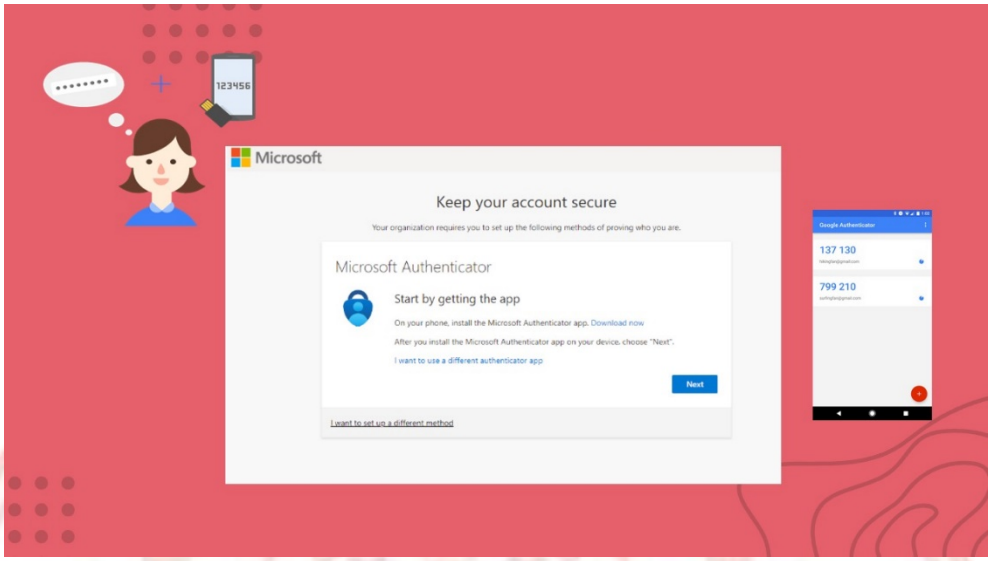
Create Strong Passwords

4. เทคนิค : ใช้เพลงที่ชอบเป็นภาษาคาราโอเกะ แปลเป็นคาราโอเกะ คือ Por Sor 2504 PhuYai Lee Tee Klong Pra Chum
อาจจะแปลงเป็นพาสเวิร์ดได้ว่า ps2504PYLtkpc


Create Strong Passwords
5.
เทคนิค : พิมพ์คำที่ชอบในภาษาไทยบนแป้นพิมพ์อังกฤษ
คำว่า สาวบางโพนั้นโก้จริงๆ ได้รหัสเป็น
lk;[k'FroyhoFdhOib'qlk
P@SSWORD


STRONG PASSWORD
OK Password
Better Password
Excellent Password
accident
AcciDent
Acc1den7
susan
Susan53
.Susan53!
jellyfish
Jelly22fish
smellycat
Sm3llcat
mapleleafs
MapleLeafs
ebay19
ebay.44
creditunion
CreditUnion
BRUTE FORCE
number of Characters
Numbers only
Upper or lower case letters
upper or lower case letters mixed
numbers, upper and lower case letters
numbers, upper and lower case letters, symbols
3 Instantly Instantly Instantly Instantly Instantly
4 Instantly Instantly Instantly Instantly Instantly
5 Instantly Instantly Instantly 3 secs 10 secs
6 Instantly Instantly 8 secs 3 mins 13 mins
7 Instantly Instantly 5 mins 3 hours 17 hours
8 Instantly 13 mins 3 hours 10 days 57 days
9 4 secs 6 hours 4 days 1 year 12 years
10 40 secs 6 days 169 days 106 years 928 years
11 6 mins 169 days 16 years 6k years 71k years
12 1 hour 12 years 600 years 108k years 5m years
13 11 hours 314 years 21k years 25m years 423m years
14 4 days 8k years 778k years 1bn years 5bn years
15 46 days 212k years 28m years 97bn years 2tn years
16 1 year 512m years 1bn years 6tn years 193tn years
17 12 years 143m years 36bn years 374tn years 14qd years
18 126 years 3bn years 1tn years 23qd years 1qt years


123456
Google Authenticator
137 130
799 210
TWO FACTOR AUTHENTICATION (2FA)
2FA ย่อมาจากคำว่า Two-Factor Authentication หมายถึงการใช้วิธีการยืนยันตัวตนสองชั้นเพื่อเข้าถึงบัญชีหรือระบบต่างๆ ซึ่งวิธีการยืนยันตัวตนสองชั้นนี้จะป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาตหรือการแฮกบัญชีที่ใช้รหัสผ่านเดียว


123456
Microsoft
Keep your account secure
Your organization requires you to set up the following methods of proving who you are.
Microsoft Authenticator
Start by getting the app
On your phone, install the Microsoft Authenticator app. Download now
After you install the Microsoft Authenticator app on your device, choose "Next".
I want to use a different authenticator app
Next
I want to set up a different method
137 130
799 210


MOBILE SECURITY
เรื่องของ Mobile Security เป็นเรื่องที่สำคัญมากในยุคปัจจุบัน เนื่องจากเราใช้โทรศัพท์มือถือในการทำกิจกรรมต่าง ๆ ทั้งการสื่อสาร การซื้อขาย การทำธุรกรรมการเงิน และอื่น ๆ ดังนั้นการรักษาความปลอดภัยในโทรศัพท์มือถือเป็นสิ่งสำคัญอย่างยิ่ง เพื่อช่วยให้ผู้ใช้ไม่ต้องเผชิญกับความเสี่ยงที่อาจเกิดขึ้นได้ เราจึงมีข้อควรระวังและวิธีป้องกัน


การใช้อุปกรณ์ส่วนบุคคลอย่างมั่นคงปลอดภัย สามารถทำได้โดยการปฏิบัติตามขั้นตอนและเทคนิคต่าง ๆ ดังนี้:
อัปเดตซอฟต์แวร์
ใช้รหัสผ่านที่ปลอดภัย
ใช้เทคโนโลยีการยืนยันตัวตนสองชั้น (2FA)
ใช้โปรแกรมและแอปพลิเคชันปลอดภัย
ไม่ควรเชื่อมต่อกับเครือข่ายไร้สายไม่ปลอดภัย
ไม่เปิดเผยข้อมูลส่วนตัว

SECURE WI-FI

การเชื่อมต่อกับ Wi-Fi ไม่ปลอดภัยอาจเป็นอันตรายต่อความเป็นส่วนตัวของคุณ ดังนั้นหากคุณต้องการใช้ Wi-Fi ให้แน่ใจว่าเป็น Wi-Fi ที่ปลอดภัย โดยสามารถดูและระบุได้ตามขั้นตอนด้านล่างนี้:

- ใช้ Wi-Fi ที่มีการเข้ารหัสข้อมูลด้วย WPA2/WPA3
- ตรวจสอบชื่อ Wi-Fi: ตรวจสอบชื่อ Wi-Fi ก่อนที่จะเชื่อมต่อ ให้แน่ใจว่าเป็นชื่อ Wi-Fi ที่ถูกต้อง
- ในการเข้าชมเว็บไซต์ในระหว่างใช้ Wi-Fi ต้องตรวจสอบว่าเว็บไซต์มีการเข้ารหัสข้อมูลด้วย HTTPS หรือไม่
- ปิดการเชื่อมต่ออัตโนมัติ
- อัปเดตโปรแกรมและแอปพลิเคชัน

LAPTOP & MOBILE DEVICES PROTECTION

การปกป้องความปลอดภัยของอุปกรณ์พกพา เช่น แล็ปท็อป และอุปกรณ์มือถือเป็นสิ่งที่สำคัญอย่างยิ่งในปัจจุบัน ดังนั้น การป้องกันอุปกรณ์ของคุณจากการแฮ็ก ไวรัส และการละเมิดความเป็นส่วนตัวควรเป็นความสำคัญสูงสุด ดังนี้เป็นวิธีการป้องกันที่ดีที่สุด:

- ติดตั้งซอฟต์แวร์แอนติไวรัส
- อัปเดตซอฟต์แวร์และเฟิร์มแวร์
- ใช้รหัสผ่านที่แข็งแกร่ง
- ใช้การยืนยันสองขั้นตอน

INFORMATION HANDLING

การจัดการข้อมูลเป็นสิ่งสำคัญที่สำคัญอย่างยิ่ง เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ดังนั้นนี่คือวิธีการจัดการข้อมูลที่ดี:

- การเข้ารหัสข้อมูล
- การสำรองข้อมูล
- การใช้งานคอมพิวเตอร์ส่วนตัว
- การควบคุมการเข้าถึง


การปฏิบัติตาม
IT SECURITY POLICY
ให้มีประสิทธิภาพ
การสนับสนุนการปฏิบัติตามนโยบาย
การประเมินความเสี่ยง
การอัปเดตนโยบาย
การตรวจสอบปฏิบัติตามนโยบาย
POLICY

ประวัติผู้วิจัย

ชื่อ : นายณภัทร ทารมย์

ชื่อการค้นคว้าอิสระ : การประเมินความเสี่ยงจากการโจมตีโดยการหลอกลวง และ.การพัฒนาโปรแกรมฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับบริษัทเอกชน

สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประวัติการศึกษา

อนุปริญญา : สาขาอิเล็กทรอนิกส์การบิน คณะเทคโนโลยีอากาศยาน
สถาบันการบินพลเรือน

ปริญญาตรี : สาขาการจัดการการขนส่งสินค้าทางอากาศ คณะการจัดการเทคโนโลยีการบิน
สถาบันการบินพลเรือน

ประวัติการทำงาน

- พฤษภาคม พ.ศ. 2567 – ปัจจุบัน :
  - ทำงาน บริษัท กสิกร บิซิเนส-เทคโนโลยี กรุ๊ป ตำแหน่ง IT Security Architect
- มกราคม พ.ศ. 2567 – เมษายน พ.ศ. 2567 :
  - ทำงาน บริษัท เอซีอินโฟเทค จำกัด ตำแหน่ง Cybersecurity and Privacy Consultant
- ธันวาคม พ.ศ. 2565 - มกราคม พ.ศ. 2567 :
  - ทำงาน บริษัท ACCENTURE SOLUTIONS CO., LTD. (Thailand)
    ตำแหน่ง SW/APP/Cloud Tech Support Analyst
- พฤศจิกายน พ.ศ. 2564 - ธันวาคม พ.ศ. 2565 :
  - ทำงาน บริษัท เน็ตไบร์ท จำกัด ตำแหน่ง Network Support Engineer
- มกราคม พ.ศ. 2564 - ตุลาคม พ.ศ. 2564 :
  - ทำงาน บริษัท เอ็น.วี.เค.อินเตอร์ จำกัด ตำแหน่ง IT Support