

GPSC Awareness Training 2023



Content

Topic	Page
1. Training and Campaign : Phishing	4-8
2. Training and Campaign : IT Policy	10-13
3. Training and Campaign : Cyber Policy	15-18
4. Training and Campaign : Cyber Awareness	20-24
5. Training and Campaign : ACT Spirit Program	26-28
• Awareness Training: Ransomware Attack	26
• Awareness Training: Cybersecurity and Cyber Threat	27
• Awareness Training: AI-Based Predictive Social Engineering	28



1. Training and Campaign : Phishing

Campaign and Training Details:

Objective: To build the awareness regarding “Phishing” in any methods for GPSC employees.

Target: GPSC employees in any level

Methodology:

- Public relations about “Phishing” from GPSC executive team via email, Sharepoint and LINE official
- Online training course in iSpark (100% passed score for examination)
- Lucky draw for attendees who finish the online training



Campaign PR : Phishing



คุณกุลพัฒน์ เพิ่มภูศรี
รองกรรมการผู้จัดการใหญ่กลุ่มธุรกิจ
และบริหารระบบไอที

CYBERSECURITY AWARENESS

“ Phishing Mail คือ อีเมลหลอกลวงที่หลอกล่อให้เหยื่อเผยข้อมูลต่างๆ รหัสผ่าน, user-password, หมายเลขบัตรประจำตัว ฯลฯ รวมถึงหลอกให้กดลิงค์เชื่อมโยงไปยัง Website ปลอม หรือเปิดไฟล์แนบเพื่อแอบติดตั้งมัลแวร์ลงบนคอมพิวเตอร์ ทำให้เกิดความเสียหายต่างๆ ได้ ”

พวกเราทุกคนต้องมีสติก่อนคลิก ใช้สติก่อนแชร์ ไม่แน่วใจให้รายงาน

Phishing Mail

เริ่มเกม

เริ่มเล่นเกม
สนุกคลิกเลย!
CLICK!

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”
ทดสอบความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !

Phishing Mail

เริ่มเล่นเกม
สนุกคลิกเลย!
CLICK!

เล่นเกมง่าย !!!
แถมจริง !!!


กติการ่วมกิจกรรม

- เล่นเกมชิงรางวัล ต่อที่ 1 “ใครเร็วและแม่นยำที่สุดคนนั้นได้”
ลุ้นรับบัตรเงินสดเติมเงิน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์ สำหรับผู้ที่เล่นเกมชนะทุกข้อและเร็วที่สุด 10 อันดับแรก สามารถเล่นได้ทุกสัปดาห์
- เล่นเกมชิงรางวัล ต่อที่ 2 เล่นเกม 4 เกม ภายในเดือนมิถุนายน 2565
ลุ้นรับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล โดยสุ่มชิงรางวัล (ขอสงวนรางวัลสำหรับผู้ที่ยังไม่ได้ชิงรางวัล จากต่อที่ 1)
- ประกาศรางวัลในต้นเดือน กรกฎาคม 2565

สอบถามข้อมูลเพิ่มเติมที่ : คุณพงษ์เทพ ม่วงแก้ว PONGTHEP.M@GPSCGROUP.COM หรือ คุณรัชรินทร์ เชื้ออริยา RATCHARINU@GPSCGROUP.COM

วิธีการเล่น

1. คลิก Link ที่ Banner
2. Log in ด้วย iSpark
3. กดปุ่ม Enrolled
4. กด Start Learning เพื่อเริ่มเล่นเกม



เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์”
ทดสอบความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !

Phishing Mail

เริ่มเกม

เริ่มเล่นเกม
สนุกคลิกเลย!
CLICK!

กติการ่วมกิจกรรม

- เล่นเกมชิงรางวัล ต่อที่ 1 “ใครเร็วและแม่นยำที่สุดคนนั้นได้”
ลุ้นรับบัตรเงินสดเติมเงิน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์ สำหรับผู้ที่เล่นเกมชนะทุกข้อและเร็วที่สุด 10 อันดับแรก สามารถเล่นได้ทุกสัปดาห์
- เล่นเกมชิงรางวัล ต่อที่ 2 เล่นเกม 4 เกม ภายในเดือนมิถุนายน 2565
ลุ้นรับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล โดยสุ่มชิงรางวัล (ขอสงวนรางวัลสำหรับผู้ที่ยังไม่ได้ชิงรางวัล จากต่อที่ 1)
- ประกาศรางวัลในต้นเดือน กรกฎาคม 2565
- วิธีการเล่น (คลิกที่นี่)

ดาวน์โหลดแอปพลิเคชัน : แอปพลิเคชัน GPSC (Android) หรือ GPSC (iOS) หรือ GPSC (Windows) หรือ GPSC (Mac) หรือ GPSC (Linux) หรือ GPSC (Other OS)



Make everyday a learning day!

Username or Email

Password

Remember me Forget Password?

Login

Revolutionizing the way people learn, teach, and develop in the age of transformation

Current version 4.0.0.1
Powered by GoSkills



Phish Phishing Mail

Enrolled

Overview

GPSC Cyber Security and Skills Competency

GPSC Privacy Policy: [Click here to read GPSC Privacy Policy](#)

Version Number 4.1.0.1



Phish Phishing Mail

กด Start Learning

Overview

GPSC Cyber Security and Skills Competency

GPSC Privacy Policy: [Click here to read GPSC Privacy Policy](#)

Version Number 4.1.0.1

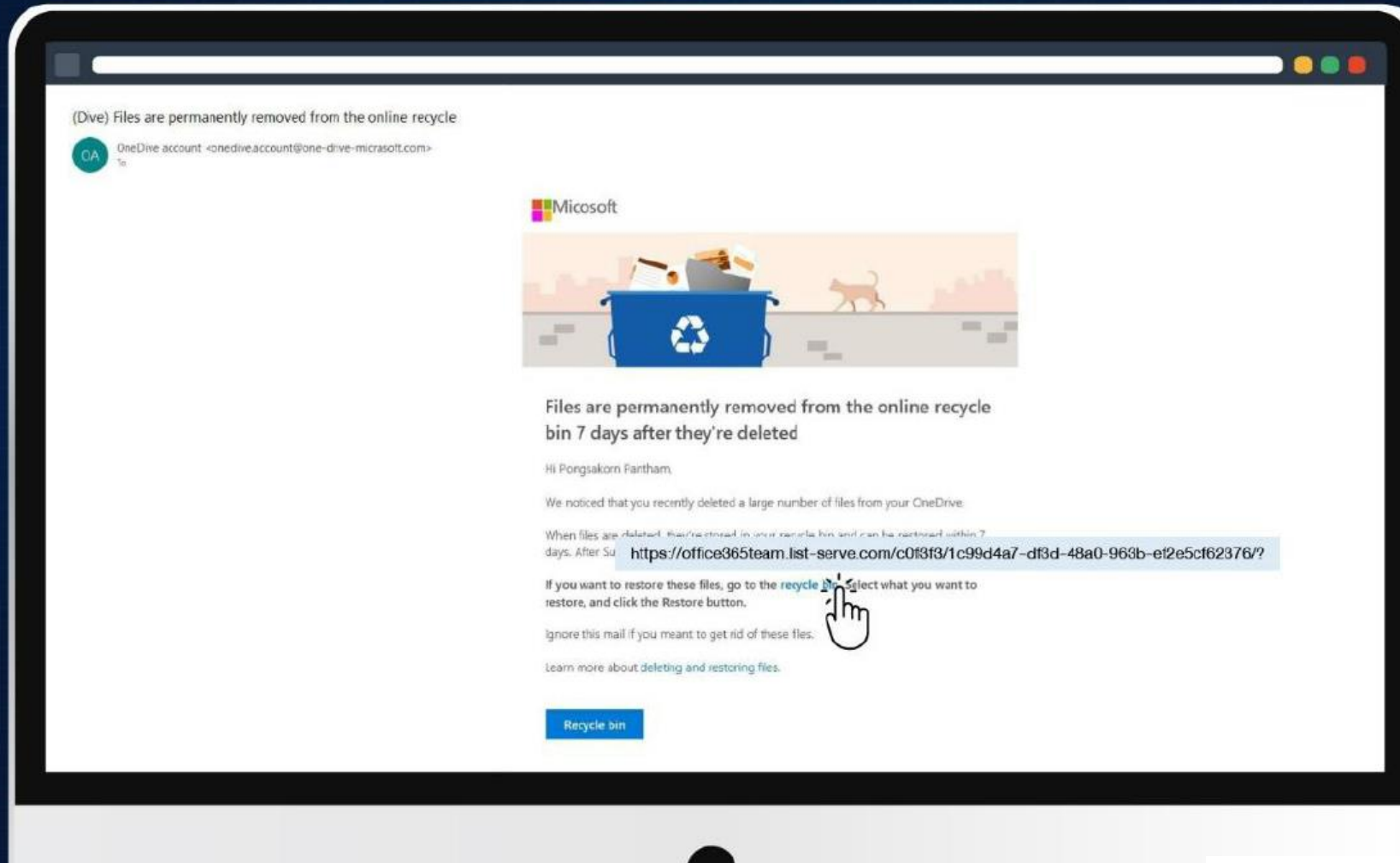
Online training : Phishing (100% passed score)



Online training : Phishing (100% passed score)

เมื่อได้รับ E-mail ต้องสังเกตอะไรบ้าง ?

กรุณาเลือกจุดสังเกต Phishing mail 3 จุด



Online training : Phishing (100% passed score)

E-mail นี้ปลอดภัยหรือไม่ ?

กรุณาระบุเหตุผลของแต่ละจุดสังเกตให้ถูกต้อง

(Dive) Files are permanently removed from the online recycle

OneDrive account <oaedrive.account@one-drive-microsoft.com>

1

A ถูกส่งมาจาก OneDrive ที่เราใช้งานอยู่ในปัจจุบัน

B น่าสงสัย เพราะเขียนคำว่า microsoft ผิด

A เนื้อหาน่าสงสัย เพราะเร่งรัดให้
รับดำเนินการและมี Link แบนมาด้วย

B เนื้อหาดูเหมือนเป็นการเขียนเพื่อแจ้งเตือน
ตามปกติ ต้องลองคลิก Link ดูก่อน
ว่าหน้าถัดไปเป็นอย่างไร

2

Files are permanently removed from the online recycle
bin 7 days after they're deleted

Hi Pongsakorn Fantham,

We noticed that you recently deleted a large number of files from your OneDrive.

When files are deleted, they're stored in your online recycle bin and can be restored within 7
days. After 7 days, they're permanently removed from the online recycle bin.

<https://office365team.list-serve.com/c013f3/1c99d4a7-d13d-48a0-963b-ef2e5cf62376/?>

If you want to restore these files, go to the recycle bin, select what you want to
restore, and click the Restore button.

Ignore this mail if you meant to delete these files.

Learn more about deleting and restoring files.

Recycle bin

3

A Link ที่แนบมาดูไม่น่าไว้วางใจ "office365team.list-serve.com" ไม่ยาวขนาดนี้

B office365team.list-serve.com เป็นของ microsoft จริง

Online training : Phishing (100% passed score)

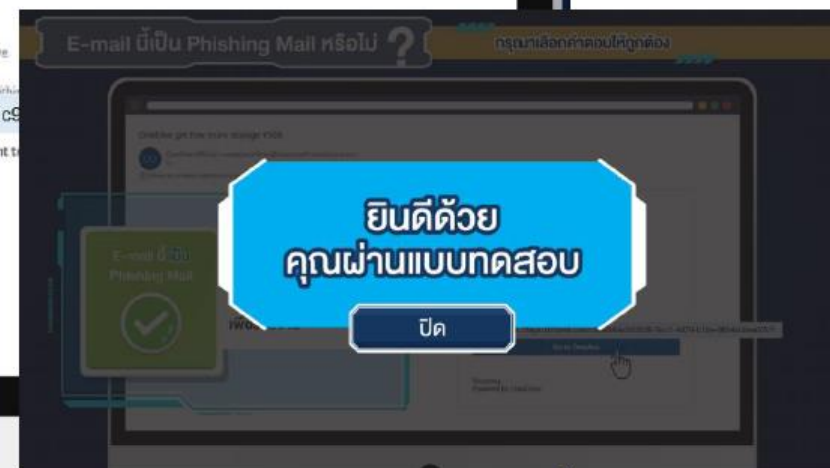
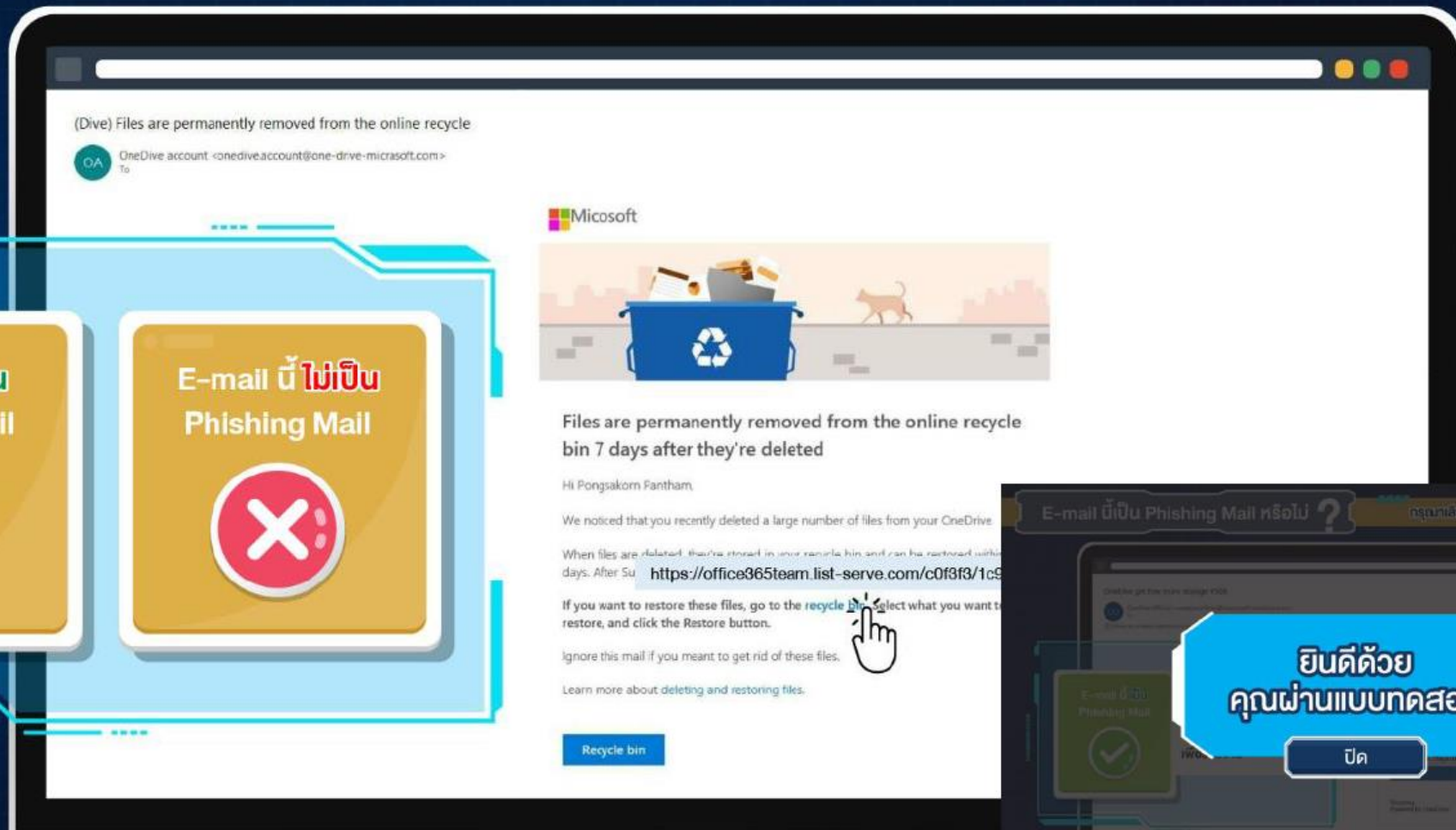
E-mail นี้เป็น Phishing Mail หรือไม่ ?

กรุณาเลือกคำตอบให้ถูกต้อง

E-mail นี้ เป็น
Phishing Mail



E-mail นี้ ไม่เป็น
Phishing Mail



2. Training and Campaign : IT Policy

Campaign and Training Details:

Objective: To educate and remind user regarding GPSC mandatory IT policy for GPSC employees.

Target: GPSC employees in any level

Methodology:

- Public relations about GPSC IT Policy ” from GPSC executive team via email, Sharepoint and LINE official
- Online training course in iSpark (100% passed score for examination)
- Lucky draw for attendees who finish the online training



Campaign PR : IT Policy





คุณศิริเมธ ลิ้มการณ
ประธานเจ้าหน้าที่ปฏิบัติการ

**CYBERSECURITY
AWARENESS**

“หัวใจสำคัญของการปฏิบัติการที่เป็นเลิศ ประกอบด้วย นโยบายและแนวทางปฏิบัติ ที่ใช้ในการกำกับให้ผู้ปฏิบัติงาน สามารถทำงานได้อย่างถูกต้องและมีประสิทธิภาพโดยเฉพาะอย่างยิ่ง นโยบายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ซึ่งต้องการให้ พนักงานทั่วทั้งองค์กรยึดถือในการใช้งานระบบสารสนเทศของบริษัทฯ

บริษัทฯ มีนโยบายด้านเทคโนโลยีสารสนเทศ ที่อยากให้พนักงานทำความเข้าใจและปฏิบัติตาม เพื่อป้องกันภัยคุกคาม ด้านสารสนเทศและไซเบอร์ และเพื่อความเป็นเลิศด้านการปฏิบัติการ

”



**CYBERSECURITY
AWARENESS**

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”
ทดสอบความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !



เริ่มเล่นเกม 2 (IT-Policy)
สนุกคลิกเลย !

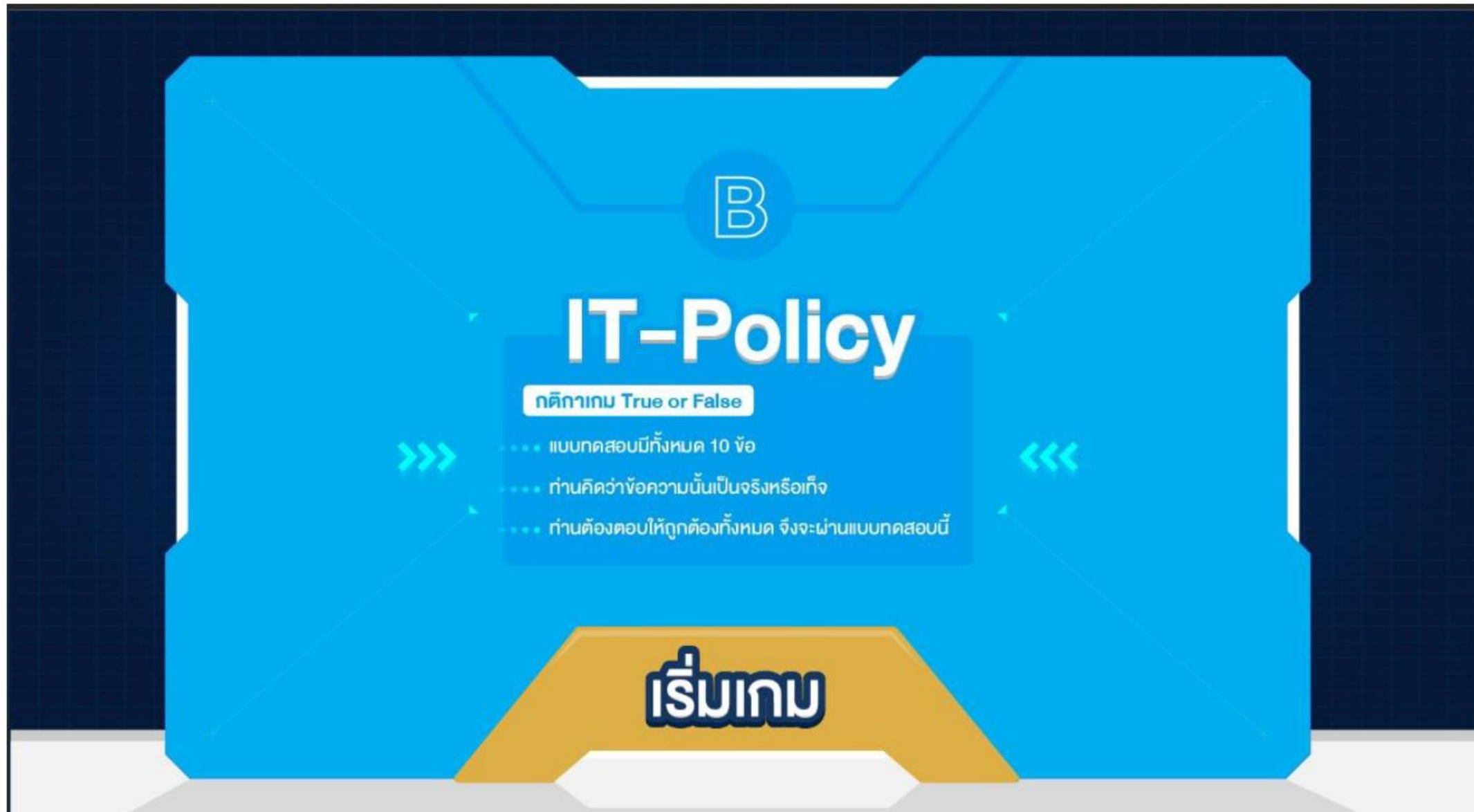
CLICK!

กติการ่วมกิจกรรม

- **เล่นเกมชิงรางวัล ต่อที่ 1 (ประจำสัปดาห์ วันที่ 16-22 มิถุนายน 2565)**
ลุ้นรับบัตรเงินสดเติมน้ำมัน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์ (ปิดสรุปรายชื่อผู้เข้าร่วมเล่นเกม ตั้งแต่ วันที่ 17-23 มิถุนายน 2565 เวลา 24.00 น.)
- **เล่นเกมชิงรางวัล ต่อที่ 2 เล่นครบ 4 เกม** ภายในเดือนมิถุนายน 2565
ลุ้นรับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล โดยสุ่มจับรางวัล (ขอสงวนรางวัลสำหรับผู้ที่ยังไม่ได้รับรางวัล จากต่อที่ 1)
- **ประกาศรางวัลในเดือนกรกฎาคม 2565**



Online training : IT Policy (100% passed score)



Online training : IT Policy (100% passed score)

โปรดอ่านข้อเท็จจริงต่อไปนี้แล้วเลือกว่า  หรือ 



พนักงานไม่ควรนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาเชื่อมต่อระบบของบริษัทโดยพลการ เพราะอาจมี malware แฝงตัวอยู่ในเครื่องส่วนตัว และแพร่กระจายเข้าระบบของบริษัทได้



พนักงานทุกคนต้องแจ้งหรือรายงานต่อหน่วยงาน IT กันทีเมื่อพบเหตุการณ์ที่อาจเป็นภัยต่อระบบหรือข้อมูลสารสนเทศของบริษัท



รหัสผ่านที่ดี ควรเปลี่ยนใหม่ทุก 90 วัน , ยาวเกิน 8 ตัว ประกอบด้วย ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และตัวอักขระพิเศษผสมกัน

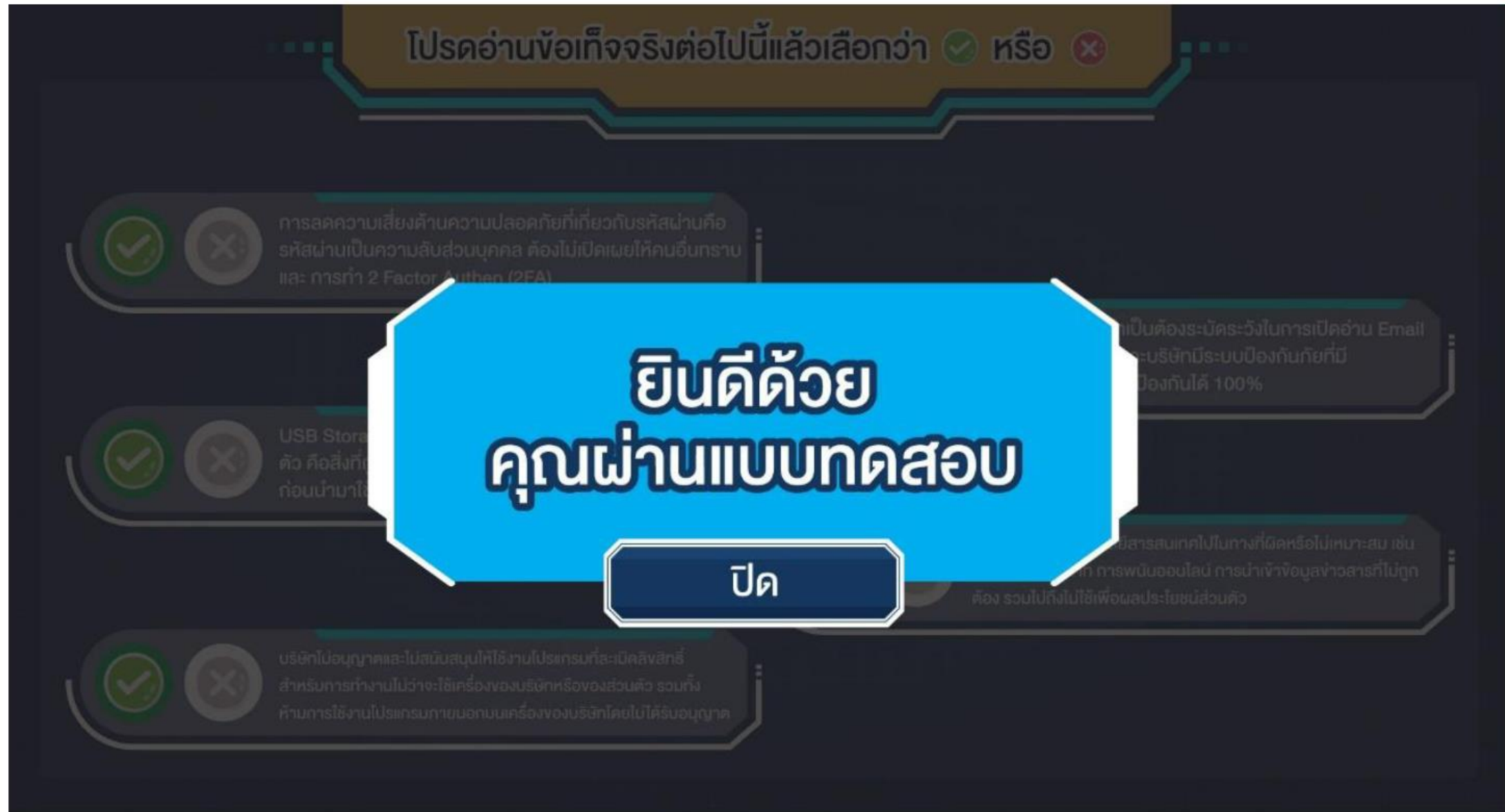


การส่งภาพอุบัติเหตุที่เกิดขึ้นในบริษัทลงโซเชียลกันก็เห็นเหตุการณ์เพื่อแจ้งให้เพื่อนร่วมงานทราบเหตุ ไม่ถือว่าเป็นการกระทำที่ขัดต่อนโยบายฯ IT ของบริษัท



ช่องทางหลักในการติดต่อแลกเปลี่ยนข้อมูลของบริษัท คือ email บริษัท และ พื้นที่เก็บข้อมูลบน Cloud ต้อง Sign-in ด้วย user name และรหัสผ่าน แบบเดียวกับที่ใช้ในระบบสารสนเทศของบริษัทเท่านั้น

Online training : IT Policy (100% passed score)



3. Training and Campaign : Cyber Policy

Campaign and Training Details:

Objective: To educate and remind user regarding GPSC Cybersecurity policy for GPSC employees.

Target: GPSC employees in any level

Methodology:

- Public relations about “GPSC Cybersecurity Policy” from GPSC executive team via email, Sharepoint and LINE official
- Online training course in iSpark
- Lucky draw for attendees who finish the online training



Campaign PR : Cyber Policy



CYBERSECURITY
AWARENESS

“ ข้อมูลของบริษัทมีความสำคัญและถือว่าเป็นทรัพย์สินอันมีค่า ซึ่งบริษัทให้ความสำคัญ มีระบบป้องกันและเฝ้าระวังเป็นอย่างดี อย่างไรก็ตามการโจมตีไซเบอร์ปัจจุบัน มุ่งโจมตีที่ตัวบุคคลโดยวิธีการ ต่างๆ เช่น Call center, Phishing Mail และถ้าผิดพลาด 1 ครั้ง ก็สามารถทำให้เกิดความเสียหายได้ จึงขอให้พวกเราทุกคน ช่วยกันปฏิบัติตาม นโยบายความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด ”



Cyber Policy

เริ่มเกม

คุณทีตพงษ์ จุลพรศิริดี
ประธานเจ้าหน้าที่บริหารการเงิน

CYBERSECURITY
AWARENESS

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”
ทดสอบความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !



Cyber Policy

เริ่มเกม

เริ่มเล่นเกมที่ 3
(Cyber Policy)
สนุกคลิกเลย !

CLICK!

เล่นง่าย !!!
แจกจริง !!!

เป้าหมาย
100%

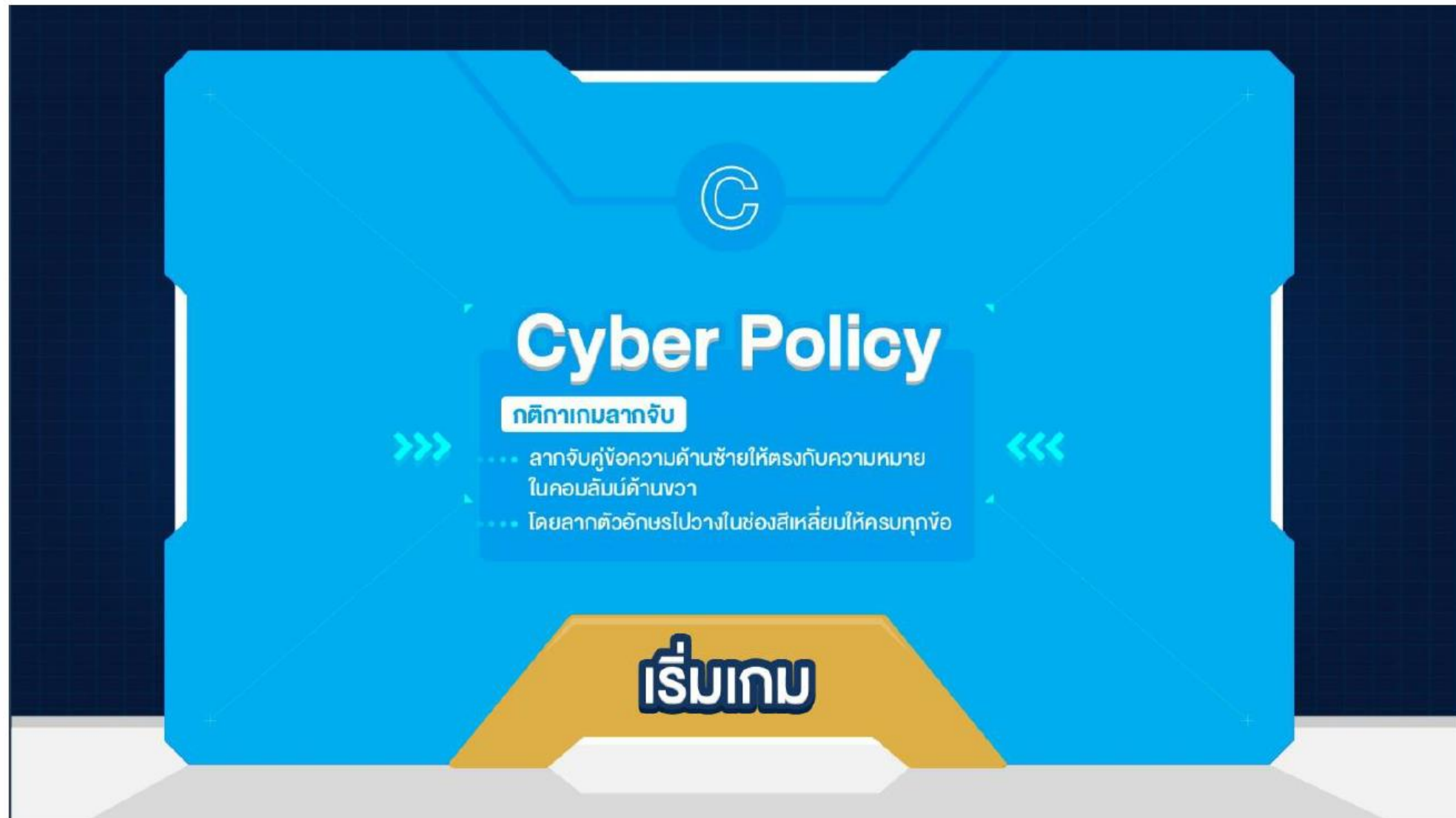


กติการ่วมกิจกรรม

- **เล่นเกมชิงรางวัล ต่อที่ 1 (ประจำสัปดาห์ วันที่ 24-29 มิถุนายน 2565)**
ลุ้นรับบัตรเงินสดเติมน้ำมัน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์ (เปิดสุ่มรายชื่อผู้เข้าร่วมเล่นเกม ตั้งแต่วันที่ 24-29 มิถุนายน 2565 เวลา 24.00 น.)
- **เล่นเกมชิงรางวัล ต่อที่ 2 เล่นครบ 4 เกม** ภายในเดือนมิถุนายน 2565
ลุ้นรับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล โดยสุ่มจับรางวัล (ขอสงวนรางวัลสำหรับผู้ที่ยังไม่ได้รับรางวัล จากต่อที่ 1)
- **ประกาศรางวัลในต้นเดือน กรกฎาคม 2565**

สอบถามข้อมูลเพิ่มเติมที่ : คุณพงษ์เทพ ปวงแก้ว PONGTHEP.M@GPSCGROUP.COM หรือ คุณรัชรินทร์ เชื้ออริยะ RATCHARINU@GPSCGROUP.COM

Online training : Cyber Policy (100% passed score)



Online training : Cyber Policy (100% passed score)

จงลากคำตอบ มาวางลงในช่องว่างให้ถูกต้อง

A » ปลอ่ยหน้าจอก้างทิ้งเอาไว้

B » ข้อมูลส่วนบุคคลรั่วไหล

C » Q89ajTS@me

D » โฟสต์ข้อมูลอันเป็นเท็จ

E » ลดความเสี่ยงจาก Malware โจมตี

F » การใช้งานโปรแกรมละเมิดลิขสิทธิ์

G » ผิดนโยบายการใช้งานอีเมล

H » P@\$w0rd

I » ป้องกัน Phishing Mail

J » Secure Web Site (HTTPS)

K » Network Access Control (NAC)

L » 2-Factor Authen (2FA)

มีความผิดตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

ตรวจสอบชื่อผู้ส่ง เนื้อหา Link และไฟล์ที่แนบมาทุกครั้งก่อนเปิดอ่าน

เข้าข่ายตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

นำอีเมลบริษัทไปสมัครบริการบัตรเครดิตและ Internet บ้าน

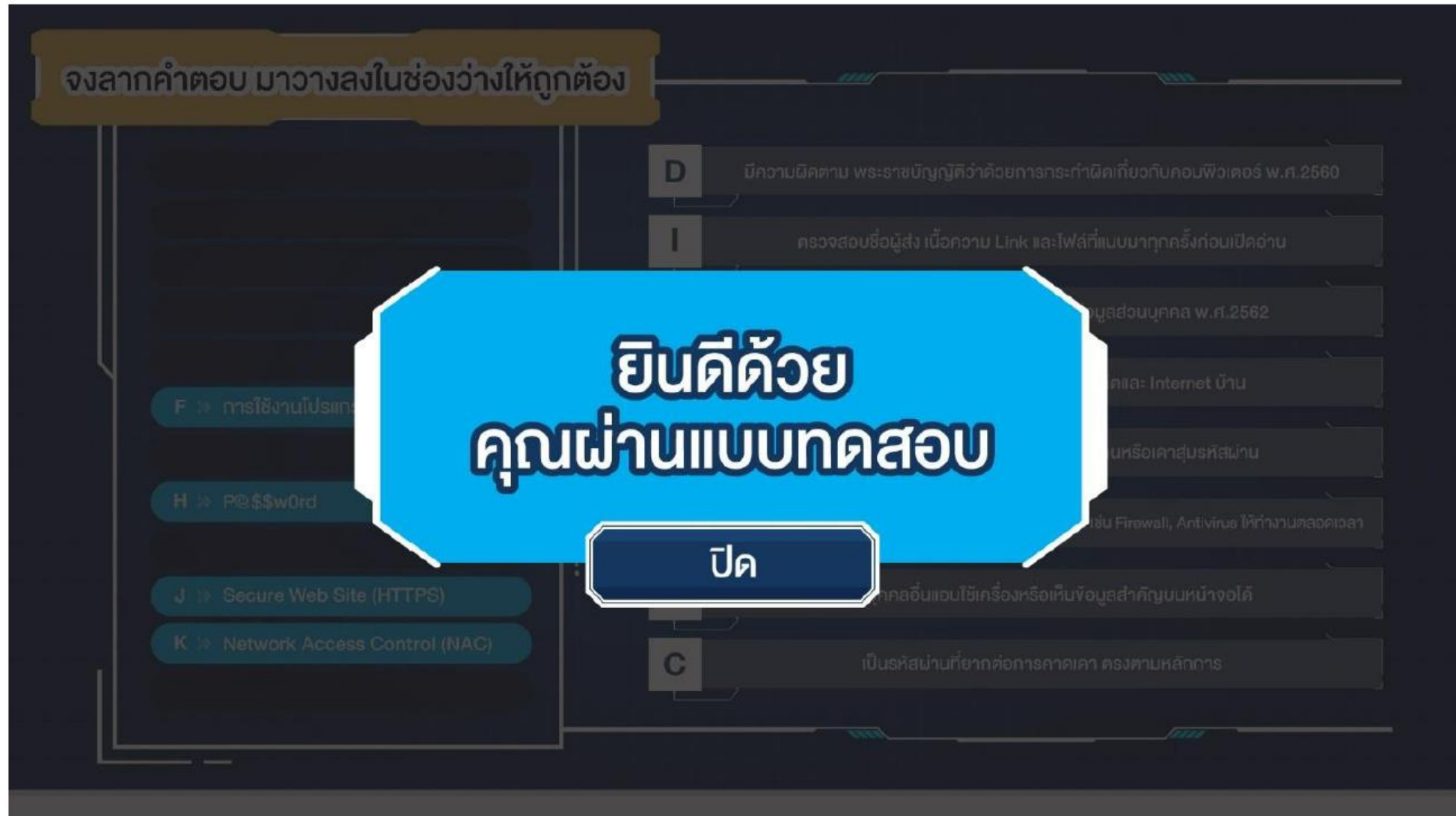
ช่วยลดความเสี่ยงหากผู้ไม่หวังดีรู้รหัสผ่านหรือเดาสຸ່มรหัสผ่าน

ไม่ download อะไรใหม่ๆ และตรวจเช็คให้ระบบป้องกันในเครื่อง เช่น Firewall, Antivirus ให้ทำงานตลอดเวลา

ทำให้บุคคลอื่นแอบใช้เครื่องหรือเห็นข้อมูลสำคัญบนหน้าจอได้

เป็นรหัสผ่านที่ยากต่อการคาดเดา ตรงตามหลักการ

Online training : Cyber Policy (100% passed score)



4. Training and Campaign : Cyber Awareness

Campaign and Training Details:

Objective: To educate and build awareness regarding cybersecurity and cyber threat for GPSC employees.

Target: GPSC employees in any level

Methodology:

- Public relations about Cybersecurity and cyber threat from GPSC executive team via email, Sharepoint and LINE official Online
- training course in iSpark
- Lucky draw for attendees who finish the online training



Campaign PR : Cyber Awareness

CYBERSECURITY AWARENESS

“ พวกเรา คือคนสำคัญที่จะช่วยบริษัท ปลอดภัยจากการโจมตีทางไซเบอร์
การโจมตีทางไซเบอร์มีรูปแบบและวิธีการใหม่ตลอดเวลา
พวกเราควรมีความตระหนักรู้ และ เมื่อพบความผิดปกติ
ให้รีบแจ้งทางหน่วยงานดิจิทัลและไซเบอร์ ให้รับทราบ
ความร่วมมือร่วมใจของทุกคนคือสิ่งสำคัญ ”



เริ่มเล่นเกมที่ 4
(Cyber Awareness)
สนุกคลิกเลย !

CLICK!

คุณรศยา เรียงวรรณ
รองกรรมการผู้จัดการใหญ่พัฒนาธุรกิจ



CYBERSECURITY AWARENESS

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”
ทดสอบความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !

เริ่มเล่นเกมที่ 4
(Cyber Awareness)
สนุกคลิกเลย !

CLICK!

กติการ่วมกิจกรรม

- **เล่นเกมชิงรางวัล ต่อที่ 1 (ประจำสัปดาห์ วันที่ 30 มิถุนายน - 6 กรกฎาคม 2565)**
ได้รับบัตรเงินสดเติมน้ำมัน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์
(ปิดสรุปรายชื่อผู้เข้าร่วมเล่นเกม ตั้งแต่ วันที่ 30 มิถุนายน - 6 กรกฎาคม 2565 เวลา 24.00 น.)
- **เล่นเกมชิงรางวัล ต่อที่ 2 เล่นครบ 4 เกม** ภายในเดือนมิถุนายน 2565
ได้รับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล
โดยสุ่มจับรางวัล (ขอสงวนรางวัลสำหรับผู้ที่ยังไม่ได้รับรางวัล จากต่อที่ 1)
- **ประกาศรางวัลในเดือน กรกฎาคม 2565**

เล่นง่าย !!!
แจกจริง !!!

เป้าหมาย 100%

GPSC

สอบถามข้อมูลเพิ่มเติมที่ : คุณพองนิพัทธ์ พ่วงแก้ว PONGTHEP.M@GPSCGROUP.COM หรือ คุณรัชรินทร์ ใจอริยะ RATCHARIN.U@GPSCGROUP.COM

Online training : Cyber Awareness (100% passed score)



Online training : Cyber Awareness (100% passed score)

กรุณาจับคู่อุปกรณ์กับวิธีใช้งานที่ถูกต้อง
ตามหลัก Cyber Awareness



Online training : Cyber Awareness (100% passed score)

กรุณาจับคู่อุปกรณ์กับวิธีใช้งานที่ถูกต้อง
ตามหลัก Cyber Awareness



Online training : Cyber Awareness (100% passed score)

กรุณาจับคู่อุปกรณ์กับวิธีใช้งานที่ถูกต้อง
ตามหลัก Cyber Awareness

**ยืนยันด้วย
คุณผ่านแบบทดสอบ**

ปิด

USB Storage

Social Media

รับมือด้วยการ
สำรองข้อมูล
เป็นประจำ และ
แยกเก็บไว้คนละที่

เป็นการยืนยันตัวตน
แบบหลายปัจจัย
เช่น รหัสผ่าน + OTP
เป็นต้น

ไม่
ข้อมูลทางอินเทอร์เน็ต
ออกสู่ภายนอก
โดยไม่ได้รับอนุญาต

เป็น
สิ่งควบคุม
ต้องขออนุญาต
ก่อนใช้งาน

อาจถูกดักจับข้อมูล
ดังนั้นใช้ Internet
ที่แชร์จากมือถือ
ปลอดภัยกว่า

หากเข้าเว็บไซต์
ของธนาคาร
ต้องมองหา
สัญลักษณ์นี้
ก่อนเสมอ

5. Training and Campaign : ACT Spirit Program

Campaign and Training Details:

Objective: To educate and build awareness on:

- Ransomware Attack
- Cybersecurity AI and Cyber Threat
- AI-Based Predictive Social Engineering

Target: GPSC employees in any level



Awareness Training: Ransomware Attack

ซอฟต์แวร์ผิดกฎหมายอันตรายกว่าที่คุณคิด

เสี่ยงด้านความปลอดภัย

- เสี่ยงต่อ Virus, Malware หรือ Ransomware รวมถึงการตกเป็นเหยื่อ Phishing
- ข้อมูลองค์กรรั่วไหล ข้อมูลลูกค้าถูกขโมย ข้อมูลส่วนบุคคลถูกนำไปใช้
- ถูกฉ้อโกงในการทำธุรกรรมออนไลน์

เสี่ยงด้านกฎหมาย

- ถูกฟ้องร้องฐานละเมิดลิขสิทธิ์
- ผู้บริหารต้องรับผิดชอบถึงทางแพ่งและทางอาญา

เสี่ยงด้านชื่อเสียงองค์กร

- ถูกนำชื่อไปแฉอย่างสร้างความเสียหาย
- ชื่อเสียงถูกทำลาย องค์กรหมดความน่าเชื่อถือ ลูกค้าไม่ไว้วางใจ

เสี่ยงด้านการเงิน

- เกิดความสูญเสียทางการเงิน
- สิ้นเปลืองงบประมาณในการแก้ปัญหา

การติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ลงบนเครื่องคอมพิวเตอร์ของบริษัท หรือคอมพิวเตอร์ส่วนตัว เข้าข่ายกระทำความผิดอาญาตามข้อละเมิดลิขสิทธิ์

มีโทษปรับ 1 - 8 แสนบาท จำคุก 6 เดือน ถึง 4 ปี หรือทั้งจำทั้งปรับ

พนักงานสามารถเข้าไปศึกษาเรียนรู้ข้อมูลเพิ่มเติมในระบบ iSpark ตั้งแต่วันนี้เป็นต้นไป เพื่อสร้างความตระหนักในการใช้งานซอฟต์แวร์ให้ปลอดภัยภายในองค์กร

พนักงานต้องเข้าไปทำการอบรมหลักสูตร ก่อนวันที่ 31 มกราคม 2567



ภัยคุกคามที่เพิ่มขึ้นจาก Ransomware Attacks

Ransomware Attacks คือมัลแวร์ (Malware) ประเภทหนึ่งที่ใช้รหัสหรือล็อกไฟล์ของเหยื่อ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ให้ไม่สามารถเข้าถึงไฟล์หรือข้อมูลนั้น ๆ ได้ จากนั้นผู้โจมตีจะเรียกค่าไถ่จากเหยื่อเพื่อให้เหยื่อจ่ายเงินแลกกับการได้ข้อมูลคืน ซึ่งโดยปกติแล้วเหยื่อจะถูกบังคับให้จ่ายเงินในรูปแบบเงินสกุลเงินดิจิทัล (Cryptocurrency) เช่น Bitcoin หรือ Ethereum

สถานการณ์ปัจจุบันของการเผชิญ Ransomware Attacks

ปี 2022 ปีแห่งการต่อสู้กับ Ransomware จากบทวิเคราะห์ของ Chainalysis กล่าวว่าแฮกเกอร์แรนซัมแวร์ได้เรียกค่าไถ่เงินอย่างน้อย 456.8 ล้าน USD จากเหยื่อในปี 2022 ซึ่งถือว่าลดลงจากปี 2021 ที่เคยเรียกเงินได้สูงถึง 756.6 ล้าน USD (ลดลงกว่า 40.3%) เป็นหลักฐานบ่งชี้ว่าเป็นเพราะเหยื่อไม่เต็มใจที่จะจ่ายเงินให้กับแฮกเกอร์แรนซัมแวร์เพิ่มขึ้น

วิธีการป้องกัน Ransomware Attacks สำหรับผู้ใช้งานทั่วไป

- ติดตั้งเฉพาะแอปพลิเคชันจากแหล่งที่เชื่อถือได้ เช่น จากเว็บไซต์ Official เท่านั้น
- เมื่อพบ Website, Link, File ที่ไม่น่าไว้ใจ ให้รีบลบทิ้ง ไม่ควรคลิกลิงก์เพื่อทดสอบว่าเป็นโปรแกรมอะไร
- ติดตั้ง Antivirus หมั่น Update และ Scan อยู่เสมอ
- ทำการ Backup File สำคัญไว้หลายๆ ที่โดยเฉพาะควรสำรองข้อมูลแบบออฟไลน์ด้วย เช่น Copy ไฟล์เก็บไว้ใน Harddisk เป็นต้น

Top 3 การโจมตีของ Ransomware ร้ายแรงสุดในประวัติศาสตร์

ชื่อ	ประเภท	ความเสียหาย
WannaCry (2017)	Crypto-ransomware	\$4 พันล้านเหรียญ
NotPetya (2017)	Locker-ransomware	\$10 พันล้านเหรียญ
Sodinokibi (2019)	Crypto-ransomware	\$0.2 พันล้านเหรียญ

เหตุการณ์สำคัญจากการถูกโจมตี

ในปี 2021 บริษัท Colonial Pipeline ได้รับความเสียหายจากการโจมตีทางไซเบอร์ด้วย Ransomware ซึ่งส่งผลกระทบต่อระบบคอมพิวเตอร์ที่จัดการท่อส่งน้ำมัน ทำให้บริษัทต้องหยุดการทำงานของท่อส่งน้ำมันทั้งหมด เพื่อระงับและป้องกันการโจมตีทางไซเบอร์ภายใต้การดูแลของเอฟบีไอ ทำให้บริษัทต้องจ่ายเงินตามจำนวนที่กลุ่มแฮกเกอร์เรียกค่าไถ่เป็นจำนวน (75 บิตคอยน์หรือ 4.4 ล้านดอลลาร์สหรัฐฯ) ภายในเวลาไม่กี่ชั่วโมง เมื่อจ่ายค่าไถ่แล้วระบบจึงสามารถกลับมาใช้งานได้เหมือนเดิม

ที่มา: Chainalysis cyfence , Trend Micro , astra, World Pipelines, Iberdrola , nt cyfence

PDV-Cybersecurity ฉบับที่ 001/67

หน่วยงานผู้จัดทำ: ฝ่ายไอทีและแพลตฟอร์ม

Awareness Training: Cybersecurity AI and Cyber Threat



Rise Of Cybersecurity AI

บทบาทของ AI ในการป้องกันความปลอดภัยทางไซเบอร์ในอนาคต



จากรายงาน World Economic Forum's Global Risks Report 2024 ระบุว่าความไม่มั่นคงปลอดภัยทางไซเบอร์ถือเป็นความเสี่ยงระดับโลกในช่วงเวลาที่จะเกิดขึ้นในอนาคต โดยมีความเสี่ยงรูปแบบต่าง ๆ เช่น Malware, Deepfakes และข้อมูลเท็จหลอกลวง นอกจากนี้ Reuters ยังระบุว่าพัฒนาอย่างรวดเร็วของ AI ในรูปแบบใหม่ส่งผลให้เกิดการโจมตีทางไซเบอร์ที่เพิ่มขึ้น และยังทำให้แฮกเกอร์สามารถโจมตีทางไซเบอร์ได้ง่ายขึ้นโดยหน่วยงานของอังกฤษ (GCHQ) ได้แจ้งเตือนว่าการเติบโตของ AI จะส่งผลกระทบต่อการโจมตีทางไซเบอร์ในอีก 2 ปีข้างหน้า (2024-2026) อย่างหลีกเลี่ยงไม่ได้

อย่างไรก็ตาม AI ก็มีบทบาทสำคัญในการป้องกันความปลอดภัยทางไซเบอร์มากขึ้นเรื่อย ๆ ในปัจจุบัน แม้ว่าจะยังอยู่ในช่วงเริ่มต้น โดย AI ที่นำมาใช้ในการสร้างความปลอดภัยทางไซเบอร์นั้น สามารถที่จะตรวจจับความผิดปกติและป้องกันภัยคุกคามได้อย่างรวดเร็วและแม่นยำมากขึ้น กับภัยคุกคามในรูปแบบใหม่ ผ่านการวิเคราะห์ข้อมูลเชิงลึก

ภัยลวงที่อาจเกิดขึ้นจากการใช้ AI



AI Hallucination เกิดจากการที่ AI ถูกสร้างข้อมูลเนื้อหาที่ไม่ถูกต้องทำให้ผู้ใช้ AI เกิดความสับสนและได้รับข้อมูลที่ผิดๆ และนำไปสู่ความผิดพลาดจากการนำข้อมูลดังกล่าวไปใช้งาน โดยไม่ตรวจสอบ



Misinformation/Disinformation เป็นการสร้างข้อมูลเท็จหรือข้อมูลบิดเบือนจากเทคโนโลยี AI เพื่อสร้างความสับสนแก่บุคคลหรือสังคมเพื่อใช้ในการก่ออาชญากรรมหรือการหลอกลวงของอาชญากรได้



Deepfakes เป็นการสร้างข้อมูลภาพเสียง วิดีโอจาก AI เสมือนจริงเพื่อหลอกลวง ชุมชนหรือเงินรวม ซึ่งการนำไปสู่การคุกคามทางเพศของประชาชนในวงกว้าง

ข้อระวังต่อการใช้งาน AI

- สร้างคุณค่าและพัฒนาทักษะ : พนักงานหรือลูกจ้างมีความจำเป็นเร่งด่วนในการพัฒนาทักษะการใช้ประโยชน์จาก AI ในการเพิ่มศักยภาพในการทำงานและสร้างคุณค่าให้กับตนเอง
- การบิดเบือนสังคมด้วย Algorithms ของ AI : ทำให้เนื้อหาในแพลตฟอร์มโซเชียลมีเดียต่าง ๆ ถูกชี้นำไปยังสิ่งที่เคยดูมาก่อน นำไปสู่ช่องว่างของข้อมูลในวงกว้างในการบิดเบือนข้อมูลข่าวสารในการขึ้นสังคม
- ความเสี่ยงด้านความปลอดภัย : ระบบ AI ที่ถูกแฮกหรือโดนบังคับใช้งานอย่างไม่เหมาะสมสามารถนำไปสู่ความเสียหายต่อข้อมูลความปลอดภัยส่วนบุคคลได้
- การสื่อสารและปฏิสัมพันธ์ : องค์การ หรือบริษัทต้องพิจารณาปัจจัยในเชิงสังคมและปฏิสัมพันธ์หากมีความจำเป็นต้งาน AI มาประยุกต์ใช้ในการติดต่อสื่อสารและการให้บริการ

ที่มา: IBM, Dooprime, Reuters, dashlane, thairath, davoy



10 อันดับแรกของการคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้นในปี 2030

enisa มีการคาดการณ์ 10 อันดับแรกของการคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้นในปี 2030 ไว้ดังนี้

1. การโจมตีหรือบุกรุกซอฟต์แวร์ ที่เกี่ยวข้องกับการโจมตีผ่านห่วงโซ่อุปทาน
2. การเผยแพร่ข้อมูลเท็จ ที่ใช้เทคนิคขั้นสูง
3. การทำกับดักและผู้คนผ่านเทคโนโลยีดิจิทัลจะเพิ่มขึ้น ความเป็นส่วนตัวของบุคคลลดลง
4. ความผิดพลาดที่เกิดจากมนุษย์และการใช้งานระบบเก่า ภายในระบบนิเวศดิจิทัลและกายภาพ
5. การมุ่งโจมตีเป้าหมายเพิ่มขึ้น โดยใช้ข้อมูลจากอุปกรณ์อัจฉริยะ
6. การขาดการวิเคราะห์และควบคุมโครงสร้างพื้นฐานของวัตถุที่อยู่ในอวกาศ
7. การคุกคามแบบผสมผสาน ทั้งออฟไลน์ออนไลน์ที่ล้ำมากขึ้น
8. การขาดแคลนบุคลากรที่มีทักษะด้าน cybersecurity
9. ผู้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสารระหว่างประเทศตกเป็นจุดที่เสี่ยง
10. การใช้ปัญญาประดิษฐ์ในทางที่ผิด ก่อให้เกิดปัญหาทางอาชญากรรม



Kaspersky เผยว่า

ในประเทศไทย Kaspersky ผู้ให้บริการด้านความปลอดภัยทางไซเบอร์ระดับโลก ล่าสุดได้เผยว่า ในปี 2023 พบภัยคุกคามจากเว็บไซต์ต่าง ๆ รวมกว่า 17 ล้านรายการ ที่กำหนดเป้าหมายโจมตีผู้ใช้ในประเทศไทย อีกทั้งประเทศไทยกำลังเผชิญกับอาชญากรรมทางไซเบอร์ทางการเงินที่เพิ่มขึ้น พบการร้องเรียน และแจ้งความเกี่ยวกับอาชญากรรมออนไลน์ผ่านเว็บไซต์ของสำนักงานตำรวจแห่งชาติสูงถึง 163,091 รายการสร้างความเสียหายโดยประมาณถึง 27,300 ล้านบาท



McKinsey & Company

McKinsey คาดการณ์ตลาด Cybersecurity

McKinsey บริษัทที่ปรึกษาชั้นนำระดับโลกได้คาดการณ์ตลาด Cybersecurity ในอนาคต ปี 2025 ว่าจะมีการใช้จ่ายถึง 101.5 พันล้านดอลลาร์ ในบริการด้าน Cybersecurity ค่าใช้จ่ายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์จะมีอัตราการเพิ่มขึ้นประมาณ 15% ต่อปี และคาดว่าจะมีค่าใช้จ่ายถึง 10.5 ล้านล้านดอลลาร์ต่อปี จากตัวชี้วัดของตลาดดังกล่าวแสดงให้เห็นถึงความกังวลเกี่ยวกับความโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง

Global Risk Report จัดอันดับประเด็นความเสี่ยงต่าง ๆ

Global Risk Report 2023 ของ World Economic Forum ได้จัดอันดับประเด็นความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นบนโลกตามระดับความรุนแรง ซึ่ง 1 ใน 10 เรื่องที่มีความเสี่ยงสูงสุดในปี 2025 และปี 2030 คืออาชญากรรมทางไซเบอร์และความไม่ปลอดภัยทางไซเบอร์ (Widespread Cybercrime and Cyber Insecurity) ดังนั้นองค์กรต่าง ๆ จึงต้องเตรียมพร้อมรับมือกับเรื่องนี้ในระยะยาว

ที่มา : World Economic Forum, Kaspersky, McKinsey, ENISA

Awareness Training: AI-Based Predictive Social Engineering

AI-Based Predictive Social Engineering

การใช้ระบบ AI เพื่อทำนายเหตุที่เกิดจากภัยทางไซเบอร์ที่หลอกลวงทางสังคม

AI และ cybercrime

ในปัจจุบัน การใช้ประโยชน์จาก AI ทางด้านความปลอดภัยไซเบอร์ได้เพิ่มมากขึ้นอย่างมีนัยสำคัญ อย่างไรก็ตาม ความเห็นจากผู้เชี่ยวชาญ 85% กลับพบการโจมตีทางไซเบอร์เพิ่มขึ้นด้วยเช่นกัน เนื่องจากในอีกทางหนึ่ง ความก้าวหน้าของ AI ก็ส่งผลให้องค์กรที่โจมตีสามารถทำการโจมตีได้มากขึ้นเช่นกัน ยกตัวอย่างเช่น

แฮกเกอร์ใช้การคาดการณ์ที่แม่นยำผ่านเครื่องมือ AI และการถอดรหัส CAPTCHA เพื่อเข้าถึงข้อมูลที่ไม่ควรเปิดเผย

Social engineers ใช้ ChatGPT เพื่อสร้างอีเมล ฟิชชิงที่น่าเชื่อถือ และถูกต้องตามกฎหมายมากขึ้น และใช้อัลกอริทึมการเรียนรู้ของเครื่องเพื่อใช้งานร่วมกับ Facial-Mapping Software เพื่อสร้าง Deepfakes ที่น่าเชื่อถือ เพื่อทำการหลอกลวง

แฮกเกอร์ทางไซเบอร์ใช้ Generate AI ที่สามารถระบุจุดอ่อนได้โดยอัตโนมัติ วางแผนและดำเนินการโจมตี ใช้การซ่อนตัวเพื่อหลีกเลี่ยงการป้องกัน และรวบรวมและขุดข้อมูลจากระบบที่ปิดไว้และ Open-Source Intelligence

จากการสำรวจของ IBM พบว่าองค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ค่าใช้จ่ายเฉลี่ยของการละเมิดข้อมูลคือ **3.60 ล้านดอลลาร์** น้อยกว่าการละเมิดในองค์กรที่ไม่ได้ใช้ AI

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการละเมิดข้อมูลได้เร็วขึ้น **108 วัน** เมื่อเทียบกับบริษัทที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ด้านความปลอดภัย และความสามารถด้านระบบอัตโนมัติ **176 ล้านดอลลาร์**

ความแตกต่างในต้นทุนการละเมิดข้อมูลเฉลี่ยถึง **39.3%**

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการละเมิดข้อมูลได้เร็วขึ้น **108 วัน** เมื่อเทียบกับบริษัทที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

Gaurav Banga, ผู้ก่อตั้งและประธานบริษัท Balbix กล่าวว่า "องค์กรต้องสร้างโครงสร้างพื้นฐานด้านความปลอดภัยที่ใช้ประโยชน์จากปัญญาประดิษฐ์ และส่งเสริมการเรียนรู้เชิงลึกเพื่อจัดการกับการโจมตีที่ซับซ้อนมากขึ้นที่ปลอดภัยและแม่นยำ"

AI-Based Predictive Social Engineering

การใช้ระบบ AI เพื่อทำนายเหตุที่เกิดจากภัยทางไซเบอร์ที่หลอกลวงทางสังคม

AI และ cybercrime

ในปัจจุบัน การใช้ประโยชน์จาก AI ทางด้านความปลอดภัยไซเบอร์ได้เพิ่มมากขึ้นอย่างมีนัยสำคัญ อย่างไรก็ตาม ความเห็นจากผู้เชี่ยวชาญ 85% กลับพบการโจมตีทางไซเบอร์เพิ่มขึ้นด้วยเช่นกัน ยกตัวอย่าง เช่น

แฮกเกอร์ใช้การคาดการณ์ที่แม่นยำผ่านเครื่องมือ AI และการถอดรหัส CAPTCHA เพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

Social Engineers ใช้ ChatGPT เพื่อสร้างอีเมลฟิชชิงที่น่าเชื่อถือและใช้อัลกอริทึมการเรียนรู้ของเครื่องเพื่อสร้าง Deepfakes ที่น่าเชื่อถือ เพื่อทำการหลอกลวง

Generate AI ที่สามารถระบุจุดอ่อนได้โดยอัตโนมัติ วางแผนและดำเนินการโจมตี ขุดข้อมูลจากระบบที่ปิดไว้

จากการสำรวจของ IBM พบว่าองค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ค่าใช้จ่ายเฉลี่ยของการละเมิดข้อมูลคือ **3.60 ล้านดอลลาร์** น้อยกว่าการละเมิดในองค์กรที่ไม่ได้ใช้ AI

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการละเมิดข้อมูลได้เร็วขึ้น **108 วัน** เมื่อเทียบกับบริษัทที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ด้านความปลอดภัยและความสามารถด้านระบบอัตโนมัติ **176 ล้านดอลลาร์**

ความแตกต่างในต้นทุนการละเมิดข้อมูลเฉลี่ยถึง **39.3%**

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการละเมิดข้อมูลได้เร็วขึ้น **108 วัน** เมื่อเทียบกับบริษัทที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ตัวอย่างการใช้ระบบ AI-Based Predictive Social Engineering ในองค์กร

กรณีศึกษา CUJOAI

ได้พัฒนาแพลตฟอร์มโดยใช้ Machine Learning เพื่อวิเคราะห์และรักษาความปลอดภัยของระบบตั้งแต่เบราว์เซอร์

สมาร์ทโฟน โปแกรม อุปกรณ์ IoT ซึ่งใช้อัลกอริทึมที่จัดรูปแบบและทำนายการโจมตีในเชิงรุก ดังนั้น มีผลตรวจเป็นลบรายและการโจมตีแบบฟิชชิงจึงถูกขัดขวางก่อนที่จะโจมตีเครือข่าย

กรณีศึกษา DARKTRACE

ได้พัฒนาแพลตฟอร์มความปลอดภัยทางไซเบอร์ที่ขับเคลื่อนด้วย AI ที่เรียกว่า Enterprise Immune System

ซึ่งได้รับการออกแบบมาเพื่อช่วยให้องค์กรตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์แบบเรียลไทม์ และสามารถตรวจจับกิจกรรมที่ผิดปกติ และการกระทำที่ผิดปกติที่อาจเกิดขึ้นได้ก่อนที่จะสร้างความเสียหายให้กับองค์กร

วิศวกรรมสังคมที่ขับเคลื่อนด้วย AI ส่งผลต่อธุรกิจอย่างไร

REAL 100%

FAKE 100%

อีเมลฟิชชิงที่สร้างโดย AI สามารถหลอกลวงพนักงานให้คลิกลิงก์ที่เป็นอันตราย ดาวน์โหลดไฟล์ที่ปลอมแปลงเป็นไฟล์ หรือโอนข้อมูลลับขององค์กรเข้าสู่ระบบหรือหน้า Landing Page ปลอม ดังนั้น บัญชี เครดิต และข้อมูลจึงถูกขโมยได้ง่ายกว่า

Deepfakes ที่สร้างโดย AI เช่น วิดีโอ รูปภาพ และการบันทึกเสียง ช่วยให้ผู้โจมตีสามารถปลอมตัวเป็นผู้บริหารและบุคคลที่เป็นที่รู้จักเพื่อหลอกลวงเอาข้อมูล

การวิเคราะห์ข้อมูลขนาดใหญ่โดย AI สามารถปรับแต่งข้อมูลเพื่อสร้างจากกรรมที่นำดึงดูดสำหรับผู้ชมเฉพาะกลุ่ม ซึ่งทำลายภาพลักษณ์ขององค์กรทำให้เสื่อมเสีย

ที่มา : Secureframe, Balbix, secureworld

AI-Based Predictive Social Engineering

การใช้ระบบ AI เพื่อทำนายเหตุที่เกิดจากภัยทางไซเบอร์ที่หลอกลวงทางสังคม

AI และ cybercrime

ในปัจจุบัน การใช้ประโยชน์จาก AI ทางด้านความปลอดภัยไซเบอร์ได้เพิ่มมากขึ้นอย่างมีนัยสำคัญ อย่างไรก็ตาม ความเห็นจากผู้เชี่ยวชาญ 85% กลับพบการโจมตีทางไซเบอร์เพิ่มขึ้นด้วยเช่นกัน ยกตัวอย่าง เช่น

แฮกเกอร์ใช้การคาดการณ์ที่แม่นยำผ่านเครื่องมือ AI และการถอดรหัส CAPTCHA เพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

Social Engineers ใช้ ChatGPT เพื่อสร้างอีเมลฟิชชิงที่น่าเชื่อถือและใช้อัลกอริทึมการเรียนรู้ของเครื่องเพื่อสร้าง Deepfakes ที่น่าเชื่อถือ เพื่อทำการหลอกลวง

Generate AI ที่สามารถระบุจุดอ่อนได้โดยอัตโนมัติ วางแผนและดำเนินการโจมตี ขุดข้อมูลจากระบบที่ปิดไว้

จากการสำรวจของ IBM พบว่าองค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ค่าใช้จ่ายเฉลี่ยของการละเมิดข้อมูลคือ **3.60 ล้านดอลลาร์** น้อยกว่าการละเมิดในองค์กรที่ไม่ได้ใช้ AI

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการละเมิดข้อมูลได้เร็วขึ้น **108 วัน** เมื่อเทียบกับบริษัทที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ด้านความปลอดภัยและความสามารถด้านระบบอัตโนมัติ **176 ล้านดอลลาร์**

ความแตกต่างในต้นทุนการละเมิดข้อมูลเฉลี่ยถึง **39.3%**

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการละเมิดข้อมูลได้เร็วขึ้น **108 วัน** เมื่อเทียบกับบริษัทที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ตัวอย่างการใช้ระบบ AI-Based Predictive Social Engineering ในองค์กร

กรณีศึกษา CUJOAI

ได้พัฒนาแพลตฟอร์มโดยใช้ Machine Learning วิเคราะห์และรักษาความปลอดภัยของระบบตั้งแต่ เบรเวอร์เซอร์ สมาร์ทโฟน โปแกรม อุปกรณ์ IoT ซึ่งใช้อัลกอริทึมที่จัดรูปแบบและทำนายการโจมตีในเชิงรุก ดังนั้น มีผลตรวจที่เป็นอันตรายและการโจมตีแบบฟิชชิงจึงถูกขัดขวางก่อนที่จะโจมตีเครือข่าย

วิศวกรรมสังคมที่ขับเคลื่อนด้วย AI ส่งผลต่อธุรกิจอย่างไร

อีเมลฟิชชิงที่สร้างโดย AI สามารถหลอกลวงพนักงานให้คลิกลิงก์ที่เป็นอันตราย ดาวน์โหลดไฟล์ที่ปลอมแปลงเป็นไฟล์ หรือโอนข้อมูลลับขององค์กรเข้าสู่ระบบหรือหน้า Landing Page ปลอม ดังนั้น บัญชี เครดิต และข้อมูลจึงถูกขโมยได้ง่ายกว่า

Deepfakes ที่สร้างโดย AI ช่วยให้ผู้โจมตีสามารถปลอมตัวเป็นผู้บริหารและบุคคลที่เป็นที่รู้จักเพื่อหลอกลวงเอาข้อมูล

การวิเคราะห์ข้อมูลขนาดใหญ่โดย AI สามารถปรับแต่งข้อมูลเพื่อสร้างจากกรรมที่นำดึงดูดสำหรับผู้ชมเฉพาะกลุ่ม ซึ่งทำลายภาพลักษณ์ขององค์กรทำให้เสื่อมเสีย

ที่มา : Secureframe, Balbix, secureworld

ตัวอย่างการใช้ระบบ AI-Based Predictive Social Engineering ในองค์กร

กรณีศึกษา CUJOAI

ได้พัฒนาแพลตฟอร์มโดยใช้ Machine Learning เพื่อวิเคราะห์และรักษาความปลอดภัยของระบบตั้งแต่ เบรเวอร์เซอร์ สมาร์ทโฟน โปแกรม อุปกรณ์ IoT ซึ่งใช้อัลกอริทึมที่จัดรูปแบบและทำนายการโจมตีในเชิงรุก ดังนั้น มีผลตรวจที่เป็นอันตรายและการโจมตีแบบฟิชชิงจึงถูกขัดขวางก่อนที่จะโจมตีเครือข่าย

วิศวกรรมสังคมที่ขับเคลื่อนด้วย AI ส่งผลต่อธุรกิจอย่างไร

อีเมลฟิชชิงที่สร้างโดย AI สามารถหลอกลวงพนักงานให้คลิกลิงก์ที่เป็นอันตราย ดาวน์โหลดไฟล์ที่ปลอมแปลงเป็นไฟล์ หรือโอนข้อมูลลับขององค์กรเข้าสู่ระบบหรือหน้า Landing Page ปลอม ดังนั้น บัญชี เครดิต และข้อมูลจึงถูกขโมยได้ง่ายกว่า

Deepfakes ที่สร้างโดย AI ช่วยให้ผู้โจมตีสามารถปลอมตัวเป็นผู้บริหารและบุคคลที่เป็นที่รู้จักเพื่อหลอกลวงเอาข้อมูล

การวิเคราะห์ข้อมูลขนาดใหญ่โดย AI สามารถปรับแต่งข้อมูลเพื่อสร้างจากกรรมที่นำดึงดูดสำหรับผู้ชมเฉพาะกลุ่ม ซึ่งทำลายภาพลักษณ์ขององค์กรทำให้เสื่อมเสีย

ที่มา : Secureframe, Balbix, secureworld

วิศวกรรมสังคมที่ขับเคลื่อนด้วย AI ส่งผลต่อธุรกิจอย่างไร

อีเมลฟิชชิงที่สร้างโดย AI สามารถหลอกลวงพนักงานให้คลิกลิงก์ที่เป็นอันตราย ดาวน์โหลดไฟล์ที่ปลอมแปลงเป็นไฟล์ หรือโอนข้อมูลลับขององค์กรเข้าสู่ระบบหรือหน้า Landing Page ปลอม ดังนั้น บัญชี เครดิต และข้อมูลจึงถูกขโมยได้ง่ายกว่า

Deepfakes ที่สร้างโดย AI ช่วยให้ผู้โจมตีสามารถปลอมตัวเป็นผู้บริหารและบุคคลที่เป็นที่รู้จักเพื่อหลอกลวงเอาข้อมูล

การวิเคราะห์ข้อมูลขนาดใหญ่โดย AI สามารถปรับแต่งข้อมูลเพื่อสร้างจากกรรมที่นำดึงดูดสำหรับผู้ชมเฉพาะกลุ่ม ซึ่งทำลายภาพลักษณ์ขององค์กรทำให้เสื่อมเสีย

ที่มา : Secureframe, Balbix, secureworld

PDV-Cybersecurity ฉบับที่ 004/67

หน่วยกลยุทธ์ดิจิทัลไอซีและแพลตฟอร์ม

PDV-Cybersecurity ฉบับที่ 004/67

หน่วยกลยุทธ์ดิจิทัลไอซีและแพลตฟอร์ม

28 GPSC

Thank You

