

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

The poster features a cartoon character with purple hair and a pink suit, smiling and holding a smartphone. The text 'CYBERSECURITY AWARENESS' is at the top. Below the character are icons of a brain, a shield, and a lock. To the left, a blue box shows a 'Phishing Mail' example with the subject 'A' and the text 'เรียนรู้ภัย Phishing Mail'.

วิธีการเล่น

1. คลิก Link ที่ Banner



2. Log in ด้วย iSpark



3. កណ្តាល Enrolled



4. กด Start Learning เพื่อเริ่มเล่นเกม



A

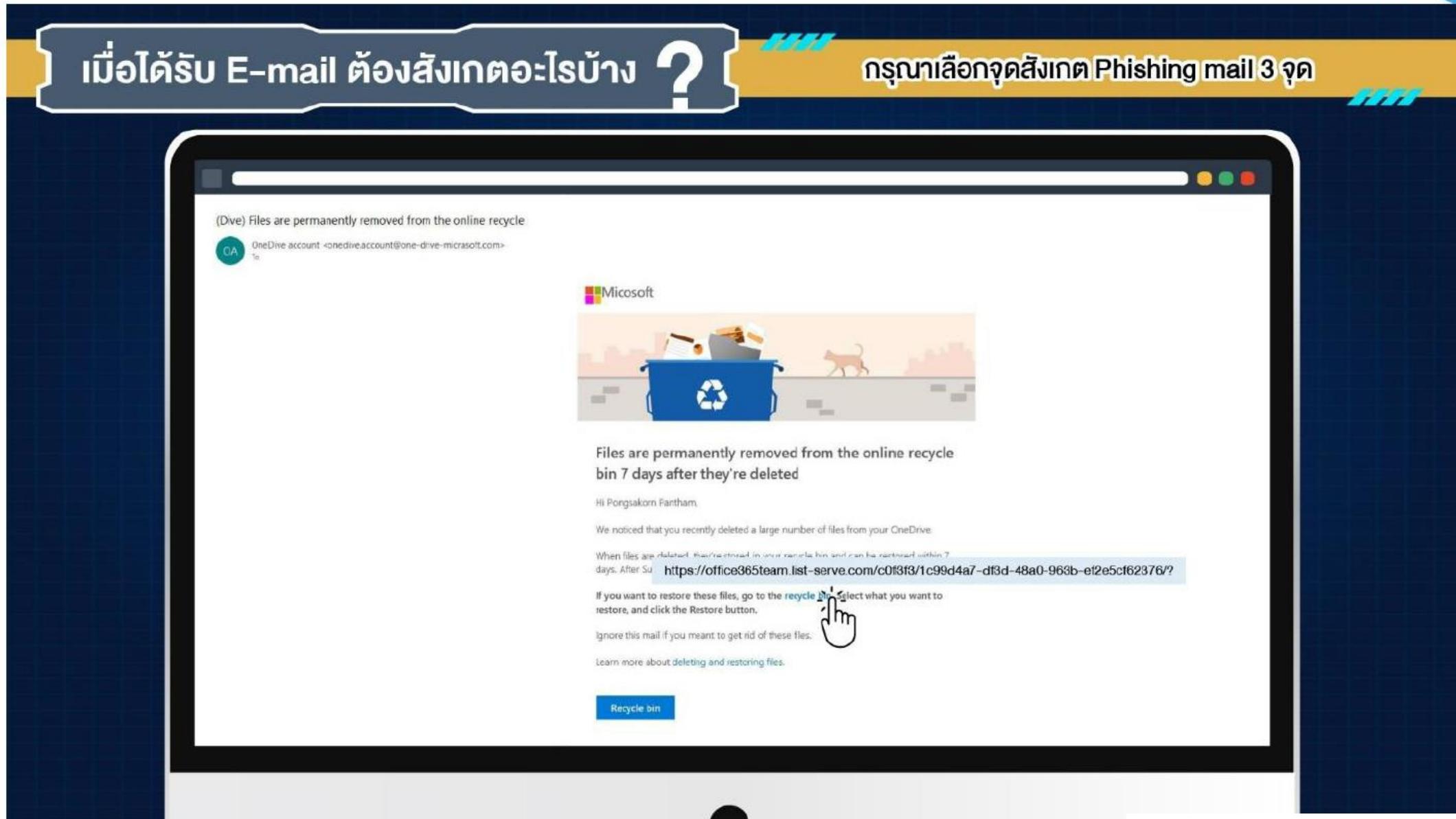
Phishing Mail

กติกาเกม Photo Hunt

- »»» โจทย์ปีกking หนาด 2 ภาพ
- »»» ในแต่ละภาพ ให้คลิกที่จุดสังเกต Phishing Mail
- »»» กำกับดูว่าอีเมลนี้ปลอดภัยหรือไม่ พร้อมระบุเหตุผล
- »»» กำกับดูว่าตัวอย่างนี้เป็น Phishing Mail หรือไม่

เริ่มเกม

Online training : Phishing (100% passed score)



Online training : Phishing (100% passed score)

E-mail นี้ปลอมกัยหรือไม่ ?

กรุณาระบุเหตุผลของแต่ละจุดสังเกตให้ถูกต้อง

1. A. ถูกส่งมาจาก OneDrive ก็เราใช้งานอยู่ในปัจจุบัน
B. บ้าสangสัย เพราะเขียนคำว่า microsoft ผิด

2. A. เนื้อความบ้าสangสัย เพราะเร่งรัดให้รับคำแนะนำการແລະປี Link แบบมาด้วย
B. เนื้อความดูเป็นการเขียนเพื่อแจ้งเตือน ตามปกติ ต้องลองคลิก Link ดูก่อนว่าหน้าตัดไปเป็นอย่างไร

3. A. Link ที่แนบมาดูไม่น่าไว้ใจ "office365team.list-serve.com" ไม่ยวบแนวนี้
B. office365team.list-serve.com เป็นของ microsoft จริง

Online training : Phishing (100% passed score)

E-mail นี้เป็น Phishing Mail หรือไม่ ?

กรุณารอการตอบให้ถูกต้อง

E-mail นี้ เป็น
Phishing Mail



E-mail นี้ **ไม่** เป็น
Phishing Mail



(Dive) Files are permanently removed from the online recycle

OneDive account <onediveaccount@one-drive-microsoft.com>
To

Microsoft



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

Hi Pongsakorn Pantham,

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

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

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 get rid of these files.

Learn more about deleting and restoring files.

Recycle bin

ยินดีด้วย
คุณผ่านแบบทดสอบ

ปิด

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



หัวใจสำคัญของการปฏิบัติการที่เป็นเลิศ ประกอบด้วย
นโยบายและแนวการปฏิบัติ ที่ใช้ในการทำกันให้ผู้ปฏิบัติงาน
สามารถทำงานได้อย่างถูกต้องและมีประสิทธิภาพอย่างยั่ง
นัยหมายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ซึ่งต้องการให้
พนักงานทั่วทั้งองค์กรรู้ดีในการใช้งานระบบสารสนเทศของบริษัทฯ

บริษัทฯ มีนโยบายด้านเทคโนโลยีสารสนเทศ
ที่อย่างให้พนักงานทำความเข้าใจและปฏิบัติตาม
เพื่อป้องกันภัยคุกคาม ด้านสารสนเทศและไซเบอร์
และเพื่อความเป็นเลิศด้านการปฏิบัติการ

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”

กติกาของรุ่นและเพื่อกำชับด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !



เริ่มเล่นเกม 2 (IT-Policy)
สบุกคลิกเลย !



กติกาของรุ่น

- เล่นเกมชิงรางวัล ต่อที่ 1 (ประจำสัปดาห์ วันที่ 16-22 มิถุนายน 2565)
ลุ้นรับบัตรเงินสดเติมบัญชี PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์
(ปิดสูตรรายชื่อผู้เข้าร่วมเล่นเกม ตั้งแต่ วันที่ 17-23 มิถุนายน 2565 เวลา 24.00 น.)
- เล่นเกมชิงรางวัล ต่อที่ 2 เล่นครุ 4 เกม ภายในเดือนมิถุนายน 2565
ลุ้นรับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล
โดยสุ่มจับรางวัล (ขอสงวนรายการรับผู้ที่ยังไม่ได้รับรางวัล จากต่อที่ 1)
- ประกาศรางวัลในต้นเดือน กรกฎาคม 2565





Online training : IT Policy (100% passed score)

โปรดอ่านข้อเท็จจริงต่อไปนี้แล้วเลือกว่า  หรือ 



พนักงานไม่ควรนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาเชื่อมต่อ
ระบบของบริษัทโดยพละการ เพราะอาจมี malware แฝงตัว
อยู่ในเครื่องส่วนตัว และแพร่กระจายเข้าระบบของบริษัทได้



การส่งภาพอุบัติเหตุที่เกิดขึ้นในบริษัทลงโซเชียลกันก็ที่เห็น
เหตุการณ์เพื่อแจ้งให้เพื่อนร่วมงานทราบเหตุ ไม่ดีอ่อนไหว
การกระทำที่ขัดต่อนโยบาย IT ของบริษัท



พนักงานทุกคนต้องแจ้งหรือรายงานต่อหน่วยงาน IT กันก็
เมื่อพบเหตุการณ์ที่อาจเป็นภัยต่อระบบหรือข้อมูลสารสนเทศ
ของบริษัท



ซองทางหลักในการติดต่อแลกเปลี่ยนข้อมูลของบริษัท คือ email บริษัท
และ พื้นที่เก็บข้อมูลบน Cloud ต้อง Sign-in ด้วย user name และรหัส
ผ่าน แบบเดียวกับที่ใช้ในระบบสารสนเทศของบริษัทฯ ท่านนั้น



รหัสผ่านที่ต้องเปลี่ยนใหม่ทุก 90 วัน , ยาวเกิน 8 ตัว
ประกอบด้วย ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข
และตัวอักษรพิเศษผสมกัน

โปรดอ่านข้อเท็จจริงต่อไปนี้แล้วเลือกว่า ✓ หรือ ✗

การลดความเสี่ยงด้านความปลอดภัยที่เกี่ยวกับรหัสผ่านต่อรหัสผ่านเป็นความลับส่วนบุคคล ต้องไม่เปิดเผยให้คนอื่นทราบ และ การทำ 2 Factor Authen (2FA)

USB Storage ต้อง ต้องล็อกทันทีเมื่อไม่ได้ใช้งาน

การเปิดต่องระบบรองรับการอ่าน Email ต้องมีระบบป้องกันภัยที่มีประสิทธิภาพ 100%

การอนุญาตให้เข้าสู่ระบบต้องมีรหัสผ่านที่มีความซับซ้อน เช่น การพิมพ์อุปกรณ์ การนำเข้าข้อมูลทั่วสารที่ไม่ถูกต้อง รวมไปถึงไม่ใช้พื้นที่ภาษาไทยนี้ส่วนตัว

บริษัทไม่อนุญาตและไม่อนุญาตให้ใช้งานโปรแกรมที่อาจเปิดล็อกสีฟ้า สำหรับการทำงานเป็นเวลา: ใช้เครื่องของตนหรือของผู้อื่น รวมถึง ห้ามการใช้งานโปรแกรมภาษาอังกฤษหรือของบริษัทโดยไม่ได้รับอนุญาต

ยินดีด้วย

คุณผ่านแบบทดสอบ

ปิด

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



“
ข้อบุคลของบริษัทมีความสำคัญและต้องเป็นกรรพ์พย์สินอันมีค่า
ซึ่งบริษัทให้ความสำคัญ มีระบบป้องกันและเฝ้าระวังเป็นอย่างดี
อย่างไรก็ตามการโขนตัวใช้เบอร์ปัจจุบัน บุ้งโขนตัวที่ตัวบุคคลโดยวิธีการ ต่างๆ
เช่น Call center, Phishing Mail และตัวผิดพลาด 1 ครั้ง ก็สามารถทำให้
เกิดความเสียหายได้ จึงขอให้พ沃กเราทุกคน ช่วยกันปฎิบัติตาม
นโยบายความมั่นคงปลอดภัยใช้เบอร์อย่างเคร่งครัด
”

คุณกิตติพงษ์ จุลพรศรีดี
ประธานเจ้าหน้าที่บริหารการเงิน

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “เดือนแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”
ทดสอบความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !



เริ่มเล่นเกมที่ 3
(Cyber Policy)
สนุกคลิกเลย !



กติการร่วบกิจกรรม

- เล่นเกมชิงรางวัล ต่อที่ 1 (ประจำสัปดาห์ วันที่ 24-29 มิถุนายน 2565)
ลุ้นรับบัตรเงินสดเติบบับัน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์
(ปิดสูตรประจำผู้เข้าร่วมเล่นเกม ตั้งแต่ วันที่ 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 (ของสองวันรางวัลสั่าแหบผู้ที่ยังไม่ได้รับรางวัล จากต่อที่ 1)
- ประกาศรายชื่อผู้ที่ได้รับรางวัล ประจำเดือน กฤกษากา 2565

สอบถามข้อมูลเพิ่มเติมที่ : คุณพงษ์ไพบูลย์ พ่วงแขก PONGTHEP.M@GPSCGROUP.COM หรือ คุณรัชนีรัก เรืองรัตน์ RATCHARIN.U@GPSCGROUP.COM





Online training : Cyber Policy (100% passed score)

จлагคำตอบ นา妄ลงในช่องว่างให้ถูกต้อง

A » ปล่อยหน้าจอค้างกึ้งเอาไว

B » ข้อมูลส่วนบุคคลรั่วไหล

C » Q89ajTS@me

D » ไฟสต์ข้อมูลอันเป็นเท็จ

E » ลดความเสี่ยงจาก Malware ใจดี

F » การใช้งานโปรแกรมล่อมิเดลลิกส์

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

ตรวจสอบซ่อผู้ส่ง เนื้อความ Link และไฟล์ที่แนบมาทุกครั้งก่อนเปิดอ่าน

เข้ามายตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

นำอีเมลบริษัทไปสมัครบริการบัตรเครดิตแล้ว: Internet บ้าน

ช่วยลดความเสี่ยงหากผู้ไม่หวังดีรู้รหัสผ่านหรือเดาสุ่มรหัสผ่าน

ไม่ download อะไรเมื่อๆ และตรวจสอบให้ระบบป้องกันในเครื่อง เช่น Firewall, Antivirus ให้ทำงานตลอดเวลา

ทำให้บุคคลอื่นแอบใช้เครื่องหรือเทิ่นข้อมูลสำคัญบนหน้าจอได้

เป็นรหัสผ่านที่ยากต่อการคาดเดา ตรงตามหลักการ

จงลากคำตอบ มาวางลงในช่องว่างให้ถูกต้อง

D บังคับใช้ตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

I ตรวจสอบเชื่อผู้ส่ง เนื้อความ Link และไฟล์แนบมาทุกครั้งก่อนเปิดอ่าน

F การใช้งานโปรแกรม

H P@\$\$w0rd

J Secure Web Site (HTTPS)

K Network Access Control (NAC)

ปิด

C เป็นหลักฟ้าบกี่รายการต่อการค่าค่า ตรงตามหลักการ

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

“ พวกรา คือคนสำคัญที่จะช่วยบริษัท ปลอดภัยจากการโจมตีทางไซเบอร์ การโจมตีทางไซเบอร์มีรูปแบบและวิธีการใหม่ตลอดเวลา พวกเรารู้ว่าความตระหนักรู้ และ เมื่อพิจารณาพิจารณาให้รับทราบ ให้รับทราบแล้วก็ต้องการให้รับทราบ ความร่วมมือร่วมใจของทุกคนคือสิ่งสำคัญ ”



เริ่มเล่นเกมที่ 4
(Cyber Awareness)
สนุกคลิกเลย !



Cyber Awareness
เริ่มเล่น

GPSC

เล่นเกมชิงรางวัลรายสัปดาห์จำนวน 4 เกม
ในกิจกรรม “ได้อ่านแห่งการตระหนักรู้
ด้านความมั่นคงปลอดภัยทางไซเบอร์”
กติกาเรื่องความรู้และเพิ่มทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ไปด้วยกัน !



เริ่มเล่นเกมที่ 4
(Cyber Awareness)
สนุกคลิกเลย !



กติกาเรื่องกิจกรรม

- เล่นเกมชิงรางวัล ต่อที่ 1 (ประจำสัปดาห์ วันที่ 30 มิถุนายน - 6 กรกฎาคม 2565)
ลุ้นรับบัตรเดินทางตั๋วเครื่องบิน PTT PRIVILEGE มูลค่า 500 บาท จำนวน 10 รางวัล/สัปดาห์
(ปิดสูตรรายชื่อผู้เข้าร่วมเล่นเกม ตั้งแต่ วันที่ 30 มิถุนายน - 6 กรกฎาคม 2565 เวลา 24.00 น.)
- เล่นเกมชิงรางวัล ต่อที่ 2 เล่นครุ 4 เกม ภายในเดือนมิถุนายน 2565
ลุ้นรับรางวัลบัตร OR Gift Card มูลค่า 300 บาท จำนวน 100 รางวัล
โดยสุ่มวันรางวัล (ขอสงวนสิทธิ์ของผู้ที่ยังไม่ได้รับรางวัล จำกัดต่อที่ 1)
- ประกาศรางวัลในเดือน กรกฎาคม 2565



สอบถามข้อมูลเพิ่มเติม : กอบพงษ์พิพิพ พ่วงแก้ว PONGTHEP.M@GPSCGROUP.COM หรือ กอบเชษฐ์ รัชรินทร์ RATCHARIN.U@GPSCGROUP.COM





กรุณางับคู่อุปกรณ์กับวิธีใช้งานที่ถูกต้อง ตามหลัก Cyber Awareness



กรุณาจับคู่อุปกรณ์กับวิธีใช้งานที่ถูกต้อง
ตามหลัก Cyber Awareness

ยินดีด้วย
คุณผ่านแบบทดสอบ

ปิด

USB Storage

Social Media

รับมือด้วยการ
สำรองข้อมูล
เป็นประจำ และ
แยกเก็บไว้คนละที่

เป็นการยืนยันตัวตน
แบบหลายปัจจัย
 เช่น รหัสผ่าน + OTP
 เป็นต้น

ไม่ใช้ชื่อ
 ข้อมูลเก่าเดิม
 ออกสู่ภายนอก
 โดยไม่ได้รับอนุญาต

ปิด
ส่งให้คุณ
ต้องขออนุญาต
 ก่อนใช้งาน

อาจถูกดักจับข้อมูล
 ดังนั้นใช้ Internet
 ที่แพร่จากมือถือ
 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

ช้อปต์แวร์ผิดกฎหมาย อันตราย กว่าที่คุณคิด

เสี่ยงด้าน ความปลอดภัย

- เสี่ยงต่อ Virus, Malware หรือ Ransomware รวมถึงการตอกเป็นหรือ Phishing
- ข้อมูลของคุณร่ำไร ข้อมูลลูกค้าถูกขโมย ข้อมูลส่วนบุคคลถูกนำไปใช้
- ถูกจับอางในการทำธุรกรรมออนไลน์

เสี่ยงด้าน กฏหมาย

- ถูกฟ้องร้องฐานละเมิดลิขสิทธิ์
- ผู้บริหารต้องรับผิดชอบทั้งทางแพ่งและทางอาญา

เสี่ยงด้าน ชื่อเสียงองค์กร

- ถูกนำไปเป็นข่าวลวง องค์กรหมัดความน่าเชื่อถือ ลูกค้าไม่ไว้วางใจ

เสี่ยงด้าน การเงิน

- เกิดความสูญเสียจากการเงิน
- สับเปลี่ยนงบประมาณในการเก็บปั้นหา

Awareness Training: Cybersecurity AI and Cyber Threat




10 อันดับแรกของภัยคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้นในปี 2030

นักการค้าการณ์ 10 อันดับแรกของภัยคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้นในปี 2030 ได้ดังนี้

- การโจมตีห้องบุกธุรกิจซอฟต์แวร์ ที่เกี่ยวข้องกับกระบวนการผลิตแห่งห่วงโซ่อุปทาน
- การเผยแพร่ข้อมูลเก็บ ที่ซักเก็ตบีบขั้นสูง
- การกำกับดูแลผู้คนผ่านเทคโนโลยีดิจิทัลจะเพิ่มขึ้น ความเป็นส่วนตัวของบุคคลลดลง
- ความติดผลลัพธ์ที่เกิดจากมนุษย์และการใช้งานระบบเก่า ภายในระบบปัจจุบันดิจิทัลและภัยคุกคาม
- การบุกโอบตีเข้ามาเพิ่มขึ้น โดยใช้ข้อมูลจากอุปกรณ์อัจฉริยะ
- การขาดการวิเคราะห์และควบคุมโครงสร้างพื้นฐานของวัตถุที่อยู่ในอวกาศ
- การคุกคามแบบผสมผสาน ก้าวอ่อนโยนอ่อนโยนไปที่ล้ำก้าวขั้น
- การขาดแคลนบุคลากรที่มีภักดีด้าน cybersecurity
- ผู้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสารระหว่างประเทศเป็นอุดกีเสี่ยง
- การใช้ปั๊มน้ำประดิษฐ์ในการที่ติด ก่อให้เกิดปัญหาทางอาชญากรรม

Kaspersky เมย์ว่า

kaspersky

ในประเทศไทย Kaspersky ผู้ให้บริการด้านความปลอดภัยทางไซเบอร์ระดับโลก ล่าสุดได้เผยแพร่ ในปี 2023 พฤติคุณนิเวศทั่วโลก ฯ รวมทั้ง 17 ล้านประเทศ ที่กำกับดูแลป้าหมายที่ผู้ใช้ในประเทศไทย ลักษณะที่น่าห่วงคือ ลักษณะเชิงกล กับอาชญากรรมทางไซเบอร์ทางการเงินที่เพิ่มขึ้น พบการร้องขอเช่น และแจ้งความที่อยู่ที่บ้านและบ้านในโลก 163,091 รายการสร้างความเสี่ยงให้โดยรวมเป็น 27,300 ล้านบาท ตั้งแต่ปี 2023 ที่ผ่านมา

McKinsey คาดการณ์ตลาด Cybersecurity

McKinsey & Company

McKinsey บริษัทที่ปรึกษาชั้นนำระดับโลกได้คาดการณ์ตลาด Cybersecurity ในอนาคต ปี 2025 ว่าจะมีมูลค่าอยู่ที่ 101.5 พันล้านดอลลาร์ ในบริการด้าน Cybersecurity คาดว่าจะมีการเติบโตอย่างต่อเนื่อง 15% ต่อปี และคาดว่าจะมีค่าใช้จ่ายต่อปี 10.5 ล้านล้านดอลลาร์ต่อปี จากการเติบโตของตลาดดังกล่าว และแสดงให้เห็นถึงความก้าวหน้าที่ยิ่งใหญ่ที่เกี่ยวกับการเงินดิจิทัลที่เพิ่มขึ้นอย่างต่อเนื่อง

Global Risk Report ตั้งอันดับประเด็นความเสี่ยงต่างๆ

Global Risk Report 2023 ของ World Economic Forum ได้ตั้งอันดับประเด็นความเสี่ยงต่างๆ ที่จะเกิดขึ้นในโลกตามระดับความรุนแรง ชั้ง 1 ใน 10 เรื่องที่มีความเสี่ยงสูงสุดในปี 2025 และปี 2030 คืออาชญากรรมทางไซเบอร์และความไม่สงบด้วยภัยคุกคามไซเบอร์ (Widespread Cybercrime and Cyber Insecurity) ดันเป็นองค์กรต่างๆ ทั่วโลกที่ต้องเผชิญหน้าในระยะยาว

ที่มา : World Economic Forum, Kaspersky, McKinsey, ENISA

PDV-Cybersecurity ฉบับที่ 003/67

หน่วยอุตสาหกรรมดิจิทัลและเพื่อสังคม

Awareness Training: AI-Based Predictive Social Engineering

AI-Based Predictive Social Engineering

การใช้ระบบ AI เพื่อกำหนายเหตุ ที่เกิดจากภัยการใช้เบอร์ที่หลอกลวงทางสังคม

AI แล้ว cybercrime

ในปัจจุบัน การใช้ประโยชน์จาก AI ทางด้านความปลอดภัยไซเบอร์ได้เพิ่มมากขึ้นอย่างมีนัยสำคัญ อย่างไรก็ตาม ความเห็นจากผู้เชี่ยวชาญ 85% กลับพบการโจมตีทางไซเบอร์เพิ่มขึ้นด้วยเช่นกัน ยกตัวอย่าง เช่น

แฮกเกอร์ใช้การคาดคะเนรหัสผ่านที่รองรับ AI และการก่อตัวรหัส CAPTCHA เพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

Social Engineers ใช้ ChatGPT เพื่อสร้างข้อความพิชิตใจที่นำไปอีเมลและใช้อัลกอริทึมในการเรียนรู้ของอัปเกรดให้ใช้งานเพื่อสร้าง Deepfakes ที่นำไปอีเมล เพื่อกำหนดลวง

Generate AI ที่สามารถระบุจุดอ่อนได้โดยอัตโนมัติ ว่างเห็นและดำเนินการโจมตี ข้อมูลของลูกค้าระบบที่ติดไวรัส

จากการสำรวจของ IBM พบว่า องค์กรที่ใช้ AI ด้านความปลอดภัย และระบบอัตโนมัติ

ค่าใช้จ่ายเฉลี่ยของการลงทุนบุลังค์ **3.60 ล้านดอลลาร์**

น้อยกว่าการลงทุนในองค์กรที่ไม่ได้ใช้ AI

ด้านความปลอดภัยและ ความสามารถดำเนินระบบด้วย AI **1.76 ล้านดอลลาร์**

ความแตกต่างในต้นทุน การลงทุนข้อมูลเฉลี่ยถึง **39.3%**

องค์กรที่ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ สามารถระบุและควบคุมการลงทุนบุลังค์ได้เร็วขึ้น **108 วัน** เมื่อเทียบกับธุรกิจที่ไม่ได้ใช้ AI ด้านความปลอดภัยและระบบอัตโนมัติ

ตัวอย่างการใช้ระบบ AI-Based Predictive Social Engineering ในองค์กร

กรณีศึกษา

ได้พัฒนาแพลตฟอร์มโดยใช้ Machine Learning วิเคราะห์และรักษาความปลอดภัยของระบบตั้งแต่ เเบรเวอร์ สมาร์ตโฟน ไปจนถึงอุปกรณ์ IoT ซึ่งใช้อัลกอริทึมที่จดจำรูปแบบและภัยการโจมตีในเชิงรุก ดังนั้น เมลแวร์ที่เป็นอันตรายและการโจมตีแบบพิชชิ่งจึงถูกขัดขวางก่อนที่จะโจมตีเครือข่าย

วิศวกรรมสังคมที่ขับเคลื่อนด้วย AI ส่งผลต่อธุรกิจอย่างไร

วิเมลพิชชิ่งที่สร้างโดย AI สามารถหลอกลวงงานให้คลิกลิงก์ที่อันตราย ดาวน์โหลดไฟล์ที่ปลอดภัยเป็นบลัฟเวอร์ รังสูงบุกรุกได้ง่ายกว่า

Deepfakes ที่สร้างโดย AI ช่วยให้ผู้โจมตีสามารถปลอมตัวเป็นผู้บริหารและบุคคลที่เป็นที่รู้จักเพื่อหลอกลวงเจ้าของข้อมูล

การวิเคราะห์ข้อมูลขนาดใหญ่ AI สามารถปรับแต่งข้อมูลเพื่อสร้างวิศวกรรมที่เป้าจุดดูดลูกค้าที่ต้องการสิ่งที่ต้องการให้ได้รับสิ่งที่ต้องการ

ที่มา : Secureframe, Balbix, secureworld

PDV-Cybersecurity ฉบับที่ 004/67

หน่วยบัญชีกิจกรรมที่ต้องการและแพลตฟอร์ม

Thank You

