

ที่ ศธ ๐๔๐๐๘/๑๖๖๒๗



สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
กระทรวงศึกษาธิการ กทม. ๑๐๓๐๐

๑

กันยายน ๒๕๖๙

เรื่อง ประชาสัมพันธ์การอบรมออนไลน์หลักสูตรสร้างความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล

เรียน ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา

สิ่งที่ส่งมาด้วย	๑. รายละเอียดการอบรม	จำนวน ๑ ชุด
	๒. กำหนดการ	จำนวน ๑ ฉบับ
	๓. โปสเตอร์	จำนวน ๑ ฉบับ

ด้วยบริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน) ร่วมกับ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และมูลนิธิสานอนาคตการศึกษา คอนเน็กซ์อีดี กำหนดจัดการอบรมออนไลน์หลักสูตรสร้างความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล ในวันศุกร์ที่ ๒ ตุลาคม ๒๕๖๙ เวลา ๑๓.๓๐ - ๑๕.๓๐ น. ผ่านช่องทาง Facebook และ Youtube OBEC Channel ให้กับผู้บริหารสถานศึกษา ครู และบุคลากรทางการศึกษา

ในการนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ขอให้สำนักงานเขตพื้นที่การศึกษา ประชาสัมพันธ์การอบรมออนไลน์หลักสูตรสร้างความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล ไปยังโรงเรียนในสังกัด ทั้งนี้ ผู้สนใจสามารถเข้าร่วมการอบรมออนไลน์ ตามวัน และเวลาดังกล่าว รายละเอียดดังสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายภูธร จันทะหงษ์ ปุณยจรัสซึ้ง)

รองเลขาธิการคณะกรรมการการศึกษาขั้นพื้นฐาน รักษาการแทน

เลขาธิการคณะกรรมการการศึกษาขั้นพื้นฐาน

สำนักพัฒนานวัตกรรมการจัดการศึกษา

โทรศัพท์ ๐ ๒๒๘๘ ๕๘๙๓

อบรมหลักสูตรสร้างความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล

รู้ทันภัยไซเบอร์ ปกป้องข้อมูลส่วนบุคคล และใช้ AI อย่างปลอดภัย

รายละเอียดหลักสูตร

หลักสูตรอบรมด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างปลอดภัย ออกแบบเพื่อเสริมสร้างความรู้ ความเข้าใจ และทักษะที่จำเป็นสำหรับครูและบุคลากรทางการศึกษาในการรับมือกับความเสี่ยงทางไซเบอร์ที่เกิดขึ้นในชีวิตประจำวันและการปฏิบัติงาน

เนื้อหามุ่งเน้นให้ผู้เข้าอบรมสามารถ รู้เท่าทันภัยไซเบอร์ยุค AI ป้องกันข้อมูลส่วนบุคคลของตนเองและนักเรียน และเลือกใช้ AI อย่างเหมาะสมและปลอดภัยผ่านตัวอย่างสถานการณ์ที่สามารถเกิดขึ้นได้จริง เช่น การหลอกลวงผ่านฟิชซิง (Phishing) การปลอมแปลงด้วย Deepfake การขโมยบัญชี การใช้ QR Code ปลอม การหลอกให้ติดตั้งแอปพลิเคชัน การเปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็น ตลอดจนความเสี่ยงจากการนำข้อมูลเข้าสู่ระบบ AI

ตารางการสอนตลอดการอบรม

เวลา	เนื้อหาการเรียนรู้
13:30 – 14:00 น.	1. ภัยไซเบอร์ยุค AI วันนี้มีมากกว่า Scammer 2. การสังเกตและตรวจสอบการหลอกลวงประเภท Phishing และ Deepfake 3. การประยุกต์ใช้แนวคิด Zero Trust ในการทำงานและชีวิตประจำวัน
14:00 – 15:00 น.	4. การคุ้มครองข้อมูลส่วนบุคคลของครูและนักเรียนในการใช้งาน AI 5. หลักการเก็บ ใช้เปิดเผย และส่งต่อข้อมูลส่วนบุคคลอย่างเหมาะสม 6. แนวทางการลดและปกป้องข้อมูลก่อนนำไปใช้กับระบบ AI
15:00 – 15:30 น.	7. สรุปสาระสำคัญและแนวทางนำความรู้ไปประยุกต์ใช้ในการปฏิบัติด้วยหลักการ “4 ก่อน”

หลักสูตรการเรียนรู้ : สร้างความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล

รายละเอียดหลักสูตร / หัวข้อการเรียนรู้

1. ภัยไซเบอร์ยุค AI วันนี้มีมากกว่า Scammer

ทำความเข้าใจรูปแบบภัยคุกคามทางไซเบอร์ที่อาจพบได้ในชีวิตประจำวัน ซึ่งปัจจุบันมีแนวโน้มเพิ่มขึ้นทั้งในด้านความหลากหลายและความซับซ้อน โดยเฉพาะการนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้ในการหลอกลวงและก่ออาชญากรรมทางไซเบอร์ โดยมีหัวข้อสำคัญ ดังนี้

- การยึดหรือขโมยบัญชีผู้ใช้งาน (Account Takeover) การเข้าถึงหรือเข้าควบคุมบัญชีของผู้ใช้งานโดยไม่ได้รับอนุญาต
- โปรแกรมประสงค์ร้าย (Malware) โปรแกรมหรือแอปพลิเคชันที่ถูกพัฒนาขึ้นเพื่อสร้างความเสียหาย ขโมยข้อมูล หรือกระทบต่อการทำงานของระบบ
- มัลแวร์เรียกค่าไถ่ (Ransomware) การเข้ารหัสหรือล็อกไฟล์และระบบ เพื่อเรียกค่าไถ่จากผู้เสียหาย
- การหลอกลวงผ่านคิวอาร์โค้ด (QR Code Scam) การใช้คิวอาร์โค้ดปลอมเพื่อนำผู้ใช้งานไปยังเว็บไซต์หรือช่องทางที่เป็นอันตราย
- หน้าเข้าสู่ระบบปลอม (Fake Login Page) การสร้างหน้าเข้าสู่ระบบเลียนแบบเว็บไซต์หรือบริการจริง เพื่อหลอกให้ผู้ใช้งานเปิดเผยชื่อผู้ใช้งานและรหัสผ่าน
- แอปพลิเคชันปลอม (Fake Application) แอปพลิเคชันที่ถูกสร้างขึ้นเพื่อเลียนแบบแอปพลิเคชันจริง โดยมีวัตถุประสงค์เพื่อหลอกลวงหรือขโมยข้อมูล
- การโจรกรรมข้อมูล (Data Theft) การเข้าถึง คัดลอก หรือขโมยข้อมูลส่วนบุคคล ข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต
- การปลอมแปลงบุคคลโดยใช้ปัญญาประดิษฐ์ (AI Impersonation) การนำเทคโนโลยี AI มาใช้ในการสร้างหรือดัดแปลงภาพ เสียง ข้อความ หรือลักษณะของบุคคล เพื่อแอบอ้างตัวตนหรือใช้ในการหลอกลวง

2. การสังเกตและตรวจสอบการหลอกลวงประเภท Phishing และ Deepfake

ศึกษาและทำความเข้าใจแนวทางการสังเกตและตรวจสอบการหลอกลวงทางไซเบอร์ที่มีความซับซ้อนและมีความสมจริงมากยิ่งขึ้นจากการนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้ โดยเฉพาะการหลอกลวงแบบฟิชซิง (Phishing) และการปลอมแปลงภาพหรือเสียงเสมือนจริง

(Deepfake) เพื่อให้สามารถประเมินความน่าเชื่อถือและลดความเสี่ยงจากการตกเป็นเหยื่อ โดยมีสาระสำคัญ ดังนี้

- สัญญาณเตือนและข้อสังเกตที่อาจบ่งชี้ถึงการหลอกลวง
- แนวทางการตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลก่อนดำเนินการหรือเปิดเผยข้อมูลสำคัญ

3. การประยุกต์ใช้แนวคิด Zero Trust ในการทำงานและชีวิตประจำวัน

ศึกษาและทำความเข้าใจหลักการ Zero Trust ภายใต้แนวคิด “ไม่เชื่อถือโดยทันที และตรวจสอบก่อนอนุญาต” เพื่อนำมาประยุกต์ใช้ในการปฏิบัติงานและการดำเนินชีวิตประจำวัน อันเป็นการเสริมสร้างพฤติกรรมการใช้งานเทคโนโลยีอย่างปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีแนวทางสำคัญ

4. การคุ้มครองข้อมูลส่วนบุคคลของครูและนักเรียนในการใช้งาน AI

เรียนรู้และทำความเข้าใจเกี่ยวกับข้อมูลส่วนบุคคลในบริบทของสถานศึกษา รวมถึงแนวทางการใช้ข้อมูลส่วนบุคคลร่วมกับเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างเหมาะสมและปลอดภัย เพื่อสร้างความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และลดความเสี่ยงจากการนำข้อมูลไปใช้หรือเปิดเผยโดยไม่เหมาะสม โดยตัวอย่างข้อมูลที่เกี่ยวข้อง ได้แก่

- ชื่อและนามสกุล
- เลขประจำตัวนักเรียน
- ข้อมูลของผู้ปกครอง
- คะแนนและผลการเรียน
- ข้อมูลด้านสุขภาพและความพิการ
- ข้อมูลเกี่ยวกับพฤติกรรมหรือการเข้าร่วมกิจกรรม
- ภาพถ่ายและวิดีโอ
- ข้อมูลหรือเอกสารภายในสถานศึกษา

5. หลักการเก็บ ใช้ เปิดเผย และส่งต่อข้อมูลส่วนบุคคลอย่างเหมาะสม

เรียนรู้และทำความเข้าใจหลักการบริหารจัดการข้อมูลส่วนบุคคลของครู นักเรียน และผู้ปกครองอย่างเหมาะสม ครอบคลุมตั้งแต่การเก็บรวบรวม การใช้ การเปิดเผย และการส่งต่อข้อมูล โดยคำนึงถึงวัตถุประสงค์ ความจำเป็น และสิทธิในการเข้าถึงข้อมูล เพื่อป้องกันและลดความเสี่ยงจากการนำข้อมูลไป

ใช้ผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลโดยไม่เหมาะสม ตลอดจนสร้างความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ซึ่งการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยต้องดำเนินการอย่างเหมาะสมภายใต้วัตถุประสงค์และขอบเขตที่กำหนด

6. แนวทางการลดและปกป้องข้อมูลก่อนนำไปใช้กับระบบ AI

เรียนรู้และทำความเข้าใจหลักการลดการใช้ข้อมูล (Data Minimization) โดยพิจารณาเลือกใช้ข้อมูลเฉพาะเท่าที่จำเป็นและสอดคล้องกับวัตถุประสงค์ ก่อนนำข้อมูลเข้าสู่ระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อช่วยลดความเสี่ยงจากการเปิดเผย การเข้าถึง หรือการนำข้อมูลส่วนบุคคลและข้อมูลสำคัญไปใช้โดยไม่เหมาะสม ตลอดจนส่งเสริมการใช้งาน AI อย่างปลอดภัยและมีความรับผิดชอบ

7. สรุปสาระสำคัญและแนวทางนำความรู้ไปประยุกต์ใช้ในการปฏิบัติด้วยหลักการ “4 ก่อน”

สรุปและทบทวนสาระสำคัญจากการอบรมเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างปลอดภัย เพื่อให้ผู้เข้ารับการอบรมสามารถนำความรู้และแนวทางที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานและชีวิตประจำวัน โดยใช้หลักการ “4 ก่อน” เป็นแนวทางประกอบการพิจารณาและตัดสินใจก่อนดำเนินการเกี่ยวกับข้อมูลหรือการใช้เทคโนโลยี

ระยะเวลาการอบรม

- อบรมผ่านระบบออนไลน์แบบถ่ายทอดสด จำนวน 2 ชั่วโมง

คุณสมบัติผู้เข้าอบรม

- ไม่กำหนด

ผลสัมฤทธิ์ (Outcome)

- ผู้เรียนมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่สำคัญในยุคปัญญาประดิษฐ์ (Artificial Intelligence: AI) และสามารถสังเกตความผิดปกติหรือความเสี่ยงเบื้องต้นได้
- ผู้เรียนสามารถระบุสัญญาณที่อาจบ่งชี้ถึงการหลอกลวงแบบฟิชซิง (Phishing) และการปลอมแปลงภาพหรือเสียงเสมือนจริง (Deepfake) รวมทั้งเลือกใช้แนวทางการตรวจสอบความถูกต้องและความน่าเชื่อถือได้อย่างเหมาะสม
- ผู้เรียนสามารถนำหลักการ Zero Trust มาประยุกต์ใช้เพื่อเสริมสร้างความปลอดภัยในการปฏิบัติงานและการใช้เทคโนโลยีในชีวิตประจำวัน
- ผู้เรียนมีความรู้ความเข้าใจเกี่ยวกับความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของครู นักเรียน และผู้ปกครอง

- ผู้เรียนสามารถพิจารณาการเก็บรวบรวม ใช้ เปิดเผย และส่งต่อข้อมูลส่วนบุคคลได้อย่างเหมาะสม โดยคำนึงถึงวัตถุประสงค์และความจำเป็นในการใช้ข้อมูล
- ผู้เรียนสามารถเลือกใช้แนวทางในการลดหรือปกปิดข้อมูลส่วนบุคคลก่อนนำข้อมูลไปใช้กับระบบ AI เพื่อลดความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่เหมาะสม

ผลผลิต (Output)

- ผู้เรียนผ่านแบบทดสอบในการประเมินความรู้และความเข้าใจจากเนื้อหาการอบรม



กำหนดการการอบรมออนไลน์
“หลักสูตรสร้างความปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล”
วันศุกร์ที่ 2 ตุลาคม 2569 เวลา 13.30-15.30 น.

เวลา	กิจกรรม
13.30 – 13.40 น.	กล่าวเปิดการอบรมและกล่าวถึงความสำคัญของการสร้างวัฒนธรรมดิจิทัลที่ปลอดภัย
13.40 – 14.00 น.	ภัยไซเบอร์ใกล้ตัวที่ครูควรรู้ และแนวโน้มภัยคุกคามในปัจจุบัน
14.00 – 14.30 น.	รู้เท่าทัน Phishing และการหลอกลวงออนไลน์ วิธีป้องกันตนเองและสถานศึกษา
14.30 – 14.50 น.	การคุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับครูและสถานศึกษา
14.50 – 15.10 น.	การใช้ AI อย่างปลอดภัยและมีความรับผิดชอบ พร้อมแนวปฏิบัติที่เหมาะสม
15.10 – 15.20 น.	Think Before Share การใช้ Social Media อย่างสร้างสรรค์และปลอดภัย
15.20 – 15.30 น.	ถาม-ตอบ แลกเปลี่ยนประสบการณ์ และข้อเสนอแนะ
15.30 น.	สรุปสาระสำคัญและปิดการอบรม

หมายเหตุ:

กำหนดการสามารถเปลี่ยนแปลงได้ตามความเหมาะสม



บริษัท ซีพีเอฟ (ประเทศไทย)
จำกัด (มหาชน)



สำนักงานคณะกรรมการคุ้มครอง
ข้อมูลส่วนบุคคล (สคส.)



ผนึกกำลัง สร้างความปลอดภัยไซเบอร์ และข้อมูลส่วนบุคคล



ความรู้ที่ครูยุคดิจิทัลต้องมี เพื่อดูแลตนเองและนักเรียนอย่างมั่นใจ

FREE

ฟรี!
ไม่มีค่าใช้จ่าย

LIVE

Live สด
ทั่วประเทศ
ผ่าน OBEC Channel



วันที่ 2 ตุลาคม 2569
เวลา 13:30 - 15:30 น.

PART 1 - CPF



จิตจินต์ ดวงสร้อยทอง
ผู้เชี่ยวชาญ
ด้าน Information
Security - GRC
บริษัท ซีพีเอฟ
(ประเทศไทย) จำกัด
(มหาชน)



ภัยไซเบอร์ยุค AI วันนี้มีมากกว่า Scammer

ทำความเข้าใจภัยที่เกิดขึ้นในปัจจุบัน เช่น การยึดบัญชี, QR Code ปลอม, แอปพลิเคชันปลอม, การขโมยข้อมูล และการปลอมตัวด้วย AI พร้อมวิธีสังเกต Phishing และ Deepfake ที่สมจริงกว่าที่เคย



Zero Trust ฉบับชีวิตประจำวัน

เรียนรู้แนวคิด "ไม่เชื่อทันที ตรวจสอบก่อนอนุญาต" พร้อมแนวทางป้องกันตนเองที่ทำได้จริงในชีวิตประจำวัน เพื่อใช้งานดิจิทัลอย่างปลอดภัย

PART 2 - PDPC



ข้อมูลส่วนบุคคลของครูและนักเรียนกับการใช้ AI
ทำความเข้าใจข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวที่ต้องระวัง รวมถึงหลักการเก็บ ใช้ เผยแพร่ และส่งต่อข้อมูลอย่างถูกต้องและเหมาะสม



วิธีลดความเสี่ยงหรือปิดกั้นข้อมูลก่อนใช้งาน
แนะนำวิธีลบ ช้อน หรือแทนที่ข้อมูลระบุตัวตน ลดความเสี่ยงการเปิดเผยข้อมูลส่วนบุคคลก่อนนำข้อมูลไปใช้งานกับ AI

พันตำรวจเอก วัชรพงษ์ พรหมจันทร์
รองเลขาธิการคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล
สำนักงานคณะกรรมการคุ้มครอง
ข้อมูลส่วนบุคคล (สคส.)



ทำไมคุณถึงพลาดไม่ได้?

- ✓ อัปเดตภัยไซเบอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลล่าสุด
- ✓ เข้าใจง่าย ใช้ได้จริงในห้องเรียนและชีวิตประจำวัน
- ✓ เสริมทักษะดิจิทัลให้ปลอดภัย มั่นใจ และถูกต้อง



QR Code นี้
จะนำท่านไปสู่

f OBEC Channel &
CPF x CONNEXT ED
>>>

