ISSUE 23
APRIL - JUNE 2023

บัวบาน

HEART HEALTH HOME

เมล็ดพันธุ์แห่งความยั่งยืน

'ไซเบอร์วัคซีน' ภูมิคุ้มกันโจรออนไลน์

สแกนเพื่ออ่าน e-book

ซีพี...เพื่อความยั่งยืน

SUSTAINABLE DEVELOPMENT

SD Story: 'โครงการไซเบอร์วัคซีน รู้ทันกลโกง ต้านภัยออนไลน์'
สำนักงานตำรวจแห่งชาติร่วมมือกับเครือซีพี

SD Talk: ทนายนิด้า - ศรันยา หวังสุขเจริญ
'รับคำขอโทษเป็นเงินสดเท่านั้น'
ราคาที่ต้องจ่าย... ให้โลกไซเบอร์

Think Forward:
ภัยคุกคามไซเบอร์ ความเสี่ยงสำคัญระดับโลก

EDITOR'S NOTE

'ไซเบอร์วัคซีน' ภูมิคุ้มกันโจรออนไลน์

ในช่วง 3-4 ปีที่ผ่านมานี้ สังคมไทยก้าวเข้าสู่ยุคสมัยแห่งโลกไซเบอร์มากขึ้นอย่างเห็นได้ชัด ส่วนหนึ่งเป็นผลจากสถานการณ์ระบาดของโรคโควิด-19 ซึ่งทำให้การติดต่อสื่อสารผ่านโซเชียลมีเดียและดำเนินการทางธุรกรรมต่างๆ ผ่านช่องทางออนไลน์สามารถทำได้อย่างง่ายดายและรวดเร็วมากยิ่งขึ้น

อย่างไรก็ตามพัฒนาการที่ก้าวหน้ามักมาพร้อมข้อควรระวังดังที่เปรียบกันไว้ว่าเหมือนดาบสองคม ในขณะที่เราใช้เทคโนโลยีกันอย่างเพลิดเพลินสะดวกสบาย ภัยจากโลกไซเบอร์ก็คืบคลานเข้ามาคุกคามทำให้หลายคนตกเป็นเหยื่อ

การประชุม World Economic Forum 2023 ที่จัดขึ้นครั้งล่าสุดได้เปิดเผยให้เราทุกคนได้ทราบว่าภัยคุกคามไซเบอร์ ถือเป็น 1 ใน 5 ความเสี่ยงที่สำคัญระดับโลกไปเรียบร้อยแล้ว ซึ่งความเสียหายที่จะเกิดขึ้นจากความเสี่ยงดังกล่าวนี้ถูกคาดการณ์ไว้ว่าภายในปี 2025 หรืออีกไม่เกิน 2 ปีข้างหน้าจะมีมูลค่าสูงขึ้นไปถึง 10.5 ล้านล้านเหรียญเลยทีเดียว

ในขณะที่ภายในประเทศของเราเอง สถานการณ์อาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ในปัจจุบันนับวันยิ่งมีสถิติเพิ่มสูงขึ้น โดยมีประชาชนเป็นจำนวนมากที่หลงกลตกเป็นเหยื่อจนได้รับความเดือดร้อน สูญเสียทรัพย์สิน และในบางรายถึงกับต้องสูญเสียชีวิต ซึ่งจากสถิติประมาณหนึ่งปีจากการรวบรวมตัวเลขคดีรับแจ้งความออนไลน์ (ตั้งแต่ต้นมีนาคม 2565 ถึงต้นเมษายน 2566) พบว่ามีการรับแจ้งความอาชญากรรมทางเทคโนโลยี จำนวนทั้งสิ้น 235,677 คดี รวมมูลค่าความเสียหาย 34,979,043,391 บาท

แน่นอนว่าภัยคุกคามไซเบอร์เหล่านี้ส่งผลกระทบต่อผู้คนทั้งโลก อีกทั้งมีโอกาสเพลี่ยงพล้ำตกเป็นเหยื่อได้ทุกเมื่อหากเผลอไผลหรือไม่รู้เท่าทันกลโกง ดังนั้นความสามารถในการตั้งรับและต่อสู้กับภัยไซเบอร์ จึงเป็นหนึ่งในเป้าหมายและความท้าทายด้านความปลอดภัยบนโลกออนไลน์ที่ใหญ่ที่สุดในเวลานี้ และถือเป็นหน้าที่ของทุกคน ไม่จำกัดเฉพาะแค่ผู้เชี่ยวชาญ หรือหน่วยงานใดหน่วยงานหนึ่งเท่านั้น

วารสารบัวบานฉบับนี้นำเสนอประเด็น 'ไซเบอร์วัคซีน' ภูมิคุ้มกันโจรออนไลน์ เพื่อร่วมเป็นส่วนหนึ่งในการสร้างความตระหนักรู้ ให้ความรู้ความเข้าใจเรื่องการรักษาความปลอดภัยในโลกไซเบอร์ ลดความเสียหายทางเศรษฐกิจที่อาจเกิดขึ้นในภาคธุรกิจอันนำไปสู่การดำเนินกิจการอย่างเติบโตและยั่งยืน ขณะเดียวกันยังเป็นการสร้างเสริมคุณภาพชีวิตที่ดีให้แก่ประชาชนคนทั่วไปให้สามารถรู้เท่าทันกลโกงภัยต่างๆ ที่มาในรูปแบบออนไลน์ เพื่อให้ทุกคนสามารถใช้ชีวิตได้อย่างมั่นคงปลอดภัย อันถือเป็นสิทธิขั้นพื้นฐานในการดำรงชีวิตของมนุษย์

เริ่มต้นด้วยคอลัมน์ SD Story ที่ถ่ายทอดเรื่องราวของความร่วมมือทั้งภาครัฐ และภาคเอกชน (Public Private Partnership หรือ PPP) เพื่อร่วมเป็นเครือข่ายในการยับยั้ง ป้องกัน และสร้างภูมิคุ้มกันผ่านโครงการไซเบอร์วัคซีนแก่ประชาชนเพื่อให้รู้เท่าทันกลโกงรูปแบบต่างๆ ของมิจฉาชีพ โดยสำนักงานตำรวจแห่งชาติ และเครือซีพีได้ร่วมสร้างสังคมตื่นรู้ในครั้งนี้ผ่านการระดมสรรพกำลังของกลุ่มธุรกิจในเครือฯ ร่วมประชาสัมพันธ์กลโกงของอาชญากรรมไซเบอร์ในทุกช่องทางการสื่อสารอย่างเต็มศักยภาพ พร้อมกันนั้นยังชวนคุณทนายคนดังแห่งยุค ทนายนิด้า-ศรันยา หวังสุขเจริญ มานั่งคุยกันผ่าน SD Talk ว่าด้วยเรื่องราคาที่ต้องจ่าย หากเผลอใช้โซเชียลอย่างขาดสติ เพราะอาจต้องไปเจอกันที่ศาลและจ่ายค่าขอโทษเป็นเงินสดเท่านั้น ดังนั้นในการแสดงความคิดเห็นใดๆ ก็ตามบนโลกโซเชียล ต้องยึดกฎกติกา มารยาท ไม่หมิ่นประมาทใครให้ได้รับเสียหาย

จากนั้นไปลองสำรวจภัยคุกคามความปลอดภัยทางไซเบอร์อันดับต้นๆ ในปี 2023 ว่ามีอะไรบ้างในคอลัมน์ Think Forward และองค์กรใหญ่ระดับโลกมีวิธีรับมือกับปัญหาด้านอาชญากรรมทางเทคโนโลยีอย่างไรบ้าง ในคอลัมน์ Catch up ก่อนไปเรียนรู้ Digital Literacy Skill ซึ่งเป็นทักษะจำเป็นแห่งยุค เพื่อรับมือกับภัยดิจิทัล จากคอลัมน์ Creating a better Life ปิดท้ายกันที่ SD LIFE ชวนผู้อ่านไปรู้เท่าทันภัยไซเบอร์ผ่านความบันเทิง ความรู้ และแรงบันดาลใจ

ทั้งหมดล้วนบ่งชี้ว่า ถึงเวลาแล้วที่ทุกองคาพยพของสังคม ไม่ว่าจะเป็นองค์กรธุรกิจ สถาบันการเงิน หน่วยงานภาครัฐที่มีส่วนเกี่ยวข้องรับผิดชอบ จำเป็นต้องวางนโยบายในการบริหารจัดการความเสี่ยงต่อภัยคุกคามทางไซเบอร์อย่างรอบด้าน เพื่อลดผลกระทบด้านความเสียหายที่อาจเกิดขึ้น ขณะเดียวกันประชาชนคนทั่วไปเองที่อยู่ในโลกยุค 5G อินเทอร์เน็ตและสมาร์ทโฟนเข้าถึงทุกระดับชั้น ทุกคนล้วนจำเป็นต้องมีความรู้เท่าทันภัยจากโซเบอร์ เพื่อลดความเสี่ยงในการตกเป็นเหยื่อในโลกไซเบอร์ตามที่เป็นข่าวไม่เว้นแต่ละวัน

เพราะท้ายที่สุดแล้วต้องถือเป็นภารกิจร่วมของทุกคน ไม่จำกัดเฉพาะแค่ผู้เชี่ยวชาญหรือหน่วยงานใดหน่วยงานหนึ่งเท่านั้น สำหรับเป้าหมายและความท้าทายในการลดความเสี่ยงและร่วมสร้างความปลอดภัยบนโลกออนไลน์ในเวลานี้

ดร.ยุทธ
บรรณาธิการบริหาร

HEART HEALTH HOME

เมล็ดพันธุ์แห่งความยั่งยืน

โลกจะยั่งยืนได้ต้องอาศัยความร่วมมือในการขับเคลื่อน ภายใต้กรอบ 3Hs HEART - HEALTH - HOME

HEART มุ่งมั่น...ทำธุรกิจด้วยใจที่ยั่งยืน

HEALTH มุ่งมั่น...สร้างสังคมยั่งยืน

HOME มุ่งมั่น...เพื่อสิ่งแวดล้อมยั่งยืน

บรรณาธิการบริหาร :
ดร.ธีระพล ถนอมศักดิ์ยุทธ (ดร. ยุทธ)
คณะบรรณาธิการ : สำนักยุทธศาสตร์ข้อมูลและการสื่อสาร เครือเจริญโภคภัณฑ์
เจ้าของ : สำนักยุทธศาสตร์ข้อมูลและการสื่อสาร
บริษัท เครือเจริญโภคภัณฑ์ จำกัด
อาคารทรูทาวเวอร์ ชั้น 27 เลขที่ 18
ถนนรัชดาภิเษก แขวงห้วยขวาง
เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ : 0-2858-6286, 0-2858-6254
อีเมล : prcpgroup@cp.co.th

จัดพิมพ์โดย : บริษัท พริ้นท์ ซิตี้ จำกัด
29/45-46 ซอยวัดสามง่าม ถนนพระราม ที่ 1 แขวงรองเมือง เขตปทุมวัน
กรุงเทพฯ 10330
ร่วมสร้างสรรค์เนื้อหาและศิลปกรรมโดย :
บริษัท เปเปอร์คอรัส จำกัด
โทรศัพท์ : 0-2887-4830
โทรสาร : 0-2887-0486
อีเมล : paperchorus@hotmail.com

GreenPrint Carbon Neutral
1777-73851277-73851278-VCU-009

เครือเจริญโภคภัณฑ์มีความตระหนักถึงผลกระทบต่อสิ่งแวดล้อม จึงเลือกผลิตวารสารเล่มนี้ผ่าน 'นวัตกรรมการพิมพ์สีเขียว' ที่มีส่วนช่วยลดปริมาณก๊าซเรือนกระจกจากกระบวนการผลิต เทียบเท่าการปิดหลอดไฟ 1 ชั่วโมง ในการรณรงค์ลดโลกร้อน จำนวน 2,712 ดวง ต่อวารสาร 3,000 เล่ม และในส่วนที่ไม่สามารถลดปริมาณก๊าซเรือนกระจก ได้จัดหาคาร์บอนเครดิตมาชดเชยเท่ากับศูนย์ จากปริมาณการปล่อยก๊าซเรือนกระจกทั้งหมด 0.56 ตัน เพื่อให้ได้หนังสือคุณภาพดีและเป็นส่วนหนึ่งในการทำให้โลกยั่งยืน

เรื่อง : ชนานันทน์

ภัยคุกคามไซเบอร์ ความเสี่ยงสำคัญระดับโลก

การประชุม World Economic Forum 2023 ชี้ให้เห็นว่า ภัยคุกคามไซเบอร์ (Cybercrime) ได้กลายเป็น 1 ใน 5 ความเสี่ยงที่สำคัญระดับโลก และคาดการณ์ว่าภายในปี 2025 ความเสี่ยงดังกล่าวจะมีมูลค่าความเสียหายสูงมากถึง 10.5 ล้านล้านเหรียญดอลลาร์สหรัฐต่อปี

ดังนั้นความสามารถในการตั้งรับและต่อสู้กับภัยไซเบอร์ (Cyber Resilience) จึงเป็นหนึ่งในเป้าหมายและความท้าทายด้านความปลอดภัยบนโลกออนไลน์ที่ใหญ่ที่สุดในเวลานี้ และถือเป็นหน้าที่ของทุกคน ไม่จำกัดเฉพาะแค่ผู้เชี่ยวชาญ หรือหน่วยงานใดหน่วยงานหนึ่ง ภารกิจสำคัญนี้จำเป็นต้องเกิดขึ้นจากความร่วมมือกันระหว่างนานาชาติในรูปแบบไร้พรมแดน

รวมภัยคุกคามความปลอดภัยทางไซเบอร์อันดับต้นในปี 2023

การโจมตีทางไซเบอร์จะซับซ้อนมากยิ่งขึ้นและสร้างความเสียหายมากขึ้นทุกขณะ สวนทางกับการขาดแคลนผู้เชี่ยวชาญ ดังที่ Heather Ricciuto จาก IBM Security ได้กล่าวกับ cnbc.com ไว้ ไม่ว่าองค์กรขนาดใหญ่หรือบุคคลธรรมดา ทุกคนต่างมีความเสี่ยงไม่น้อยไปกว่ากัน เป็นเหตุผลให้ผู้เชี่ยวชาญด้านไซเบอร์ รวมถึงมหาวิทยาลัยซานดิเอโก รัฐแคลิฟอร์เนีย สหรัฐอเมริกา รวบรวมแนวโน้มภัยคุกคามความปลอดภัยทางไซเบอร์อันดับต้นปี 2023 มาแบ่งปัน เพื่อให้ทุกคนตระหนักถึงภัยไซเบอร์รอบตัว ได้แก่

‘การโจมตีช่องโหว่ในระบบคลาวด์’ เช่น จากช่องโหว่ของการที่มีผู้เข้าใช้ร่วมกัน อาจรวมถึง API ที่ไม่ปลอดภัยและขาดการตรวจสอบสิทธิ์แบบหลายขั้นตอน ‘การโจมตีด้วยการละเมิดข้อมูล’ คือการที่ข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต และการที่จะนำหรือกู้ข้อมูลกลับมาได้อาจมีค่าใช้จ่ายราคาแพงที่ต้องแลก ‘การโจมตีระหว่างการทำงานแบบไฮบริด’ การทำงานทางไกล จากที่ไหนก็ได้ เสี่ยงที่จะถูกโจมตีมากกว่าการนั่งทำงานในออฟฟิศจากหลายปัจจัย เช่น การเข้าถึงข้อมูลละเอียดอ่อนผ่านเครือข่าย Wi-Fi ที่ไม่ปลอดภัย ‘การโจมตีผ่านตัวสมาร์ตโฟน’ เช่น ฟิชชิง (โดยเฉพาะการส่งข้อความ) รหัสผ่านปลอดภัยต่ำ สปายแวร์ และแอปพลิเคชันอันตราย

‘การโจมตีแบบฟิชชิงที่ซับซ้อนขึ้น’ ได้แก่ การหลอกให้คลิกลิงก์ที่ติดตั้งมัลแวร์ หรือให้เปิดเผยข้อมูลที่ละเอียดอ่อนจะซับซ้อนอีกขั้น ‘การโจมตีผ่าน IoT-Internet of Things’ มาในรูปแบบอุปกรณ์ เช่น ระบบรักษาความปลอดภัยภายในบ้าน สมาร์ตวอตช์ แท็บเล็ต อุปกรณ์การแพทย์ ฯลฯ ‘การโจมตีโดย Ransomware ที่มาพร้อมกลยุทธ์’ ขณะที่บริษัทต่างๆ ให้ความสำคัญกับระบบความปลอดภัยที่แข็งแกร่ง แฮ็กเกอร์อาจปรับแผนไปที่เหยื่อรายอื่น เช่น บุคคลที่มีรายได้สูง ‘การโจมตีโดย Cryptojacking’ การแอบเข้าถึงอุปกรณ์คอมพิวเตอร์แล้วขโมยทรัพยากรคอมพิวเตอร์มาใช้งานขุดเหมืองเงินดิจิทัล โดยเจ้าของไม่รู้ตัว

ความหวังในระดับนานาชาติ เมื่อมองหาความปลอดภัยในโลกไซเบอร์

บทความ Global Risks Report 2023: We know what the risks are - here’s what experts say we can do about it จากการประชุม World Economic Forum 2023 ได้ย้ำว่า ความไม่แน่นอนทางการเมืองและเศรษฐกิจ ทำให้ภัยคุกคามจากการโจมตีทางไซเบอร์รุนแรงขึ้น เพิ่มความเสี่ยงให้แก่ธุรกิจทั่วโลกอย่างเลี่ยงไม่ได้ และยังคงเป็นหนึ่งในประเด็นที่ต้องแก้ไขอย่างเร่งด่วนที่สุด

ขณะเดียวกันเรายังสามารถเห็นถึงความหวัง เมื่อ Akshay Joshi หัวหน้าฝ่ายอุตสาหกรรมและพันธมิตร ศูนย์ความปลอดภัยทางไซเบอร์ของ World Economic Forum ได้กล่าวไว้ว่า ในปัจจุบันมีความคืบหน้าในการส่งเสริมความตระหนักรู้และเตรียมการด้านความปลอดภัยทางไซเบอร์โดยเฉพาะภาคธุรกิจที่สามารถติดอาวุธให้ตนเองได้ด้วยการปรับปรุงความรู้ทางไซเบอร์ การสื่อสาร และการแบ่งปันข้อมูล เพื่อเพิ่มความยืดหยุ่น (Resilience) ให้องค์กรสามารถลุกได้ไว ฟื้นตัวกลับมาได้อย่างรวดเร็วหากถูกโจมตี

ที่มา : https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/ https://www.cyfence.com/article/10-cyber-threats-expected-in-2023/ https://www.mandiant.com/resources/reports/mandiant-cyber-security-forecast-2023 https://www.bangkokbiznews.com/pr-news/news/corporate-moves/1036849 https://www.the101.world/cybercrime-in-21st-century/ https://www.weforum.rg/agenda/2023/01/global-risks-report-2023-experts-davos2023 https://www.cyfence.com/it-360/what-is- cryptojacking/

แสดงความคิดเห็นคอลัมน์นี้

● เรื่อง : กองบรรณาธิการ ภาพ : เนาวรัตน์ บุญวิภาส

ไซเบอร์วัคซีน ภูมิคุ้มกันโจรออนไลน์

ภัยคุกคามไซเบอร์เป็น 1 ใน 5 ความเสี่ยงที่สำคัญระดับโลก ในการประชุม World Economic Forum 2023 ระบุไว้เช่นนั้น ซึ่งความเสียหายที่จะเกิดขึ้นจากความเสี่ยงภัยดังกล่าวนี้ คาดการณ์ว่าจะเป็นมูลค่าสูงถึง 10.5 ล้านล้านเหรียญ ภายในปี 2568 ขณะที่ประเทศไทยนั้นสถิติการรับแจ้งความคดีเกี่ยวกับออนไลน์นับวันยิ่งพุ่งสูง ภายใน 1 ปี (ปี 2565-2566) มีผู้เสียหายเข้าแจ้งความกว่า 200,000 ราย รวมมูลค่าความเสียหายกว่า 3.4 หมื่นล้านบาท ยังไม่นับรวมความสูญเสียทางจิตใจ ความรู้สึกไม่มั่นคงปลอดภัยในชีวิตและทรัพย์สิน ซึ่งล้วนเป็นความเสียหายที่ไม่อาจนิ่งนอนใจได้

วารสารบัวบานฉบับนี้จึงนำเสนอประเด็นอาชญากรรมทางเทคโนโลยีเพื่อสร้างความตระหนักรู้ ให้ความรู้ความเข้าใจเรื่องของการรักษาความปลอดภัยในโลกไซเบอร์ เพื่อลดความเสียหายทางเศรษฐกิจที่อาจเกิดขึ้นในภาคธุรกิจอันนำไปสู่การดำเนินธุรกิจอย่างเติบโตและยั่งยืน ขณะเดียวกันยังเป็นการสร้างเสริมคุณภาพชีวิตที่ดีให้แก่ประชาชนคนทั่วไป ให้สามารถรู้เท่าทัน ไม่หลงเชื่อหรือตกเป็นเหยื่อกลโกงของมิจฉาชีพที่มาในรูปภัยออนไลน์ ลดความสูญเสียต่อประชาชนและประเทศชาติ

"อาชญากรรมทางเทคโนโลยีอยู่ในภาวะวิกฤติ เราต้องเร่งสร้างภูมิคุ้มกันด้วยไซเบอร์วัคซีน"

พล.ต.อ. ดำรงศักดิ์ กิตติประภัสร์

ผู้บัญชาการตำรวจแห่งชาติ

ภาพจาก : เครือซีพี

● ดังที่มักปรากฏเป็นข่าวรายวันให้รับทราบกันมาตลอดถึงสถานการณ์อาชญากรรมทางเทคโนโลยี หรืออาชญากรรมไซเบอร์หลากหลายรูปแบบที่เกิดขึ้นในบ้านเรา และนับวันยิ่งมีสถิติที่เพิ่มสูงขึ้น ซึ่งจากการรวบรวมตัวเลขคดีรับแจ้งความออนไลน์ (ตั้งแต่ 1 มี.ค. 2565 ถึงล่าสุดเมื่อวันที่ 8 เม.ย. 2566) พบว่ามีการรับแจ้งความอาชญากรรมทางเทคโนโลยี จำนวนทั้งสิ้น 235,677 คดี รวมมูลค่าความเสียหาย 34,979,043,391 บาท สามารถติดตามอายัดบัญชีได้ทัน 465,932,428 บาท สำนักงานตำรวจแห่งชาติ โดย พล.ต.อ. ดำรงศักดิ์ กิตติประภัสร์ ผู้บัญชาการตำรวจแห่งชาติ ตระหนักถึงความสำคัญและห่วงใยในสวัสดิภาพของประชาชนคนไทย จึงบูรณาการความร่วมมือระหว่างองค์กรทั้งในส่วนของภาครัฐ ภาคเอกชน และภาคประชาชน (Public-Private Partnership หรือ PPP) เพื่อร่วมเป็นเครือข่ายในการยับยั้ง ป้องกัน และสร้างภูมิคุ้มกัน (Cyber Vaccine) แก่ประชาชนเพื่อให้รู้เท่าทันกลโกงรูปแบบต่างๆ ของมิจฉาชีพ ซึ่งตลอดระยะเวลาการดำเนินงานได้รับความร่วมมือเป็นอย่างดีจากทุกภาคส่วน เพื่อร่วมประชาสัมพันธ์สร้างการรับรู้ไปยังประชาชนทั้งประเทศอย่างทั่วถึง

"ปัจจุบันคดีอาชญากรรมทางเทคโนโลยี หรือที่เรามักเรียกกันว่าคดีออนไลน์มีสถิติการรับแจ้งความเพิ่มมากขึ้น บางวันมียอดรับแจ้งสูงเกือบ 1,000 เรื่องต่อวัน ซึ่งคนร้ายมีการพัฒนารูปแบบและกลโกงที่แปลกใหม่และหลากหลาย ส่งผลให้ประชาชนได้รับความเดือดร้อน และสูญเสียทรัพย์สินเป็นจำนวนมาก ถือได้ว่าขณะนี้สถานการณ์อาชญากรรมทางเทคโนโลยีอยู่ในภาวะวิกฤติ"

สำนักงานตำรวจแห่งชาติจึงกำหนดมาตรการเพื่อแก้ไขปัญหาให้ครอบคลุมในทุกมิติ ไม่ว่าจะเป็นด้านการป้องกัน ปราบปราม และพัฒนาระบบงานสืบสวนสอบสวน ปรับปรุงแก้ไขกฎหมายที่ไม่เอื้ออำนวยกับการปฏิบัติงาน และการประชาสัมพันธ์ให้ประชาชนได้รู้เท่าทัน ไม่ตกเป็นเหยื่อกลโกงของคนร้ายบนโลกออนไลน์ รวมทั้งได้จัดทำระบบรับแจ้งความที่สะดวกและรวดเร็วผ่านระบบออนไลน์

www.thaipoliceonline.com ทำให้สามารถจำแนกลักษณะพฤติกรรมของคนร้าย ซึ่งมีการเปลี่ยนรูปแบบกลโกงอยู่ตลอดเวลา และช่วยประมวลผลให้เห็นความเชื่อมโยงของคดีที่ได้รับแจ้ง ช่วยให้เจ้าหน้าที่ตำรวจได้นำไปวิเคราะห์และวางแผนในการป้องกันปราบปรามสืบสวน จับกุมคนร้ายได้อย่างมีประสิทธิภาพยิ่งขึ้น

“สำหรับการแก้ไขปัญหาในระยะเร่งด่วน ขณะนี้อยู่ในระหว่างการดำเนินการ 2 เรื่อง ที่สำคัญ หนึ่งคือการเสนอร่างกฎหมาย ซึ่งได้ร่วมกับทางกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) ในการขอออกพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งเป็นกฎหมายที่จะส่งผลให้การอายัดบัญชีและการตรวจสอบเส้นทางการเงินของคนร้ายเพื่อติดตามเงินกลับมาคืนผู้เสียหาย การสืบสวนสอบสวนและการคุ้มครองประชาชนที่ถูกหลอกลวง กลโกงจากคนร้ายในรูปแบบต่างๆ เป็นไปอย่างมีประสิทธิภาพมากขึ้น ซึ่งขณะนี้ดำเนินการสำเร็จแล้วและได้ประกาศใช้เมื่อวันที่ 17 มี.ค. 2566 สองคือการเร่งประชาสัมพันธ์สื่อสร้างภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยี หรือที่เราเรียกว่า ไซเบอร์วัคซีน เพื่อนำเสนอรูปแบบกลโกงใหม่ๆ ของคนร้าย เพื่อให้ประชาชนไทยทุกสาขาอาชีพในวงกว้างทั่วประเทศสามารถเข้าถึงข้อมูลได้ง่าย แสวงหาความร่วมมือจากทุกภาคส่วน ทั้งหน่วยงานราชการและภาคเอกชน เพื่อสนับสนุนการเตือนภัย”

นอกจากนี้สำนักงานตำรวจแห่งชาติได้เล็งเห็นศักยภาพของบริษัท เครือเจริญโภคภัณฑ์ จำกัด มีการดำเนินธุรกิจที่หลากหลายกลุ่มอุตสาหกรรม ทำให้มีช่องทางที่สามารถเข้าถึงประชาชนได้เป็นจำนวนมาก ไม่ว่าจะเป็นร้านเซเว่นอีเลฟเว่น ห้างแม็คโคร ห้างโลตัส ที่มีสาขาอยู่ทั่วประเทศ เครือข่ายโทรศัพท์ทรูมูฟ เอช สถานีโทรทัศน์ช่องทีเอ็นเอ็น จึงได้ประสานขอความร่วมมือผนึกกำลังในการประชาสัมพันธ์สื่อจาก ‘โครงการไซเบอร์วัคซีน รู้ทันกลโกง ต้านภัยออนไลน์’ ซึ่งทางเครือเจริญโภคภัณฑ์พร้อมนำศักยภาพของบริษัทในเครือฯ สนับสนุนอย่างเต็มกำลัง ทั้งการร่วมผลิตสื่อและช่วยสื่อสารประชาสัมพันธ์ให้ประชาชนได้รับรู้ข้อมูลรูปแบบกลโกงของอาชญากรรมอย่างทั่วถึงและทันต่อสถานการณ์

** เรียบเรียงจากถ้อยแถลงในพิธีลงนามความร่วมมือการประชาสัมพันธ์สื่อ สร้างภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยี ระหว่างสำนักงานตำรวจแห่งชาติกับเครือเจริญโภคภัณฑ์ และข้อมูลจากเจ้าหน้าที่ผู้เกี่ยวข้อง เมื่อวันที่ 10 ก.พ. 2566*

“สูตรท่องคาถา เช็กก่อนเชื่อ แล้วจะอยู่รอด”

พล.ต.อ. สมพงษ์ ชิงดวง

ที่ปรึกษาพิเศษ สำนักงานตำรวจแห่งชาติ

วารสารบัวบานมีโอกาสพูดคุยกับ พล.ต.อ. สมพงษ์ ชิงดวง ที่ปรึกษาพิเศษ สำนักงานตำรวจแห่งชาติ ผู้รับภารกิจเป็นหัวหน้าคณะทำงานไซเบอร์วัคซีน ซึ่งเป็นโครงการที่เกิดขึ้นจากดำริของ พล.ต.อ. ดำรงศักดิ์ กิตติประภัสร์ ผู้บัญชาการตำรวจแห่งชาติ และมี พล.ต.อ. รอย อิงคไพโรจน์ รองผู้บัญชาการตำรวจแห่งชาติ รับตำแหน่งหัวหน้าศูนย์ ถึงแนวทางการทำงานและเป้าหมายที่หวังผลของโครงการดังกล่าว

สถานการณ์อาชญากรรมไซเบอร์นับวันยิ่งมีสถิติเพิ่มสูงขึ้น

ที่ปรึกษาพิเศษ สำนักงานตำรวจแห่งชาติ เปิดเผยสถานการณ์ปัจจุบันของอาชญากรรมไซเบอร์ให้ได้เห็นภาพชัดยิ่งขึ้นจากจำนวนคดีที่ได้รับแจ้งเหตุผ่านระบบออนไลน์เกี่ยวกับภัยจากคอลเซนเตอร์ที่โทรศัพท์หลอกลวงพี่น้องประชาชนทั่วประเทศ ปรากฏว่าตั้งแต่ 1 มี.ค. 2565 ถึงล่าสุดเมื่อวันที่ 8 เม.ย. 2566 มีการรับแจ้งความทั้งหมด 235,677 ราย เป็นคดีที่เชื่อมโยงกัน 119,012 คดี เป็นคดีที่ไม่เชื่อมโยงกัน 116,665 คดี ทั้งหมดมาจาก 14 ประเภทคดี มูลค่าความเสียหายรวมอยู่ที่ 34,979,043,391 ล้านบาท ซึ่งถือเป็นเม็ดเงินมหาศาล และมีแนวโน้มว่าจะสูงขึ้นเรื่อยๆ

“ส่วนใหญ่แล้วเท่าที่เราได้สอบปากคำผู้เสียหายก็จะเป็นลักษณะที่ผู้เสียหายรู้ไม่เท่าทันพวกกลุ่มมิจฉาชีพ ขาดข้อมูลข่าวสาร ท่านผู้บัญชาการตำรวจแห่งชาติได้เล็งเห็นความสำคัญก็เลยมีแนวคิดที่จะตั้งคณะทำงานขึ้นมา เรียกว่า ไซเบอร์วัคซีน สร้างภูมิคุ้มกันให้พี่น้องประชาชนรู้เท่าทัน ซึ่งผมเชื่อว่า ถ้าคนไทยได้รับรู้ข้อมูล เบาะแสกลโกงต่างๆ เท่าทันแก๊งมิจฉาชีพ ก็จะลดความเสียหายได้มาก และตรงนี้เป็นภัยใกล้ตัว ก็เลยต้องประสานความร่วมมือกับผู้ทรงคุณวุฒิทุกภาคส่วน ทั้งหน่วยงานของรัฐ ทั้งภาควิชาการ จากจุฬาฯ สถาบันบัณฑิตพัฒนบริหารศาสตร์ สื่อมวลชน ผู้บริหารสถานีโทรทัศน์ ไปรษณีย์ไทย ปตท. สำนักงานสลากกินแบ่งรัฐบาล รวมทั้งภาคเอกชน เช่น ซีพี เป็นความพยายามส่วนหนึ่งที่จะให้ความรู้แก่พี่น้องประชาชนให้ได้มากที่สุด เพื่อให้รู้เท่าทันกลโกงของแก๊งมิจฉาชีพ โดยเฉพาะกลุ่มต่างประเทศที่มาตั้งเซิร์ฟเวอร์อยู่ประเทศเพื่อนบ้านเรา พยายามลวงพี่น้องประชาชนคนไทยไปทำงาน บางคนถูกหลอกไปบางคนไปแล้วก็สมัครใจอยู่ เพราะได้ค่าคอมมิชชันจากการหลอกพี่น้องคนไทยด้วยกัน อันนี้ก็เป็นสิ่งที่น่าห่วง

“ด้วยความที่โทรศัพท์มือถือมีเกือบทุกบ้าน ทุกคน อินเทอร์เน็ตเข้าไปถึงห้องนอน ห้องครัว ประเทศไทยเรามีคนเกือบ 70 ล้านคน บางคนอยู่บ้าน บางคนก็อาจไม่ได้ติดตามข่าวสาร ไม่ได้รับรู้ภัยตรงนี้ อีกทั้งกลุ่มมิจฉาชีพ แก๊งคอลเซนเตอร์ มีการพัฒนาเรื่อยๆ กลโกงไปเรื่อย พอจับได้ก็หาวิธีการใหม่ๆ มาใช้ จึงต้องมีการสร้างภูมิคุ้มกันให้พี่น้องประชาชน ให้รู้เท่าทันกลโกงต่างๆ”

เปิดโผท็อป 5 รูปแบบกลโกง

จากการเก็บข้อมูลของสำนักงานตำรวจแห่งชาติ ประมวลผลออกมาว่าคดีที่ได้รับแจ้งสามารถแบ่งกว้างๆ ได้เป็น 14 ประเภทคดี โดยที่ปรึกษาพิเศษ ตร. ได้เปิดเผยถึง 5 อันดับแรกของประเภทคดีที่ได้รับแจ้งเข้ามามากที่สุด

“อันดับ 1 ที่นำมาเลยคือการหลอกลวงซื้อขายสินค้า โดยกลยุทธ์คือการขายสินค้าราคาไม่แพง เช่น ชิ้นละ 300 500 บาท แล้วไม่ส่งของให้ ซึ่งด้วยธรรมชาติของคนไทยหรือผู้เสียหาย พอเป็นเงินจำนวนไม่มาก ก็ไม่อยากเสียเวลาไปแจ้งความ อันนี้คือสิ่งที่เราห่วงกังวล อันดับ 2 คือการหลอกให้โอนเงินเพื่อทำงาน พวกนี้จะมาในรูปแบบของการเปิดรับสมัครน้องๆ นักศึกษาไปทำอาชีพเสริม ถูกหลอกกันเยอะ ฝากเตือนเยาวชน หรือน้องๆ ที่เรียนมหาวิทยาลัย ต้องพยายามศึกษาให้ดีในการที่จะไปรับงานพวกนี้

“ส่วนอันดับ 3 เป็นเรื่องของหลอกให้กู้เงินทางออนไลน์ โดยมีสิ่งที่เป็นแรงจูงใจ เช่น ดอกเบี้ยถูกบ้าง ปลอมเป็นเว็บไซต์บริษัทสินเชื่อบ้าง หรือให้กู้ส่วนตัวบ้าง พวกนี้จะก๊อปโลโก้ของธนาคารให้เกิดความน่าเชื่อถือ เท่าที่เราประชุมกับทุกธนาคาร นโยบายของทุกธนาคารจะไม่มีการทำธุรกรรมทางออนไลน์แล้ว เพราะถูกแอบอ้างเยอะ อันดับ 4 เป็นเรื่องหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ เช่น อ้างว่าบริษัทในตลาดหลักทรัพย์ ต้องการพนักงานใหม่ มีหัวคิดกว้างไกล แล้วหลอกให้ลงทุนเล็กๆ น้อยๆ แต่ได้กำไรหรือผลตอบแทนต่อเดือนสูงถึง 50% ทำยอดได้ถึงจะโอนให้ก่อน พอเห็นได้เงินง่ายคนก็จะชวนญาติพี่น้องมาร่วม แต่พอคุณจะถอน คุณก็ต้องเอาเงินมาโปะเพื่อเป็นหลักประกัน บางทีหลอกว่าเป็นเงินคริปโตฯ ปั้นตัวเลขขึ้นมาแต่เงินมีจริงหรือไม่จริงไม่รู้ คนเห็นว่ามีโบนัส เด็กอยากหารายได้เสริม อยากช่วยแบ่งเบาภาระพ่อแม่ ก็ยอมลงทุน พวกนี้จะมีเทคนิคการพูดที่เป็นแรงจูงใจทำให้คนหลงเชื่อ ส่วนอันดับที่ 5 คือกรณีข่มขู่ทางโทรศัพท์ (Call Center) เช่น ท่านมีบัญชีพัวพันกับการทำผิดกฎหมาย ท่านต้องให้ข้อมูลดังนี้ 1 2 3 4 พอกดปุ๊บ เข้าสู่ลิงก์ที่เขาฝังไว้ในสปายแวร์ดูดข้อมูลและควบคุมบัญชีของผู้เสียหาย เงินก็จะหมดบัญชีภายในไม่กี่นาที

“แล้วก็ทราบว่าตอนนี้มีระบบ AI ซึ่งเลียนแบบเสียงของคนด้วย เพราะพวกกลุ่มคนร้ายนี่พอเรารู้ทันวิธีการเหล่านี้ เขาก็จะดัดแปลงหาวิธีการใหม่ไปเรื่อยๆ ซึ่งเท่าที่เก็บสถิติกลโกงต่างๆ ตอนนี้ก็มีประมาณ 14 ประเภทครับ”

แนวทางป้องกันภัยไซเบอร์ที่ทุกคนควรต้องรู้

“กลุ่มที่น่าเป็นห่วงคือผู้หลักผู้ใหญ่คนวัยเกษียณแล้วที่มักจะเก็บเงินไว้ในบัญชีเดียว เป็นเงินจำนวนมากจากการสร้างเนื้อสร้างตัวมาทั้งชีวิต แล้วถูกคนพวกนี้หลอกให้หลงเชื่อกดลิงก์แล้วเข้ามาควบคุมบัญชีดูดเงินไปเก็บเงินมาทั้งชีวิต 5 ล้าน 10 ล้าน บางคนแทบฆ่าตัวตาย เพราะเงินหายไปหมดเลย

“ทางแก้หนึ่งคือ เปิดอีกบัญชีหนึ่งแยกถ้าต้องการทำธุรกรรมการเงินผ่านโทรศัพท์ต้องการใช้เดือนละ 10,000 บาท ก็ใส่ไว้เท่านั้น อย่างน้อยถ้าหลงพลาดไป ก็ยังเสียเงินหลักหมื่นไม่ได้หมดไปทั้งบัญชี

“แต่ทางที่ดีที่สุดคือ ต้องเช็กก่อนเชื่อ แล้วจึงจะปลอดภัย อยากฝากประชาสัมพันธ์ไปกับน้องๆ เยาวชน พยายามให้ข้อมูลคนเฒ่าคนแก่ที่บ้านด้วยนะครับว่ากรณีที่มีคนโทรศัพท์มาติดต่อ ไม่ว่าจะเป็นทางโทรศัพท์ทางไลน์เฟซบุ๊ก หรือโซเชียลมีเดียต่างๆ อย่าเชื่อโดยเด็ดขาด ให้ตั้งสมมติฐานไว้ก่อนเลยว่าเป็นแก๊งคอลเซนเตอร์ ถ้าเขาอ้างเป็นหน่วยงานของรัฐมีการออกหนังสือหรือมีหมายเรียกให้ติดต่อไปที่ทำการของรัฐ ไฟฟ้า ประปา ศาล หรือสถานีตำรวจ ก่อนที่จะทำตามอะไรเขา ขอให้เช็กก่อนอะไรที่ไม่มั่นใจ ขอให้โทรศัพท์ถามบุตรหลานหรือเจ้าตัวคนที่ถูกแอบอ้างก่อน ยอมเสียเวลาอีกนิดหนึ่ง ตรวจสอบให้ละเอียด เช็กก่อนเชื่อแล้วเราจะไม่ถูกหลอก”

วัคซีน 14 เข็ม รูปแบบอาชญากรรมทางออนไลน์ รู้ไว้... เท่าทันภัยไซเบอร์

1. คดีหลอกลวงซื้อขายสินค้าหรือบริการที่ไม่มีลักษณะเป็นขบวนการ
2. คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน
3. คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)
4. คดีหลอกลวงให้โอนเงินเพื่อรับรางวัล หรือวัตถุประสงค์อื่นๆ
5. คดีหลอกลวงให้กู้เงิน
6. คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ
7. คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน
8. คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking) ที่ทำให้เกิดความเสียหายในทางทรัพย์สิน
9. คดีเรียกค่าไถ่ทางคอมพิวเตอร์ (Ransomware)
10. คดีหลอกลวงให้ติดตั้งโปรแกรมเพื่อควบคุมระบบในเครื่องโทรศัพท์
11. คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล
12. คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์
13. คดีหลอกลวงซื้อขายสินค้าหรือบริการที่มีลักษณะเป็นขบวนการ
14. คดีหลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก. กู้ยืมเงินอันเป็นการฉ้อโกงประชาชน พ.ศ. 2527

5 ประเภทคดีติดอันดับ คนถูกหลอกมากที่สุด*

อันดับ 1	หลอกลวงซื้อขายสินค้าหรือบริการ	83,309	ราย
อันดับ 2	หลอกให้โอนเงินเพื่อทำงาน	32,342	ราย
อันดับ 3	หลอกให้กู้เงิน	29,766	ราย
อันดับ 4	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	20,942	ราย
อันดับ 5	กรณีข่มขู่ทางโทรศัพท์ (Call Center)	18,653	ราย

* สถิติสะสมในช่วงเวลาราว 1 ปี ตั้งแต่ 1 มี.ค. 2565 - 8 เม.ย. 2566

กฎหมายปราบโกงออนไลน์ ช่วยเหยื่อเอื้อประโยชน์ผู้เสียหาย

เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน โดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ได้มีการออกพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และเริ่มมีผลบังคับใช้หลังประกาศในราชกิจจานุเบกษาวันที่ 17 มี.ค. 2566 ที่ผ่านมา เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ โดยมีสาระสำคัญหลายมาตรา อาทิ มาตรา 6 และ 7 ซึ่งจะอำนวยความสะดวกให้ผู้เสียหายสามารถดำเนินการอายัดบัญชีและแจ้งความร้องเรียนได้รวดเร็วยิ่งขึ้น

“กรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหายซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่าได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินหรือผู้ประกอบธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว ถือเป็นการคุ้มครองผู้เสียหายที่ถูกหลอกให้สามารถแจ้งธนาคารได้เลย และเป็นหน้าที่ธนาคารที่จะต้องรีบอายัดบัญชี จากนั้นแจ้งเจ้าหน้าที่ตำรวจภายใน 72 ชั่วโมง ถ้าแจ้งแล้ว ธนาคารไม่อายัดให้ธนาคารก็ต้องชดใช้ เคยมีคำพิพากษาศาลฎีกากำหนดให้ธนาคารร่วมชดใช้ครึ่งหนึ่งของยอดเงินผู้เสียหาย เพราะเมื่อธนาคารเป็นผู้ให้บริการและเก็บค่าบริการจากลูกค้า จะต้องมีหน้าที่ในการดูแลหามาตรการความปลอดภัยกลุ่มลูกค้า ต้องมีมาตรการช่วยเหลือหรือต้องยอมลงทุนกับเทคโนโลยีที่จะสามารถตรวจสอบได้ว่ามีเงินเกินเข้ามาหรือออกไปอย่างผิดธรรมชาติหรือไม่ ถ้าไม่มีก็เป็นโอกาสให้ผู้เสียหายฟ้องเรียกค่าเสียหายได้”

ในขณะที่การร้องทุกข์ความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีนั้นสามารถกระทำต่อพนักงานสอบสวน ณ สถานีตำรวจแห่งใดในราชอาณาจักร หรือต่อกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีก็ได้และจะร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ “บางทีการต้องไปถึงสถานีตำรวจท้องที่ที่เกิดเหตุจะเสียเวลา บางทีอาจอายัดเงินไม่ทัน กฎหมายก็เลยเปิดช่องให้ผู้เสียหายได้ใช้ช่องทางออนไลน์ในการที่จะรีบแจ้งเจ้าหน้าที่ให้มีอำนาจในการสอบสวน”

ส่วนบทลงโทษผู้กระทำความผิด มาตรา 9 มาตรา 10 และมาตรา 11 ต่างระบุให้เอาผิดผู้ที่ยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตนเอง โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน

“เป็นกฎหมายที่ทำให้เรามีเครื่องไม้เครื่องมือในการหาตัวผู้ทำความผิด ช่วยในการทำงานของเจ้าหน้าที่ อยากฝากพี่น้องประชาชนทุกคนไว้ด้วยว่า หากเกรงว่าจะมีคนนำสำเนาบัตรที่เราไปสมัครงานหรือติดต่อหน่วยราชการไปใช้ ควรจะไปตรวจสอบดูว่าเรามีเปิดบัญชีอะไรมั้ย สามารถยื่นคำร้องธนาคารเขาตรวจสอบให้ได้ และถ้าเราพบว่าผิดปกติ มีการแอบอ้างไปใช้เป็นบัญชีม้า รีบปิด จะไม่โดนข้อหานี้”

ความร่วมมือภาคเอกชนโครงการไซเบอร์วัคซีน

เมื่อวันที่ 10 กุมภาพันธ์ ที่ผ่านมา พล.ต.อ. ดำรงศักดิ์ กิตติประภัสร์ ผู้บัญชาการตำรวจแห่งชาติ เป็นผู้แทนลงนามบันทึกความเข้าใจความร่วมมือว่าด้วยการประชาสัมพันธ์สื่อสร้างภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยี ร่วมกับเครือเจริญโภคภัณฑ์ โดยมี นายศุภชัย เจียรวนนท์ ประธานคณะผู้บริหาร บริษัท เครือเจริญโภคภัณฑ์ เป็นผู้แทนลงนาม ทั้งนี้มีผู้บังคับบัญชาระดับสูงของสำนักงานตำรวจแห่งชาติ พร้อมด้วยผู้แทนบริษัทในเครือเจริญโภคภัณฑ์เข้าร่วม

“ต้องขอบคุณเครือซีพีที่เล็งเห็นถึงความเดือดร้อนของพี่น้องประชาชนในประเด็นนี้ และได้ให้การสนับสนุนในเรื่องการติดป้ายประชาสัมพันธ์ตามเซเว่นอีเลฟเว่น หรือจะมีช่องทางอื่นที่ทางซีพีทำได้ และทราบว่าทางผู้บริหารของซีพีก็ให้ความสำคัญเรื่องนี้

“การที่สำนักงานตำรวจแห่งชาติต้องสร้างความร่วมมือกับภาคเอกชน เพราะดูจากสถิติเมื่อเราประชาสัมพันธ์ไปแล้ว พี่น้องประชาชนก็ยังมาแจ้งความเพิ่มขึ้น เหตุก็เกิดสูงขึ้นเรื่อยๆ มูลค่าความเสียหายก็สูงขึ้น และเงินพวกนี้ออกนอกประเทศ เพราะฉะนั้นถ้าเราไม่หยุดยั้งตรงนี้ มันเหมือนสูบเลือดคนไทยไปเรื่อยๆ มันจะเกิดปัญหากระทบต่อเศรษฐกิจบ้านเรา

“ผมเชื่อว่าถ้าเราไม่ร่วมมือกัน ทุกคนได้รับผลกระทบหมด เพราะฉะนั้นต้องให้ความรู้กับญาติพี่น้องกับคนไทยทุกคน ซึ่งต้องได้รับความร่วมมือจากภาคเอกชน ซึ่งมีบุคลากรที่จะได้ช่วยกันคนละไม้คนละมือ ถ้าการแจ้งความลดลงมากเท่าไร ความเดือดร้อนของพี่น้องประชาชนก็น้อยลงเท่านั้น”

ภาพจาก : CybercopTH

ไซเบอร์วัคซีนหวังผลเลิศ ยอดผู้เสียหายลดเศรษฐกิจดีขึ้น

“ตอนนี้เราหวังว่า ทำอย่างไรให้พี่น้องประชาชนเดือดร้อนน้อยลง ไม่ถูกหลอก เราเก็บสถิติจากยอดแจ้งความ ซึ่งตอนนี้วันหนึ่งเฉลี่ยแล้วมีประมาณ 500-600 ราย ถ้าในอนาคตลดลงแสดงว่าสิ่งที่เราทำได้ผล แต่ถ้าตัวเลขยังคงเพิ่มขึ้น ก็ต้องเพิ่มเรื่องของการประชาสัมพันธ์เข้าไปอีก และอัดเรื่องการสืบสวน ปราบปราม จับกุมเข้าไปอีก ต้องทำงานหนักเพิ่มขึ้น ด้วยการแชร์ข้อมูล หรือส่งข้อมูลไปถึงพี่น้องประชาชนให้มากที่สุด รวมถึงบอกให้รู้ถึงกลโกงต่างๆ ของแก๊งมิจฉาชีพ เพื่อให้ยอดลดลงให้ได้ เพราะถ้ายอดคนโดนหลอกยังสูงขึ้น มูลค่าความเสียหายก็สูงขึ้น เงินไหลออกนอกประเทศ เพราะมีกลุ่มต่างชาติที่เป็นตัวหลักโดยไปใช้ประเทศเพื่อนบ้านในการติดตั้งเซิร์ฟเวอร์ ซึ่งกระทบภาพรวมเศรษฐกิจของประเทศ เหมือนร่างกายเราถูกดูดเลือดไปเรื่อยๆ วันหนึ่งเลือดหมดร่างกายก็อยู่ไม่ได้ อันนี้คือปัญหาในอนาคต

“ฝากไปยังน้องๆ เด็กรุ่นใหม่นะครับ เวลากลับบ้านช่วงเทศกาลก็พยายามเอาข้อมูลเหล่านี้ไปให้ผู้หลักผู้ใหญ่ ปู่ย่าตายายที่อยู่ที่บ้านให้รู้เท่าทัน สูตรท่องคาถาเลยนะครับ เช็กก่อนเชื่อ แล้วจะอยู่รอด จะทำให้การถูกหลอกลดน้อยลง แต่คงไม่หมดไป เพราะกลยุทธ์ของมิจฉาชีพ เปลี่ยนรูปแบบที่จะหลอกลวงพี่น้องประชาชนคนไทยไปเรื่อยๆ ดังนั้นตอนนี้เราต้องสร้างภูมิคุ้มกัน ด้วยการให้ความรู้ให้เท่าทันรู้กลโกงของแก๊งมิจฉาชีพออนไลน์ต่างๆ แล้วเราก็คาดหวังไว้ว่าเมื่อเราร่วมไม้ร่วมมือกันทุกฝ่าย สถิติการรับแจ้งความคงน้อยลง แต่ไซเบอร์วัคซีนคงต้องอยู่ตลอดไป เพราะวัคซีนคือการป้องกัน เหมือนกับที่เราต้องฉีดวัคซีนไข้หวัดใหญ่ทุกปี เช่นเดียวกัน งานให้ความรู้พี่น้องประชาชนเพื่อเข้าถึงกลโกงและรู้เท่าทันก็เป็นงานไม่มีวันจบสิ้น”

MORE INFO

ร้องเรียนภัยไซเบอร์หรือขอคำปรึกษาได้ที่
สายด่วน บช.สอท. 1441
หรือศูนย์ PCT 081-8663000
หรือแจ้งความผ่านระบบออนไลน์ได้ที่
www.thaipoliceonline.com

ร่วมสร้าง ‘สังคมตื่นรู้’ ด้วย ‘ไซเบอร์วัคซีน’ ไม่ตกเป็นเหยื่อภัยออนไลน์

ศุภชัย เจียรวนนท์

ประธานคณะผู้บริหาร บริษัท เครือเจริญโภคภัณฑ์ จำกัด

ที่มาของรูป : เครือซีพี

ซ้าย : พล.ต.อ. ดำรงศักดิ์ กิตติประภัสร์ ผู้บัญชาการตำรวจแห่งชาติ
ขวา : คุณศุภชัย เจียรวนนท์ ประธานคณะผู้บริหาร บริษัท เครือเจริญโภคภัณฑ์ จำกัด

● สำหรับเครือเจริญโภคภัณฑ์และบริษัทในเครือฯ ถือว่าเป็นภาคเอกชนนำร่องรายแรกที่จับมือกับสำนักงานตำรวจแห่งชาติในการสื่อสารสร้างภูมิคุ้มกันไซเบอร์วัคซีน เพื่อต้านภัยอาชญากรรมทางเทคโนโลยี โดยมี คุณศุภชัย เจียรวนนท์ ประธานคณะผู้บริหาร บริษัท เครือเจริญโภคภัณฑ์ จำกัด เป็นตัวแทนลงนามในพิธี MOU พิธีลงนามความร่วมมือการประชาสัมพันธ์สื่อ สร้างภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยี ระหว่างสำนักงานตำรวจแห่งชาติ กับ เครือเจริญโภคภัณฑ์ เมื่อเดือนกุมภาพันธ์ที่ผ่านมา

“เนื่องจากเครือฯ ได้ตระหนักดีถึงความสำคัญของการรู้เท่าทันการรับรู้เกี่ยวกับกลโกงต่างๆ ของอาชญากรรมไซเบอร์ เพราะโลกกำลังเผชิญกับความไม่ปลอดภัยทางไซเบอร์ที่มีสถิติเพิ่มสูงขึ้น มิจฉาชีพได้อาศัยเทคโนโลยีฉ้อโกงหลอกลวงประชาชน ทำให้เกิดปัญหาอาชญากรรมทางเทคโนโลยีอย่างต่อเนื่อง และในการประชุม World Economic Forum 2023 จัดให้ ‘ภัยคุกคามไซเบอร์’ เป็น 1 ใน 5 ความเสี่ยงที่สำคัญระดับโลก อีกทั้งยังมีการคาดการณ์ว่าจะมีการโจมตีทางไซเบอร์ที่รุนแรงภายใน 2 ปี โดยเฉพาะการโจมตีจากมัลแวร์และแรนซัมแวร์ที่จะเพิ่มขึ้น 400% และมีการคาดการณ์ว่าผลกระทบจากการโจมตีทางไซเบอร์จะสูงถึง 10.5 ล้านล้านเหรียญภายในปี 2568

“เครือเจริญโภคภัณฑ์และกลุ่มบริษัทในเครือฯ ในฐานะของผู้นำธุรกิจภาคเอกชน จึงมีความยินดีเป็นอย่างยิ่งในการร่วมมือกับสำนักงานตำรวจแห่งชาติ นำร่องด้านการสื่อสารประชาสัมพันธ์สร้างการรับรู้เกี่ยวกับกลโกงต่างๆ ของอาชญากรรมไซเบอร์เป็นองค์กรแรก เพื่อสร้างภูมิคุ้มกันไซเบอร์วัคซีนให้ประชาชนชาวไทยมีความรู้เท่าทันอาชญากรรมทางเทคโนโลยีในรูปแบบต่างๆ

“ความร่วมมือการประชาสัมพันธ์สื่อครั้งนี้เป็น ‘หมุดหมายสำคัญ’ ของความร่วมมือระหว่างรัฐกับเอกชนในการร่วมสร้าง ‘สังคมตื่นรู้’ ผ่านการกระตุ้นด้วย ‘ไซเบอร์วัคซีน’ สร้างภูมิคุ้มกันแก่ประชาชนไม่ให้ตกเป็นเหยื่อจากภัยบนโลกออนไลน์ ซึ่งการร่วมสร้างความตื่นรู้ให้สังคมไทยในครั้งนี้สอดคล้องกับค่านิยม 3 ประโยชน์ ที่เครือฯ ยึดมั่นในการตอบแทนบุญคุณแผ่นดิน สร้างประโยชน์ต่อประเทศชาติและประชาชนเป็นสำคัญ”

สำหรับการร่วมประชาสัมพันธ์ในครั้งนี้ ทางเครือฯ ได้ระดมสรรพกำลังของกลุ่มธุรกิจในเครือ ได้แก่ บริษัท เครือเจริญโภคภัณฑ์ จำกัด บริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน) บริษัท ซีพี ออลล์ จำกัด (มหาชน) บริษัท สยามแม็คโคร จำกัด (มหาชน) รวมถึง ธุรกิจโลตัส ประเทศไทย เพื่อร่วมประชาสัมพันธ์กลโกงของอาชญากรรมไซเบอร์ในทุกช่องทางการสื่อสารอย่างเต็มศักยภาพ รวมระยะเวลา 2 ปี ทั้งจากกลุ่มโทรคมนาคมและร้านค้าปลีกค้าส่ง คือการส่ง SMS เตือนภัยผ่านเครือข่ายทรูมูฟ เอช ซึ่งมีผู้ใช้บริการรวม 37 ล้านเลขหมาย ซึ่งได้เริ่มดำเนินการตั้งแต่ ม.ค. 2566 รวมถึงมีการเผยแพร่ข่าวสารผ่านสื่อภายในลักษณะต่างๆ ในร้านเซเว่นอีเลฟเว่นกว่า 13,000 สาขาทั่วประเทศ ซึ่งมีจำนวนลูกค้าเข้าใช้บริการ 11,404,314 คนต่อวัน ในแม็คโคร 152 สาขา และโลตัสมากกว่า 2,000 สาขา การประชาสัมพันธ์รายการในสถานีข่าว TNN16 และช่อง True4U รวมถึงการกระจายข่าวสารผ่านพนักงานกว่า 361,570 คน ทั่วประเทศ ซึ่งความหลากหลายทางธุรกิจฯ ของเครือ จะเป็นส่วนสำคัญที่ทำให้ข่าวสารเข้าถึงประชาชนทุกกลุ่มเป้าหมายอย่างทั่วถึง และทำให้ประชาชนรู้เท่าทันกลโกงรูปแบบต่างๆ ของมิจฉาชีพได้อย่างรวดเร็ว เพื่อลดความสูญเสียทั้งต่อประชาชนและประเทศชาติที่อาจเกิดขึ้นต่อไป

“หวังเป็นอย่างยิ่งว่า ความร่วมมือในครั้งนี้จะเป็นส่วนหนึ่งในการสื่อสารเพื่อสร้างภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยีให้แก่ประชาชนทั่วประเทศ” ประธานคณะผู้บริหารเครือซีพีกล่าวปิดท้ายด้วยความหวังอย่างเต็มเปี่ยม

แม็คโครเดินหน้าให้ความรู้ลูกค้าต้านภัยออนไลน์

● ด้วยเล็งเห็นความสำคัญของการต้องรู้เท่าทันภัยคุกคามไซเบอร์ ทางบริษัท สยามแม็คโคร จำกัด (มหาชน) บริษัทในเครือซีพี จึงเร่งต่อยอดโครงการไซเบอร์วัคซีนดำเนินกิจกรรมนำร่องร่วมรณรงค์ให้ลูกค้าประชาชนรู้เท่าทันกลโกงและให้ความรู้ด้านภัยไซเบอร์ตลอดห่วงโซ่การดำเนินธุรกิจในทุกช่องทาง ทั้ง 154 สาขาทั่วประเทศ รวมถึงในงานตลาดนัดโชห่วย 13 ที่อิมแพ็ค เมืองทองธานี ซึ่งเป็นกิจกรรมใหญ่ประจำปี อีกทั้งยังมีการเผยแพร่ข่าวสารผ่านช่องทางออนไลน์ ไม่ว่าจะเป็นเฟซบุ๊ก ไลน์ และติ๊กต็อก ของแม็คโครตลอดทั้งปี เพื่อสร้างการรับรู้ในวงกว้าง เป็นเกราะป้องกันที่แข็งแกร่งให้ประชาชนปลอดจากภัยไซเบอร์ นอกจากนี้ยังได้จัดอบรมพนักงานแม็คโครกว่า 20,000 คน ทั่วประเทศ ทั้งที่สำนักงานใหญ่และสาขา เพื่อเสริมสร้างความเข้าใจที่ถูกต้องเกี่ยวกับภัยคุกคามไซเบอร์ และสามารถให้ข้อมูลจากสำนักงานตำรวจแห่งชาติกับลูกค้าของแม็คโครได้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ในโลกออนไลน์ทุกรูปแบบ

ที่มา : www.siammakro.co.th

PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล นักท่องไซเบอร์ต้องรู้

ดร.สุนทรีย์ ส่งเสริม
ผู้เชี่ยวชาญด้าน PDPA

ภาพจาก : สคส.

● ตัวแทนจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีสถานะเป็นองค์การมหาชนตามพระราชบัญญัติเฉพาะ เป็นหน่วยงานที่แยกออกมาโดยอยู่ภายใต้สังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รับหน้าที่ถ่ายทอดมุมมองเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ที่นักท่องไซเบอร์ต้องรู้โดยเปิดเผยว่า ในยุคไซเบอร์ส่งผลให้การติดต่อดำเนินการทางธุรกรรมต่างๆ สามารถทำได้ง่ายและรวดเร็วมากยิ่งขึ้น หากแต่ความสะดวกดังกล่าวก็สามารถนำมาซึ่งภัยคุกคามไซเบอร์ทางด้านข้อมูลส่วนบุคคลของประชาชนมากขึ้นตามไปด้วย ซึ่งมักเกิดขึ้นในลักษณะของเหตุข้อมูลรั่วไหลและถูกนำไปขาย ส่งผลให้มิจฉาชีพหรือผู้ไม่หวังดีนำข้อมูลส่วนบุคคลดังกล่าวมาใช้ติดต่อมายังเจ้าของข้อมูลส่วนบุคคล ก่อให้เกิดความเดือดร้อนรำคาญ รวมถึงนำไปสู่การหลอกลวงให้เกิดความเสียหายได้ อย่างไรก็ตาม นับตั้งแต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้โดยสมบูรณ์ ทำให้องค์กรหรือหน่วยงานต่างๆ รวมถึงประชาชนมีความตระหนักถึงสิทธิส่วนบุคคลมากขึ้น

“กฎหมายคุ้มครองข้อมูลส่วนบุคคลทำให้องค์กรต้องมีความระมัดระวังไม่ให้เกิดเหตุการละเมิดข้อมูลส่วนบุคคลขึ้น เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ว่าเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล หน่วยงานหรือองค์กรมีหน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลมายังสำนักงานฯ หรือหากหน่วยงานหรือองค์กรพิจารณาแล้วปรากฏว่าเป็นเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล หน่วยงานหรือองค์กรมีหน้าที่ต้องแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคล (ประชาชน) ทราบด้วย ดังนั้นหน่วยงานหรือองค์กรต่างๆ ต้องเพิ่มความตระหนัก และจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้ประชาชนได้รับความปลอดภัยในการใช้เทคโนโลยีมากขึ้น

“ขณะเดียวกันผู้ใช้โซเชียลมีเดียควรมีความระมัดระวังในการเผยแพร่ข้อมูลของตนเองที่ติดข้อมูลส่วนบุคคลของผู้อื่นด้วย เช่น กรณีบริษัทมีการลงเลขพัสดุผ่านช่องทางออนไลน์เพื่อให้ลูกค้าสามารถเข้ามาเช็กเลขพัสดุของตนเอง แต่ได้ลงเลขพัสดุที่มีข้อมูลการสั่งซื้อสินค้าของลูกค้าท่านอื่นด้วย หรือกรณีผู้ใช้โซเชียลมีเดียโพสต์ผลสอบของตนเองผ่านทางช่องทางออนไลน์ส่วนตัวแต่ติดข้อมูลส่วนบุคคลของคนอื่นไปด้วย

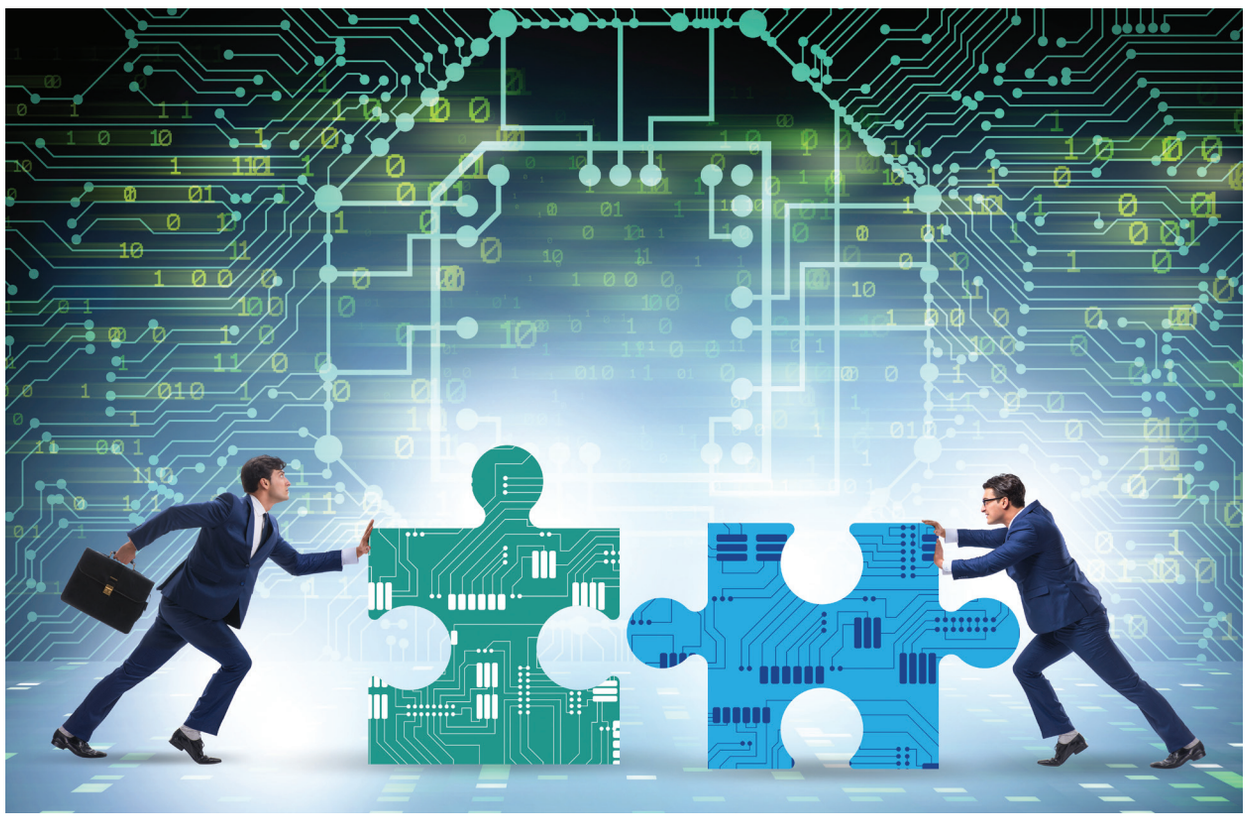
“หากพบว่ามีการเปิดเผยข้อมูลส่วนบุคคลของตนเองบนโลกโซเชียลมีเดีย เจ้าของข้อมูลส่วนบุคคลควรติดต่อไปยังต้นทางหรือบริษัทที่มีการเปิดเผยข้อมูลส่วนบุคคลโดยตรงก่อน เพื่อให้บริษัทดำเนินการนำข้อมูลดังกล่าวออกจากโซเชียลมีเดีย หากบริษัทไม่ดำเนินการตามคำขอก็ควรแจ้งให้ทราบไปเลยว่าต้องดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ทั้งนี้ทั้งนั้นสิ่งที่ผู้ใช้โซเชียลมีเดียจะต้องรู้เพิ่มเติมคือ ต้องไม่เผยแพร่ข้อมูลส่วนบุคคลของตนเองบนสื่อโซเชียลมีเดีย เช่น นำข้อมูลพาสปอร์ตและตั๋วเครื่องบินไปโพสต์ เนื่องจากบนตั๋วมีข้อมูลสำคัญที่ทำให้สามารถสืบหาข้อมูลส่วนตัวได้ โดยเฉพาะส่วนที่มีบาร์โค้ดจะสามารถถอดรหัสออกมาเป็นชื่อ นามสกุล รายละเอียดเที่ยวบิน ที่นั่ง เลขที่ไฟลต์บิน

“ทั้งนี้ทั้งนั้นการที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ ถือเป็นส่วนสำคัญในการผลักดันให้หน่วยงานหรือองค์กร ซึ่งเป็นผู้ควบคุมหรือประมวลผลข้อมูลส่วนบุคคลต่างๆ ต้องยกระดับมาตรการรักษาความมั่นคงปลอดภัย (Security) ของหน่วยงานหรือองค์กรนั้นๆ อันจะส่งผลให้ปริมาณภัยคุกคามทางไซเบอร์ลดน้อยลงได้ในที่สุด”

แสดงความคิดเห็นคอลัมน์นี้

เรื่อง : ชนานันทน์

‘Digital Literacy Skill’ ทักษะที่ต้องมีในยุคดิจิทัล



ในโลกที่ขับเคลื่อนด้วยเทคโนโลยีดิจิทัล ตั้งแต่วันที่เราตื่นเต้นกับการท่องอินเทอร์เน็ตครั้งแรก มาจนถึงยุคเมตาเวิร์ส (Metaverse) ที่ผู้คนติดต่อและทำธุรกรรมกันได้ในโลกเสมือน ทำอย่างไรเราจึงจะเป็นผู้ใช้เทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพ สามารถนำไปพัฒนาเพิ่มเติมเพื่อใช้ชีวิตเชื่อมโยงกับโลกดิจิทัลได้อย่างราบรื่น ก้าวทันโลกที่กำลังเปลี่ยนแปลง ทั้งยังต้องรู้เท่าทัน สามารถใช้ได้อย่างปลอดภัยจากภัยไซเบอร์ที่นับวันยิ่งเพิ่มมากขึ้นทั้งรูปแบบและความรุนแรง

เป็นเหตุผลให้เราทุกคนต้องมี ‘Digital Literacy Skill’ หรือทักษะดิจิทัล เพื่อยกระดับตนเองเป็นพลเมืองดิจิทัล (Digital Citizenship) การเป็นพลเมืองผู้ฉลาดในโลกออนไลน์

Digital Literacy Skill ทักษะจำเป็นในการใช้ชีวิตยุคใหม่

ปัจจุบัน ‘Digital Literacy Skill’ หรือทักษะดิจิทัล เป็นหนึ่งทักษะจำเป็นในการใช้ชีวิต ซึ่ง World Economic Forum เปรียบให้เป็นกล่องเครื่องมือแห่งศตวรรษที่ 21 ที่จะช่วยให้เราสามารถสำรวจโลกดิจิทัลของเราได้อย่างง่ายดายและมั่นใจในการเชื่อมต่อ เรียนรู้ และเติบโตในสภาพแวดล้อมที่ต้องตามให้ทัน นอกจากนี้ Development Employability ยังได้กล่าวว่าการมีความรู้ดิจิทัล รวมถึงทักษะดิจิทัลจำเป็นต่อการเติบโตและความสำเร็จในหน้าที่การงาน เราจึงควรสำรวจและพัฒนาตนเองให้มีทักษะดิจิทัลใหม่ๆ อยู่เสมอ จึงเป็นหน้าที่ของทุกคนที่ควรเรียนรู้ ขณะเดียวกันภาครัฐเองมีส่วนสำคัญในการสร้างความตระหนักและสนับสนุนให้ประชาชนมีทักษะดิจิทัล อย่างน้อยคือทักษะพื้นฐานที่จำเป็น

ข้อมูลจากบทความเกี่ยวกับทักษะดิจิทัลจาก World Economic Forum ระบุว่า ในปี 2021 ผู้คนกว่าครึ่งในสหภาพยุโรปมีทักษะดิจิทัลขั้นพื้นฐาน ขณะที่เนเธอร์แลนด์ ฟินแลนด์ และไอร์แลนด์ ทำคะแนนสูงสุด ตามรายงานของสำนักงานสถิติยุโรป (Eurostat) ขณะที่โรมาเนีย บัลแกเรีย และโปแลนด์ อยู่ในกลุ่มที่มีคะแนนน้อยที่สุด มีแนวโน้มที่จะสนับสนุนให้มีทักษะดิจิทัลมากขึ้น

สำหรับตัวอย่างของทักษะดิจิทัลที่มีความสำคัญต่อโลกการทำงาน Amazon Web Services บริษัทในเครือของแอมะซอนที่ให้บริการแพลตฟอร์มคลาวด์คอมพิวติง และ Gallup บริษัทที่ปรึกษาด้านสถานที่ทำงานที่ได้ศึกษาเกี่ยวกับทักษะด้านดิจิทัลในเอเชียแปซิฟิกล่าสุด เผยแพร่ต้นปี 2023 ได้นำเสนอข้อมูลว่า จากปัจจัยพื้นฐานเดียวกัน พนักงานในเอเชียแปซิฟิกที่มีทักษะดิจิทัลขั้นสูงอาจมีรายได้มากกว่าผู้ที่ไม่ได้ใช้ทักษะดิจิทัลในที่ทำงานถึง 65%

ในสิงคโปร์ พนักงานที่ใช้ทักษะดิจิทัลในระดับใดก็ตามจะได้รับค่าจ้างที่สูงขึ้น 97% และในหัวข้อสำรวจเดียวกัน อินโดนีเซียมีตัวเลขอยู่ที่ 93% ขณะที่ไทย ผลสำรวจระบุว่าผู้ที่มีทักษะดิจิทัลขั้นสูงจะมีรายได้มากกว่า 57% ตัวเลขเหล่านี้ยิ่งทำให้ตระหนักถึงความจำเป็นของทักษะดิจิทัลที่มีผลต่อโอกาสในการทำงาน

ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล 9 ด้าน สู่การเป็นประเทศไทย 4.0

ในการปรับตัวให้ก้าวทันโลกดิจิทัล ทางภาครัฐได้แบ่งทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลออกเป็น 9 ด้าน เพื่อก้าวไปสู่การเป็นประเทศไทย 4.0 และเพื่อให้บุคลากรสามารถพัฒนาตนเองสู่สังคมยุคใหม่ ประกอบด้วย 1. การใช้งานคอมพิวเตอร์ 2. การใช้งานอินเทอร์เน็ต 3. การใช้งานเพื่อความปลอดภัย 4. การใช้โปรแกรมประมวลผลคำ 5. การใช้โปรแกรมตารางคำนวณ 6. การใช้โปรแกรมนำเสนอ 7. การทำงานร่วมกันแบบออนไลน์ 8. การใช้โปรแกรมสร้างสื่อดิจิทัล 9. การใช้ดิจิทัลเพื่อความมั่นคงปลอดภัย

โดยครอบคลุมความสามารถ 4 มิติ คือ 1. การใช้ (Use) 2. ความเข้าใจ (Understand) 3. การสร้าง (Create) 4. การเข้าถึง (Access) เทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพ นำไปสู่การทำงานในลักษณะ ‘ทำน้อยได้มาก’ (Work less but get more impact) ‘สร้างคุณค่า’ (Value Co-Creation) และ ‘คุ้มค่าในการดำเนินงาน’ (Economy of Scale)

ที่มา : สำนักงานคณะกรรมการข้าราชการพลเรือน (กพ.)

ที่มา : https://www.ocsc.go.th/DLProject/mean-dlp - What is Digital Literacy https://www.westernsydney.edu.au/studysmart/home/study_skills_guides/digital_literacy/what_is_digital_literacy - 4 Key Elements of Successful Digital Literacy in the Workplace https://builtin.com/company-culture/digital-literacy-business https://www.dga.or.th/document-sharing/infographic/36321/Digital Literacy https://th.jobsdb.com/th-th/articles/digital-literacy/ https://web.facebook.com/AntiFakeNewsCenter/photos/a.113638500070332/ 581833403250837/ https://ict.moph.go.th/th/extension/606 https://www.okmd.or.th/okmd-kratooktomkit/4673/ https://www.scimath.org/article-technology/item/10611-digital-intelligence https://www.weforum.org/agenda/2022/04/europe-basic-digital-skills/ https://positioningmag.com/1420493

แสดงความคิดเห็นคอลัมน์นี้

เปิด 5 ทักษะรับมือกับภัยดิจิทัล

ทักษะดิจิทัลไม่ใช่แค่เรื่องของแผนกไอทีอีกต่อไป นับตั้งแต่เรามีสมาร์ตโฟนที่เชื่อมต่อกับอินเทอร์เน็ตได้ และนับตั้งแต่รู้ตัวว่าต้องเข้าสู่สนามแข่ง ทั้งกับคนทำงานด้วยกันและปัญญาประดิษฐ์ (Artificial Intelligence) ที่หลายคนมองว่าอาจกำลังวางแผนแย่งเราทำงานอยู่ในเวลานี้ เราจึงจำเป็นต้องมีทักษะด้านดิจิทัลรอบด้านผสานคู่กับการพัฒนาของเทคโนโลยี และพร้อมรับมือกับภัยดิจิทัลใกล้ตัว

1. ทักษะการใช้เครื่องมือ : หมายถึงทั้งอุปกรณ์ โปรแกรม และระบบ หากเราทำงานแบบทีมเวิร์กจากที่ไหนก็ได้ อย่าง Buffer บริษัทการตลาดที่มีพาร์ตเนอร์ในหลายประเทศ พนักงานทุกสาขาสามารถเรียนรู้วิธีทำงานได้จากโปรแกรมเทรนนิ่ง เพื่อให้ทุกคนเข้าใจและพูดคุยภาษาเดียวกัน โดยโปรแกรมประชุมอย่าง ‘Microsoft Teams’ ‘Google Meet’ หรือ ‘Zoom’ นับเป็นเครื่องมือประเภทหนึ่ง

2. ทักษะการใช้โซเชียลมีเดียให้เกิดประโยชน์ : ทักษะนี้ช่วยสร้างโอกาสได้ เช่น โอกาสทางการตลาดที่จะช่วยสร้างรายได้จากการเป็นนักขายออนไลน์ หรือนักสร้างคอนเทนต์ ขณะเดียวกันธุรกิจต่างๆ ต้องมีบัญชีโซเชียลมีเดียทางการ (Official Account) ของตัวเองไว้เพื่อทำการตลาด ให้บริการหลังการขาย และประชาสัมพันธ์ ทั้งยังเป็นช่องทางสนับสนุนสินค้าทางวัฒนธรรม (Soft Power) ไปสู่ระดับสากล

3. ทักษะด้านมารยาทในสังคมดิจิทัล : ผู้ท่องโลกไซเบอร์จำเป็นต้องมีมารยาทดิจิทัล (Digital Etiquette) เพื่อป้องกันไม่ให้ตนเองกลายเป็น ‘เกรียนคีย์บอร์ด’ สร้างความเดือดร้อนให้ผู้อื่น ละเมิดสิทธิไปจนถึงสร้างบาดแผลทางใจ (Cyberbullying) ให้แก่ผู้ที่ใช้พื้นที่เดียวกัน ยิ่งหากเป็นระดับธุรกิจ ยิ่งสำคัญอย่างมาก เพราะอาจนำไปสู่การฟ้องร้องมูลค่ามหาศาล และสร้างความเสียหายด้านภาพลักษณ์ให้แบรนด์

4. ทักษะป้องกันภัยทางไซเบอร์ : เราต้องตระหนักถึงทักษะการใช้เทคโนโลยีให้ปลอดภัยมากขึ้น จำเป็นต้องมีความรู้เบื้องต้นเพื่อป้องกันข้อมูลตนเอง เช่น พิจารณาความจำเป็นก่อนให้ข้อมูล หมั่นอัพเดตระบบความปลอดภัย ใช้ระบบยืนยันตัวตนที่มีความน่าเชื่อถือสูง ไม่คลิกลิงก์หรือสิ่งที่แนบมากับอีเมลประเภทสแปม หากสงสัยว่าข้อมูลส่วนตัวถูกนำไปใช้ให้แจ้งเจ้าหน้าที่ทันที

5. ทักษะด้านกฎหมายในโลกดิจิทัล : พลเมืองดิจิทัลควรรู้ พ.ร.บ. คอมพิวเตอร์ เพื่อให้ทราบว่าประเด็นใดได้รับการคุ้มครองและรู้ไว้ก่อนเผลอกระทำผิด ไปจนถึงติดตามข่าวสารด้านกฎหมายล่าสุด โดยเฉพาะ PDPA พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีผลบังคับใช้ทั้งฉบับวันที่ 1 มิถุนายน พ.ศ. 2565 ที่หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตาม มีโทษทั้งทางแพ่ง โทษทางอาญา และโทษทางปกครอง

นอกจากนี้อีกหนึ่งทักษะสำคัญที่เราต้องมีคือ ‘การเปิดรับและอัพเดตความรู้’ เปรียบได้กับแอปพลิเคชันที่พร้อมอัพเดตเวอร์ชันใหม่ได้ตลอด เพื่อให้ทันกับที่ประเทศไทยและภูมิภาคเอเชียแปซิฟิกกำลังจะเปลี่ยนแปลงสู่การเป็นสังคมดิจิทัลที่เข้มข้นขึ้นอย่างรวดเร็วในอนาคตอันใกล้นี้ ควบคู่กับการมี ‘ทักษะการคิดวิเคราะห์อย่างมีวิจารณญาณ’ ที่ดี ที่จำเป็นอย่างยิ่งทั้งในโลกออฟไลน์และออนไลน์

● เรื่อง : ศศิธร ภาพ : เนาวรัตน์ บุญวิภาส

ทนายนิด้า - ศรันยา หวังสุขเจริญ

'รับคำขอโทษเป็นเงินสดเท่านั้น' ราคาที่ต้องจ่าย... ให้โลกไซเบอร์

● ในยุคที่โลกแห่งการสื่อสารทั้งใบย่อลงมาอยู่ในมือ ทุกคนพร้อมส่งข้อความแสดงความเห็น ชื่นชม ติเตียน เสียดสีใครก็ได้โดยไม่จำเป็นต้องรู้จักเป็นการส่วนตัว โซเชียลมีเดียจึงเป็นเหมือนดาบสองคมที่หากใช้ให้ดีก็เกิดประโยชน์มหาศาล แต่หากพลั้งเผลอใช้ในทางไม่ถูกไม่ควรก็ต้องพึงระวังผลลัพธ์ที่ตามมา เพราะใดๆ ในโลกไซเบอร์ล้วนมีราคาที่ต้องจ่าย บัวบานฉบับนี้ชวนสะท้อนมุมคิดที่ต้องใช้สติให้มากเวลาท่องโลกโซเชียล ผ่านมุมมองของทนายความคนดัง นิด้า - ศรันยา หวังสุขเจริญ ผู้มีประสบการณ์รับทำคดีฟ้องร้องเกี่ยวกับ Cyberbullying มามากมาย เป็นคนดังที่คนในสังคมรู้จักดีก็หลายเคส เรียกได้ว่ามีส่วนร่วมสร้างมาตรฐานใหม่ให้โลกโซเชียล 'รับคำขอโทษเป็นเงินสดเท่านั้น'

หมิ่นประมาท คดีไซเบอร์รับฟ้องยอดฮิต

ทนายนิด้าเปิดเผยว่า คดีเกี่ยวข้องกับโลกไซเบอร์ที่รับฟ้องส่วนใหญ่มักหนีไม่พ้นคดีว่าด้วยเรื่องหมิ่นประมาทโดยการโฆษณา "สมัยก่อนถ้าการหมิ่นประมาทนั้นกระทำโดยแพร่หลายให้บุคคลอื่นสามารถรับรู้ได้ เช่น โฆษณาหนังสือพิมพ์ หรือใส่ความใครผ่านสื่อวิทยุ ก็จะเป็นเรื่องของการหมิ่นประมาทโดยการโฆษณา มีใช้มาตั้งนานแล้วในประมวลกฎหมายในการกระทำความผิดฐานหมิ่นประมาทฐานใส่ความคนบนสื่อโซเชียลพอเทียบเคียงแล้วองค์ประกอบความผิดลงล็อกเดียวกันกับการด่าทอใครสักคนให้บุคคลที่สามฟังแบบในยุคที่ไม่มีโซเชียล ถือเป็นการหมิ่นประมาทโดยการโฆษณา จึงใช้กฎหมายข้อนี้ในการพิจารณา

"สุดท้ายแล้วอยู่ที่ดุลพินิจของศาล ซึ่งในยุคนี้ก็มีศัพท์ใหม่ศัพท์สแลงต่างๆ เกิดขึ้นที่ยังไม่เคยมีปรากฏในคำพิพากษาฎีกา เช่นคำว่า สตรอว์เบอร์รี หากทนายสามารถนำสืบได้ว่าคำนี้เป็นคำที่เกิดขึ้นใหม่ เป็นศัพท์สแลงที่คนอ่านแล้วเข้าใจได้ว่ามันคือคำด่า ศาลเห็นด้วย เชื่อได้ว่าเป็นการหมิ่น ศาลก็จะพิพากษาลงโทษ หรือถ้าไม่ ศาลก็จะยกฟ้อง ดังนั้นเมื่อนำคดีฟ้องร้องขึ้นสู่ศาลแล้ว ผลที่ออกมาจึงมีทั้งแพ้และชนะ"

'รับคำขอโทษเป็นเงินสดเท่านั้น' สร้างกระแสผลักดันการใช้โซเชียลอย่างมีสติ

ในการรับว่าความคดีที่เกิดขึ้นในสังคมไซเบอร์ให้บุคคลมีชื่อเสียงในวงการบันเทิง ทนายนิด้าชี้แจงว่าอันที่จริงถือเป็นส่วนน้อยเมื่อเทียบกับคดีอื่นๆ ที่ทางทีมทนายนิด้ารับว่าความให้ เพียงแต่ด้วยความเป็นคนดังจึงทำให้สื่อสนใจติดตาม ส่งผลให้คนในวงกว้างได้รับรู้

"คนดังบางคนที่ต้องการฟ้องร้องคดีหมิ่นประมาทในโลกโซเชียล เพราะมีเป้าประสงค์ 2 อย่าง หนึ่งคือต้องการแก้ไขชื่อเสียงของตัวเองที่คนกำลังเข้าใจเขาผิดให้กลับมาเข้าใจอย่างถูกต้อง เพราะการมีชื่อเสียงเวลาที่เขาถูกด่า เสียงมันก็ดังไปด้วย สองต้องการให้สังคมรับรู้ว่าการกระทำแบบนี้เป็นความผิด และกฎหมายสามารถลงโทษได้ เหมือนยิงกระสุนนัดเดียวได้นกสองตัว ซึ่งส่วนตัวก็เห็นด้วยนะคะ เพราะในปัจจุบันทุกคนใช้สื่อโซเชียลในการทำลายคนอื่น ในการต่อว่าใส่ความคนอื่นอย่างสนุกสนาน แล้วไม่ใช่ว่าทุกคนจะถูกดำเนินคดี ดังนั้นการที่เราได้เป็นทนายความว่าความให้คนดังที่มายื่นฟ้องคดีประเภทนี้ เราเห็นตรงกันว่าต้องการให้สังคมเห็นว่าการกระทำของคุณแบบนี้ไม่ได้แปลว่าจะไม่ได้รับผลกระทบอะไรเลย

"และคนที่จะได้เรียนรู้ก็คือตัวจำเลยหรือผู้ถูกฟ้องว่าการกระทำอย่างนี้ที่พิมพ์อะไรลงไปง่ายๆ ด้วยความรู้สึกแค่สนุก แต่ผลที่ตามมาทั้งเสียเวลา เสียค่าใช้จ่าย ค่าทนายความ ค่าเดินทาง ที่สำคัญมากคือเสียสุขภาพจิต เพราะต่อให้สุดท้ายศาลอาจไม่พิพากษาลงโทษ แต่ระหว่างทางก็ต้องเป็นทุกข์แน่นอน แล้วกระบวนการเรียนรู้จะเกิดขึ้นกับฝ่ายของจำเลยว่าถ้าย้อนเวลากลับไปได้ก็ไม่น่าจะทำแบบนั้น ต่อไปเขาก็คงจะไม่ทำอีก"

สำหรับคนที่ท่องโลกโซเชียลเป็นประจำและติดตามข่าวสารในวงการบันเทิงอยู่บ้างย่อมเคยได้ยินคำกล่าวติดปากที่กลายเป็นไวรัลในโลกไซเบอร์มาจนถึงวันนี้ 'รับคำขอโทษเป็นเงินสดเท่านั้น' นัยหนึ่งถือเป็นการเตือนสติคนที่กำลังจะแสดงความเห็นเชิงลบอย่างได้ผลไม่น้อย

"ที่จริงข้อความนี้ในแง่ดีมันก็เป็นการป้องปรามคนได้ ทำให้คนได้เข้าใจและตระหนักว่า การด่าทอใครสักคน หรือพิมพ์ข้อความให้ใครได้รับความเสียหาย มันมีราคาที่ต้องจ่ายมากกว่าแค่คำว่าขอโทษ

เป็นค่าเสียหายในการเยียวยาต่อชื่อเสียงของบุคคลนั้นด้วย ทำให้คนที่คิดจะพิมพ์อะไรแล้วไปกระทบคนอื่นได้ฉุกคิดมากขึ้น

“ที่สำคัญราคาที่ต้องจ่าย ไม่ใช่แค่เรื่องเม็ดเงินเท่านั้น เพราะการหมิ่นประมาทโดยการโฆษณายังมีโทษในทางอาญาอีกด้วย อีกทั้งคนที่ตกเป็นจำเลยในคดีนี้ต้องมาศาล บางคนไม่ได้ร่ำรวย ทำงานกินเงินเดือน ต้องลางานมา ขาดรายได้ ต้องเสียเงินจ้างทนายความ เสียค่าเดินทาง ที่สำคัญมองว่าราคาที่เสียมากที่สุด คือเสียสุขภาพจิต เกิดความทุกข์ขึ้นในจิตใจ มันไม่คุ้มที่จะจ่าย ดังนั้นถ้าเราตระหนักถึงเรื่องนี้ทุกขณะเวลาที่ใช้สื่อโซเชียลก็จะสามารถใช้ป้องปราม ยับยั้งตัวเองให้มีสติมากขึ้น

“อีกประการหนึ่งคนอาจจะมองว่า แค่ด่ากัน ไม่ได้ทำให้ใครตาย แต่ถ้าเราไม่พยายามเบรกตัวเอง ใช้สื่อโซเชียลโดยไม่มีสติ ไม่มีจิตสำนึกที่ดี มันอาจจะทำให้ใครสักคนตายผ่อนส่งก็ได้นะคะ บางคนอาจถูกบูลลี ถูกกระทำซ้ำๆ โดยกฎหมายทำอะไรไม่ได้ ทำให้เขาต้องอยู่กับสิ่งนั้นจนเป็นโรคซึมเศร้า ไม่มีความสุขในชีวิต จนสุดท้ายเขาอาจไม่อยากอยู่บนโลกนี้”

หลอกลวง ฉ้อโกงในโลกไซเบอร์ ภัยคุกคามที่ต้องระวัง

ทนายนิด้าเปิดเผยว่า ภัยไซเบอร์ที่ได้รับการติดต่อขอความช่วยเหลือเพื่อฟ้องร้องดำเนินคดีในจำนวนที่มีมากไม่แพ้กันคือ คดีถูกหลอกลวงฉ้อโกงผ่านโลกออนไลน์ “ที่เขาบอกว่ารู้หน้าไม่รู้ใจ แต่ในโลกไซเบอร์นี่แม้แต่หน้าก็ไม่รู้นะคะ จึงยิ่งถูกหลอกได้ง่าย และต้องบอกตามตรงว่าบางคนมีจริตที่โลภด้วยอยู่แล้ว ยิ่งถูกชักจูงไปได้ง่าย ดังนั้นก็ต้องพยายามข่มจิตข่มใจตัวเองว่าของดี ของฟรี ของที่ได้มากกว่าที่ควรจะได้นั้นไม่มีจริง มันเป็นไปไม่ได้

“แต่มีเหมือนกันที่เราแค่เข้าไปซื้อของที่อยากจะได้ แต่เจอมิจฉาชีพหลอกโอนเงินแล้วไม่ได้รับของ ด้วยความที่ไม่ได้เห็นหน้าค่าตา รู้แต่เลขบัญชี การตรวจสอบจึงไม่ง่าย บางคนใช้การโกงเงินจำนวนน้อยๆ แต่คาดหวังคนจำนวนมากๆ ซึ่งเหยื่อก็ไม่อยากไปเสียเวลาดำเนินคดี มีคนเยอะมากที่ทักมาปรึกษานิด้าว่าถูกหลอกให้โอนเงิน 2,000-3,000 บาท ลองคิดดูว่าถ้าหลอกไปสักพันคนหมื่นคน อาชญากรก็ได้ไปเยอะมากแล้ว แต่สุดท้ายเวลาเราแนะนำให้เอาหลักฐานไปแจ้งความตำรวจ เขาจะไม่ทำ เพราะเงินหลักพันกับการต้องหยุดงาน ต้องเดินทางไปหาตำรวจ ต้องไปขึ้นศาล เขาก็ยอมเสียเงินไป พอเป็นแบบนี้อาชญากรก็ยิ่งทำผิด

“ในเรื่องของการซื้อขายออนไลน์ ต้องบอกเลยว่าไม่มีวิธีป้องกันถูกหลอก 100% ถ้าไม่เคยรู้จักหรือเคยซื้อขายกันมาก่อนอาจมีวิธีในการสกรีนได้แค่เบื้องต้นเท่านั้น เมื่อเขาส่งเลขบัญชีมา เราอาจขอตรวจสอบบัตรประชาชนว่าชื่อนามสกุลในบัตรตรงกันกับชื่อบัญชีธนาคารมั้ย ถ้าเขาไม่สะดวกใจที่จะส่งให้ ส่วนตัวนิด้าจะสันนิษฐานไว้ก่อนว่าเขาไม่บริสุทธิ์ใจ อาจเป็นมิจฉาชีพได้ ก็ต้องเลี่ยง ยอมที่จะไม่ซื้อสินค้ากับเขา

“อีกกรณีหนึ่งที่อาจเกิดขึ้นได้ก็คือการหลอกลวงทางสื่อโซเชียล โดยหลอกให้เกิดความรัก เพื่อไปกระทำความผิดทางอาชญากรรมอื่นๆ เช่น ล่วงละเมิดทางเพศ ข่มขืน อนาจาร เพราะสื่อโซเชียล ง่ายต่อการสร้างภาพลวง จนอาจจะเคลิ้มไปกับภาพที่เห็น ทำให้ถูกหลอกลวงได้ง่าย เป็นเรื่องที่มีให้เห็นได้ทุกวัน วันละหลายเวลา”

DO & DON’T กฎกติกามารยาทท่องโลกโซเชียล

“DO หรือกฎที่ควรทำคือการแชร์เผยแพร่เรื่องดีๆ ที่ให้ความรู้ เหมือนโลกอินเทอร์เน็ตในยุคแรกๆ ที่รวบย่อโลกเล็กลงมาให้เราเข้าไปหาข้อมูลความรู้ เป็นเหมือนห้องสมุดย่อมๆ ที่เข้าถึงได้ง่ายโดยไม่ต้องเดินทาง โซเชียลยุคตอนเริ่มๆ เป็นพื้นที่ของการให้ความรู้ ความบันเทิง มีแพลตฟอร์มต่างๆ ให้เราเข้าไปดูไลฟ์สไตล์ ชีวิตประจำวัน แต่วันหนึ่งมันกลับถูกปรับเปลี่ยนไปใช้ในการโจมตีคู่แข่ง ด่าทอคนที่ไม่ชอบ ซึ่งเป็นเรื่องไม่ควรทำและกฎหมายไม่อนุญาตให้ทำ

“ดังนั้นก่อนจะพิมพ์ข้อความอะไรลงไป ถ้าเรามั่นใจว่าข้อความนี้เกิดประโยชน์แน่นอน ไม่ได้ทำให้ใครได้รับความเสียหาย บางประเด็นเป็นประโยชน์ต่อสังคม ต่อสาธารณะ เราก็สามารถเข้าไปแลกเปลี่ยนกันได้ แต่ต้องทำแบบมีสติ ให้ตระหนักและทบทวนก่อนว่าสิ่งที่เราทำเกิดประโยชน์ในข้อไหน ถ้าทำแล้วเกิดข้อเสียมากกว่าข้อดีก็ไม่ใช่เรื่องที่ควรทำ

“Don’t สำหรับสิ่งที่ทำไม่ได้โดยเด็ดขาดก็คือการทำอะไรหรือพิมพ์ข้อความอะไรลงไปบนสื่อโซเชียล แล้วใครสักคนหนึ่งได้รับผลกระทบ ได้รับความเสียหาย ไม่ว่าจะต่อจิตใจ หรือทางใดทางหนึ่งก็ไม่ควรทำ และเดี๋ยวนี้คนไปโฟกัสที่ควรพิมพ์อย่างไรให้ข้อความนี้ไม่เสี่ยงถูกฟ้อง แต่ลืมเรื่องมารยาทไปแล้วด้วยซ้ำว่าจริงๆ แล้วจุดที่ควรพิจารณาตั้งแต่แรกเลยคือพิมพ์ข้อความอย่างไรที่ไม่เสียมารยาท และทำให้คนอื่นไม่พอใจหรือเสียใจ พวกข้อความตำหนิคนอื่นในเรื่องรูปร่าง หน้าตา วุฒิภาวะ ความรู้ การศึกษา โดยไม่ได้เป็นประโยชน์ต่อสังคม เป็นแค่ความพึงพอใจของคนพิมพ์เพียงคนเดียว คุณไม่จำเป็นต้องพิจารณาข้ามช็อตไปถึงกรณีว่ามันผิดกฎหมายหรือไม่ผิดกฎหมาย เพราะสารตั้งต้นของการทำผิดกฎหมายมันเริ่มมาจากคนไม่มีมารยาทก่อน การทำอะไรแบบไม่มีมารยาทบ่อยๆ ซ้ำๆ ทำให้เกิดความเคยชินจนนำไปสู่การใช้ข้อความที่มีความรุนแรงขึ้นจนกลายเป็นผิดกฎหมาย คนเราต้องมีศีลธรรมในใจก่อน นิด้าเชื่อว่าถ้าเรามีจิตใจที่ดีเป็นสารตั้งต้นก็จะส่งความดีต่อไปในความคิด”

โลกโซเชียลมีเดียแบบนี้ที่ฝันอยากเห็น

“อยากให้โลกออนไลน์เสมือนกับโลกออฟไลน์ คือเวลาที่เราเจอกันตัวเป็นๆ อยู่ต่อหน้า แทบจะไม่มีทางเลยที่เราจะไปพูดกับคนที่อยู่ต่อหน้าให้เขารู้สึกไม่ดีกับเรา เช่น ทำไมดำจัง อ้วนจัง ทำไมไม่ดูแลรูปร่างหน้าตาตัวเองเลย เราไม่ทำแน่ๆ เมื่ออยู่กันต่อหน้าอีกคน เริ่มมาจากการตระหนักในเรื่องการมีมารยาทเสมือนในโลกออฟไลน์ที่เราไม่กล้าทำ แล้วโลกออนไลน์จะสวยงามน่าอยู่”

สแกน QR Code เพื่อชมวิดีโอ

แสดงความคิดเห็นคอลัมน์นี้

เรื่อง : ชนานันทน์

องค์กรกับปัญหาด้านอาชญากรรมทางเทคโนโลยี วันนี้คุณพร้อมรับมือแล้วหรือยัง

ในยุคดิจิทัล ความสามารถในการดำเนินธุรกิจและความสามารถในการรับมือภัยไซเบอร์มีความจำเป็นและแยกจากกันไม่ได้ไปแล้ว เราจึงได้เห็นความพยายามของภาคธุรกิจในการพัฒนานโยบาย นวัตกรรม และการปฏิบัติจริงเพื่อสร้างความปลอดภัยให้แก่ข้อมูล ไม่ว่าจะเป็นข้อมูลการเงิน กลยุทธ์ในการแข่งขัน ไปจนถึงข้อมูลส่วนตัวของลูกค้าที่ละเอียดอ่อน อันจะนำไปสู่ความมั่นใจในการใช้บริการ

5 อันดับแรกภัยคุกคามทางไซเบอร์ที่ธุรกิจเผชิญในปัจจุบัน

ปัจจุบันเหล่าแฮกเกอร์ได้พัฒนาตัวเองให้มีทักษะโจมตีระบบที่ฉลาดและซับซ้อนขึ้นทุกขณะ ดังนั้นเราจึงต้องรู้เท่าทัน โดยเริ่มได้จากการศึกษาและทบทวนภัยไซเบอร์รูปแบบต่างๆ รวมถึง 5 อันดับแรกภัยคุกคามที่ธุรกิจกำลังเผชิญ ได้แก่

1. การโจมตีแบบฟิชชิง เป็นการโจมตีทางไซเบอร์ที่พบบ่อยที่สุด โดยแฮกเกอร์จะส่งอีเมลหรือข้อมูลมาจากผู้ส่งที่ดูเหมือนแหล่งจริง เช่น ธนาคาร หรือเว็บไซต์ เพื่อให้ผู้ใช้ป้อนข้อมูลส่วนบุคคล แล้วนำไปสู่การเข้าระบบบัญชีออนไลน์

2. การโจมตีโดยมัลแวร์ เป็นซอฟต์แวร์ที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ ซึ่งเมื่อมัลแวร์จู่โจม จะเท่ากับการเปิดทางแฮกเกอร์เข้าถึงข้อมูล และควบคุมคอมพิวเตอร์ของเหยื่อไว้ ทำให้ข้อมูลหายหรือเกิดการทำงานที่ผิดปกติ

3. การโจมตีด้วย SQL Injection เป็นการโจมตีโดยอาศัยช่องโหว่จากการกรอกข้อมูลผู้ใช้ด้วยการแอบดูคำสั่งหลักในระบบ ก่อนที่จะ ‘ฉีดยา’ หรือแอบต่อคำสั่งอื่นเข้าไปเพิ่ม เพื่อที่จะดึงข้อมูลหรือเปลี่ยนแปลงแก้ไขข้อมูล

4. การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service-DoS) โดยแฮกเกอร์จะส่งคำขอจำนวนมากไปยังเซิร์ฟเวอร์เพื่อให้ระบบทำงานหนัก ทำให้เว็บไซต์หรือเซิร์ฟเวอร์ล่ม และทำให้ผู้ใช้ไม่สามารถเข้าถึงข้อมูลที่ต้องการ

5. ภัยคุกคามจากวงใน (Insider Threats) เป็นภัยที่มาจากภายในองค์กร อาจเกิดจากพนักงาน ผู้รับเหมา หรือแม้แต่แทรกซึมโดยคู่ค้าทางธุรกิจ เป็นภัยที่ตรวจจับและป้องกันได้ยาก เพราะผู้โจมตีมีสิทธิ์เข้าถึงทรัพยากรอย่างถูกต้องตามกฎหมาย

สร้างกำแพงที่เข้มแข็งแก้ปัญหาภัยไซเบอร์

เมื่อทราบปัญหาภัยคุกคามทางไซเบอร์ที่ธุรกิจมักเผชิญในปัจจุบัน ขั้นตอนต่อไปคือการเตรียมพร้อมที่จะสร้างหรือซ่อมบำรุง ‘กำแพงป้องกันภัยไซเบอร์’ เพื่อขจัดทุกความเสี่ยง เสริมความปลอดภัย ได้แก่

• ทบทวนความเสี่ยงที่จะเกิดกับธุรกิจ เริ่มจากประเมินสถานการณ์เลวร้ายที่สุด (Worst-Case Scenario) ที่อาจเกิดขึ้นว่ามีอะไรบ้าง อย่างรอบด้านและครบถ้วนมากที่สุด จากนั้นเตรียมวางแผน และกำหนดให้มีผู้รับผิดชอบชัดเจน

• วางแผนโดยใช้กฎ 20 : 80 ทำแผนปฏิบัติการตามกฎ ‘ทำน้อยแต่ได้มาก’ เน้นการเรียงลำดับความสำคัญของสิ่งที่ต้องทำ 20% แรก ภายในเวลาจำกัด จดจ่อกับสิ่งที่สำคัญก่อนอย่างแท้จริง เพื่อป้องกันความเสียหายในภาพรวม

• จัดหาเทคโนโลยีที่มีประสิทธิภาพ จัดให้มีศูนย์ปฏิบัติการ CSOC (Cyber Security Operation Center) หรือศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ที่ควรมีเทคโนโลยีตรวจจับภัยคุกคามไซเบอร์ เช่น ระบบ Security Information Event Management (SIEM) ที่ช่วยเฝ้าระวัง ตรวจจับและแจ้งเตือนภัยคุกคาม เพื่อการรับมือที่รวดเร็ว

• เตรียมความพร้อมให้ทีมงาน องค์กรจำเป็นต้องเตรียมความรู้และความพร้อมเพื่อป้องกันภัยไซเบอร์ให้แก่บุคลากร ด้วยการจัดให้มีการฝึกอบรม สร้างความตระหนักถึงอันตรายของภัยคุกคามทางดิจิทัล ไปจนถึงอาจกำหนดให้เป็นหน้าที่ที่ทุกคนต้องไม่ประมาทและร่วมมือกัน

• รับมือด้วยหลัก Cybersecurity Incident Response Cycle หากเกิดการโจมตีขึ้น องค์กรต้องมั่นใจได้ว่าระบบป้องกันทั้งหมดจะต้องสามารถดำเนินการตาม ‘วงจรการตอบสนองเหตุการณ์ความปลอดภัยทางไซเบอร์’ หรือหลัก Cybersecurity Incident Response Cycle ได้ทันที อย่างถูกต้องตามขั้นตอน

1. Preparation – ขั้นตอนการเตรียมความพร้อมเพื่อรับมือเหตุการณ์

2. Detection & Analysis – ขั้นตอนการตรวจสอบและวิเคราะห์สถานการณ์

3. Containment Eradication – ขั้นตอนการจำกัดและกักกันความเสียหายที่อาจเกิดขึ้น

4. Recovery – ขั้นตอนการกู้คืนข้อมูลที่มีความสำคัญต่อองค์กร

องค์กรที่เตรียมความพร้อมภัยไซเบอร์รอบด้าน

นาทีนี้ทุกองค์กรธุรกิจต่างตระหนักถึงการป้องกันทางภัยไซเบอร์ เพื่อ

รักษาข้อมูลลูกค้า และลดความเสี่ยงจากความเสียหายด้านอื่นๆ ที่จะนำไปสู่การประกอบธุรกิจได้อย่างยั่งยืนในอนาคต

รวมถึง ‘IBM’ องค์กรธุรกิจระดับโลก ที่ปัจจุบันมุ่งเน้นการให้บริการเรื่องดิจิทัลโซลูชันแก่องค์กร และมีหนึ่งในจุดแข็ง คือ การวิจัยในระดับลึกและการพัฒนาระบบความปลอดภัยทางไซเบอร์ จนได้รับการจัดอันดับจากหลายสื่อว่าควรค่าแก่การถอดบทเรียน มาดูกันว่า ‘IBM’ ลดช่องโหว่ภัยคุกคามทางไซเบอร์ได้อย่างไร

• พัฒนาทักษะบุคลากรในทุกระดับ ตั้งแต่บุคลากรฝ่าย IT กฎหมาย การเงิน การตลาด และประชาสัมพันธ์ ไปจนถึง C-Levels หรือผู้บริหารระดับสูง ภายใต้การทำงานของหน่วยงาน ‘IBM X-Force Command Center’ ห้องปฏิบัติการเตรียมความพร้อมให้ทุกหน่วยงานสำคัญขององค์กร ไม่ว่าจะอยู่ในระดับงานใด

• มีแนวทางให้ทุกฝ่ายรับมือในทิศทางเดียวกัน โดยเมื่อเกิดการโจมตีขึ้น ทุกคนจะต้องสามารถรับมือไปในทิศทางเดียวกันได้ ได้แก่ 1. สร้างความร่วมมือระหว่างหน่วยงาน เปิด War Room เพื่อประเมินสถานการณ์ 2. สื่อสารอย่างเหมาะสมทันเหตุการณ์ เพื่อเลี่ยงการสื่อสารที่ผิดพลาดจากแหล่งข่าวอื่น ที่อาจผิดไปจากความเป็นจริง 3. จัดการปัญหาอย่างรวดเร็วที่สุด เพื่อป้องกันความเสียหายแบบทวีคูณ

นอกจากนี้ยังมีตัวอย่างของธุรกิจอื่นอย่าง ‘หัวเว่ย’ ที่จัดตั้งศูนย์ความโปร่งใสด้านความมั่นคงไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลระดับโลก (Global Cyber Security and Privacy Protection Transparency Center) ครอบคลุมการทำงาน 3 ด้าน ได้แก่ การจัดแสดงความมั่นคงปลอดภัยไซเบอร์ของหัวเว่ยแบบครบวงจร การอำนวยความสะดวกให้หน่วยงานที่ร่วมขับเคลื่อนนวัตกรรมด้านความปลอดภัยกับหัวเว่ย และการเปิดพื้นที่ให้ทดสอบและตรวจสอบความปลอดภัยของผลิตภัณฑ์และบริการ

ที่มา : https://www.pentestpeople.com/the-top-5-cyber-threats-facing-businesses-today/ https://www.quickserv.co.th/knowledge-base/solutions/1 https://www.adslthailand.com/post/14054 https://www.cyfence.com/article/cyber-threats-detect-with-cybersecurity-monitoring/ https://techsauce.co/news/ibm-security-report-cyber-attacks-in-2021 https://www.marketingoops.com/exclusive/insider-exclusive/cyberattack-ibm-x-force-command-center-boston/ https://www.avtechguide.com/tag/global-cyber-security-and-privacy-protection-transparency-center/

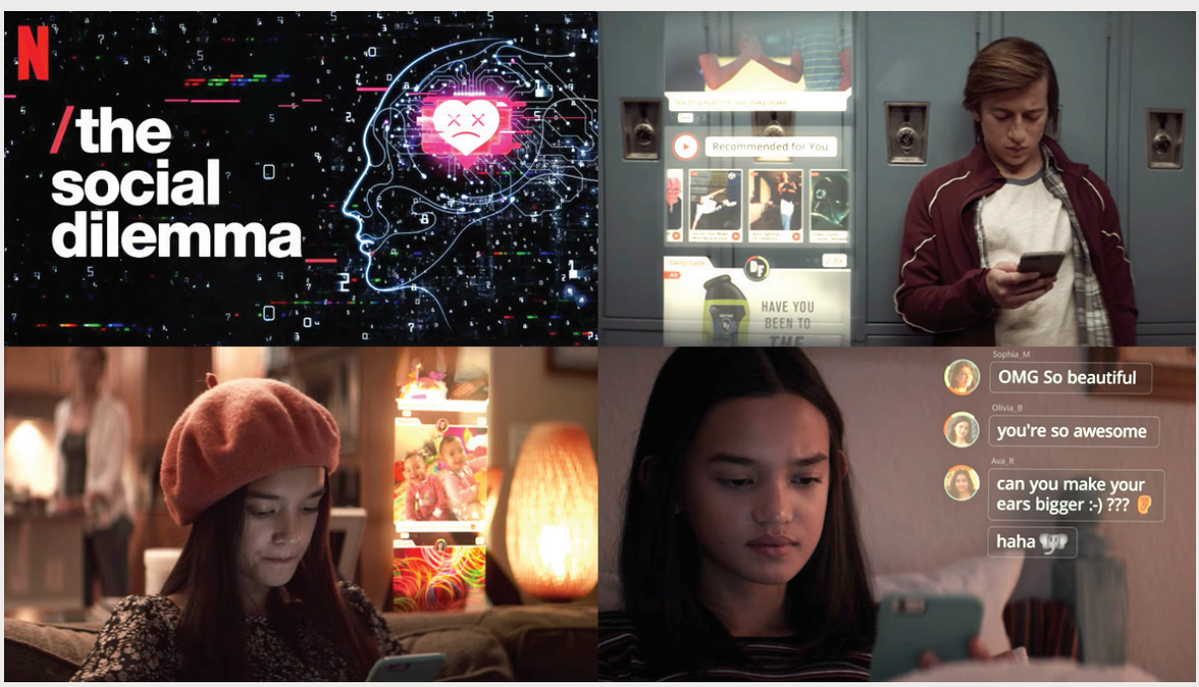
แสดงความคิดเห็นคอลัมน์นี้

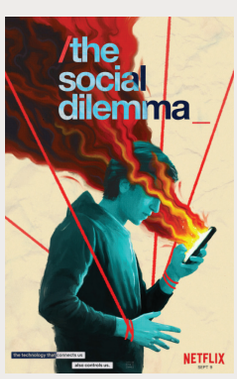
เรื่อง : Mr.Tea

บันเทิงต้านภัย (ไซเบอร์)

เมื่อโลกดิจิทัลถูกผนวกเข้าเป็นส่วนหนึ่งในชีวิตประจำวันของผู้คน ดังนั้นการตระหนักรู้ เข้าใจเรื่องของการรักษาความปลอดภัยในโลกไซเบอร์จึงเป็นอีกหนึ่งทักษะสำคัญ SD LIFE ฉบับนี้ขอชวนคุณมารู้เท่าทันผ่านความบันเทิง ความรู้ และแรงบันดาลใจ

DOCUMENTARY





The Social Dilemma

The Social Dilemma นับเป็นสารคดีที่กระตุกต่อมคิดและตั้งคำถามกับเราว่า ทุกๆ ครั้งที่เราเสิร์ชข้อมูลค้นหาใน google กดไลก์ภาพเพื่อนในเฟซบุ๊ก ข้อมูลที่อยู่ของเรา ไลฟ์สไตล์ และความสนใจของเราก็ถูกบันทึกเก็บข้อมูลไว้หมดแล้ว ‘ทั้งหมดไม่ใช่เรื่องบังเอิญ แต่คือการออกแบบอย่างตั้งใจ’ และกลไกการทำงานนั้นถูกออกแบบมาเพื่อให้ผู้ใช้งาน ‘เสพติด’ ทุกแพลตฟอร์มที่เราใช้ฟรีอยู่นั้น แท้จริงแล้วล้วนมีราคาที่ต้องจ่าย ดังประโยคที่ว่า “If you’re not paying for the product, then you are the product.” ถ้าคุณไม่ได้จ่ายเงินเพื่อซื้อสินค้า คุณนั่นแหละก็คือสินค้าเสียเอง

สารคดีเล่าถึงมุมมองของอดีตพนักงานในวงการเทคชื่อดัง เช่น อดีตวิศวกรของ Facebook (หนึ่งในทีมสร้างปุ่มกด Like) อดีตผู้บริหารของ Pinterest อดีตนักจริยธรรมการออกแบบ Google ทุกคนมีเป้าหมายของการทำอาชีพนี้เพื่อยกระดับชีวิตผู้คนให้ดีขึ้นด้วยเทคโนโลยี แต่แล้ววันหนึ่งเมื่อเทคโนโลยีเข้ามาเป็นส่วนหนึ่งของชีวิตผู้คนอย่างถอนตัวไม่ขึ้น พวกเขาจึงเลือกวางโทรศัพท์มือถือและมาบอกเล่าความจริงหลังม่านโลกไซเบอร์

ภาพยนตร์ใช้วิธีสัมภาษณ์บุคคลจริง ควบคู่ไปกับเรื่องราวของครอบครัวหนึ่ง (นักแสดง) เมื่อลูกติดโซเชียลจนเกิดปัญหาตามมา สะท้อนว่าเทคโนโลยีที่เราใช้นั้นถูกติดตั้งเครื่องมือละเมิดสิทธิความเป็นส่วนตัว เราจะหลงเชื่อไปกับเหล่าข่าวปลอม Fake News การเมือง ทัศนคติ ถ้าหลงเข้าไปในโลกนี้นานเท่าไร อาการป่วยวิตกกังวลและซึมเศร้าก็จะคืบคลานมาหา สารคดีเรื่องนี้ไม่ได้มุ่งต่อต้านการใช้เทคโนโลยี แต่เปรียบเหมือนการยกมือชูธงให้ผู้คนหันมาสนใจและปรับสมดุลการใช้เทคโนโลยีอย่างรู้จักมันให้ดีมากขึ้น รวมถึงอยากจะตะโกนบอกถึงรัฐบาล ในการออกกฎหมายควบคุมการทำงาน และเหล่าผู้สร้างในบริษัทเทคชื่อดังควรคำนึงถึงจริยธรรมในสังคม แต่สุดท้ายแล้วหน้าที่สำคัญคือครอบครัวในการปกป้องดูแลเยาวชนในบ้านให้เติบโตมาอย่างเท่าทันเทคโนโลยี

WEBSITE

RTP CYBER VACCINATED เว็บไซต์เตือนภัยออนไลน์

● ข้อความ ‘งานเสริมออนไลน์รายได้ดี คลิกเลย’ หรือจู่ๆ เอ๊ะ มีคนรู้จักมาทักขอยืมเงินทางไลน์ กลเม็ดหลอกลงทุนในรูปแบบต่างๆ สารพันกลโกงจากเหล่ามิจฉาชีพออนไลน์ รวบรวมให้รู้ทันโดยคณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ จัดทำเว็บไซต์ https://24hicarecenter.com/cybervaccinated ให้ประชาชนรับชมสื่อความรู้ป้องกันตนเอง ผ่านภาพโฆษณาสื่อสารง่าย เข้าถึงประชาชน พร้อมให้คำแนะนำในการป้องกัน เช่น ก่อนซื้อสินค้า คุณสามารถตรวจสอบชื่อเพจหรือบัญชีที่ขายสินค้าผ่านทางเว็บ https://www.black-listseller.com/ ด้วยเช่นกัน เมื่อมีความรู้ เราก็จะรู้เท่าทัน ชวนกันส่งต่อคลิกเข้าเว็บไซต์นี้กันเยอะๆ หรือแอดเฟรนด์เฟซบุ๊กกันไว้เลย https://www.facebook.com/CybercopTH

ที่มา : https://pctpr.police.go.th/about.php

TREND

Passkey เอาใจคนไม่อยากจำล็อกอินแบบไร้รหัสผ่าน

● ฟีเจอร์ Passkey ซอฟต์แวร์ตัวใหม่ ที่ Google, Apple และ Microsoft ประกาศความร่วมมือกันในเดือนพฤษภาคมปี 2022 ผลักดันให้เกิดความปลอดภัยที่รัดกุมยิ่งขึ้น เพราะปัญหาจากภัยโจรกรรมออนไลน์หลายๆ ครั้งเกิดจากคนร้ายรู้รหัสผ่านของเหยื่อ เนื่องด้วยผู้ใช้ตั้งรหัสผ่านที่เดาง่าย ซ้ำไปซ้ำมา และหากเจาะทะลวงจากรหัสผ่านในบริการใดๆ ก็มักจะเข้าทะลวงไปยังบริการอื่นได้ทันที (เพราะเราชอบตั้งรหัสผ่านเดียวกันทั้งหมด)

การทำงานของ Passkey คือการยืนยันตัวตนผ่านอุปกรณ์ที่รองรับของผู้ใช้งาน โดยไม่ต้องพิมพ์รหัสผ่านแต่สามารถรองรับการปลดล็อกที่หลากหลาย เช่น สแกนลายนิ้วมือ สแกนใบหน้า รหัสพิน หรือสแกน QR Code และแอปพลิเคชัน วิธีนี้จะช่วยให้ผู้ใช้งานไม่ต้องมาคอยจำรหัสผ่านของอุปกรณ์ ช่วยเรื่องความสะดวกและรวดเร็วในการล็อกอิน และมีความปลอดภัยกว่าการกรอกรหัสแบบเดิมๆ เพราะกุญแจที่ถูกเรียกใช้งานในแต่ละครั้งจะไม่ถูกนำไปใช้งานซ้ำได้ วิธีนี้ Google บอกว่าปลอดภัยต่อการโจมตีในรูปแบบเว็บฟิชชิง* อีกด้วย และนี่คือนวัตกรรมที่ถูกพัฒนาอย่างต่อเนื่องในอนาคต เป็นข้อพิสูจน์ว่ามิจฉาชีพมาทางไหน โปรแกรมเมอร์ก็พร้อมวิ่งหนีให้ไกลที่สุด

*เว็บฟิชชิง (Phishing) คือเว็บไซต์ที่ถูกสร้างขึ้นให้คล้ายกับเว็บจริงแล้วหลอกให้เหยื่อใส่รหัสผ่าน หรือ OTP

รู้เท่ากลโกงแฮกเกอร์ใน ChatGPT

● กองกำลังตำรวจของสหภาพยุโรป หรือ ยูโรโพล ได้ออกมาเตือนเกี่ยวกับภัยอันตรายของการใช้งานโมเดลภาษาขนาดใหญ่ ของ LLMs (Large Language Models) รูปแบบของปัญญาประดิษฐ์ หรือ AI ที่สามารถสร้างบทสนทนาและสร้างข้อมูลได้คล้ายคลึงกับการสร้างภาษาของมนุษย์ เช่น แชตจีพีที (ChatGPT)

เพราะความอัจฉริยะของเจ้าเอไอนี้เอง มาพร้อมความสามารถของโมเดลภาษาขนาดใหญ่ มีผู้เข้าใช้งานถึง 100 ล้านคน ตั้งแต่ช่วงสองเดือนแรกของการเปิดตัว ได้มีส่วนเกี่ยวข้องกับการฉ้อฉลทุกประเภท ตั้งแต่การโกงข้อสอบไปจนถึงอาชญากรรมไซเบอร์ ยูโรโพลได้กล่าวไว้ว่า ความสามารถของแชตจีพีทีในการร่างข้อความที่มีความเหมือนจริงและเป็นธรรมชาติทำให้ตัวเอไอกลายเป็นเครื่องมือที่มีประโยชน์สำหรับการฟิชชิง บางครั้งเหยื่อได้รับอีเมลจากธนาคาร หรือหน่วยงานต่างๆ และมองไม่ออกว่านี่คืออีเมลหลอกลวง

ยูโรโพลได้แนะนำว่า หน่วยงานบังคับใช้กฎหมายควรสร้างความตระหนักรู้เกี่ยวกับประเด็นนี้และร่วมมือกับภาคส่วนด้านไอทีเพื่อหาทางควบคุมปัญหาร่วมกัน พัฒนาความเชี่ยวชาญในองค์กรของตัวเอง รวมถึงอาจจะต้องพัฒนาโมเดลภาษาขนาดใหญ่ของตัวเองขึ้นมาด้วย

ที่มา : https://www.forbes.com/sites/emmawoollacott/2023/03/28/europol-sets-out-grim-prospects-for-law-enforcement-in-the-era-of-

แสดงความคิดเห็นคอลัมน์นี้

เครือซีพีหนุนทัพนักกีฬาไทยสู้สุดทุกสนาม ต่อเนื่องปีที่ 7

● เครือเจริญโภคภัณฑ์ (ซีพี) สนับสนุนทัพนักกีฬาไทยต่อเนื่องเป็นปีที่ 7 เสริมแกร่งทั้งกายใจให้พร้อมสู้สุดใจ เต็มที่ในทุกสนามการแข่งขัน ประกาศศักดาในศึกซีเกมส์ ครั้งที่ 32 และอาเซียนพาราเกมส์ ครั้งที่ 12 ที่กรุงพนมเปญ ประเทศกัมพูชา เติมเต็มความแข็งแกร่งของร่างกายด้วยเสบียงอาหารหลากเมนูจากซีพีเอฟ และซีพี ออลล์ ที่เปี่ยมด้วยคุณค่าทางโภชนาการ และอร่อยเด็ดโดนใจ พร้อมเติมกำลังใจด้วย ชิมทรูโรมมิ่ง บนเครือข่าย 5G โทรฟรีไม่อั้นจากกลุ่มทรู เพื่อเชื่อมโยงแรงใจจากครอบครัว พร้อมมอบสิทธิพิเศษในการปรึกษาแพทย์ออนไลน์ผ่านแอปพลิเคชัน MORDEE (หมอดี) และชวนคนไทยร่วมส่งแรงใจเชียร์ทัพไทยคว้าชัยชนะศึกนี้ผ่านแฮชแท็ก #สู้สุดทุกสนาม #คนไทยหัวใจนักสู้ บนโซเชียลมีเดียทุกช่องทาง

เครือซีพี จับมือเกษตรกรบ้านสบขุ่น จ.น่าน สร้างฝายอนุรักษ์แหล่งน้ำชุมชน

● เครือเจริญโภคภัณฑ์ (ซีพี) โดยสำนักงานด้านความยั่งยืนและพัฒนาชุมชน จ.น่าน เครือเจริญโภคภัณฑ์ ร่วมกับโครงการสถานีพัฒนาการเกษตรที่สูงตามพระราชดำริบ้านสบขุ่น จ.น่าน และเกษตรกรบ้านสบขุ่นในโครงการสบขุ่นโมเดล จัดกิจกรรมสร้างฝายอนุรักษ์ ‘น้ำคืนชีวิต’ พื้นที่สบขุ่นโมเดล พร้อมเชิญชวนเพื่อนพนักงานในเครือซีพี ได้แก่ บริษัท ซีพีเอฟ โกลบอล ฟู้ด โซลูชั่น จำกัด (มหาชน) (CPFGS) บริษัท ซีพี ออลล์ จำกัด (มหาชน) (CP ALL) บริษัท ซี.พี. อินเตอร์เทรด จำกัด (CPI) และทรู คอร์ปอเรชั่น ร่วมกิจกรรม โดยมีหน่วยงานภาคีเครือข่ายในพื้นที่และเกษตรกรบ้านสบขุ่นร่วมร้อยเรียงความดี สร้างฝายอนุรักษ์แหล่งน้ำชุมชน ณ บ้านสบขุ่น ต.ป่าคา อ.ท่าวังผา จ.น่าน

เซเว่น อีเลฟเว่น จับมือ จส.100 พาผู้ป่วยสมองเสื่อมอัลไซเมอร์กลับบ้าน

● คุณวิชัย จันทร์จริยากุล กรรมการผู้จัดการ (ร่วม) บริษัท ซีพี ออลล์ จำกัด (มหาชน) ผู้บริหารเซเว่น อีเลฟเว่น และเซเว่น เดลิเวอรี่ เปิดเผยว่า เซเว่น อีเลฟเว่น ได้ร่วมกับบริษัท แปซิฟิค คอร์ปอเรชั่น จำกัด (จส.100) สมาคมโรคสมองเสื่อมแห่งประเทศไทย คณะแพทยศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย และพันธมิตรต่างๆ ในการเผยแพร่สัญลักษณ์ดอกฟอร์เก็ตมีนอต (Forget Me Not) ตัวแทนของผู้ป่วยอัลไซเมอร์ ให้เป็นที่ตระหนักรู้ในสังคม และล่าสุดมีการให้ความรู้ทำความเข้าใจแก่พนักงานร้าน 6,105 สาขา ทั่วกรุงเทพฯ และปริมณฑล ในการดูแลผู้ป่วยเบื้องต้น เพื่อเป็นจุดรองรับประสานส่งต่อกรณีพบผู้ป่วยอัลไซเมอร์พลัดหลงให้ได้กลับคืนสู่ครอบครัวอย่างปลอดภัย

แสดงความคิดเห็นคอลัมน์นี้

“

แทนที่จะหวั่นกลัวหรือเพิกเฉยต่อการโจมตีทางไซเบอร์
เราควรสร้างมาตรการรับมือให้เท่าทันต่อภัยคุกคามเหล่านั้น

”

สเตฟาน แนปโป
รองประธานหัวหน้าเจ้าหน้าที่รักษาข้อมูล
ความปลอดภัยระดับโลก กลุ่ม SEB

LET THEM SEE LOVE

ถึง... ชีวิตที่รอคอย "หัวใจ" จากใครซักคน

เรื่องราวของหนึ่งชีวิต
ที่ได้รับการปลูกถ่ายหัวใจจากผู้บริจาค
หนึ่งในเรื่องจริงของการบริจาคอวัยวะ
ที่ส่งต่อการให้ไม่สิ้นสุด

จากผู้ป่วยเฉียดตาย
โรคกล้ามเนื้อหัวใจอ่อนแรง
เคยหัวใจวาย 3 ครั้ง
ก่อนได้รับการปลูกถ่ายหัวใจ

คุณณัฏฐ์ ลาภบุญอุดม
ผู้รับบริจาคอวัยวะ

ติดตามชม วิดีโอซีรี่ส์
EP1 ต่อชีพจรความรักให้กลับมา
ร่วมส่งต่อแรงบันดาลใจ พร้อมร่วมแสดง
ความจำนงบริจาคอวัยวะ-ดวงตา
และเงินสมทบทุนได้ที่สภากาชาดไทย
ทาง **www.letthemseelove.com**
#InfinityGiving
#ต่อการให้ไม่สิ้นสุด

สแกน
เพื่อชมภาพยนตร์