**Security Awareness ภัยใกล้ตัว**
**(Cybersecurity Awareness and Cyber Streetwise)**

Cyber ได้ถูกให้ความหมายจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ว่าคือคำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต(Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” ตามพจนานุกรม Cyberspace Operations Lexicon ของ กห.สหรัฐ กำหนดให้ Cyber Security คือกระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรปราศจากความเสี่ยง และ ความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ), ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการ เก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย อุบัติเหตุ และความผิดพลาดต่างๆ ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่างๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้ถือผลประโยชน์ร่วม (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

เหตุการณ์ในการการโจมตีทางไซเบอร์ครั้งใหญ่ ในประเทศไทยและนอกประเทศ เพื่อเล็งเห็นถึงความสำคัญของการตระหนักรู้ความมั่นคงปลอดภัยทางไซเบอร์ เนื่องด้วยในปัจจุบันการโจมตีทางไซเบอร์ได้ขยายขอบเขตสร้างความเสียหายให้แก่เศรษฐกิจภาพลักษณ์และสังคมรุนแรงขึ้นเรื่อยๆโดยเฉพาะอย่างยิ่งหน่วยงานของภาครัฐซึ่งถือว่าเป็นหน้าเป็นตาของในแต่ละประเทศ การโจมตีในที่นี้นั้นได้ขยายวงกว้างมากกว่าภาคธนาคารหรือสถาบันการเงินไปมากอีกทั้งบุคคลากรที่มีความรู้ความเข้าใจด้านความปลอดภัยก็ยังขาดแคลนและไม่เพียงพอ ทำให้ภัยคุกคามที่โจมตีองค์กรในแต่ละวันยิ่งทวีความรุนแรงขึ้น ซึ่งระบบที่มีอยู่ในปัจจุบันไม่สามารถป้องกันการโจมตีที่เปลี่ยนรูปแบบไปในแต่ละวันได้ รวมทั้งรูปแบบการดำเนินงานของภาครัฐก็มีส่วนทำให้เกิดความไม่ปลอดภัยกับข้อมูลของประชาชนจึงขอรวบรวมและแสดงตัวอย่างเหตุการณ์เพื่อให้ได้เข้าใจถึงลักษณะการโจมตี วิธีการ และรวมรูปแบบการโจมตีที่แฮกเกอร์ใช้ในปัจจุบันดังนี้คือ

๑.ธนาคารรัสเซียถูกโจมตีทางไซเบอร์ครั้งใหญ่ ซึ่งธนาคาร ๕ รายใหญ่ในรัสเซียไดแก่ ธนาคาร Sberbank, Alfa-Bank, Bank of Moscow, Rosbank และ Moscow Exchange ตกเป็นเป้าหมายสำคัญของ Botnet โดยพบว่าการโจมตีดังกล่าวมาจากอุปกรณ์จาก ๓๐ ประเทศ เช่น สหรัฐอเมริกา อินเดีย เป็นต้น ซึ่งการโจมตีดังกล่าวมาในรูปแบบของ DDos Attack โดยเป็นการส่งคำสั่งไปยัง Server จำนวนล้านครั้งเพื่อทำให้ระบบทั้งหมดเข้าสู่สถานะ Offline จากนั้นแฮกเกอร์เดินเข้ามาสู่ระบบเก็บข้อมูลไปอย่างง่ายดาย

๒.ATM ธนาคารออมสินประเทศไทยโดนขโมยเงินกว่า ๑๒ ล้าน การโจมตีนี้เรียกว่า ATM Jackpotting ซึ่งอาศัยช่องโหว่ของซอฟต์แวร์ภายในตู้ ATM ปล่อยมัลแวร์เข้าไปหลอกเครื่องว่ากำลังมีคนกดเงินทำให้เครื่องจ่ายเงินออกมา ซึ่งแฮกเกอร์ต้องอาศัยระยะเวลาในการรอให้เงินออกมาเรื่อยๆและต้องทำมากกว่า ๑ ตู้ถึงจะได้เงินจำนวน๑๒ล้านบาท ซึ่งธนาคารใช้บริการตู้ ATM จากหลายๆแบรนด์แต่ในกรณีนี้เป็นตู้ของบริษัท NCR เพียงอย่างเดียวหากมองในแง่ดี เหตุการณ์ในครั้งนี้ทำให้คนไทยหันมาใส่ใจเรื่องซีเคียวริตี้มากขึ้น

๓.สหรัฐฯกล่าวหารัสเซียว่าแทรกแซงการเมืองประเทศ ในข่าวระดับโลก เมื่อสำนักงานผู้อำนวยการข่าวกรองแห่งชาติของสหรัฐอเมริกาได้ประกาศว่าผู้นำของประเทศที่ถือว่าเป็นศัตรูกับสหรัฐอเมริกามาช้านานได้สั่งการให้แฮกเกอร์โจรกรรมอีเมลของคณะกรรมการพรรคเดโมแครต (ดีเอ็นซี) และส่งไปให้วิกิลีกส์เผยแพร่เพื่อช่วยให้โดนัลด์ทรัมป์ ตัวแทนพรรครีพับลิกันอยู่ในสถานการณ์ได้เปรียบเหนือฮิลลารี คลินตันตัวแทนจากฝั่งเดโมแครตในการเลือกตั้งชิงตำแหน่งประธานาธิบดีสหรัฐอเมริกา ซึ่งการแผยแพร่ข้อมูลดังกล่าวมีส่วนทำให้ทรัมป์ชนะการเลือกตั้งที่ผ่านมา สำหรับวิธีการนั้นทางสหรัฐอเมริกาไม่ได้ออกมาเปิดเผยรายละเอียดใดๆ

๔. Edward Snowden หนุ่มชาวอเมริกันที่ออกมาเปิดเผยความลับของประเทศตัวเองให้ทั่วโลกรับรู้ว่าหน่วยงาน NSA ของสหรัฐอเมริกาได้มีการแอบลักลอบขโมยข้อมูลการประชุมต่างๆทั่วโลกซึ่งเป็นการกระทำที่ขัดต่อหลักกฎหมายอย่างสิ้นเชิงประชาชนอเมริกันไม่เห็นด้วยกับการกระทำดังกล่าวเพราะทำให้ประเทศของตนเองเสียหาย แต่ในทางกลับกันทั่วโลกกลับให้ความสำคัญเพราะสหรัฐอเมริกาสามารถสอดแนมได้ถึงระดับข้อมูลบุคคลเกือบทุกประเทศทั่วโลกนอกจากนี้ยังสอดแนมในเรื่องธุรกิจซึ่งเป็นการเอาเปรียบคู่แข่งทางการค้าด้วยที่เห็นได้ชัดคือการดักฟังข่าวสารในการประชุมสุดยอดของ EU ถึงขึ้นมีการวางอุปกรณ์ดักฟังในห้องทำงานส่วนตัวของผู้แทน EU ในสหประชาชาติซึ่งทำให้ประเทศสมาชิกสหภาพ EU หรือพันธมิตรทางการค้าของสหรัฐอเมริกาเกิดความไม่พอใจเป็นอย่างมากจากเรื่องที่เกิดขึ้น

๕.หนุ่มประดับยนต์โดนแฮกเกอร์หลอกเอาเงินจากบัญชี เรื่องนี้เกิดขึ้นในประเทศไทยซึ่งวิธีการของมิจฉาชีพนั้นได้ปลอมตัวเป็นลูกค้าแล้วใช้เล่ห์กลในการขอเลขบัตรประชาชนจากเหยื่อจากนั้นนำข้อมูลไปเปลี่ยนแปลงกับเครือข่ายโทรศัพท์ ซึ่งเครือข่ายโทรศัพท์เองก็มีความผิดที่ยอมให้มิจฉาชีพเปลี่ยนแปลงข้อมูลต่อจากนั้นได้ใช้เล่ห์ขอให้เหยื่อสมัคร K-Cyber Banking ซึ่งเป็นบริการแอพพลิเคชันด้านการเงินของธนาคารกสิกรไทย ต่อมามิจฉาชีพจึงใช้ข้อมูลส่วนตัวของเหยื่อที่ได้มาล๊อกอินเข้าในแอพพริเคชันแล้วโอนเงินไปอย่างง่ายดาย เหตุการณ์นั้นทำให้เกิดความตื่นตระหนกอย่างมากในไทย ซึ่งทำให้หลายคนหมดความเชื่อมั่นในระบบดิจิทัล

๖.โรงแรมหรูในออสเตเลียโดนแรนซัมแวร์ล๊อกประตูเข้าออกทั้งหมด โรงแรม Romantik Seehotel Jaegerwit ๔-Star Superior Hotel เป็นโรงแรมหรูในออสเตรเลียที่ใช้ระบบล๊อกประตูแบบดิจิทัลแต่เนื่องจากแฮกเกอร์เจาะระบบไอทีของโรงแรมแล้วใช้ Ransomware เปลี่ยนข้อมูลคีย์การ์ดทั้งหมดทำให้แขกของโรงแรมไม่สามารถเข้าที่พักได้และบางคนก็ถูกขังในห้องซึ่งทางโรงแรมต้องเสียค่าใช้จ่ายปลดล๊อกถึง ๑,๕๐๐ Bitcoin เพื่อกู้ชื่อเสียงกลับมา

๗. เว็บ FBI ถูกแฮก ข้อมูลเจ้าหน้าที่ถูกนำไปขายต่อในตลาดมืด CyberZeist คือชื่อของแฮกเกอร์ที่อ้างว่าตนเองสามารถแฮกเว็บไซต์ของ FBI ที่ fbi.gov ได้สำเร็จและนำข้อมูลเจ้าหน้าที่ FBI ๑๕๕ คนมาเปิดเผย โดย CyberZeost ได้เริ่มต้นโจมตีเว็บไซต์ของ FBI โดยอาศัยช่องโหว่ Zero-day Vulnerability บนระบบ Content Management System (CMS) ที่มีชื่อว่า Plone CMS ซึ่งเป็นระบบ CMS ที่ถูกออกแบบมาสำหรับการใช้งานในระดับองค์กรโดยเฉพาะและเป็นหนึ่งใน CMS ที่มีความปลอดภัยสูงจนได้รับการยอมรับและใช้งานโดยหน่วยงานที่หลากหลายทั้งโดย Google และหน่วยงานรัฐอื่นๆในประเทศสหรัฐอเมริกา นอกจากนี้ทาง CyberZeist ยังได้ออกมาเปิดเผยอีกด้วยว่าเว็บไซต์ของ FBI นั้นใช้ระบบปฏิบัติการ FreeBSD รุ่นที่ปรับแต่งมาเป็นพิเศษและได้ทำการเปิดเผยข้อมูลส่วนตัวของพนักงาน FBI ที่ถูกจัดเก็บอยู่ภายในระบบนี้เอาไว้บน Pastebin ซึ่งประกอบไปด้วยชื่อผู้ใช้งาน รหัสผ่านและอีเมล

จากตัวอย่างข้างต้นนั้นทำให้เราผู้เป็นผู้บริโภคการใช้ข้อมูลสารสนเทศบนโลกไซเบอร์จำเป็นต้องรู้เท่าทันและสามารถรับมือกับการป้องกันข้อมูลเบื้องต้นได้ในระดับหนึ่งเพื่อความปลอดภัยของข้อมูลของท่านเอง

เราจำเป็นต้องเรียนรู้เทคนิคของโจรในโลกไซเบอร์ที่จะมาใช้ กลโกง หลอกล่อ เหยื่อ หรือใช้ความรู้เท่าไม่ถึงการณ์ของเราแล้วเอารัดเอาเปรียบทำให้เกิดผลกระทบต่อการทำงานหรือข้อมูลส่วนตัวได้ เพื่อนำมาสู่การป้องกันและรับมือกับสิ่งต่างๆในโลกไซเบอร์ที่เราอาจจะยังไม่พบไม่เจอ

การสร้างความมั่นคงปลอดภัยทางไซเบอร์จึงไม่ใช่เรื่องเพียงแค่เป็นวิสัยทัศน์อีกต่อไป ภายในปัจจุบันได้มีผู้คนหันมาให้ความสนใจกับการป้องกันข้อมูลไซเบอร์มากขึ้นเพราะหากไม่ลงมือสร้างขีดความสามารถของตัวบุคคลและเครื่องมือทางเทคโนโลยีเองเราก็จะประสบกับหายนะที่รับมือไม่ได้ในอนาคตแน่นอน จากการสำรวจและผลการวิจัยจากสถานบันหลายแห่งพบว่า องค์กรต้องเผชิญกับความเสี่ยงที่เพิ่มขึ้นอย่างมากจากการโจมตีทางไซเบอร์ในช่วง ๑–๒ ปีที่ผ่านมา ซึ่งการโจมตีทางไซเบอร์ที่เกิดขึ้น ทำให้องค์กรต้องมีภาระค่าใช้จ่ายในการดูแลรักษาระบบและทรัพยากรบุคคลที่มีความสามารถด้านความมั่นคงทางไซเบอร์เพิ่มมากขึ้นอย่างมหาศาลซึ่งการโจมตีทางไซเบอร์ได้ทวีความรุนแรงมีความซับซ้อนมากขึ้นและมีความถี่เพิ่มขึ้นมากขึ้น ทุกขณะผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ทั่วโลกต่างหาวิธีการที่จะรับมือกับภัยคุกคามทางไซเบอร์นี้รวมทั้งภัยคุกคามอื่นๆที่อาจจะเกิดขึ้นในอนาคตด้วยเนื่องจากต่างเห็นว่าอุตสาหกรรมต่างๆจะปลอดภัยขึ้นหากมีการรับมือป้องกันและตอบสนองต่อการคุกคามดังกล่าวอย่างมีประสิทธิภาพ

โดยมีการค้นพบว่าในปี ๒๐๑๗ องค์กรหลายๆองค์กรเริ่มมองเห็นความสำคัญในการนำความเชี่ยวชาญของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์มาใช้ร่วมกับเทคโนโลยีในการดำเนินงาน โดยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์จะถือเป็นส่วนหนึ่งของระบบงานในองค์กรด้วยเช่นมีเครื่องตรวจจับ มีการติดตามและป้องกันการโจมตีซึ่งหากองค์กรมีเพียงซอฟท์แวร์ในการป้องกันอย่างเดียวจะทำให้องค์กรแทบจะไม่มีความพร้อมในการตอบสนองต่อเหตุการณ์ได้ทันซึ่งไม่ใช้วิธีการแก้ปัญหาที่ดี การแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ที่ใช้ซอฟท์แวร์และเทคโนโลยีร่วมกับบุคลากรที่มีความเชี่ยวชาญในองค์กรจึงเป็นวิธีการที่ดีกว่าแต่ก็เป็นไปไม่ได้ที่จะจ้างทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยนี้ได้ในทุกจุดอย่างเพียงพอส่วนใหญ่องค์กรจึงได้จ้างผู้เชี่ยวชาญประจำอยู่สาขาใหญ่ขององค์กรนั้นๆเพื่อที่จะได้วิเคราะห์การโจมตี ที่อาจเกิดขึ้นได้จากทุกทางจนลดความเสี่ยงและความเสียหายได้

## ข้อแนะนำในการป้องกันภัยคุกคามทางไซเบอร์

**ป้องกันอุปกรณ์ของคุณให้ปลอดภัย (Secure your online devices)** ประเด็นนี้เป็นเรื่องการตั้งรหัสผ่านส่วนตัวที่ปลอดภัย ความเฉลียวฉลาดในการตั้งรหัสผ่านด้วยควรใช้วิธีการตั้งรหัสผ่านที่บุคคลอื่นคาดไม่ถึง เช่นใช้คำที่อาจจะจำได้ง่ายแต่เมื่อผสมกันแล้วทำให้ยากต่อการคาดเดา โดยหลักการตั้งควรหลีกเลี่ยงรหัสผ่านที่เป็นสิ่งใกล้ตัว เช่น ชื่อคนในครอบครัว ชื่อแฟน สถานที่เกิด วันเกิดเป็นต้น

**ป้องกันความปลอดภัยของข้อมูลในโลกออนไลน์ (Protect your online privacy)** ประเด็นนี้คือการใช้งาน ระบบ Social network การใช้ข้อมูลอย่างเฉลียวฉลาด เราควรรำลึกให้รู้ตัวเสมอว่าทุกครั้งที่เราจะแชร์ข้อมูลหรือโพสท์บน Social network ให้คิดให้ถี่ถ้วนทุกครั้งว่าเราจะแชร์อะไร “ให้ใคร” บ้างหากเป็น Facebook เราสามารถกำหนดได้ว่าเราต้องการแชร์ให้ใครเห็นบ้าง เราควรจะเลือกการแชร์อย่างเหมาะสม แต่ Social network ที่ควบคุมการแชร์ได้น้อย เช่น Twitter หรือ Instagram ก็ควรหลักเลี่ยงที่จะแชร์ข้อมูลส่วนตัวลงไป

**ดูแลเงินบนโลกออนไลน์ให้ดี (Look after your money online)** การช็อปปิ้งออนไลน์ในปัจจุบันกลายเป็นเรื่องปกติไปเสียแล้วในทุกวันนี้เนื่องด้วยการที่มีความสะดวกสบายต่อการซื้อขายและการที่มีโปรโมชั่นต่างๆมากมายที่มาล่อตาล่อใจชาวช็อปทั้งหลาย ก็มีคำแนะนำให้นักช็อปว่าทุกๆครั้งที่จะทำการซื้อของออนไลน์ควรจะเลือกเว็บที่มี (https:// และมีรูปกุญแจอยู่ใน URL) หากเป็นเว็บใหม่ที่พึ่งเปิดทำการมาไม่นานควรมีการตรวจสอบข้อมูลของเว็บไซต์นั้นให้แน่ใจก่อนทำการเข้าเว็บไซต์นั้น ก่อนที่จะกรอกข้อมูลส่วนตัวลงไป ถ้าคิดว่าไม่ปลอดภัยควรรีบออกจากเว็บนั้นทันทีและทำการส่ง URL ของเว็บไปยังหน่วยงานที่เกี่ยวข้องเพื่อตรวจสอบ เพราะส่วนใหญ่แล้วมักจะหลอกลวง

## แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับตัวเองและองค์กรด้วยวิธีดังนี้

**สำหรับบุคคล**

๑. ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์ที่ไม่มีการตรวจสอบแน่ชัดหรือเปิดไฟล์จาก บุคคลที่ไม่รู้จัก และระมัดระวังการเปิดไฟล์ผ่าน Social Media ทั้งนี้เพื่อหลีกเลี่ยงพวกมัลแวร์

๒. ไม่ใช้รหัสผ่านบน โลก cyber เป็นรหัสชุดเดียวกันทุกระบบ

๓. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และพิจารณาข้อมูลก่อนการแชร์ข้อมูลต่อเพื่อป้องกันตนเองเป็นต้นตอ ต่อการส่งแพร่กระจายไวรัส

**สำหรับหน่วยงาน**

๑. ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและข้อมูล

๒. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของ ไวรัส Web Application Firewall หรือ DDos Protection โดยสามารถขอรับบริการได้ที่ ThaiCERT/ERDA 838B-54271ED9A871}

๓. แจ้งเจ้าหน้าที่ของหน่วยงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงความเหมาะสมป้องกัน ข้อความจาก Social Media

๔. หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้าปกติ ควรตรวจสอบ Log การ login ย้อนหลังทุกๆ เดือน

๕. ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ต่างๆตามที่กฎหมายกำหนดไว้

จากตัวอย่างและข้อแนะนำต่างๆที่ได้กล่าวมา เห็นสมควรว่าบุคลากรควรเสริมสร้างความรู้ความเข้าใจให้สามารถป้องกันและเรียนรู้ว่าพฤติกรรมแบบไหนที่เสี่ยงต่อการเกิดการคุกคามทางไซเบอร์ ทางหน่วยงานควรมีการจัดอบรมให้บุคคลากรเสริมสร้างความรู้ในส่วนนี้แต่การจัดอบรมเฉยๆควรจะไม่สร้างความน่าเบื่อให้กับผู้อบรมเกินไปข้อแนะนำในการจัดอบรมให้น่าสนใจควรปฏิบัติดังนี้

๑. จัดอบรมเล็กๆเพื่อให้ความสนใจแก่ผู้อบรมอย่างทั่วถึง

๒. อบรมเป็นระยะเวลาสั้นๆ โดยทั่วไปพนักงานจะมีสมาธิต่อการอบรมไม่มาก จึงจำเป็นต้องอบรมไม่เกิน ๔๕–๖๐นาทีเพื่อดึงความสนใจของผู้อบรม

๓. เน้นเจาะจงเป็นเรื่องๆที่มีความสำคัญมากๆเพราะเรื่องความปลอดภัยของไซเบอร์ไม่ใช่เรื่องใหม่แต่บุคคลทั่วไปมักมองข้ามในเรื่องนี้ไปเราจึงต้องสร้างความสำคัญให้แก่หัวข้ออบรมให้มากขึ้น โดยไม่นำมารวมกันจะทำให้ผู้อบรมไม่เข้าใจ

๔. อัปเดตเนื้อหาและยกตัวอย่างในน่าสนใจและเป็นเรื่องราวใหม่ๆเสอมๆ โดยตามปกติคนเราชอบเสพข่าวหรือสิ่งที่น่าสนใจอยู่แล้ว

๕. นำไปปฏิบัติ การอบรมทั่วไปคนมักจะมาอบรมแค่เพียงให้ผ่านไปโดยไม่นำไปปฏิบัติจริงมากเท่าที่ควร ทางฝ่ายผู้ทำการอบรมควรจะติดตามผู้อบรมหลังจากการอบรมผ่านไป

๖. ผู้บริหารต้องมีส่วนร่วมด้วย โดยปกติการอบรมจะมีเพียงแค่พนักงานทำให้ปัญหาไม่ถูกแก้ทุกจุดของหน่วยงาน

สรุป การสร้างความมั่นคงทางไซเบอร์ทางผู้ใช้จำเป็นต้องมีความรู้และความเข้าใจในปัญหาจากการคุกคามว่าเกิดขึ้นได้อย่างไรต้นตอเกิดจากอะไร เพราะไม่ว่าจะมีระบบป้องกันที่ดีขนาดไหนหาก เกิดช่องโหว่ในระบบก็สามารถถูกแฮกเกอร์เจาะเข้าระบบได้เช่นกัน ผู้ใช้งานทุกคนควรมีความระมัดระวังในการใช้งานระบบ ไซเบอร์ เพื่อให้ทุกคนมีความตระหนักรู้ในเรื่องของความมั่นคงปลอดภัยและควรมีไหวพริบในขณะที่กำลังเจอกับปัญหา ถือเป็นการรู้จักป้องกันการก่อให้เกิดปัญหาทางความมั่นคงทางไซเบอร์อีกด้วยเพื่อป้องกันการเกิดเหตุการณ์ที่ไม่คาดคิดที่จะเกิดขึ้นได้ตลอดเวลา

ที่มา : https://bit.ly/38lKxSY