The Latest Cybercrime Trends in Thailand: Staying Vigilant in the Digital Age –

แนวโน้มอาชญากรรมทางไซเบอร์ในประเทศไทยล่าสุด: เราควรตระหนักรู้ถึงการใช้งานในยุคดิจิทัล

Author – Andrew Smith

February 2024

ความก้าวหน้าของเทคโนโลยีเกิดขึ้นอย่างรวดเร็ว ทำให้ภัยคุกคามทางไซเบอร์ก็เกิดขึ้นอย่างแพร่หลายและมีการพัฒนาอยู่ตลอดเวลา ซึ่งกลายเป็นภัยคุกคามต่อบุคคล ธุรกิจ และรัฐบาลทั่วโลก ประเทศไทยก็เป็นเหมือนกับประเทศอื่น ๆ ที่ไม่รอดพ้นจากภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นนี้ เมื่อเทคโนโลยีมีความก้าวหน้า กลยุทธ์ที่อาชญากรทางไซเบอร์นำมาใช้ก็เช่นกัน สิ่งสำคัญสำหรับบุคคลและองค์กรในประเทศไทยคือ ควรต้องรับทราบข้อมูลที่เกี่ยวกับแนวโน้มอาชญากรรมทางไซเบอร์ล่าสุด เพื่อป้องกันจากการโจมตีที่อาจจะเกิดขึ้น ในบทความนี้ เราจะมาสำรวจแนวโน้มของอาชญากรรมทางไซเบอร์ที่เกิดขึ้นภายในประเทศไทยล่าสุด และพิจารณาถึงความสำคัญของการเฝ้าระวังภัยคุกคามในยุคดิจิทัล

ความซับซ้อนที่เพิ่มขึ้นของการโจมตีทางไซเบอร์:

ในช่วงไม่กี่ปีที่ผ่านมา การโจมตีทางไซเบอร์มีความซับซ้อนเพิ่มขึ้นอย่างมากในประเทศไทย อาชญากรไซเบอร์ใช้เทคนิคขั้นสูงในการละเมิดเครือข่าย ทำการขโมยข้อมูลที่ละเอียดอ่อน และขัดขวางโครงสร้างพื้นฐานที่สำคัญ ตั้งแต่ การหลอกลวงแบบฟิชชิ่ง (Phishing) และการโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks) ไปจนถึงการโจรกรรมข้อมูลส่วนบุคคลและการฉ้อโกงทางการเงิน ภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อบุคคลและองค์กรในประเทศไทยเผชิญอยู่นั้น มีการเกิดขึ้นอย่างมากมายและขยายวงกว้างไปเรื่อย ๆ

แนวโน้มหนึ่งที่โดดเด่น คือ กลุ่มภาคธุรกิจที่มีมูลค่าสูงหรือหน่วยงานของภาครัฐที่มีความสำคัญ กลุ่มแฮกเกอร์มุ่งเน้นไปที่กลุ่มเป้าหมายที่มีความสำคัญและมีมูลค่าสูง เช่น สถาบันการเงิน บริษัทประกันภัย ผู้ให้บริการดูแลสุขภาพ และหน่วยงานของภาครัฐหรือหน่วยงานที่เกี่ยวกับความมั่นคงประเทศชาติ การโจมตีดังกล่าวสามารถทำให้เกิดความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และความมั่นคงของชาติได้ในกรณีที่เกิดขึ้นอย่างรุนแรง

การโจมตีแบบหลอกลวงหรือฟิชชิ่ง (Phishing) เป็นการหลอกให้บุคคลเปิดเผยข้อมูลที่ละเอียดอ่อน เช่น รหัสผ่านหรือรายละเอียดบัตรเครดิต โดยการแอบอ้างเป็นหน่วยงานที่มีความน่าเชื่อถือ เช่น ธนาคารหรือเว็บไซต์บริการออนไลน์ที่มีชื่อเสียง อาชญากรไซเบอร์มักจะส่งอีเมลหลอกลวงหรือสร้างเว็บไซต์ปลอมเพื่อหลอกล่อเหยื่อให้หลงเชื่อ นั่นเป็นเหตุผลที่สำคัญที่ต้องใช้ความระมัดระวังเมื่อคลิกลิงก์หรือให้ข้อมูลส่วนบุคคลทางออนไลน์

การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks) ยังเห็นมีเพิ่มขึ้นในประเทศไทยเช่นกัน ซึ่งซอฟต์แวร์อันตรายนี้ จะเข้ารหัสข้อมูลของเหยื่อ ทำให้ไม่สามารถเข้าถึงข้อมูลได้จนกว่าจะชำระเงินค่าไถ่ อาชญากรไซเบอร์มักเรียกร้องให้ชำระเงินด้วยสกุลเงินดิจิทัลเพื่อปกปิดตัวตน เพื่อลดความเสี่ยงของการตกเป็นเหยื่อของแรนซัมแวร์ สิ่งที่สำคัญคือการสำรองข้อมูลอย่างสม่ำเสมอและการตรวจสอบให้แน่ใจว่าซอฟต์แวร์รักษาความปลอดภัยมีการอัปเดตอยู่เสมอ

การโจรกรรมข้อมูลส่วนตัวเพิ่มมากขึ้นเป็นหนึ่งในแนวโน้มที่น่ากังวลอย่างมาก อาชญากรทางไซเบอร์ได้โจรกรรมข้อมูลส่วนบุคคล เช่น หมายเลขประกันสังคมหรือรายละเอียดบัญชีธนาคาร เพื่อกระทำการฉ้อโกงที่เกี่ยวกับการเงิน ประชาชนคนไทยควรระมัดระวังในการแบ่งปันข้อมูลส่วนตัวในโลกออนไลน์ และทำการตรวจสอบบัญชีการเงินของตนเป็นประจำเพื่อตรวจสอบกิจกรรมที่น่าสงสัย นอกจากนี้คนในประเทศไทยชื่นชอบการซื้อขายของออนไลน์และทำธุรกรรมทางดิจิทัลเพิ่มมากขึ้น การปลอมแปลงในการทำธุรกรรมออนไลน์ก็เป็นปัญหาที่สำคัญ อาชญากรทางไซเบอร์ใช้ช่องโหว่ในระบบการชำระเงินออนไลน์หรือใช้ข้อมูลบัตรเครดิตที่ถูกขโมยมาในการทำธุรกรรมที่ไม่ได้รับอนุญาต ผู้บริโภคควรระวังอย่างรอบคอบเมื่อทำธุรกรรมออนไลน์และใช้แพลตฟอร์มที่เชื่อถือและปลอดภัยเท่านั้น

เพื่อรับมือกับแนวโน้มอาชญากรรมไซเบอร์ ทั้งบุคคลและองค์กรควรจัดลำดับความสำคัญในด้านความปลอดภัยทางไซเบอร์อย่างเหมาะสม การใช้รหัสผ่านที่มีความปลอดภัย การใช้ระบบยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication - 2FA) และการอัปเดตซอฟต์แวร์อย่างสม่ำเสมอเป็นขั้นตอนสำคัญที่ควรทำเพื่อป้องกันการโจมตีที่อาจเกิดขึ้น การแนะนำและการเผยแพร่ข้อมูลเกี่ยวกับการป้องกันภัยทางไซเบอร์ จะช่วยสร้างความตื่นตัวในผู้ใช้งานและองค์กรเกี่ยวกับอันตรายของการโจมตีทางไซเบอร์ล่าสุด และส่งเสริมการใช้วิธีการปฏิบัติทางออนไลน์ที่ปลอดภัยอีกด้วย

การเกิดขึ้นของโปรแกรมประสงค์ร้าย (Malware) บนโทรศัพท์มือถือ:

การใช้งานโทรศัพท์มือถือและอุปกรณ์เคลื่อนที่ได้แพร่หลายในสังคมปัจจุบัน ซึ่งเป็นการเปิดช่องทางใหม่สำหรับอาชญากรไซเบอร์ในการแสวงหาผลประโยชน์ โปรแกรมประสงค์ร้าย (Malware) ในโทรศัพท์มือถือมักเป็นแอปพลิเคชันที่เป็นอันตรายที่สามารถทำการฟิชชิ่ง (Phishing) ได้ ซึ่งเป็นปัญหาที่มีความเสี่ยงเพิ่มมากขึ้นในประเทศไทย เนื่องจากผู้คนมักพึ่งพาอุปกรณ์เคลื่อนที่ของตนในการทำธุรกรรมกับธนาคาร การซื้อขายสินค้า และการสื่อสาร ซึ่งทำให้เป็นเหยื่อที่มีความเสี่ยงต่อการโจมตีทางไซเบอร์บนอินเทอร์เน็ตได้ง่ายขึ้น

การโจมตีแบบฟิชชิ่ง (Phishing) ที่มีเป้าหมายไปยังผู้ใช้งานอุปกรณ์เคลื่อนที่ มีความซับซ้อนมากขึ้น โดยส่วนใหญ่จะปลอมแปลงให้เหมือนแอปพลิเคชันหรือเว็บไซต์ที่ถูกต้องตามกฎหมาย เพื่อล่อให้ผู้ใช้งานเปิดเผยข้อมูลส่วนบุคคลและข้อมูลทางการเงินของตน ผู้ใช้งานควรใช้ความระมัดระวังเมื่อจะดาวน์โหลดแอปพลิเคชัน และควรอัปเดตโปรแกรมอยู่เสมอและระวังข้อความหรือการโทรที่น่าสงสัย

บทบาทของวิศวกรรมสังคม: The Role of Social Engineering:

การปฏิบัติการวิศวกรรมสังคม (Social engineering) เป็นกลยุทธ์ที่อาชญากรไซเบอร์ที่ใช้เพื่อเข้าถึงข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต โดยใช้ประโยชน์จากจิตวิทยาของมนุษย์และการชักจูง เทคนิคนี้มักจะใช้การสื่อสารหรือเทคนิคอื่น ๆ เพื่อหลอกล่อเหยื่อให้เปิดเผยข้อมูลที่สำคัญ เช่น รหัสผ่าน ข้อมูลทางการเงิน หรือข้อมูลอื่น ๆ ที่เป็นความลับได้

การโจมตีแบบฟิชชิ่งผ่านทางอีเมล (Email phishing), การโทรหาโดยปลอมแปลงตัวเองให้ดูเหมือนคอลเซ็นเตอร์หรือบุคคลอื่น (Caller ID spoofing) และการใช้เทคนิคการหลอกลวงเพื่อแอบอ้างว่าเป็นบุคคลอื่น เป็นเทคนิคที่ได้รับความนิยมในการโจมตีทางวิศวกรรมสังคมในประเทศไทย โดยอาชญากรไซเบอร์จะใช้แพลตฟอร์มโซเชียลมีเดีย เว็บไซต์หาคู่ออนไลน์ หรือแม้แต่ชุมชนเกมออนไลน์เป็นช่องทางในการเข้าถึงเหยื่อที่เป็นเป้าหมาย

การปกป้องตนเองจากภัยคุกคามทางไซเบอร์: Protecting Yourself from Cyber Threats:

ด้วยธรรมชาติของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป จึงเป็นสิ่งสำคัญสำหรับบุคคลและองค์กรในประเทศไทยที่จะนำมาตรการเชิงรุกมาใช้ เพื่อปกป้องตนเองจากการตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ ต่อไปนี้เป็นขั้นตอนสำคัญบางประการในการปรับปรุงความปลอดภัยทางไซเบอร์ของคุณ:

- *ใช้รหัสผ่าที่แข็งแกร่งและไม่ซ้ำกัน: หลีกเลี่ยงการใช้รหัสผ่านที่สามารถคาดเดาได้ง่าย และพิจารณาใช้โปรแกรมจัดการรหัสผ่านเพื่อสร้างและเก็บรักษารหัสผ่านที่ซับซ้อนสำหรับบัญชีต่าง ๆ*
- *เปิดใช้งานการรับรองความถูกต้องด้วยสองขั้นตอน (2FA): การเพิ่มระดับการรักษาความปลอดภัยให้กับบัญชีออนไลน์ของคุณสามารถลดความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาตได้อย่างมาก*
- *อัปเดตซอฟต์แวร์อยู่เสมอ: อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ป้องกันไวรัส และแอปพลิเคชันอื่น ๆ ของคุณเป็นประจำเพื่อให้แน่ใจว่าคุณมีการอัปเดตโปรแกรมรักษาความปลอดภัยที่ทันสมัยที่สุด*

- *ระวังอีเมลและลิงก์ที่น่าสงสัย: ระมัดระวังเมื่อเปิดอีเมลจากผู้ส่งที่ไม่รู้จัก และหลีกเลี่ยงการคลิกลิงก์หรือดาวน์โหลดไฟล์แนบที่น่าสงสัย*
- *ใช้เครือข่ายส่วนตัวเสมือน (VPN): เมื่อเข้าถึงอินเทอร์เน็ต โดยเฉพาะบนเครือข่าย Wi-Fi สาธารณะ ให้ใช้ VPN เพื่อเข้ารหัสการเชื่อมต่อของคุณและปกป้องข้อมูลของคุณจากการแอบติดตาม*
- *ติดตามข่าวสารอยู่เสมอ: ติดตามแนวโน้มอาชญากรรมในโลกไซเบอร์ล่าสุด ให้ความรู้เกี่ยวกับการหลอกลวงทั่วไป และติดตามแนวทางปฏิบัติที่ดีที่สุดในการปกป้องทรัพย์สินดิจิทัลของคุณ*

ร่วมกันสร้างอนาคตที่ปลอดภัย: Collaborative Efforts for a Secure Future:

การจัดการกับภัยคุกคามที่เพิ่มขึ้นของอาชญากรรมทางไซเบอร์ต้องอาศัยความร่วมมือจากผู้มีส่วนได้ส่วนเสียต่างๆ ไม่ว่าจะเป็น รัฐบาล ธุรกิจต่างๆ และตัวบุคคล ต้องทำงานร่วมกันเพื่อพัฒนากลยุทธ์ความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง ส่งเสริมความตระหนักรู้ และแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามที่เกิดขึ้นใหม่

ในประเทศไทย ภาครัฐบาลได้ดำเนินการเสริมสร้างมาตรการรักษาความปลอดภัยทางไซเบอร์โดยการจัดตั้งหน่วยงานเฉพาะ การบังคับใช้กฎหมาย และส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชน อย่างไรก็ตาม เพื่อปกป้องตนเอง ความรับผิดชอบยังขึ้นอยู่กับบุคคลและองค์กรในการจัดลำดับความสำคัญด้านความปลอดภัยทางไซเบอร์และดำเนินการเชิงรุก

ด้วยการเฝ้าระวัง ติดตามข่าวสาร และดำเนินการตามแนวทางปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ เราสามารถร่วมกันต่อสู้กับกระแสอาชญากรรมทางไซเบอร์ที่เพิ่มขึ้นและสร้างสภาพแวดล้อมทางดิจิทัลที่ปลอดภัยยิ่งขึ้นสำหรับทุกคน