

"เมตา" แนะนำ 5 เคล็ดลับป้องกันตัวเองจากมิจฉาชีพทางออนไลน์

นำเสนอเมื่อ : 9 ก.พ. 2565

เนื่องในวัน Safer Internet Day (วันรณรงค์อินเทอร์เน็ตปลอดภัย) เมตา (Meta) ตอกย้ำภารกิจช่วยผู้คนสร้างการเชื่อมต่อที่มีความหมายในสภาพแวดล้อมที่น่าเชื่อถือและปลอดภัยทางออนไลน์.....

เนื่องในวัน Safer Internet Day (วันรณรงค์อินเทอร์เน็ตปลอดภัย) เมตา (Meta) ตอกย้ำภารกิจช่วยผู้คนสร้างการเชื่อมต่อที่มีความหมายในสภาพแวดล้อมที่น่าเชื่อถือและปลอดภัยทางออนไลน์ โดยเฉพาะในขณะที่โลกยังคงต้องรับมือกับการระบาดใหญ่ของโควิด-19 อย่างต่อเนื่อง บรรดามิจฉาชีพได้พัฒนากลโกงออนไลน์ที่ซับซ้อนมากขึ้นเพื่อใช้เอาเปรียบแก่ผู้ที่หลงเชื่อ

เมื่อผู้คนหันมาพึ่งพาช่องทางดิจิทัลในการเชื่อมต่อกับชุมชน ครอบครัว และเพื่อน ๆ มากขึ้นกว่าที่เคย Meta จึงก้าวไปอีกขั้นเพื่อช่วยคนไทยเฝ้าระวังต่อต้านการหลอกลวงด้านความปลอดภัยและฟิชชิ่ง โดยทำให้บัญชีของผู้ใช้ปลอดภัยขึ้นด้วยเครื่องมือต่าง ๆ เช่น การยืนยันตัวตนแบบสองชั้น การแจ้งเตือนการเข้าสู่ระบบ หรือการเตือนให้ผู้คนเลือกรหัสผ่านที่คาดเดายากขึ้น

เพื่อเสริมความรู้และปกป้องผู้คนจากภัยหลอกลวงทางออนไลน์ Facebook ประเทศไทยได้เปิดตัวแคมเปญ #StayingSafeOnline เพื่อสร้างการตระหนักรู้ผ่านโครงการ We Think Digital Thailand ร่วมกับ จุฬาลงกรณ์มหาวิทยาลัย โคแฟค ประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และสำนักงานส่งเสริมเศรษฐกิจดิจิทัล มีวัตถุประสงค์เพื่อช่วยให้ทุกคนเข้าใจถึงกลโกงการหลอกลวงทางออนไลน์ประเภทต่าง ๆ และแบ่งปันเคล็ดลับความปลอดภัยเพื่อหลีกเลี่ยงการตกเป็นเหยื่อของการหลอกลวง โดยจะให้ความรู้เกี่ยวกับประเภทของภัยออนไลน์ที่พบได้บ่อยและเคล็ดลับความปลอดภัยผ่านรูปแบบวิดีโอสั้น โดยสามารถติดตามเนื้อหาในสัปดาห์วันอินเทอร์เน็ตปลอดภัยได้ที่ Meta Thailand Official Page <https://www.facebook.com/MetaTH>

โครงการนี้ประกอบด้วยโมดูลและวิดีโอสั้นต่าง ๆ ที่มีรายละเอียดเชิงลึกซึ่งสร้างขึ้นโดยผู้เชี่ยวชาญด้านความปลอดภัยกว่า 35,000 คนของ Meta จากฝ่ายความมั่นคงและความปลอดภัยที่ได้ทำการวิจัยเกี่ยวกับการฉ้อโกงออนไลน์และการหลอกลวงที่พบบ่อยที่สุด ได้แก่ การหลอกลวงประเภทเงินกู้ การหลอกลวงประเภทรางวัลตลอด đời การหลอกลวงประเภทโรแมนติคหรือแก๊งลวงรักออนไลน์ การหลอกลวงประเภทจัดหางาน และการหลอกลวงประเภทขายของออนไลน์

เราแต่ละคนมีหน้าที่รับผิดชอบในการป้องกันตนเองจากการหลอกลวงทางออนไลน์และสร้างความมั่นใจเรื่องความปลอดภัยทางออนไลน์ ต่อไปนี้คือเคล็ดลับง่าย ๆ 5 ข้อที่คุณสามารถทำได้เพื่อป้องกันตัวเองจากนักหลอกลวงทางออนไลน์ ได้แก่

อย่าส่งเงินหรือข้อมูลส่วนบุคคลไปให้คนที่คุณไม่รู้จัก :

บ่อยครั้งที่นักต้มตุ๋นจะขอข้อมูลส่วนบุคคล เช่น ที่อยู่จริงหรือรายละเอียดธนาคารเพื่อสวมรอยแอบอ้างทรัพย์สินหรือส่งพัสดุหลอกลวงไปให้ที่บ้าน หรืออ้างว่าคุณถูกลอตเตอรี่ ประกาศรับสมัครงานเพื่อเป็นขออ้างสอบถามข้อมูลส่วนบุคคล คุณจึงไม่ควรให้ข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเมื่อฟังดูดีเกินจริง

อย่าคลิกลิงก์ที่ไม่รู้จัก :

จับตาดูลิงก์ที่คุณไม่คุ้นเคย โดยเฉพาะอย่างยิ่งลิงก์ที่มาจากคนที่你不รู้จักหรือเชื่อถือ ระวังอย่าคลิกลิงก์ต้องสงสัย เปิดไฟล์นางสงสัย หรือติดตั้งซอฟต์แวร์ที่เป็นอันตราย แมวจะดูเหมือนมาจากเพื่อนหรือบริษัทที่คุณรู้จักก็ตาม

อย่าบอกรหัสผ่านของคุณให้ใครรู้ :

อย่าเปิดเผยข้อมูลรหัสผ่านของคุณแก่ใครก็ตาม แม้แต่เพื่อนหรือครอบครัว และอย่าลืมเปลี่ยนรหัสผ่านเป็นประจำเพื่อป้องกันไม่ให้บัญชีของคุณถูกแฮ็กโดยมิจฉาชีพ ซึ่ง Facebook และ Instagram จะไม่ขอรหัสผ่านจากคุณทางอีเมล หรือส่งรหัสผ่านให้คุณในรูปแบบของเอกสารแนบ ผู้ใช้สามารถยืนยันได้ว่า อีเมลที่อ้างว่ามาจาก Facebook นั้นเชื่อถือได้หรือไม่

โดยตรวจสอบอีเมลล่าสุดที่เราส่งให้คุณจากรายการในการตั้งค่าการรักษาความปลอดภัยและการเข้าสู่ระบบได้ที่นี้ (<https://www.facebook.com/settings>) หากคุณเห็นโพสต์หรือข้อความที่พยายามหลอกให้คุณแชร์ข้อมูลส่วนบุคคล โปรดรายงานไปที่นี้ (<https://www.facebook.com/help/reportlinks>)

อย่ายอมรับคำขอเป็นเพื่อนจากคนแปลกหน้า :

นักต้มตุ๋นอาจสร้างบัญชีปลอมเพื่อส่งคำขอเป็นเพื่อนด้วยเจตนาที่จะหลอกลวง การยอมรับคำขอเป็นเพื่อนจากนักต้มตุ๋นอาจทำให้เกิดการโพสต์สแปมบนไทม์ไลน์และอาจเกิดการแชร์ไปให้เพื่อน ๆ อื่นๆ นักต้มตุ๋นอาจแท็กคุณในโพสต์และส่งข้อความที่เป็นอันตรายถึงคุณและผู้ติดต่อของคุณ ดังนั้น Meta สนับสนุนให้ผู้คนระมัดระวังและยอมรับคำขอเป็นเพื่อนจากคนรู้จักและไว้วางใจเท่านั้น

ตั้งค่าการยืนยันตัวตนแบบสองชั้น :

คุณควรตั้งค่าการยืนยันตัวตนแบบสองชั้นเพื่อเพิ่มความปลอดภัยให้บัญชีโดยเพิ่มการปกป้องอีกหนึ่งชั้น เมื่อคุณตั้งค่าการยืนยันตัวตนแบบสองชั้น Meta

จะขอให้คุณกรอกรหัสเข้าสู่ระบบพิเศษหรือยืนยันการเข้าสู่ระบบของคุณทุกครั้งที่มีคนพยายามเข้าถึงบัญชี Facebook ของคุณจากเบราว์เซอร์หรืออุปกรณ์มือถือเครื่องใหม่ที่เราไม่รู้จัก

และคุณสามารถรับการแจ้งเตือนเมื่อมีคนพยายามเข้าสู่ระบบจากเบราว์เซอร์หรืออุปกรณ์มือถือที่เราไม่รู้จักได้อีกด้วย ผู้ใช้สามารถเข้าไปที่ศูนย์ช่วยเหลือเพื่อเรียนรู้เพิ่มเติมเกี่ยวกับวิธีตั้งค่าและจัดการยืนยันตัวตนแบบสองชั้น และวิธีตั้งรับการแจ้งเตือนเกี่ยวกับการเข้าสู่ระบบที่ไม่รู้จัก

ขอบคุณที่มาเนื้อหาจาก [เดลินิวส์ วันที่ 8 กุมภาพันธ์ 2565](#)