การดูแลปกป้องตนเอง

และการปกป้องความเป็นส่วนตัว บนโลกวิถีใหม่

KRITSANANUT NUNCHOO


STEM ERROR
LOGIN

ชีวิตเราอยู่บนความเสี่ยง ทั้งกายภาพและโลกดิจิทัล

โจรกรรม แอบอ้าง ถูกโจมตี เช่น ปลอมเป็นตัวเรา โจรกรรมข้อมูลเรา การแอบอ้างเรา

เราคุยกับเพื่อน ก็ยังเสี่ยงมีคนแอบฟังแล้วนำสิ่งที่ได้ยินไปทำอย่างอื่นต่อ

DIGITAL FOOTPRINT

DIGITAL FOOTPRINT

รอยเท้าของเราบนโลกดิจิทัล โลกอินเทอร์เน็ต มันคือร่องรอยที่เราไปใช้เว็บต่างๆเช่น อัปโหลดรูปภาพ ไฟล์ บันทึกข้อมูลการใช้งาน(เวลาเรากรอกข้อมูลในเว็บ) ไม่ว่าจะ ชื่อ ที่อยู่ เบอร์โทร วันเดือนปีเกิด พวกนี้ล้วนเป็นรอยเท้าของเราทั้งสิ้นและแน่นอนว่ามันอยู่ในเกือบทุกเว็บที่เราไปไม่ว่าจะเป็น Facebook ,IG หรือ เว็บไซต์ต่างๆ เป็นต้น

ร่องรอยดิจิทัล ที่ผู้ใช้เจตนาบันทึก (ACTIVE DIGITAL FOOTPRINTS)

รอยเท้าดิจิทัล ของผู้ใช้งานที่เจตนาบันทึกไว้ในโลกออนไลน์ ข้อมูลที่เราตั้งใจเปิดเผยโดยที่เรายินยอมหรือรู้ตัว เช่น ชื่อ นามสกุล อีเมล เบอร์โทร ชื่อโปรไฟล์ รวมถึงสิ่งที่เราตั้งใจโพสต์ รูปภาพ ข้อความ การกดถูกใจ รีทวีต หรือ การแชร์โลเคชัน เป็นต้น

การโพสต์ลงบนโซเชียลมีเดียส่วนตัว แพลตฟอร์มต่าง ๆ เช่น FACEBOOK, TWITTER, INSTAGRAM และ YOUTUBE หรือการส่งอีเมล การเขียนบล็อก การคอมเมนต์เป็นข้อความหรือรูปภาพ ซึ่งสามารถสืบค้นและส่งผลต่อชีวิตเราได้

ร่องรอยดิจิทัล ที่ผู้ใช้ไม่มีเจตนาบันทึก (PASSIVE DIGITAL FOOTPRINTS)

เป็นข้อมูลทางดิจิทัลที่เราทิ้งไว้โดยไม่เจตนา โดยไม่ตั้งใจ ไม่รู้ตัวว่าได้ทิ้งร่องรอยไว้บนอินเทอร์เน็ต เช่น IP ADDRESS รวมทั้งการค้นหาข้อมูลในเว็บไซต์ต่าง ๆ เป็น SEARCH HISTORY หรือแม้กระทั่งพาสเวิร์ดคอมพิวเตอร์ พาสเวิร์ดเข้าเว็บไซต์ที่ถูกบันทึกไว้อัตโนมัติ การติดตามระบบ GPS ต่างๆ

DIGITAL FOOTPRINT ส่งผลต่อเราอย่างไร

หากดูจากสองข้อด้านบนแล้วเราจะรู้ว่ามันมีทั้งข้อดีและข้อเสีย ข้อดีมันคือทำให้เรามีความสะดวกสบายมากขึ้น เวลาเราเข้าเว็บก็ไม่ต้องกรอกข้อมูลบ่อยๆ

แต่ข้อเสียมันก็เยอะทีเดียว เพราะมีผลการศึกษาพบว่าหลายครั้งรอยเท้านี้มันชัดเจนจนสามารถระบุตัวตนเราได้เลย ซึ่งมันอาจนำไปสู่การใช้ข้อมูลในทางไม่ชอบ หรือใกล้ตัวมากๆเช่นเราเคยโพสต์อะไรไว้ มันอาจกลับมาทำร้ายเราในภายหลัง หรือมันอาจจะถูกนำข้อมูลไปเปิดเผยจนเราได้รับความเสียหายได้

DIGITAL FOOTPRINT
กับโลกการทำงาน

Digital Footprint ที่แสดงถึงพฤติกรรมการใช้งานโซเชียลมีเดียของเรา ยังส่งผลต่อการทำงานได้ด้วย เพราะปัจจุบันหลายองค์กรนอกจากขอดูประวัติการทำงานผ่าน Resume หรือ Portfolio แล้ว ยังเข้าไปสืบค้นประวัติของคุณผ่านโซเชียลมีเดียเพื่อประกอบการพิจารณารับเข้าทำงาน เพื่อให้เข้าถึงและรู้จักตัวตนของผู้สมัครมากยิ่งขึ้น ว่ามีความเหมาะสมกับองค์กรหรือไม่

โดยจากผลสำรวจของ CareerBuilder พบว่า ผู้ประกอบการกว่า 70% ยอมรับว่าใช้โซเชียลมีเดียในการค้นหาข้อมูลผู้สมัครประกอบการพิจารณา โดยกว่า 40% ปฏิเสธที่จะรับผู้สมัครเข้าทำงานหากโพสต์ภาพ วิดีโอ หรือข้อมูลในทางไม่เหมาะสม ฉะนั้นการที่จะโพสต์ ไลก์ แชร์ หรือคอมเมนต์ใด ๆ ขอให้คงความเป็นมืออาชีพ และมีความคิดสร้างสรรค์ไว้เป็นหลัก

แล้วเราควรระวังอย่างไรดี ?

1 **การโพสต์หรือการคอมเมนต์**
สามารถส่งผลดีและผลเสียต่อชีวิตของเราได้ ฉะนั้น เตือนตัวเองเสมอก่อนจะเขียนอะไรลงไป ใช้สติ และวิจารณญาณ และเขียนในเชิงที่สร้างสรรค์แทน

2 **ถึงจะลบโพสต์หรือคอมเมนต์ไปแล้ว**
แต่รอยเท้าดิจิทัลนี้ก็ยังสามารถสืบค้นได้และอยู่ตลอดไปในโลกออนไลน์ จึงต้องเพิ่มความระมัดระวัง

3 **ก่อนจะรับใครเป็นเพื่อน**
ไม่ว่าจะเป็นช่องทางออนไลน์ไหน ให้พิจารณาให้ดี เพราะเราอาจไปเปิดเผยข้อมูลส่วนตัวให้กับมิจฉาชีพหรือแฮ็กเกอร์ล้วงความลับแบบไม่รู้ตัว

แล้วเราควรระวังอย่างไรดี ?

- ตั้งค่าความเป็นส่วนตัวใน ACCOUNT ต่าง ๆ
- หลีกเลี่ยงการคลิกเข้าไปในเว็บไซต์ที่ไม่ใช่ Official Account เพื่อตอบแบบสอบถาม เพราะจะเป็นการดึงข้อมูลส่วนตัวของเราไปได้
- ทำการตั้งค่าระบบความปลอดภัยเพื่อป้องกันอุปกรณ์สื่อสารและคอมพิวเตอร์ของคุณจากภัยคุกคามทางไซเบอร์ และมีการแบ็กอัปข้อมูลไว้เสมอ
- หลีกเลี่ยงการโพสต์ที่เป็นสินทรัพย์ส่วนตัวที่จะทำให้สูญเสียทรัพย์สิน เช่น โพสต์อวดบ้าน อวดรถ เป็นต้น และหลีกเลี่ยงการแชร์โลเคชันหากเป็นไปได้ เนื่องจากมิจฉาชีพเข้าถึงได้ง่าย
- ปิดโหมดบลูทูธเมื่อไม่ได้ใช้งาน เพราะเป็นช่องทางดึงข้อมูลส่วนตัวจากมิจฉาชีพ
- หมั่นอัปเดตระบบปฏิบัติของโทรศัพท์หรือเครื่องคอมพิวเตอร์เสมอ
- ตรวจสอบระบบ Wi-fi สาธารณะก่อนใช้งาน ไม่ใช้ Wi-fi ที่ให้เปิดเผยข้อมูลส่วนตัว

DIGITAL FOOTPRINT หลีกเลี่ยงไม่ได้

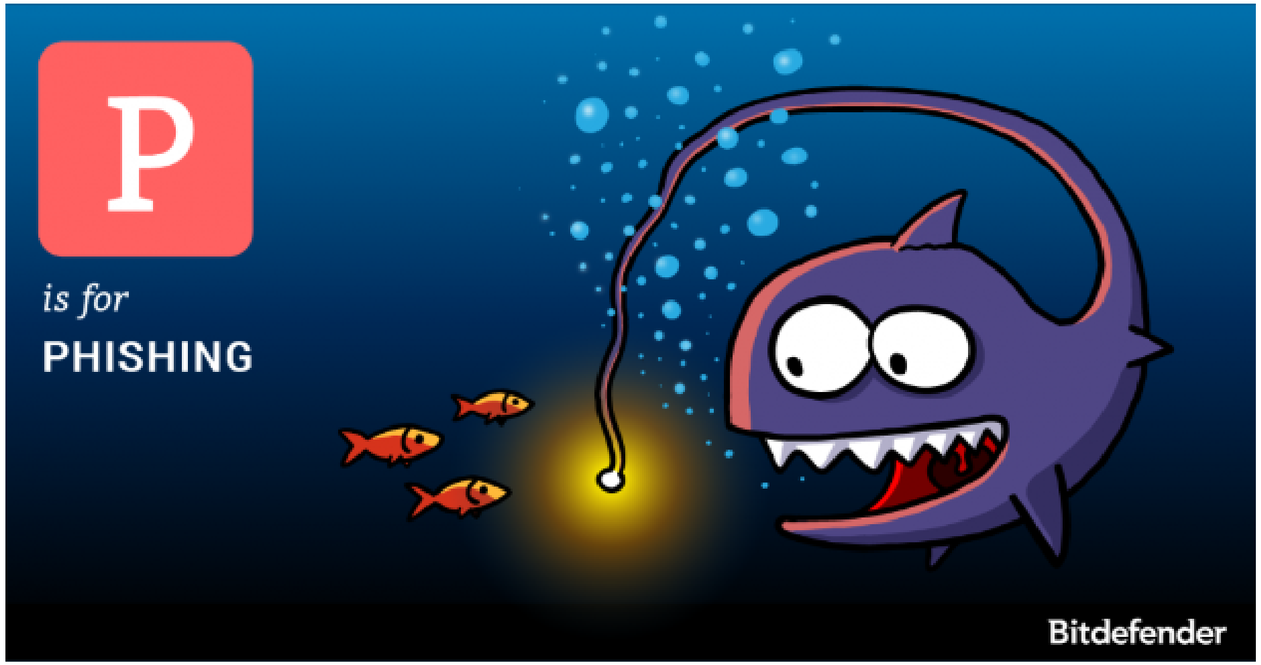
ดังนั้นต้องท่องโลกอินเทอร์เน็ตด้วยความระมัดระ


Personal
Data

ฟิชชิง (PHISHING) คืออะไร?

- คำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล ซึ่งอาจไม่ใช่การล่อลวงธรรมดาที่เราพบเห็นกันทั่วไป แต่จะเป็นกลยุทธ์การหลอกที่ใช้วิธีทางจิตวิทยาเข้าร่วมด้วย

- ส่วนใหญ่แล้วจะมาในรูปแบบของอีเมล์ เว็บไซต์ และสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น

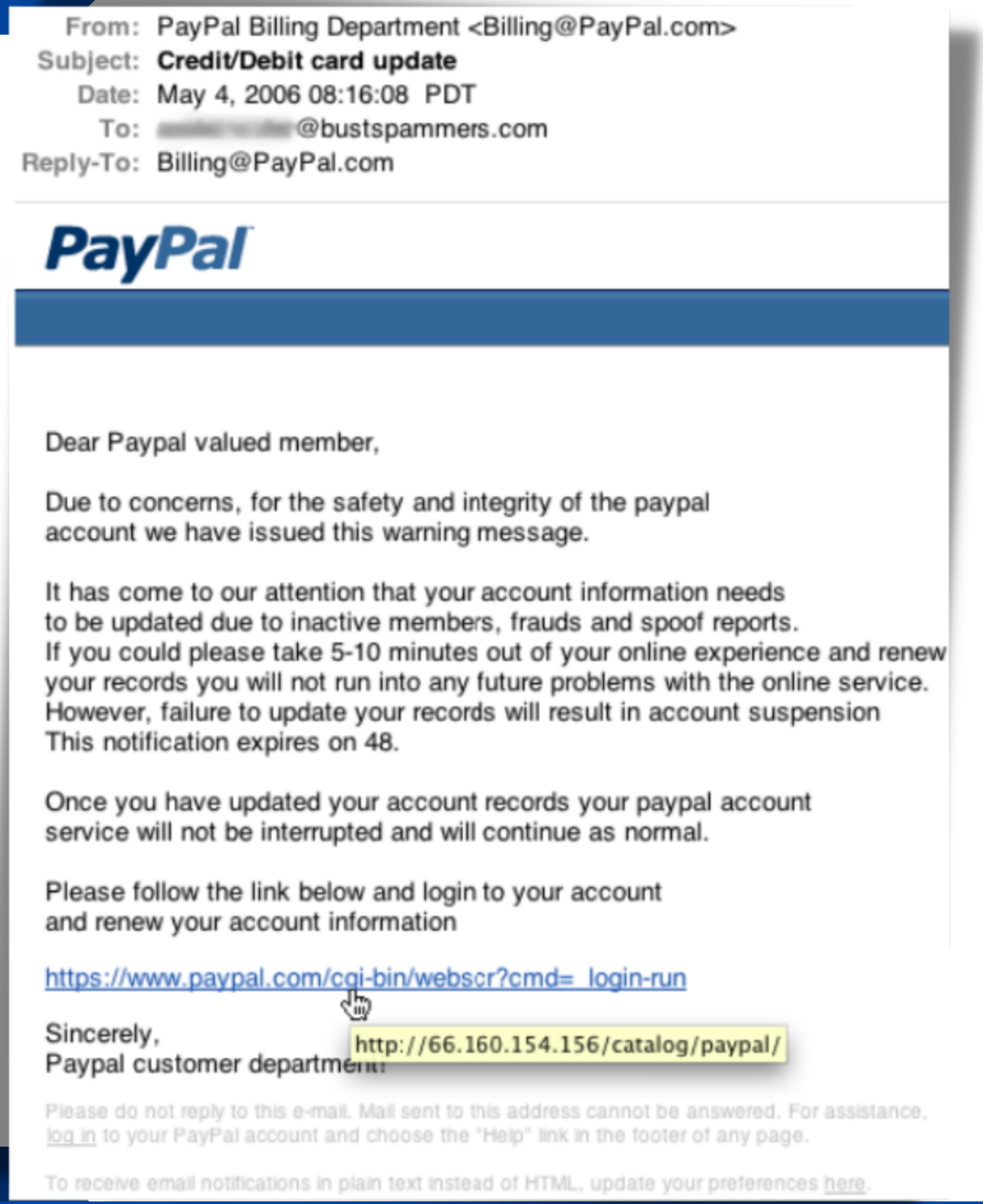


ฟิชชิง (PHISHING) คืออะไร?

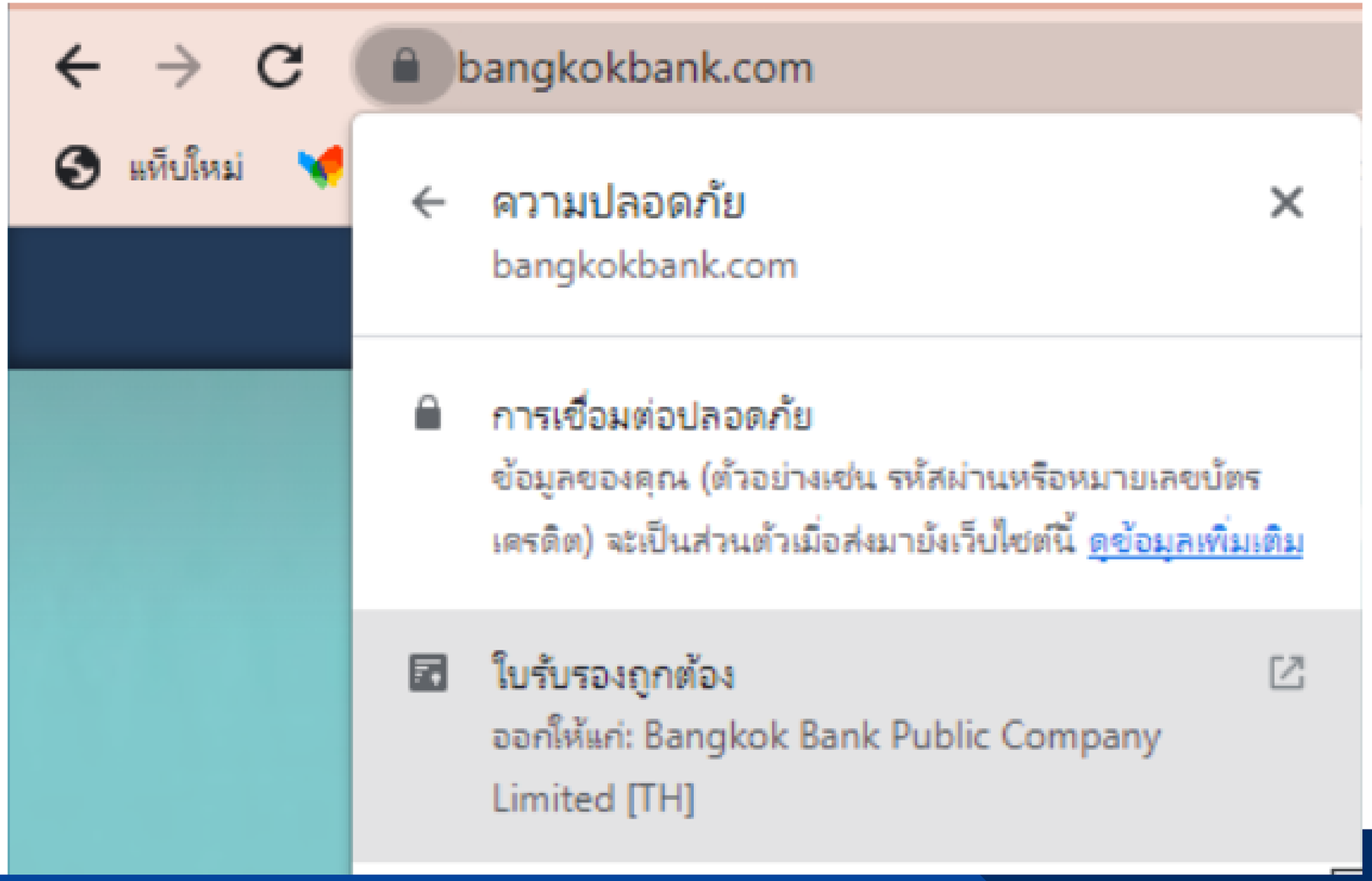
Phishing เป็นคำพ้องเสียงจากคำว่า Fishing ซึ่งหมายถึงการตกปลา หากจะเปรียบเทียบง่าย ๆ เหยื่อล่อที่ใช้ในการตกปลา เป็นกลวิธีที่ผู้โจมตีใช้ในการหลอกลวงผู้เสียหาย ซึ่งเหยื่อล่อที่เด่น ๆ ในการหลอกลวงแบบ Phishing มักจะเป็นการปลอมอีเมล หรือปลอมหน้าเว็บไซต์ที่มีข้อความซึ่งทำให้ผู้เสียหายอ่านแล้วหลงเชื่อ

เช็คลิงค์ดีๆ
อย่าเพิ่งคลิก

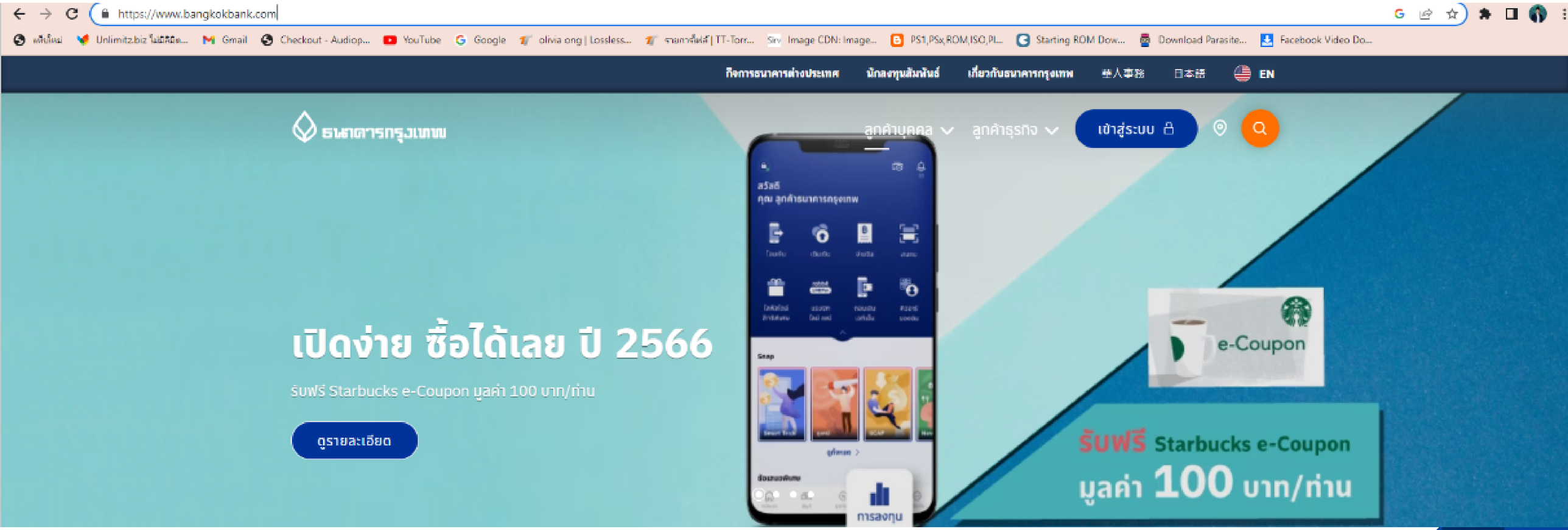
พึงระวังอีเมลที่ขอให้กรอกข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นอีเมลที่มาจากสถาบันการเงิน ทั้งนี้ธนาคารหลายแห่งได้แจ้งอย่างชัดเจนว่า ธนาคารไม่มีนโยบายในการขอให้ลูกค้าเปิดเผยเลขประจำตัว หรือข้อมูลที่มีความสำคัญอื่นๆ ผ่านทางอีเมลโดยเด็ดขาด



เช็คเว็บไซต์ดีๆ ก่อนกรอกข้อมูล

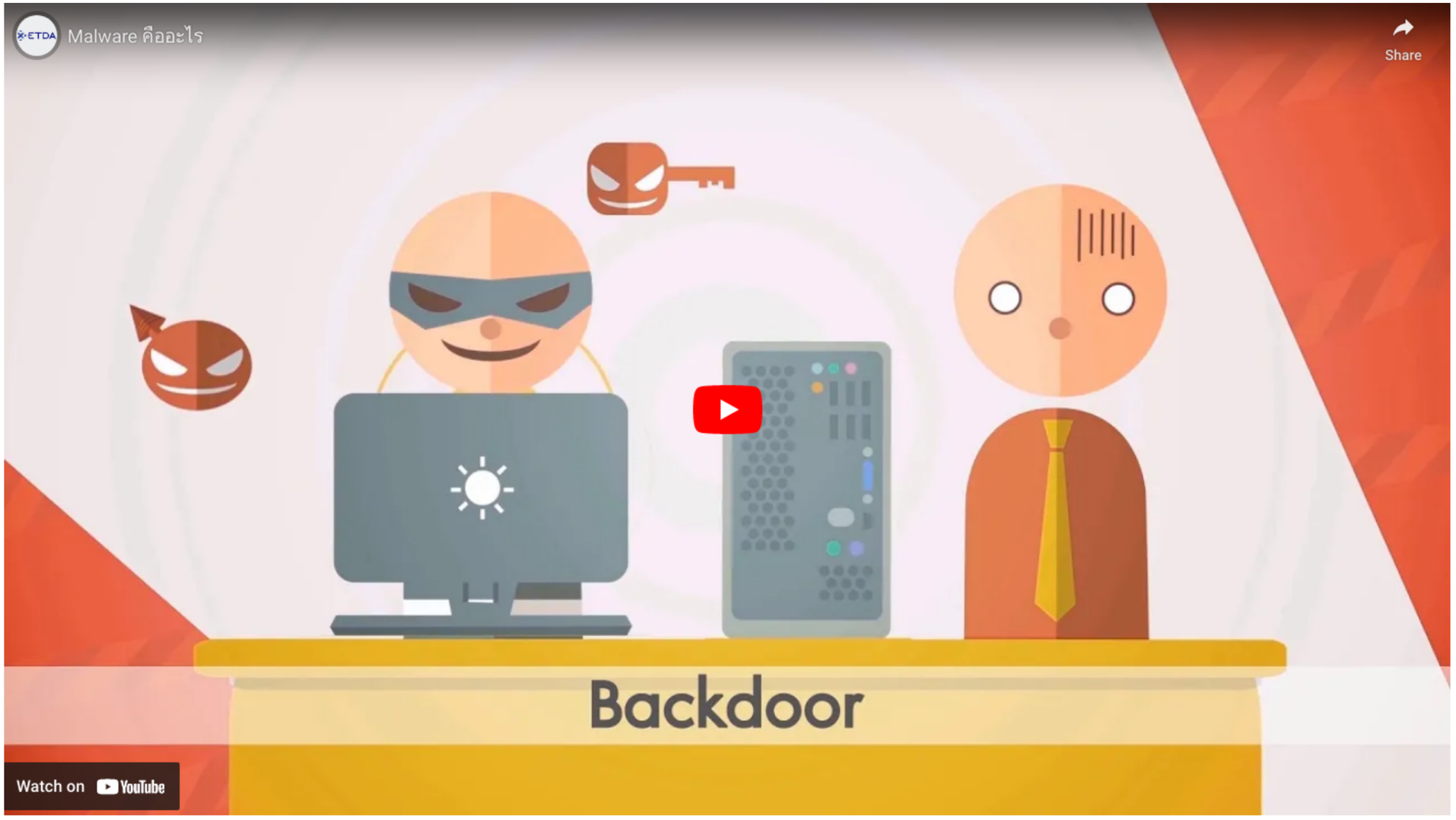


สังเกตระบบความปลอดภัยที่ด้านหน้าลิงค์



สังเกตให้แน่ใจว่าเว็บไซต์ที่ใช้งานเป็น HTTPS ก่อนให้ข้อมูลที่สำคัญ

ควรอ่านข้อความก่อนคลิกเข้าลิงค์ หรือคลิกตกลงทุกครั้ง
ใช้สติ ใช้วิจารณญาณของเราเองให้ดี
จะช่วยให้ไม่ตกเป็นเหยื่อได้ง่าย


ETDA
Malware คืออะไร
Share
Backdoor
Watch on YouTube

ป้องกันข้อมูลส่วนตัวอย่างไรให้ปลอดภัยขึ้น

หมั่น Back Up ข้อมูล

หนึ่งในวิธีการเก็บรักษาข้อมูลส่วนตัวแบบง่ายๆ ที่มักจะถูกมองข้ามคือการทำ back up ข้อมูลไว้นอกอุปกรณ์สื่อสารที่คุณใช้เป็นประจำ เพื่อป้องกันการสูญหายของข้อมูลในกรณีที่คุณทำอุปกรณ์สื่อสารของคุณหายไป วิธีการง่ายๆ คือ back up ข้อมูลไว้ใน hard drive

ป้องกันระบบการเชื่อมต่อกับสัญญาณ Wifi

การเชื่อมต่อสัญญาณ Wifi นอกพื้นที่บ้านหรือที่ทำงานของคุณกลายเป็นเรื่องปกติในชีวิตประจำวัน แต่ต้องระวังว่านี่จะเป็นอีกหนึ่งช่องทางที่ทำให้แฮคเกอร์สามารถขโมยข้อมูลของคุณได้ เพราะฉะนั้นคุณจะต้องมั่นใจว่าพาสเวิร์ตส่วนตัวต่างๆ ของคุณซับซ้อนและปลอดภัยมากพอที่จะใช้งานในที่สาธารณะได้แบบไร้กังวล และควรจะตระหนักไว้เสมอว่าการใช้ Wifi สาธารณะในการเข้าเว็บไซต์ต่างๆ ต้องเริ่มต้นด้วย HTTPS ไม่ใช่ HTTP เพราะมันจะปลอดภัยมากกว่า

ติดตั้งระบบจัดการตรวจสอบไวรัส

มัลแวร์ หรือโปรแกรมที่ไม่พึงประสงค์ รวมไปถึงเข้าไวรัสเป็นสิ่งที่ต้องระแวดระวังมากที่สุดในการใช้คอมพิวเตอร์ วิธีการจัดการที่ดีที่สุดคือคุณควรจะต้องติดตั้งซอฟแวร์ที่ช่วยสแกนเพื่อค้นหาไวรัสและจัดการกับมันได้อย่างทันท่วงที่ โปรแกรมที่เป็นที่รู้จักกันดีอาทิเช่น Norton และ McAfee.

ระวังการใช้อีเมล์

เหล่าแฮคเกอร์ทั้งหลายมักจะใช้วิธีการขโมยข้อมูลส่วนตัวต่างๆ ผ่านทางอีเมล์ เพราะฉะนั้นคุณจะต้องระวังการเปิดอีเมล์จากคนแปลกหน้าหรือจากแหล่งที่มาที่คุณไม่รู้จัก หากคุณสงสัยในความไม่ปลอดภัยในการใช้งานของอีเมล์ควรจะแจ้งกับบริษัทแม่ของอีเมล์ที่คุณใช้อยู่โดยตรง

คอยระวังสอดส่องดูไวรัส

มีสัญญาณบ่งบอกมากมายว่าคอมพิวเตอร์ของคุณอาจจะติดไวรัส เช่น หน้าต่าง Pop Ups ที่มักจะเด้งขึ้นมา หรือการที่เครื่องของคุณเปิดตัวช้า หรือทำงานช้าลงกว่าเดิม มีข้อความแปลกๆ เข้ามา หรือการบ่งบอกว่า hard drive ของคุณทำงานหนักกว่าปกติ รวมไปถึงบางครั้งมันอาจจะทำให้ไฟล์ของคุณหายไปโดยที่ความจุในคอมพิวเตอร์ลดลง

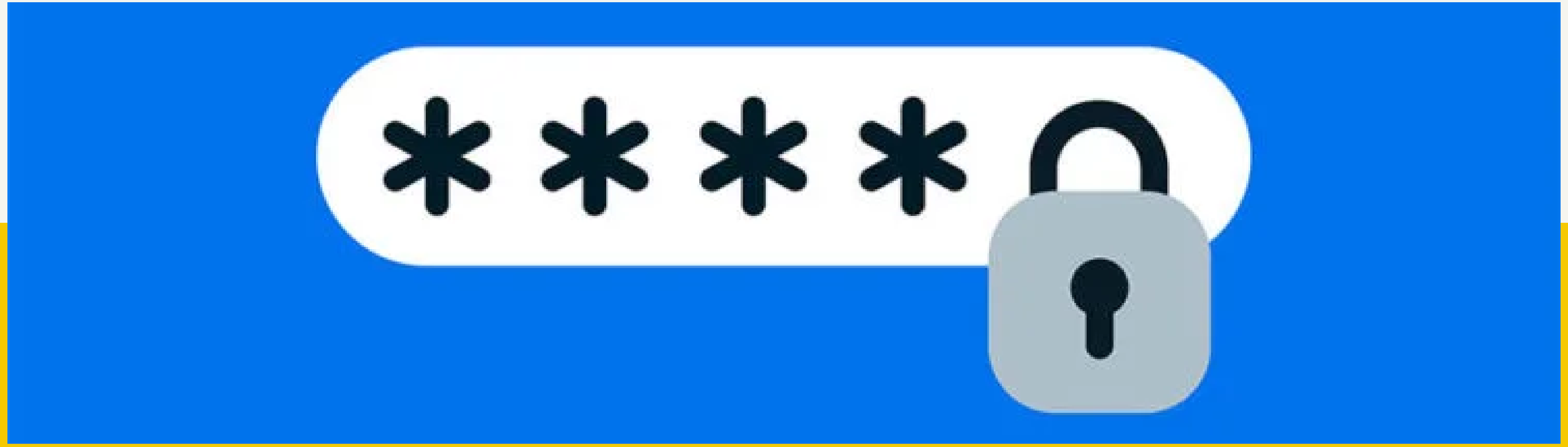
อย่าเปิดเผยข้อมูลบนโซเชียลมีเดียมากเกินไป

แนะนำว่าอย่าเข้าใช้บัญชีโซเชียลมีเดียของคุณในอุปกรณ์สื่อสารจำนวนหลายเครื่อง และในการใช้โซเชียลมีเดียควรจะต้องมีการระวังในเรื่องของการแชร์ข้อมูลส่วนตัวให้มากไม่ควรใส่รายละเอียดมาเกินไป ไม่ว่าจะเป็นวันเกิด ที่อยู่ หรือเบอร์โทรศัพท์

เปลี่ยน Password เป็นประจำ

พาสเวิร์ดของคุณควรจะประกอบไปด้วยตัวอักษรและตัวเลขอย่างน้อย 12-15 ตัว รวมไปถึงการที่คุณควรจะต้องเปลี่ยนพาสเวิร์ตเป็นประจำ ที่สำคัญอย่าบันทึกพาสเวิร์ตของคุณไว้ในอุปกรณ์สื่อสาร หรือจดมันไว้ในที่ๆ หาง่ายจนเกินไป

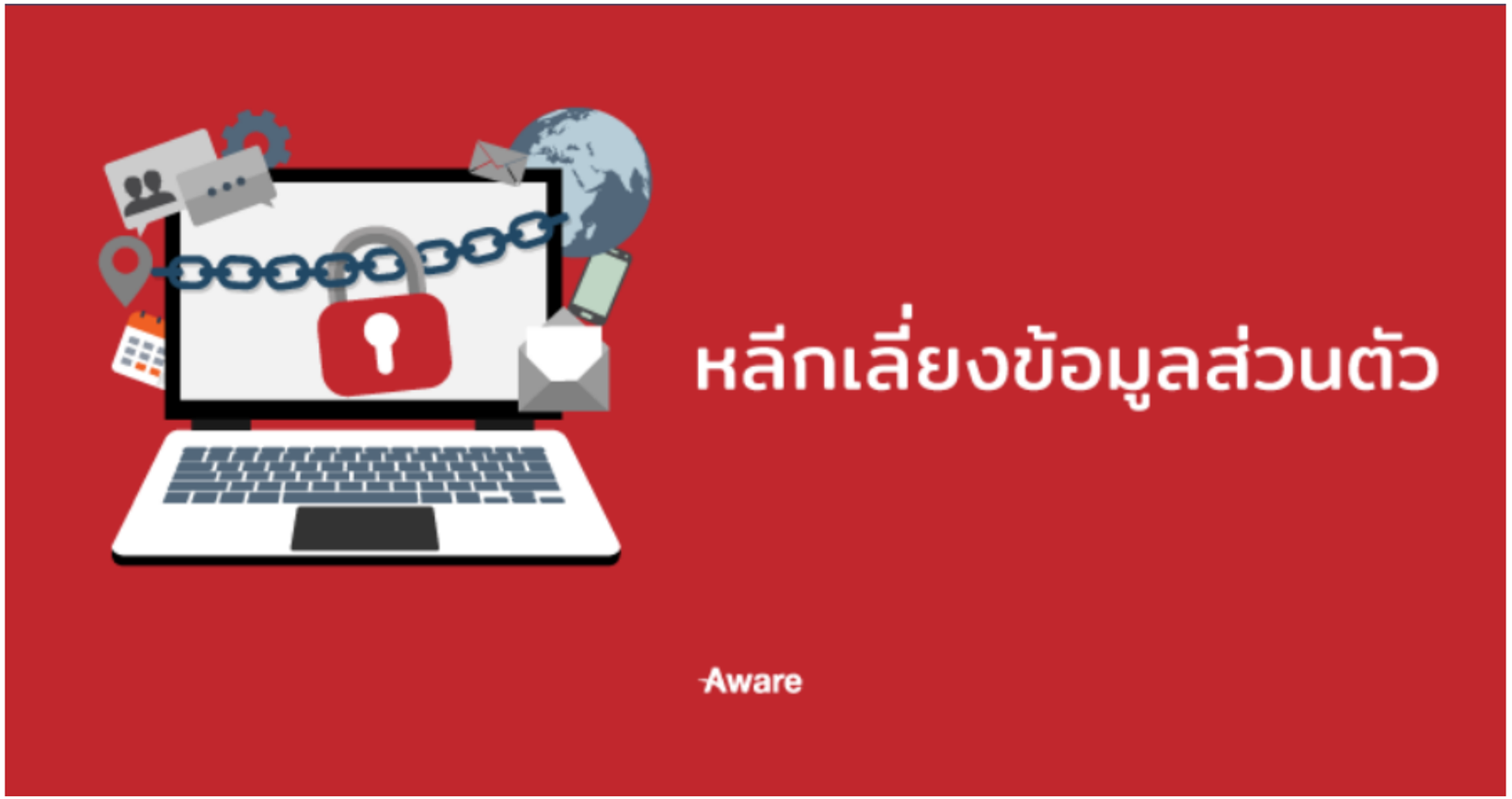
ตั้ง Password อย่างไรให้ปลอดภัยขึ้น



ควรตั้งรหัสผ่าน 8-12 ตัวอักษรขึ้นไป เพราะรหัสผ่านที่มีความยาว 10 ตัวอักษรนั้นก็คาดเดาได้ยากกว่ารหัสผ่าน 8 ตัวอักษรถึง 4,000 เท่า! หรืออาจต้องใช้เวลาถึง 4,000 วัน! และถ้าจะเอาแบบแฮ็กยากๆเราแนะนำที่ 14 ตัว ยิ่งยาวยิ่งเดายาก แต่ถ้าคุณตั้งรหัสผ่านแบบ 88888888888888 เลขแปด 14 ตัว แบบนี้ก็ท่าทางจะไม่รอดฮะ ขอร้องล่ะ...อย่าทำนะ นอกจากนั้นเรื่องความยาวเดี๋ยวนี้หลายๆเว็บกำหนดความยาวรหัสผ่านที่ 8 ตัวอักษรเป็นขั้นต่ำอยู่แล้ว แต่ถ้าให้ปลอดภัยจริงๆ แนะนำว่าตั้งเริ่มต้นที่ 10 ตัวอักษรจะดีกว่า

สร้างรหัสผ่านด้วยการใช้คีย์บอร์ดแบบกระจายๆ ด้วยการผสมตัวอักษรภาษาอังกฤษทั้งพิมพ์เล็ก/ใหญ่ ตัวเลข เครื่องหมายพิเศษ เข้าด้วยกัน เพราะเมื่อเราใช้แบบนั้นแล้วโอกาสที่จะเดารหัสผ่านถูกจะมีแค่ 1 ในหลาย 100,000,000,000 (แสนล้าน) เช่น การสร้างรหัสผ่าน 1A!2b@3C#4d$ ต่อให้เดาสุ่ม หรือแม้ว่าปัจจุบันจะมีโปรแกรมที่ใช้ช่วยเดาก็ยังถือว่าเข้าถึงได้ยาก ดังนั้นเพื่อความปลอดภัยควรผสานรหัสผ่านด้วยตัวอักษรหลากหลายแบบเอาไว้เสมอ

ไม่ควรใช้ข้อมูลส่วนตัวที่หาได้ง่ายได้แก่ ชื่อ วันเดือนปีเกิด เลขบัตรประชาชน มาตั้งรหัสผ่าน หรือ ข้อมูลส่วนตัวที่หาเจอได้ง่าย เช่น ชื่อแฝงที่เราชอบใช้มาผูกกับรหัสผ่าน ถ้าชอบใช้ชื่อใน Internet ว่า Pamaham ก็เลยตั้งรหัสผ่านว่า “Pamaham123456” อย่างนี้ก็ให้หลีกเลี่ยงไปเลยจะดีกว่า



นี่เราไม่ได้ล้อคุณเล่นนะ เรากำลังจะบอกคุณว่าอย่าใช้คำที่ปรากฏอยู่ในพจนานุกรมเลย เพราะคำศัพท์เหล่านั้นถูกนำไปบรรจุลงในโปรแกรมคาดเดารหัสผ่านเป็นที่เรียบร้อยแล้ว ใช่... ทั้งเล่มเลย ต่อให้คำนั้นสะกดยากและยาวแค่ไหน โปรแกรมก็คาดเดาคำได้อยู่ดี เพราะฉะนั้นอย่าตั้งให้พวกแฮ็กเกอร์อ่านได้รู้เรื่องด้วยตัวอักษรธรรมดา

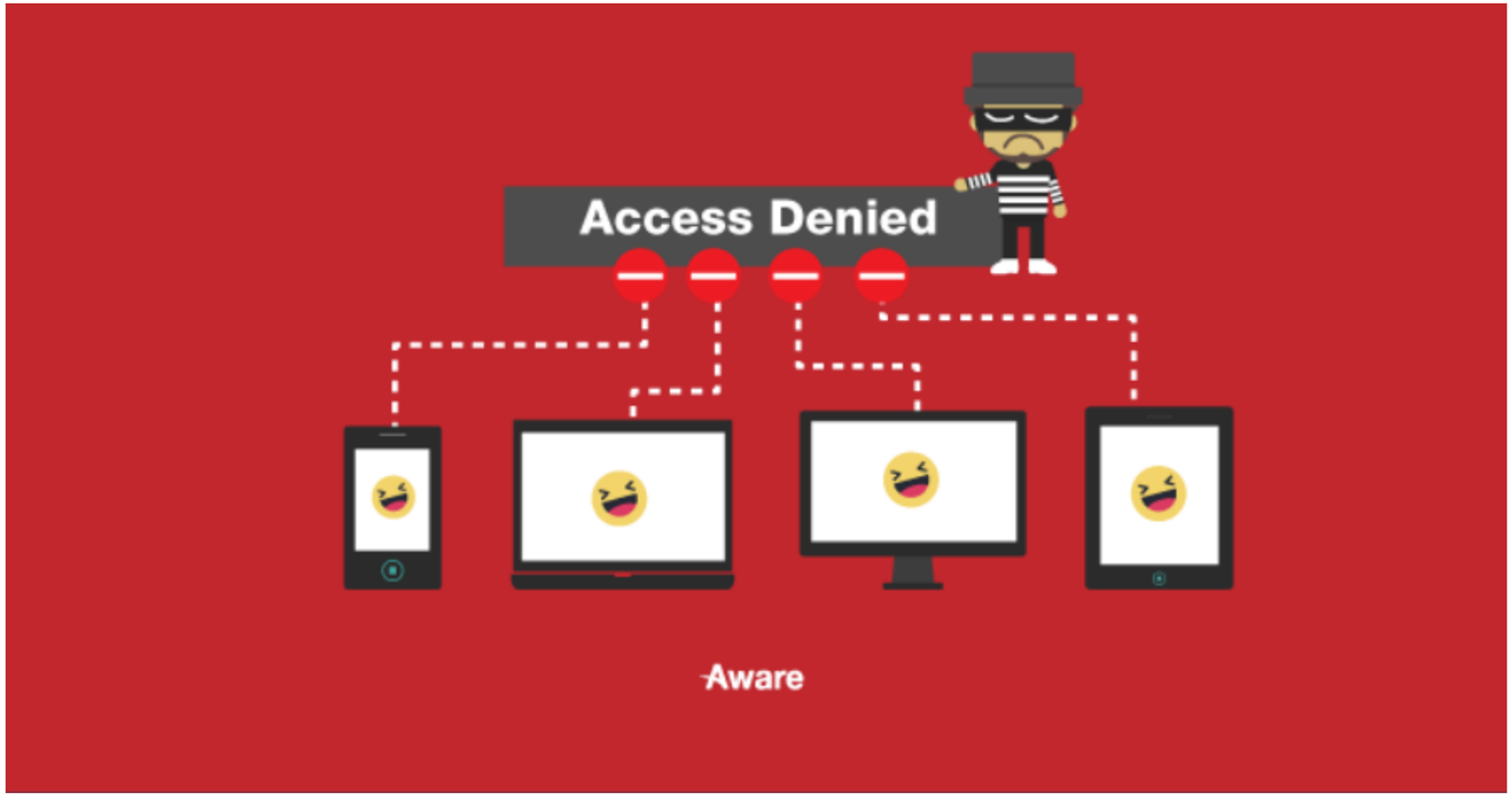
ในแต่ละปีจะมีรายงานว่าผู้คนตั้งรหัสผ่านยอดแย่ว่าอะไรบ้าง อย่างปี 2022
อันดับ 1 : 123456
อันดับ 2 : 123456789
อันดับ 3 : qwerty
อันดับ 4 : password
อันดับ 5 : 12345
หาดูได้จาก keyword นี้
“the Worst Passwords of 2022”

ไม่ควรใช้รหัสผ่านซ้ำเหมือนกันทุกเว็บไซต์ เพราะเมื่อไหร่ที่รหัสหลุดไปอยู่ที่ผู้ร้าย ข้อมูลส่วนตัวเราอาจถูกขโมยไปได้ เตรียมร้องเพลงธรณีกรรแสงในเวอร์ชันที่คุณชอบได้เลย แต่แนะนำว่าให้ตั้งให้เป็นเอกลักษณ์ของเว็บนั้นๆเลยจะดีกว่า เช่น รหัสผ่านของเว็บ Gmail เราอาจใช้ตัวย่อมาตั้งต่อจากที่เราเคยตั้งก็ได้ L,=kp,KPxv’1 แล้วต่อด้วย GM คุณจะได้ L,=kp,KPxv’1GM ส่วนของ Hotmail ก็เป็น L,=kp,KPxv’1HM ดีมั้ยล่ะทีนี้ ไม่ซ้ำแต่มีนัยยะให้ระลึกได้

py'w'dHiydgTv gTv8nv8;k,iyd gTv8nv],skp.0

ใช่... รักใครชอบใครให้บอก แต่รหัสผ่านของคุณอย่าบอกใครเลย ยิ่งถ้าเกี่ยวข้องกับความเป็นส่วนตัว หรือเกี่ยวข้องกับเรื่องเงินๆทองๆแล้ว เก็บไว้ในใจของคุณเองก็น่าจะดีกว่า คุณเห็นด้วยมั้ย?

ลองเอาไปใช้ดูนะครับ



สิ่งที่ไม่แนะนำให้แชร์ในโลกออนไลน์

เผยข้อมูลส่วนตัว

การเปิดเผยที่อยู่จริง เป็นเรื่องที่อันตรายมาก ใครที่ประสงค์ร้ายอาจเข้าใกล้คุณได้มากขึ้น การเปิดเผยเบอร์โทร อายุ วันเกิด

ผลสำรวจบอกไว้ว่า ผู้คนมักจะเอาข้อมูลเหล่านั้นไปตั้ง Password กัน หรือเอาไปตั้งสำหรับคำถามรักษาความปลอดภัยของข้อมูล Security Question

ถ่ายส่วนหนึ่งของตัวบ้าน

เหมือนกับการแชร์ว่า “บ้านเราอยู่ไหน” แต่อันตรายมากกว่าเยอะ อย่าไปคิดว่า “การถ่ายภาพหรือ Live ในบ้านโชว์คนในโซเชียลว่า จัดบ้านใหม่ รีโนเวทบ้าน นั้นจะไม่เป็นอะไร” เพราะ การโชว์ภายในตัวบ้านให้เห็นเหมือนอนุญาตให้โจรเข้ามาแล้วทำให้พวกนั้นรู้มุมต่างๆ ของบ้านเรา ยิ่งไปกว่านั้นอาจพบเห็นของมีค่าที่อยู่ภายในบ้าน สร้างสิ่งล่อตาล่อใจให้กับโจรไปอีก

ตั๋วเครื่องบิน

ทำไมอะ ก็กำลังจะไปเที่ยวต่างประเทศก็ต้องอวดให้โลกรู้หน่อย คิดแบบนั้นไม่ได้เลย อันตรายกว่าที่เราคิดเยอะ เพราะ มิจฉาชีพสามารถใช้โปรแกรมตรวจบาร์โค้ดของตั๋วเครื่องบิน ซึ่งทำให้เข้าถึงข้อมูลส่วนตัวได้อย่างง่ายดาย บัตรเครดิตชนิดใด เดินทางไปที่ไหน ชื่อ-นามสกุลที่ปรากฏบนตั๋วเครื่องบิน และ สามารถยกเลิกตั๋วเครื่องบินได้

หนังสือเดินทาง

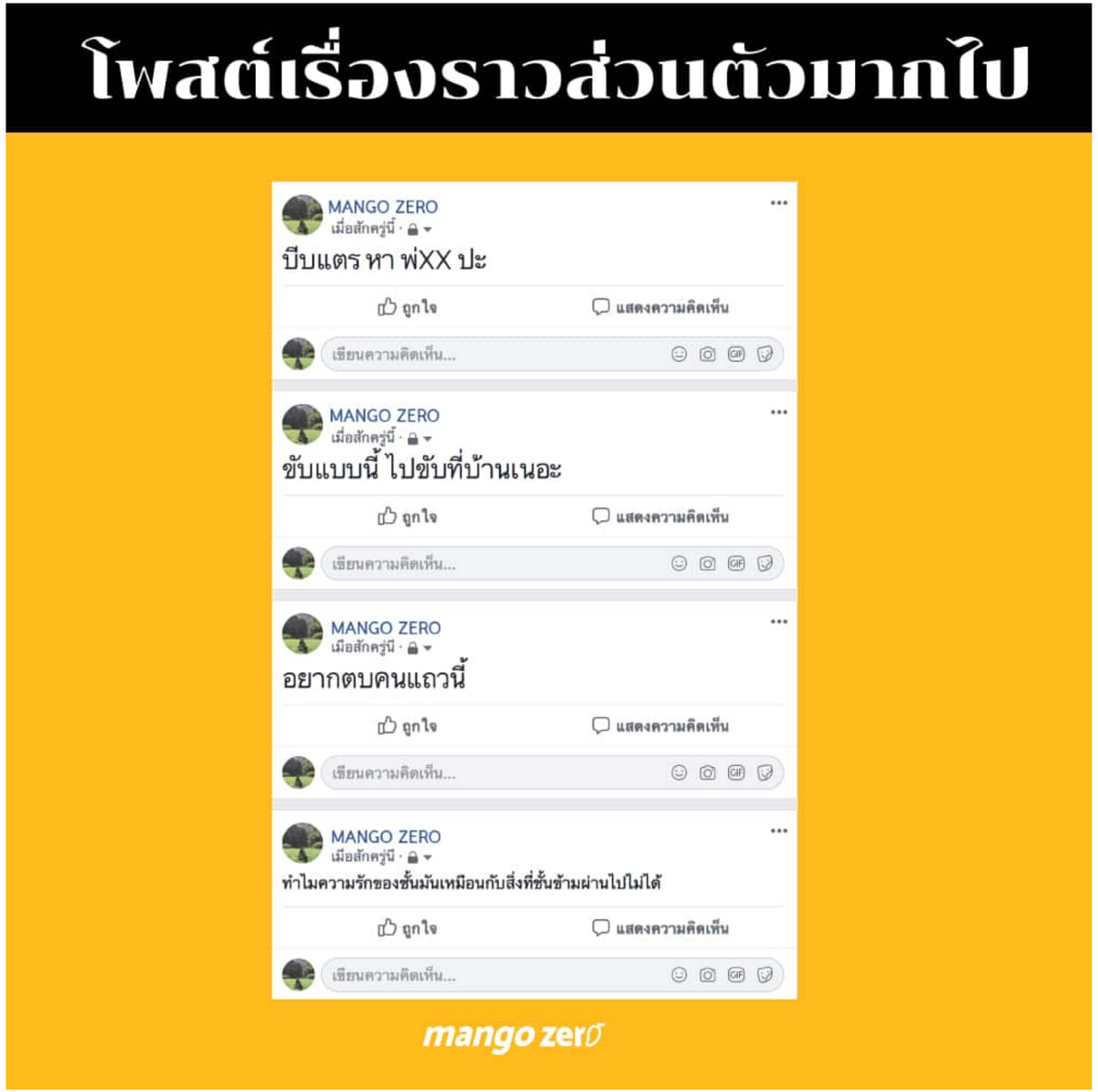
หนังสือเดินทางก็เหมือนกับบัตรประชาชน เพราะ มีข้อมูลของ ชื่อ นามสกุลเรา วันเดือนปีเกิด อายุ สัญชาติ และ เลข Passport เพราะมีสิทธิที่ผู้ไม่หวังดีจะใช้ช่องทางนี้ในการปลอมแปลง Passport ของเราได้

CHECK IN สถานที่

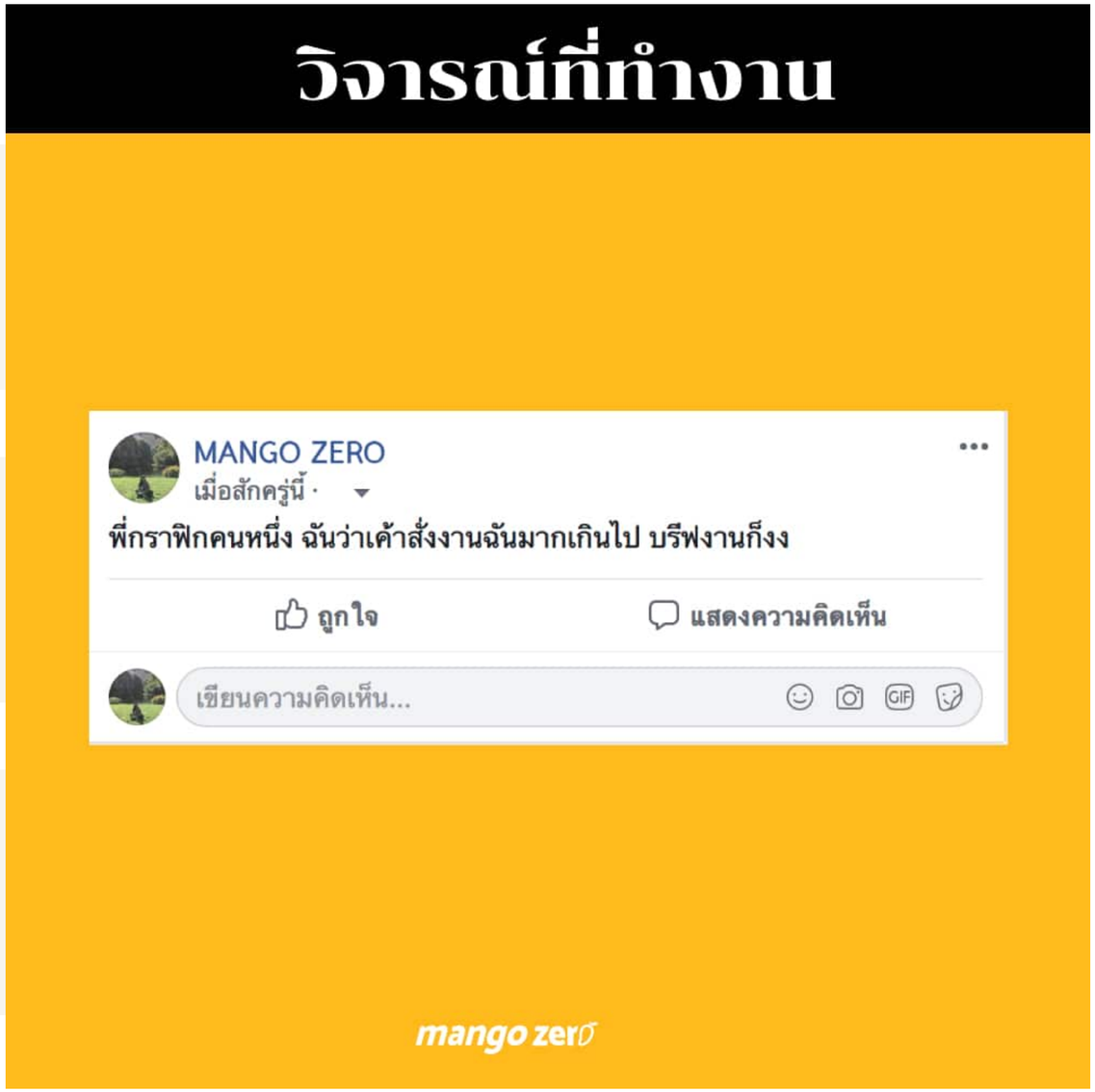
ไปเที่ยวไหน เราก็อยากสร้างความทรงจำด้วยการ Check in หน่อยว่าตอนนี้เราอยู่ที่ไหน ซึ่งบอกเลยว่าอันตรายมาก เพราะ มันแสดงให้รู้ว่าคุณอยู่ที่ไหน คนที่ไม่หวังดีอาจจะง่ายขึ้นในการเข้าถึงตัวคุณ หรือ ที่แย่ไปกว่านั้นคือ โจรไปขึ้นบ้านคุณในขณะที่คุณไปเที่ยวอยู่

โพสต์เรื่องราวตัวเองมากเกินไป

จริงอยู่ว่าพื้นที่ของเรา เราจะแชร์อะไรออกไปก็ได้ แต่การที่เราโพสต์เรื่องราวของตัวเองบ่อย และ ถี่ เต็มไปเรื่องราวดราม่า ร้ายกว่านั้นคือ หยาบคายด้วย ก็จะเป็นการสร้างภาพลักษณ์ที่ลบให้กับตัวคุณเอง สร้างความน่ารำคาญให้กับคนรอบข้างด้วย มีผลต่อการสมัครงาน (ถ้าบริษัทแอบเข้ามาเช็คประวัติเราก่อนนะ) สิ่งที่ควรทำคือ ต้องมีสติ และ ยับยั้งอารมณ์ชั่ววูบที่มักจะเกิดขึ้นบ่อยๆ เวลามีอารมณ์โกรธ โมโห อย่าพิมพ์เมื่อกำลังโกรธ เพราะ จะเสียใจในภายหลัง



วิจารณ์ที่ทำงาน



เป็นการสร้างภาพลักษณ์แย่ๆ ให้กับตัวคุณเอง การที่คุณเม้าส์ หรือ บ่นเรื่องราวในที่ทำงาน มันต้องมีสักคนในที่ทำงานบ้างแหละเอาเรื่องราวไปบอก หรือ ที่ร้ายกว่านั้นคือ เจ้านายหรือเพื่อนร่วมงานของคุณมาเห็นเอง มันจะสร้างสถานการณ์ที่น่าอึดอัดของคุณอย่างมากเมื่ออีกฝ่ายรู้เรื่องแล้ว มองหน้ากันไม่ติด ความสัมพันธ์เลวร้ายลงไป จนถึงขั้นลาออกจากงานก็เป็นไปได้ ดังนั้นถ้าจะวิจารณ์ “ตั้งค่าก่อน” ไม่ให้คนที่ทำงานเห็นก็ดีนะ

ข่าวปลอม

“ตั้งสติก่อนแชร์” ดูก่อนว่าข่าวที่เห็นในโซเชียลนั้นเป็นเรื่องจริงหรือไม่ น่าเชื่อถือแค่ไหน มีที่มาอย่างไร เพราะการแชร์ข่าวสารที่ปลอมออกไป อาจเป็นการสร้างการตื่นตระหนก ทำให้คนที่พบเห็นเกิดการเข้าใจผิดได้ ดังนั้น “ไม่ชัวร์ อย่าแชร์”

เทคนิคการซื้อของออนไลน์ไม่ให้โดนโกง

กรณีศึกษา

ปลายปี 2021 มีข่าวเด็ก ม.2 ซื้อโทรศัพท์มือถือผ่าน IG แล้วถูกโกง ทำให้เครียด จนเส้นเลือดในสมองแตก เสียชีวิต

เลือกร้านค้าที่น่าเชื่อถือ และอย่าเห็นแก่ของถูกเกินไป

โดยการดูว่าร้านมีลูกค้าเคยซื้อของจากร้านนี้มากน้อยแค่ไหน เสียงตอบรับจากรีวิวผู้ซื้อ การจดทะเบียนพาณิชย์ของร้านค้า ระยะเวลาในการเปิดดำเนินการ ต่าง ๆ เหล่านี้จะเป็นตัวช่วยสกรีนในเบื้องต้นถึงความปลอดภัยว่าคุณจะมีโอกาสถูกหลอกน้อยมาก

****ที่สำคัญควรหลีกเลี่ยงการซื้อผ่านเฟสบุ๊กไลน์ หรือไอจีส่วนตัวโดยไม่มีหน้าร้าน

เดี๋ยวอ.พาเข้าดูใน SHOPEE

เว็บไซต์ไหนปลอดภัยให้ดูจาก URL

เว็บไซต์ขายของออนไลน์ที่ขึ้นต้นด้วย https:// คือเว็บที่ปลอดภัย บวกกับไอคอนรูปแม่กุญแจด้านหน้า ถ้าเห็นสัญลักษณ์ดังกล่าวก็สามารถอุ่นใจได้เลยว่าสั่งซื้อสินค้าแล้วจะมีการเชื่อมต่อแบบ Secure Sockets Layer (SSL) ซึ่งจะไม่โดนหลอกอย่างแน่นอน

ระวังเรื่อง Wi-Fi สาธารณะตอนจ่ายเงิน

การสั่งซื้อสินค้าออนไลน์ผ่านการเชื่อมต่อ Wi-Fi สาธารณะ มีความเสี่ยง เนื่องจากเครือข่ายเหล่านี้สามารถถ่ายเทข้อมูลได้ง่ายโดยเฉพาะข้อมูลบัตรเครดิต แนะนำให้ใช้เน็ตมือถือหรือ Wi-Fi จากที่บ้านปลอดภัยกว่า

เป็นไปได้อย่าให้ระบบจดจำหมายเลขบัตร Debit หรือ Credit และควรตรวจสอบบิลบัตรเครดิตอยู่เสมอ

เก็บหลักฐานการโอนเงินให้ครบ

หลังจากทำการโอนเงินเรียบร้อยแล้ว ควรเก็บหลักฐานการโอนเงิน หลักฐานการชำระเงินซื้อสินค้า หรือแคปเจอร์หน้าจอประวัติการสนทนาซื้อขายไว้ให้ครบ ที่สำคัญคือ ชื่อ-นามสกุล เลขบัญชีของผู้ขาย ชื่อของร้านค้า เบอร์ติดต่อ เผื่อว่าในอนาคตอาจจำเป็นต้องใช้

ตอบคำถามชิงรางวัล

จาก อ.นัท