สสย.
ศูนย์ส่งเสริมสื่อเด็กและเยาวชน
สถาบันสื่อเด็กและเยาวชน

สสส
สำนักงานกองทุนสนับสนุน
การสร้างเสริมสุขภาพ

# การรักษาความปลอดภัย บนโลกไซเบอร์

## Cybersecurity

# การรักษาความปลอดภัยบนโลกไซเบอร์

# (Cybersecurity)

โลกดิจิทัลได้เปลี่ยนวิถีชีวิตของผู้คนในยุคปัจจุบันในหลายๆ ด้าน เช่น วิธีการติดต่อกับเพื่อนและคนรู้จัก การทำธุรกรรมทางการเงิน การซื้อขายสินค้า และการรับชมสันทนาการความบันเทิงต่างๆ แต่อย่างไรก็ตามโลกไซเบอร์ซึ่งรวมถึง อินเทอร์เน็ต เครือค่ายสังคมออนไลน์ โทรศัพท์มือถือ เกมออนไลน์ แอปพลิเคชั่น และอื่นๆ ยังมีภัยคุกคามที่แฝงมากับความสะดวกสบายและความบันเทิงเหล่านี้ด้วย การเข้าใจ 3 แนวคิดสำคัญต่อไปนี้ช่วยให้ผู้ใช้งานรับมือและจัดการภัยคุกคามบนโลกไซเบอร์ได้ดียิ่งขึ้น

**1) การรักษาความเป็นส่วนตัวในโลกออนไลน์ (Online Privacy)**

**2) การจัดการรอยเท้าดิจิทัล (Digital Footprint Management)**

**3) การรักษาความปลอดภัยทางดิจิทัล (Digital Security Management)**

## การรักษาความเป็นส่วนตัวในโลกออนไลน์

ความเป็นส่วนตัวในโลกออนไลน์ คือสิทธิการปกป้องข้อมูลความส่วนตัวในโลกออนไลน์ของผู้ใช้งานที่บุคคลหรือหน่วยงานอื่นจะนำไปจัดเก็บ นำไปใช้ประโยชน์ หรือนำข้อมูลนั้นไปเผยแพร่ ในปัจจุบันส่วนหนึ่งของข้อมูลส่วนตัวของเราได้ถูกจัดเก็บไว้โดยผู้ให้บริการโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ต และผู้ให้บริการสื่อสังคมออนไลน์ ซึ่งมีนโยบายด้านความเป็นส่วนตัวของผู้ใช้งานในระดับหนึ่ง แต่ปัญหาอาจจะเกิดขึ้นได้หากข้อมูลส่วนตัวของเราตกไปอยู่ในมือของผู้ที่ไม่น่าไว้ใจ ข้อมูลส่วนตัวของผู้ใช้งานอินเทอร์เน็ตอาจถูกละเมิดได้ ในกรณีต่อไปนี้

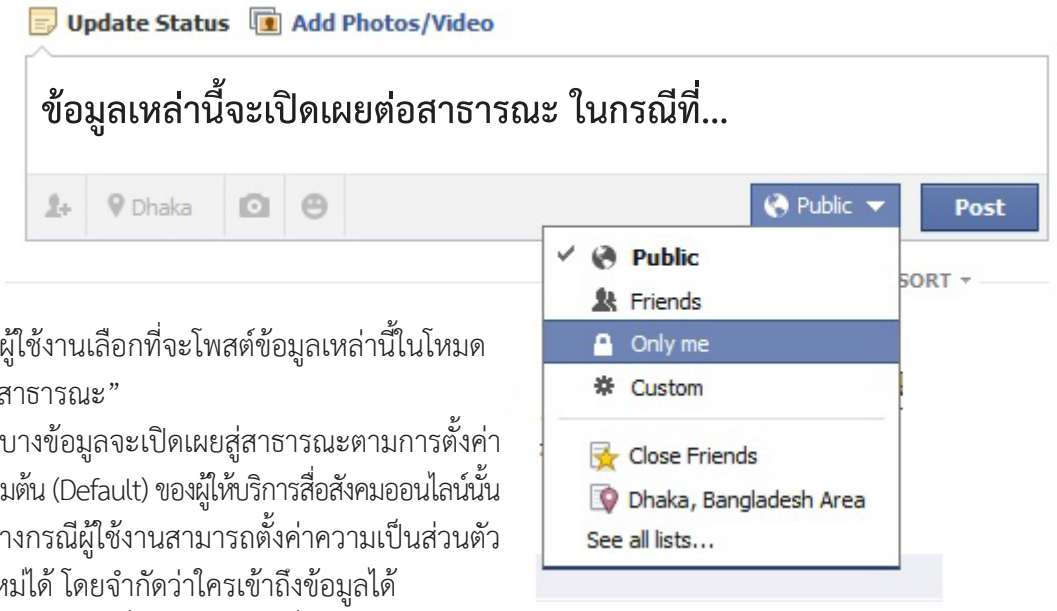
## ผู้ใช้งานอินเทอร์เน็ต ถูกติดตามความเคลื่อนไหวออนไลน์ได้อย่างไร

เมื่อผู้ใช้งานเข้าสู่โลกออนไลน์ ข้อมูลของผู้ใช้งานจะถูกบันทึกไว้ตลอดเวลา ขั้นตอนในการติดตามกิจกรรมออนไลน์ของผู้ใช้งานมีขั้นตอนดังนี้

# การรักษาความเป็นส่วนตัว ในสื่อสังคมออนไลน์

สื่อสังคมออนไลน์มีระบบการตั้งค่าความเป็นส่วนตัวให้ผู้ใช้ปรับเปลี่ยนให้เข้ากับตัวผู้ใช้งาน ข้อมูลที่สื่อสังคมออนไลน์จัดเก็บมี 2 ประเภทคือ

1 **ข้อมูลที่ผู้ใช้งานแชร์ลงสื่อออนไลน์** สื่อสังคมออนไลน์ไม่จัดเก็บข้อมูลของผู้ใช้งานไว้ในคอมพิวเตอร์ของผู้ใช้ แต่เก็บไว้ในที่เก็บข้อมูลของผู้ให้บริการแทน ข้อมูลเหล่านี้ได้แก่

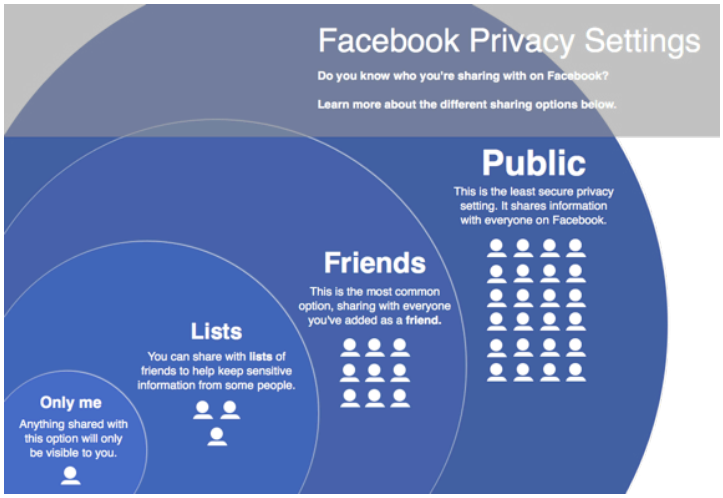



• ผู้ใช้งานเลือกที่จะโพสต์ข้อมูลเหล่านี้ในโหมด “สาธารณะ”

• บางข้อมูลจะเปิดเผยสู่สาธารณะตามการตั้งค่าเริ่มต้น (Default) ของผู้ให้บริการสื่อสังคมออนไลน์นั้น บางกรณีผู้ใช้งานสามารถตั้งค่าความเป็นส่วนตัวใหม่ได้ โดยจำกัดว่าใครเข้าถึงข้อมูลได้

• ผู้ติดต่อคนอื่นของผู้ใช้งานที่ได้รับอนุญาตสามารถบันทึกและแบ่งบันข้อมูล เช่น รูปภาพของผู้ใช้งานได้ โดยไม่จำเป็นต้องได้รับอนุญาตจากผู้ใช้งาน

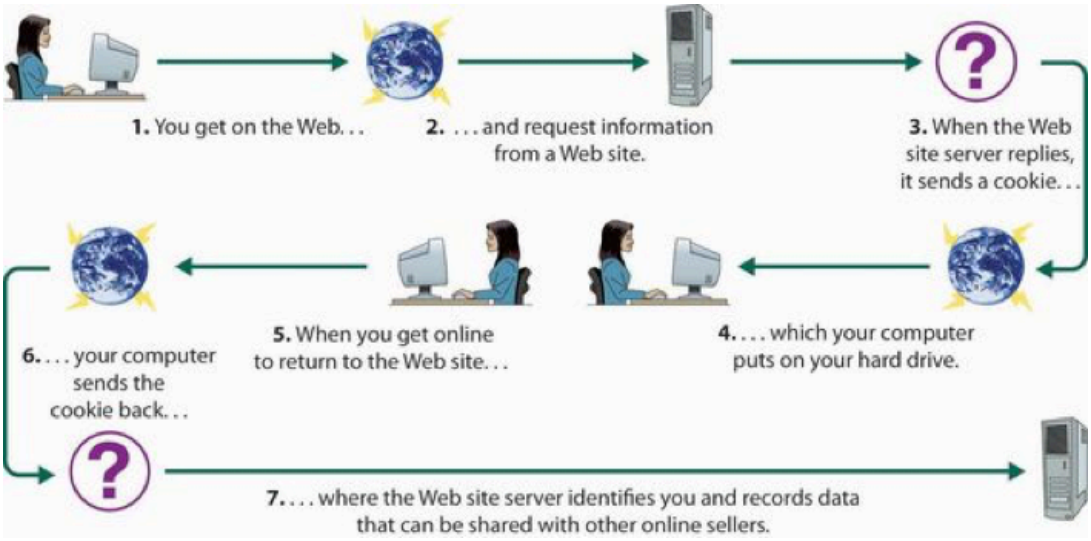
• แอปพลิเคชั่นภายนอก (Third-party applications) ที่ได้รับอนุญาตจากผู้ใช้งานสามารถเข้าถึงข้อมูลที่ผู้ใช้งานโพสต์ในโหมดความเป็นส่วนตัวได้




*(https://www.gcflearnfree.org/facebook101/understanding-facebook-privacy/1/ : สืบค้นข้อมูล 3 มีนาคม 2561)*

อย่างไรก็ตาม ผู้ให้บริการสื่อสังคมออนไลน์ไม่อาจรับประกันความปลอดภัยของข้อมูลส่วนตัวของผู้ใช้งานได้ แม้ว่าผู้ใช้งานจะตั้งค่าความเป็นส่วนตัวไว้แล้วก็ตาม เนื่องจากภัยคุกคามในโลกออนไลน์มีหลายรูปแบบ

**2. ข้อมูลที่จัดเก็บผ่านระบบการสะกดรอยทางอิเลคทรอนิค** (Electronic Tracking) ข้อมูลความเคลื่อนไหวออนไลน์ของผู้ใช้จะถูกจัดเก็บไว้ใน*ระบบคุกกี้* ซึ่งจะสะกดรอยผู้ใช้งานจากเว็บหนึ่งไปสู่อีกเว็บหนึ่ง




*(https://www.pinterest.com/pin/74450200065869858/ : สืบค้นข้อมูล 3 มีนาคม 2561)*

# ใครเข้าถึงข้อมูลของผู้ใช้งาน ในสื่อสังคมออนไลน์ได้บ้าง

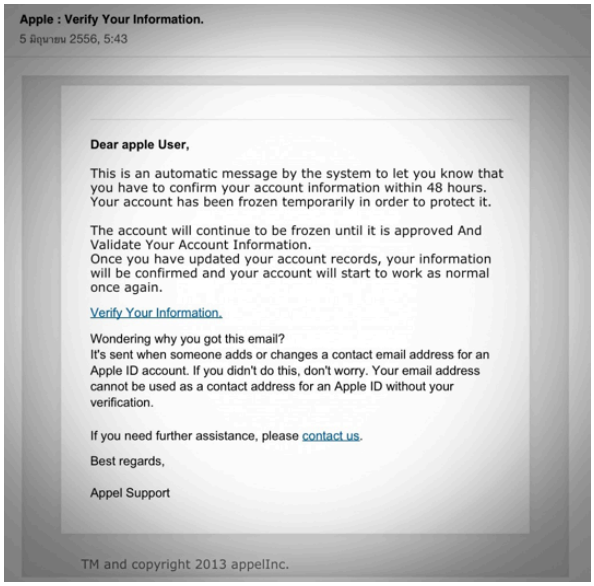
1 องค์กรซึ่งต้องการรวบรวมข้อมูลส่วนตัวของผู้ใช้งานที่ได้รับอนุญาตตามกฎหมาย

- บริษัทขายสินค้าและบริการซึ่งสนใจข้อมูลส่วนตัวของผู้ใช้งาน เพื่อที่จะเลือกกลุ่มเป้าหมายได้ตรงกับสินค้าและบริการของบริษัท
- ผู้พัฒนาซอฟต์แวร์ที่ร่วมมือกับสื่อสังคมออนไลน์ เพื่อที่จะพัฒนาแอปที่ตรงกับความต้องการของผู้ใช้งาน

2 บุคคลซึ่งต้องการรวบรวมข้อมูลส่วนตัวของผู้ใช้งานที่ไม่ได้รับอนุญาตตามกฎหมาย

- มิจฉาชีพที่มุ่งโจรกรรมอัตลักษณ์ของผู้ใช้งานโดยการรวบรวมสิ่งที่ผู้ใช้งานโพสต์และสิ่งที่คนอื่นโพสต์เกี่ยวกับผู้ใช้งาน
- ผู้ไม่หวังดีในโลกไซเบอร์อื่นๆ เช่น ผู้ที่หวังจะคุกคามผู้ใช้งาน หรือต้องการที่จะเจาะระบบ หรือปล่อยไวรัสคอมพิวเตอร์

ดังเช่นกรณีที่มิจฉาชีพส่งอีเมลไปยังผู้ใช้งานอุปกรณ์ของบริษัท Apple เพื่อหลอกลวงโดยแจ้งเตือนให้ผู้ใช้งานยืนยันรหัสประจำตัว (ID) ตามลิ้งก์ที่แจ้งไว้ในอีเมล ซึ่งหากเหยื่อหลงเชื่อ มิจฉาชีพก็จะเข้าถึงข้อมูลบัตรเครดิตของเจ้าของบัญชีได้อย่างง่ายดาย



**Apple : Verify Your Information.**

5 มิถุนายน 2556, 5:43

**Dear apple User,**

This is an automatic message by the system to let you know that you have to confirm your account information within 48 hours. Your account has been frozen temporarily in order to protect it.

The account will continue to be frozen until it is approved And Validate Your Account Information.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

Verify Your Information.

Wondering why you got this email?
It's sent when someone adds or changes a contact email address for an Apple ID account. If you didn't do this, don't worry. Your email address cannot be used as a contact address for an Apple ID without your verification.

If you need further assistance, please contact us.

Best regards,

Appel Support

TM and copyright 2013 appelInc.

*(https://tech.mthai.com/tips-technic/27699.html : สืบค้นข้อมูล 3 มีนาคม 2561)*

3 โฆษณาที่เลือกกลุ่มเป้าหมายตามพฤติกรรมการใช้สื่อออนไลน์ สื่อสังคมออนไลน์ที่ให้บริการโดยไม่ได้เก็บค่าสมาชิกจากผู้ใช้งานจะมีรายได้จากการขายโฆษณาที่ขึ้นบนหน้าฟีดของสื่อสังคมออนไลน์ (behavior advertising) สื่อสังคมออนไลน์จะเก็บข้อมูลของผู้ใช้งานที่มีแนวโน้มและศักยภาพในการการซื้อสินค้าและบริการ บริษัทผู้ผลิตยินดีที่จะได้ข้อมูลเหล่านี้เพื่อจะได้เข้าถึงกลุ่มเป้าหมาย ในขณะที่ผู้ใช้งานอาจจะรู้สึกสะดวกที่ได้เห็นโฆษณาที่ตรงกับความสนใจของตนเองขณะที่ใช้สื่อสังคมออนไลน์นั้นๆ

4 แอปพลิเคชั่นภายนอก (Third-party applications) บนเครือข่ายสังคมออนไลน์ แอปเหล่านี้คือโปรแกรมที่สามารถเชื่อมต่อกับสื่อสังคมออนไลน์ แต่ไม่ได้เป็นส่วนหนึ่งของสื่อสังคมออนไลน์ โดยมีรูปแบบต่างๆ เช่น

- เกมที่ผู้ใช้จะเล่นกับรายชื่อผู้ติดต่อ
- โพลหรือคำถามออนไลน์
- ซอฟต์แวร์ที่ยินยอมให้ผู้ใช้งานโพสต์ลงสื่อสังคมออนไลน์โดยผ่านแอปพลิเคชั่นในมือถือ

เพื่อที่จะให้แอปหล่านี้ใช้งานได้ สื่อสังคมออนไลน์จะยินยอมให้นักพัฒนาแอปเข้าถึงข้อมูลของผู้ใช้งานในส่วนที่เป็นสาธารณะ แอปพลิเคชั่นภายนอกเหล่านี้ยังสามารถเข้าถึงข้อมูลส่วนตัวของผู้ใช้งานได้ หากว่าได้รับการยินยอมจากผู้ใช้งาน แต่ผู้ใช้งานไม่อาจทราบได้ถึงขอบเขตการเข้าถึงข้อมูลส่วนตัวเมื่อยินยอมให้แอปพลิเคชั่นภายนอกได้เข้าไปแล้ว นอกจากนั้นแอปเหล่านี้ไม่จำเป็นต้องปฏิบัติตามนโยบายความเป็นส่วนตัวของสื่อสังคมออนไลน์ที่ผู้ใช้งานได้ยินยอมให้แอปเหล่านี้เชื่อมต่อด้วย

# การจัดการรอยเท้าดิจิทัล

รอยเท้าดิจิทัลคือ ร่องรอยการกระทำต่าง ๆ ที่ฝังไว้และติดตามได้ เมื่อผู้ใช้งานสื่อดิจิทัลหรืออินเทอร์เน็ต ได้กระทำการใดๆ ในโลกดิจิทัล เช่น การใช้งานกล้องดิจิทัล สมาร์ตโฟน แท็บเล็ต และคอมพิวเตอร์ รอยเท้าดิจิทัลจะบันทึกข้อมูลของผู้ใช้งาน คือชื่อ และข้อมูลส่วนตัว เช่น วันเกิด ที่อยู่ รอยเท้าดิจิทัล สามารถบอกให้ผู้อื่นทราบถึงสิ่งที่เราชอบ สิ่งที่สนใจ และสิ่งที่เราอยากทำ ข้อมูลบางอย่างเป็นเรื่องที่เราพอที่จะทราบว่าเราได้ทิ้งร่อยรอยไว้ ในขณะที่บางอย่างเราไม่เคยทราบมาก่อนเลยว่าได้ถูกบันทึกไว้ รอยเท้าดิจิทัลมี 2 ประเภทคือ

**1. Active Digital Footprints** รอยเท้าดิจิทัลที่ผู้ใช้งานเจตนาบันทึกไว้ในโลกออนไลน์ เช่น

สิ่งที่เราพูดหรือโพสต์ลงในอีเมลหรือในสื่อสังคมออนไลน์

สิ่งที่เรากดไลค์ รีทวิต หรือแชร์

ที่ตั้งสถานที่ที่เราอยู่หรือเคยไป

**2. Passive Digital Footprints** รอยเท้าดิจิทัลที่ผู้ใช้งานไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ เช่น

สิ่งที่เราเคยคลิกเข้าไป

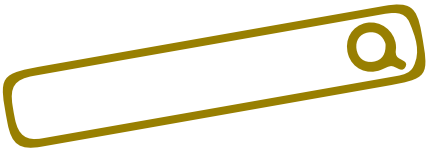
ประวัติการค้นหาในโลกออนไลน์

การซื้อสินค้าออนไลน์ของเรา


IP address ของเรา

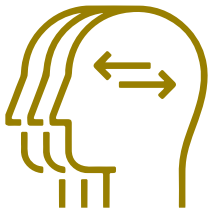
การเปิดระบบ GPS ของเรา

# รอยเท้าดิจิทัลสำคัญอย่างไร

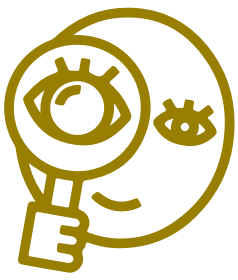


ช่วยให้เราสะดวกและประหยัดเวลามากขึ้นเวลาเรากรอกข้อมูลส่วนตัวลงในช่องว่างของหน้าเว็บไซต์ เราไม่ต้องพิมพ์ใหม่ เพราะรอยเท้าดิจิทัลได้บันทึกข้อมูลเราไว้ก่อนแล้ว รอยเท้าดิจิทัลจึงเหมือนสมุดบันทึกที่สะท้อนให้เห็นถึงกิจกรรมออนไลน์ของผู้ใช้งาน

รอยเท้าดิจิทัลสามารถบอกข้อมูลเกี่ยวกับบุคลิกของผู้ใช้งานได้มากมาย เช่น รูปภาพแบบไหนที่ผู้ใช้งานกดถูกใจ และนิสัย รสนิยมต่างๆ แต่ละคนใช้รอยเท้าดิจิทัลด้วยเหตุผลที่แตกต่างกันออกไป บางคนใช้รอยเท้าดิจิทัลเพื่อบ่งบอกให้คนอื่นทราบว่าตัวเขาเองเป็นคนอย่างไร มีรสนิยมอย่างไร



ร้านค้าอาจใช้รอยเท้าดิจิทัลเพื่อเสนอขายสินค้าที่ผู้ใช้งานเพิ่งค้นหาในกูเกิ้ล หรือบริษัทอาจใช้เพื่อตรวจสอบประวัติก่อนรับพนักงานใหม่เข้ามาทำงาน



# ปัญหาของรอยเท้าดิจิทัล

รอยเท้าดิจิทัลอาจจะดูเหมือนไม่มีพิษภัยใดๆ แต่อย่างไรก็ตาม ร่องรอยนี้จะไม่หายไป และจะคงอยู่ตลอด และสามารถติดตามร่องรอยได้ แม้ผู้ใช้งานจะปิดเว็บไซต์หรือออกจากบัญชีการใช้งานไปแล้ว ดังนั้นในวันข้างหน้า ร่องรอยนี้อาจส่งผลดีหรือผลเสียต่อผู้ใช้งานได้ รอยเท้าดิจิทัลยังทำให้เราสูญเสียความเป็นส่วนตัว เนื่องจากคนอื่นยังสามารถเห็นรอยเท้าดิจิทัลของเราได้ หรือแกะรอยได้จากดาต้าเบสที่ได้บันทึกกิจกรรมออนไลน์ของเราไว้ นอกจากนั้น บริษัทและหน่วยงานที่จัดเก็บข้อมูลของผู้ใช้งานสื่อดิจิทัลยังหาประโยชน์ทางการค้าจากรอยเท้าดิจิทัลของผู้ใช้งานอินเทอร์เน็ต โดยมอนิเตอร์รอยเท้าดิจิทัลและนำไปวิเคราะห์กลุ่มเป้าหมายทางการตลาด พฤติกรรมการใช้สื่อออนไลน์ และอื่นๆ

ผู้ใช้งานอินเทอร์เน็ตจึงควรตระหนักว่า รอยเท้าดิจิทัลเปิดเผยข้อมูลส่วนตัวของเราได้ และข้อมูลเหล่านี้จะคนอื่นสามารถที่จะ ค้นหา เผยแพร่ ทำซ้ำ ขโมย และติดตามได้เพราะร่องรอยนั้นจะไม่หายไปไหนในโลกไซเบอร์

# ความสำคัญของรอยเท้าดิจิทัล

01

**เพื่อปกป้องชื่อเสียงของผู้ใช้งาน** รอยเท้าดิจิทัลสามารถสะท้อนทั้งแง่บวกและแง่ลบของผู้ใช้งาน รอยเท้าดิจิทัลที่ไม่ดีคือเรื่องราวของเราบนอินเทอร์เน็ตที่เราไม่อยากให้ใครได้มาพบ เช่นกรณี กองประกวดนางงามของประเทศไทยเคยประกาศปลดผู้ชนะประกวดที่เพิ่งได้รับรางวัลออก เนื่องจากพบภาพและข้อความที่มีลักษณะไม่เหมาะสมที่ของเจ้าตัวในสื่ออินเทอร์เน็ต ในต่างประเทศ การมีรอยเท้าดิจิทัลในแง่ลบอาจส่งผลต่อการสมัครเข้ามหาวิทยาลัย หรือเข้าทำงานในบริษัทได้

02

**เพื่อช่วยตัดสินใจว่าควรจะจัดการข้อมูลส่วนตัวของผู้ใช้งานอย่างไร** การเปิดเผยข้อมูลส่วนตัวของผู้ใช้งานสามารถจำกัดขอบเขตได้ว่าใครควรจะได้เห็นบ้าง หรือใครควรจะไม่ได้เห็น เช่น ข้อมูลด้านสุขภาพ หรือด้านการเงิน แอปพลิเคชั่นบางตัวที่ติดตั้งบนโทรศัพท์ก็สามารถเข้าถึงข้อมูลส่วนตัวของผู้ใช้งานได้เช่น ภาพถ่าย เบอร์โทรศัพท์ รายชื่อผู้ติดต่อ ผู้ใช้งานควรระมัดระวังหากข้อมูลส่วนตัวนี้รั่วไหลไปยังบุคคลที่สาม เช่นเคยพบว่า แอปทำนายชื่อ ดูดวง หาคู่ บางตัวต้องการเข้าถึงข้อมูลส่วนตัวของผู้ใช้งานเกินความจำเป็น และอาจใช้ข้อมูลนั้นสวมรอยบัญชีสังคมออนไลน์ของผู้ใช้งานได้

03

**เพื่อปกป้องการสูญเสียทรัพย์สิน** การขโมยข้อมูลทางดิจิทัลเป็นอีกช่องทางหนึ่งที่เหล่ามิจฉาชีพใช้ในการหลอกลวงและทำให้เหยื่อสูญเสียเงินเป็นอันมาก การโพสต์ภาพของมีค่าในบ้านของผู้ใช้งานลงสื่อสังคมออนไลน์ ก็อาจเป็นการอันตรายต่อความปลอดภัยของทรัพย์สินได้

04

**เพื่อรักษาอิสรภาพและความเป็นส่วนตัว** เนื่องจากการก่อการร้ายในบางประเทศเป็นเรื่องอ่อนไหว รัฐบาลบางประเทศสอดส่องสิ่งที่ผู้ใช้งานโพสต์ลงอินเทอร์เน็ต การวิพากษ์วิจารณ์รัฐบาลด้วยถ้อยคำที่รุนแรงอาจทำให้ผู้ใช้งานถูกทางการจับตาเป็นพิเศษ ผู้ใช้งานอาจได้รับข้อความสแปมหรือการส่งอีเมลที่มีข้อความโฆษณาไปให้โดยไม่ได้รับอนุญาตจากผู้รับที่อาจสร้างความรำคาญจากผู้ขายสินค้าและบริการ หากแชร์ข้อมูลส่วนตัวของผู้ใช้งานผ่านแอปพลิเคชั่นช็อปปิ้งออนไลน์ ในประเด็นความเป็นส่วนตัวของบุคคลอื่นก็เช่นกัน การเผยแพร่ข้อมูลส่วนตัวของเด็ก หรือการโพสต์ภาพของเด็กในสื่อสังคมออนไลน์ที่มีการแชร์ตำแหน่งของที่ตั้ง อาจทำให้เด็กอาจไม่ปลอดภัยจากผู้แสวงหาประโยชน์ได้ นอกจากนั้นการโพสต์ภาพหรือคลิปที่มีผลต่อความรู้สึกและสภาพจิตใจของเด็กอาจเข้าข่ายการละเมิดสิทธิเด็กได้

# การรักษาความปลอดภัยในทางดิจิทัล

การรักษาความปลอดภัยในทางดิจิทัลคือ การปกป้องระบบและอุปกรณ์ดิจิทัลจากการบุกรุกโดยผู้ใช้ภายนอก และจากความผิดพลาดของระบบที่เกิดจากผู้ให้บริการ การพัฒนาของเทคโนโลยีดิจิทัลและระบบออนไลน์ทำให้ผู้ใช้งานต้องบันทึกข้อมูลส่วนตัวลงในอุปกรณ์ดิจิทัลซึ่งอุปกรณ์เหล่านี้นับวันจะเชื่อมต่อถึงกันมากยิ่งขึ้น ทั้งในอินเทอร์เน็ต ในสื่อสังคมออนไลน์และในแอปพลิเคชั่นที่เราใช้ในชีวิตประจำวัน จึงมีความเสี่ยงด้านความปลอดภัยมากขึ้น การรักษาความปลอดภัยทางดิจิทัลจึงมีความสำคัญดังนี้

**1. เพื่อรักษาความเป็นส่วนตัวและความลับ** หากไม่ได้รักษาความปลอดภัยให้กับอุปกรณ์ดิจิทัล ข้อมูลส่วนตัวและข้อมูลที่เป็นความลับอาจจะรั่วไหลหรือถูกโจรกรรมได้

**เพื่อป้องกันการขโมยอัตลักษณ์** การขโมยอัตลักษณ์เริ่มมีจำนวนที่มากขึ้นในยุคข้อมูลข่าวสาร เนื่องจากมีการทำธุรกรรมทางออนไลน์มากยิ่งขึ้น ผู้คนเริ่มทำการชำระค่าสินค้าผ่านสืออินเทอร์เน็ตและทำธุรกรรมกับธนาคารทางออนไลน์ หากไม่มีการรักษาความปลอดภัยที่เพียงพอมิจฉาชีพอาจจะล้วงข้อมูลเกี่ยวกับบัตรเครดิตและข้อมูลส่วนตัวของผู้ใช้งานไปสวมรอยทำธุรกรรมได้ เช่น ไปซื้อสินค้า กู้ยืมเงิน หรือสวมรอยรับผลประโยชน์และสวัสดิการ

**เพื่อป้องกันการโจรกรรมข้อมูล** เนื่องจากข้อมูลต่างๆ มักเก็บรักษาในรูปของดิจิทัล ไม่ว่าจะเป็นเอกสาร ภาพถ่าย หรือคลิปวีดิโอ ข้อมูลเหล่านี้อาจจะถูกโจรกรรมเพื่อนำไปขายต่อ แบล็คเมล์ หรือเรียกค่าไถ่

**เพื่อป้องกันความเสียหายของข้อมูลและอุปกรณ์** ภัยคุกคามทางไซเบอร์อาจส่งผลเสียต่อข้อมูลและอุปกรณ์ดิจิทัลได้ ผู้ไม่หวังดีบางรายอาจมุ่งหวังให้เกิดอันตรายต่อข้อมูลและอุปกรณ์ที่เก็บรักษามากกว่าที่จะโจรกรรมข้อมูลนั้น ภัยคุกคามอย่างไวรัสคอมพิวเตอร์ โทรจัน และมัลแวร์สร้างความเสียหายร้ายแรงให้กับคอมพิวเตอร์หรือระบบปฏิบัติการได้

# ประเภทของภัยคุกคามทางไซเบอร์

## พบว่าปี 2560

ปริมาณการโจมตีทางไซเบอร์
ทั่วโลกเพิ่มขึ้น **24%**

โดยการโจมตีในลักษณะที่เป็นการแพร่
กระจายมัลแวร์ผ่านอีเมล
ฟิชชิ่ง (Phishing) มีสูงถึง **67%**


ซึ่งส่วนใหญ่มักเป็นการหลอกให้คลิกลิงก์หรือเปิดไฟล์แนบที่มีสคริปต์อันตรายฝังอยู่ ผู้ใช้งานอุปกรณ์ดิจิทัลและสื่อออนไลน์จึงควรทำความรู้จักภัยคุกคามประเภทต่างๆ เพื่อจะได้ป้องกันและแก้ไข

**1. Malicious Software** หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ดังนั้นผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

- **Virus** มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่นๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- **Worm** สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

• **Trojan** หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริงๆแล้วจะทำให้เกิดความเสียหาย เมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย

• **Backdoor** เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว

• **Spyware** แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย

• **Ransomware** ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

• **Scareware** เป็นโปรแกรมที่ถูกเขียนขึ้น เพื่อทำให้ผู้ใช้งานคอมพิวเตอร์เข้าใจว่า เครื่องคอมพิวเตอร์ของตัวเองมีไวรัส โดยมักมีการแจ้งเตือนว่าพบไวรัสในเครื่องคอมพิวเตอร์ ทำให้ผู้ใช้หลงเชื่อให้ข้อมูลบัตรเครดิต ซื้อหรือดาวน์โหลดซอฟต์แวร์ เพื่อกำจัดไวรัสนั้น ซึ่งซอฟต์แวร์ดังกล่าวเป็นซอฟต์แวร์ปลอมที่ส่งผลให้เกิดอันตรายต่อความปลอดภัยของข้อมูลส่วนตัวและคอมพิวเตอร์ของผู้ใช้

• **Adware** หมายถึงแพ็กเกจซอฟต์แวร์ใดๆ ที่สามารถทำงาน แสดง หรือดาวน์โหลดสื่อโฆษณาโดยอัตโนมัติ ไปยังคอมพิวเตอร์ที่ได้รับการติดตั้งซอฟต์แวร์ชนิดนี้ไว้ หรือขณะที่โปรแกรมประยุกต์กำลังเรียกใช้ ซอฟต์แวร์โฆษณาบางประเภทเป็นซอฟต์แวร์สอดแนม (spyware)

**2. DoS Attack (denial-of-service attack)** หรือ distributed denial-of-service (DDoS) attack การโจมตีโดยปฏิเสธการให้บริการ เป็นความพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายสำหรับผู้ใช้เป้าหมายใช้บริการไม่ได้ เช่น ขัดขวางหรือชะลอบริการของแม่ข่ายที่เชื่อมโยงกับอินเทอร์เน็ตอย่างชั่วคราวหรือถาวร อาชญากรผู้โจมตีมักมุ่งเป้าไปยังเว็บไซต์หรือบริการซึ่งตั้งอยู่ในเว็บเซิร์ฟเวอร์ที่มีการเข้าชมสูงอย่างเช่น ธนาคาร เกตเวย์ชำระบัตรเครดิต โดยมีแรงจูงใจเบื้องหลังเป็นการแก้แค้น การแบล็กเมล์ หรือการเคลื่อนไหวทางการเมือง เป็นต้น

**3. Phishing** คือ กลลวงที่แยบยลทางอินเทอร์เน็ตซึ่งมักมาในรูปแบบของการปลอมแปลงอีเมลหรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่างๆ Phishing สามารถทำได้โดยการส่งอีเมล หรือข้อความที่อ้างว่ามาจากองค์กรต่างๆ ที่ท่านติดต่อด้วย เช่น บริษัทให้บริการอินเทอร์เน็ตหรือธนาคาร โดยส่งข้อความเพื่อขอให้ท่าน “อัปเดต” หรือ “ยืนยัน” ข้อมูลบัญชีของท่าน หากท่านไม่ตอบกลับอีเมลดังกล่าว อาจก่อให้เกิดผลเสียตามมาได้

# ข้อแนะนำในการรักษาความปลอดภัยบนโลกไซเบอร์

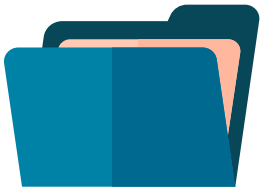
การเข้าใจแนวคิดของการปกป้องความเป็นส่วนตัวในโลกออนไลน์ รอยเท้าดิจิทัล การรักษาความปลอดภัยทางดิจิทัลช่วยป้องกันภัยคุกคามบนโลกไซเบอร์ได้ ข้อแนะนำต่อไปนี้ช่วยให้ผู้ใช้งานรักษาความปลอดภัยของข้อมูลส่วนตัวและอุปกรณ์ดิจิทัล

**1. ไม่ตั้งรหัสผ่านที่ง่ายเกินไป** รหัสผ่านเป็นกุญแจที่ไขเข้าสู่ข้อมูลและเอกสารของเรา อาชญากรไซเบอร์จะใช้วิธีการต่างๆ เพื่อที่จะเข้าผ่านเข้ารหัสให้ได้ เพื่อที่จะไม่ให้คนพวกนี้เข้าถึงได้ง่าย ควรตั้งรหัสที่ยากและซับซ้อน และไม่ควรบันทึกรหัสผ่านไว้ในอุปกรณ์ดิจิทัล

**2. ใส่ใจกับการตั้งค่าความเป็นส่วนตัว** แอปส่วนใหญ่จะมีตัวเลือกในการตั้งค่าความเป็นส่วนตัวให้แก่ผู้ใช้งาน เพื่อที่จะตัดสินใจได้ว่าข้อมูลไหนจะแบ่งปันให้ใครได้เท่าไร ทางที่ดีควรจะเลือกตั้งค่าให้มีความเป็นส่วนตัวให้มากที่สุด ระมัดระวังในการเปิดเผยชื่อและที่ตั้งของเรา และปฏิเสธแอปที่พยายามจะเข้าถึงกล้องถ่ายรูปของเรา

**3. ใส่ใจรอยเท้าดิจิทัล** สิ่งที่ผู้ใช้โพสต์ลงโลกออนไลน์แล้ว สิ่งนั้นจะคงอยู่ตลอดไป แม้ว่าโพสต์ต้นทางจะลบแล้ว คนอื่นก็จะตามร่องรอยเราจนได้ เมื่อคิดจะโพสต์ ควรโพสต์แต่เรื่องที่ดีๆ และระมัดระวังการเปิดเผยข้อมูลส่วนตัว

**4. ควรติดตั้งโปรแกรมรักษาความปลอดภัยให้กับอุปกรณ์ดิจิทัลทุกตัว** รวมถึงโทรศัพท์ด้วย เพื่อที่จะปกป้องอุปกรณ์เหล่านั้นจากภัยคุกคามในโลกไซเบอร์



**5. สำรองข้อมูลไว้เสมอ** การสำรองข้อมูลมักถูกมองข้ามเสมอ แต่เป็นเรื่องสำคัญที่จะปกป้องข้อมูลที่สำคัญ โปรแกรมเรียกค่าไถ่จะยึดข้อมูลของผู้ใช้งานไว้เป็นตัวประกัน

**6. ติดตั้งเครื่องมือติดตามอุปกรณ์หรือล็อคหน้าจอ** ในกรณีที่ทำหาย เพื่อป้องกันไม่ให้ผู้ที่เอาไปเข้าถึงข้อมูลในเครื่องได้

**7. ระมัดระวังการใช้บลูทูธ** ถึงแม้ว่าจะสะดวกสบาย แต่บลูทูธก็ยังมีความเสี่ยงด้านความปลอดภัย ควรจะปิดโหมดบริการนี้ไว้เสมอ เมื่อไม่ได้ใช้งาน

**8. อัปเดตระบบปฏิบัติการอยู่เสมอ** ทั้งระบบปฏิบัติการของอุปกรณ์ดิจิทัล และโปรแกรมและแอปพลิเคชั่นที่ติดตั้งในอุปกรณ์นั้น เพื่อที่จะรับบริการด้านความปลอดภัยและซ่อมแซมข้อบกพร่องของรุ่นเก่าๆ


**9. ระมัดระวังการใช้ไวไฟ** อุปกรณ์ไวไฟที่ใช้ควรจะมีความปลอดภัย ควรตั้งรหัสผ่านไว้ตลอดเวลา และไม่ใช้ไวไฟสาธารณะ เมื่อต้องเปิดเผยข้อมูลส่วนตัวหรือทำธุรกรรม

**10. ลบข้อมูลหรือโปรแกรมที่ไม่ได้ใช้งานแล้ว** หากว่ามีโปรแกรมหรือแอปที่ไม่ได้ใช้งานหลายเดือนและควรจะเอาออกเสีย เช่นเดียวกับข้อมูลที่ไม่ได้ใช้แล้ว ควรจะลบออก หรือมิฉะนั้นควรจะเก็บข้อมูลเหล่านั้นในฮาร์ดไดร์ฟต่างหาก หรือเก็บไว้ในลักษณะออฟไลน์ เพื่อที่จะปกป้องข้อมูลส่วนตัวในกรณีที่ผู้ใช้งานอาจจะลืม

**11. ระมัดระวังการหลอกลวงให้กรอกข้อมูล (Phishing)** มิจฉาชีพจะปลอมตัวเป็นองค์กรที่เป็นที่รู้จัก และหลอกล่อให้ผู้ใช้งานเปิดเผยข้อมูลส่วนตัว เพื่อจะเข้ารหัสผ่านหรือเพื่อติดตั้งมัลแวร์ ควรสังเกต URL ของเว็บไซต์ให้ชัดเจนและอย่ากดลิ้งก์หรือเปิดไฟล์ที่แนบเข้ามา และระมัดระวังการหลอกลวงของแก๊งค์คอลเซ็นเตอร์ที่พยายามล้วงข้อมูลส่วนตัว และนำไปเปิดบัญชีอินเทอร์เน็ตแบงกิ้งที่สามารถโอนเงินจากบัญชีธนาคารของผู้ใช้งานออกไปได้

**12. ใช้สื่อสังคมออนไลน์อย่างระมัดระวัง** ไม่ควรรับคนที่ไม่รู้จักเป็นเพื่อน หลีกเลี่ยงการแชตกับคนแปลกหน้า ไม่เปิดเผยข้อมูลส่วนตัวในโหมดสาธารณะ ลบบัญชีสื่อสังคมออนไลน์ที่ไม่ได้ใช้แล้ว

# เอกสารอ้างอิง


**เตือนภัย!! Email แจ้งระงับ Apple id ปลอม หลอกขอข้อมูลบัตรเครดิต!!** [Online]. แหล่งที่มา https://tech.mthai.com/tips-technic/27699.html

**ทำความรู้จักกับมัลแวร์ (Malware) และวิธีการป้องกันง่ายๆด้วยตัวคุณเอง** [Online]. แหล่งที่มา https://www.it.chula.ac.th/th/node/3084 [14 มกราคม 2561]

**สถิติภัยคุกคามไตรมาส 2 ปี 2560 มัลแวร์กว่า 67% แพร่กระจายผ่านอีเมลฟิชชิ่ง** [Online]. แหล่งที่มา https://www.thaicert.or.th/newsbite/2017-08-10-02.html [16 มกราคม 2561]

**Call Security: Tips To Protect Your Data and Privacy online** [Online]. แหล่งที่มา https://www.theguardian.com/lloydsbank-new-normal/2017/nov/29/call-security-tips-to-protect-your-data-and-privacy-online [2 มกราคม 2561]

**Digital Footprint** [Online]. แหล่งที่มา https://techterms.com/definition/digital_footprint [11 มกราคม 2561]

**Digital Footprint** [Online]. แหล่งที่มา https://www.virtuallibrary.info/digital-footprint.html [4 มกราคม 2561]

**Online Privacy: Using Internet Safely** [Online]. แหล่งที่มา https://www.privacyrights.org/consumer-guides/online-privacy-using-internet-safely [7 มกราคม 2561]

**Social Networking Privacy: How to be Safe, Secure and Social** [Online]. แหล่งที่มา https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social [9 มกราคม 2561]

**Your Digital Footprint Matters** [Online]. แหล่งที่มา https://www.internetsociety.org/tutorials/your-digital-footprint-matters/ [13 มกราคม 2561]

# การรักษาความปลอดภัยบนโลกไซเบอร์ (Cybersecurity)

**พิมพ์ครั้งที่ 1 :** สิงหาคม 2561
**จำนวนการพิมพ์ :** 500 เล่ม
**เขียนและเรียบเรียง :** ดร.สรานนท์ อินทนนท์
**บรรณาธิการ :** เข็มพร วิรุณราพันธ์, ลักษมี คงลาภ
**ฝ่ายศิลป์/ออกแบบรูปเล่ม :** อรสุมน ศานติวงศ์สกุล
**จัดพิมพ์และเผยแพร่ :** มูลนิธิส่งเสริมสื่อเด็กและเยาวชน (สสย.)
6/5 ซอยอารีย์ 5 พหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพฯ
โทรศัพท์ 02-617-1919
E-mail : childmedia2017@gmail.com
Website : www.childmedia.net
**พิมพ์ที่ :** บริษัท นัชชาวัตน์ จำกัด
42/19 หมู่ 5 ต.คูคต อ.ลำลูกกา จ.ปทุมธานี 12130
โทรศัพท์ 02-193-2549 แฟกซ์ 02-193-2550
E-mail : natchawat.print@gmail.com
Website : www.natchawatprinting.com