

ปลอดภัย ไซเบอร์

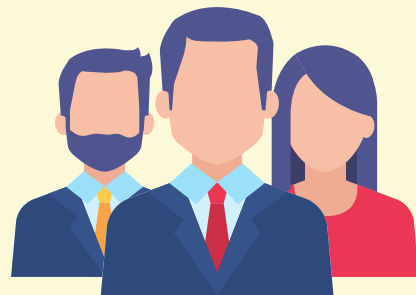
Cyber Security



แนะนำตัว



ปริญธร เล่าพิทักษ์
DLICT NARA 1



ส่งเสริมการศึกษาทางไกล
เทคโนโลยีสารสนเทศ
และการสื่อสาร

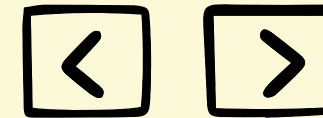


091-902-1995



parinthon.l
@narathiwat1.go.th

Contents



01

เทคโนโลยีกับปัญหา
ความปลอดภัย

02

การใช้อินเทอร์เน็ต
ผ่านสมาร์ทโฟนหรือ
แท็บเล็ตให้ปลอดภัย

03

เมื่อเรื่องส่วนตัวไม่
เป็นความลับอีกต่อไป

04

ระวังอันตรายจากการ
หลอกลวง

05

ระวัง! แอปพลิเคชัน
เคชั้นอันตราย

06

วิธีการป้องกันตัวจาก
โลกออนไลน์

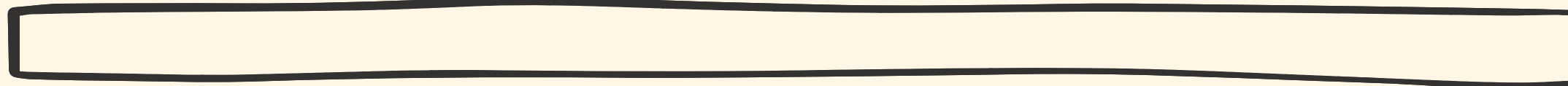
07

พรบ.คอมพิวเตอร์ใน
ชีวิตประจำวัน

08

การดูแลบุตรหลาน
ในการใช้อินเทอร์เน็ต



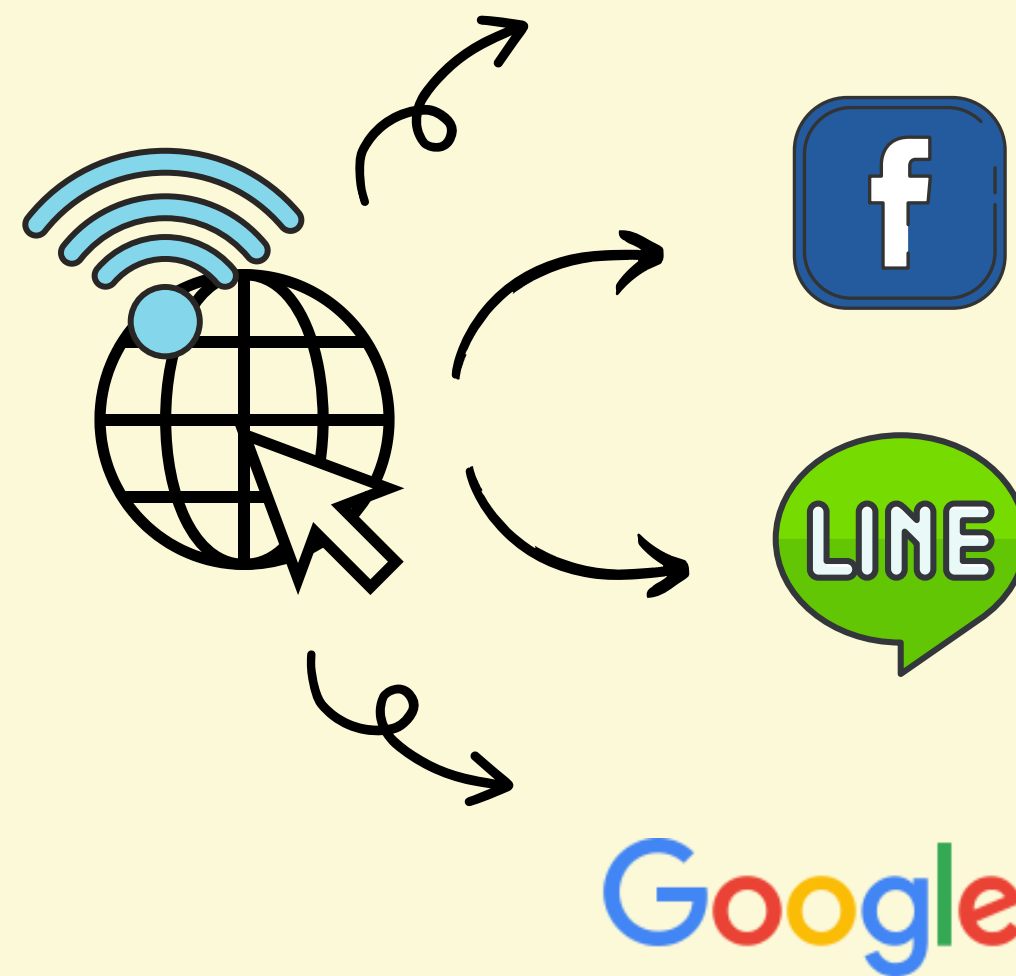
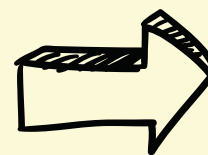


01

**เทคโนโลยีกับปัญหา
ความปลอดภัย**

เทคโนโลยีกับปัญหา ความปลอดภัย

เดี๋ยวนี้ใครๆ ก็ใช้เน็ตได้จากทุกที่ทุกเวลา บาง
แอปหรือบางบริการก็จะรับส่งข้อมูลอยู่เป็นระยะ
ทำให้ข้อมูลต่างๆ เช่น การแบ็คอัพรูปและข้อมูล
จากในเครื่อง การอัปเดตซอฟต์แวร์ออนไลน์
อัตโนมัติ
อันตรายจึงมาถึงเราได้ตลอดเวลา 24 ชม. ที่
เชื่อมต่ออินเทอร์เน็ต



ภัยคุกคามทางเทคโนโลยี

ภัยคุกคามทางเทคโนโลยีมี 3 ประเภท

01

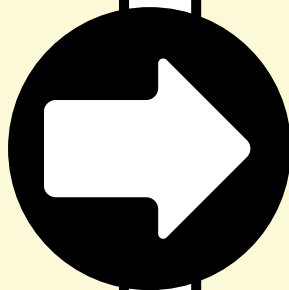
ภัยคุกคามทางระบบฮาร์ดแวร์หรือตัวเครื่อง
ภัยที่โดนกระทำทางกายภาพโดยตรง เช่น แรมเสียบ ฮาร์ดดิสพัง และ การโดนขโมย โทรคัพท์ โน้ตบุ๊ก

02

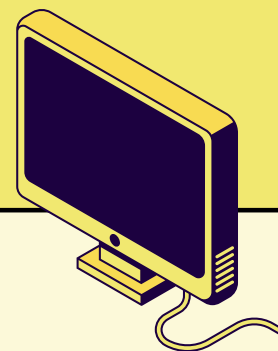
ภัยคุกคามทางระบบซอฟต์แวร์หรือโปรแกรม
malware เช่น virus, trojan, spyware เป็นต้น malware จะทำการเปลี่ยนแปลง หรือ ลบข้อมูลเราทิ้งได้

03

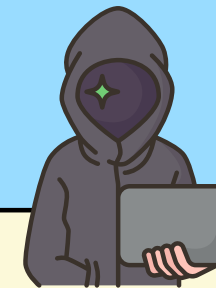
ภัยคุกคามทางระบบข้อมูล
เป็นการโจรกรรมข้อมูล โดยข้อมูลอาจถูกเปิดเผยหรือเปลี่ยนแปลงโดยที่เราไม่ได้อนุญาต



ภัยคุกคาม
ทางระบบ
ฮาร์ดแวร์



ภัยคุกคาม
ทางระบบ
ซอฟต์แวร์



ภัยคุกคาม
ทางระบบ
ข้อมูล



01

ข้อเสนอแนะสำหรับการป้องกัน

ระวัง!!!



- ระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดรฟ์ (USB) เป็นต้น
- การเปิดอีเมลหรือ ลิงค์ รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ

หลีกเลี่ยง!!!



- หลีกเลี่ยงการกดลิงค์ของข้อความโดยการใช้อำนาจหรือรูปภาพพาดหัวที่ทำให้ดูชวนสงสัยใคร่รู้ (Clickbait)
- หลีกเลี่ยงการดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ

อัปเดตและป้องกัน



- อัปเดตซอฟต์แวร์ในเครื่องให้ทันสมัยอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware)

ล็อคเครื่องไว้ ปลอดภัยกว่า

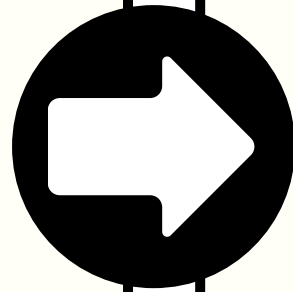
คอมพิวเตอร์ หรือ โทรศัพท์ต่างก็มีข้อมูลที่
สำคัญ ไม่ว่าจะเป็นอีเมล รูปภาพ จดบันทึก แชก
บางคนอาจใช้ทำธุรกรรมต่างๆ ควรที่จะตั้งรหัส
ล็อคหน้าจอไว้ ถ้าเป็นโน้ตบุ๊กหรือโทรศัพท์ยุคใหม่
จะมีการสแกนลายนิ้วมือช่วยเพิ่มความปลอดภัย
ในการใช้ได้มากยิ่งขึ้น



การตั้งค่าล็อคหน้าจอ

ios 🍏

- 01 ไปที่ ⚙️ แล้วเลื่อนลงมา "👉 Touch ID และรหัส"
- 02 แตะ "👉 Touch ID และรหัส"
- 03 แตะ เปิดการเข้ารหัส
- 04 จะปรากฏหน้ากรอกรหัส กรอกให้ KSU



01



03

01

การตั้งค่าล็อคหน้าจอ

ios 🍏

01

ไปที่  แล้วเลื่อนลงมา
"  Touch ID และรหัส "

02

แตะ "  Touch ID และรหัส "

03

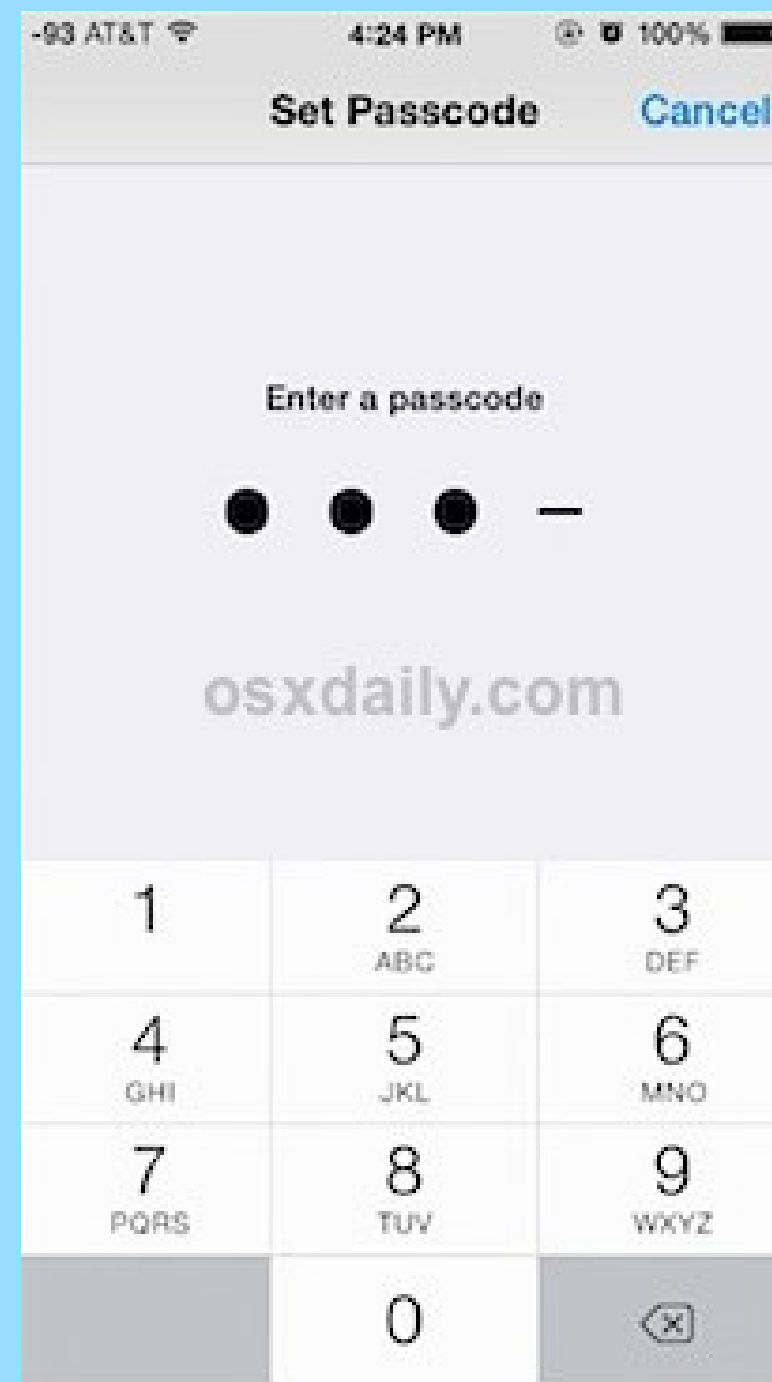
แตะ เปิดการใช้รหัส

04

จะปรากฏหน้าต่างกรอกรหัส กรอกให้
คสย




01

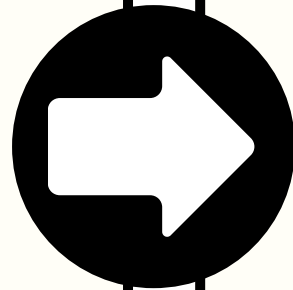
02



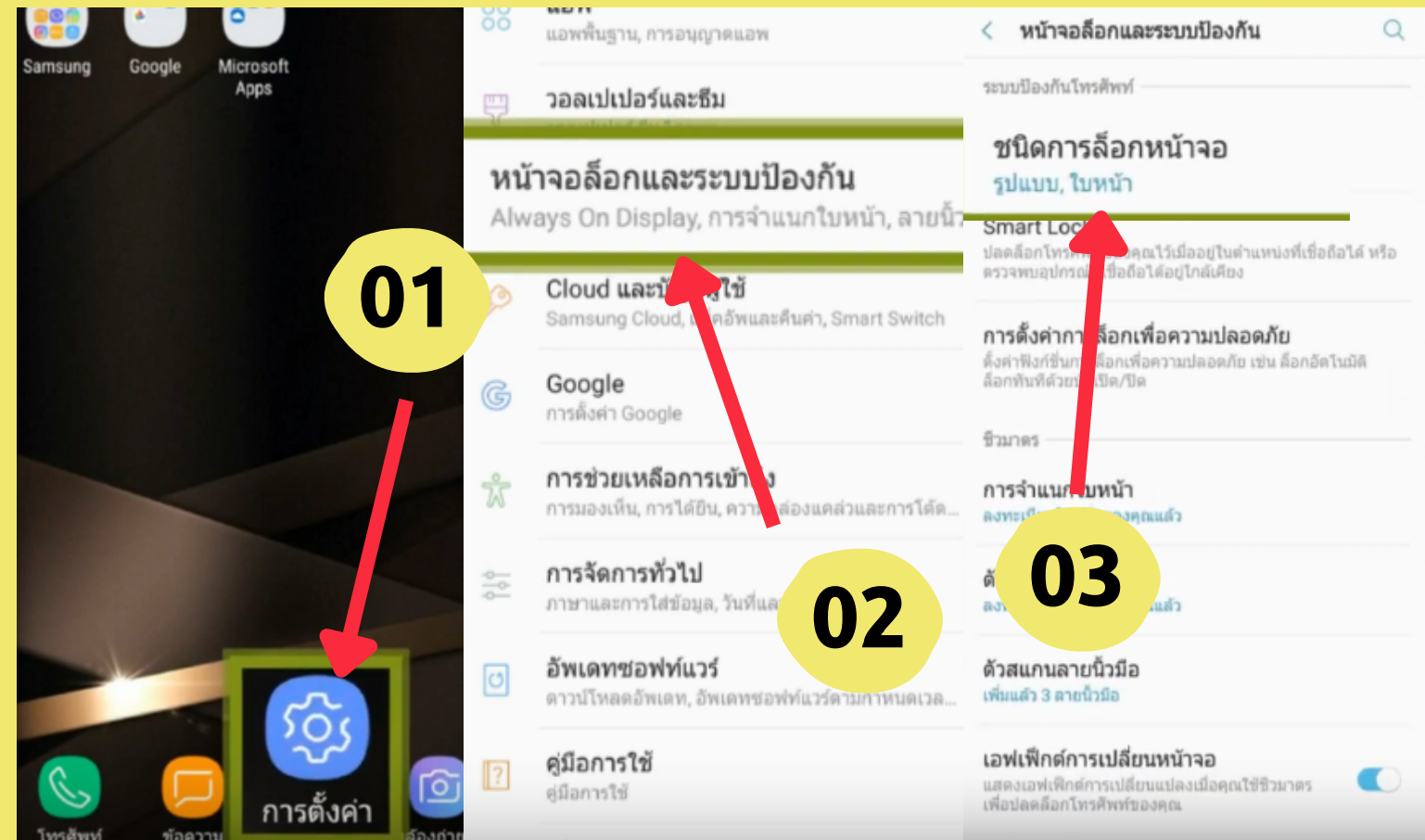
การตั้งค่าล็อคหน้าจอ

Android ๕ (Samsung)

- 01 ไปที่  แล้วเลื่อนลงมา
"  หน้าจอล็อค และระบบป้องกัน"
- 02 แตะ "  หน้าจอล็อค และระบบ
ป้องกัน"
- 03 แตะ ชนิดการล็อคหน้าจอ
- 04 แตะรูปแบบ PIN กรอกรหัสแล้ว
"ตกลง"



01



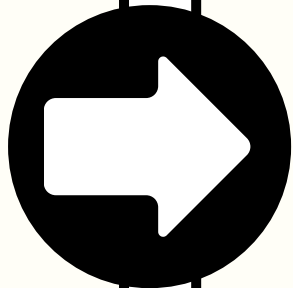
01

01

การตั้งค่าล็อคหน้าจอ

Android 11 (Samsung)

- 01 ไปที่  แล้วเลื่อนลงมา "  หน้าจอล็อค และระบบป้องกัน"
- 02 แตะ "  หน้าจอล็อค และระบบป้องกัน"
- 03 แตะ ชนิดการล็อคหน้าจอ
- 04 แตะรูปแบบ PIN กรอกรหัสแล้ว "ตกลง"




02




การตั้งค่าหาโทรศัพท์

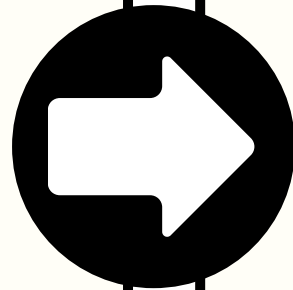
ios 🍏

01 เข้า  และ "Apple ID ของคุณ"

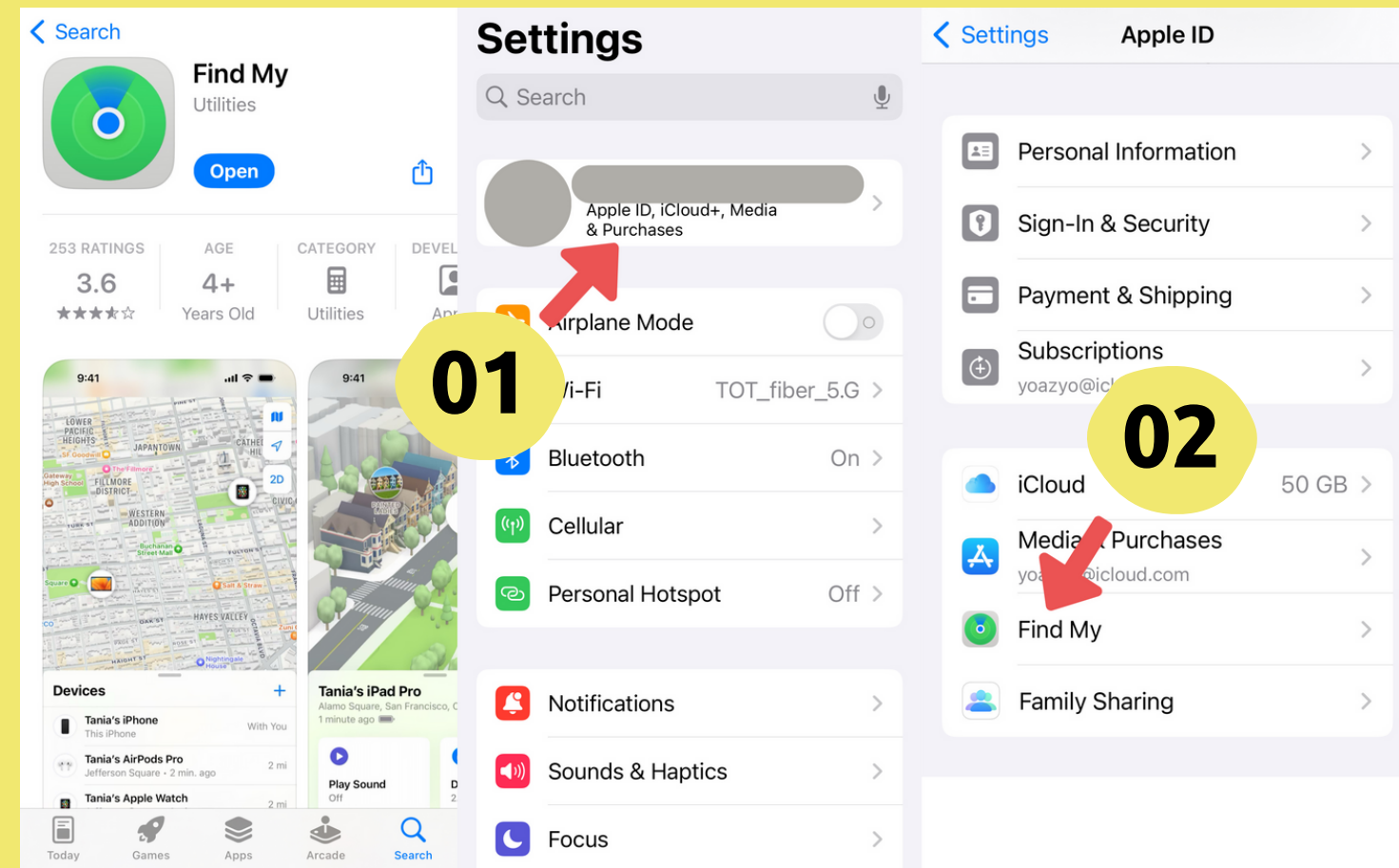
02 และ "  Find My"

03 หลังจากแตะ  Find My แล้ว
สามารถเลือกฟังก์ชันได้ดังนี้ :

- ค้นหา iphone ของฉัน
(Find My iPhone)
- เครือข่าย "ค้นหาของฉัน"
(Find My network)
- ส่งตำแหน่งที่ตั้งล่าสุด
(send Last Location)




01




01

การตั้งค่าหาโทรศัพท์

ios ๘

01 เข้า  และ "Apple ID ของคุณ"

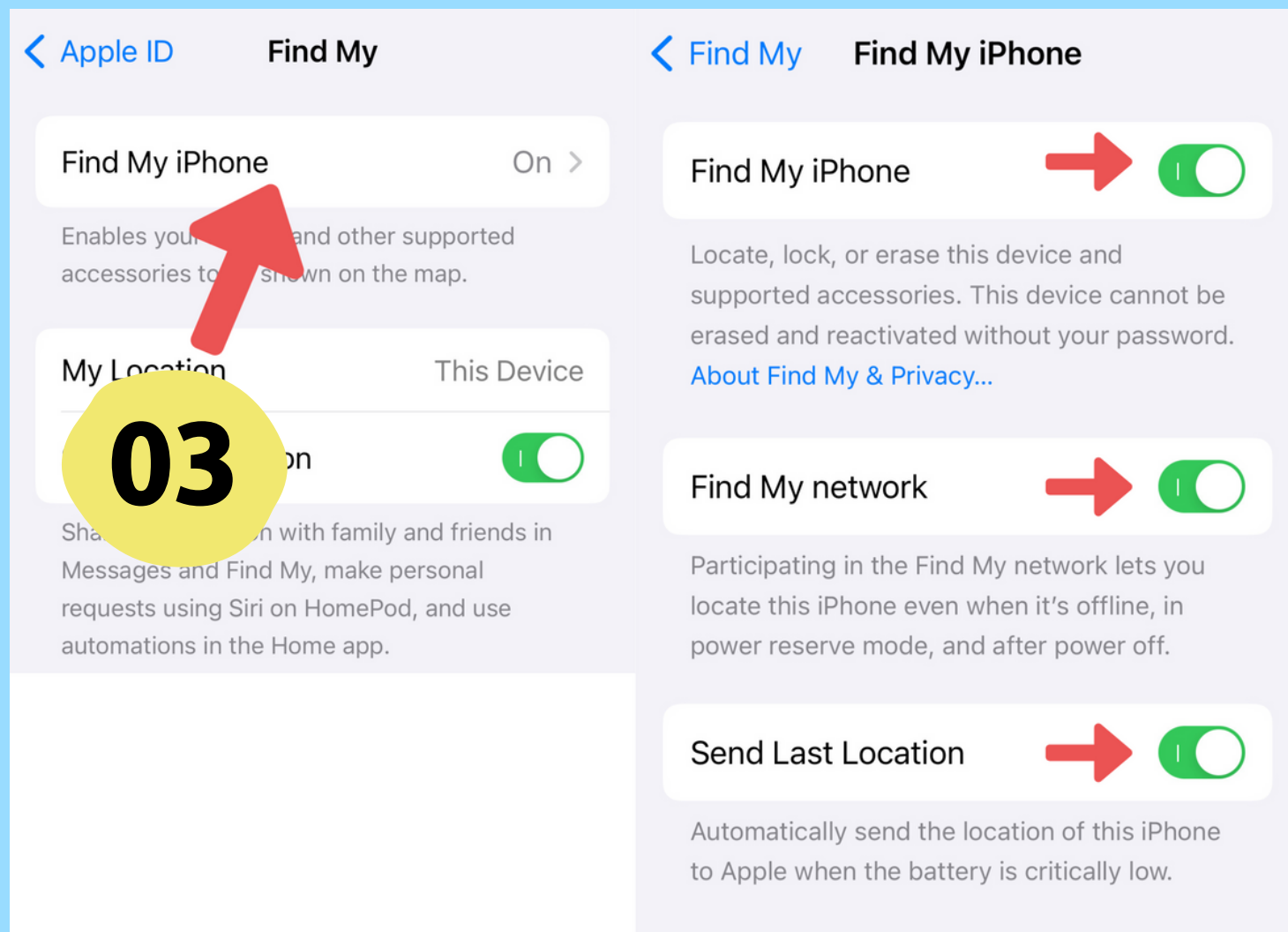
02 และ "  Find My"

03 หลังจากแตะ  Find My แล้ว
สามารถเลือกฟังก์ชันได้ดังนี้ :

- ค้นหา iphone ของฉัน (Find My iPhone)
- เครือข่าย "ค้นหาของฉัน" (Find My network)
- ส่งตำแหน่งที่ตั้งล่าสุด (send Last Location)

01


02

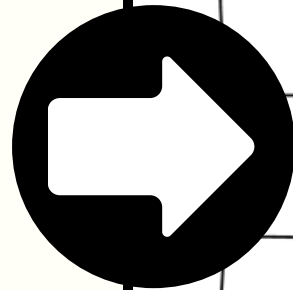


03

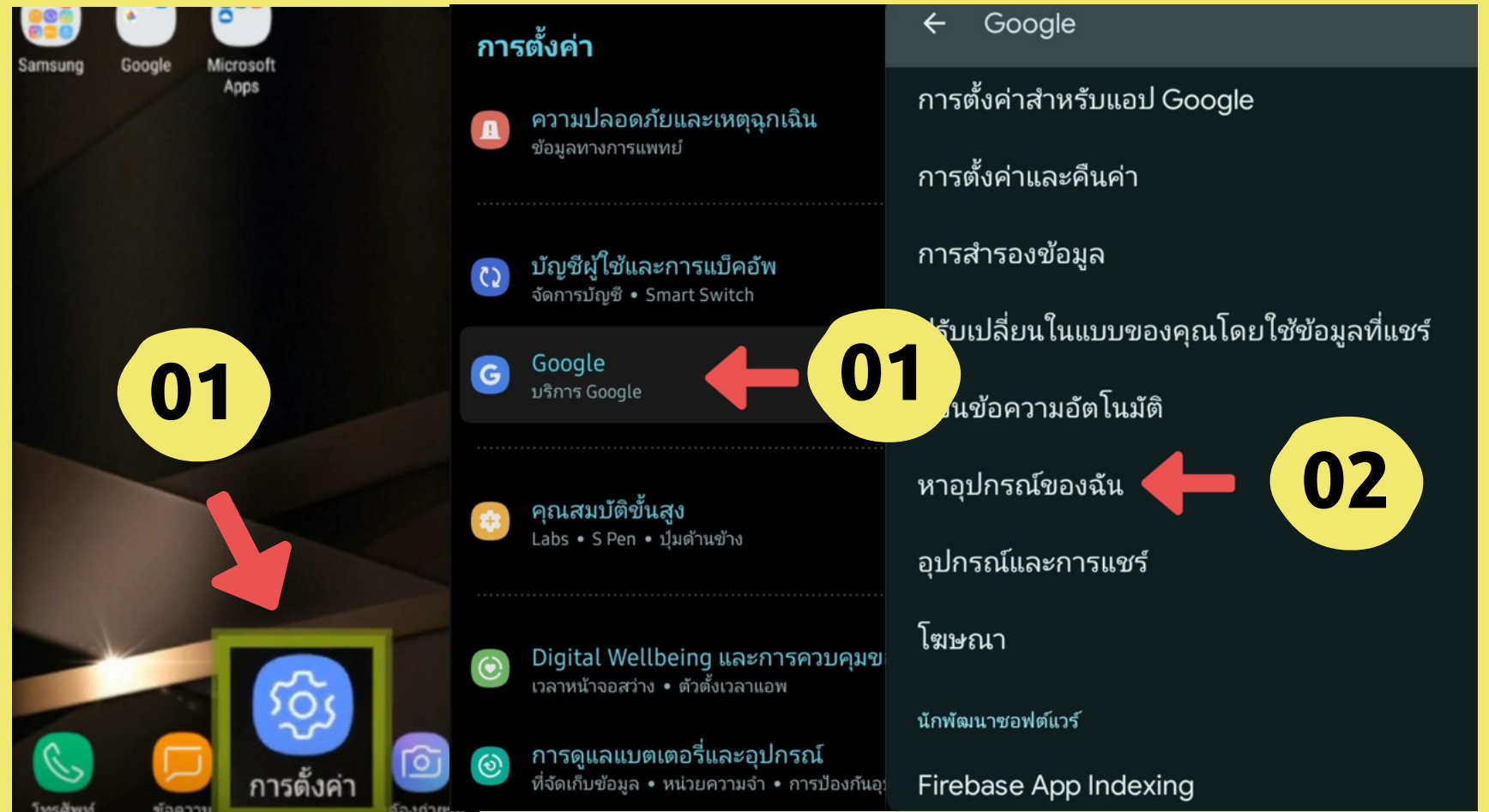
การตั้งค่าหาโทรศัพท์

Android ๕

- 01 เข้า  "การตั้งค่า"
แตะ "Google" (บริการ Google)
- 02 แตะ "หาอุปกรณ์ของฉัน"
- 03 เปิดใช้บริการหาอุปกรณ์ของฉัน
ออกมาหน้าหลัก
- 04 แตะ แอปพลิเคชัน ค้นหา
- 05 ลงชื่อเข้าใช้ แอปพลิเคชัน
"หาอุปกรณ์"



01




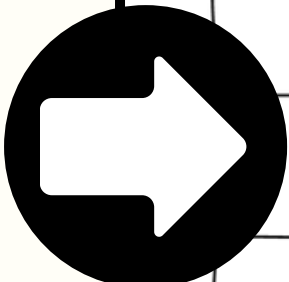
01

01

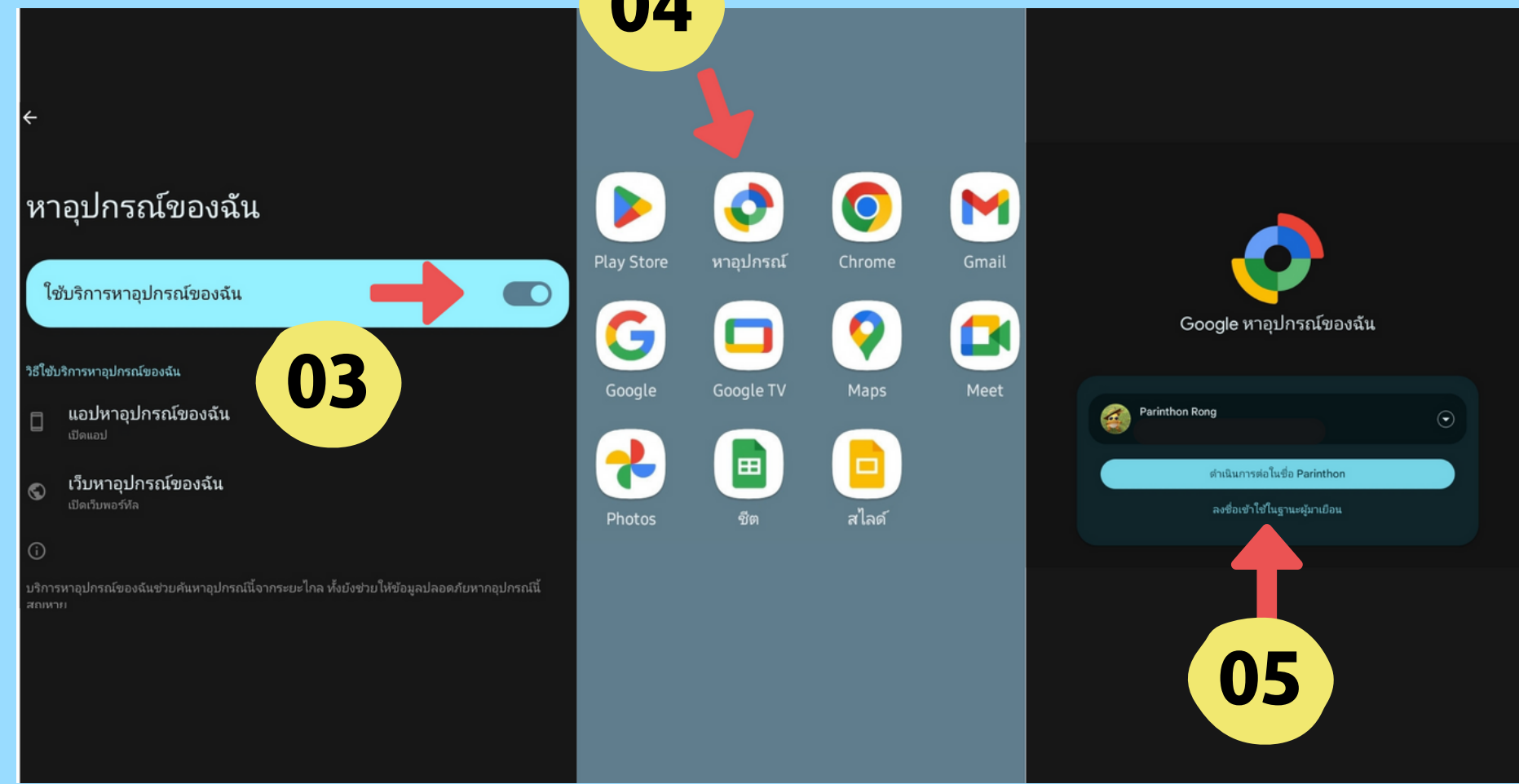
การตั้งค่าโทรศัพท์

Android ๕

- 01 เข้า  "การตั้งค่า" และ "Google" (บริการ Google)
- 02 แตะ "หาอุปกรณ์ของฉัน"
- 03 เปิดใช้บริการหาอุปกรณ์ของฉัน ออกมาหน้าหลัก
- 04 แตะ แอปพลิเคชัน ค้นหา
- 05 ลงชื่อเข้าใช้ แอปพลิเคชัน "หาอุปกรณ์"



02



04

03

05

การหาโทรศัพท์ ผ่าน web/app

iOS (แอปพลิเคชัน Find My)

01

แตะ "ค้นหาของฉัน (Find My)"

02

แตะ Devices เลือกอุปกรณ์ของคุณจากเมนู "อุปกรณ์"

03

โดยฟังก์ชัน มีดังนี้

- ส่งเสียงดัง
- เส้นทาง (ระยะทางจากอุปกรณ์ที่เปิดแอป Find My)
- การแจ้งเตือน (แจ้งเตือนไปยังหน้าจอของอุปกรณ์นั้น)
- ระบุว่าสูญหาย (เครื่องจะล็อค) ลบข้อมูลอุปกรณ์นี้

01

01




การหาโทรศัพท์ ผ่าน web/app

iOS (แอปพลิเคชัน Find My)

01

แตะ "  ค้นหาของฉัน (Find My)"

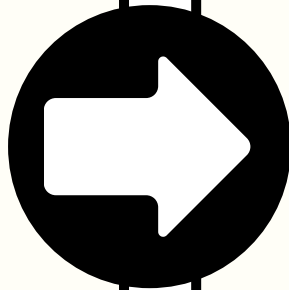
02

แตะ  Devices เลือกอุปกรณ์ของคุณจากเมนู "อุปกรณ์"

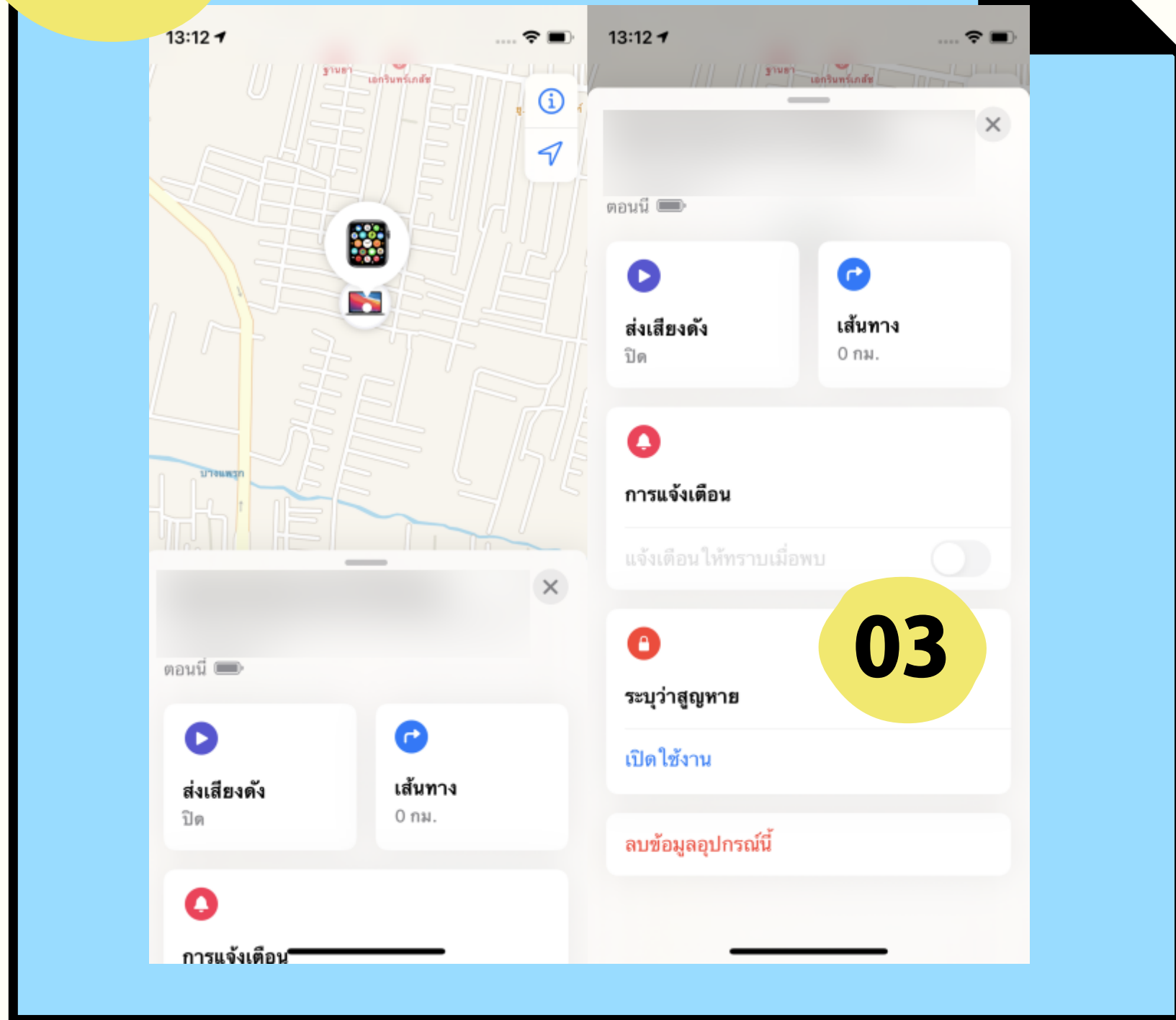
03

โดยฟังก์ชัน มีดังนี้

- ส่งเสียงดัง
- เส้นทาง (ระยะทางจากอุปกรณ์ที่เปิดแอป Find My)
- การแจ้งเตือน (แจ้งเตือนไปยังหน้าจอของอุปกรณ์นั้น)
- ระบุว่าสูญหาย (เครื่องจะล็อค)
- ลบข้อมูลอุปกรณ์นี้



02



03

01

การหาโทรศัพท์ ผ่าน web/app

ios (เว็บ)

01 เมื่อเข้า icloud.com กด “ลงชื่อเข้า”

02 กด Find My 

03 เมื่อเข้า Find My คุณสามารถ เลือก อุปกรณ์ได้จาก “All Devices” และดู ตำแหน่งที่อยู่ของอุปกรณ์ได้

- เมื่อเลือกอุปกรณ์ได้แล้ว ฟังก์ชันจะมีทั้งหมด 3 ฟังก์ชัน
 1. เล่นเสียง (Play Sound)
 2. โหมดศูนย์หาย (Lost Mode)
- สามารถตั้งข้อความ
- สามารถตั้งคำโทรที่เรากำหนด
 3. ลบข้อมูล (Erase iPhone)

01

03

icloud.com 

01

ลงชื่อเข้าด้วย Apple ID

อีเมลหรือเบอร์โทรศัพท์


ให้อ่านอยู่ในระบบเสมอ

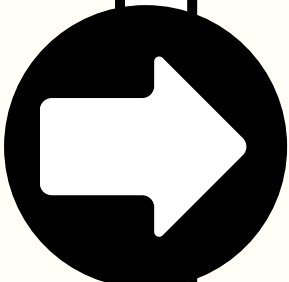
[ลืมรหัสผ่านหรือไม่? >](#)

[สร้าง Apple ID](#)

การหาโทรศัพท์ ผ่าน web/app

ios ๓ (เว็บ)

- 01** เมื่อเข้า icloud.com กด “ลงชื่อเข้า”
- 02** กด Find My 
- 03** เมื่อเข้า Find My คุณสามารถ เลือก อุปกรณ์ได้จาก “All Devices” และดู ตำแหน่งที่อยู่ของอุปกรณ์ได้
 - เมื่อเลือกอุปกรณ์ได้แล้ว ฟังก์ชันจะมีทั้งหมด 3 ฟังก์ชัน
 1. เล่นเสียง (Play Sound)
 2. โหมดสูญหาย (Lost Mode)
 - สามารถตั้งข้อความ
 - สามารถตั้งค่าโทรที่เรากำหนด
- 3. ลบข้อมูล (Erase iPhone)**



04



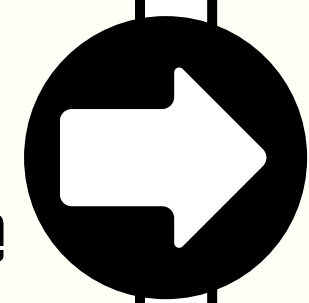
01

การหาโทรศัพท์ ผ่าน web/app...

ios 📱 (เว็บ)

- 01** เมื่อเข้า icloud.com กด “ลงชื่อเข้า”
- 02** กด Find My 📍
- 03** เมื่อเข้า Find My คุณสามารถเลือกอุปกรณ์ได้จาก “All Devices” และดูตำแหน่งที่อยู่ของอุปกรณ์ได้
 - เมื่อเลือกอุปกรณ์ได้แล้ว ฟังก์ชันจะมีทั้งหมด 3 ฟังก์ชัน
 - 1. เล่นเสียง (Play Sound)
 - 2. โหมดศูนย์หาย (Lost Mode)
- สามารถตั้งข้อความ
- สามารถตั้งค่าโทรที่เรากำหนด
- 3. ลบข้อมูล (Erase iPhone)

01



04

The screenshot shows the iCloud.com interface. At the top, the URL 'icloud.com' is visible. A dropdown menu titled 'All Devices' is open, listing several devices: 'All Devices', 'Apple Watc... krissada', 'iPhone', 'shine's MacBook Pro', 'Beats Flex', and 'iPad ของ krissada'. Below this, the 'Lost Mode' screen for an iPhone is shown. It includes a 'Number' field with the value '0851234567' and a text input field for a message. The message field contains the Thai text: 'iPhone หาย ติดต่อกลับมาหาได้ตลอด 24 ชม. ครับ'. At the bottom of the screen, there are three buttons: 'Play Sound', 'Lost Mode', and 'Erase iPhone'. A yellow circle with the number '03' is overlaid on the bottom right of the screenshot.

การหาโทรศัพท์ ผ่าน web/app

Android ทีวี (แอปพลิเคชัน หาอุปกรณ์)

01

แตะ "หาอุปกรณ์ของฉัน"

02

ลงชื่อเข้าใช้ แอปพลิเคชัน "หาอุปกรณ์"

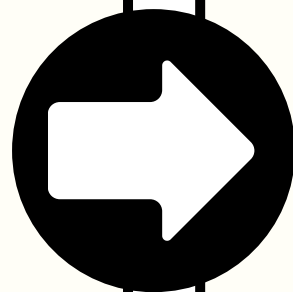
03

เลือกอุปกรณ์ของคุณได้จากกลุ่มอุปกรณ์

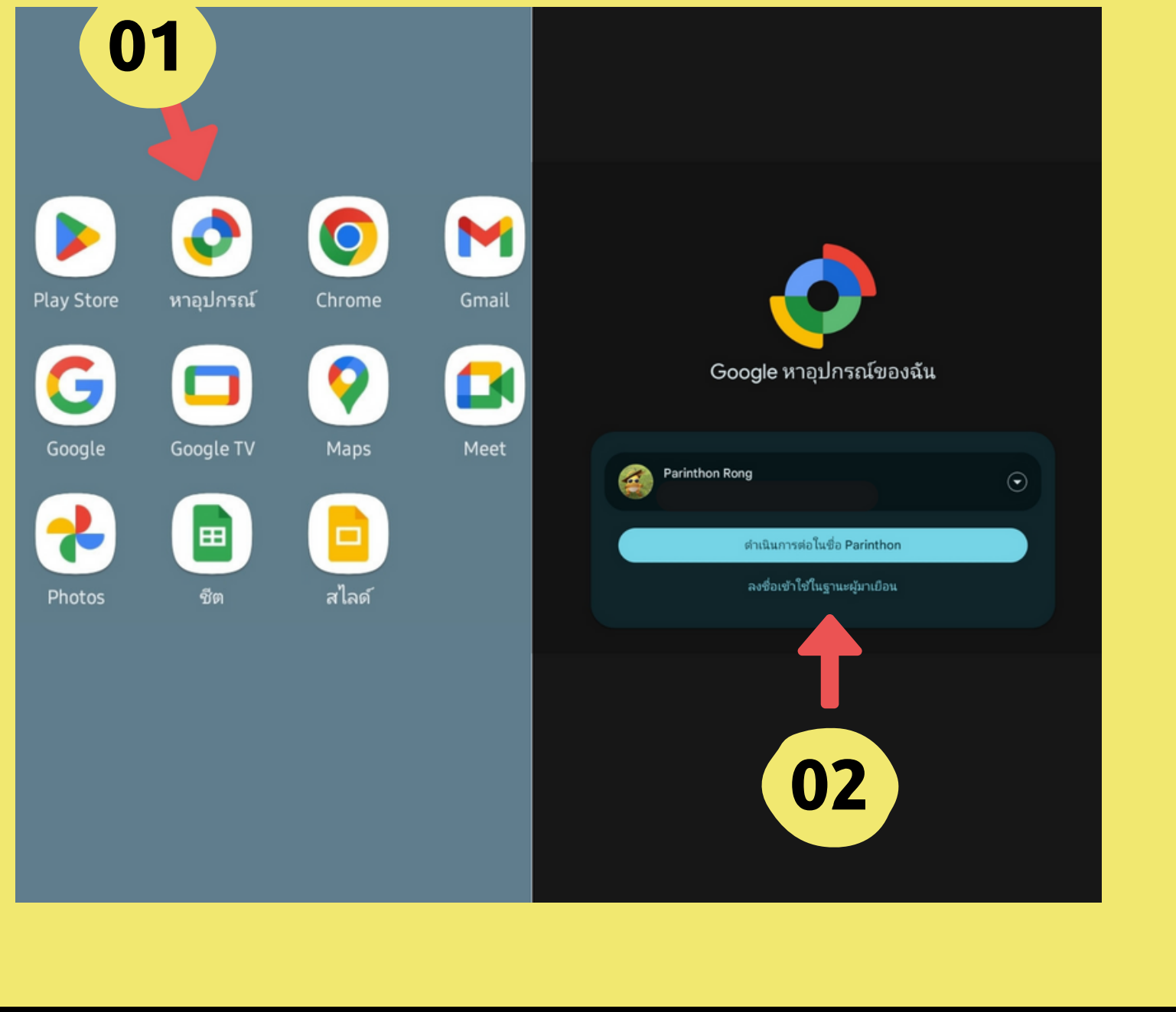
04

รายละเอียดโทรศัพท์และฟังก์ชัน มีดังนี้

- 📞 ส่งเสียงดัง
- 🔒 รักษาความปลอดภัยข้อมูล
- 🗑️ ล้างข้อมูลในเครื่อง



01



01

การหาโทรศัพท์ ผ่าน web/app

Android ทีวี (แอปพลิเคชัน หาอุปกรณ์)

01

แตะ "หาอุปกรณ์ของฉัน"

02

ลงชื่อเข้าใช้ แอปพลิเคชัน "หาอุปกรณ์"

03

เลือกอุปกรณ์ของคุณได้จากกลุ่มอุปกรณ์

04

รายละเอียดโทรศัพท์และฟังก์ชัน มีดังนี้

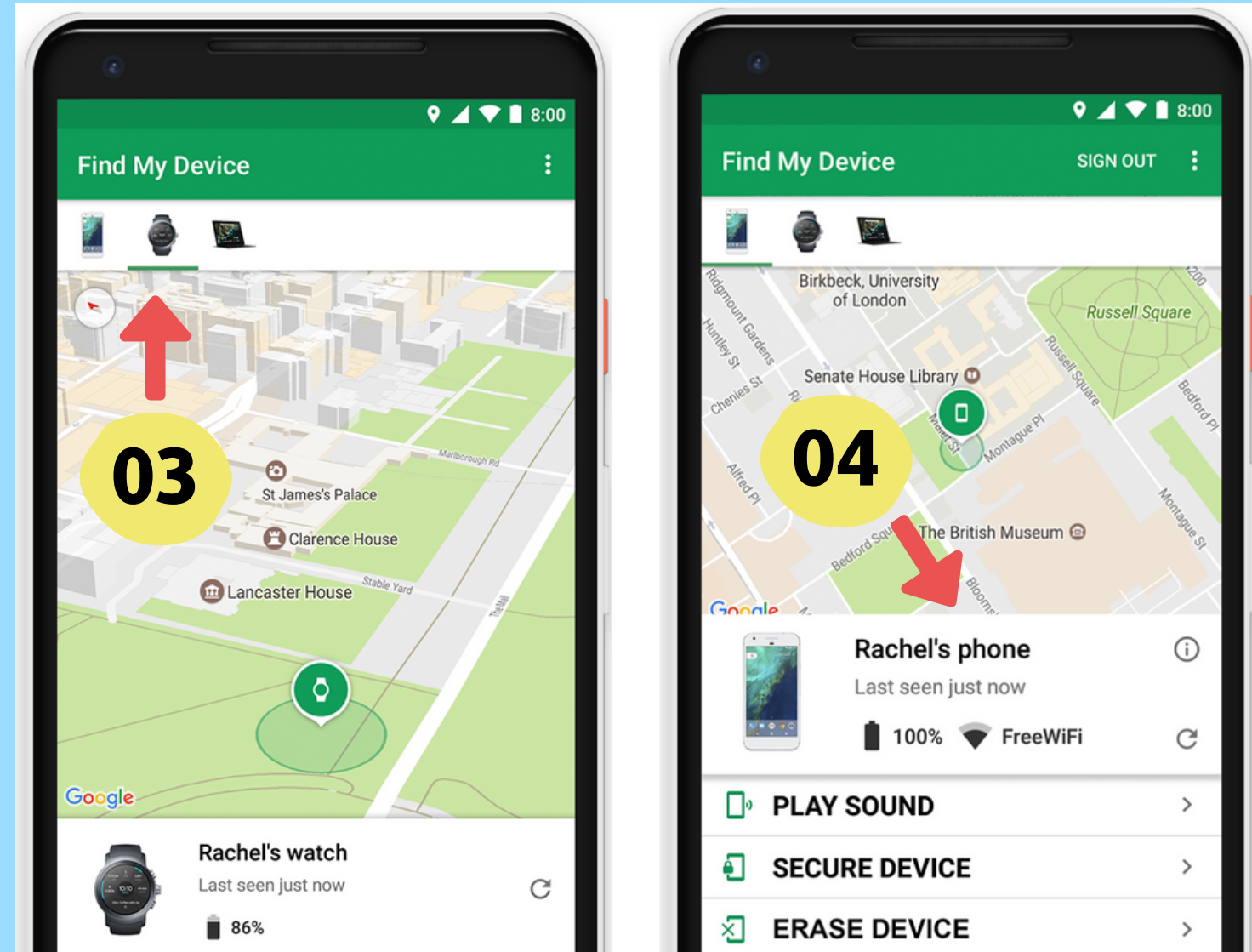
📞 ส่งเสียงดัง

🔒 รักษาความปลอดภัยข้อมูล

🗑️ ล้างข้อมูลในเครื่อง

01

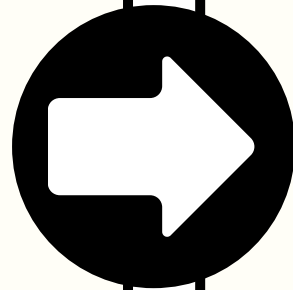
02



การหาโทรศัพท์ ผ่าน web/app

Android ทีวี (เว็บ)

- 01** เมื่อเข้า google.com/android/find/ กด “ลงชื่อเข้าใช้”
- 02** รายชื่ออุปกรณ์ Android ต่างๆ พร้อมข้อมูล
- 03** ลายละเอียดโทรศัพท์และฟังก์ชัน มีดังนี้
 - 📞 ส่งเสียงดัง
 - 🔒 รักษาความปลอดภัยข้อมูล
 - 🗑️ ล้างข้อมูลในเครื่อง



01

Google

ลงชื่อเข้าใช้

ไปยัง [Find My Device](#)

อีเมลหรือโทรศัพท์

[หากลืมอีเมล](#)

คุณอ่านนโยบายความเป็นส่วนตัวและข้อกำหนดในการให้บริการ Find My Device ได้ก่อนใช้แอปนี้

[สร้างบัญชี](#) [ถัดไป](#)

01

การหาโทรศัพท์ ผ่าน web/app

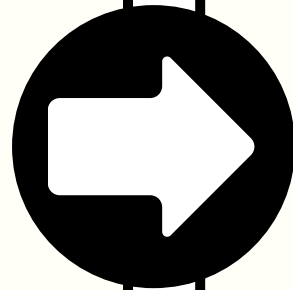
Android ทีวี (เว็บ)

01 เมื่อเข้า google.com/android/find/
กด “ลงชื่อเข้า”

02 รายชื่ออุปกรณ์ Android ต่างๆ
พร้อมข้อมูล

03 ลายละเอียดโทรศัพท์และฟังก์ชัน มี
ดังนี้

- 📞 ส่งเสียงดัง
- 🔒 รักษาความปลอดภัยข้อมูล
- 🗑️ ล้างข้อมูลในเครื่อง



02

Screenshot of the Google Find My Device website on a mobile browser. The page shows search results for a 'Poco X4 GT' phone. A yellow circle labeled '02' highlights the phone's status bar at the top of the browser window. A yellow circle labeled '03' highlights the 'เล่นเสียง' (Play Sound) option in the device's status menu. A map of the phone's location is visible on the right side of the screen.

01



02

**การใช้อินเทอร์เน็ต
ผ่านสมาร์ทโฟนหรือ
แท็บเล็ตให้ปลอดภัย**

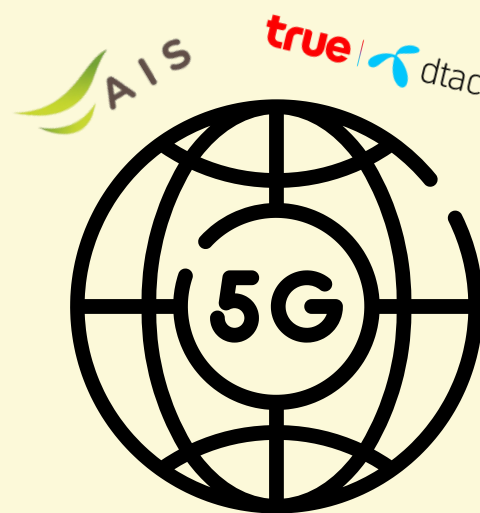
การใช้อินเทอร์เน็ตผ่าน สมาร์ทโฟนหรือแท็บเล็ต ให้ปลอดภัย

ในปัจจุบันการใช้งานสมาร์ทโฟน แท็บเล็ต หรือ คอมพิวเตอร์ ทุกคนล้วนต่ออินเทอร์เน็ตเพื่อเข้าใช้งาน เช่น สั่งซื้อของออนไลน์ หรือ ทำธุรกรรม เป็นต้น ซึ่งการต่ออินเทอร์เน็ตจะทำได้ 2 วิธี



ผ่าน WIFI เน็ตบ้าน เช่น NT,AIS&3BB,True

การเชื่อมต่อผ่าน Wifi สามารถเชื่อมต่อได้ตามบ้าน ที่ทำงาน หรือ บางที่ก็มีให้ใช้ฟรี



ผ่านผู้ให้บริการเครือข่าย เช่น Dtac,AIS,True

การเชื่อมต่อผ่าน เครือข่ายผู้ให้บริการ สามารถเชื่อมต่อได้ทุกที่ตามที่เราต้องการใช้

ต่อเน็ตแบบไหน แล้วต่อเมื่อไหร่ดี ???

WiFi

- สามารถใช้ได้ไม่จำกัดปริมาณข้อมูล
- ได้ความเร็วที่คงที่
- ความปลอดภัยขึ้นอยู่กับสถานที่ที่ใช้งาน เช่น wifi ในที่สาธารณะ ใช้การฟรี ไม่มีรหัสผ่าน จะมีความปลอดภัยน้อย เนื่องจาก มีผู้ใช้งานเยอะและ อาจจะเป็นwifi ที่ผู้ไม่ประสงค์ทำการดักข้อมูลได้ แต่ถ้าเป็นที่บ้าน ก็สามารถใช้งานได้ปกติ ไม่ต้องกังวล

5G

- ใช้ได้จำกัดปริมาณข้อมูลขึ้นอยู่กับแพ็คเกจ
- ได้ความเร็วขึ้นอยู่กับแพ็คเกจ และ สถานที่
- ปลอดภัยกว่าการใช้ wifi แบบสาธารณะ เพราะ ไม่ต้องผ่าน ตัวกระจาย wifi

Keyword “เลือกให้เหมาะกับการใช้งาน”

เทคนิค

“เพื่อความปลอดภัย”

เมื่อใช้แอปพลิเคชันธนาคารบนโทรศัพท์มือถือ



ควรปิดการใช้สัญญาณ Wi - Fi โดยเฉพาะ Wi - Fi สาธารณะ

กรณีจะใช้แอปฯ ธนาคาร หรือ Mobile Banking ควรใช้สัญญาณโทรศัพท์มือถือ 3G 4G หรือ 5G เท่านั้น

(ควรตั้งค่าปิดการใช้ Wi-Fi ใน โทรศัพท์มือถือไว้ แล้วเปิดใช้เมื่อจำเป็นต้องใช้เท่านั้น)

เพื่อป้องกันมิอาจชีพแฝงตัวแฮ็กรหัสผ่าน ด้วยความปรารถนาดีจากสำนักงานตำรวจแห่งชาติ

แจ้งความออนไลน์ www.thaipoliceonline.com

เท่านั้น !

ที่มา : กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี www.PreventOnlineCrime.com

เทคนิค “เพื่อความปลอดภัย”
เมื่อใช้แอปพลิเคชันธนาคารบนโทรศัพท์มือถือ





03

**เมื่อเรื่องส่วนตัวไม่
เป็นความลับอีกต่อไป**

เมื่อเรื่องส่วนตัวไม่เป็นความลับอีกต่อไป

ทัศนคติของคนยุคนี้เปลี่ยนไปจากเรื่องส่วนตัวต้องเก็บ กลายเป็นต้องแชร์

Keyword : เปิดเผยเรื่องส่วนตัวให้น้อย



ท่องเว็บก็โดนเก็บข้อมูลไม่รู้ตัว

“หลายเว็บๆ จะเก็บข้อมูลการเข้าชมว่าคุณสนใจเกี่ยวกับอะไร แล้วนำเสนอสินค้าหรือสิ่งที่คุณสนใจ”



ข้อมูลส่วนตัวควรเป็นความลับ

“การกรอกข้อมูลส่วนตัว ไม่ว่าจะเป็นข้อความ หรือ รูปภาพ ในเว็บให้บริการด้านต่างๆ จะต้องใช้ความระมัดระวังเป็นอย่างมาก”



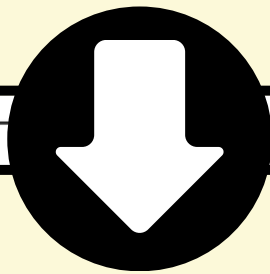
Chat, like, comment แต่พอดี

“การใช้ใน *Social media* ควรระวังเรื่องการใช้คำพูดหรือเปิดเผยข้อมูลส่วนตัว อาจจะเสี่ยงที่จะถูกจับภาพหน้าจอ หรือเก็บข้อมูลจากบุคคลที่สามได้”

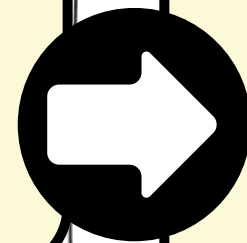


เปิดเผยเรื่องส่วนตัวแค่ไหนถึงพอดี?

ถึงแม้วันนี้คุณอาจยังไม่มีชื่อเสียง ทำให้โพสต์สิ่งต่างๆ ลงในเว็บสาธารณะ หรือ Social Media ต่างๆ ไปอย่างไม่ได้คิด แต่ขอให้นึกถึงว่าข้อมูลเหล่านั้นไม่ได้หายไปตามกาลเวลา



ใครบ้างที่จะเห็นโพสต์ของคุณ??



ครอบครัว
หรือ ญาติ

เพื่อนสนิท

คนรู้จัก
ที่ทำงาน

บุคคลอื่น

ข้อมูลส่วนบุคคลหลุดไป ความเสียหายที่อาจเกิดขึ้น !!

หลุดไปได้อย่างไร

- จากตัวผู้ใช้เอง
- เว็บไซต์หรือแอปพลิเคชันต่างๆ ที่ใช้งาน
- โดนแฮกหรือเจาะขโมยข้อมูลในบริษัทที่เราให้ข้อมูล
- การหลอกลวงด้วยวิธีการต่าง ๆ

นำไปทำอะไรต่อ

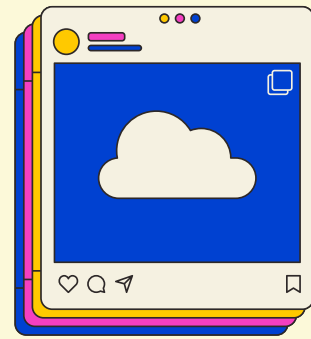
- ซื้อ-ขาย ข้อมูลส่วนบุคคล
- หาผลประโยชน์
- ปลอมแปลงตัวตน
- เปิดบัญชีม้า

ความเสียหาย

- ถูกนำไปในทางผิดกฎหมาย
- โดนโจรกรรมทางการเงิน
- ถูกแอบอ้างตัวตน

วิธีการปกป้องข้อมูลส่วนบุคคล

เพื่อไม่ให้เกิดความเสียหายต่อตนเอง เราควรมีมาตรการป้องกันที่ไม่ได้ความเสียหายเข้าถึงตัวเราได้



ไม่โพสต์ข้อมูลส่วนบุคคลต่าง ๆ ที่สำคัญ

เช่น ข้อมูลทางการเงิน, ประวัติส่วนตัว, ที่อยู่ปัจจุบัน, การเดินทาง



ตั้งค่าและดูแลพาสเวิร์ดหรือรหัสผ่านให้ปลอดภัย

- ควรมีความยาวที่เหมาะสม ประมาณ 10-14 ตัวอักษร
- ใช้ทุกอย่างบนแป้นพิมพ์ ตัวอักษรเล็ก (abcd) ตัวอักษรใหญ่ (ABCD) ตัวเลข (1234) เป็นสัญลักษณ์ (\$#!?)



ตั้งค่าความเป็นส่วนตัว

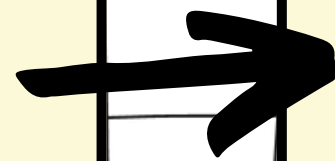
ในบัญชีออนไลน์ต่าง ๆ เพื่อจำกัดวงผู้อ่านหรือนำข้อมูลไปใช้ เช่น Facebook สามารถปรับการตั้งค่าความเป็นส่วนตัว



วิธีการปกป้องข้อมูลส่วนบุคคล

บุคคล

เพื่อไม่ให้เกิดความเสียหายต่อตนเอง เราควรมีมาตรการป้องกันที่ไม่ได้ความเสียหายเข้าถึงตัวเราได้



อย่าใช้รหัสผ่านเดียวกันกับทุกบริการ

ปกติเราต้องมีรหัสผ่านสำหรับเข้าใช้สารพัดบริการออนไลน์ เยอะแยะมากมาย หลายคนใช้รหัสผ่านเดียวกัน **แต่ต้องระวัง!** ถ้าถูกแฮกไปสักอันก็อาจถูกแฮกที่อื่นไปด้วยง่าย ๆ **ควรมีระบบล็อก 2 ชั้น**



การตั้งค่าความเป็นส่วนตัว

Facebook

01

ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ
"⚙️ การตั้งค่าและความเป็นส่วนตัว"

02

🔒 แตะ ทางลัดไปการตั้งค่าความ
เป็นส่วนตัว

03

🔒 แตะ เริ่มตรวจสอบความเป็นส่วน
ตัว

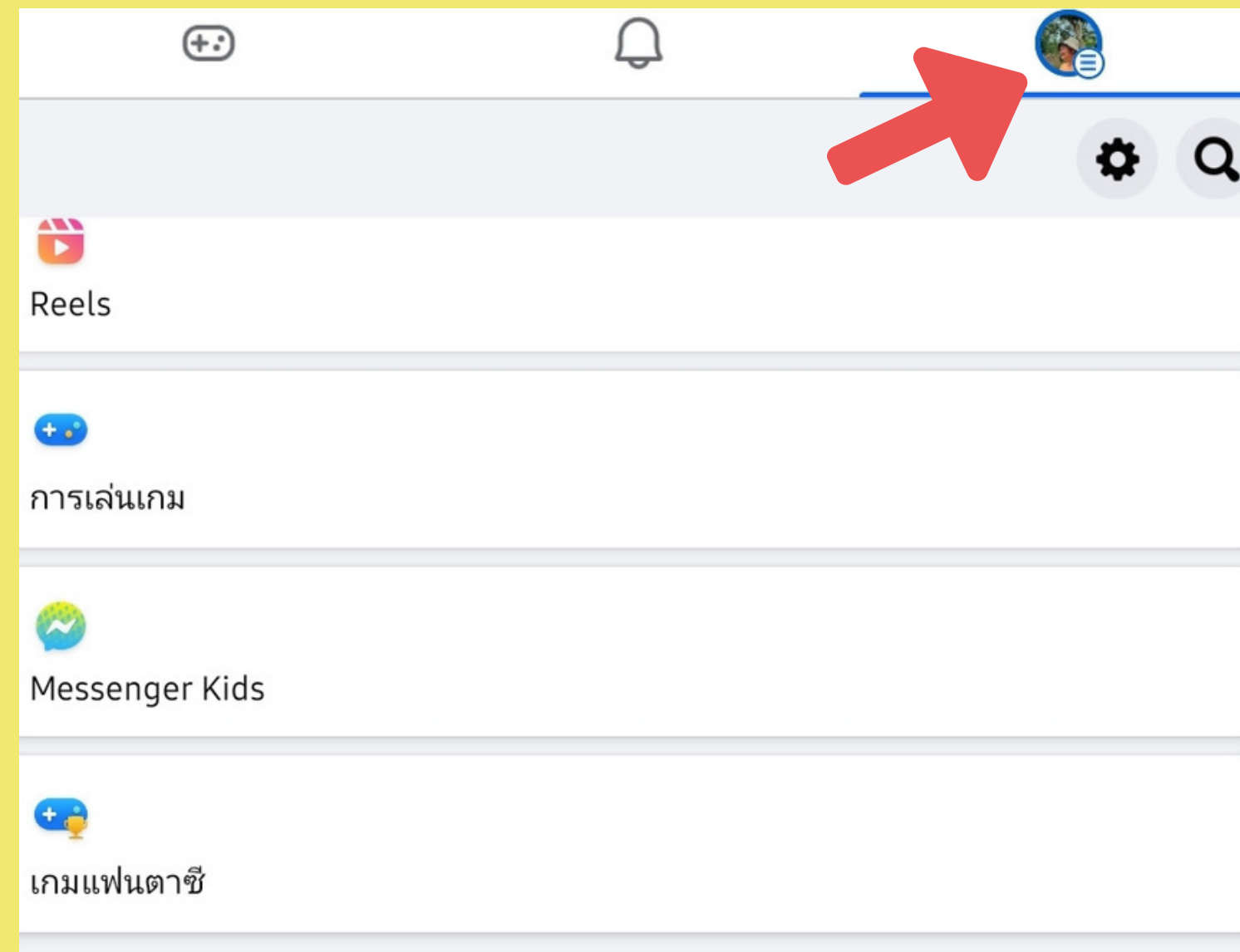
04

จะปรากฏเมนู ดังต่อไปนี้ :

- คนที่สามารถเห็นสิ่งที่คุณแชร์ได้
- วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- วิธีที่คนอื่นจะค้นหาคุณพบบน Facebook
- การตั้งค่าข้อมูลบน Facebook
- การกำหนดลักษณะโฆษณาของคุณบน Facebook

03

01



การตั้งค่าความเป็นส่วนตัว

Facebook

01

ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ
"⚙️ การตั้งค่าและความเป็นส่วนตัว"

02

🔒 แตะ ทางลัดไปการตั้งค่าความ
เป็นส่วนตัว

03

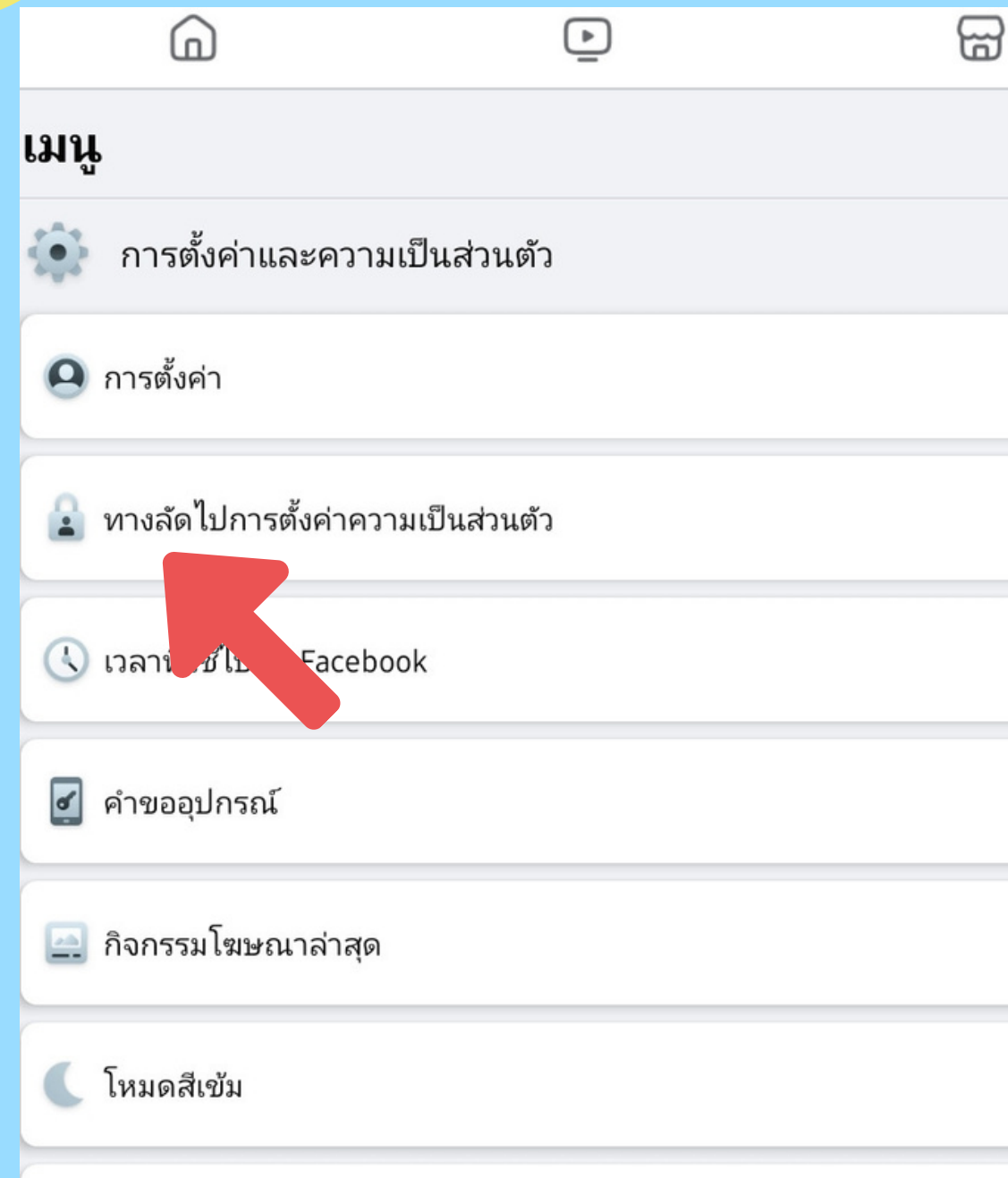
🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว

04

จะปรากฏเมนู ดังต่อไปนี้ :

- คนที่สามารถเห็นสิ่งที่คุณแชร์ได้
- วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- วิธีที่คนอื่นจะค้นหาคุณพบบน Facebook
- การตั้งค่าข้อมูลบน Facebook
- การกำหนดลักษณะโฆษณาของคุณบน Facebook

02



03

การตั้งค่าความเป็นส่วนตัว

Facebook

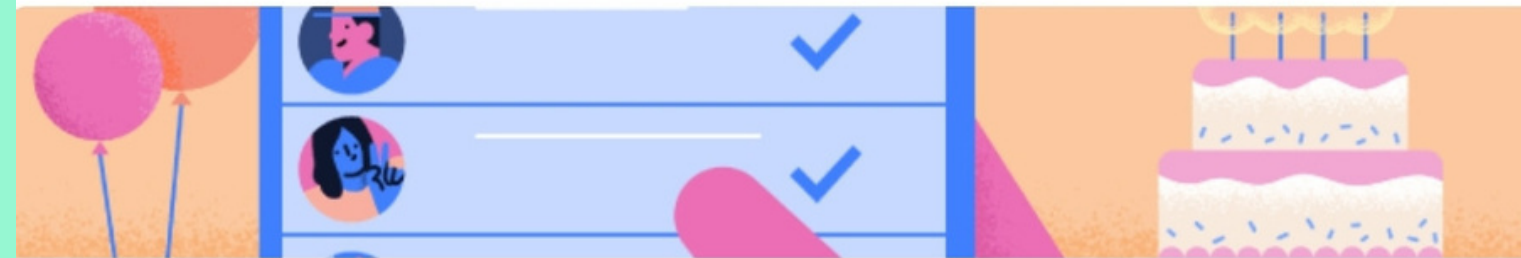
- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 จะปรากฏ เมนู ดังต่อไปนี้ :
 - คนที่สามารถเห็นสิ่งที่คุณแชร์ได้
 - วิธีการรักษาบัญชีของคุณให้ปลอดภัย
 - วิธีที่คนอื่นจะค้นหาคุณพบบน Facebook
 - การตั้งค่าข้อมูลบน Facebook
 - การกำหนดลักษณะโฆษณาของคุณบน Facebook

03

03



เครื่องมือที่จะช่วยให้คุณควบคุมความเป็นส่วนตัวและความปลอดภัยบน Facebook



ความเป็นส่วนตัว

ควบคุมว่าจะให้ใครเห็นสิ่งที่คุณแชร์บน Facebook และจัดการข้อมูลที่เราสามารถปรับแต่งประสบการณ์ให้เหมาะกับแต่ละบุคคลได้ดียิ่งขึ้น

- 🔒 เริ่มตรวจสอบความเป็นส่วนตัว
- 🎓 เรียนรู้เกี่ยวกับความเป็นส่วนตัวของคุณบน Facebook
- 📍 จัดการการตั้งค่าตำแหน่งของคุณ
- ⋮ ดูการตั้งค่าความเป็นส่วนตัวเพิ่มเติม

การตั้งค่าความเป็นส่วนตัว

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 จะปรากฏเมนู ดังต่อไปนี้ :
 - คนที่สามารถเห็นสิ่งที่คุณแชร์ได้
 - วิธีการรักษาบัญชีของคุณให้ปลอดภัย
 - วิธีที่คนอื่นจะค้นหาคุณพบบน Facebook
 - การตั้งค่าข้อมูลบน Facebook
 - การกำหนดลักษณะโฆษณาของคุณบน Facebook

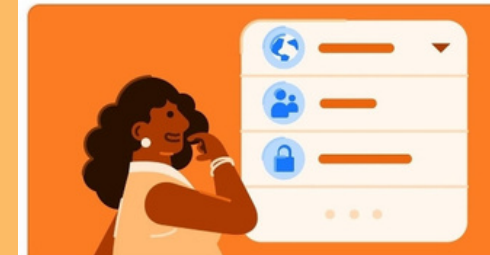
03

04

การตรวจสอบความเป็นส่วนตัว

เราจะแนะนำการตั้งค่าบางส่วนให้คุณทราบ เพื่อช่วยให้คุณตัดสินใจเกี่ยวกับบัญชีของคุณได้อย่างถูกต้อง

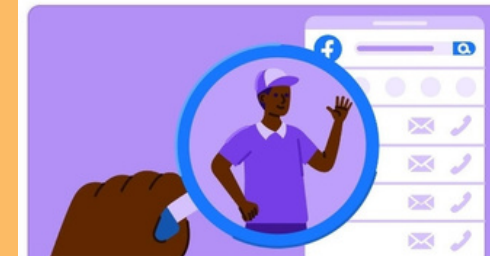
คุณต้องการเริ่มต้นกับหัวข้ออะไร



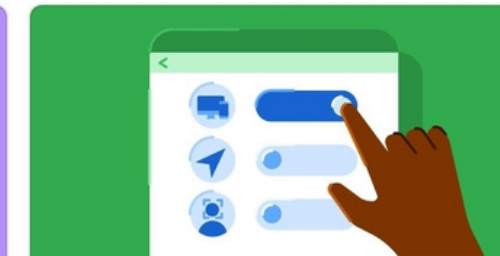
คนที่สามารถเห็นสิ่งที่คุณแชร์ได้
เมื่อวานนี้



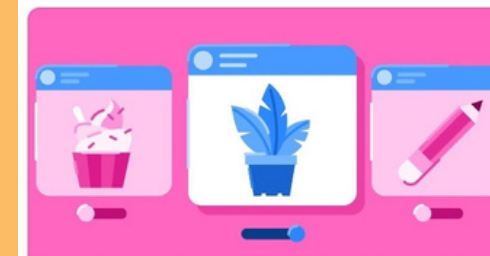
วิธีการรักษาบัญชีของคุณให้ปลอดภัย
เมื่อวานนี้



วิธีที่คนอื่นจะค้นหาคุณพบบน Facebook



การตั้งค่าข้อมูลบน Facebook



การกำหนดลักษณะโฆษณาของคุณบน Facebook
เมื่อวานนี้

คุณสามารถดูการตั้งค่าความเป็นส่วนตัวบน Facebook เพิ่มเติมได้ในการตั้งค่า

*ลายละเอียดจะมีคู่มือให้

การตั้งค่าความเป็นส่วนตัว

Line

01

ไปที่ เมนู  ตั้งค่า

02

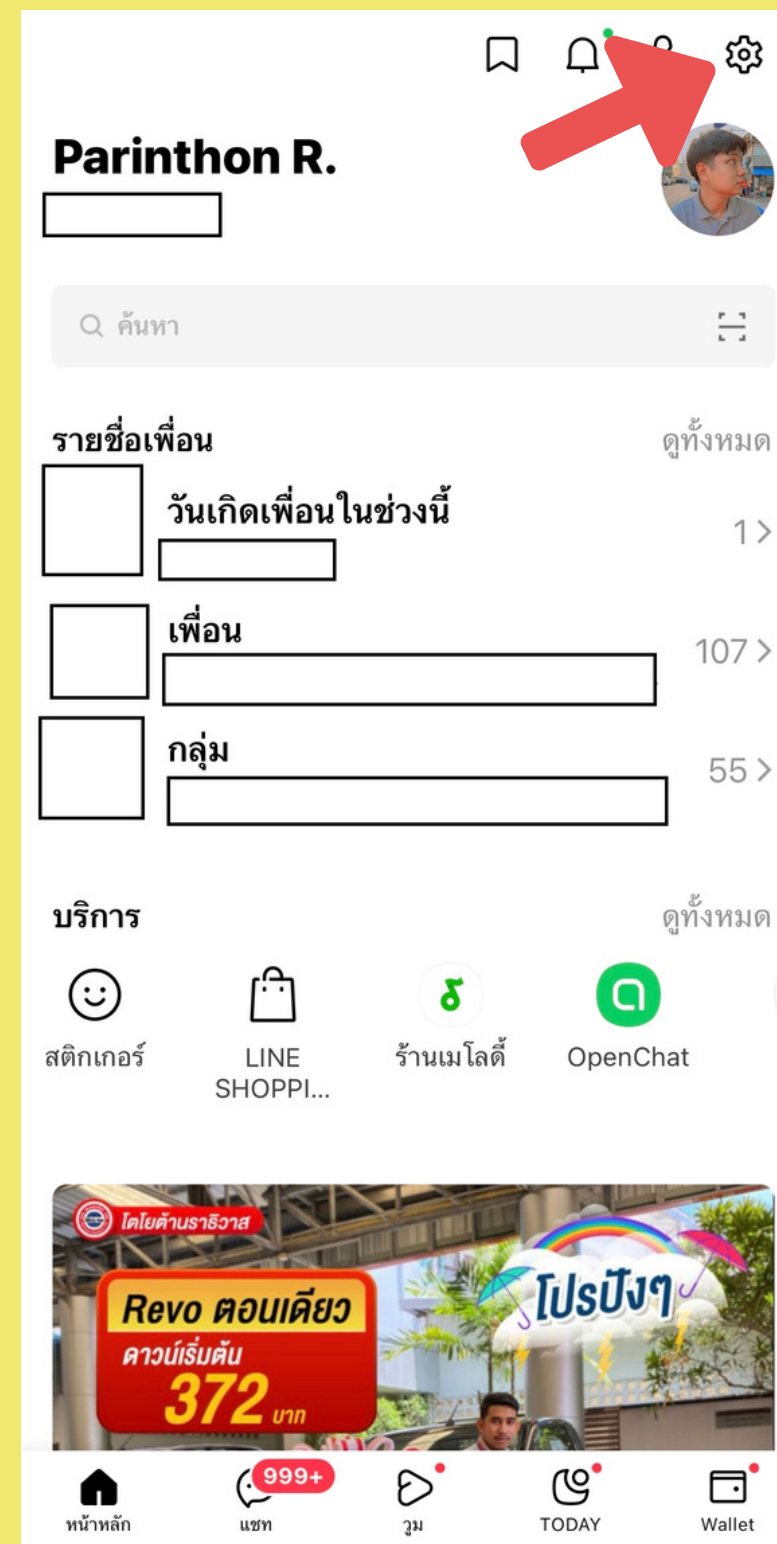
 แตะ ความเป็นส่วนตัว

03

หน้าต่างในเมนู ความเป็นส่วนตัว


03

01



การตั้งค่าความเป็นส่วนตัว

Line

01 ไปที่ เมนู  ตั้งค่า

02  แตะ ความเป็นส่วนตัว

03 หน้าต่างในเมนู ความเป็นส่วนตัว

03


02

ตั้งค่า



ค้นหา

ข้อมูลส่วนตัว

 บัญชี >


 ความเป็นส่วนตัว >

 Keep >

สำรองข้อมูล & โอนย้ายบัญชี


 สำรองข้อมูลการแชท >

 คิวอาร์โค้ดสำหรับโอนย้ายบัญชีแบบ
ง่าย >

 โอนย้ายบัญชี >

ร้าน

 สติกเกอร์  >

 ธีม >

 LINE Melody >

การตั้งค่าความเป็นส่วนตัว

Line

01

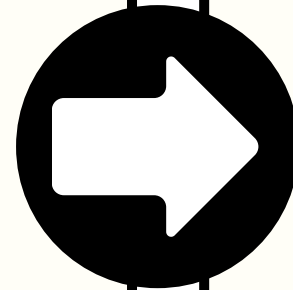
ไปที่ เมนู  ตั้งค่า

02

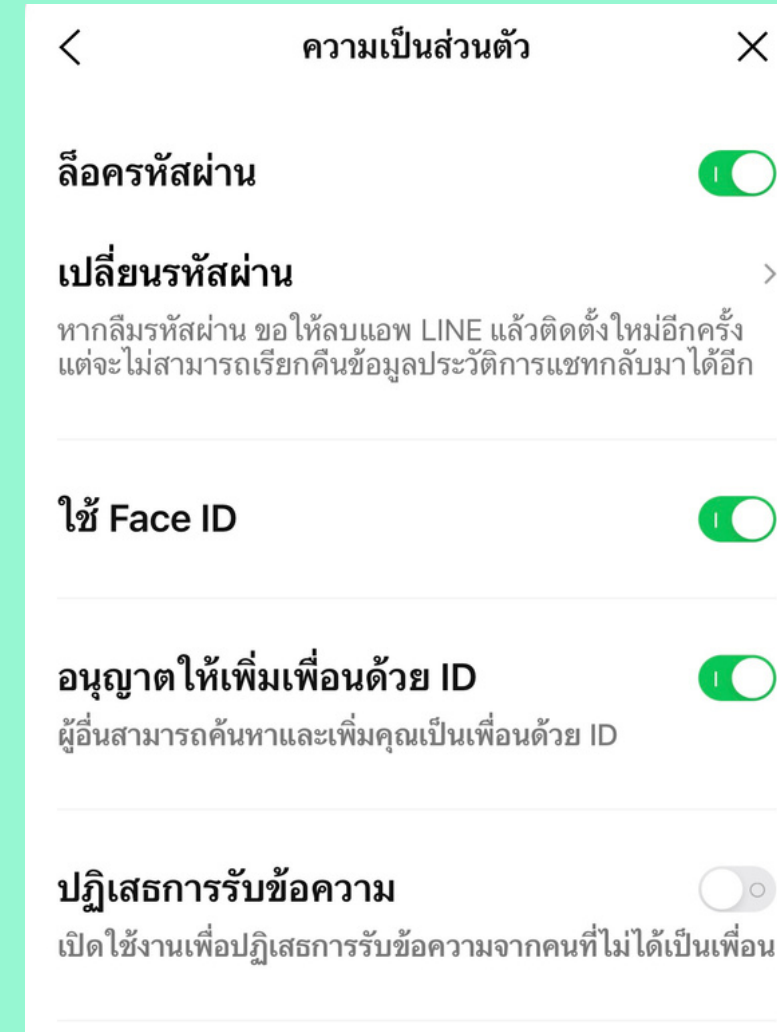
 แตะ ความเป็นส่วนตัว

03

หน้าต่างในเมนู ความเป็นส่วนตัว



03



03

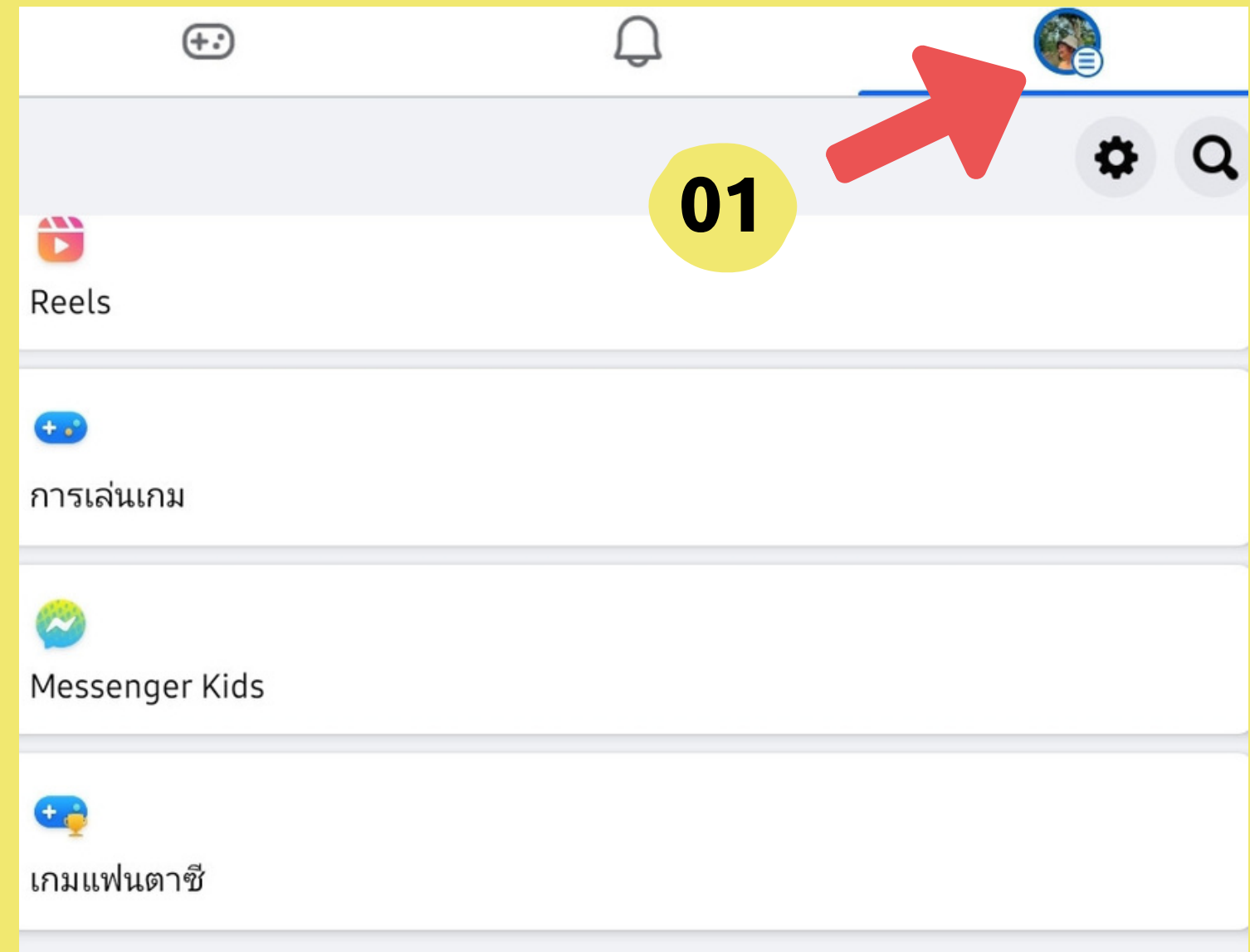
การตั้งพาสเวิร์ด 2 ชั้น

Facebook

- 01** ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02** 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03** 🔒* แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04** แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05** แตะ ตรวจสอบ **06** แตะ เปิด

03

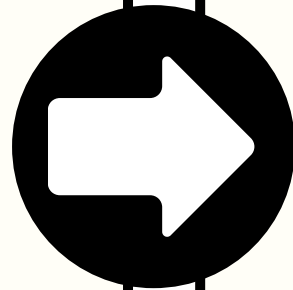
01



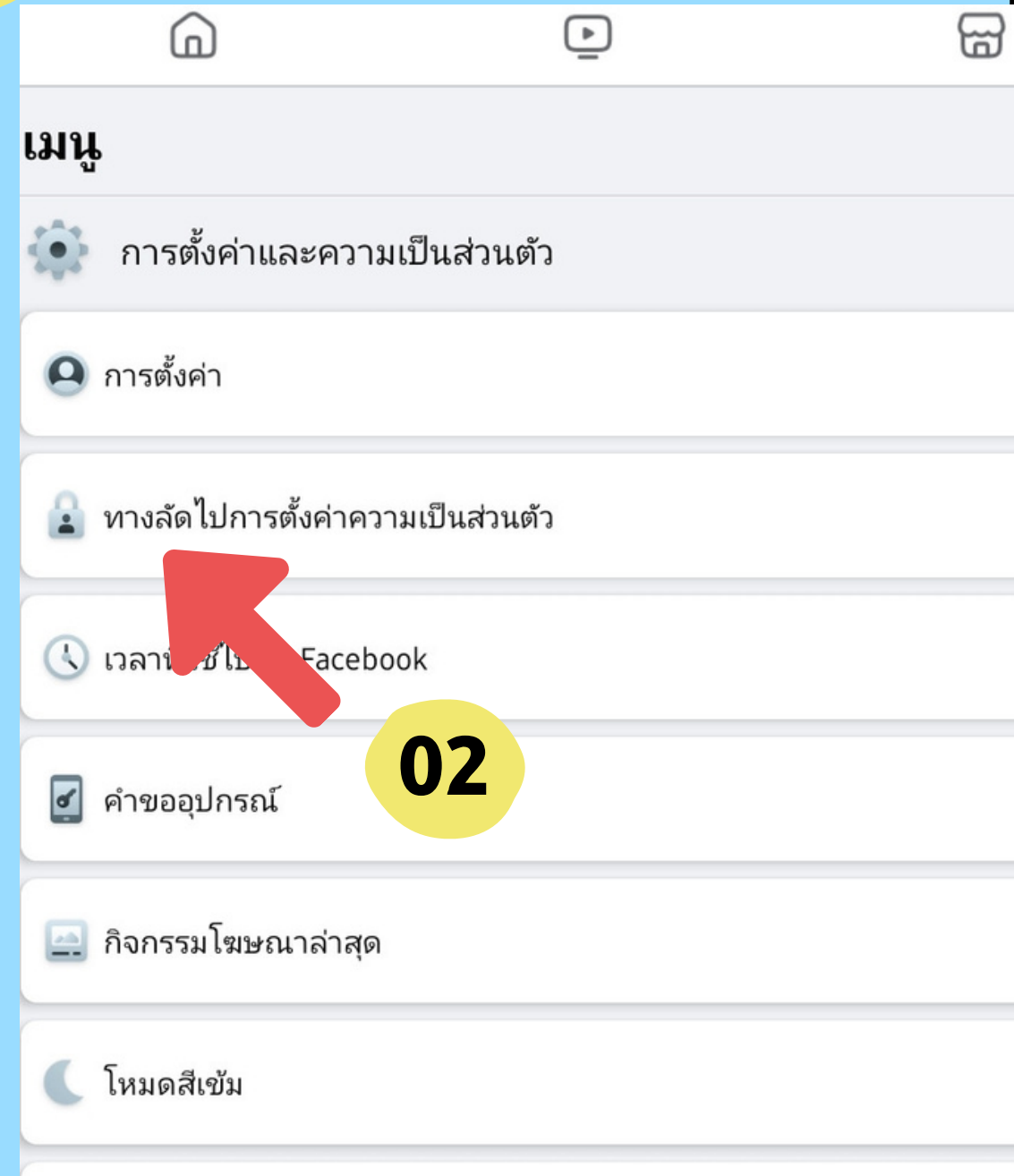
การตั้งพาสเวิร์ด 2 ชั้น

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔓 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05 แตะ ตรวจสอบ
- 06 แตะ เปิด



02



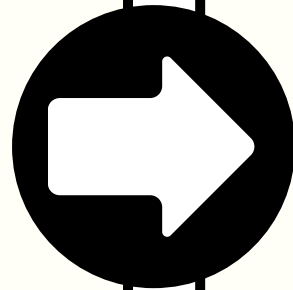
02

03

การตั้งค่าเวอร์ด 2 ชั้น

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🗝️ แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05 แตะ ตรวจสอบ
- 06 แตะ เปิด



03

เครื่องมือที่จะช่วยให้คุณควบคุมความเป็นส่วนตัวและความปลอดภัยบน Facebook

ความเป็นส่วนตัว
ควบคุมว่าจะให้ใครเห็นสิ่งที่คุณแชร์บน Facebook และจัดการข้อมูลที่เราสามารถปรับแต่งประสบการณ์ให้เหมาะกับแต่ละบุคคลได้ดียิ่งขึ้น

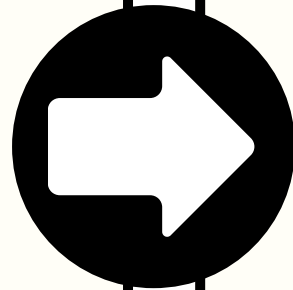
- 🗝️ เริ่มตรวจสอบความเป็นส่วนตัว
- 🎓 เรียนรู้เกี่ยวกับความเป็นส่วนตัวของคุณบน Facebook
- 📍 จัดการการตั้งค่าความเป็นส่วนตัวของคุณ
- ⋮ ดูการตั้งค่าความเป็นส่วนตัวเพิ่มเติม

03

การตั้งพาสเวิร์ด 2 ชั้น

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05 แตะ ตรวจสอบ
- 06 แตะ เปิด

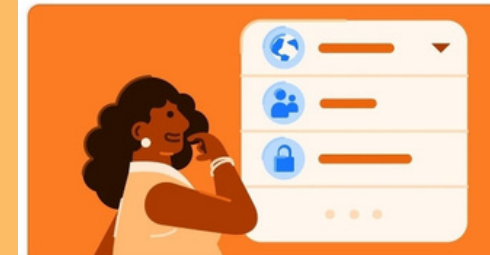


04

การตรวจสอบความเป็นส่วนตัว

เราจะแนะนำการตั้งค่าบางส่วนให้คุณทราบ เพื่อช่วยให้คุณตัดสินใจเกี่ยวกับบัญชีของคุณได้อย่างถูกต้อง

คุณต้องการเริ่มต้นกับหัวข้ออะไร



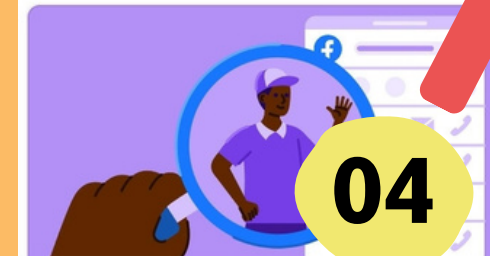
คนที่สามารถเห็นสิ่งที่คุณแชร์ได้

เมื่อวานนี้

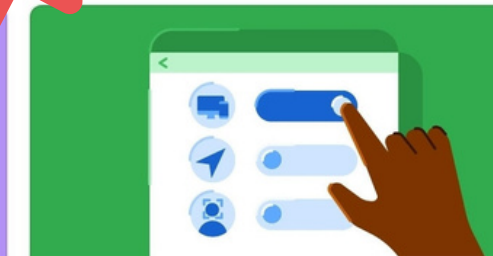


วิธีการรักษาบัญชีของคุณให้ปลอดภัย

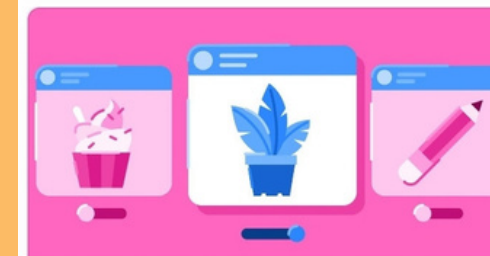
เมื่อวานนี้



วิธีที่คนอื่นจะค้นหาคุณเพบบน Facebook



การตั้งค่าข้อมูลบน Facebook



การกำหนดลักษณะโฆษณาของคุณบน Facebook

เมื่อวานนี้

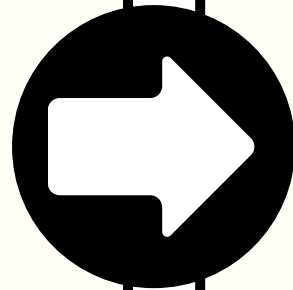
คุณสามารถดูการตั้งค่าความเป็นส่วนตัวบน Facebook เพิ่มเติมได้ในการตั้งค่า

03

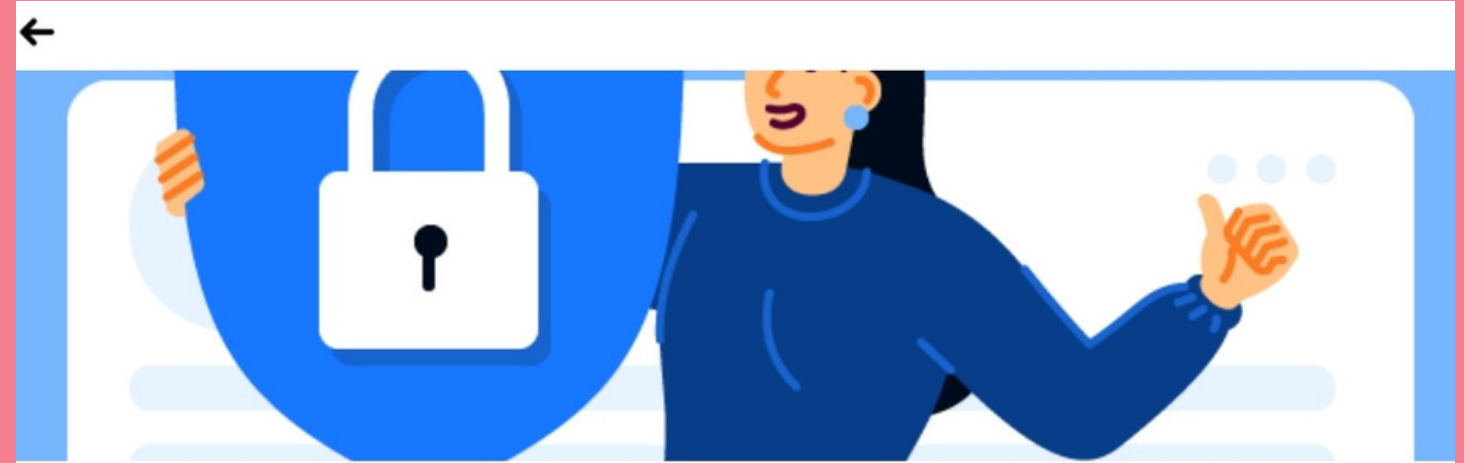
การตั้งพาสเวิร์ด 2 ชั้น

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05 แตะ ตรวจสอบ
- 06 แตะ เปิด



05



วิธีการรักษาบัญชีของคุณให้ปลอดภัย

คุณดำเนินการเรียบร้อยแล้ว ไม่มีขั้นตอนการรักษาความปลอดภัยใดๆ แนะนำเพิ่มเติมในขณะนี้

- 🔑 รหัสผ่านของคุณเดาได้ยากดี
- 🛡️ การยืนยันตัวตนแบบสองชั้นเปิดอยู่
- 🔔 การเตือนการเข้าสู่ระบบเปิดอยู่

05

ตรวจสอบ

03

การตั้งพาสเวิร์ด 2 ชั้น

Facebook

01

ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ
"⚙️ การตั้งค่าและความเป็นส่วนตัว"

02

🔒 แตะ ทางลัดไปการตั้งค่าความ
ความเป็นส่วนตัว

03

🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว

04

แตะ วิธีการรักษาบัญชีของคุณให้
ปลอดภัย

05

แตะ ตรวจสอบ

06

แตะ เปิด

03

06

← รหัสผ่าน

รหัสผ่านของคุณเป็นความลับหรือไม่

หากคุณใช้รหัสผ่าน Facebook ของคุณที่อื่นบนออนไลน์ รหัสผ่านของคุณจะมีความปลอดภัยน้อยลง ปกป้องตัว
คุณเองและเพื่อนๆ ของคุณบน Facebook โดยการเลือกรหัสผ่านที่เดาได้ยากขึ้น

เปลี่ยนรหัสผ่าน

ข้าม

การตั้งพาสเวิร์ด 2 ชั้น

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 🔒 แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05 แตะ ตรวจสอบ
- 06 แตะ จัดการ

03

07

← การยืนยันตัวตนแบบสองชั้น

การยืนยันตัวตนแบบสองชั้นเปิดใช้งานอยู่

เราจะขอรหัสและรหัสผ่านของคุณ หากเราพบว่าคุณมีความพยายามเข้าสู่ระบบจากอุปกรณ์หรือเบราว์เซอร์ที่ไม่รู้จัก

จัดการ

06

การตั้งพาสเวิร์ด 2 ชั้น

Facebook

- 01 ไปที่ ☰ แล้วเลื่อนลงมาจะเจอกับ "⚙️ การตั้งค่าและความเป็นส่วนตัว"
- 02 ⚔️ แตะ ทางลัดไปการตั้งค่าความเป็นส่วนตัว
- 03 🔒 แตะ เริ่มตรวจสอบความเป็นส่วนตัว
- 04 แตะ วิธีการรักษาบัญชีของคุณให้ปลอดภัย
- 05 แตะ ตรวจสอบ
- 06 แตะ จัดการ

03

07

← การยืนยันตัวตนแบบสองชั้น



เปิดใช้งานการยืนยันตัวตนแบบสองชั้นแล้ว

เราจะขอรหัสยืนยันผ่านทางวิธีการรักษาความปลอดภัยของคุณหากเราสังเกตเห็นความพยายามเข้าสู่ระบบจากอุปกรณ์หรือเบราว์เซอร์ที่ไม่รู้จัก [ต้องการความช่วยเหลือใช่ไหม](#)

ปิด

วิธีการรักษาความปลอดภัยของคุณ

☎️ *** **63

ข้อความ SMS

📱 แอปยืนยันตัวตน

คุณจะได้รับรหัสเข้าสู่ระบบผ่านแอปการยืนยันตัวตน

➕ เพิ่มวิธีการสำรอง

ตั้งค่าวิธีการสำรองเพื่อให้คุณสามารถเข้าสู่ระบบได้แม้ว่าวิธีการรักษาความปลอดภัยของคุณจะใช้งานไม่ได้ก็ตาม

📱 แอปยืนยันตัวตน

คุณจะได้รับรหัสเข้าสู่ระบบผ่านแอปการยืนยันตัวตน

📄 รหัสกู้คืน

ใช้รหัสกู้คืนเพื่อเข้าสู่ระบบหากคุณทำโทรศัพท์หายหรือไม่สามารถรับรหัสยืนยันผ่านทางข้อความ SMS หรือแอปยืนยันตัวตนได้

🔒 คีย์รักษาความปลอดภัย

ใช้คีย์รักษาความปลอดภัยตัวจริงเพื่อช่วยปกป้องบัญชี Facebook ของคุณจากการเข้าถึงที่ไม่ได้รับอนุญาต โดยที่คุณจะไม่จำเป็นต้องป้อนรหัส

🔊 ขั้นสูง

รับการแจ้งเตือนทางข้อความ SMS เกี่ยวกับข้อความใหม่ โฟสต์ และอื่นๆ

การตั้งพาสเวิร์ด 2 ชั้น

Line

01

ไปที่ เมนู  ตั้งค่า

02

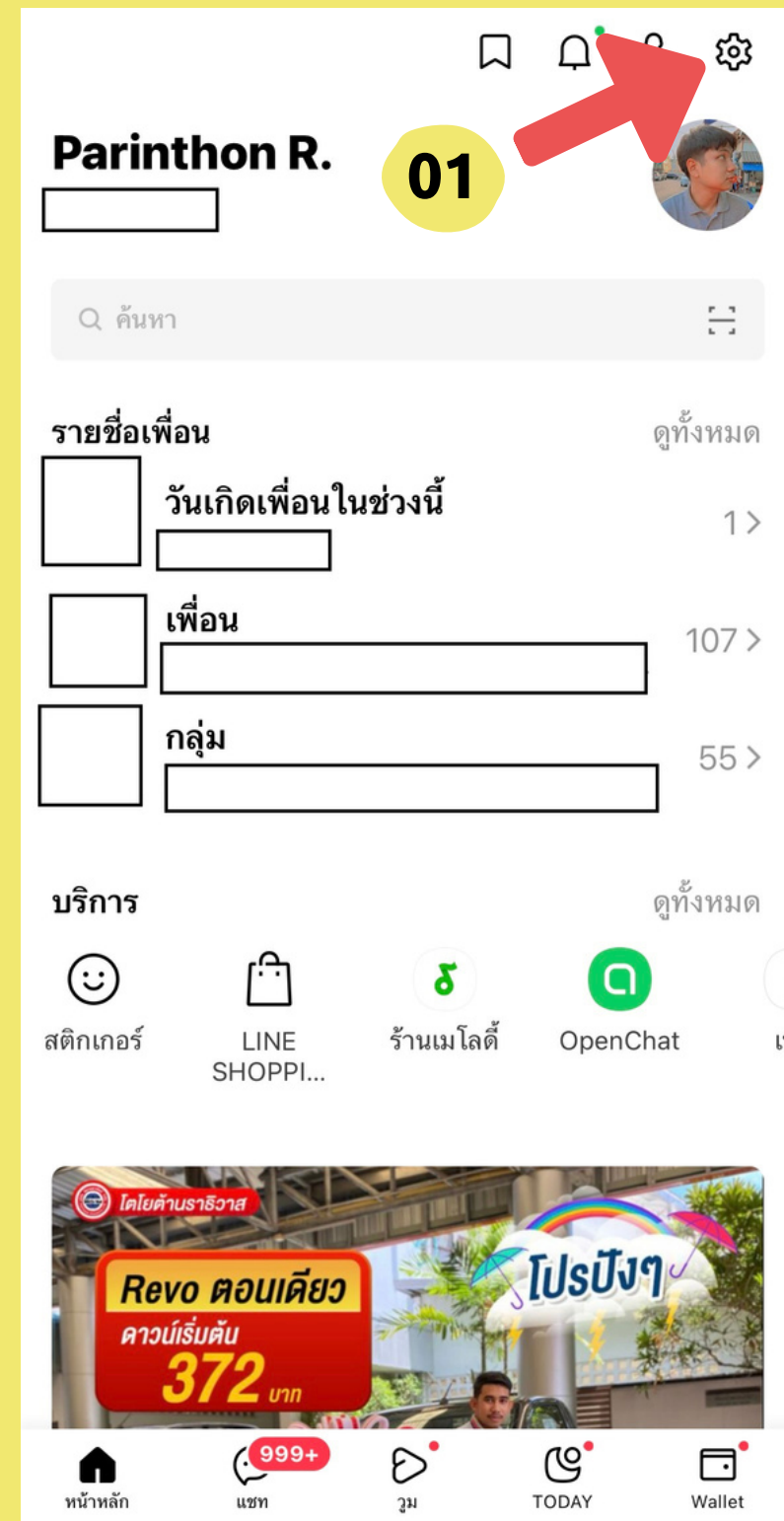
แตะ บัญชี

03

แตะ เปิดฟังก์ชัน “การตรวจสอบยืนยัน 2 ระดับ”

03

01



การตั้งพาสเวิร์ด 2 ชั้น



Line

01

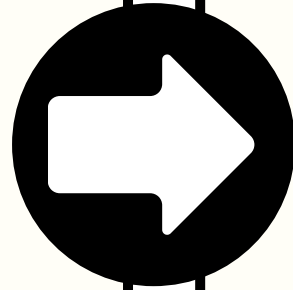
ไปที่ เมนู  ตั้งค่า

02

แตะ บัญชี

03

แตะ เปิดฟังก์ชัน “การตรวจสอบยืนยัน 2 ระดับ”



02



03

การตั้งพาสเวิร์ด 2 ชั้น




Line

01

ไปที่ เมนู  ตั้งค่า

02

แตะ  แตะ บัญชี

03

แตะ เปิดฟังก์ชัน “การตรวจสอบยืนยัน 2 ระดับ”

03

03



04

**ระวังอันตรายจากการ
หลอกหลวง**

ระวังอันตรายจากการ หลอกหลวง

บนอินเทอร์เน็ตนั้นมีการหลอกหลวงสารพัดรูปแบบ ไม่ว่าจะสร้างหน้าเว็บหลอก โดยอาศัยช่องโหว่ด้านพฤติกรรมของผู้คนบนอินเทอร์เน็ต ซึ่งยังไม่มีระบบใดๆ ป้องกันได้ โดยจะยกตัวอย่างวิธีการหลอกได้ ดังนี้



อาศัยความอยากรู้อยากเห็นของแต่ละคน

โดยหลอกด้วยหัวข้อข่าวหรือเรื่องราวที่น่าสนใจ เมื่อคลิกเข้าไปก็จะให้กรอกข้อมูล หรือ นำเข้าเว็บพนันออนไลน์

อาศัยความกลัว


เช่น call center โดยโทรศัพท์เข้าหาเหยื่อแจ้งว่าเกี่ยวข้องกับการส่งพัสดุผิดกฎหมาย การกระทำผิดกฎหมายหรือโดนอายัดบัญชีธนาคาร แล้วจะอ้างเป็นหตำรวจหรือเจ้าหน้าที่รัฐ ข่มขู่เรื่องกฎหมาย

ชอบของฟรี

หลอกให้โหลดโปรแกรมที่มีลิขสิทธิ์ฟรี แล้วแฝงด้วยไวรัส หรือ โปสท์แจกของ เช่น iPhone 15 Pro Max เมื่อยอดการแชร์เยอะ ก็จะเปลี่ยนข้อความที่โปสท์ เป็นข้อความเชิญชวนของเว็บพนัน

อาศัยความใจดี

ใช้ความเป็น "ดราม่า" หลอกให้บริจาค เช่น เพื่อผู้พิการ ผู้ป่วยระยะสุดท้าย ช่วยเหลือแมว-หมาไร้บ้าน เป็นต้น ทำให้คนที่พบเห็นอดสงสารไม่ได้



อาศัยช่องทางออนไลน์

เข้ามาตีสอนิก เข้ากลุ่ม หรือแม้แต่เข้าถึงตัวจริง เพื่อหลอกหลวง เช่น ลงทุนร่วมกัน หลอกขาย บริการอื่นๆ ประทุษร้ายต่อร่างกายหรือทรัพย์สิน

▶

ตัวอย่างการหลอกหลวง



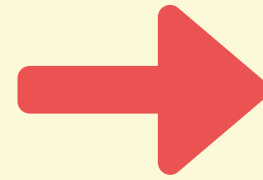
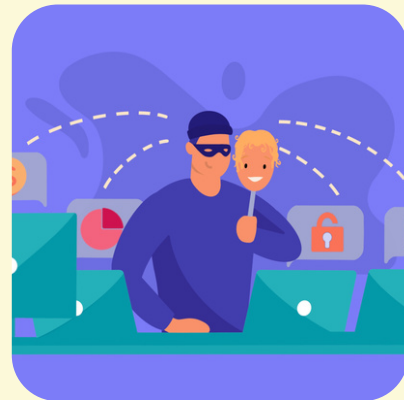
ร้องถูกหลอกสแกนหน้า ดูดเงิน 2 ล้าน

แก๊งคอลเซ็นเตอร์อ้างเป็นกรมที่ดิน

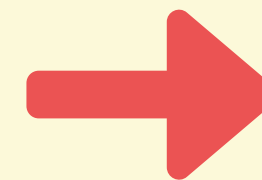
ข้าราชการเกษียณ ร้องถูกแก๊งคอลเซ็นเตอร์วิดีโอคอลอ้างเป็นกรมที่ดิน ให้เพิ่มเพื่อนทางไลน์เพื่อคืนเงินภาษี สุดท้าย หลอกสแกนหน้า ดูดเงินจากบัญชี 2 ล้านบาท

ลำดับเหตุการณ์

แอบอ้างเป็นเจ้าของหน้าที่



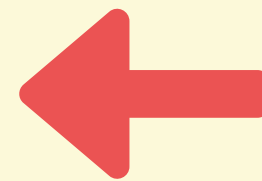
โทรมาเพื่อให้แอดไลน์



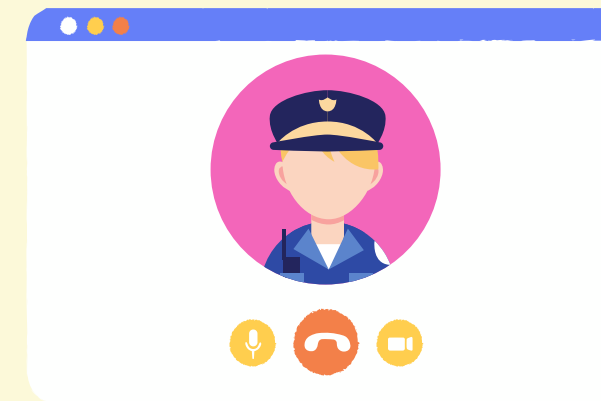
ทำให้ผู้เสียหายตกใจโดยบอกกล่าวละเอียดยข้อมูลส่วนบุคคลได้ถูกต้อง



หลอกให้ผู้เสียหายทำตามขั้นตอนเพื่อโอนทรัพย์สินแก่มีจจาชีพ



ผู้เสียหายหลงเชื่อจึงวิตโศคุยเรื่อง สิทธิพิเศษต่างๆ



อ้างว่ามีพัสดุมาส่งที่บ้าน
โดยให้ชำระเงินปลายทาง

อ้างว่ามีส่วนเกี่ยวข้องกับ
กับอาชญากรรมร้ายแรง

อ้างว่าค้างชำระค่าบัตรเครดิต

อ้างว่าค้างชำระค่าบริการ
เครือข่ายโทรศัพท์มือถือ

อ้างว่าเป็นเจ้าหน้าที่ของรัฐเพื่อตรวจสอบข้อมูล
และหลอกให้ติดต่อทางไลน์

อ้างว่าถูกอายัดบัญชี

อ้างว่าได้เงินคืนจากการเสียหาย

ข้ออ้าง

แก๊งคอลเซ็นเตอร์



www.PreventOnlineCrime.com

ข้ออ้าง call center



ROMANCE SCAM

การหลอกให้หลงรัก หลอกให้เชื่อว่ารัก หลอกให้เชื่อใจ ให้ความหวังว่าแต่งงานใช้ชีวิตอยู่ด้วยกันตลอดไป และใช้ความรักความเชื่อใจหรือความหวังของเหยื่อเพื่อแสวงหาประโยชน์

อะไรคือสัญญาณ

- โปรไฟล์ชวนหลงใหล
- อาชีพการงานดี
- สร้างบ้าน
- ซื้อรถยนต์
- หลอกโอนเงิน

www.PreventOnlineCrime.com

Romance scam
“หลอกให้รัก แล้วจากไป”

ระวัง !! "บัญชีม้า"

มิจฉาชีพหลอกเปิด

กลลวงของมิจฉาชีพ



ประกาศรับสมัครงานออนไลน์

จะหลอกให้เปิดบัญชีธนาคารผ่านช่องทางออนไลน์ และหลอกให้ส่งหลักฐานข้อมูลส่วนตัว



ชักชวนเพื่อเล่นการพนันออนไลน์

และหลอกให้เปิดบัญชีธนาคารไว้สำหรับรับเงินจากการเล่นการพนัน



ประกาศเงินกู้ออนไลน์

หลอกให้เปิดบัญชีและส่งข้อมูลส่วนตัวมาก่อนทำการกู้ยืม



มิจฉาชีพจะทำการสุ่มเบอร์โทรศัพท์เพื่อโทรหาเหยื่อ และแอบอ้างเป็นเจ้าของที่ต่าง ๆ ให้ส่งข้อมูลส่วนตัวมาไว้สำหรับการเปิดบัญชีธนาคาร

www.PreventOnlineCrime.com

บัญชีม้า

หลอก ทำบุญออนไลน์

การหลอกทำบุญออนไลน์มีจดาชีพโพสต์ข้อความโฆษณาตาม
สื่อออนไลน์ต่าง ๆ ผ่านระบบคอมพิวเตอร์เพื่อเชิญชวนทำบุญ
การกระทำดังกล่าวของมีจดาชีพนั้นผิดตาม พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
และที่แก้ไขเพิ่มเติม มาตรา 14 (1)

พฤติกรรมของมีจดาชีพ

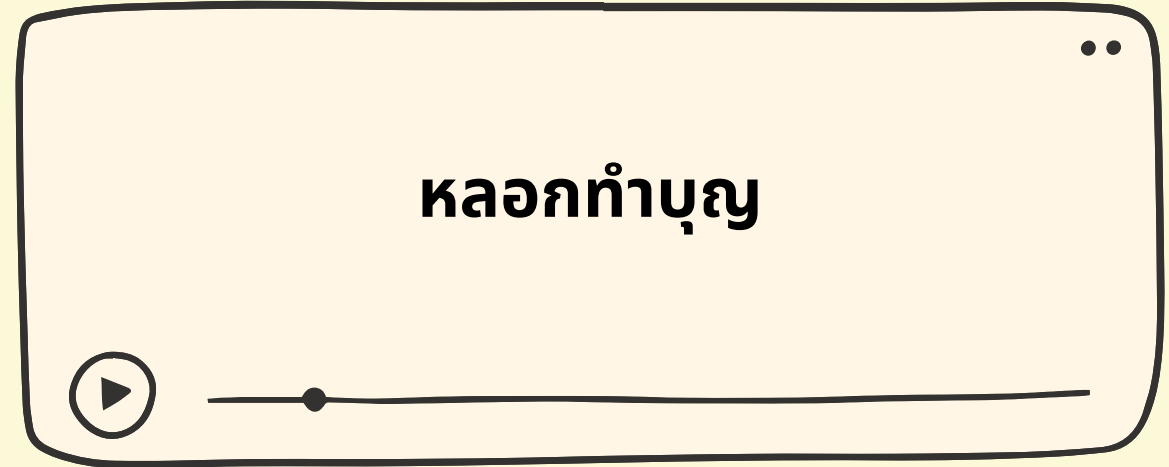
สมัครเฟซบุ๊กปลอม ให้มีโปรไฟล์ดี
หลอกให้คนหลงเชื่อมาทำบุญออนไลน์

หลอกเหยื่อให้ดาวน์โหลดแอปพลิเคชัน
ทำบุญออนไลน์ด้วย

หลอกเหยื่อที่เข้ามาคุย
ให้โอนเงินทำบุญตามสถานที่ต่างๆ

จากนั้นหลอกให้เหยื่อโอนเงินเข้าแอปพลิเคชัน
โดยผ่านบัญชีม้า

www.PreventOnlineCrime.com



หลอกให้โอนเงินค่ามัดจำ สินค้า Pre-order



1 โอนเงินมัดจำอย่างน้อย
50 %



2 เร่งรีบ
ให้โอนเงิน



3 ถึงกำหนดส่งของแล้วไม่ยอมส่งสินค้า



เลื่อนส่งสินค้า
เช่น เลื่อนเวลาการส่งสินค้า
สินค้าติดศุลกากร สินค้าหมด ฯลฯ

www.PreventOnlineCrime.com

หลอกให้โอนค่ามัดจำ



เพจจริง เพจปลอม สังเกตอย่างไร?



แอดเคาท์หรือหน้าเพจใน facebook ทั้งของคนดัง ร้านค้า หรือองค์กรนั้น ถ้าเป็นบุคคลที่มีชื่อเสียงหรือองค์กรใหญ่ๆ ก็จะมีการยืนยันว่าเป็นเจ้าของ จะสังเกตได้สัญลักษณ์ (Verify)

- เพจต้องได้รับการยืนยัน** มีเครื่องหมายรับรองตัวตน **Verified badge**
- ดูรายละเอียดของเพจ** เช่น วันที่สร้างเพจ และเคยเปลี่ยนชื่อเพจมาก่อนไหม
- ระวังโดนหลอกยกยอดคนถูกใจ** มีจข อาจพิมพ์ยอดผู้ติดตามปลอมไว้ที่รายละเอียดของเพจ
- ชื่อเพจสะกดถูกต้องหรือไม่** มีจข อาจทำเลียนแบบ เช่น มีจุดหรืออักขระพิเศษ
- การโพสต์เนื้อหาและโต้ตอบในเพจ** จำนวนคนกดไลค์ และคอมเมนต์
- สังเกตที่ url ของเพจ** อาจเป็นคำแปลกๆ ที่ไม่มีความหมาย

ระวัง! LINE ปลอมจากมิจฉาชีพ



ส่วนใหญ่ของแก๊งมิจฉาชีพมักจะเลือกใช้ Line ติดต่อและแอบอ้างเป็นเจ้าของหน้าหรือ Line ปลอม ดังนั้น ควรจะสังเกตสัญลักษณ์



ประเภทของ Line account



UNVERIFIED ACCOUNT
บัญชีทั่วไป



VERIFIED ACCOUNT
บัญชีรับรอง



PREMIUM ACCOUNT
บัญชีพรีเมียม

1. บัญชีทั่วไป (โล่เทา) คือ บัญชีทั่วไป
2. บัญชีรับรอง (โล่น้ำเงิน) คือ บัญชีที่ได้รับการรับรองจาก LINE ว่ามีตัวตนจริง และน่าเชื่อถือ
3. บัญชีพรีเมียม (โล่เขียว) คือ บัญชีที่ได้รับการรับรองจาก LINE มีค่าใช้จ่ายค่อนข้างสูง เหมาะกับธุรกิจขนาดใหญ่



ใช้ชื่อและรูปโปรไฟล์เหมือนของจริง

ไม่มีเครื่องหมายโลโก้หรือสีฟ้า



มักเข้ามาหาก่อน โดยไม่ได้เป็นเพื่อนกันมาก่อน

บทสนทนาพูดคุยโต้ตอบแบบคนจริงๆ



มักจะมีการสอบถามขอข้อมูลส่วนตัว และจะให้โอนเงินเพื่อเป็นค่าธรรมเนียม

วิธีสังเกต Line Official (ปลอม)

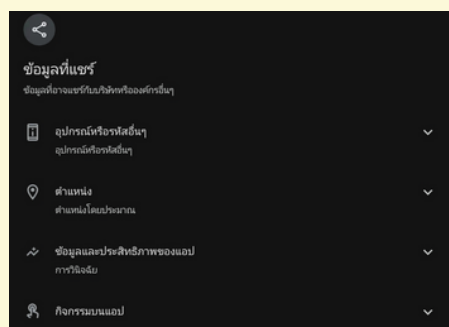


05

**ระวัง! แอปพลิเคชัน
อันตราย**

ระวัง! แอปพลิเคชันอันตราย

อุปกรณ์สมาร์ทโฟนหรือแท็บเล็ตในปัจจุบันนี้มีความสามารถมากมาย โดยสามารถดาวน์โหลดเพิ่มจาก App Store (iOS) หรือ Play Store (Android) ถ้าจะติดตั้งแอปพลิเคชัน นอกเหนือจากนั้น ต้องระมัดระวังเป็นอย่างมาก



Installs
1,000,000,000+

อย่าไว้ใจแอปพลิเคชันนอก Official Store

การติดตั้งแอปพลิเคชันด้วยวิธีการอื่น ๆ นั้นเป็นการเพิ่มความเสี่ยงที่จะได้รับแอปพลิเคชันแต่อาจจะแฝงมัลแวร์หรือไวรัสมาด้วยก็ได้

เช็คคะแนนรีวิวแอปพลิเคชัน

อ่านรีวิวของแอปพลิเคชันก่อนกดดาวน์โหลดใช้งาน นี่เป็นอีกหนึ่งวิธีที่ช่วยให้เราตรวจสอบได้ว่าแอปพลิเคชันสามารถใช้งานได้จริง

อ่านรายละเอียดคำอธิบายของแอปพลิเคชันก่อนเลือกติดตั้ง

รายละเอียดแอปพลิเคชันจะมีการแจ้งการเข้าถึงข้อมูลโทรศัพท์ เช่น การเข้าถึงกล้อง รายชื่อเบอร์โทรศัพท์

ดูยอดการติดตั้งแอปพลิเคชัน

แอปพลิเคชันที่มียอดติดตั้งมากกว่า 1,000,000 ครั้ง กับ 1,000 ครั้ง ความที่น่าเชื่อถือของแอปมีความแตกต่างกันมาก

ตัวอย่างมิจลาชีพหลอกให้หลง แอปพลิเคชันอันตราย



ผู้ประกาศข่าวสาวถูกแก๊งคอลเซ็นเตอร์แอบอ้างกรมที่ดิน หลอกอัปเดตข้อมูลที่ดิน ดาวน์โหลดแอปฯ หลอกสแกนใบหน้า หลอกขอเลข OTP ก่อนรู้ความจริงถูกถอนเงินในบัญชี แคมถูกกดเงินสดผ่านวงเงินบัตรเครดิต เสียหายราว 1 ล้านบาท พบกรมที่ดิน ประกาศแล้ว ยังมีผู้เสียหายแจ้งเบาะแสนับร้อยราย หลอกให้โหลดแอปฯ Smartland



4 วิธีการป้องกันตัวเอง จากไวรัส

การป้องกันตัวเองจากสิ่งแปลกปลอมไม่เพียง
ประสงค์ สามารถทำได้หลายวิธี โดยควรทำทั้ง ใน
คอมพิวเตอร์ โทรศัพท์ และแท็บเล็ต



คิดให้ดีก่อนจะคลิกลิงก์หรือดาวน์โหลดข้อมูล

เว็บแจกโปรแกรม โปรแกรมเถื่อน มักจะแฝงด้วยโปรแกรมที่เราไม่
ต้องการ เพราะอาจจะมีความเสี่ยงที่จะติดมัลแวร์

อย่าเชื่อหน้าต่างป๊อปอัพที่ชวนให้คุณกดคลิก

เวลาที่คุณท่องเว็บ คุณอาจพบเว็บที่มีโฆษณา เด็งขึ้นมาเป็น
หน้าต่างป๊อปอัพ ให้ดาวน์โหลด หรือ เป็นข้อความ “เครื่องคุณ
ติดไวรัส กดที่นี่เพื่อสแกนไวรัส”

สำหรับ Android ให้ยกเลิกการอนุญาตให้ติดตั้ง แอปพลิเคชันภายนอก (Unkown Sources)

ควรตรวจสอบ การอนุญาตให้ติดตั้งแอปพลิเคชันภายนอก
(Unkown Sources) ของคุณเปิดอยู่หรือไม่ ถ้าเปิดอยู่เป็น
ช่องทางที่มีโอกาสหลอกให้เราติดตั้งแอปพลิเคชัน ไม่พึง
ประสงค์ได้

หมั่นสแกนไวรัสเป็นประจำ


ไม่ว่าจะเป็นคอมพิวเตอร์ โทรศัพท์ หรือแท็บเล็ต ต่างก็มี
ไวรัส ดังนั้นการที่สแกนไวรัสเป็นประจำก็สามารถ
ป้องกันภัยออนไลน์ได้รูปแบบหนึ่ง

การยกเลิกการอนุญาตให้ติดตั้งแอปพลิเคชันภายนอก (Unkown Sources)

01

เข้า  "การตั้งค่า"

02

แตะ  "ความปลอดภัยและความเป็นส่วนตัว"

03

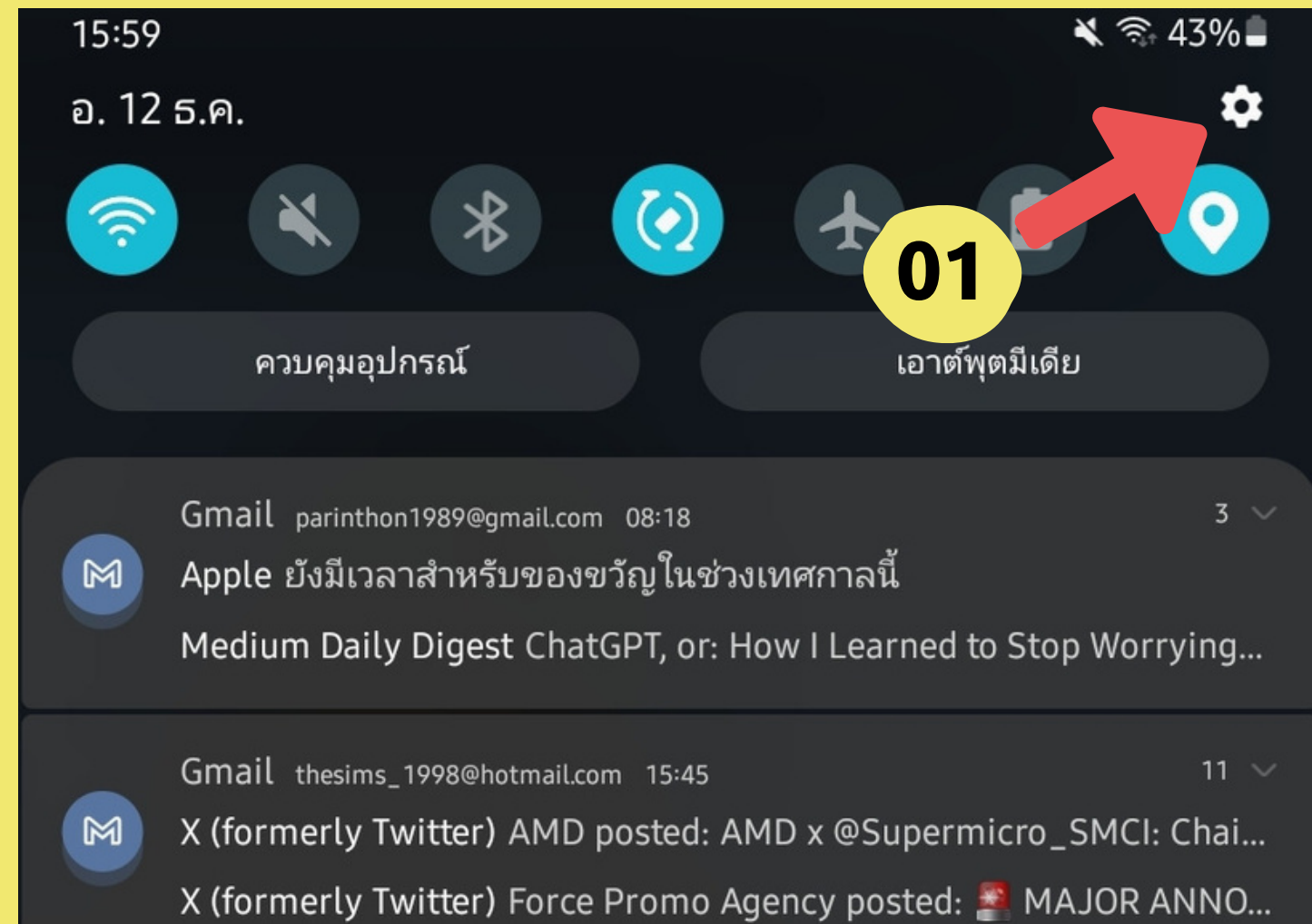
แตะ "ติดตั้งแอปที่ไม่รู้จัก"

04

เลื่อน ปิด เพื่อไม่อนุญาตในการติดตั้งแอปพลิเคชันภายนอก ผ่านแอป


05

01




การยกเลิกการอนุญาตให้ติดตั้งแอปพลิเคชันภายนอก (Unkown Sources)

01

เข้า  "การตั้งค่า"

02

แตะ  "ความปลอดภัยและความเป็นส่วนตัว"

03

แตะ "ติดตั้งแอปที่ไม่รู้จัก"

04

เลื่อน ปิด เพื่อไม่อนุญาตในการติดตั้งแอปพลิเคชันภายนอก ผ่านแอป

05

02

การตั้งค่า



จอภาพ

ความสว่าง • Eye comfort shield • แล่นการนำทาง



วอลเปเปอร์และสไตล์

วอลเปเปอร์ • จานสี



ล็อกหน้าจอ

ชนิดการล็อกหน้าจอ



ความปลอดภัยและความเป็นส่วนตัว

ชีวมาตร • ตัวจัดการการอนุญาต



ตำแหน่ง

คำขอตำแหน่ง



ความปลอดภัยและเหตุฉุกเฉิน

ข้อมูลทางการแพทย์

02




การยกเลิกการอนุญาตให้ติดตั้งแอปพลิเคชันภายนอก (Unkown Sources)

01

เข้า  "การตั้งค่า"

02

แตะ  "ความปลอดภัยและความเป็นส่วนตัว"

03

แตะ "ติดตั้งแอปที่ไม่รู้จัก"


04


เลื่อน ปิด เพื่อไม่อนุญาตในการติดตั้งแอปพลิเคชันภายนอก ผ่านแอป

05

03

ความปลอดภัยและความเป็นส่วนตัว

ไอ้ ความปลอดภัยแอป 

อัปเดต 

รายการส่วนตัว 

ระบบป้องกัน

ชีวมาตร

ไฟลเดอร์ที่ปลอดภัย

03


Private Share

แชร์ไฟล์อย่างเป็นส่วนตัว, อนุญาตให้ผู้อื่นดูไฟล์ของคุณได้โดยไม่ต้องแชร์ชื่ และตั้งค่าวันหมดอายุ

ติดตั้งแอปที่ไม่รู้จัก

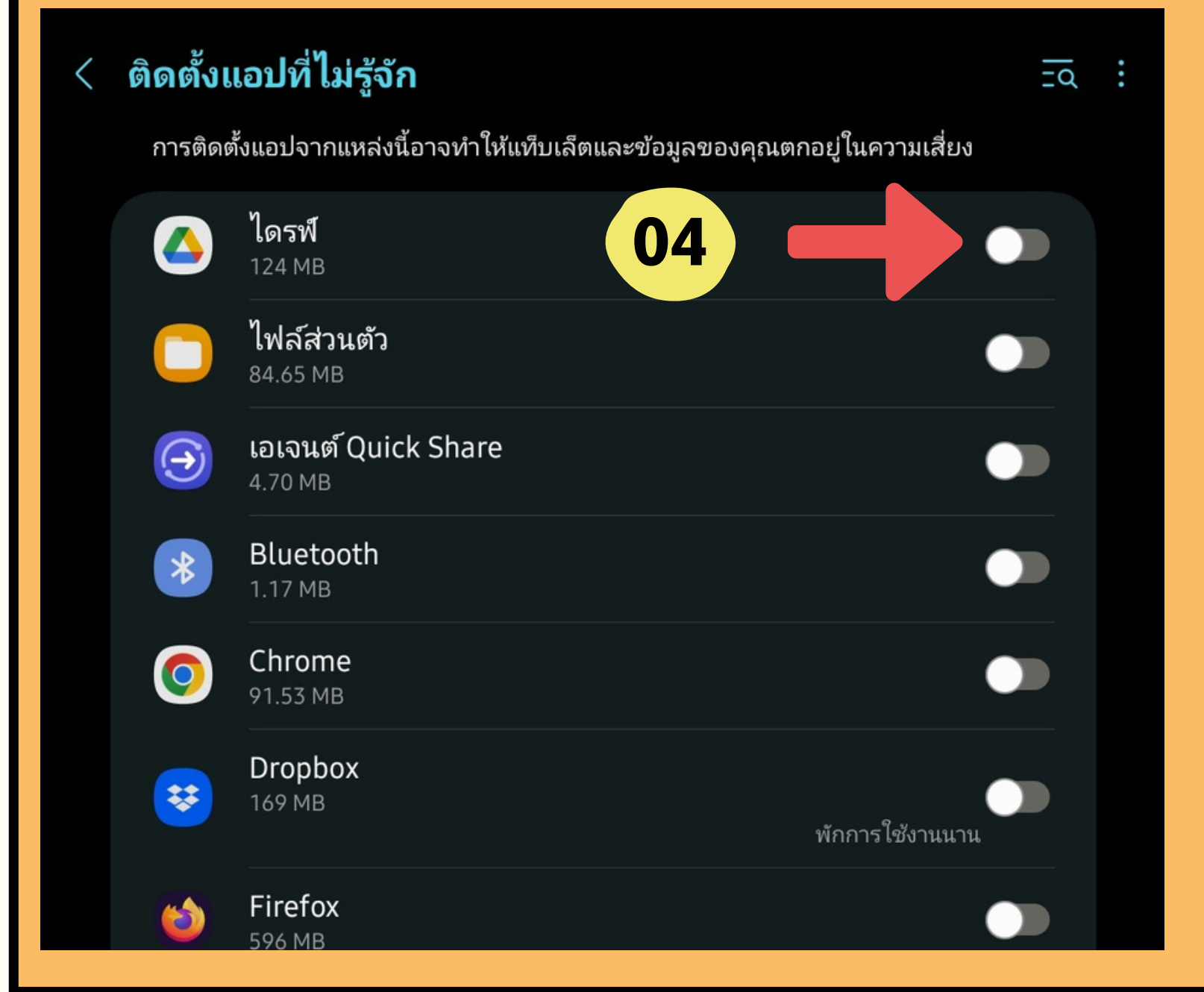
การตั้งค่าความปลอดภัยอื่นๆ

การยกเลิกการอนุญาตให้ติดตั้งแอปพลิเคชันภายนอก (Unkown Sources)

- 01 เข้า  "การตั้งค่า"
- 02 แตะ  "ความปลอดภัยและความเป็นส่วนตัว"
- 03 แตะ "ติดตั้งแอปที่ไม่รู้จัก"
- 04 เลื่อน ปิด เพื่อไม่อนุญาตในการติดตั้งแอปพลิเคชันภายนอก ผ่านแอป

05

04



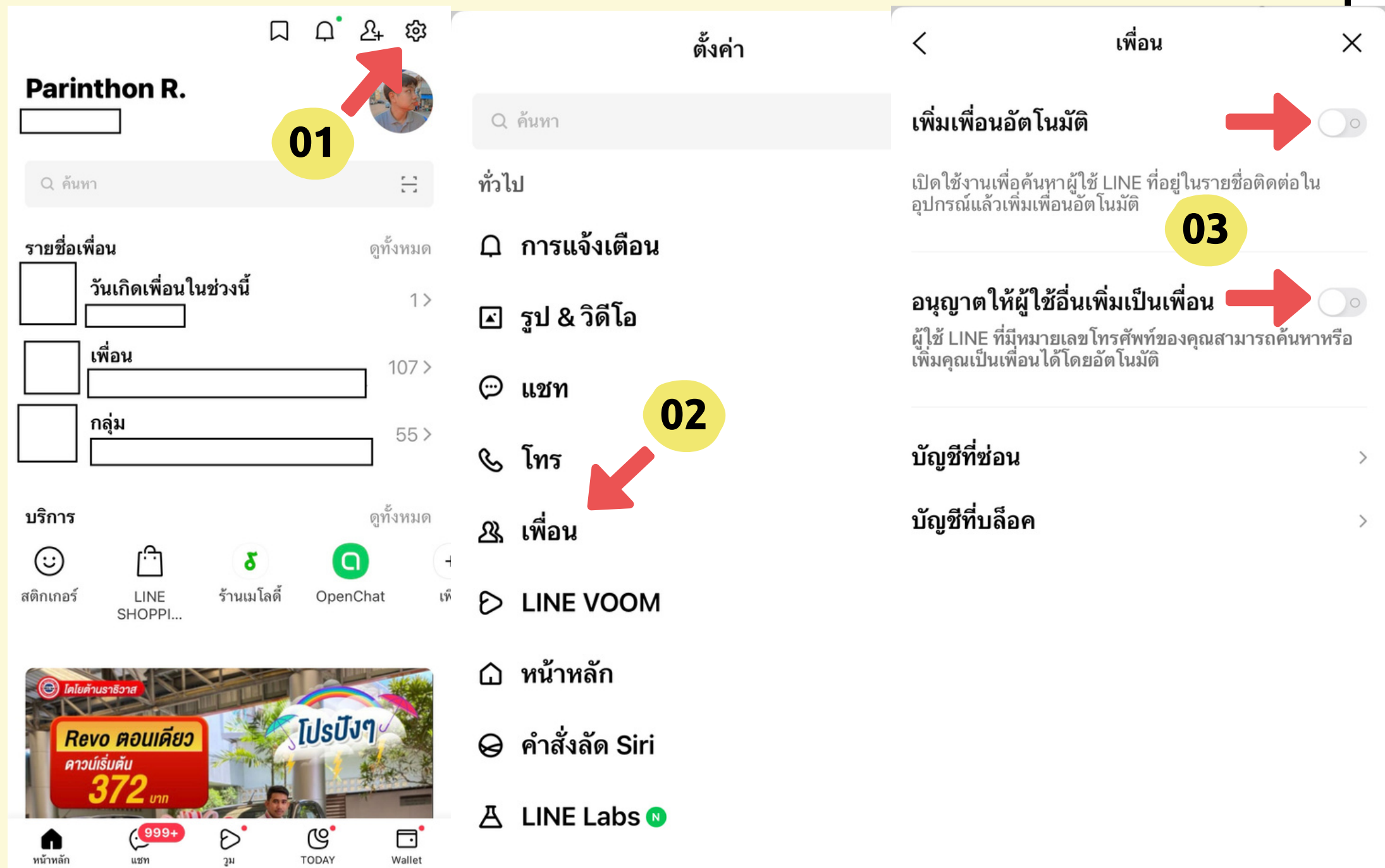


06

วิธีการป้องกันตัวจาก โลกออนไลน์

ไม่อนุญาตให้เพิ่มเพื่อนอัตโนมัติ Line

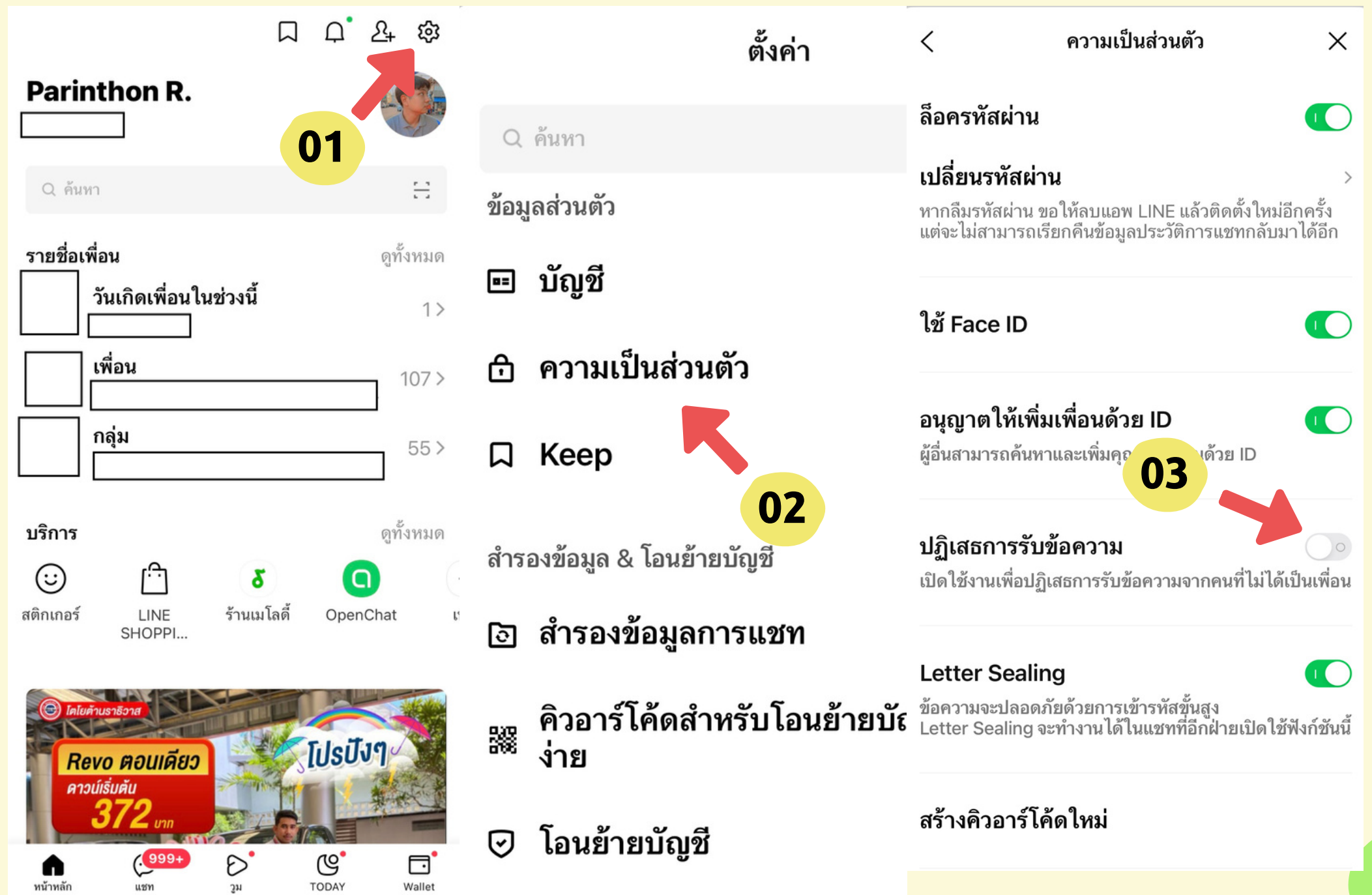
บางครั้งมีจิวาชิพมักเลือกการเพิ่มเพื่อน ผ่านทางหมายเลขโทรศัพท์ และ ใช้ในการหลอกลวง เช่น หลอกว่าเป็นคนรู้จักเปลี่ยนไลน์ใหม่ หรือ ส่งข้อความชวนพนันออนไลน์ การป้องกันเพิ่มเพื่อนอัตโนมัติสามารถทำได้ดังนี้



การบล็อกข้อความจากผู้ อื่นที่ไม่ได้เป็นเพื่อน Line

บางครั้งมีจิวาชิพมักเลือกการเพิ่มเพื่อน ผ่านทาง
หมายเลขโทรศัพท์ และ ใช้ในการหลอกหลวง เช่น
หลอกว่าเป็นคนรู้จักเปลี่ยนไลน์ใหม่ หรือ ส่งข้อความ
ชวนพนันออนไลน์ การป้องกันเพิ่มเพื่อนอัตโนมัติ
สามารถทำได้ดังนี้

06




ท่องเว็บแบบไร้ประวัติ

เมื่อต้องการท่องเว็บแบบส่วนตัว หรือใช้เครื่องสาธารณะ แล้วไม่อยากให้มีการเก็บประวัติการเข้าชมเว็บ รวมทั้งข้อมูลที่คุณได้กรอกเข้าไปในเว็บ โดยไม่ต้องคอยลบเอง เพื่อเก็บข้อมูลเหล่านั้นให้เป็นความลับ





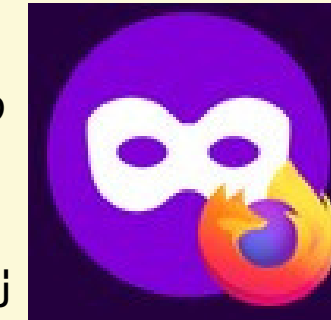
Google chrome

- ที่ด้านขวาบน ให้คลิกเพิ่มเติม : หน้าต่างที่ไม่ระบุตัวตนใหม่
- หรือ กด *Ctrl + Shift + N*
- หน้าต่างใหม่จะปรากฏขึ้น มองหาไอคอนไม่ระบุตัวตน  ที่มุมด้านบน


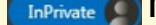


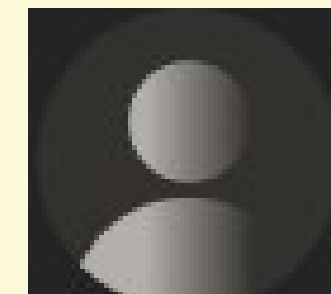
Firefox

- ที่ด้านขวาบน ให้คลิกเพิ่มเติม  หน้าต่างที่ไม่ระบุตัวตนใหม่
- หรือ กด *Ctrl + Shift + P*
- หน้าต่างใหม่จะปรากฏขึ้น มองหาไอคอนไม่ระบุตัวตน  ที่มุมด้านบน



Microsoft Edge

- ที่ด้านขวาบน ให้คลิกเพิ่มเติม  หน้าต่างที่ไม่ระบุตัวตนใหม่
- หรือ กด *Ctrl + Shift + N*
- หน้าต่างใหม่จะปรากฏขึ้น มองหาไอคอนไม่ระบุตัวตน  ที่มุมด้านบน




5 วิธีทำธุรกรรมออนไลน์อย่างปลอดภัย ป้องกันเงินหายไม่รู้ตัว!

สาเหตุหลัก ๆ ที่มักตกเป็นเหยื่อของมิจฉาชีพ คือ เพลอกดลิงก์ปลอม จาก SMS ที่มีจดหมายส่งมาหาเรา หรือเข้าไปกรอกข้อมูลสำคัญในเว็บไซต์ปลอมที่มิจฉาชีพสร้างขึ้น ซึ่งมีลักษณะคล้ายเว็บไซต์จริงที่เราใช้เป็นประจำ



เลือกใช้ App หรือ Website ที่มีความปลอดภัย

- การเลือกใช้แอปพลิเคชันที่น่าเชื่อถือควรโหลดจาก *Official Store* ของระบบปฏิบัติการ เช่น *play store, app store*
- การทำธุรกรรมผ่านเว็บไซต์ ควรมี *HTTPS* และสัญลักษณ์ 

UPDATE

อัปเดตระบบปฏิบัติการ iOS และ Android ให้เป็นเวอร์ชันล่าสุด

การอัปเดตระบบปฏิบัติการ *iOS* หรือ *Android* ช่วยอัปเดตความปลอดภัยในการใช้งานสมาร์ทโฟนให้ดีขึ้นอีก



อัปเดตบัญชีเงินฝากให้ปลอดภัยด้วย OTP

สำหรับ OTP คือรหัสผ่านที่สร้างมาเพื่อเข้าใช้งานเพียงครั้งเดียว โดยจะส่งไปที่เบอร์โทรศัพท์ หรืออีเมลของเรา และรหัสผ่านชุดนี้จะมีเวลาการใช้งานแบบจำกัด หรือถ้ามีการใส่รหัสชุดนี้ผิดก็จะไม่สามารถเข้าใช้งานแอปพลิเคชันได้เลย

5 วิธีทำธุรกรรมออนไลน์อย่างปลอดภัย ป้องกันเงินหายไม่รู้ตัว!

สาเหตุหลัก ๆ ที่มักตกเป็นเหยื่อของมิจฉาชีพ คือ เพลอกดลิงก์ปลอม จาก SMS ที่มีจดหมายส่งมาหาเรา หรือเข้าไปกรอกข้อมูลสำคัญในเว็บไซต์ปลอมที่มีจดหมายสร้างขึ้น ซึ่งมีลักษณะคล้ายเว็บไซต์จริงที่เราใช้เป็นประจำ



เปลี่ยน Password

จะใช้บริการประเภท *Password Generator* ที่ช่วยสร้างรหัสผ่านให้กับเราเป็นตัวเลขแบบสุ่ม ทำให้มิจฉาชีพหมดโอกาสในการคาดเดาแบบ 100%



เปิดการใช้งาน Face ID หรือ แสกนลายนิ้วมือ

เปิดใช้งานระบบ *Biometric* ที่มีในสมาร์ทโฟนของเรา เช่น *Face ID* หรือ *Fingerprint Scanner* จะช่วยป้องกันได้อย่างดี



07

**พสบ.คอมพิวเตอร์ใน
ชีวิตประจำวัน**

โซเซียลอย่างไรไม่ผิดพ.ร.บ.

ตัวอย่างการกระทำผิดพ.ร.บ. 3 ตัวอย่าง

01

นำเข้ามูลปลอม ข่าวปลอม

ข้อมูลปลอม ข้อมูลอันเป็นเท็จ ไม่เป็นความจริง หลอกลวง ที่มีผลทำให้เกิดความเสียหายต่อผู้อื่น จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือ ทั้งจำทั้งปรับ

02

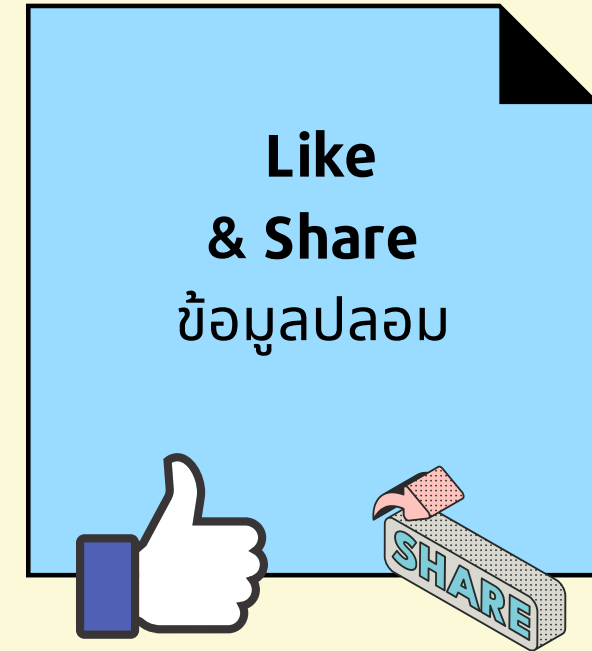
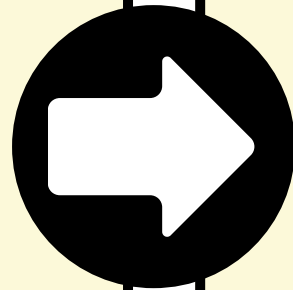
กดไลค์ (Like) กดแชร์ (Share)

Like และ Share ข้อมูลอันเป็นเท็จ จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท

03

การโพสต์ต่อว่าผู้อื่น

หากโพสต์ต่อว่าผู้อื่นโดยข้อมูลนั้นเป็นเท็จ ก็มีโทษ หากเข้าลักษณะเป็นความผิด พ.ร.บ.คอมพิวเตอร์ จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท



01

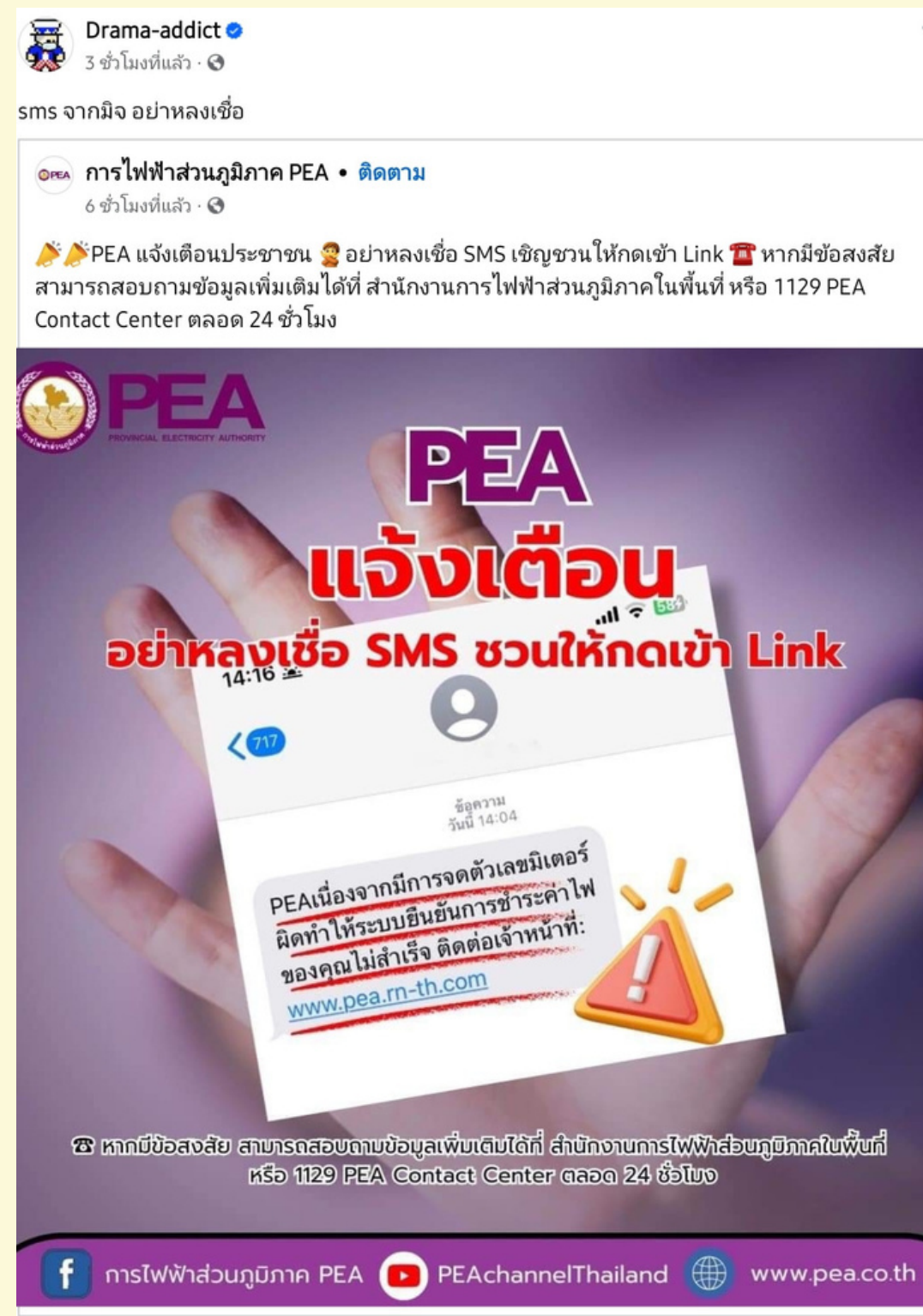
นำภาพหรือข้อความของผู้อื่นไป ใช้ย่ำลึ่มให้เครดิต!

ภาพหรือข้อความที่เผยแพร่อยู่บน
อินเทอร์เน็ตนั้น ล้วนแล้วมีลิขสิทธิ์ ถ้าจำเป็น
ต้องนำมาใช้ แชร์ หรือส่งต่อควรให้เครดิต
เจ้าของ ถ้ามาจากแหล่งออนไลน์ ควรทำเป็น
ลิงค์ให้คลิกกลับไปยังต้นทาง

03

COPYRIGHT

ตัวอย่างการการโพสต์หรือแชร์บนโลกโซเชี่ยลมีเดียอย่าง ปลอดภัย ไม่เข้าข่ายละเมิดลิขสิทธิ์



The image shows a screenshot of a Facebook post from the user 'Drama-addict'. The post is about a service from PEA (Provincial Electricity Authority) regarding SMS. The main text of the post says 'PEA แจ้งเตือนประชาชน อย่าหลงเชื่อ SMS เชิญชวนให้กดเข้า Link' and provides contact information for PEA. Below the text is a graphic with the PEA logo and the text 'PEA แจ้งเตือน อย่าหลงเชื่อ SMS ชวนให้กดเข้า Link'. The graphic also includes a warning icon and a link to the PEA website. At the bottom of the graphic, there is a warning message: 'PEAเนื่องจากการจดตัวเลขมือถือทำให้ระบบยืนยันการชำระค่าไฟของคุณไม่สำเร็จ ติดต่อเจ้าหน้าที่: www.pea.rn-th.com'. The post also includes a comment from a user named 'Drama-addict' with the text 'sms จากมิจ อย่าหลงเชื่อ'.

นำภาพหรือข้อความของผู้อื่นไป ใช้อะลัมให้เครดิต!

ภาพหรือข้อความที่เผยแพร่อยู่บน
อินเทอร์เน็ตนั้น ล้วนแล้วมีลิขสิทธิ์ ถ้าจำเป็น
ต้องนำมาใช้ แชร์ หรือส่งต่อควรให้เครดิต
เจ้าของ ถ้ามาจากแหล่งออนไลน์ ควรทำเป็น
ลิงค์ให้คลิกกลับไปยังต้นทาง

COPYRIGHT

ตัวอย่างการการโพสต์หรือแชร์บนโลกโซเชี่ยลมีเดียอย่าง
ปลอดภัย ไม่เข้าข่ายละเมิดลิขสิทธิ์



The screenshot shows a Facebook post from the page 'devbanban.com' dated May 17 at 12:09pm. The post content is: '63 คลิป+ฟรี Code + Bootstrap + PHP + MySQL คุ้นไป 😊' followed by a link 'https://www.youtube.com/playlist...'. Below the text is a video player with a blue thumbnail featuring the letters 'PHI' and a house icon with 'DEVB.' underneath. To the right of the video, the text reads: 'FREE TUTORIALS : BOOTSTRAP+PHP+DATABASE+D W by devbanban.com - YouTube' and 'FREE TUTORIALS : PHP+DATABASE+BOOTSTRAP+DREAMVEAWER...'. At the bottom of the video player, it says 'YOUTUBE.COM'. Below the video player, it indicates '312 people reached' and has a 'Boost Post' button. At the bottom of the post, there are icons for 'Love', 'Comment', and 'Share', along with a notification of '28' likes and a 'Write a comment...' input field.



08

**การดูแลบุตร หลาน
ในการใช้อินเทอร์เน็ต**

อายุ 4-6 ปี

- ไม่ควรใช้มือถือ หรือ Tablet เลย
- เด็กควรเน้นกิจกรรมเพื่อพัฒนาการเรียนรู้ที่รอบด้าน เช่น กิจกรรมกลางแจ้งกับพ่อแม่หรือเพื่อน

อายุ 7-9 ปี

- ไม่ควรใช้ Internet เกิน 2 ชั่วโมงต่อวัน เพราะเด็กจะขาดทักษะ การคิดวิเคราะห์ ความจริงของสิ่งต่างๆ รอบตัว
- ควรใช้มือถือ หรือ Tablet เพื่อการสื่อสารที่จำเป็น เช่น การติดต่อกับ ครู ผู้ปกครอง

ด้วยความปรารถนาดีจาก
ผศ.ดร.ก.บ.ศุภลักษณ์ เข็มทอง
อาจารย์นักกิจกรรมนำบัณฑิตสังคม คณะกายภาพบำบัด
มหาวิทยาลัยมหิดล

อายุ 10-12 ปี

- เด็กมีแนวโน้มติดมือถือ เกม
- ควรแนะนำให้เด็กเห็นผลดี ผลเสียของการเล่นมือถือ หรือ Tablet มากเกินไป

อายุ 13 ขึ้นไป

- อนุญาตให้ใช้ Internet, Social Media โดยมีผู้ปกครองให้คำแนะนำอย่างเคร่งครัด
- ตั้งกติกาให้เด็กปฏิบัติ เช่น สามารถเล่นมือถือได้เมื่อทำการบ้านเสร็จแล้ว

อายุ 18 ปี

- คือช่วงอายุที่เหมาะสมในการให้อิสระในการใช้มือถือ Social Media ต่างๆ และผู้ปกครองควรฝึกให้ลูกรับผิดชอบในการชำระค่าใช้จ่ายที่เกิดขึ้น

เลี้ยงลูกด้วย “จอมือถือ” อย่างไร ให้เหมาะสม



9 วิธีที่พ่อแม่ ควรดูแลลูกในโลกออนไลน์



พ่อแม่ควรสร้างจิตสำนึกที่ดีสอนให้ลูกรู้เท่าทันภัย ดีกว่าปิดกั้น
เด็กจากสื่อออนไลน์และสื่อดิจิทัล ที่เป็นแหล่งเรียนรู้ใกล้ตัวและ
เข้าถึงได้ง่าย ทั้งยังช่วยให้พ่อแม่ลูกสร้างความสัมพันธ์ ความ
เข้าใจ และ ความใกล้ชิด มากขึ้นด้วย



1. ให้การเล่นอินเทอร์เน็ตของลูก
เป็นเวลาของครอบครัวด้วย



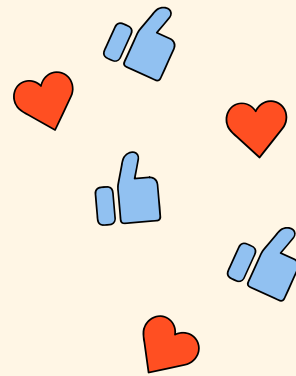
2. สร้างวินัยและกำหนด
ขอบเขตเวลาการเล่นเน็ต



3. อย่าให้ลูกอยู่ในโลกออนไลน์
จนลืมโลกแห่งความเป็นจริง



4.อย่าแชทกับคนแปลกหน้า



5.พ่อแม่ควรเรียนรู้เรื่อง
อินเทอร์เน็ตบ้าง



6.สอนลูกให้รู้จักการใช้งานด้าน
อื่นๆที่เป็นประโยชน์



7.ส่งดูพฤติกรรมการใช้งาน
ผ่านบัญชีที่พ่อแม่สร้างให้



8.สังเกตพฤติกรรมของลูก



9.หมั่นเช็คประวัติการท่องเว็บ
ของลูก

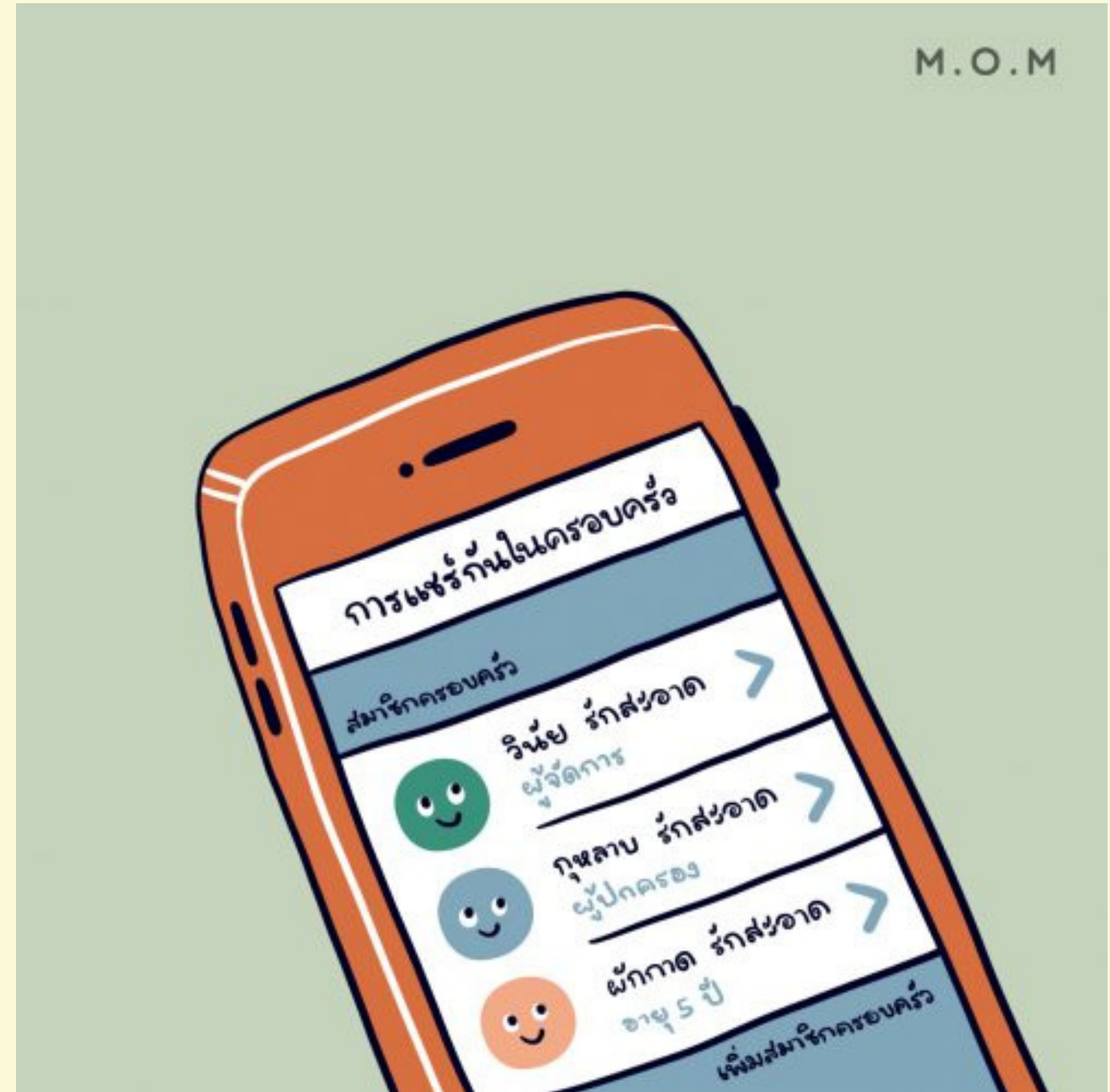
4 ทริค ให้ลูกใช้อินเทอร์เน็ต ได้อย่างปลอดภัย



1.แชร์แอดเดสกันต์ร่วมกับลูก

ระบบปฏิบัติการ ทั้ง iOS และ Android มีให้บริการ
ฟีเจอร์สำหรับแชร์แอปพลิเคชัน เกมส์ ภาพยนตร์ หรือ
หนังสือ ระหว่างสมาชิกในครอบครัว และยังสามารถควบคุม
การดาวน์โหลดแอปพลิเคชันหรือเกมที่ต้องเสียเงินซื้อ

เพราะจะต้องได้รับการอนุมัติจากหัวหน้าครอบครัวที่
กำหนดไว้ในระบบเสียก่อน



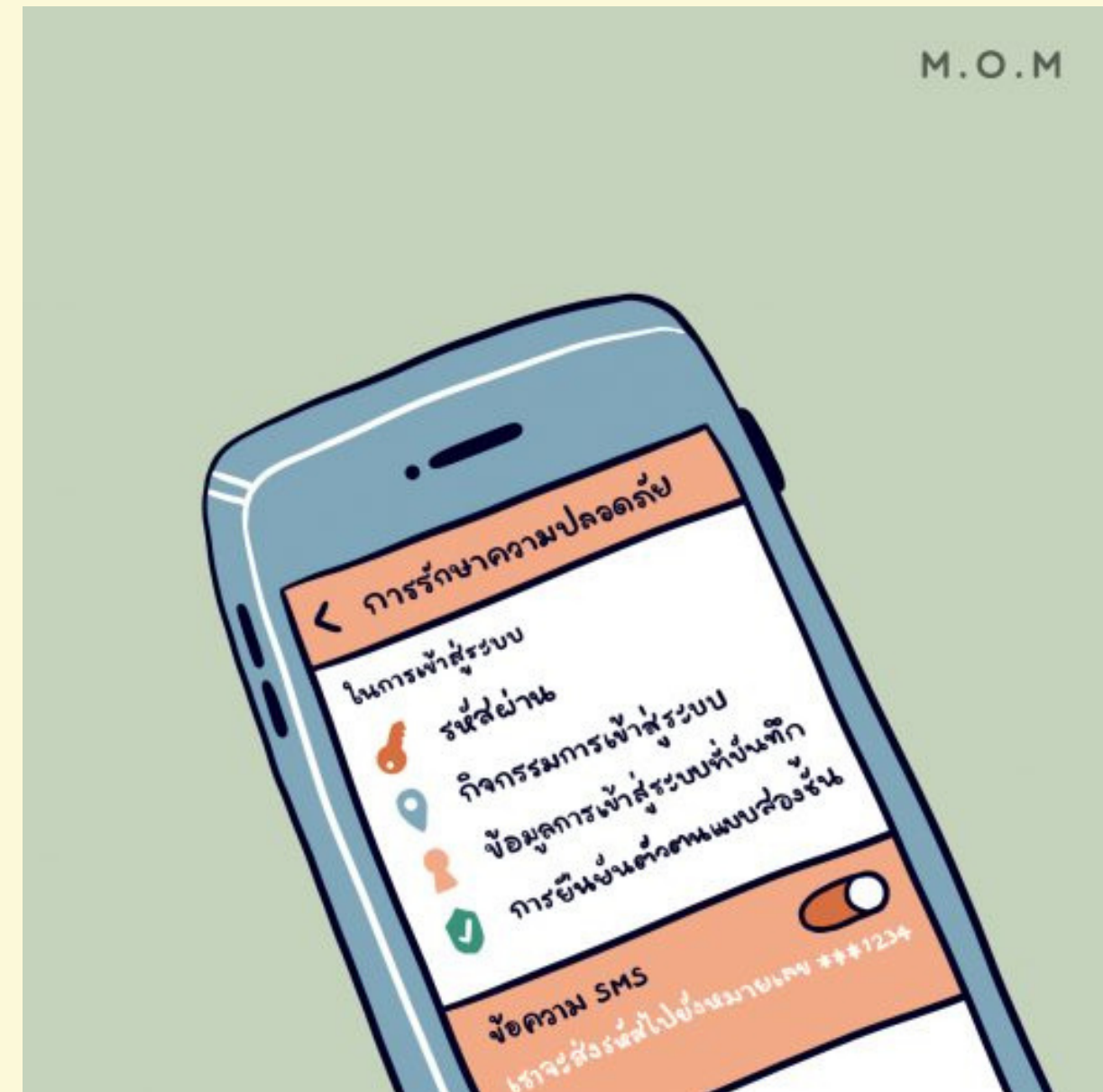
4 ทริค ให้ลูกใช้อินเทอร์เน็ต ได้อย่างปลอดภัย



2. ตั้งค่าความเป็นส่วนตัวและความปลอดภัยบนโซเชียลมีเดียของลูก

ควรตรวจสอบและตั้งค่าความเป็นส่วนตัวในแอปพลิเคชันต่างๆ ให้ลูกก่อนการใช้งาน

แอปพลิเคชันสำหรับแชตและพูดคุยต่างๆ ไม่ควรตั้งค่าเปิดเป็นเพิ่มเพื่อนอัตโนมัติเพื่อให้ลูกสามารถคัดกรองบุคคลที่จะเข้ามาอยู่ในเฟรนด์ลิสต์ก่อนทุกครั้ง

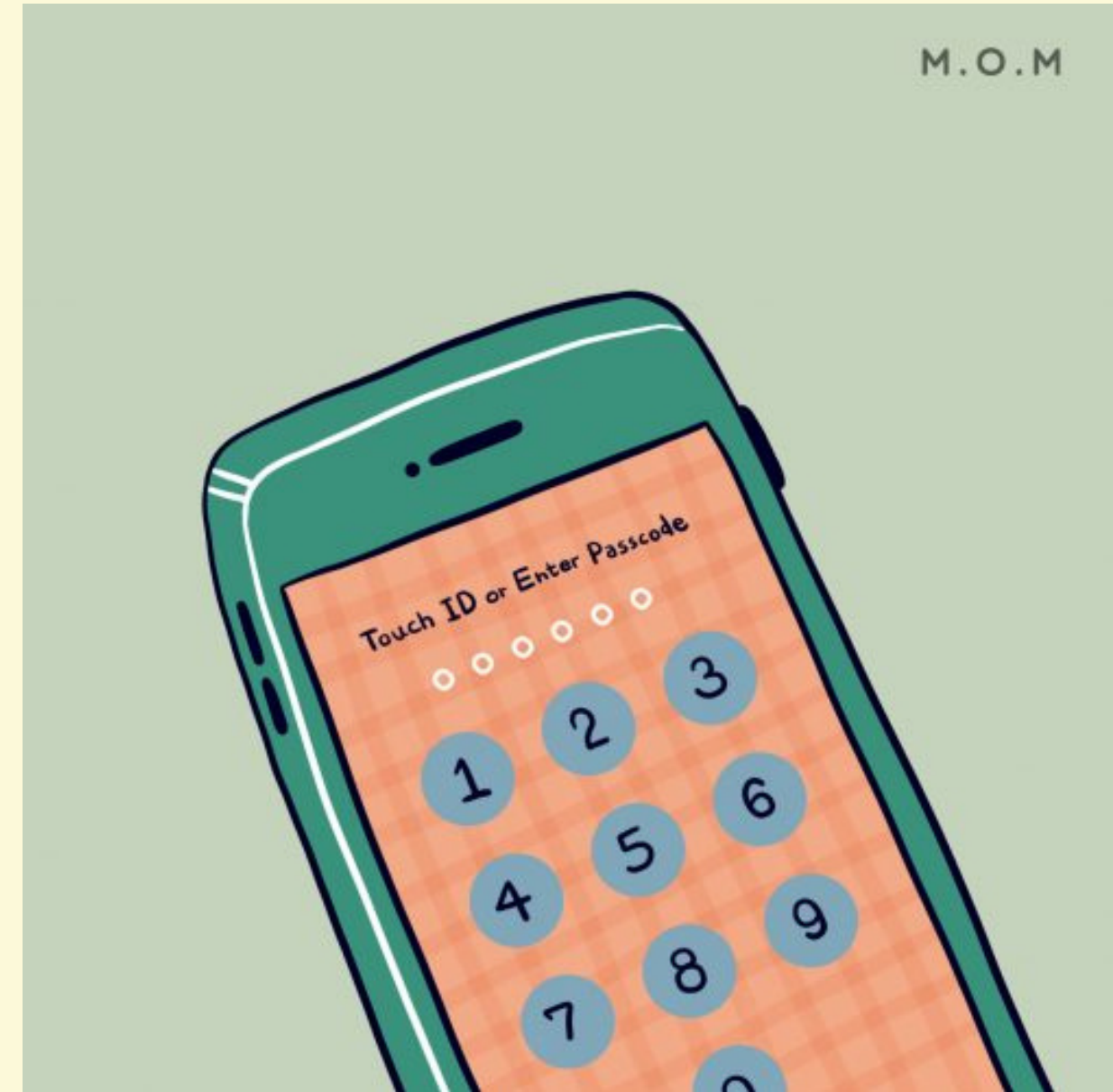


4 ทริค ให้ลูกใช้อินเทอร์เน็ต ได้อย่างปลอดภัย



3. ควรรู้รหัสปลดล็อกเครื่องหรือแอปพลิเคชันที่สำคัญ

ควรทำข้อตกลงกับลูก และอธิบายถึงความจำเป็นที่จะต้องรู้รหัสปลดล็อกเครื่องและแอปพลิเคชันที่สำคัญ เพราะหากเกิดเหตุฉุกเฉินที่จำเป็นต้องอาศัยข้อมูลในโทรศัพท์ของลูก คุณพ่อคุณแม่จะได้สามารถทำได้ทันที

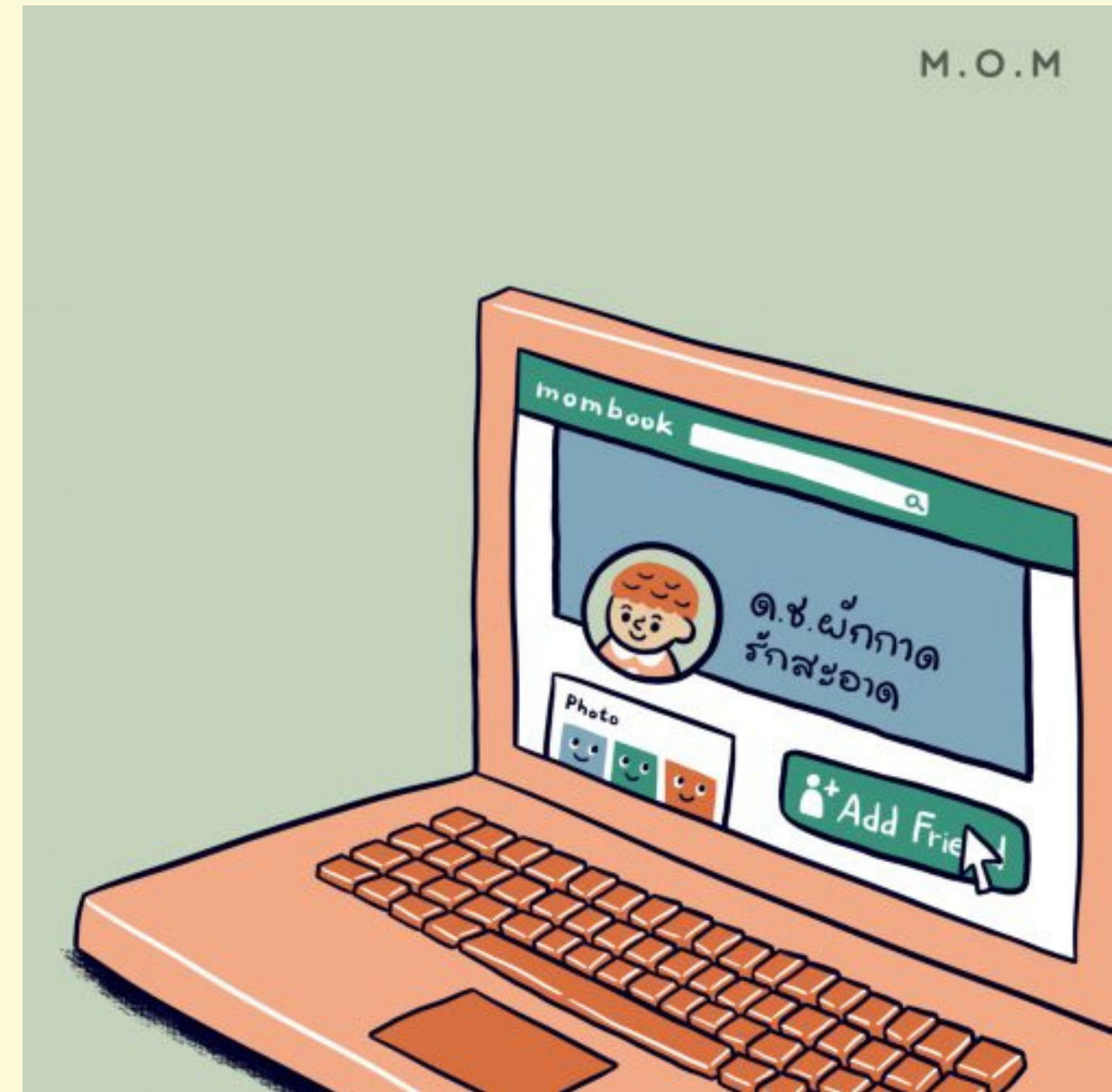


4 ทริค ให้ลูกใช้อินเทอร์เน็ต ได้อย่างปลอดภัย



4. กดติดตาม (follow) และแอดเฟรนด์ลูกในโซเชียลมีเดีย

ควรบอกหรือตกลงกับลูกว่า คุณจะทำการติดตามหรือแอดเฟรนด์เขาในช่องทางต่างๆ ไม่ใช่เพื่อเป็นการสอดส่องหรือจับผิดลูก แต่เป็นการติดตามดูความเคลื่อนไหวของลูกด้วยความเป็นห่วงและคุณพ่อคุณแม่จะไม่โพสต์หรือคอมเมนต์ในลักษณะที่จะทำให้ลูกอับอาย รวมถึงจะให้เคารพในการใช้โซเชียลมีเดียของลูกด้วย



แอปพลิเคชันและซอฟต์แวร์ ช่วยผู้ปกครองดูแลบุตรหลาน

แอปพลิเคชันที่เป็นตัวช่วยให้ผู้ปกครองสามารถดูแลบุตรหลานของคุณ ให้ห่างไกลจากเนื้อหาที่ล่อแหลมบนโลกออนไลน์ได้ โดยมี 3 แอปพลิเคชันแนะนำดังนี้



Messenger Kids

ติดต่อพูดคุยระหว่างผู้ใช้เฟซบุ๊ก แต่สร้างขึ้นสำหรับเด็กๆ โดยเฉพาะเด็กอายุต่ำกว่า 13 ปี โดยคุณพ่อคุณแม่สามารถใช้บัญชีเฟซบุ๊กของตัวเองสร้างบัญชี Messenger Kids ให้กับลูก และสามารถอนุมัติรายชื่อหรือลบรายชื่อผู้ติดต่อที่ไม่ต้องการแทนลูกได้ และตรวจสอบการสนทนาได้



YouTube Kids

ยูทูปที่คัดสรรสำหรับให้ความบันเทิงและความรู้กับเด็กโดยเฉพาะ



Google Family Link

สามารถตรวจสอบการใช้งานแอปพลิเคชันของลูกได้ เช่น ใช้แอปฯ อะไร เป็นเวลาเท่าไร หากพบความผิดปกติก็สามารถจำกัดระยะเวลาหรือล็อกอุปกรณ์ของลูกได้ รวมถึงสามารถคัดกรองคำค้นหาในเบราว์เซอร์ Google Chrome หรือการดาวน์โหลดแอปพลิเคชันที่ไม่เหมาะสมใน Play Store ได้อีกด้วย

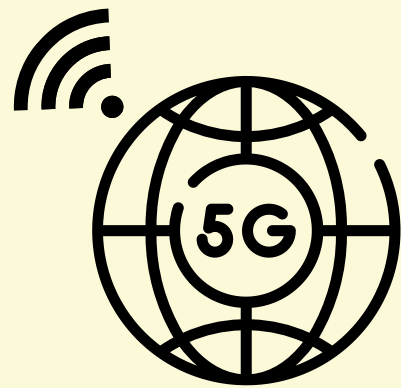
แอปพลิเคชันนี้ออกแบบมาสำหรับใช้งานกับเด็กอายุต่ำกว่า 13 ปี เมื่อลูกอายุครบ 13 ปี จะมีการแจ้งเตือนและถามว่าคุณพ่อคุณแม่จะควบคุมการใช้งานต่อไปหรือไม่

สรุปข้อควรระวังในการใช้อินเทอร์เน็ต



ออนไลน์แต่พอดีไม่มีโทษ

การออนไลน์ใช้ *Social Media* มากไปก็อาจทำให้เกิดผลเสียต่อร่างกายและเสียสมาธิ เช่น ขาดปฏิสัมพันธ์กับคนรอบข้าง ขับรถหรือข้ามถนน ก็อาจทำให้เกิดอุบัติเหตุได้ นอกจากนี้ยังเสียสุขภาพ สายตา



การใช้อินเทอร์เน็ตเพื่อทำธุรกรรม

การเลือกใช้อินเทอร์เน็ตเพื่อทำธุรกรรมต้องเลือกใช้ให้เหมาะสม เช่น กรณีที่อยู่นอกบ้านใช้ *Wifi* สาธารณะ ในการเล่นเว็บ แต่ถ้าทำธุรกรรม ควรใช้ *4G/5G*



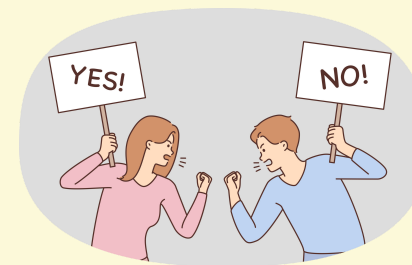
เก็บเรื่องส่วนตัวไว้ไม่ต้องบอกใคร

ไม่เปิดเผยเรื่องส่วนตัวจนมากเกินไป โดยเฉพาะชื่อ ที่อยู่ เบอร์โทรศัพท์ ตำแหน่งปัจจุบัน ถ้าจำเป็นต้องให้ข้อมูล ควรตรวจสอบว่าเป็นเว็บที่เชื่อถือได้



ระวังอันตรายจากการหลอกลวง

บนอินเทอร์เน็ตนั้นมีการหลอกลวงสารพัดรูปแบบ ไม่ว่าจะสร้างหน้าเว็บหลอก โดยอาศัยช่องโหว่ด้านพฤติกรรมของผู้คนบนอินเทอร์เน็ต



โพสต์สิ่งใดให้ทำด้วยความระมัดระวัง

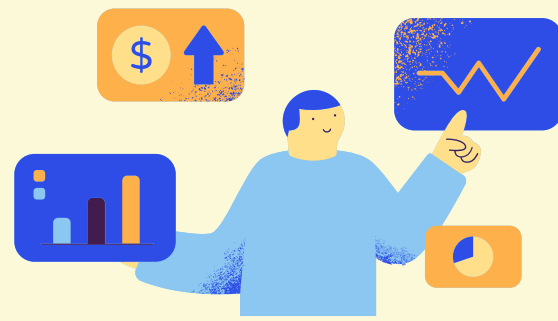
ไม่โพสต์ข้อความหรือรูปภาพไม่เหมาะสม หรือกล่าวหาผู้อื่นที่ไม่รู้จริง หรือไม่ได้อยู่ในเหตุการณ์ด้วย ระวังคำพูดคำจา ไม่ข้องแวะกับคนที่พูดจาหยาบคายหรือหาเรื่องชวนทะเลาะ



แชร์ต่ออย่างมีสติ

ไม่สร้างเรื่องเท็จเผยแพร่หรือส่งต่อข่าวลือ เรื่องเสียๆ หายๆ ที่ทำให้เกิดความเข้าใจผิด ทำให้ผู้อื่นเสียชื่อเสียง และส่งผลกระทบต่อประเทศชาติ

สรุปข้อควรระวังในการใช้อินเทอร์เน็ต



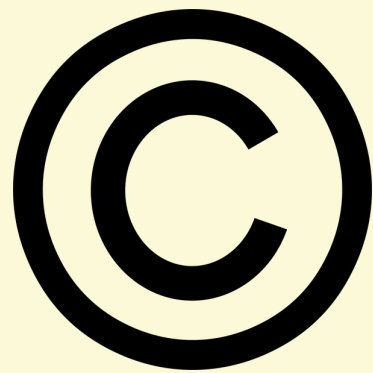
เสปสื้ออย่างมีวิจารณญาณ

อย่าหลงเชื่อข้อความหรือรูปภาพใดๆ ในอินเทอร์เน็ตโดยไม่วิเคราะห์เหตุและผลก่อน เพราะบางอย่างในเน็ตอาจไม่ใช่เรื่องจริงเสมอไป ควรใช้วิจารณญาณเป็นอย่างมากในการเสปสื้อ ไม่ว่าจะได้พบเห็นอะไรให้ฟังหูไว้หู



ระวังร้านออนไลน์ไม่ซื้อสัตย์

ซื้อปั้งออนไลน์กับร้านที่เชื่อถือได้ หากข้อมูลร้านก่อนซื้อ อ่านเงื่อนไขของร้านให้เข้าใจก่อนสั่งซื้อ ถ้าโอนเงินแล้วให้เก็บหลักฐานการโอนไว้ จนกว่าจะได้ของครบ



ระวังการละเมิดลิขสิทธิ์

ภาพและข้อความต่างๆ ในอินเทอร์เน็ตล้วนมีเจ้าของ ถ้านำไปใช้หรือแชร์ต่อก็ควรให้เครดิตเจ้าไว้ด้วย หรือต้องขออนุญาตด้วยซ้ำ