ความมั่นคงปลอดภัยในการปฏิบัติงานบนอินเตอร์เนต

กรมควบคุมมลพิษ
POLLUTION CONTROL DEPARTMENT

ตวงพร แป้นพุ่ม นักวิชาการสิ่งแวดล้อมชำนาญการ
สำนักงานสิ่งแวดล้อมและควบคุมมลพิษที่ 16 (สงขลา)

ความมั่นคงปลอดภัยทางอินเตอร์เนต และไซเบอร์

“การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ”

การใช้งาน Social Media อาทิ การ Share/ Like/ Follow ทำให้การกระจายตัวของข้อมูลเป็นไปอย่างรวดเร็ว ยากต่อการควบคุม

การเปลี่ยนแปลงพฤติกรรมจากสถานการณ์การระบาดของ Covid-19ทำ ให้เกิดการปลี่ยนแปลงในโลกออนไลน์มากขึ้น เช่น การทำธุรกรรมทางการเงินผ่านแอปพลิเคชั่น *การทำงานการส่งภาพ ข้อความ เสียง วิดีโอต่างๆ ผ่าน Smart phone และการประชุมออนไลน์*

ประเทศไทยมีการใช้งานอินเตอร์เนตค่อนข้างสูงอย่างต่อเนื่อง และประชากรใช้ Social Media เพิ่มมากขึ้นด้วย อุปกรณ์ที่ใช้งานอินเตอร์เนตส่วนใหญ่เป็นโทรศัพท์มือถือ แทปเล็ตมากกว่าการใช้งานผ่านเครื่องคอมพิวเตอร์ จึงมีความเสี่ยงต่อภัยคุกคามเข้าถึงได้ทุกที่ทุกเวลา

ภัยคุกคามทางอินเตอร์เนต

เป็นการกระทำหรือการดำเนินการใด ๆ ผ่านการใช้อินเตอร์เนตที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่ายและ / หรือข้อมูลภายใน

รูปแบบภัยคุกคาม

Cracker : จะเป็นบุคคลที่จะพยายามเจาะระบบรักษาความปลอดภัยเพื่อวัตถุประสงค์ไม่ดีต่าง ๆ เช่น การแพร่กระจาย virus , spyware , adware หรืออื่นๆ

Script kiddy : เจาะโปรแกรม อยากรู้อยากเห็น

spy: การแฝงตัวเป็นขโมยข้อมูล

Employee : เป็นการทำให้เกิดปัญหา เช่น Flash drive ติดไวรัสมาใช้ในองค์กร

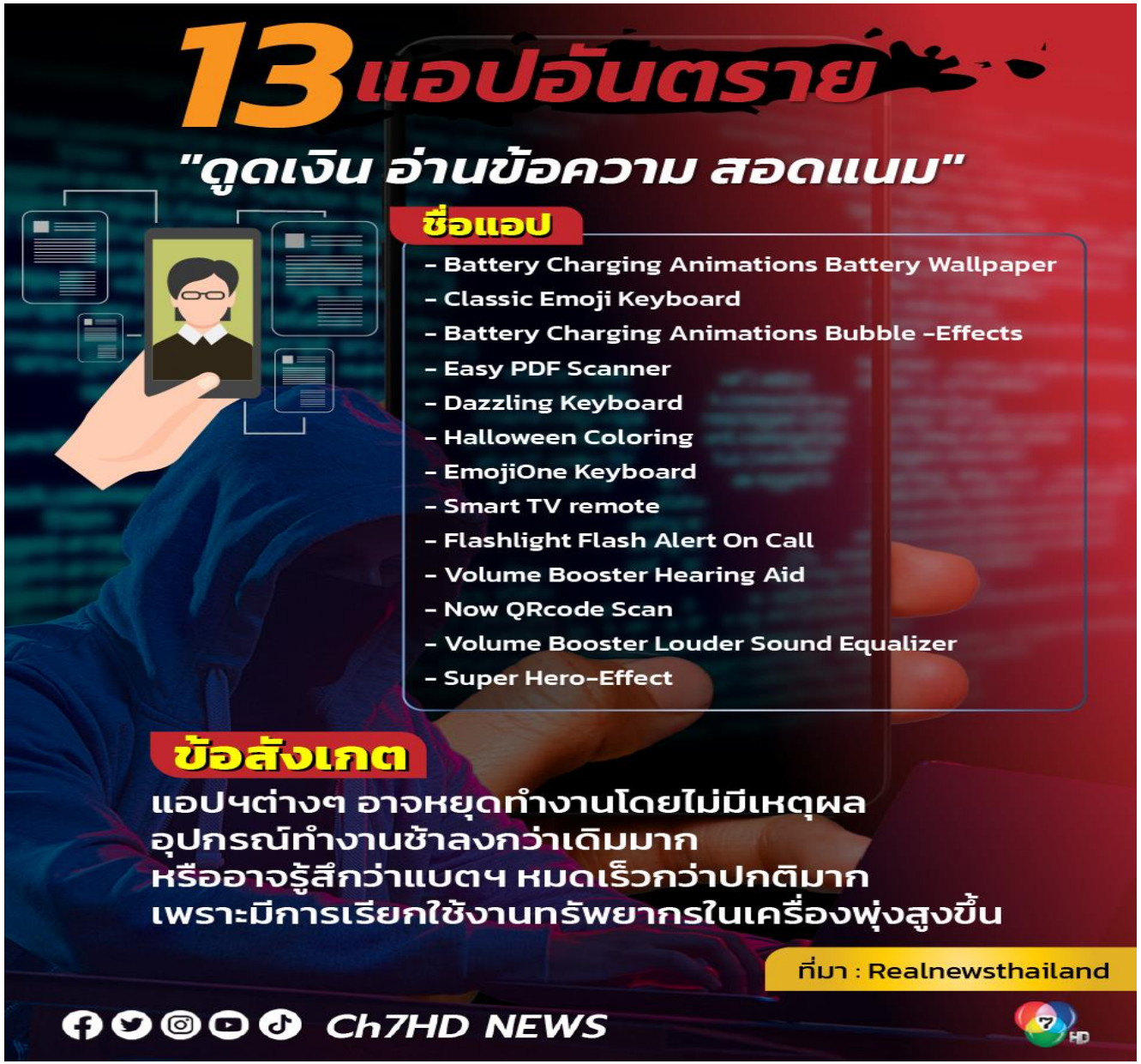
Social Engineering : จิตวิทยาหลอกลวง โดยไม่ได้มีความรู้อินเทอร์เน็ตมากมาย เช่น หลอกว่าถูกรางวัลหรือได้รับสิทธิพิเศษต่างๆ

Password Guessing : เดารหัสผ่าน

Dos : รบกวนของระบบ ทำให้ระบบมีความสามารใช้งานได้

ที่มา : หลักสูตรความมั่นคงปลอดภัยบนอินเตอร์เนตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล สำนักงาน กพ.


ระวังมิจฉาชีพ!!
ออกอุบายหลอกแจก
อั่งเปาออนไลน์
และระมัดระวังการเกิดอัคคีภัย
มิจฉาชีพอาจชักจูงให้เหยื่อหลงเชื่อ
ว่ามีการ "แจกอั่งเปาฟรี!!"
แล้วส่งลิงก์ให้กรอกข้อมูลส่วนบุคคลต่างๆ
ผ่านทางข้อความ SMS , LINE , FACEBOOK , ฯลฯ
หรือให้ติดตั้งแอปพลิเคชันที่สามารถควบคุมมือถือ
ระยะไกล หรือแอปรีโมท แล้วทำการดูดเงินในบัญชี
ห้ามกดลิงก์หรือกดติดตั้ง
โดยเด็ดขาด!!
อย่า!!
หลงเชื่อ
ระมัดระวังการเกิดเพลิงไหม้
การประกอบพิธีเซ่นไหว้บรรพบุรุษในเทศกาลตรุษจีน
ถือเป็นอีกช่วงหนึ่งที่มีสถิติการเกิดอุบัติภัยสูงกว่าปกติ
ทั้งเพลิงไหม้ อุบัติภัยจากประทัดจีนของเด็กและประชาชน
ระมัดระวังการจุดธูปเทียนบูชา การเผากระดาษเซ่นไหว้
รวมถึงการจุดประทัดต่างๆเพื่อป้องกันการเกิดอัคคีภัย
สอบถาม/แจ้งเบาะแส
สายด่วน
สอท.
1441
081-866-3000


13 แอปอันตราย
"ดูดเงิน อ่านข้อความ สอดแนม"
ชื่อแอป
- Battery Charging Animations Battery Wallpaper
- Classic Emoji Keyboard
- Battery Charging Animations Bubble -Effects
- Easy PDF Scanner
- Dazzling Keyboard
- Halloween Coloring
- EmojiOne Keyboard
- Smart TV remote
- Flashlight Flash Alert On Call
- Volume Booster Hearing Aid
- Now QRcode Scan
- Volume Booster Louder Sound Equalizer
- Super Hero-Effect
ข้อสังเกต
แอปฯต่างๆ อาจหยุดทำงานโดยไม่มีเหตุผล
อุปกรณ์ทำงานช้าลงกว่าเดิมมาก
หรืออาจรู้สึกว่าแบตฯ หมดเร็วกว่าปกติมาก
เพราะมีการเรียกใช้งานทรัพยากรในเครื่องพุ่งสูงขึ้น
ที่มา : Realnewsthailand
Ch7HD NEWS


ที่มาของปัญหา
1 ช่วงโควิด-19 ที่ทำให้เราเปลี่ยนมาโกออนไลน์ รวมถึงเรื่องการเงิน จึงพบความเสี่ยงต่าง ๆ เพิ่มขึ้น ล่าสุดคือ “การถูกตัดเงินจากบัญชีธนาคารโดยไม่รู้ตัว”
2 Case ที่เงินหายจากบัญชีมีหลายรูปแบบ เช่น จาก App ซื้อของออนไลน์ จากโฆษณาในเฟซบุ๊ก จากเครื่องรับบัตรหรือเครื่องรูดบัตร EDC (Electronic Data Capture)
3 จากการตรวจสอบของธนาคารแห่งประเทศไทย และสมาคมธนาคารไทย พบว่าเป็นการทำธุรกรรมชำระค่าสินค้าและบริการกับร้านค้าออนไลน์ที่จดทะเบียนในต่างประเทศ ไม่ใช่ “App ดูดเงิน”
1212 OCC

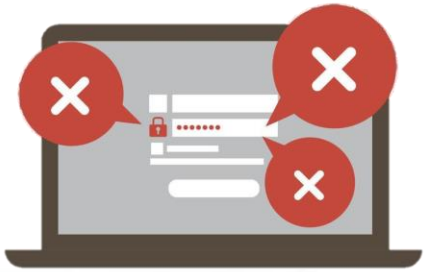

ไทยคู่ฟ้า
เตือนภัย ปชช.
อย่าคลิกลิงก์ SMS
หลอกรับเงินเยียวยาฯ
ระวังถูกขโมยข้อมูล - ดูดเงินหมดบัญชี
พบเบาะแสแจ้งสายด่วน สตช. 1599
หรือ กสทช. Call Center 1200
9:41
คุณได้รับเงินเยียวยา COVID-19
คลิ้ก:https://bit.ly/5RfswsN
ข้อมูล ณ วันที่ 19 ก.ย. 65
ไทยคู่ฟ้า
THAIGOV.GO.TH

ที่มา :Facebook กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

คำแนะนำในการใช้งานรหัสผ่าน

- ไม่กำหนดรหัสผ่านจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว
- ควรกำหนดรหัสผ่านให้ยากต่อการคาดเดา และควรกำหนดรหัสผ่านด้วยตัวอักษรไม่ต่ำกว่า 6 ตัวอักษร และควรประกอบกอบด้วย ตัวเลข ตัวอักษร และตัวอักษรพิเศษ (@ # %)
- ไม่ให้รหัสผ่านส่วนบุคคลแก่ผู้อื่น
- ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหสผ่านอัตโนมัติ
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

รหัสผ่านที่พบบ่อยและคาดได้ง่าย



Top 30 Most Used Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

ที่มา https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/

การรักษาความปลอดภัยให้กับมือถือและอุปกรณ์ IoT

Lock หน้าจอ

ตั้งค่า Lock หน้าจอเครื่อง เพื่อป้องกันบุคคลอื่นแอบใช้งาน

ไม่ Root/ Jailbreak เครื่อง

ซึ่งจะทำให้เครื่องหมดประกันแล้วยังทำให้อาจโดนฝังคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ไฟล์สำคัญในเครื่องได้

ไม่ลงโปรแกรมที่ไม่ได้มาจาก Google Play Store หรือ Apple AppStore

Google และ Apple มีขั้นตอนในการตรวจสอบโปรแกรมก่อนอนุญาตให้เผยแพร่ใน Store จึงมั่นใจได้ระดับหนึ่งว่าโปรแกรมมีความน่าเชื่อถือและปลอดภัย

ตรวจสอบ App ที่จะใช้งาน

การติดตั้ง Application ที่ดี คือ การอ่าน Review ของผู้ใช้งานอื่นและดูจำนวนยอดผู้ติดตั้ง

ปรับปรุง Software ให้ทันสมัย

การ Update Software จะเป็นการปิดช่องโหว่ของ Software ตัวเดิมอีกด้วย

ที่มา IT Security Awareness Training โดย ชาญยุทธ ลือสิริพาณิชย์

การรักษาความปลอดภัยให้กับอุปกรณ์ Wifi

- เปลี่ยนรหัสโรงงานเป็นรหัสใหม่
  หลังทำการตั้งค่าเสร็จแล้วให้ทำการตั้งค่ารหัสผ่านใหม่ทันที

- ปรับปรุง Software ให้ทันสมัย
  การ Update Software จะเป็นการปิดช่องโหว่ของ Software ตัวเดิมอีกด้วย

- ไม่เปิดฟังก์ชั่น WPS
  WPS เป็นฟังก์ชั่นที่ทำให้การเชื่อมต่อระหว่างอุปกรณ์อื่นๆกับ Wifi ทำได้ง่าย และก็ง่ายต่อการโจรกรรมข้อมูลเช่นกัน

- การตั้งชื่อ Wifi ส่วนบุคคล
  ควรเป็นชื่อที่ไม่สื่อให้ทราบอย่างชัดเจนว่าเป็น Wifi ผู้ใด และควรซ่อน Wifi เพื่อความปลอดภัยต่อเข้าถึงจากผู้ที่ไม่พึงประสงค์

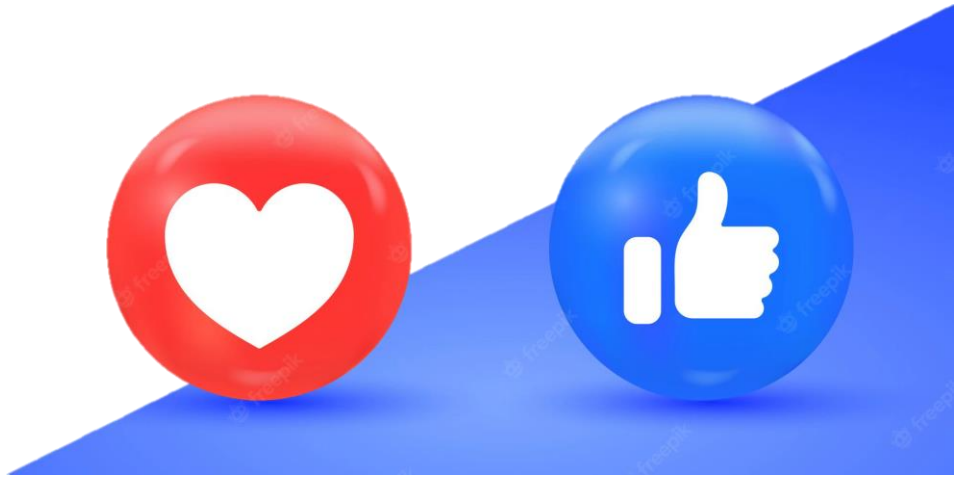
ที่มา IT Security Awareness Training โดย ชาญยุทธ ลือสิริพาณิชย์


Welcome to Facebook
https://www.facebook.com
TNN ONLINE
facebook
ไม่อยากถูกแฮกต้องอ่าน!


facebook
Facebook helps
the people in yo


facebook
แชร์ข้อมูลส่วนตัวมากไปใช่จะดี
ใคร ๆ ก็มองว่า Facebook คือ พื้นที่ส่วนตัว จึงกล้าแชร์ กล้าโพสต์เรื่องเกี่ยวกับตัวเองหลายอย่าง
อาจหลงลืมไปว่า ที่จริงแล้ว มันไม่ได้ปลอดภัยอย่างที่เราคิด ควรเปิดเผยแต่พอเหมาะดีกว่า
ข้อมูลส่วนตัว
ที่มักจะโดนสวมรอยได้ง่าย
เพจสาธารณะ
เพจส่วนตัว
ใส่ชื่อที่เป็นทางการ
อีเมล์หลัก
ที่อยู่สำนักงาน
เบอร์โทรศัพท์
ชื่อบริษัท หรือธุรกิจ
อธิบายเกี่ยวกับองค์กร
FULL NAME
E-MAIL
ADDRESS
PHONE NUMBER
COMPANY NAME
JOB TITLE
ชื่อ-นามสกุลจริง
อีเมล์
แชร์บางโอกาสดีกว่า
ไม่ควรระบุลงไป
บริษัทปัจจุบันที่ทำงาน
ตำแหน่งงานปัจจุบัน
อาการที่ Facebook ฟ้องว่า...มีคนกำลังสวมรอยคุณ
แจ้งเตือนข้อความว่า
"มีคนกล่าวถึงคุณในความ
คิดเห็น" ที่คุณไม่ได้โพสต์เอง
ได้รับ SMS แจ้ง
การล็อกอินที่ไม่ใช่คุณ
facebook
เปิดหน้า Facebook แล้ว
ให้กลับมาใส่รหัสผ่าน
อีกครั้ง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมทางหลวงชนบท
ThaiCERT
ETDA
ขอขอบคุณข้อมูลดีๆจาก
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
MINISTRY OF DIGITAL ECONOMY AND SOCIETY

facebook




4 ข้อ ป้องกันโดนแฮก
เฟสบุ๊ค
1
AW01fgy2001
Egd89po001
เปลี่ยนรหัสผ่านอยู่เสมอ
และควรตั้งรหัสให้ยากต่อการคาดเดา
2
ใช้งานการยืนยันตัวตน
แบบสองชั้น
3
ตั้งค่าความปลอดภัยอีเมล
และใช้งานผ่านอุปกรณ์
ที่เชื่อถือได้เท่านั้น
4
เปิดระบบรับการแจ้งเตือน
ในกรณีที่อาจมีการเชื่อมต่อ
จากเครื่องมืออื่น ๆ
SME Development Bank
ยื่นขอสินเชื่อออนไลน์ผ่าน SME D Bank
www.smebank.co.th

การตั้งค่าความปลอดภัยของ Line

พฤติกรรมเสี่ยงใช้งาน Line ที่ง่ายต่อการสวมรอยบัญชี

การโดนสวมรอยบัญชี LINE ไม่ใช่เรื่องไกลตัวอีกต่อไป หากคุณมีพฤติกรรมการใช้งานส่วนใหญ่เข้าข่ายกรณีเหล่านี้

- อีเมล์ที่ใช้ลงทะเบียน ไม่ใช่อีเมล์ที่ล็อกอินทุกวัน
- ใช้รหัสผ่านที่คาดเดาง่าย
- เพิ่มคนที่ไม่รู้จักมาไว้ในรายชื่อ
- เชื่อมต่อกับ Facebook ด้วยอีเมล์และรหัสผ่านชุดเดียวกัน
- อนุญาตให้ล็อกอินหลายๆ อุปกรณ์ได้
- ละเลยการอัปเดตซอฟต์แวร์

ที่มา : หลักสูตรความมั่นคงปลอดภัยบนอินเตอร์เนตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล สำนักงาน กพ.

สัญญาณเตือนว่า กำลังมีใครใช้งานบัญชีคุณอยู่

- พบข้อความแจ้งเตือนว่ามีคนอื่นล็อกอิน
- ล็อกอินไม่ได้ แจ้งว่ารหัสผ่านผิด
- ใช้งานอยู่ แล้วบัญชีเด้งกลับไปหน้าล็อกอิน
- เจอข้อความที่เราไม่ได้พิมพ์

ที่มา : หลักสูตรความมั่นคงปลอดภัยบนอินเตอร์เนตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล สำนักงาน กพ.

LINE

วิธีป้องกัน การถูกขโมยบัญชี LINE

ทรูปลูกปัญญา

- ไม่ให้ผู้อื่นรู้ข้อมูลบัญชี และรหัสผ่าน
- ทีมงาน LINE จะไม่ขอ รหัสผ่านจากคุณในทุกกรณี
- อย่าคลิกและหลงเชื่อ เว็บไซต์แปลกปลอม
- โปรดระวังบัญชีทางการปลอม (LINE Official Account)
- ลงชื่อออกทุกครั้ง เมื่อใช้งานผ่านอุปกรณ์อื่น

วิธีรับมือโทรศัพท์หายชีวิต ไม่วุ่นวายเพราะข้อมูลไม่รั่วไหล

ANDROID ป้องกันก่อนมือถือหาย

1) ไปที่ Setting
2) เข้า Security
3) เข้า Device Administrators
4) กดติ๊กถูกที่ Find My Device
5) กด Activate

ANDROID จัดการหากมือถือหาย

1) เข้าเว็บไซต์ Android Device Manager
2) ล็อกอินด้วย E-mail ของ Google (Gmail) ที่ลงทะเบียนในเครื่อง
3) กดเลือกอุปกรณ์ที่ต้องการหา
4) คุณสามารถรู้ได้ว่า ตอนนี้มือถือคุณอยู่ที่ไหน โดยดูจากแผนที่ที่ปรากฏ
5) จากนั้นเลือกคำสั่ง “ควบคุมระยะไกล” ให้มือถือล็อกและล้างข้อมูล

ที่มา : หลักสูตรความมั่นคงปลอดภัยบนอินเตอร์เนตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล สำนักงาน กพ.

iOS

BEFORE

iOS ป้องกันก่อนมือถือหาย

1) เข้าไปที่ Setting

2) เข้า iCloudและล็อกอินด้วย Apple ID

3) เข้า Find My iPhone แล้วกดเปิดการใช้งาน

4) หน้าจอเปิดการใช้งาน iCloud

AFTER

iOS จัดการหากมือถือหาย

1) เข้าเว็บ iCloud ล็อกอินด้วยบัญชีเดียวกับอุปกรณ์ที่ต้องการตามหา

2) คลิก “ค้นหา iPhone ของฉัน”

3) ระบบกำลังค้นหาตำแหน่งมือถือ

4) เลือกอุปกรณ์ที่ต้องการค้นหา

5) จากนั้นเลือกคำสั่ง “ควบคุมระยะไกล” ให้มือถือล็อกและล้างข้อมูล

ที่มา : หลักสูตรความมั่นคงปลอดภัยบนอินเตอร์เนตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล สำนักงาน กพ.

THANK YOU