



Australian Government



ลงมือทำตอนนี้
ให้ตนเองปลอดภัยเสมอ

คู่มือความปลอดภัยบนโลก ออนไลน์

ฉบับอ่านง่าย



วิธีใช้งานคู่มือนี้



เราคือรัฐบาลออสเตรเลีย

เราเป็นผู้จัดทำคู่มือนี้



เราเขียนคำบางคำเป็น**ตัวหนา**

เพื่ออธิบายความหมายของคำเหล่านั้น

นอกจากนี้ยังมีรายการคำเหล่านี้อยู่ในหน้า 28 ด้วย



ท่านสามารถขอให้คนที่ท่านไว้วางใจช่วยในการ:

- อ่านคู่มือนี้
- ค้นหาข้อมูลเพิ่มเติม



คู่มือนี้เป็นคู่มือฉบับสรุปอ่านง่ายของคู่มืออีกฉบับหนึ่ง

ซึ่งรวบรวมเฉพาะแนวคิดที่สำคัญที่สุดเท่านั้น



ท่านสามารถดูคู่มืออีกฉบับหนึ่งได้ที่เว็บไซต์ของเรา

www.actnowstaysecure.gov.au

คู่มือนี้มีอะไรบ้าง

คู่มือนี้มีอะไรบ้าง	3
เกี่ยวกับคู่มือนี้	4
เก็บรักษาบัญชีของท่านให้ปลอดภัย	6
ตรวจสอบการตั้งค่าของท่านเพื่อปกป้องข้อมูลของท่าน	10
ปกป้องอุปกรณ์ต่าง ๆ ของท่าน	16
การหลอกลวง	20
แสดงความคิดเห็น	25
รายการคำศัพท์	28
ติดต่อเรา	30

เกี่ยวกับคู่มือนี้



เราทุกคนจำเป็นต้องคิดถึงวิธีการรักษาความปลอดภัยบนโลกออนไลน์

ซึ่งเราเรียกว่าความปลอดภัยทาง**ไซเบอร์**



คำว่า**ไซเบอร์** หมายถึงสิ่งที่เกี่ยวข้องกับอินเทอร์เน็ต



คู่มือนี้จะอธิบายถึงสิ่งที่ท่านสามารถทำได้ เพื่อปกป้องตนเองบนโลกออนไลน์

ตัวอย่างเช่น จาก**อาชญากรรมทางไซเบอร์**



อาชญากรรมทางไซเบอร์ คือการที่อาชญากรใช้อินเทอร์เน็ตในการก่ออาชญากรรม

ตัวอย่างเช่น พวกเขาอาจใช้อินเทอร์เน็ตเพื่อ:

- ขโมยข้อมูลส่วนบุคคลของท่าน
- เข้าควบคุมบัญชีหรือโปรไฟล์ออนไลน์ของท่าน

อาชญากรรมทางไซเบอร์สามารถเกิดขึ้นบนอุปกรณ์ใดก็ได้



ซึ่งรวมถึง:

- คอมพิวเตอร์
- สมาร์ทโฟน
- สมาร์ทวอตช์



มีหลายสิ่งที่คุณสามารถทำได้ เพื่อป้องกันตนเองจาก
อาชญากรรมทางไซเบอร์



เราจะอธิบายสิ่งที่คุณสามารถทำได้ในหน้าถัดไป

เก็บรักษาบัญชีของท่านให้ปลอดภัย



ท่านควรคิดหาวิธีเก็บรักษาบัญชีออนไลน์ของท่านให้ปลอดภัย

ใช้ลึรหัสผ่านที่แข็งแกร่งและไม่ซ้ำกัน



วลีรหัสผ่าน (Passphrase) เป็นรหัสผ่านประเภทที่มีความแข็งแกร่งมากขึ้น

ซึ่งเป็นวลีรหัสผ่านที่คนอื่นจะเดาได้ยาก



การใช้วลีรหัสผ่านที่แข็งแกร่งและแตกต่างกันเป็นหนึ่งในวิธีที่ดีที่สุดในการปกป้องบัญชีของท่าน



ท่านควรใช้วลีรหัสผ่านที่แตกต่างกันสำหรับบัญชีออนไลน์แต่ละบัญชีของท่าน



วิธีการผ่านที่แข็งแกร่งควรมีลักษณะดังนี้:

- คำสุ่ม 4 คำขึ้นไป
- ตัวอักษรและตัวเลข 15 ตัวขึ้นไป



บางตัวอักษร ท่านสามารถใช้ตัวพิมพ์ใหญ่ได้



ท่านยังสามารถใช้สัญลักษณ์ต่าง ๆ ได้ เช่น:

- เครื่องหมายขีดกลาง (dash)
- เครื่องหมายดอลลาร์ (\$)
- เครื่องหมายอีเมล (@)



ท่านไม่ควรใช้ข้อมูลส่วนบุคคลใด ๆ ในวิธีการผ่านของท่าน



ตัวอย่างเช่น:

- วันเกิดของท่าน
- ชื่อของสมาชิกในครอบครัวหรือสัตว์เลี้ยงของท่าน

เพิ่มขั้นตอนต่าง ๆ ในการเข้าสู่ระบบบัญชีของท่าน



ท่านสามารถปกป้องบัญชีออนไลน์ของท่านด้วย **การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication – MFA)**

MFA คือการใช้วิธีการตั้งแต่ 2 วิธีขึ้นไปในการเข้าสู่ระบบบัญชีของท่านทุกครั้ง



ตัวอย่างเช่น ท่านอาจต้องป้อนวลีรหัสผ่านก่อน

จากนั้นจึงป้อนรหัสที่ท่านได้รับทางโทรศัพท์

ท่านอาจใช้ตัวเลือกดังต่อไปนี้:



- ใช้แอปบนโทรศัพท์ของท่านเพื่อรับรหัส



- รับรหัสทางอีเมล



- รับรหัสเป็นข้อความทางโทรศัพท์



การยืนยันตัวตนแบบหลายปัจจัย (MFA) ทำให้คนอื่นเข้าถึงบัญชีออนไลน์ของท่านได้ยากขึ้น

แม้ว่าพวกเขาจะทราบวิธีการรับรหัสผ่านของท่านก็ตาม

ตรวจสอบการตั้งค่าของท่านเพื่อปกป้องข้อมูลของท่าน



ท่านสามารถตรวจสอบได้ว่า การตั้งค่าของท่านจะปกป้องข้อมูลของท่านบนโลกออนไลน์ได้หรือไม่



ซึ่งรวมถึงการตั้งค่าของท่านใน:

- บัญชีออนไลน์ต่าง ๆ
- อุปกรณ์ต่าง ๆ
- แอปต่าง ๆ



ท่านสามารถ:

- เปลี่ยนการตั้งค่าของท่านได้
- เลือกว่าแอปใดที่สามารถใช้ข้อมูลของท่านได้

ท่านสามารถดูการตั้งค่าบนอุปกรณ์ของท่านได้โดย:



- มองหาไอคอนรูปเฟือง
- หรือ
- พิมพ์ 'การตั้งค่า' ลงในแถบค้นหาของอุปกรณ์ของท่าน



ท่านอาจดูการตั้งค่าในแอปหรือบัญชีออนไลน์ได้โดยการไปที่เมนู

เมนูมักจะมีสัญลักษณ์เป็นเส้นตรง 3 เส้น



การตั้งค่าบางอย่างเหล่านี้สามารถแชร์ข้อมูลว่า:

- ท่านเป็นใคร
- ท่านอยู่ที่ใด
- ท่านอาศัยอยู่ที่ใด



การแชร์ข้อมูลนี้บนโลกออนไลน์อาจทำให้ท่านมีความเสี่ยง
ต่ออาชญากรรมทางไซเบอร์



อาชญากรรมทางไซเบอร์สามารถใช้ข้อมูลของท่านเพื่อแอบอ้าง
เป็นตัวท่านได้

ตัวอย่างของข้อมูลที่พวกเขาอาจใช้ เช่น:



- ที่อยู่ของท่าน



- ชื่อสมาชิกในครอบครัวของท่าน



- ชื่อสัตว์เลี้ยงของท่าน



ท่านสามารถตั้งค่าบัญชีของท่าน เพื่อให้เพียงเฉพาะคนที่ท่านรู้จักเท่านั้นที่สามารถเห็นโปรไฟล์บนโซเชียลมีเดียของท่านได้

ตัวอย่างเช่น โปรไฟล์ Facebook ของท่าน



การตั้งค่าเหล่านี้มักเรียกว่าการตั้งค่าความเป็นส่วนตัว



ท่านยังสามารถควบคุมการตั้งค่าตำแหน่งของท่านได้
การตั้งค่าตำแหน่งจะแสดงตำแหน่งของอุปกรณ์ของท่าน



ท่านสามารถเปิดหรือปิดการตั้งค่าตำแหน่งได้
ท่านยังสามารถเลือกได้ว่าแอปใดบ้างที่สามารถใช้การตั้งค่า
ตำแหน่งของท่านได้



ท่านสามารถทำได้สำหรับ:

- บัญชีออนไลน์ต่าง ๆ ของท่าน
- อุปกรณ์ต่าง ๆ ของท่าน
- แอปต่าง ๆ ของท่าน

บางแอปอาจถามท่านว่าสามารถ:



- ใช้กล้องของท่านได้หรือไม่



- ดูรูปถ่ายของท่านได้หรือไม่



ท่านควรอนุญาตเฉพาะแอปที่ท่านคุ้นเคยเท่านั้นในการให้ใช้
กล้องและรูปถ่ายของท่าน

ปกป้องอุปกรณ์ต่าง ๆ ของท่าน



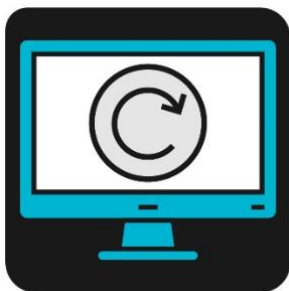
ท่านควรคิดถึงวิธีปกป้องอุปกรณ์ต่าง ๆ ของท่าน เพื่อช่วยให้ท่านปลอดภัยบนโลกออนไลน์

ตัวอย่างเช่น โทรศัพท์หรือสมาร์ทวอตช์ของท่าน



การที่อุปกรณ์ต่าง ๆ เชื่อมต่อกับอินเทอร์เน็ตนั้นเป็นเรื่องสำคัญ

อัปเดตอุปกรณ์ต่าง ๆ ของท่าน



ท่านสามารถอัปเดตอุปกรณ์ต่าง ๆ ของท่าน เพื่อความปลอดภัยบนโลกออนไลน์ได้

ตัวอย่างเช่น โทรศัพท์และแล็ปท็อปของท่าน



อุปกรณ์ของท่านอาจเรียกขั้นตอนนี้ว่าการอัปเดตซอฟต์แวร์



การอัปเดตช่วยให้อุปกรณ์ปกป้องตัวเองจากอาชญากรรมทางไซเบอร์ได้



ท่านสามารถตั้งค่าอุปกรณ์ให้ทำการอัปเดตโดยอัตโนมัติได้



ท่านสามารถเรียนรู้เพิ่มเติมเกี่ยวกับวิธีการอัปเดตอุปกรณ์ต่าง ๆ ของท่านได้ที่เว็บไซต์ของเรา

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

เครือข่าย Wi-Fi สาธารณะ



ท่านควรระมัดระวังเมื่อใช้ **Wi-Fi สาธารณะ**



Wi-Fi สาธารณะคืออินเทอร์เน็ตไร้สายฟรีที่ท่านสามารถใช้ได้ในที่สาธารณะ



ตัวอย่างเช่น ที่:

- ร้านกาแฟ
- สนามบิน
- โรงแรม



ท่านควรระมัดระวังการป้อนข้อมูลลงในเว็บไซต์เมื่อใช้ Wi-Fi สาธารณะ



ตัวอย่างเช่น:

- รายละเอียดบัญชีธนาคาร
- บัญชีอีเมล
- โปรไฟล์โซเชียลมีเดีย



อาชญากรทางไซเบอร์บางรายสามารถใช้ Wi-Fi สาธารณะ เพื่อ:

- ดูว่าท่านกำลังทำอะไรอยู่บนอินเทอร์เน็ต
- ขโมยข้อมูลของท่าน

เนื่องจาก:



- ใคร ๆ ก็สามารถใช้ Wi-Fi ได้



- การปกป้องอุปกรณ์ของท่านทำได้ยากขึ้น



ท่านสามารถเรียนรู้วิธีการรักษาความปลอดภัยเมื่อใช้ Wi-Fi
สาธารณะได้ที่เว็บไซต์ของเรา

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

การหลอกลวง



เราเรียกว่าการหลอกลวง เมื่อมีคนพยายามที่จะ:

- หลอกลวงท่าน
- เอาเงินของท่าน



มิจฉาชีพคือคนที่กระทำการหลอกลวง

มิจฉาชีพอาจพยายามหลอกลวงท่านผ่านทาง:



- ข้อความหรือโทรศัพท์
- อีเมล
- โซเชียลมีเดีย
- เว็บไซต์



พวกเขาอาจดูเป็นมิตร

แต่อาจหลอกลวงให้ท่านให้ข้อมูลส่วนบุคคลแก่พวกเขา

พวกเขาสามารถใช้ข้อมูลนี้เพื่อ:



- เข้าถึงบัญชีออนไลน์ของท่าน



- แสร้งทำเป็นตัวท่าน



- ขโมยเงินของท่าน

มิจฉาชีพยังอาจที่จะ:



- สร้างบัญชีปลอมเพื่อหลอกท่าน



แชร์ลิงก์และโฆษณาเพื่อให้ท่านคลิก

ข้อสังเกตว่าสิ่งใดเป็นการหลอกลวง

อาจเป็นการหลอกลวงหาก:



- มีการขอให้ท่านทำอะไรบางอย่างอย่างรวดเร็ว



- เสนอเงินจำนวนมากให้ท่าน



- ขอเงินจากท่าน



- ขอให้ท่านคลิกที่ลิงก์



มิจนาศีพยงอาจสรงทำเป็นองคกรที่ท่านรู้จกและไว้วางใจ

ตัวอย่างเช่น ธนาคารของท่าน



มิจนาศีพทำเช่นนี้เพื่อให้ท่านเปิดเผยข้อมูลส่วนบุคคลของ
ท่านให้พวกเขา



ท่านควรหยุดพูดคุยกับบุคคลนั้นหากท่านคิดว่าพวกเขาเป็น
มิจนาศีพ



ท่านควรตรวจสอบว่าบุคคลนั้นเป็นคนที่เขาอ้างจริงหรือไม่

ท่านสามารถติดต่อบุคคลหรือองคกรนั้นได้โดยใช้รายละเอียดที่
ท่านไว้วางใจและหามาได้ด้วยตนเอง



รีบดำเนินการเพื่อปกป้องตัวเองทันที หากรู้สึกว่ามีบางอย่าง
ผิดปกติ

การรายงานการหลอกลวง



Scamwatch ช่วยเหลือชาวออสเตรเลียในเรื่องต่อไปนี้:

- การทำความเข้าใจเรื่องการหลอกลวง
- การรายงานการหลอกลวง



นอกจากนี้ Scamwatch ยังช่วยเหลือชาวออสเตรเลียที่ตกเป็นผู้เสียหายของการหลอกลวงอีกด้วย



ท่านสามารถรายงานเรื่องการหลอกลวงได้ที่เว็บไซต์
Scamwatch

www.scamwatch.gov.au/report-a-scam

แสดงความคิดเห็น



ท่านควรเป็นกระบอกเสียงถึงวิธีที่ผู้อื่นสามารถปกป้องตนเองบนโลกออนไลน์ได้

ซึ่งรวมถึง:



- การรายงานอาชญากรรมทางไซเบอร์



- การแบ่งปันสิ่งที่ท่านทราบกับครอบครัวและเพื่อน ๆ



เราจะอธิบายวิธีการที่ท่านสามารถเป็นกระบอกเสียงได้ในหน้าถัดไป

การรายงานอาชญากรรมทางไซเบอร์

การรายงานอาชญากรรมทางไซเบอร์ช่วยให้รัฐบาล:



- ได้เรียนรู้ว่าอาชญากรรมทางไซเบอร์พยายามโจมตีผู้คนอย่างไร



- ปกป้องผู้คนได้มากขึ้น



ท่านสามารถรายงานอาชญากรรมทางไซเบอร์ได้ที่เว็บไซต์
ReportCyber

www.cyber.gov.au/report

พูดคุยกับครอบครัวและเพื่อน ๆ เกี่ยวกับการรักษาความปลอดภัยบนโลกออนไลน์



ท่านควรแบ่งปันเคล็ดลับเกี่ยวกับการรักษาความปลอดภัยบนโลกออนไลน์กับครอบครัวและเพื่อน ๆ ของท่าน

ท่านเองก็สามารถเรียนรู้จากพวกเขาได้เช่นกัน



ท่านสามารถปกป้องตัวเองและคนรอบข้างได้ด้วยการแบ่งปันสิ่งที่ท่านทราบเกี่ยวกับการรักษาความปลอดภัยบนโลกออนไลน์



เรื่องนี้เป็นสิ่งสำคัญเช่นกัน หากท่านใช้อุปกรณ์ร่วมกับผู้อื่น

รายการคำศัพท์

รายการคำศัพท์นี้จะอธิบายความหมายของคำที่เป็นตัวหนาในคู่มือนี้



ไซเบอร์

ไซเบอร์ หมายถึงสิ่งที่เกี่ยวข้องกับอินเทอร์เน็ต

อาชญากรรมทางไซเบอร์



อาชญากรรมไซเบอร์ คือการที่อาชญากรใช้อินเทอร์เน็ตในการก่ออาชญากรรม

ตัวอย่างเช่น อาชญากรอาจใช้อินเทอร์เน็ตเพื่อ:

- ขโมยข้อมูลส่วนบุคคลของท่าน
- เข้าควบคุมบัญชีออนไลน์ของท่าน



การตั้งค่าตำแหน่ง

การตั้งค่าตำแหน่งจะแสดงตำแหน่งของอุปกรณ์ของท่าน



การยืนยันตัวตนแบบหลายปัจจัย (MFA)

MFA คือการใช้วิธีการตั้งแต่ 2 วิธีขึ้นไปในการเข้าสู่ระบบบัญชีของท่านทุกครั้ง



วลีรหัสผ่าน

วลีรหัสผ่านเป็นรหัสผ่านประเภทที่มีความแข็งแกร่งมากขึ้น
ซึ่งทำให้คนอื่นคาดเดาวลีรหัสผ่านได้ยาก



Wi-Fi สาธารณะ

Wi-Fi สาธารณะคืออินเทอร์เน็ตไร้สายฟรีที่ท่านสามารถใช้ได้ในที่สาธารณะ



การหลอกลวง

เราเรียกสิ่งนี้ว่าการหลอกลวง เมื่อมีคนพยายามที่จะ:

- หลอกลวงท่าน
- เอาเงินของท่านไป



มิจฉาชีพ

มิจฉาชีพคือคนที่กระทำการหลอกลวง

ติดต่อเรา



ท่านสามารถโทรสายด่วนความปลอดภัยทางไซเบอร์ของ
ออสเตรเลีย (Australian Cyber Security Hotline) ได้ที่
หมายเลข
1300 292 371



ท่านสามารถไปที่เว็บไซต์ของเราได้ที่
www.actnowstaysecure.gov.au



ท่านสามารถรายงานอาชญากรรมทางไซเบอร์ได้ที่เว็บไซต์
ReportCyber
www.cyber.gov.au/report



กลุ่มการเข้าถึงข้อมูล (Information Access Group) ได้จัดทำ
เอกสารฉบับอ่านง่ายนี้ โดยใช้ภาพถ่ายจากคลังภาพและภาพที่สร้างขึ้น
เอง ห้ามนำภาพไปใช้ซ้ำโดยมิได้รับอนุญาต หากมีคำถามเกี่ยวกับภาพ
โปรดไปที่ www.informationaccessgroup.com และระบุ
หมายเลขงาน 6342