



Australian Government  
Australian Signals Directorate

**ASD** AUSTRALIAN  
SIGNALS  
DIRECTORATE  
**ACSC** Australian  
Cyber Security  
Centre



# วิธีใช้อินเทอร์เน็ต อย่างปลอดภัย คู่มือสำหรับผู้สูงอายุ

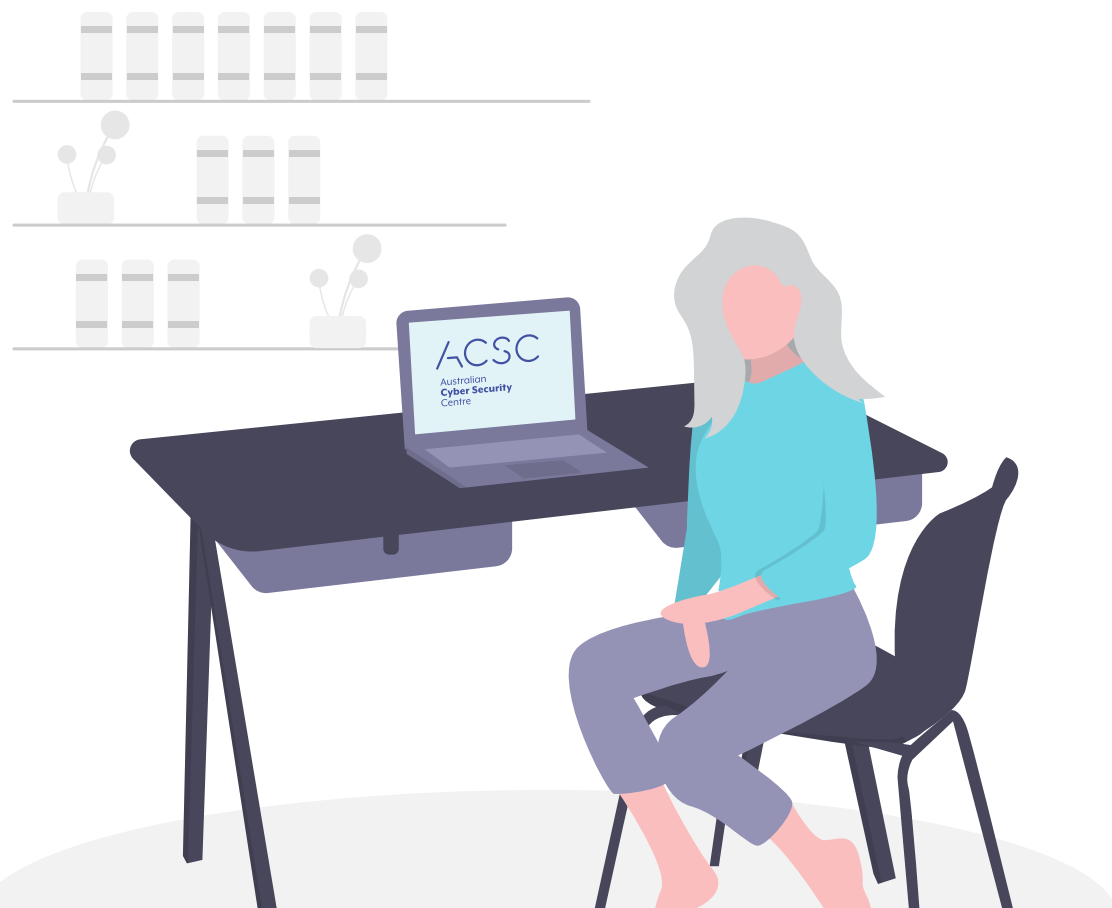
[cyber.gov.au](http://cyber.gov.au)

# คำนำ

การใช้อินเทอร์เน็ตช่วยให้คุณได้ติดต่อกับเพื่อน ๆ และครอบครัว เรียนรู้เกี่ยวกับเรื่องต่าง ๆ และแม้แต่เล่นเกม

เช่นเดียวกับการรัดเข็มขัดนิรภัยก่อนการขับรถ ก่อนใช้อินเทอร์เน็ต คุณควรดำเนินการตามขั้นตอนต่าง ๆ เพื่อรักษาให้คุณปลอดภัยยิ่งขึ้น

ศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย หรือ Australian Cyber Security Centre (ACSC) ต้องการให้ทุกคนปลอดภัยในขณะที่ออนไลน์ เอกสารนี้ครอบคลุมแนวทางปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์ขั้นพื้นฐานบางประการที่คุณสามารถใช้เพื่อป้องกันตัวเองในเวลาที่ใช้อินเทอร์เน็ต



ศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย (ACSC) ในฐานะส่วนหนึ่งของกรมสัญญาณแห่งออสเตรเลีย หรือ Australian Signals Directorate (ASD) เป็นผู้แนะนำ ให้ความช่วยเหลือ และตอบสนองด้านการปฏิบัติ เพื่อป้องกัน ตรวจสอบ และแก้ไขภัยคุกคามทางไซเบอร์ให้กับประเทศออสเตรเลีย ACSC เป็นองค์กรที่คอยช่วยทำให้ออสเตรเลียเป็นสถานที่ที่ปลอดภัยที่สุดที่จะเชื่อมต่อทางออนไลน์

สำหรับข้อมูลเพิ่มเติม คู่มือและคำแนะนำด้านการรักษาความปลอดภัยทางไซเบอร์ โปรดไปที่ [cyber.gov.au](https://cyber.gov.au)

# การรักษาความปลอดภัยทางไซเบอร์สำหรับผู้สูงอายุ

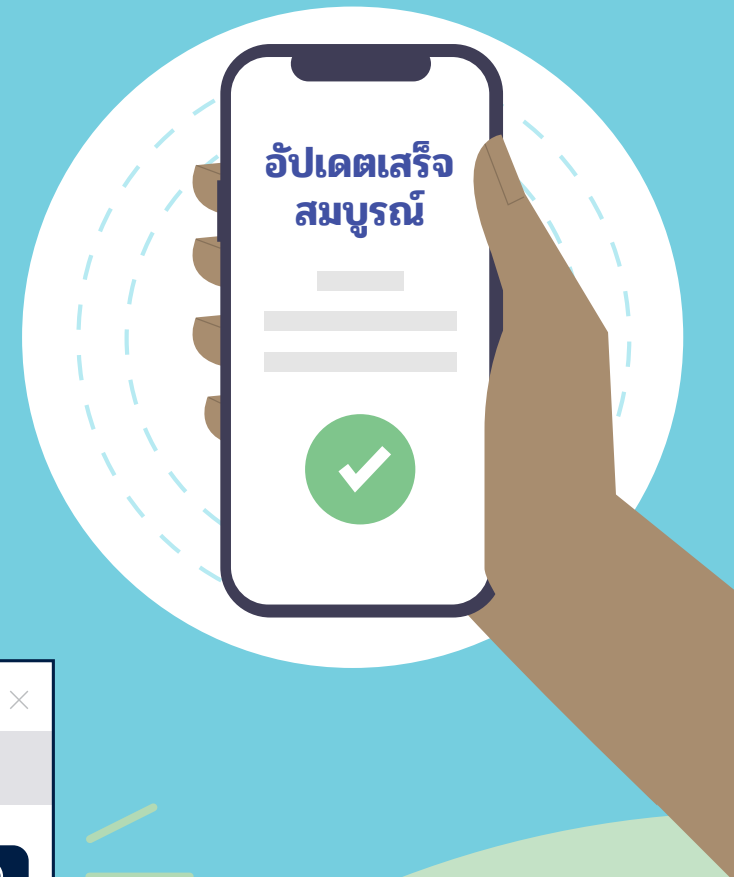


## เคล็ดลับที่ 1 อัปเดตอุปกรณ์ของคุณ

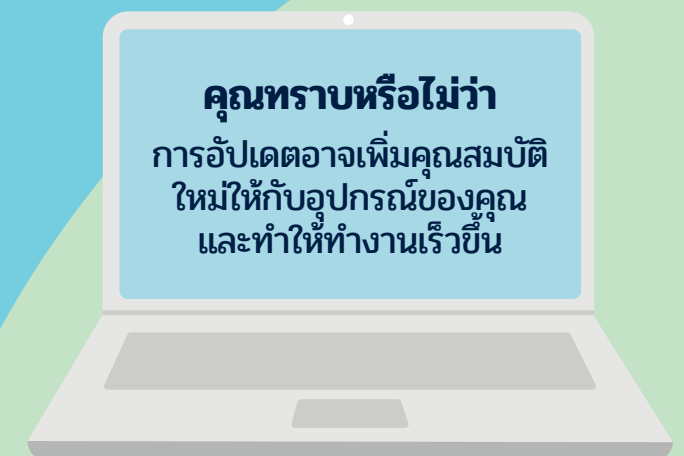
การอัปเดตซอฟต์แวร์ของคุณเปรียบเสมือนการนำรถของคุณเข้ารับบริการตรวจสอบสภาพเครื่อง ซึ่งเป็นการปรับปรุงประสิทธิภาพอุปกรณ์ของคุณให้ดีขึ้นและทำให้ปลอดภัยยิ่งขึ้น

อาชญากรไซเบอร์มักจะค้นหาวิธีการใหม่ ๆ ในการแฮก (Hack) เข้าอุปกรณ์ต่าง ๆ การตั้งค่าอุปกรณ์ของคุณให้มีการติดตั้งการอัปเดตอัตโนมัติจะช่วยแก้ไขจุดอ่อนต่าง ๆ ในซอฟต์แวร์ของคุณ และทำให้แฮกเกอร์ไม่สามารถทำอะไรคุณได้

หากต้องการข้อมูลเพิ่มเติม ให้ค้นหาคำว่า 'Updates' บนเว็บไซต์ [cyber.gov.au](https://cyber.gov.au)



**คุณทราบหรือไม่ว่า**  
การอัปเดตอาจเพิ่มคุณสมบัติใหม่ให้กับอุปกรณ์ของคุณ และทำให้ทำงานเร็วขึ้น





### เคล็ดลับที่ 2 เปิดการยืนยันตัวตนโดยใช้หลากหลายปัจจัย

การยืนยันตัวตนโดยใช้หลากหลายปัจจัย  
ในบัญชีของคุณเปรียบเสมือนประตูมั่งคั่ง  
นิรภัยที่บ้านคุณ  
ซึ่งช่วยปกป้องคุณจากอาชญากรที่พยายาม  
บุกรุกเข้ามา

เมื่อเปิดใช้งานการยืนยันตัวตนโดยใช้หลากหลายปัจจัย  
คุณต้องให้ข้อมูลหลายส่วนเพื่อเข้าถึงบัญชีของคุณ  
ตัวอย่างเช่น คุณอาจต้องป้อนรหัสผ่านและเลขรหัสที่ส่งมา  
ทางข้อความเพื่อเข้าสู่ระบบโทรศัพท์มือถือของคุณ

ระบบซับซ้อนหลายชั้นนี้ทำให้อาชญากรไซเบอร์แฮกเข้า  
ระบบได้ยากขึ้น พวกเขาอาจค้นพบส่วนหนึ่งส่วนใด เช่น  
รหัสผ่านของคุณ แต่ยังคงต้องได้รับชิ้นส่วนอื่น ๆ ของ  
ปริศนาเพื่อเข้าถึงบัญชีของคุณ

หากต้องการข้อมูลเพิ่มเติม ให้ค้นหาคำว่า  
'Multi-factor authentication' หรือ 'MFA'  
บนเว็บไซต์ [cyber.gov.au](https://www.cyber.gov.au)



#### โปรดจำไว้ว่า

หากคุณต้องการความช่วยเหลือในการเปิดการยืนยันตัวตนโดยใช้หลากหลายปัจจัย  
ให้ขอความช่วยเหลือจากเพื่อนหรือสมาชิกในครอบครัว



### เคล็ดลับที่ 3 สำรองข้อมูลในอุปกรณ์ของคุณ

การดำเนินการ 'สำรองข้อมูล' เป็นการ  
ทำสำเนาไฟล์สำคัญต่าง ๆ และเก็บไว้ในที่  
ที่ปลอดภัย ซึ่งเหมือนกับการถ่ายเอกสาร  
ภาพถ่ายที่มีค่าเพื่อเก็บไว้ในที่ปลอดภัย  
ในกรณีที่คุณทำต้นฉบับหาย

เมื่อคุณสำรองข้อมูลในคอมพิวเตอร์ โทรศัพท์ หรือ  
แท็บเล็ต สำเนาของไฟล์ของคุณจะถูกบันทึกทาง  
ออนไลน์หรือไปยังอุปกรณ์อื่น การสำรองข้อมูลไฟล์  
สำคัญต่าง ๆ และรูปภาพที่คุณรักจะช่วยให้คุณอุ่นใจ  
ได้มากขึ้น

หากมีสิ่งผิดปกติเกิดขึ้นกับอุปกรณ์ของคุณ หรือ  
คุณถูกแฮกโดยอาชญากรไซเบอร์ คุณสามารถกู้คืน  
ไฟล์ของคุณจากข้อมูลสำรองได้อย่างง่ายดาย

หากต้องการข้อมูลเพิ่มเติม ให้ค้นหาคำว่า  
'Backups' บนเว็บไซต์ [cyber.gov.au](https://www.cyber.gov.au)



#### คุณทราบหรือไม่ว่า

การสำรองข้อมูลในอุปกรณ์ของคุณเป็นประจำ หมายความว่า你能สามารถเข้าถึงไฟล์ล่าสุดได้เสมอ

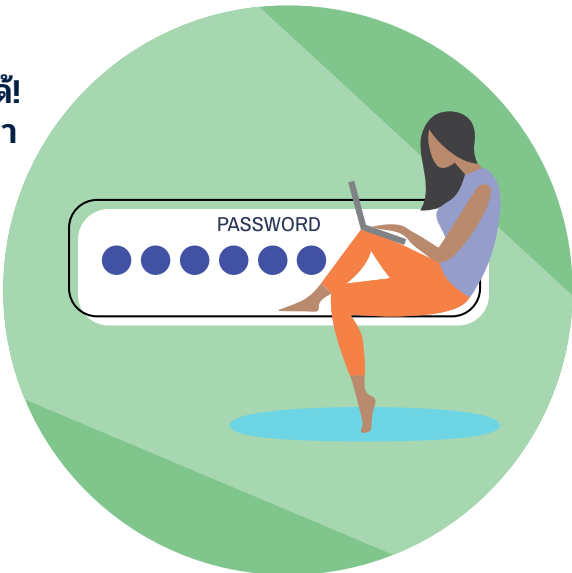
## เคล็ดลับที่ 4 ใช้ข้อความรหัสผ่าน

หากรหัสผ่านเป็นกุญแจให้กับบัญชีของคุณ รหัสผ่านที่เป็นข้อความจะช่วยรักษาระบบให้ปลอดภัยในตัวเองได้! ข้อความรหัสผ่านรัดกุมและปลอดภัยกว่ารหัสผ่านธรรมดา

ในเวลาที่ท่านไม่สามารถเปิดใช้ MFA ได้ ให้ใช้ข้อความรหัสผ่านเพื่อรักษาความปลอดภัยให้กับบัญชีของคุณ ข้อความรหัสผ่านใช้คำสุ่มสี่คำขึ้นไปเป็นรหัสผ่านของคุณ ซึ่งทำให้อาชญากรไซเบอร์เดาได้ยาก แต่ง่ายสำหรับคุณที่จะจดจำ

เมื่อคุณสร้างข้อความรหัสผ่าน ให้ทำดังนี้

- **มีความยาว ยิ่งยาวยิ่งดี** ตั้งเป้าหมายให้มีความยาวอย่างน้อย 14 ตัวอักษร คำสุ่มสี่คำขึ้นไปที่คุณจำได้นั้นจะดีที่สุด. ตัวอย่างเช่น 'purple duck potato boat'
- **คาดเดาไม่ได้** ยิ่งข้อความรหัสผ่านของคุณคาดเดายากเท่าไร ก็ยิ่งดีเท่านั้น ประโยคสามารถนำมาทำเป็นข้อความรหัสผ่านที่ดี แต่คาดเดาได้ง่ายกว่า การผสมคำแบบสุ่มตั้งแต่สี่คำขึ้นไปจะทำให้ข้อความรหัสผ่านคาดเดายากขึ้น
- **มีเอกลักษณ์** ยื่อนำข้อความรหัสผ่านของคุณกลับมาใช้อีก ใช้ข้อความรหัสผ่านที่แตกต่างกันสำหรับบัญชีต่าง ๆ หากคุณมีปัญหาในการจำข้อความรหัสผ่านทั้งหมด ให้พิจารณาใช้แอปจัดการรหัสผ่าน (Password Manager) ด้วยแอปจัดการรหัสผ่าน คุณเพียงต้องจดจำรหัสผ่านตัวเดียวเท่านั้น จากนั้นแอปจัดการรหัสผ่านจะดูแลส่วนที่เหลือเอง ค้นหาว่า 'Password Manager' บนเว็บไซต์ cyber.gov.au เพื่อขอคำแนะนำเพิ่มเติม



เรียนรู้เพิ่มเติมเกี่ยวกับการสร้างข้อความรหัสผ่านที่ปลอดภัยโดยค้นหาคำว่า 'Passphrases' บนเว็บไซต์ cyber.gov.au

## เคล็ดลับที่ 5 รู้จักจำแนกและรายงานสแกม

ยิ่งคุณรายงานสแกมได้เร็วเท่าไร เราก็ยิ่งดำเนินการได้เร็วเท่านั้น

หากคุณเชื่อว่ามีคนพยายามใช้อินเทอร์เน็ตเพื่อสแกมคุณ ควรตั้งรับมือและระมัดระวังตัวไว้ก่อนยอมตกเป็นเหยื่อที่จะถูกเอาเปรียบ

ถ้ามันฟังดูดีเกินจริง ก็อาจจะเป็นเช่นนั้นจริง ๆ แม้ว่าข้อความอาจบอกว่า คุณได้รับรางวัลหรือคอมพิวเตอร์ของคุณมีไวรัส แต่ข้อความนั้นไม่ได้มีไว้สำหรับคุณโดยเฉพาะ

มันอาจมาจากสแกมเมอร์และพวกเขาต้องการเอารัดเอาเปรียบคุณ

โปรดจำไว้ว่า สแกมเมอร์มักจะสร้างทำเป็นบุคคลหรือองค์กรที่คุณไว้วางใจ ตั้งเป็นข้อสงสัยไว้หากคุณได้รับข้อความที่ดูเหมือนมาจากคนที่คุณไว้วางใจ แต่ใช้หมายเลขโทรศัพท์ ที่อยู่อีเมล หรือโปรไฟล์โซเชียลมีเดียใหม่ ก่อนที่คุณจะตอบกลับ ให้ตรวจสอบว่าบุคคลหรือองค์กรที่ส่งข้อความมาหาคุณนั้นมีตัวตนอยู่จริง โดยติดต่อผ่านช่องทางที่คุณไว้วางใจได้ ตัวอย่างเช่น หากคุณได้รับข้อความตัวอักษรที่ดูเหมือนมาจากลูกคนใดคนหนึ่งของคุณ แต่มาจากหมายเลขใหม่ จงอย่าตอบกลับ ส่งข้อความไปหาลูกบนโซเชียลมีเดียก่อน เพื่อตรวจสอบว่าพวกเขาได้เปลี่ยนหมายเลขโทรศัพท์จริงหรือไม่



**คุณทราบหรือไม่ว่า**

อาชญากรไซเบอร์นั้นฉลาดแถมโกง และอาจใช้ชื่อและที่อยู่อีเมลที่คุณคุ้นเคยให้ระมัดระวังตัวไว้ หาก

- คุณถูกขอให้จ่ายใบเรียกเก็บเงินอย่างเร่งด่วน
- คุณถูกขอให้เปลี่ยนรายละเอียดหรือรหัสผ่านของคุณ
- คุณถูกขอให้คลิกลิงก์หรือเปิดไฟล์ที่แนบมากับอีเมล



## บทสรุป

ตอนนี้คุณมีความรู้ในการใช้อินเทอร์เน็ตอย่างปลอดภัยมากขึ้นแล้ว คุณสามารถท่องเว็บด้วยความมั่นใจและเพลิดเพลินกับการใช้เวลาออนไลน์ต่อไปได้

โปรดอย่าลืมว่า อาชญากรไซเบอร์มักค้นคิดหาวิธีการใหม่ ๆ เพื่อพุ่งเป้าหาเหยื่ออยู่เสมอ

จึงไม่ใช่เรื่องเสียหายอะไรที่จะปิดฝนความรู้ความชำนาญด้านการรักษาความปลอดภัยทางไซเบอร์เป็นครั้งคราว และเรียนรู้วิธีใหม่ ๆ ในการรักษาความปลอดภัย

# เคล็ดลับเพิ่มเติม

ต้องการเรียนรู้วิธีเพิ่มเติมในการอยู่อย่างปลอดภัยทางออนไลน์หรือไม่? ตรวจสอบเคล็ดลับต่อไปนี้

### คิดเกี่ยวกับสิ่งที่คุณโพสต์

คิดอย่างรอบคอบเกี่ยวกับข้อมูลที่คุณจะแชร์ทางออนไลน์และผู้ที่มองเห็น รับเฉพาะคำขอเป็นเพื่อนจากคนที่คุณรู้จักในชีวิตจริงเท่านั้น

### รับการแจ้งเตือนเกี่ยวกับภัยคุกคามใหม่ ๆ

สมัครใช้บริการแจ้งเตือนฟรีของเรา ซึ่งจะแจ้งให้คุณทราบเมื่อใดก็ตามที่เราพบภัยคุกคามทางไซเบอร์ใหม่

โดยจะให้คำแนะนำคุณเกี่ยวกับสิ่งที่ต้องทำ หากเกิดการโจรกรรมขึ้น

พูดคุยเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์กับครอบครัวและเพื่อน ๆ

ตอนนี้คุณได้เพิ่มทักษะด้านการรักษาความปลอดภัยทางไซเบอร์แล้ว แบ่งปันสิ่งที่คุณได้เรียนรู้กับครอบครัวและเพื่อนของคุณ ความรู้ของคุณสามารถช่วยพวกเขาให้พ้นจากสถานการณ์ที่ยากลำบากได้!

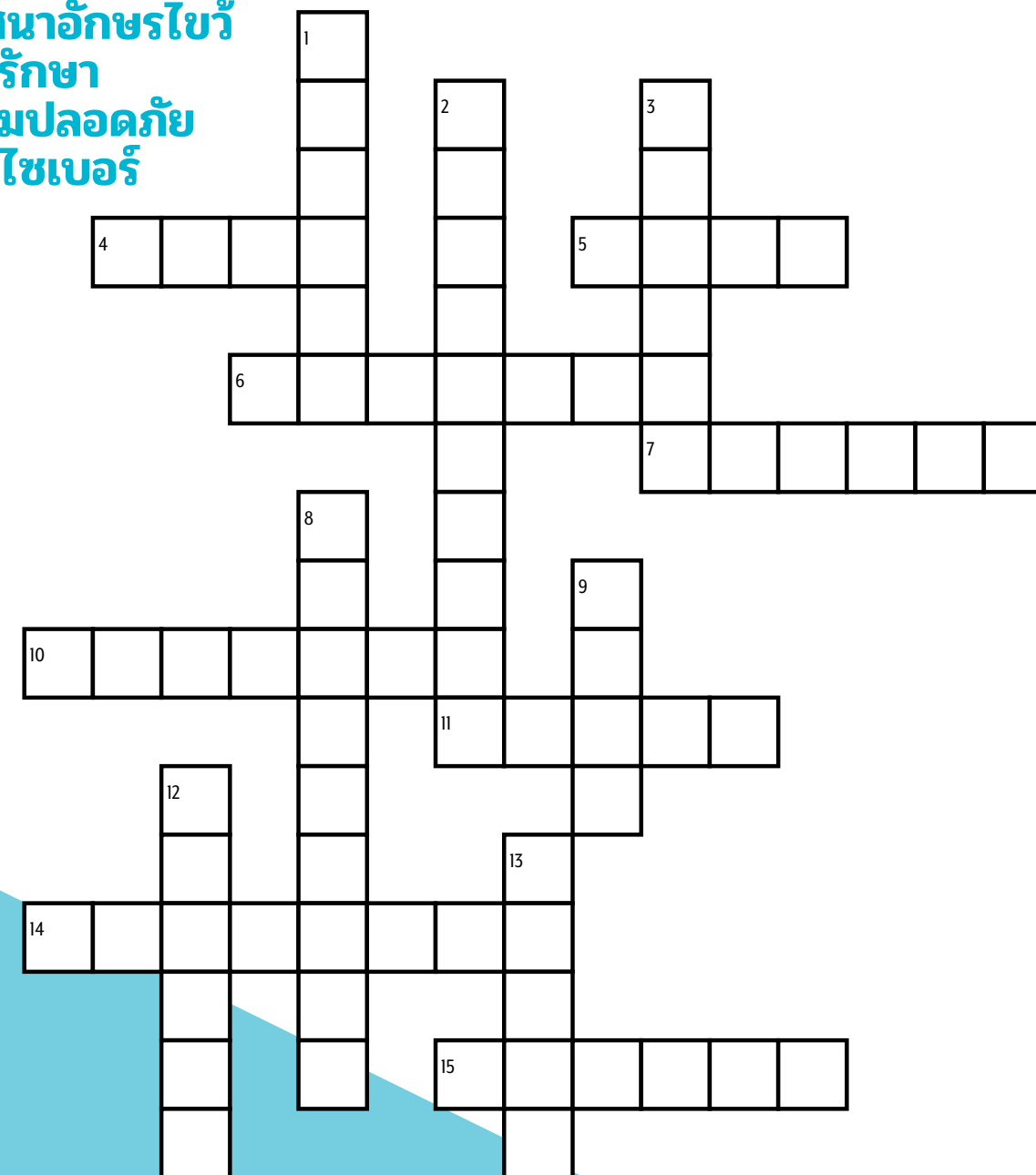
### หลีกเลี่ยงการใช้ Wi-Fi สาธารณะเมื่อคุณทำธุรกรรมธนาคารหรือจ่ายซื้อของทางออนไลน์

Wi-Fi สาธารณะนั้นดีสำหรับการดูวิดีโอหรืออ่านเว็บไซต์ แต่เก็บบกกิจกรรมออนไลน์อื่นใดที่เกี่ยวข้องกับเงินไว้เมื่อคุณเชื่อมต่ออินเทอร์เน็ตที่บ้านของคุณเท่านั้น Wi-Fi สาธารณะอาจมีความเสี่ยง

### รายงานอาชญากรรมและเหตุการณ์ทางไซเบอร์ต่าง ๆ เพื่อรักษาให้ออสเตอร์เลียปลอดภัย

หากคุณคิดว่าคุณตกเป็นเหยื่อของอาชญากรไซเบอร์ ให้รีบดำเนินการอย่างรวดเร็ว คำแนะนำเพิ่มเติมสามารถพบได้ที่เว็บไซต์ [cyber.gov.au](http://cyber.gov.au)

## ปริศนาอักษรไขว้ การรักษา ความปลอดภัย ทางไซเบอร์



### บนลงล่าง

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

### ตามขวาง

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

คู่มือเพิ่มเติม

สำหรับข้อมูลเพิ่มเติม โปรดดูชุดการรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคลของเรา ซึ่งเป็นคู่มือ 3 ฉบับที่ออกแบบมาเพื่อช่วยให้ชาวออสเตรเลียเข้าใจพื้นฐานของการรักษาความปลอดภัยทางไซเบอร์ในชีวิตประจำวัน และวิธีที่คุณสามารถดำเนินการเพื่อป้องกันตนเองจากภัยคุกคามทางไซเบอร์ทั่วไป



คุณสามารถเข้าถึงคู่มือทั้งสามได้ที่เว็บไซต์ [cyber.gov.au](https://www.cyber.gov.au)

คำตอบปริศนาอักษรไขว้:

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

หมายเหตุ

Handwriting practice lines consisting of 15 horizontal lines.

#### ข้อจำกัดความรับผิดชอบ (Disclaimer)

เนื้อหาในคู่มือนี้มีลักษณะทั่วไปและไม่ควรยึดถือเป็นคำแนะนำทางกฎหมายหรือเป็นที่พึ่ง  
สำหรับความช่วยเหลือในสถานการณ์เฉพาะหรือ สถานการณ์ฉุกเฉินใด ๆ ในเรื่องที่สำคัญใด ๆ  
คุณควรขอคำแนะนำจากผู้เชี่ยวชาญอิสระที่เหมาะสมกับสถานการณ์ของตนเอง

เครือรัฐจะไม่รับผิดชอบหรือมีส่วนรับผิดชอบต่อความเสียหาย การสูญเสีย หรือค่าใช้จ่ายที่เกิดขึ้น  
จากการพึ่งพาข้อมูลที่มีอยู่ในคู่มือนี้

#### ลิขสิทธิ์ (Copyright)

© เครือรัฐออสเตรเลีย 2023

ยกเว้นตราแผ่นดิน (Coat of Arms) และที่ระบุไว้เป็นอย่างอื่น เนื้อหาทั้งหมดที่นำเสนอ  
บนสื่อพิมพ์นี้จัดทำขึ้นภายใต้ ใบอนุญาตระหว่างประเทศของครีเอทีฟคอมมอนส์  
(Creative Commons Attribution International licence) ([www.creativecommons.org/licenses](http://www.creativecommons.org/licenses))

เพื่อมิให้เกิดข้อสงสัย ใบอนุญาตในที่นี้ใช้กับเนื้อหาตามที่กำหนดไว้ในเอกสารนี้เท่านั้น



รายละเอียดเงื่อนไขใบอนุญาตที่เกี่ยวข้องมีอยู่ในเว็บไซต์ของครีเอทีฟคอมมอนส์  
เช่นเดียวกับประมวลกฎหมายฉบับเต็มสำหรับใบอนุญาต CC BY 4.0

([www.creativecommons.org/licenses](http://www.creativecommons.org/licenses))

#### การใช้ตราแผ่นดิน (Use of the Coat of Arms)

ข้อกำหนดการใช้ตราแผ่นดินมีนำเสนอในรายละเอียดบนเว็บไซต์ของสำนักนายกรัฐมนตรี  
และคณะรัฐมนตรี (Department of Prime Minister and Cabinet website)  
([www.pmc.gov.au/government/commonwealth-coat-arms](http://www.pmc.gov.au/government/commonwealth-coat-arms))

สำหรับข้อมูลเพิ่มเติมหรือรายงานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัย  
ทางไซเบอร์ ติดต่อเราที่

[cyber.gov.au](http://cyber.gov.au) | 1300 CYBER1 (1300 292 371)

หมายเลขนี้มีไว้สำหรับใช้ภายในออสเตรเลียเท่านั้น



Australian Government  
Australian Signals Directorate

ASD AUSTRALIAN  
SIGNALS  
DIRECTORATE  
ACSC Australian  
Cyber Security  
Centre