

คู่มือการดูแลรักษาเครื่องคอมพิวเตอร์ Windows 11 สำหรับผู้ใช้ทั่วไป

สารบัญ

การใช้งาน Disk Cleanup	2
การตรวจสอบและอัปเดต Windows	5
การจัดการพื้นที่เก็บข้อมูล(Storage Sense)	7
การสแกนไวรัสและมัลแวร์ด้วย Microsoft Defender	10
การถอนการติดตั้งโปรแกรมที่ไม่จำเป็น	13
จัดการ Startup Programs	15
การตรวจสอบสุขภาพของฮาร์ดดิสก์และ SSD	18
การสำรองข้อมูล(Backup)	21
การทำความสะอาดภายนอกเครื่องคอมพิวเตอร์	27
การตั้งค่าความปลอดภัยพื้นฐาน	29

บทนำ

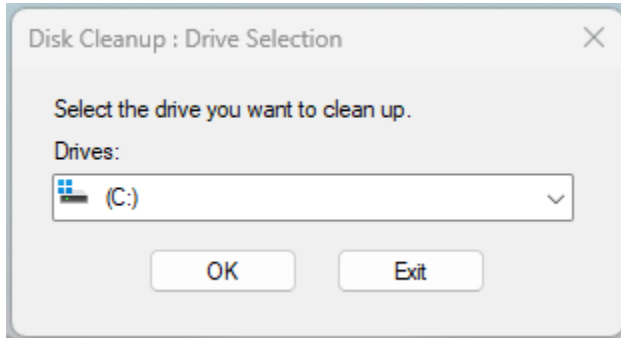
Disk Cleanup เป็นเครื่องมือใน Windows ที่ช่วยให้ผู้ใช้สามารถลบไฟล์ที่ไม่จำเป็นออกจากระบบ เพื่อเพิ่มพื้นที่ว่างในฮาร์ดดิสก์และปรับปรุงประสิทธิภาพของเครื่องคอมพิวเตอร์

คำอธิบายรายการไฟล์ที่สามารถลบได้

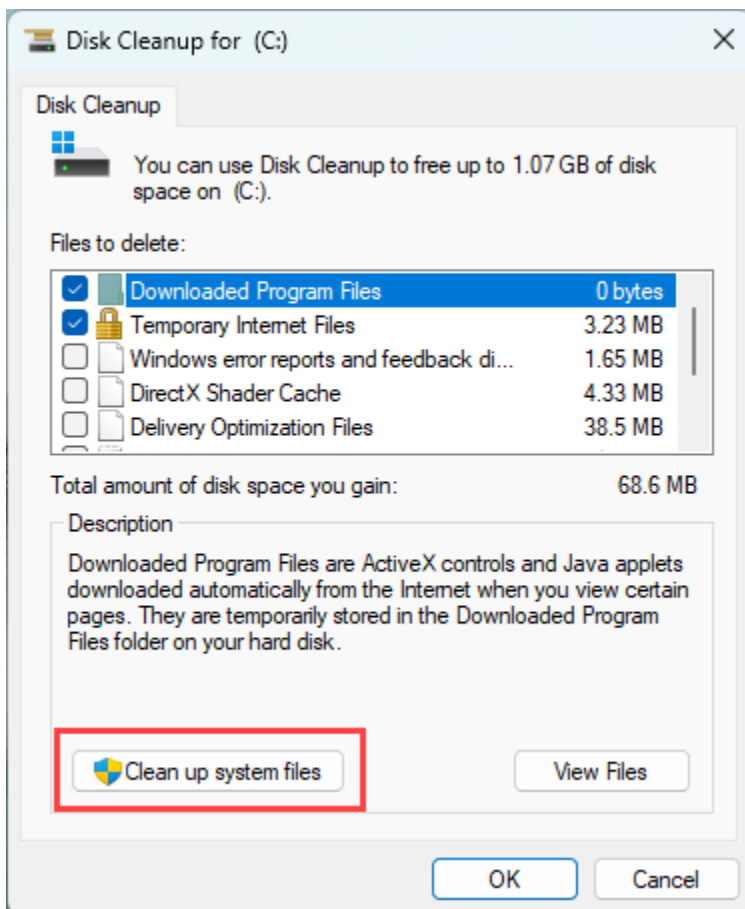
- **Windows Upgrade Cleanup:** ไฟล์เก่าจากการอัปเดต Windows สามารถลบได้หากไม่ต้องการย้อนกลับ
- **Microsoft Defender Antivirus:** ไฟล์จากการสแกนไวรัสของ Defender ลบได้โดยไม่กระทบการทำงาน
- **Windows Upgrade Log Files:** ไฟล์บันทึกการอัปเดต ลบได้หากไม่มีปัญหาหลังอัปเดต
- **System Error Minidump Files:** ไฟล์ข้อผิดพลาดระบบ ใช้วิเคราะห์ Blue Screen ลบได้หากไม่ต้องการวิเคราะห์
- **Windows Error Reports and Feedback:** รายงานข้อผิดพลาดที่ส่งไปยัง Microsoft ลบได้
- **DirectX Shader Cache:** แคชกราฟิก DirectX ลบได้ ระบบจะสร้างใหม่เมื่อจำเป็น
- **Delivery Optimization Files:** ไฟล์อัปเดตที่แชร์กับอุปกรณ์อื่น ลบได้หากไม่ใช่พีเจอรัน
- **Device Driver Packages:** ไดรเวอร์เก่าที่ไม่ได้ใช้งาน ลบได้หากไม่มีปัญหากับอุปกรณ์
- **Temporary Files:** ไฟล์ชั่วคราวจากแอปและระบบ ลบได้เพื่อเพิ่มพื้นที่
- **Recycle Bin:** ไฟล์ในถังขยะ ลบได้หากไม่ต้องการกู้คืน
- **Thumbnails:** ภาพตัวอย่างไฟล์ ลบได้ ระบบจะสร้างใหม่เมื่อเปิดโฟลเดอร์

ขั้นตอนการใช้งาน Disk Cleanup

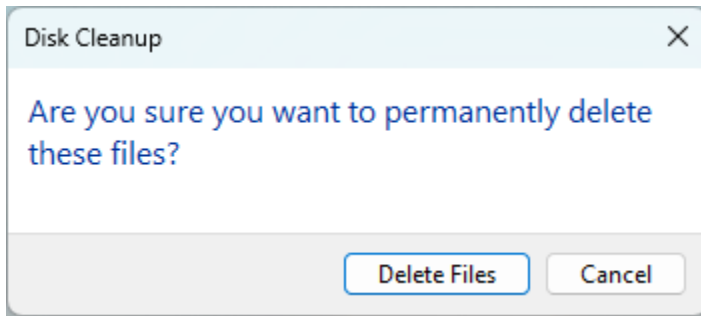
1. คลิกปุ่ม Start แล้วพิมพ์ 'Disk Cleanup' จากนั้นคลิกที่โปรแกรมที่แสดงขึ้นมา
2. เลือกไดรฟ์ที่ต้องการทำความสะอาด (เช่น C:) แล้วคลิก OK



3. รอให้ระบบคำนวณพื้นที่ที่สามารถลบได้
4. เลือกรายการไฟล์ที่ต้องการลบโดยการติ๊กเครื่องหมายถูก หากต้องการลบ system file ให้คลิกที่ปุ่ม Clean up system files จะมีรายการของ system files มาให้เลือกลบได้



5. เลือกไฟล์ที่ต้องการลบ และคลิกปุ่ม 'OK' แล้วเลือก 'Delete Files' เพื่อยืนยันการลบ



คำแนะนำเพิ่มเติม

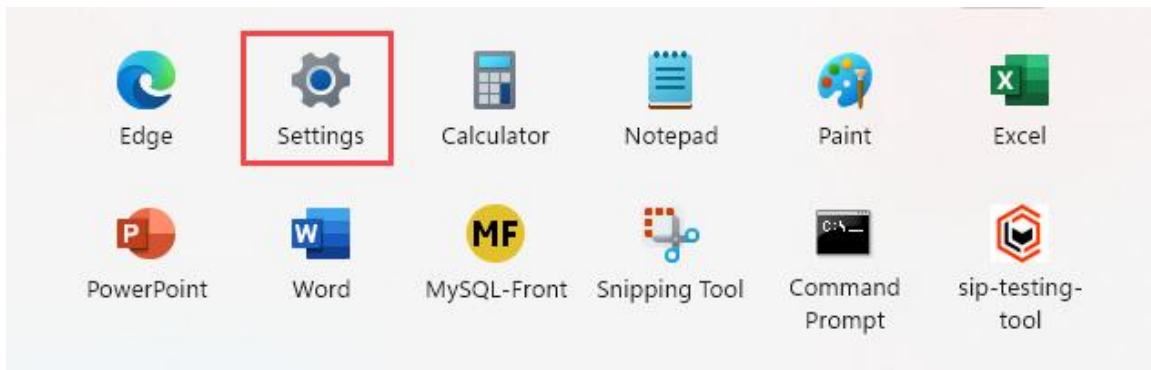
การลบไฟล์เหล่านี้ส่วนใหญ่ปลอดภัยและช่วยเพิ่มพื้นที่ว่างในเครื่อง อย่างไรก็ตาม
ควรตรวจสอบให้แน่ใจว่าไม่ต้องการย้อนกลับระบบหรือกู้คืนไฟล์ก่อนทำการลบ

คู่มือการตรวจสอบและอัปเดต Windows (Windows Update)

การอัปเดต Windows เป็นสิ่งสำคัญที่ช่วยให้ระบบปฏิบัติการมีความปลอดภัย เสถียร และสามารถใช้งานฟีเจอร์ใหม่ ๆ ได้อย่างเต็มประสิทธิภาพ
ผู้ใช้ทั่วไปสามารถตรวจสอบและตั้งค่าให้อัปเดตอัตโนมัติได้ง่าย ๆ ตามขั้นตอนด้านล่างนี้

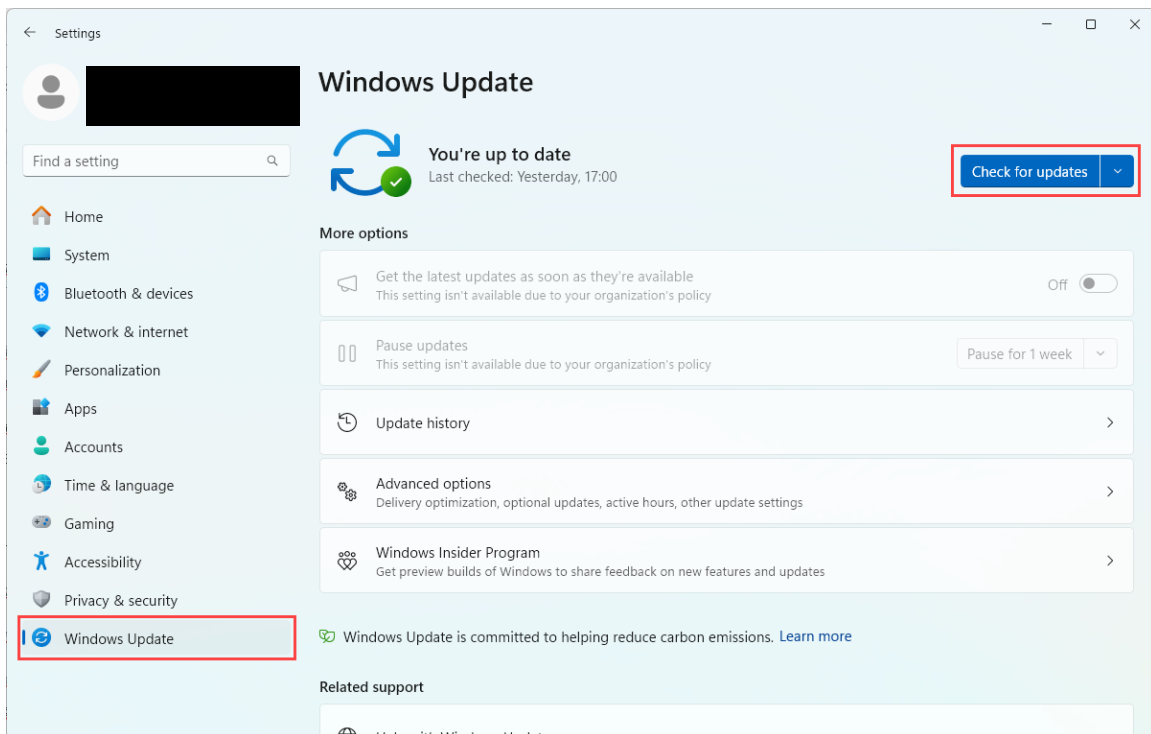
ขั้นตอนการตรวจสอบและติดตั้งอัปเดต

1. คลิกที่ปุ่ม "Start" แล้วเลือก "Settings" (การตั้งค่า)



2. ในหน้าต่าง Settings ให้เลือก "Windows Update" ที่แถบด้านซ้าย

3. คลิกปุ่ม "Check for updates" (ตรวจสอบการอัปเดต)



4. หากมีอัปเดตใหม่ ระบบจะดาวน์โหลดและติดตั้งโดยอัตโนมัติ
5. หลังติดตั้งเสร็จ อาจต้องรีสตาร์ทเครื่องเพื่อให้การอัปเดตมีผล

ประโยชน์ของการอัปเดต Windows

- ปรับปรุงความปลอดภัยของระบบ
- แก้ไขข้อผิดพลาดและบั๊กต่าง ๆ
- เพิ่มฟีเจอร์ใหม่และปรับปรุงประสิทธิภาพ
- รองรับฮาร์ดแวร์และซอฟต์แวร์ใหม่ ๆ

การตั้งค่าให้อัปเดตอัตโนมัติ

หมายเหตุ สำหรับเครื่องที่ใช้งานภายในมหาวิทยาลัยนเรศวรจะถูกปิดการตั้งค่าไว้ตามข้อกำหนดของมหาวิทยาลัย

1. ไปที่ "Settings" > "Windows Update"
2. คลิกที่ "Advanced options" (ตัวเลือกขั้นสูง)
3. เปิดใช้งาน "Receive updates for other Microsoft products" และ "Download updates over metered connections" ตามต้องการ
4. ตรวจสอบว่า "Automatic updates" ถูกตั้งค่าเป็น "On"

เคล็ดลับและการแก้ไขปัญหา

- ตรวจสอบการเชื่อมต่ออินเทอร์เน็ตก่อนอัปเดต
- หากอัปเดตไม่สำเร็จ ให้ลองรีสตาร์ทเครื่องแล้วตรวจสอบอีกครั้ง
- ใช้เครื่องมือ "Troubleshoot" ใน Settings เพื่อแก้ไขปัญหา Windows Update
- ตรวจสอบพื้นที่ว่างในไดรฟ์ C: เพื่อให้การอัปเดตสามารถติดตั้งได้

การจัดการพื้นที่เก็บข้อมูล (Storage Sense)

บทนำ

Storage Sense เป็นฟีเจอร์ใน Windows 11

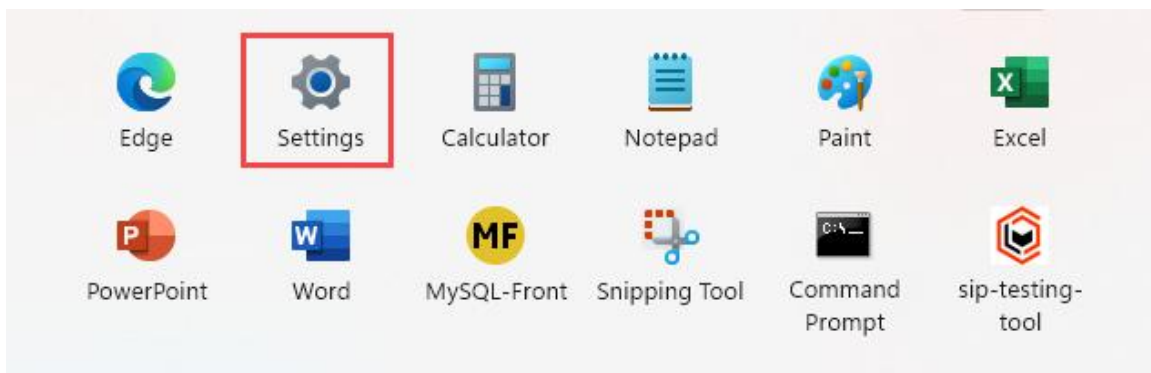
ที่ช่วยให้ผู้ใช้สามารถจัดการพื้นที่เก็บข้อมูลได้อย่างมีประสิทธิภาพ โดยระบบจะลบไฟล์ที่ไม่จำเป็น เช่น ไฟล์ชั่วคราว ไฟล์ในถังรีไซเคิล และไฟล์ในโฟลเดอร์ดาวน์โหลดตามระยะเวลาที่กำหนด ช่วยเพิ่มพื้นที่ว่างในเครื่องและทำให้ระบบทำงานได้ราบรื่นยิ่งขึ้น

ประโยชน์ของ Storage Sense

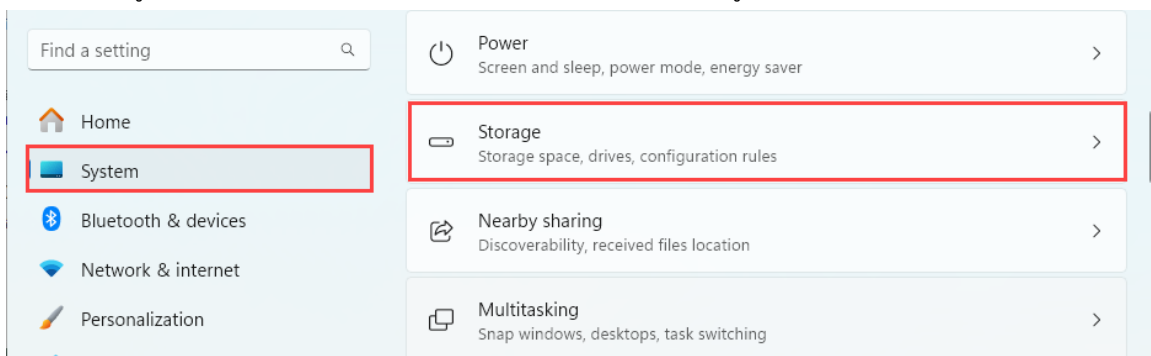
- เพิ่มพื้นที่ว่างในฮาร์ดดิสก์โดยอัตโนมัติ
- ลดความจำเป็นในการลบไฟล์ด้วยตนเอง
- ช่วยให้ระบบทำงานได้เร็วขึ้นและมีประสิทธิภาพ

ขั้นตอนการเปิดใช้งานและตั้งค่า Storage Sense

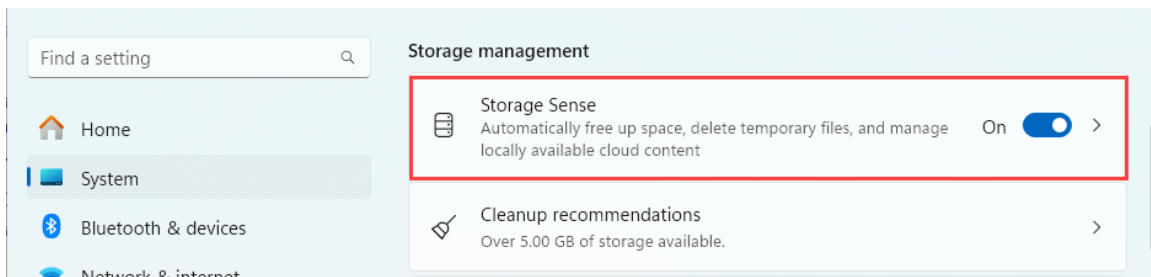
6. คลิกที่ปุ่ม Start แล้วเลือก 'Settings' (การตั้งค่า)



7. ไปที่เมนู 'System' (ระบบ) แล้วเลือก 'Storage' (พื้นที่เก็บข้อมูล)



8. คลิกที่ 'Storage Sense'

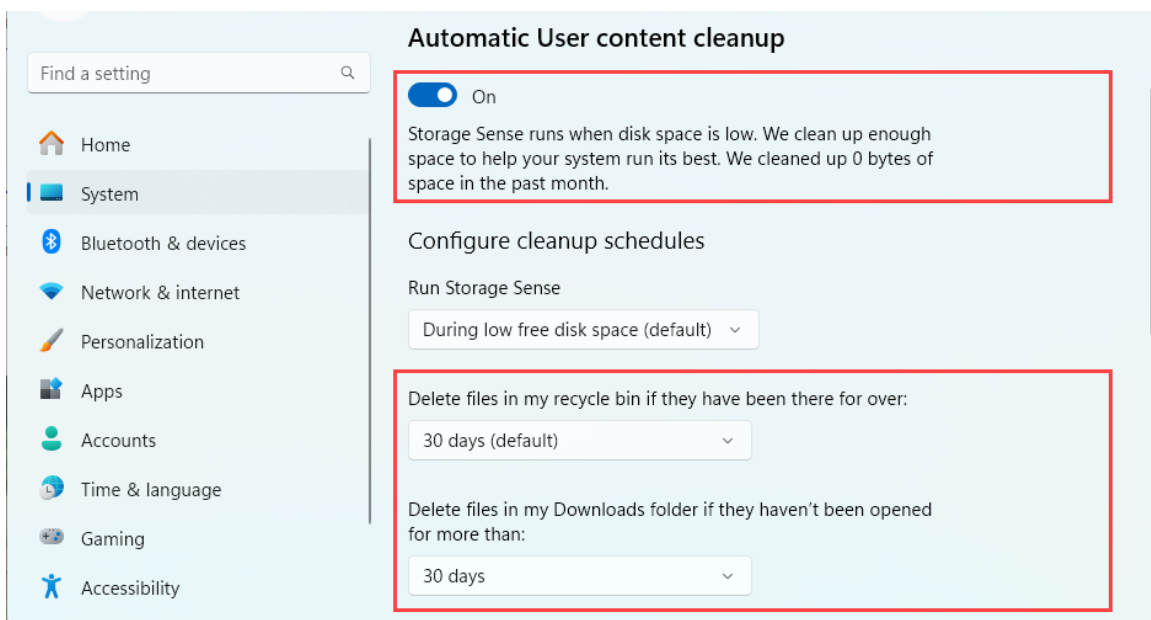


9. เปิดสวิตช์ 'Automatic User content cleanup' เพื่อเปิดใช้งาน

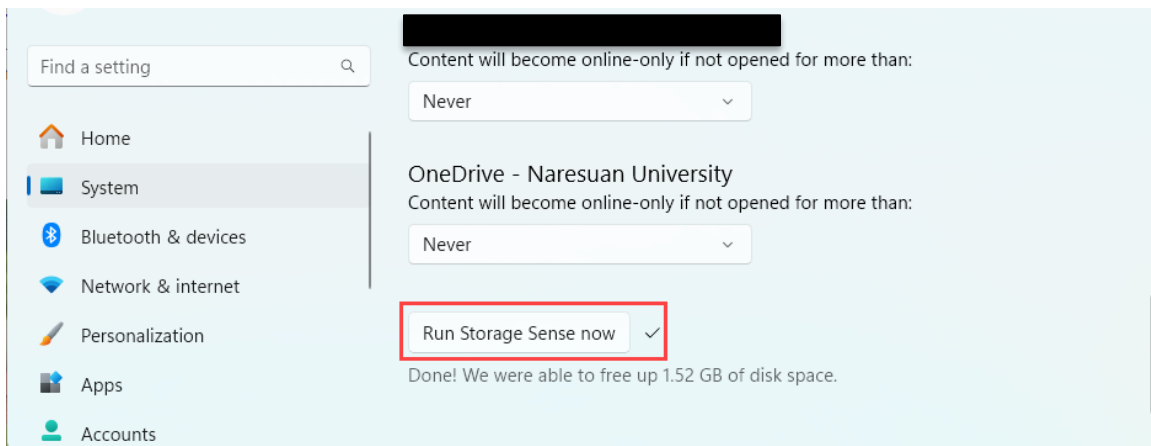
10. ตั้งค่าระยะเวลาในการลบไฟล์ เช่น:

11. ลบไฟล์ในถังรีไซเคิลหลังจาก: 1, 14, 30 หรือ 60 วัน

12. ลบไฟล์ในโฟลเดอร์ดาวน์โหลดหลังจาก: ไม่เคย, 1, 14, 30 หรือ 60 วัน



13. คลิก 'Run Storage Sense now' หากต้องการล้างไฟล์ทันที



เคล็ดลับในการใช้งาน Storage Sense อย่างมีประสิทธิภาพ

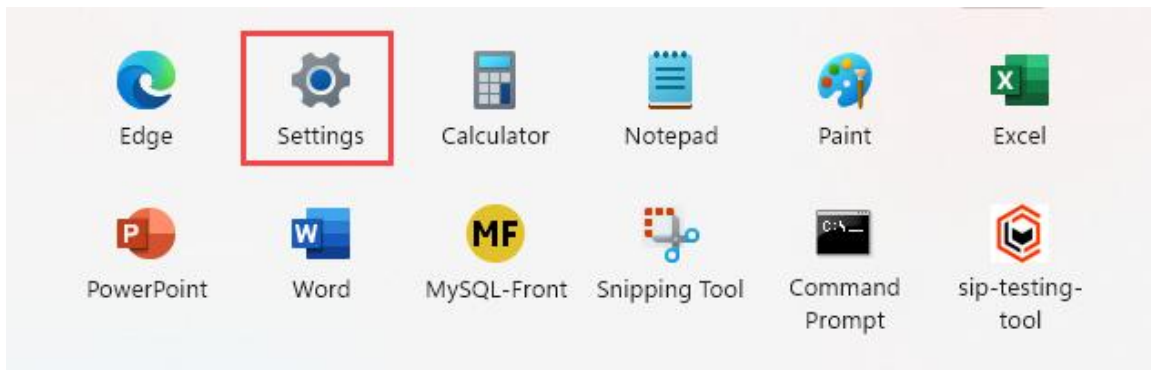
- เปิดใช้งาน Storage Sense แบบอัตโนมัติ เพื่อให้ระบบจัดการพื้นที่อย่างต่อเนื่อง
- ตรวจสอบไฟล์เดอร์ตาวน์โหลดก่อนตั้งค่าให้ลบอัตโนมัติ เพื่อไม่ให้ไฟล์สำคัญถูกลบ
- ใช้ร่วมกับ Disk Cleanup เพื่อเพิ่มประสิทธิภาพในการจัดการพื้นที่
- ตรวจสอบพื้นที่เก็บข้อมูลในแต่ละไดรฟ์เป็นระยะ เพื่อวางแผนการใช้งาน

การสแกนไวรัสและมัลแวร์ด้วย Microsoft Defender

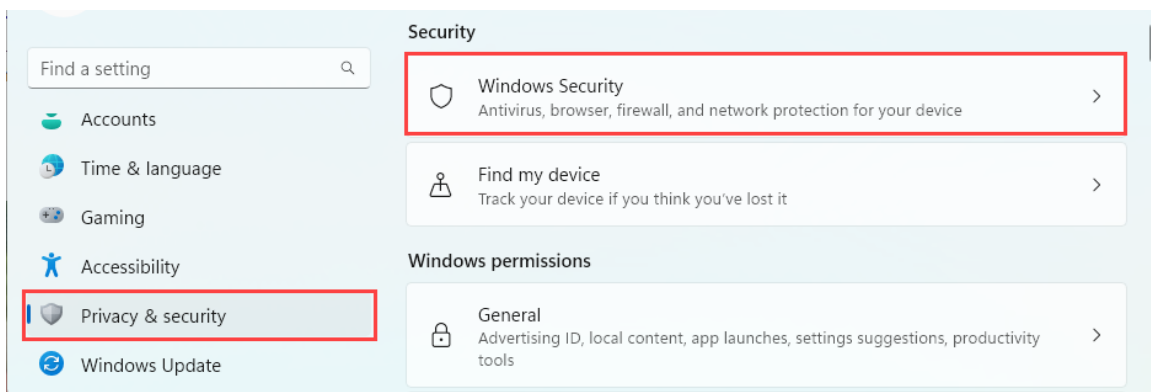
Microsoft Defender เป็นโปรแกรมป้องกันไวรัสและมัลแวร์ที่มาพร้อมกับ Windows 11 โดยไม่ต้องติดตั้งเพิ่มเติม สามารถช่วยป้องกันภัยคุกคามจากอินเทอร์เน็ต ไฟล์ที่เป็นอันตราย และโปรแกรมไม่พึงประสงค์ได้อย่างมีประสิทธิภาพ

ขั้นตอนการสแกนไวรัสและมัลแวร์

1. คลิกที่ปุ่ม "Start" แล้วเลือก "Settings" (การตั้งค่า)



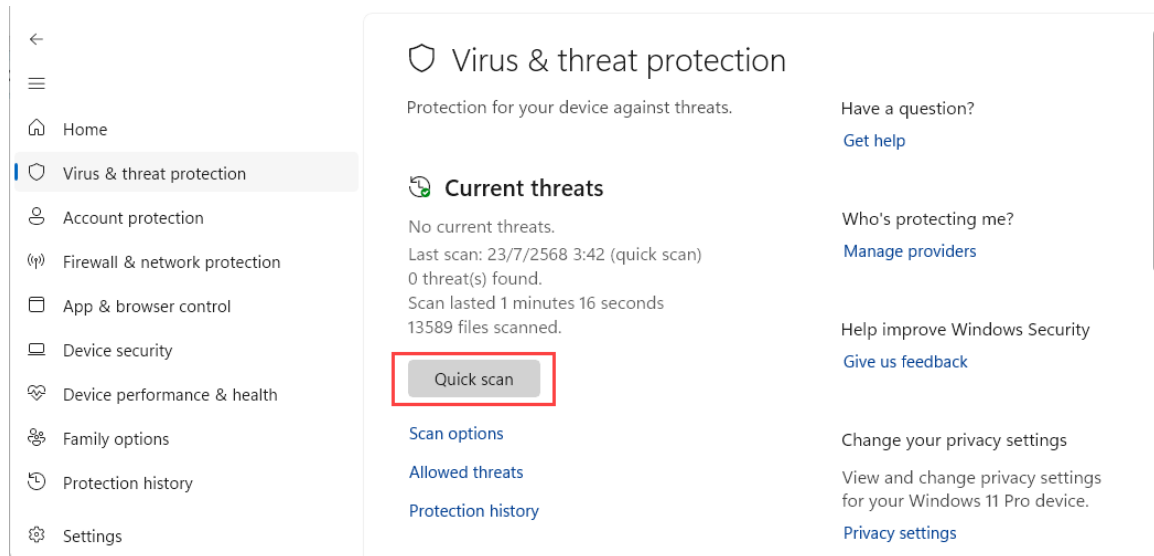
2. ในหน้าต่าง Settings ให้เลือก 'Privacy & Security' > 'Windows Security' ที่แถบด้านซ้าย



3. คลิก 'Virus & threat protection'



4. ในหน้าต่างใหม่ คลิก 'Quick scan' เพื่อเริ่มการสแกนแบบรวดเร็ว
5. หากต้องการสแกนแบบละเอียด ให้คลิก 'Scan options' แล้วเลือก 'Full scan' หรือ 'Custom scan'



การตั้งค่าการป้องกันแบบเรียลไทม์

1. ในหน้าต่าง 'Virus & threat protection' คลิก 'Manage settings' ได้หัวข้อ 'Virus & threat protection settings'
2. เปิดสวิตช์ 'Real-time protection' เพื่อให้ระบบตรวจสอบไฟล์และกิจกรรมต่าง ๆ แบบทันที

การอัปเดตฐานข้อมูลไวรัส

1. ในหน้าต่าง 'Virus & threat protection' คลิก 'Check for updates' ได้หัวข้อ 'Virus & threat protection updates'
2. คลิก 'Check for updates' อีกครั้งเพื่อให้ระบบตรวจสอบและติดตั้งฐานข้อมูลไวรัสล่าสุด

การแปลผลลัพธ์การสแกน

หลังจากการสแกนเสร็จสิ้น ระบบจะแสดงผลพบว่าเจอภัยคุกคามหรือไม่ หากพบภัยคุกคาม Microsoft Defender จะดำเนินการกักกันหรือแจ้งเตือนให้ผู้ใช้เลือกการจัดการ

เคล็ดลับการใช้งานอย่างปลอดภัย

- หมั่นอัปเดต Windows และฐานข้อมูลไวรัสอย่างสม่ำเสมอ
- หลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่น่าเชื่อถือ
- อย่าเปิดลิงก์หรือไฟล์แนบจากอีเมลที่ไม่รู้จัก
- ใช้รหัสผ่านที่ปลอดภัยและเปิดใช้งานการยืนยันตัวตนแบบสองขั้นตอน

เมื่อใดควรขอความช่วยเหลือ

หากพบว่าเครื่องทำงานผิดปกติ เช่น เปิดโปรแกรมช้า มีหน้าต่างแปลก ๆ ปรากฏขึ้น หรือ Microsoft Defender ไม่สามารถลบภัยคุกคามได้ ควรติดต่อฝ่าย IT หรือผู้เชี่ยวชาญเพื่อขอความช่วยเหลือเพิ่มเติม

คู่มือการถอนการติดตั้งโปรแกรมที่ไม่จำเป็น

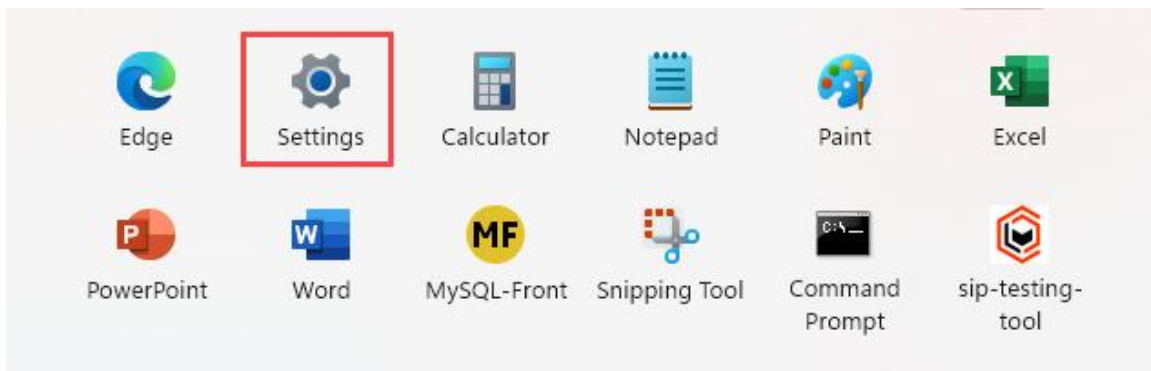
การถอนการติดตั้งโปรแกรมที่ไม่จำเป็นเป็นหนึ่งในวิธีที่ช่วยให้เครื่องคอมพิวเตอร์ทำงานได้เร็วขึ้น ลดการใช้ทรัพยากรระบบ และเพิ่มพื้นที่ว่างในฮาร์ดดิสก์ โดยเฉพาะในระบบ Windows 11 ผู้ใช้สามารถดำเนินการได้ง่าย ๆ ผ่านเมนูการตั้งค่า

ประโยชน์ของการลบโปรแกรมที่ไม่จำเป็น

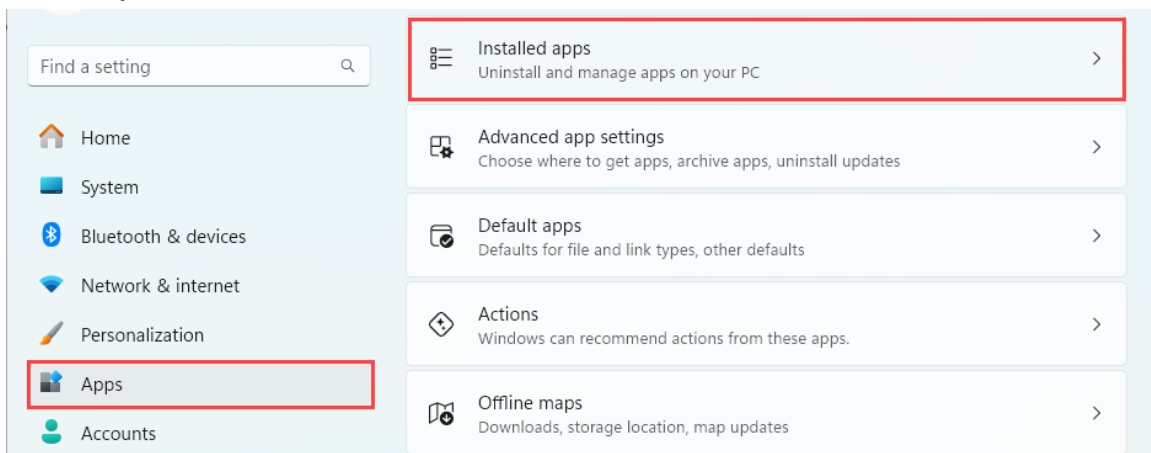
- เพิ่มพื้นที่ว่างในฮาร์ดดิสก์
- ลดการใช้หน่วยความจำและทรัพยากรระบบ
- ลดความเสี่ยงจากโปรแกรมที่อาจมีมัลแวร์หรือช่องโหว่
- ทำให้ระบบเริ่มต้นและทำงานได้เร็วขึ้น

ขั้นตอนการถอนการติดตั้งโปรแกรมผ่าน Settings

1. คลิกขวาที่ปุ่ม Start แล้วเลือก 'Settings' (การตั้งค่า)

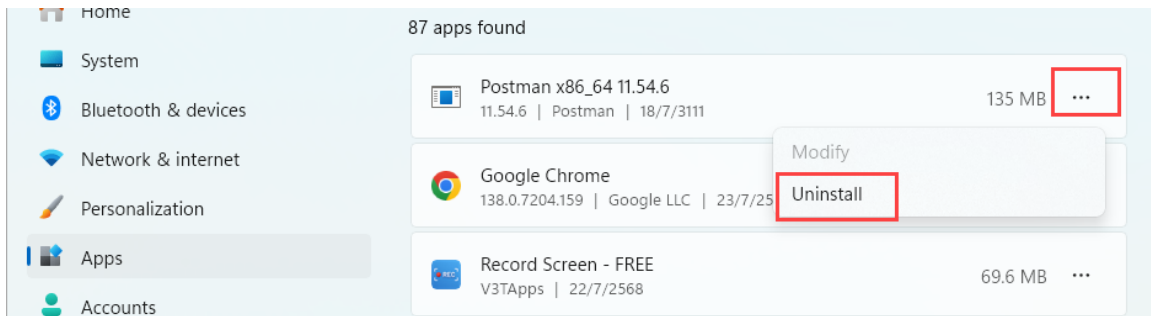


2. ไปที่เมนู 'Apps' แล้วเลือก 'Installed apps' หรือ 'Apps & features'

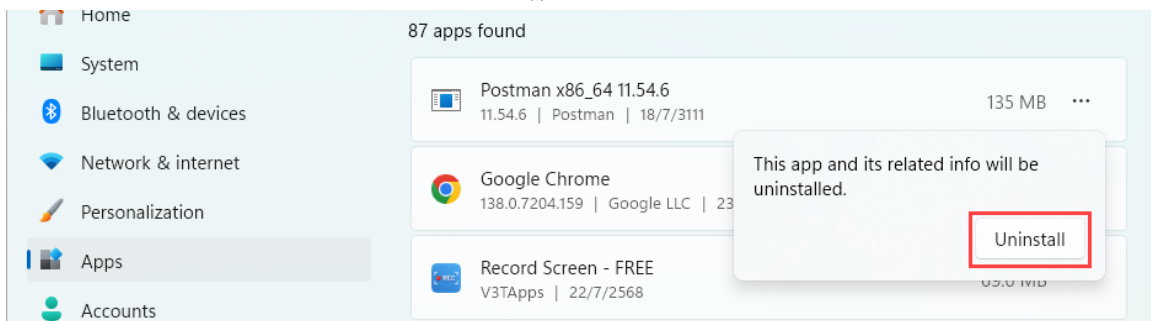


3. ค้นหาโปรแกรมที่ต้องการลบจากรายการ

4. คลิกที่ปุ่มสามจุด (...) ข้างชื่อโปรแกรม แล้วเลือก 'Uninstall'



5. ยืนยันการลบโปรแกรมตามคำแนะนำที่ปรากฏบนหน้าจอ



เคล็ดลับในการเลือกโปรแกรมที่ควรลบ

- โปรแกรมที่คุณไม่เคยใช้งานหรือไม่รู้จัก
- โปรแกรมทดลอง (Trial) ที่หมดอายุแล้ว
- โปรแกรมที่ติดตั้งมาพร้อมกับเครื่อง (Bloatware)
- โปรแกรมที่มีขนาดใหญ่แต่ไม่จำเป็น
- โปรแกรมที่มีชื่อซ้ำซ้อนหรือดูไม่น่าเชื่อถือ

ข้อควรระวัง

หลีกเลี่ยงการลบโปรแกรมที่เกี่ยวข้องกับระบบหรือไดรเวอร์ของอุปกรณ์ เช่น โปรแกรมจาก Microsoft, Intel, AMD, NVIDIA เว้นแต่คุณแน่ใจว่าไม่จำเป็นต่อการทำงานของเครื่อง

การจัดการ Startup Programs

การจัดการโปรแกรมที่เปิดอัตโนมัติเมื่อเริ่มต้นระบบ (Startup Programs)

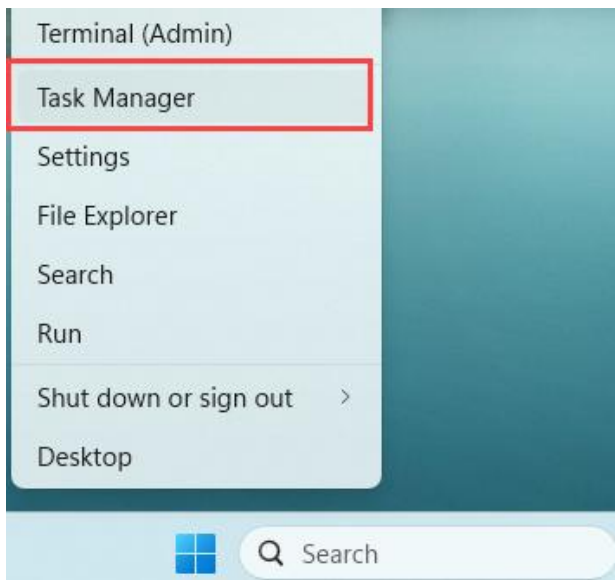
เป็นหนึ่งในวิธีที่ช่วยให้เครื่องคอมพิวเตอร์ทำงานได้เร็วขึ้น โดยเฉพาะในช่วงที่เปิดเครื่องใหม่

โปรแกรมบางตัวอาจไม่จำเป็นต้องเปิดทุกครั้งที่เริ่มต้นระบบ

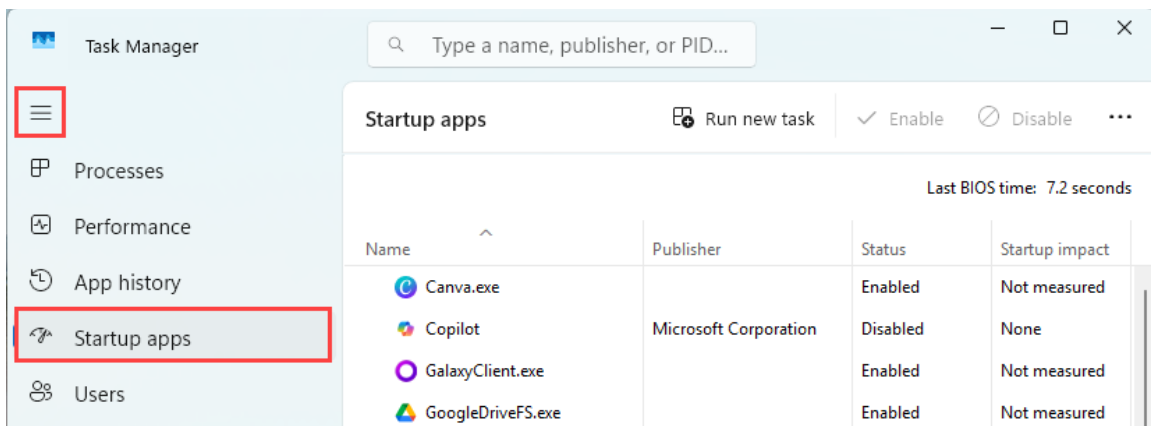
การปิดการทำงานของโปรแกรมเหล่านี้จะช่วยลดการใช้ทรัพยากรและเพิ่มประสิทธิภาพของเครื่องได้

วิธีการปิด Startup Programs ผ่าน Task Manager

1. คลิกขวาที่แถบ Taskbar แล้วเลือก 'Task Manager' หรือกดปุ่ม Ctrl + Shift + Esc เพื่อเปิด Task Manager

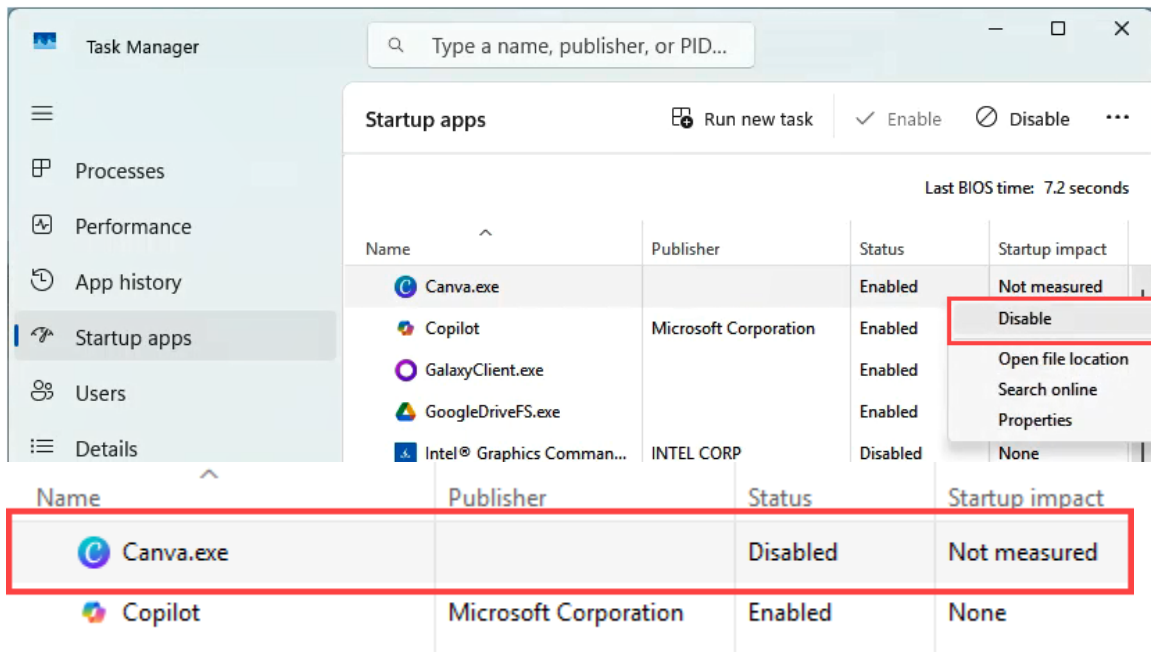


2. คลิกที่แท็บ 'Startup'



3. จะเห็นรายการโปรแกรมที่เปิดอัตโนมัติเมื่อเริ่มต้นระบบ

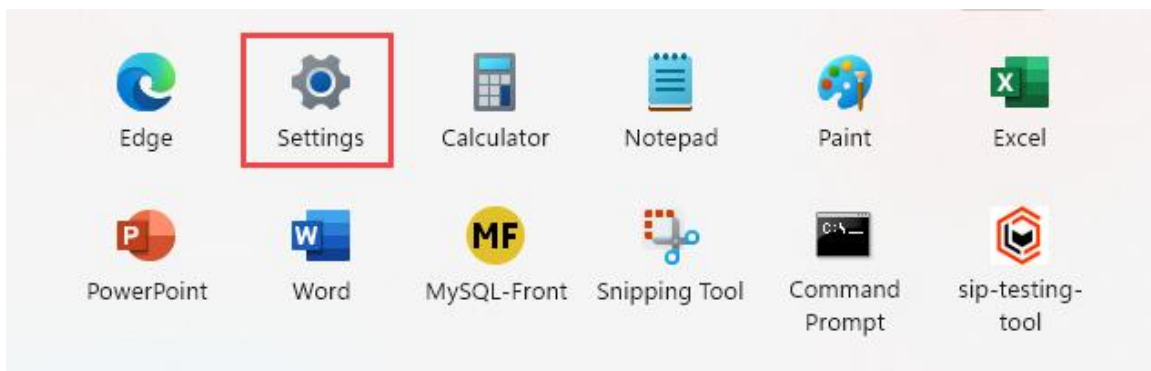
4. คลิกขวาที่โปรแกรมที่ไม่ต้องการให้เปิดอัตโนมัติ แล้วเลือก 'Disable'



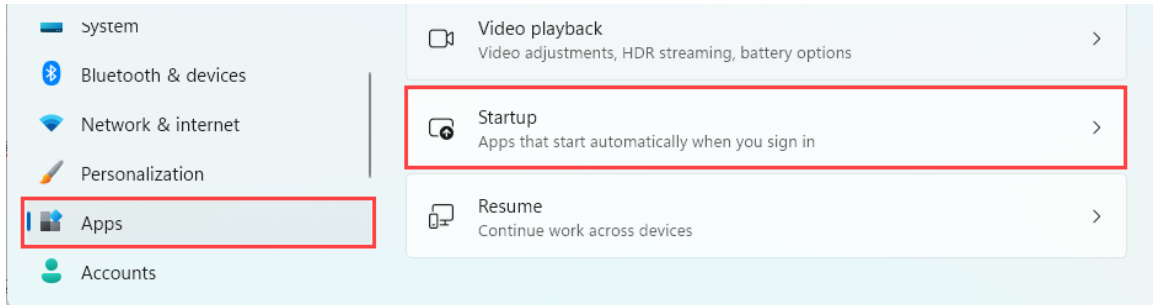
5. ปิดหน้าต่าง Task Manager

วิธีการปิด Startup Programs ผ่าน Settings

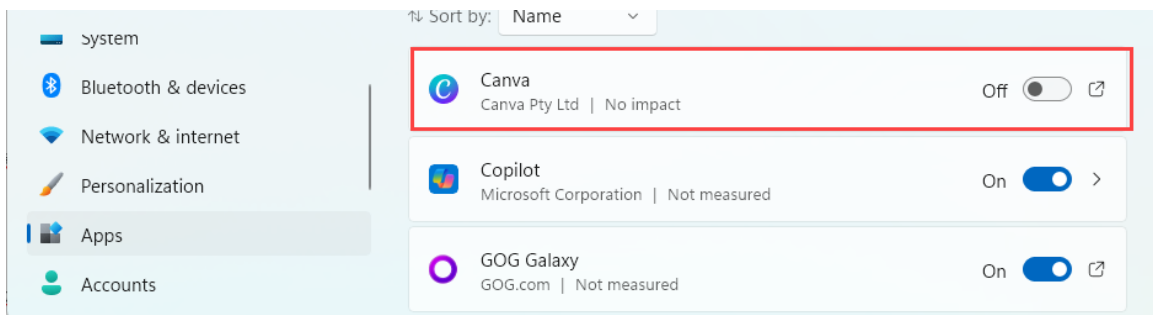
1. คลิกที่ปุ่ม Start แล้วเลือก 'Settings'



2. ไปที่เมนู 'Apps' แล้วเลือก 'Startup'



3. จะเห็นรายการโปรแกรมที่สามารถเปิด/ปิดการทำงานเมื่อเริ่มต้นระบบ



4. ปิดสวิตช์ของโปรแกรมที่ไม่ต้องการให้เปิดอัตโนมัติ

ประโยชน์ของการจัดการ Startup Programs

- ลดเวลาในการบูตเครื่อง
- ลดการใช้หน่วยความจำ (RAM) และ CPU
- เพิ่มความเร็วในการใช้งานโดยรวม
- ลดความเสี่ยงจากโปรแกรมที่อาจเป็นมัลแวร์หรือไม่จำเป็น

เคล็ดลับในการเลือกโปรแกรมที่ควรปิด

- ปิดโปรแกรมที่คุณไม่ใช้งานบ่อย เช่น โปรแกรมแชทหรือซอฟต์แวร์ที่ไม่จำเป็น
- ควรเปิดไว้เฉพาะโปรแกรมที่เกี่ยวข้องกับระบบหรือความปลอดภัย เช่น Antivirus
- หากไม่แน่ใจว่าโปรแกรมนั้นคืออะไร ให้ค้นหาข้อมูลก่อนปิดการทำงาน
- หลีกเลี่ยงการปิดโปรแกรมของผู้ผลิตฮาร์ดแวร์ เช่น ไดรเวอร์เสียงหรือกราฟิก

การตรวจสอบสุขภาพของฮาร์ดดิสก์และ SSD

การตรวจสอบสุขภาพของฮาร์ดดิสก์และ SSD เป็นสิ่งสำคัญในการดูแลรักษาเครื่องคอมพิวเตอร์

เพื่อป้องกันข้อมูลสูญหายและเพิ่มประสิทธิภาพการทำงานของระบบ Windows 11

เอกสารนี้จะแนะนำวิธีการตรวจสอบสุขภาพของดิสก์ด้วยเครื่องมือในระบบและคำแนะนำเพิ่มเติมสำหรับผู้ทั่วไป

สัญญาณที่บ่งบอกว่าดิสก์อาจมีปัญหา

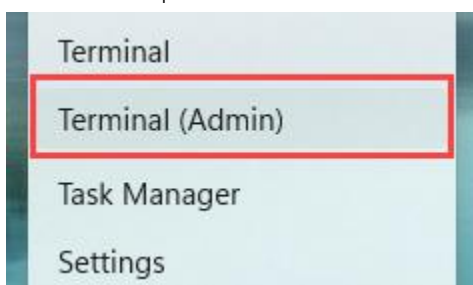
- เครื่องทำงานช้าลงอย่างผิดปกติ
- ไฟล์เปิดไม่ได้หรือเสียหาย
- ระบบค้างหรือเกิด Blue Screen บ่อย
- มีเสียงผิดปกติจากฮาร์ดดิสก์ (เฉพาะ HDD)
- Windows แจ้งเตือนเกี่ยวกับดิสก์

ประโยชน์ของการตรวจสอบสุขภาพดิสก์

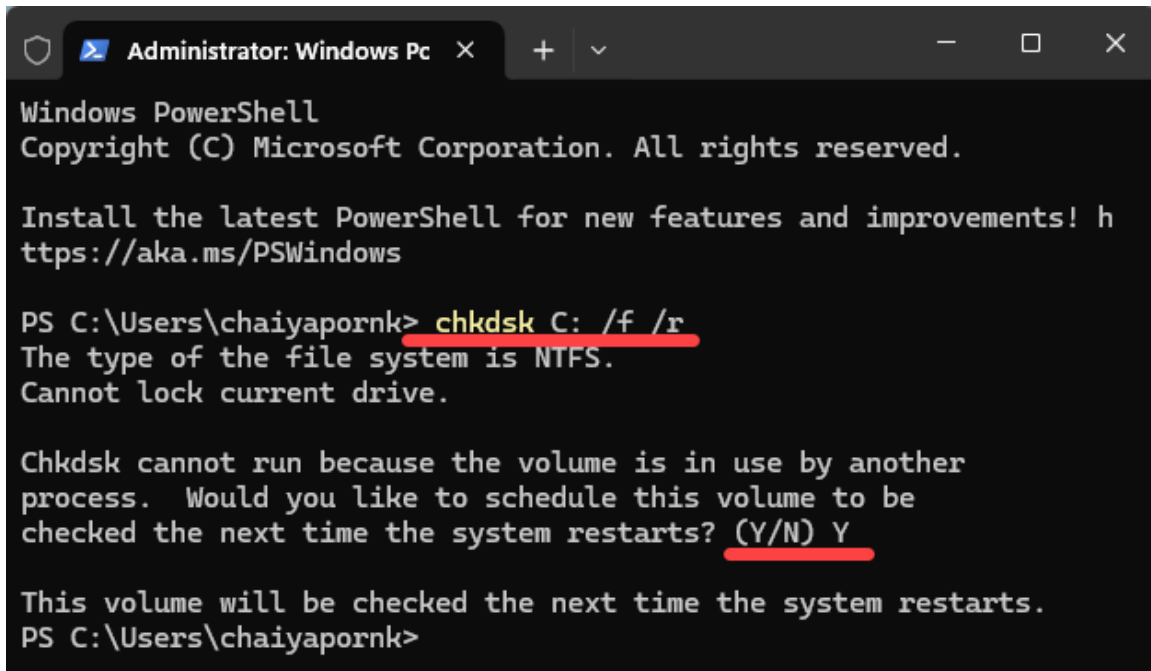
- ป้องกันข้อมูลสูญหาย
- เพิ่มความเร็วและประสิทธิภาพของระบบ
- ตรวจพบปัญหาได้ก่อนที่จะเกิดความเสียหายรุนแรง
- ยืดอายุการใช้งานของฮาร์ดดิสก์และ SSD

วิธีตรวจสอบสุขภาพดิสก์ด้วย CHKDSK

1. คลิกขวาที่ปุ่ม Start แล้วเลือก 'Windows Terminal (Admin)'



2. พิมพ์คำสั่ง: `chkdsk C: /f /r` แล้วกด Enter



```
Administrator: Windows Pc
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\chaiyapornk> chkdsk C: /f /r
The type of the file system is NTFS.
Cannot lock current drive.

Chkdsk cannot run because the volume is in use by another
process. Would you like to schedule this volume to be
checked the next time the system restarts? (Y/N) Y

This volume will be checked the next time the system restarts.
PS C:\Users\chaiyapornk>
```

3. หากมีการใช้งานไดรฟ์อยู่ ระบบจะขอให้รีสตาร์ทเครื่องเพื่อดำเนินการตรวจสอบ

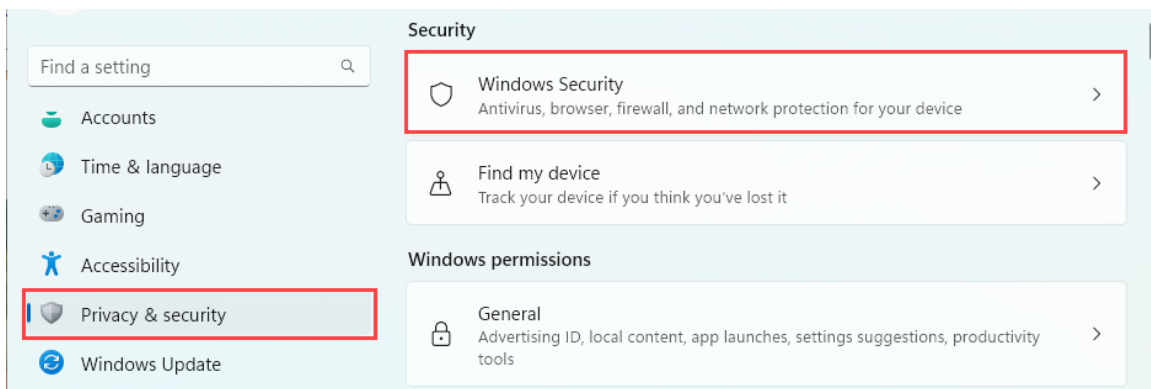
4. หลังรีสตาร์ท ระบบจะเริ่มตรวจสอบและซ่อมแซมดิสก์โดยอัตโนมัติ

การใช้ Windows Security ตรวจสอบ SSD

Windows Security ไม่มีฟีเจอร์ตรวจสอบสุขภาพ SSD โดยตรง

แต่สามารถตรวจสอบปัญหาที่เกิดจากมัลแวร์หรือไวรัสที่ส่งผลต่อดิสก์ได้:

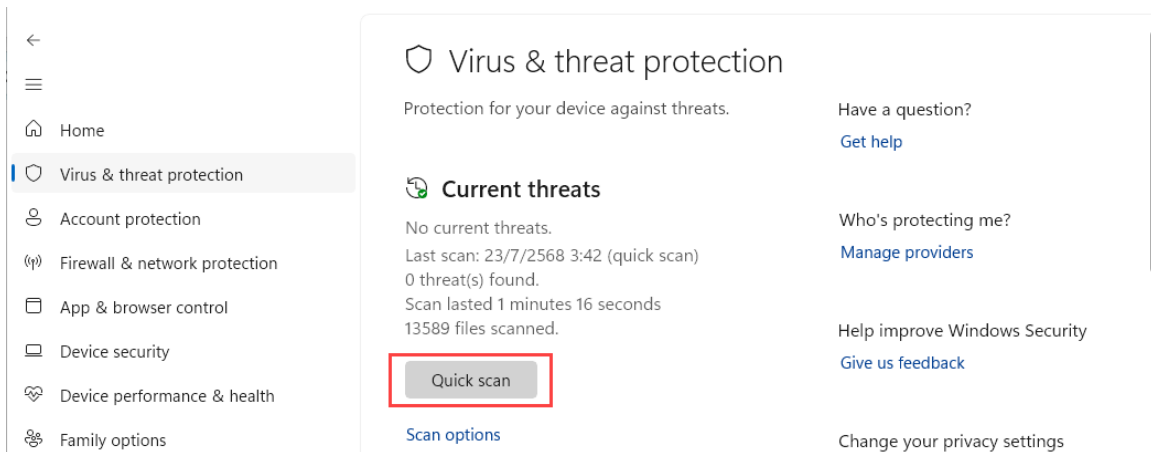
1. เปิด Settings > Privacy & Security > Windows Security



2. คลิก 'Virus & threat protection'



3. เลือก 'Quick scan' หรือ 'Full scan' เพื่อสแกนระบบ



การใช้แอปของผู้ผลิต SSD

ผู้ผลิต SSD หลายรายมีโปรแกรมตรวจสอบสุขภาพของ SSD เช่น:

- Samsung: Samsung Magician
- Kingston: Kingston SSD Manager
- Crucial: Crucial Storage Executive

โปรแกรมเหล่านี้สามารถแสดงสถานะ SMART, อุณหภูมิ, อายุการใช้งาน และการอัปเดตเฟิร์มแวร์

เคล็ดลับในการดูแลรักษาดีสก์

- หลีกเลี่ยงการปิดเครื่องแบบไม่ถูกต้อง
- อย่าปล่อยให้พื้นที่เก็บข้อมูลเต็มเกินไป
- สำรองข้อมูลเป็นประจำ
- ใช้โปรแกรม Disk Cleanup เพื่อลบไฟล์ขยะ
- ตรวจสอบสุขภาพดีสก์ทุก 1-2 เดือน

การสำรองข้อมูล

บทนำ

การสำรองข้อมูลและการกู้คืนระบบเป็นสิ่งสำคัญในการดูแลรักษาเครื่องคอมพิวเตอร์ เพื่อป้องกันการสูญหายของข้อมูลจากความผิดพลาดของระบบหรือการโจมตีจากมัลแวร์ Windows 11 มีเครื่องมือในตัวที่ช่วยให้ผู้ใช้สามารถสำรองข้อมูลและกู้คืนระบบได้อย่างง่ายดาย

ประโยชน์ของการสำรองข้อมูลเป็นประจำ

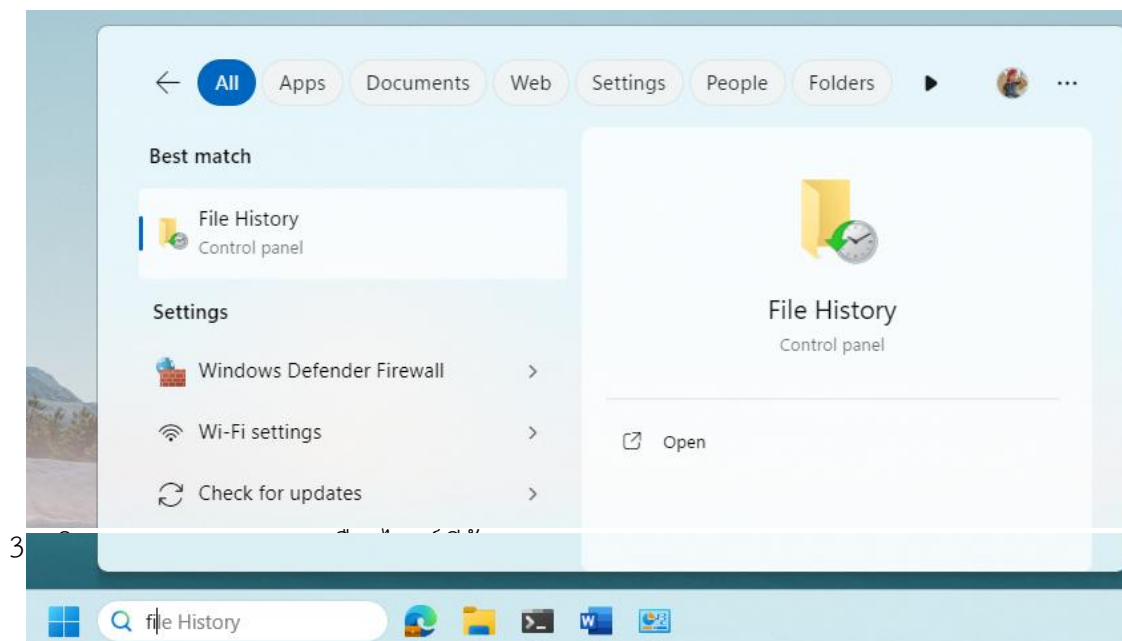
- ป้องกันการสูญหายของไฟล์สำคัญ
- สามารถย้อนกลับไปยังสถานะก่อนเกิดปัญหา
- ลดเวลาในการแก้ไขปัญหาเมื่อระบบมีข้อผิดพลาด
- เพิ่มความมั่นใจในการใช้งานเครื่องคอมพิวเตอร์

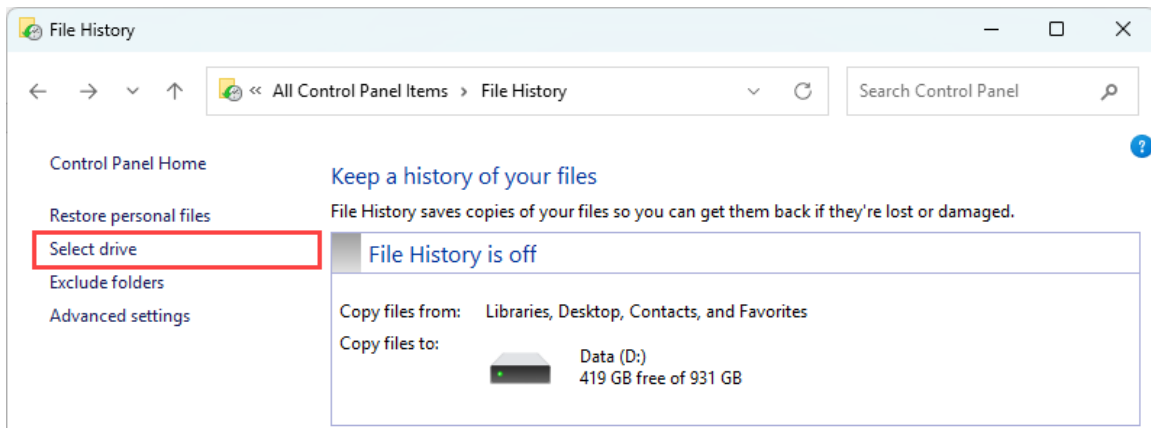
การใช้งาน File History เพื่อสำรองข้อมูล

File History เป็นฟีเจอร์ที่ช่วยสำรองไฟล์ส่วนตัว เช่น เอกสาร รูปภาพ และวิดีโอ โดยสามารถเรียกคืนไฟล์เวอร์ชันก่อนหน้าได้

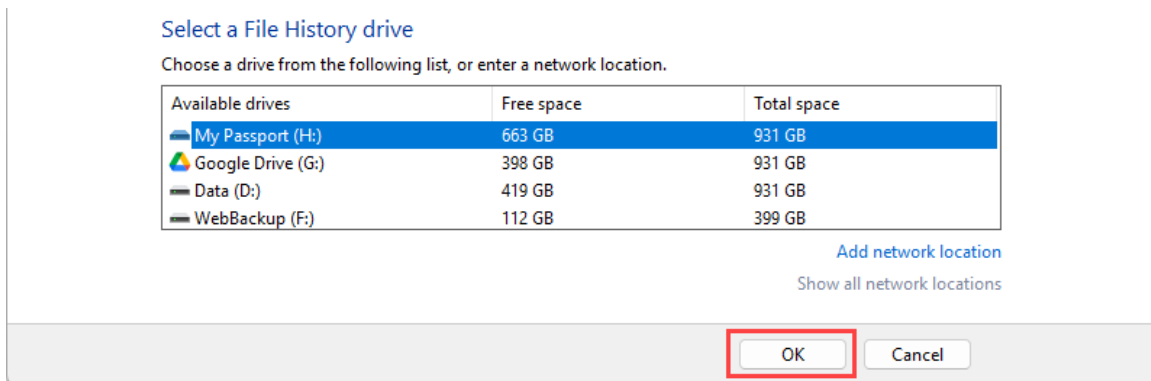
ขั้นตอนการเปิดใช้งาน File History:

1. เชื่อมต่อ External Drive หรือ Network Location สำหรับเก็บข้อมูลสำรอง
2. คลิกปุ่ม Start แล้วพิมพ์ 'File History' จากนั้นคลิกที่โปรแกรมที่แสดงขึ้นมา

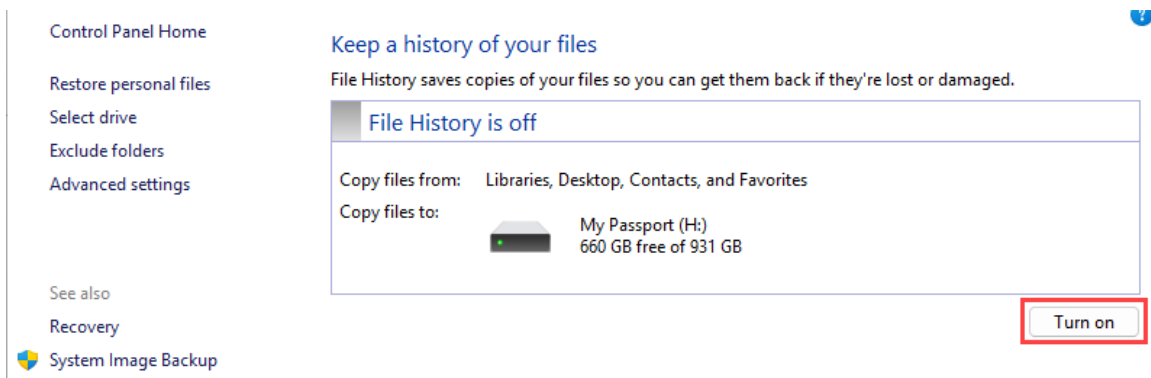




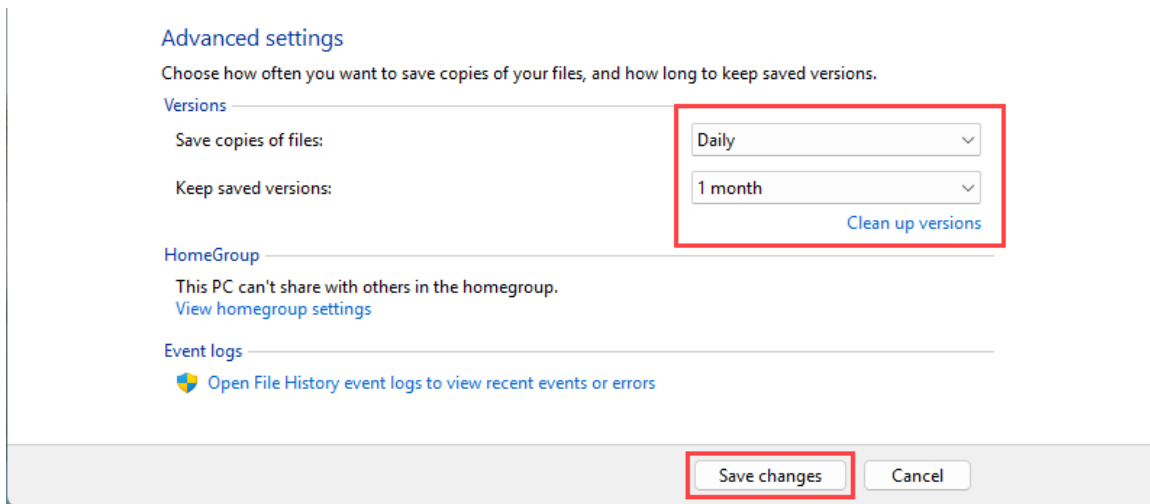
เลือกไดรฟ์ที่ต้องการ และ คลิก "OK"



4. เปิดใช้งาน "Automatically back up my files"



5. คลิก "Advanced settings" เพื่อกำหนดโฟลเดอร์ที่ต้องการสำรองและระยะเวลาในการเก็บข้อมูล



เคล็ดลับเพิ่มเติม

- ควรสำรองข้อมูลอย่างน้อยสัปดาห์ละครั้ง
- ใช้ External Drive หรือ Cloud Storage เพื่อความปลอดภัย
- ตรวจสอบการทำงานของ File History เป็นระยะ

การสำรองข้อมูล ด้วย OneDrive

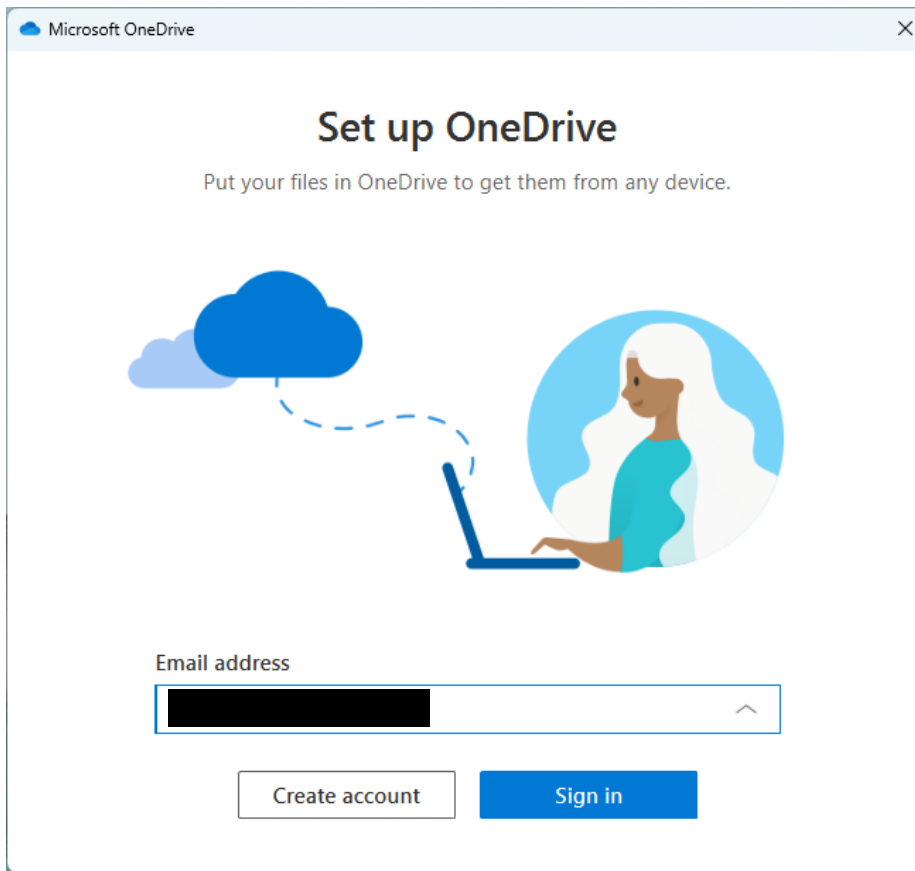
ขั้นตอนการตั้งค่า OneDrive เพื่อสำรองข้อมูลอัตโนมัติ

1. เปิดใช้งาน OneDrive

- ตรวจสอบว่า OneDrive เปิดอยู่หรือไม่ โดยดูที่มุมล่างขวาของหน้าจอ (ไอคอนรูปเมฆ)

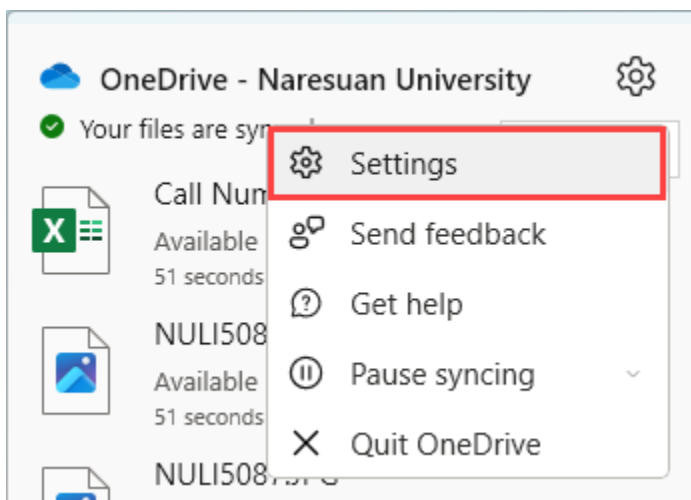


- หากไม่มี ให้ดาวน์โหลดจากเว็บไซต์ Microsoft <https://www.microsoft.com/en-us/microsoft-365/onedrive/download>
- ล็อกอินด้วยบัญชี Microsoft เช่น @outlook.com, @hotmail.com หรือบัญชีองค์กร

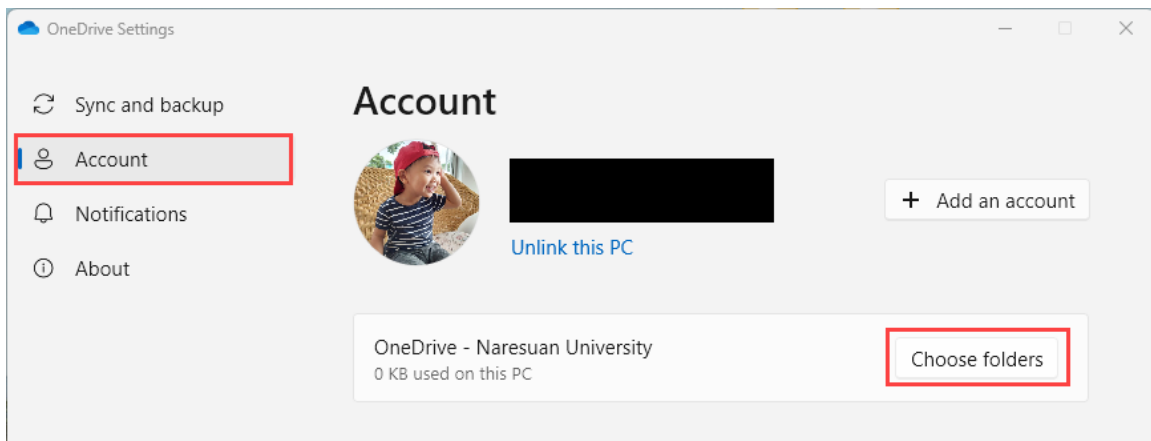


2. ตั้งค่าการสำรองข้อมูลอัตโนมัติ

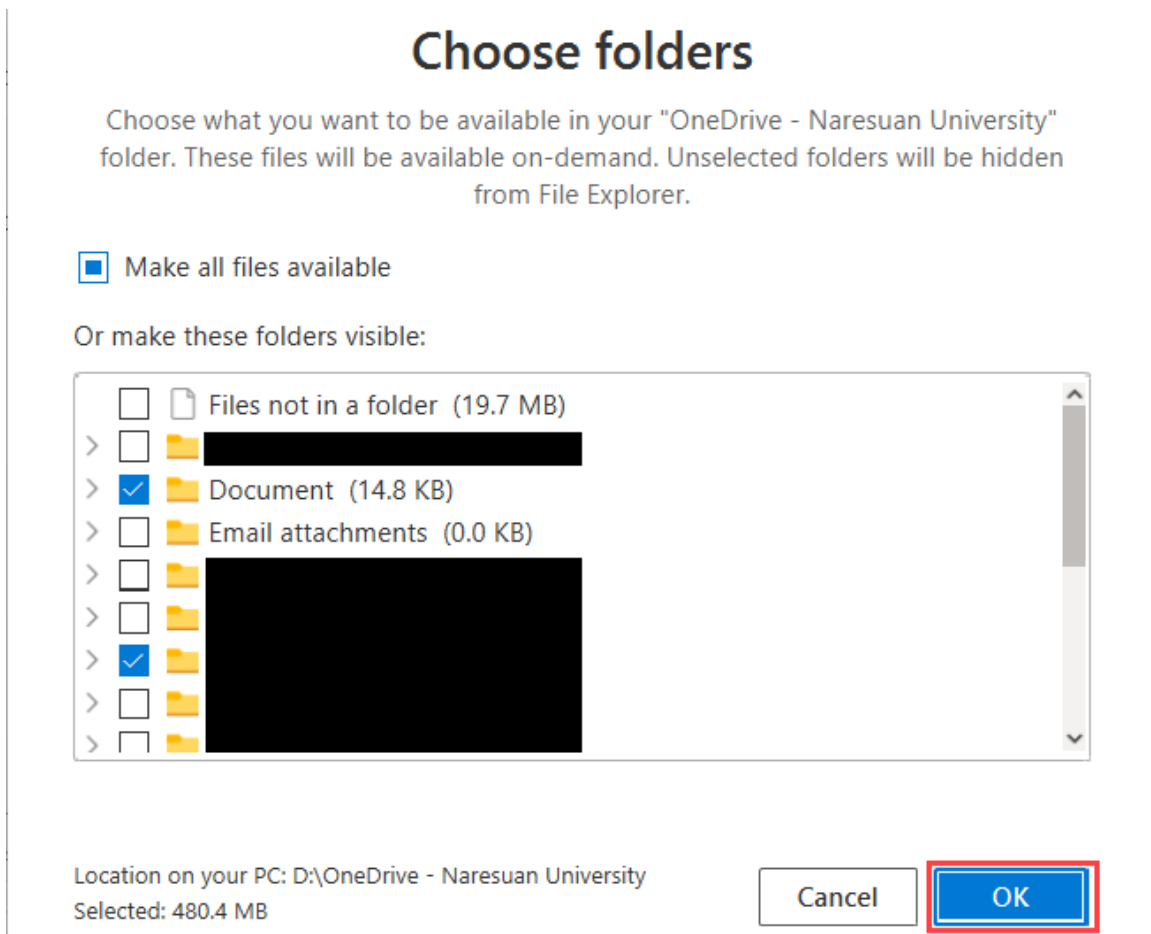
- คลิกขวาที่ไอคอน OneDrive > Settings > ไปที่แท็บ Backup



- กดปุ่ม Account > Choose folders



- เลือกโฟลเดอร์ที่ต้องการสำรองข้อมูล เช่น Desktop, Documents, Pictures
- กด Start Backup เพื่อเริ่มการสำรองข้อมูลอัตโนมัติ



วิธี Sync โฟลเดอร์อื่น ๆ เพิ่มเติม

- ลากไฟล์หรือโฟลเดอร์ที่ต้องการเข้าไปในโฟลเดอร์ OneDrive บนเครื่อง
- ไฟล์จะถูก Sync ขึ้น Cloud โดยอัตโนมัติ (มีไอคอนเมฆแสดงสถานะ)
- คลิกขวาที่ไฟล์ > OneDrive > เลือก:
 - Always keep on this device = เก็บไว้ทั้งในเครื่องและ Cloud
 - Free up space = เก็บไว้เฉพาะใน Cloud

การเรียกคืนไฟล์หรือเวอร์ชันก่อนหน้า

- ไปที่ onedrive.live.com > Recycle Bin เพื่อกู้คืนไฟล์ที่ลบ
- คลิกขวาที่ไฟล์ในโฟลเดอร์ OneDrive > Version History เพื่อย้อนกลับไปยังเวอร์ชันก่อนหน้า

การใช้งานบนอุปกรณ์อื่น

- มือถือ (iOS / Android): ดาวน์โหลดแอป OneDrive แล้วล็อกอินด้วยบัญชีเดียวกัน
- เว็บเบราว์เซอร์: เข้าผ่าน onedrive.live.com เพื่อดูไฟล์จากคอมพิวเตอร์อื่น

เคล็ดลับความปลอดภัย

- เปิดการยืนยันตัวตนแบบ 2 ขั้นตอน (2FA) ที่บัญชี Microsoft
- ใช้ Personal Vault สำหรับไฟล์สำคัญ เช่น สัญญา หรือเอกสารส่วนตัว
- อย่าลบไฟล์จาก OneDrive โดยไม่แน่ใจ เพราะอาจหายทั้งจากเครื่องและ Cloud

การทำความสะอาดภายนอกเครื่องคอมพิวเตอร์

บทนำ

การทำความสะอาดภายนอกเครื่องคอมพิวเตอร์เป็นสิ่งสำคัญที่ช่วยให้เครื่องทำงานได้ดี ลดความร้อนสะสม และยืดอายุการใช้งานของอุปกรณ์ต่าง ๆ เช่น แป้นพิมพ์ หน้าจอ พัดลมระบายความร้อน และเมาส์

เอกสารนี้จะอธิบายขั้นตอนการทำความสะอาดอย่างปลอดภัยและมีประสิทธิภาพสำหรับผู้ทั่วไป

ประโยชน์ของการทำความสะอาดอย่างสม่ำเสมอ

- ป้องกันฝุ่นสะสมที่อาจทำให้เครื่องร้อนเกินไป
- ลดความเสี่ยงจากการทำงานผิดปกติของแป้นพิมพ์หรือเมาส์
- ช่วยให้หน้าจอแสดงผลได้ชัดเจน
- ยืดอายุการใช้งานของอุปกรณ์

ข้อควรระวังในการทำความสะอาด

- ปิดเครื่องและถอดปลั๊กไฟก่อนทำความสะอาด
- ห้ามใช้น้ำหรือสารเคมีที่มีฤทธิ์กัดกร่อน
- ใช้ผ้าไมโครไฟเบอร์หรือผ้านุ่มที่ไม่เป็นขุย
- หลีกเลี่ยงการฉีดน้ำหรือสเปรย์โดยตรงลงบนอุปกรณ์

ขั้นตอนการทำความสะอาดอุปกรณ์แต่ละส่วน

1. แป้นพิมพ์ (Keyboard)

- พลิกคีย์บอร์ดคว่ำลงเบา ๆ เพื่อให้เศษฝุ่นหลุดออก
- ใช้แปรงขนนุ่มหรือเครื่องเป่าลมทำความสะอาดระหว่างปุ่ม
- ใช้ผ้าไมโครไฟเบอร์ชุบน้ำหมาด ๆ เช็ดพื้นผิว

2. หน้าจอ (Screen)

- ใช้ผ้าไมโครไฟเบอร์แห้งเช็ดฝุ่นเบา ๆ
- หากมีคราบ ให้ใช้ผ้าชุบน้ำกลั่นหมาด ๆ เช็ดเบา ๆ โดยไม่กดแรง

3. ช่องระบายอากาศ (Vents)

- ใช้เครื่องเป่าลมไล่ฝุ่นออกจากช่องระบายอากาศ
- หลีกเลี่ยงการใช้ผ้าหรือวัตถุแข็งแหย่เข้าไปในช่อง

4. เมาส์ (Mouse)

- ถอดสายหรือปิดการเชื่อมต่อก่อนทำความสะอาด
- ใช้ผ้าไมโครไฟเบอร์เช็ดพื้นผิวเมาส์
- ทำความสะอาดบริเวณเซ็นเซอร์ด้วยผ้าแห้ง

การตั้งค่าความปลอดภัยพื้นฐาน

การตั้งค่าความปลอดภัยพื้นฐานเป็นสิ่งสำคัญสำหรับผู้ทั่วไป

เพื่อป้องกันข้อมูลส่วนตัวและระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต Windows 11

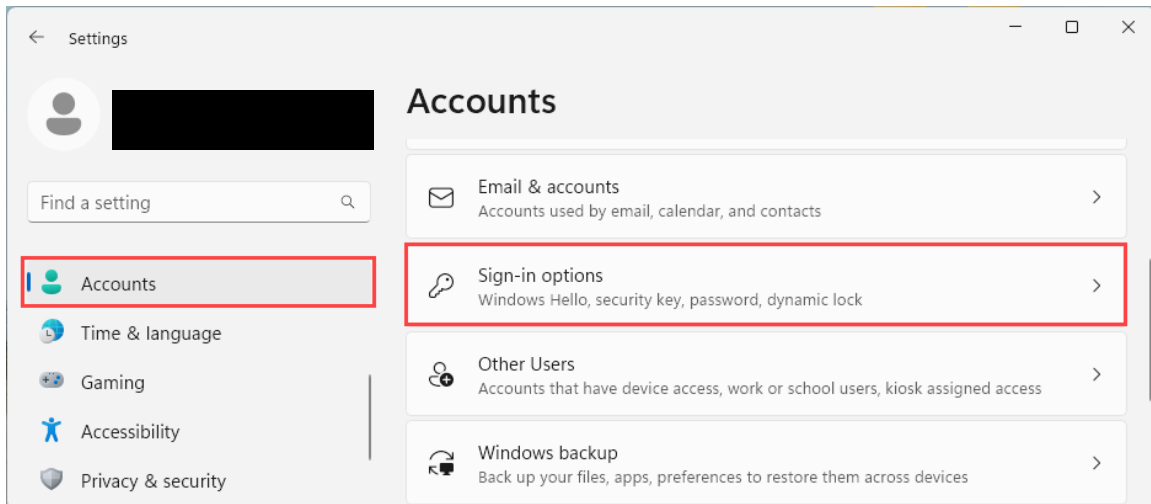
มีฟีเจอร์ด้านความปลอดภัยหลายอย่างที่สามารถตั้งค่าได้ง่ายและมีประสิทธิภาพ

การตั้งรหัสผ่านหรือ PIN

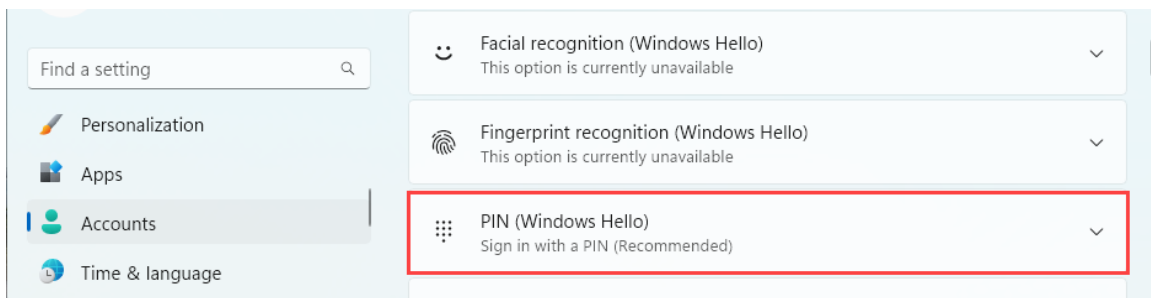
การตั้งรหัสผ่านหรือ PIN เป็นวิธีพื้นฐานในการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ของคุณ

ขั้นตอน:

14. ไปที่ Settings > Accounts > Sign-in options



15. เลือก 'PIN (Windows Hello)' หรือ 'Password'



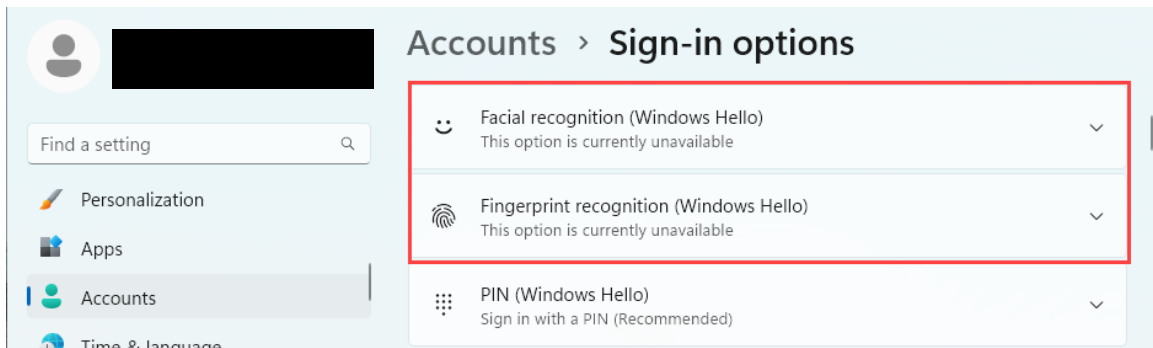
16. คลิก 'Set up' และทำตามขั้นตอนที่ปรากฏ

เคล็ดลับ: ใช้ PIN ที่ไม่ซ้ำกับรหัสผ่านอื่น และหลีกเลี่ยงการใช้วันเกิดหรือเลขง่าย ๆ

การเปิดใช้งาน Windows Hello

Windows Hello เป็นฟีเจอร์ที่ช่วยให้คุณเข้าสู่ระบบด้วยใบหน้า ลายนิ้วมือ หรือ PIN ได้อย่างปลอดภัย
ขั้นตอน:

1. ไปที่ Settings > Accounts > Sign-in options
2. เลือก 'Facial recognition' หรือ 'Fingerprint recognition'



3. คลิก 'Set up' และทำตามคำแนะนำ

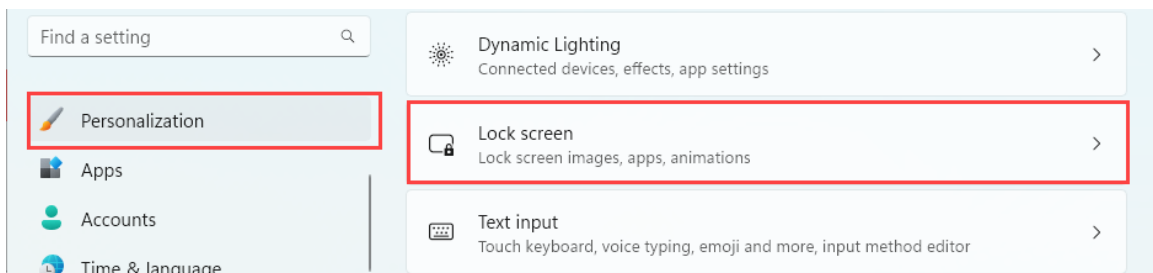
ประโยชน์: สะดวก รวดเร็ว และปลอดภัยกว่าการใช้รหัสผ่าน

การตั้งค่าการล็อกหน้าจออัตโนมัติ

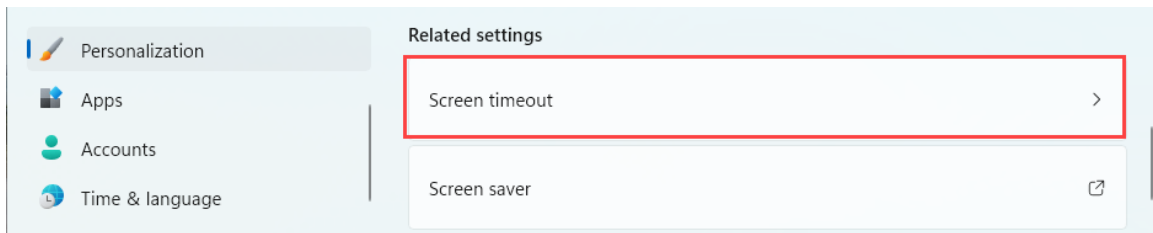
การล็อกหน้าจออัตโนมัติช่วยป้องกันการเข้าถึงเครื่องเมื่อคุณไม่ได้ใช้งาน

ขั้นตอน:

1. ไปที่ Settings > Personalization > Lock screen

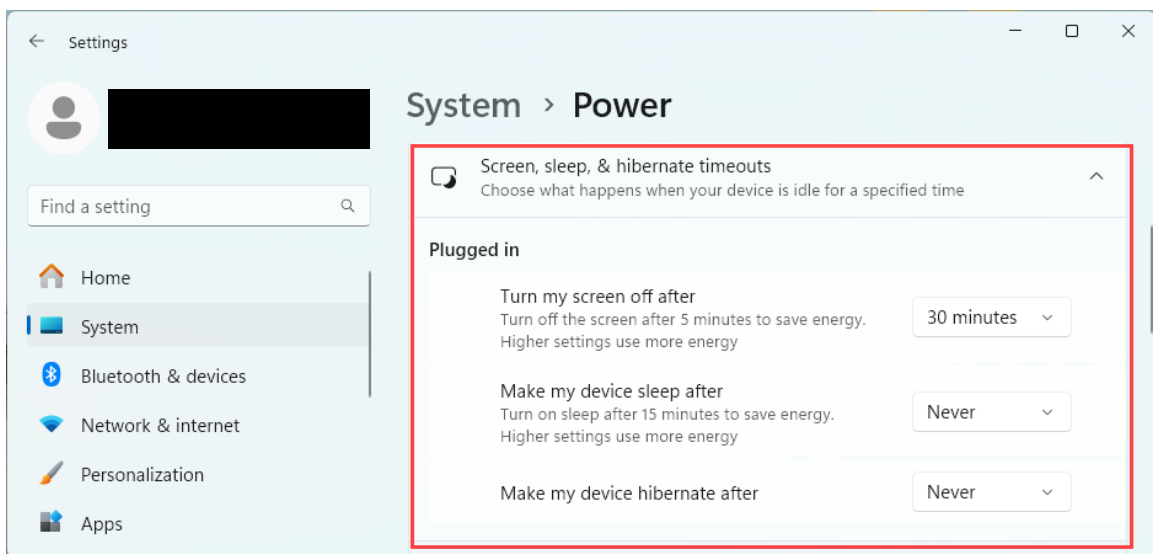


2. เลือก 'Screen timeout settings'



3. ตั้งเวลาให้หน้าจอล็อกโดยอัตโนมัติหลังไม่มีการใช้งาน

เคล็ดลับ: ตั้งเวลาให้เหมาะสม เช่น 5-10 นาที เพื่อความปลอดภัย

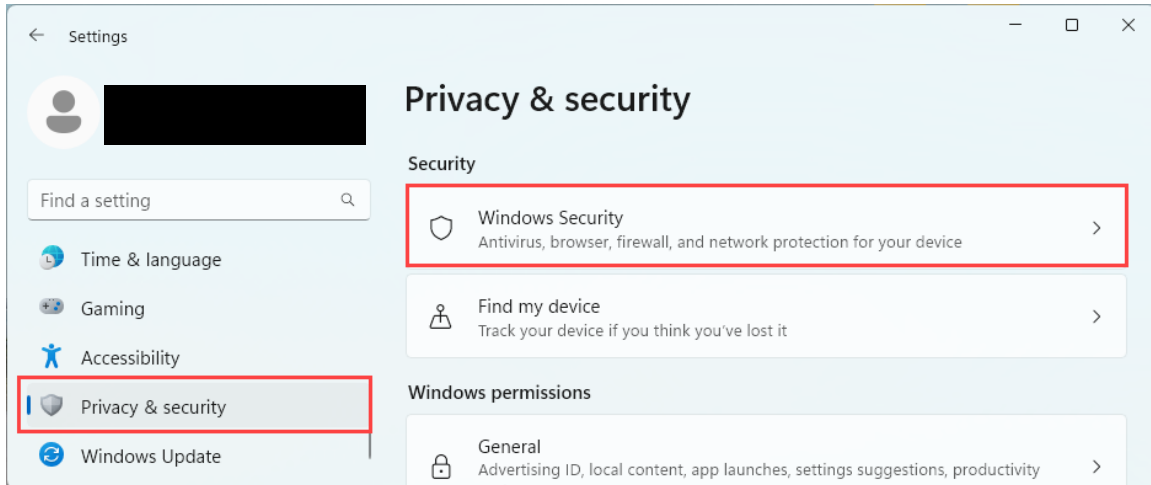


การใช้ฟีเจอร์ SmartScreen และ Firewall

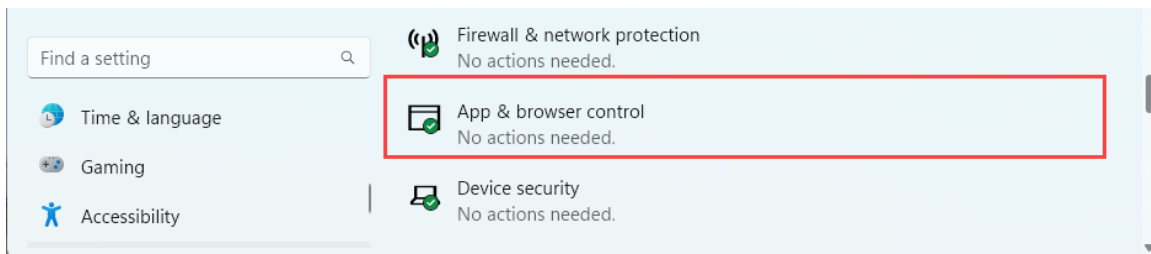
SmartScreen และ Firewall เป็นฟีเจอร์ที่ช่วยป้องกันมัลแวร์และการโจมตีจากเครือข่าย

ขั้นตอนเปิดใช้งาน SmartScreen:

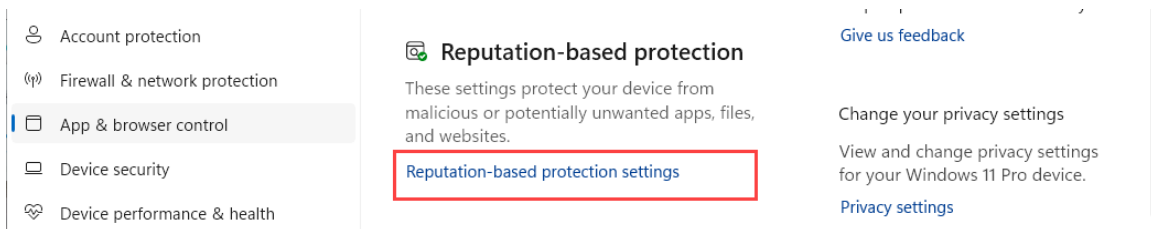
1. ไปที่ Settings > Privacy & security > Windows Security



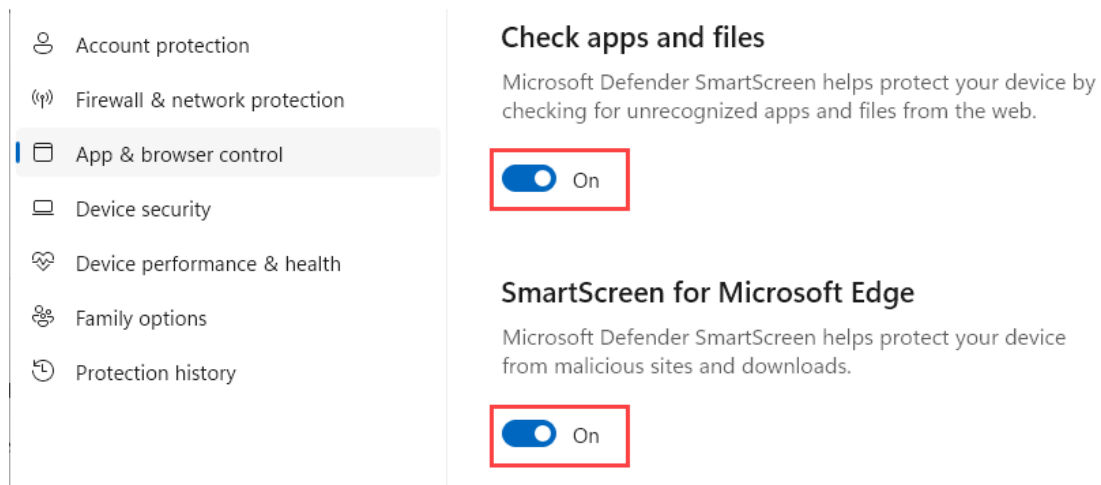
2. คลิก 'App & browser control'



3. คลิก 'Reputation-based protection settings'

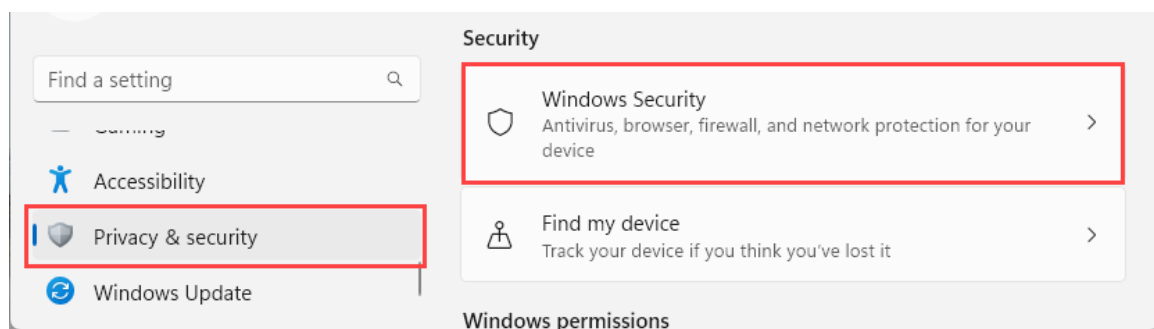


4. เปิดใช้งาน 'SmartScreen for Microsoft Edge' และ 'SmartScreen for apps'

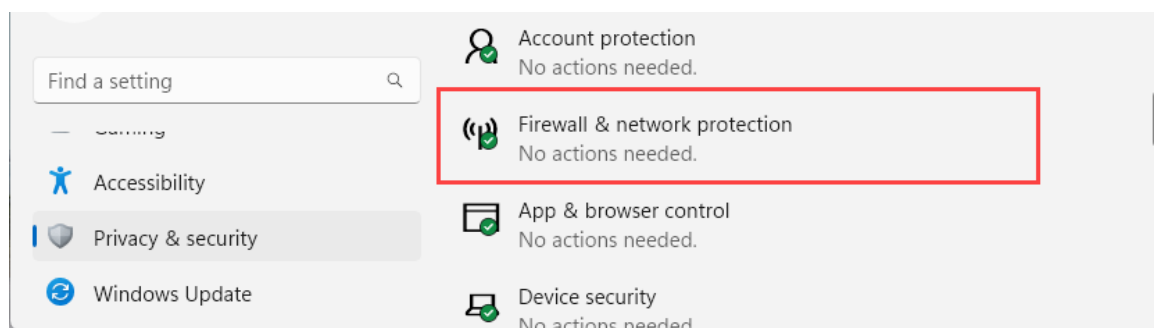


ขั้นตอนตรวจสอบ Firewall:

1. ไปที่ Settings > Privacy & security > Windows Security

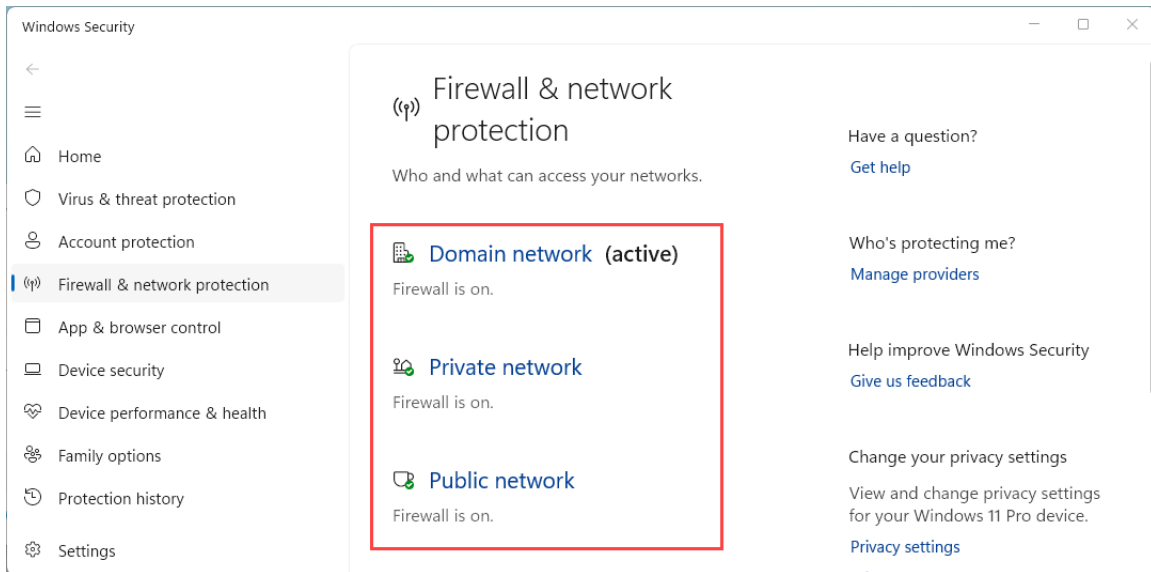


2. คลิก 'Firewall & network protection'



3. ตรวจสอบว่า Firewall เปิดอยู่ในทุกเครือข่าย

เคล็ดลับ: อย่าปิด Firewall เว้นแต่คุณมีระบบป้องกันอื่นที่เชื่อถือได้



อ้างอิง

Microsoft Copilot. (2025). *AI-assisted writing support*. Microsoft. <https://copilot.microsoft.com>