บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

โทร. ๐๗-๔๓๑๗-๑๔๖ เบอร์ภายใน ๑๑๖๐, ๑๑๖๒

ที่ อว ๐๖๕๕.๑๒/๔๐๑ **วันที่** ๑๘ เมษายน ๒๕๖๘

เรื่อง ประชาสัมพันธ์แนวทางการป้องกันการบุกรุกโจมตีสำหรับเครื่องคอมพิวเตอร์

เรียน หัวหน้าหน่วยงานในสังกัดมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ด้วยสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้มีการตรวจสอบระบบเฝ้าระวังความปลอดภัย (Firewall) ในช่วงต้นเดือนเมษายน ๒๕๖๘ ที่ผ่านมา พบว่าได้มีการบุกรุกโจมตีระบบเครือข่ายอินเทอร์เน็ตจากเส้นทางการสื่อสารภายในเครือข่ายของมหาวิทยาลัยโดยเครื่องคอมพิวเตอร์ ซึ่งส่งผลกระทบต่อการใช้งานอินเทอร์เน็ตของมหาวิทยาลัย ทำให้อินเทอร์เน็ตเกิดความล่าช้าและทำงานไม่เต็มประสิทธิภาพ นั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงขอส่งหนังสือมายังหน่วยงานของท่าน เพื่อประชาสัมพันธ์คู่มือขั้นตอนการเปิดใช้งาน Microsoft Defender Antivirus เพื่อเป็นแนวทางในการป้องกันการบุกรุกโจมตีดังกล่าวข้างต้น หากมีข้อสงสัยประการใดสามารถติดต่อสอบถามได้ที่ นายจักรพงศ์ สุขเพ็ง ตำแหน่งนักวิชาการคอมพิวเตอร์ โทร. ๐๘ ๗๒๙๔ ๑๓๒๗ รายละเอียดดังเอกสารที่แนบมาพร้อมหนังสือฉบับนี้

จึงเรียนมาเพื่อโปรดทราบ

(ผู้ช่วยศาสตราจารย์สิทธิโชค อุ่นแก้ว)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

เรียน คณบดี
เพื่อโปรดทราบ
สวส. ประชาสัมพันธ์คู่มือขั้นตอนการเปิดใช้งาน Micrisoft Defender Antivirus เพื่อเป็นแนวทางในการป้องกันการบุกรุกโจมตีสำหรับเครื่องคอมพิวเตอร์
เห็นควรมอบนายอภิวัชร์ ระวีสกุลวัฒน์ ปชส. แจ้งให้บุคลากรในสังกัดทุกคนทราบ

18 เม.ย. 68

๑๘ เม.ย. ๖๘

ทราบและมอบ

๒๒ เม.ย. ๖๘

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ขั้นตอนการเปิดใช้งาน

Microsoft Defender Antivirus

โปรแกรมป้องกันไวรัสและมัลแวร์

บนระบบปฏิบัติการWindows 10 และ Windows 11

สารบัญ

ความสำคัญของการป้องกันไวรัส

การป้องกันไวรัสเครื่องคอมพิวเตอร์ที่ใช้งานภายในมหาวิทยาลัย มีความจำเป็นอย่างยิ่ง โดยเฉพาะในยุคที่มีภัยคุกคามทางไซเบอร์มีความซับซ้อนและเกิดขึ้นได้ตลอดเวลา

1. **ปกป้องข้อมูลสำคัญของมหาวิทยาลัย**

   มหาวิทยาลัยมีข้อมูลสำคัญจำนวนมาก เช่น ข้อมูลนักศึกษา บุคลากร ผลงานวิจัย ระบบการเรียนการสอน ฯลฯ หากข้อมูลเหล่านี้รั่วไหล จะเกิดผลกระทบอย่างรุนแรง ทั้งในด้านชื่อเสียง และการดำเนินงาน

2. **ลดความเสี่ยงจากการโจมตีของแรนซัมแวร์ (Ransomware)**

   การโจมตีในลักษณะนี้สามารถเข้ารหัสไฟล์และเรียกค่าไถ่เพื่อให้สามารถเข้าถึงข้อมูลได้อีกครั้ง ส่งผลให้ระบบไม่สามารถใช้งานได้ชั่วคราว หรือถาวร

3. **สร้างความเชื่อมั่นให้กับองค์กร**

   นักศึกษา อาจารย์ และบุคลากร ต้องใช้ระบบไอทีของมหาวิทยาลัยอย่างต่อเนื่อง หากระบบมีการป้องกันที่ดี จะสร้างความมั่นใจในความปลอดภัยในการใช้งาน

4. **ลดภาระในการกู้คืนระบบและข้อมูล**

   หากไม่มีระบบป้องกันไวรัสหรือระบบสำรองข้อมูลที่ดี เมื่อถูกโจมตีอาจต้องใช้เวลานานในการกู้คืนระบบ และบางครั้งอาจกู้คืนไม่ได้เลย

5. **ส่งเสริมการใช้เทคโนโลยีอย่างปลอดภัย**

   การมีระบบป้องกันไวรัส ทำให้เกิดการตระหนักรู้เรื่อง Cybersecurity ในหมู่ผู้ใช้ และส่งเสริมพฤติกรรมการใช้งานเทคโนโลยีอย่างเหมาะสม

ภัยคุกคามทางไซเบอร์ส่วนใหญ่มักเกิดจากภายในองค์กร โดยเฉพาะจากอุปกรณ์ที่ใช้งานภายในระบบเครือข่าย ดังนั้นจึงจำเป็นต้องมีการป้องกันอย่างรัดกุม เช่น การติดตั้งและอัปเดตโปรแกรม Antivirus อย่างสม่ำเสมอ รวมถึงการใช้งานอินเทอร์เน็ตอย่างระมัดระวัง หลีกเลี่ยงการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย

Microsoft Defender Antivirus คืออะไร

Microsoft Defender Antivirus (ก่อนหน้านี้รู้จักในชื่อ Windows Defender) คือโปรแกรมป้องกันไวรัส (Antivirus) และมัลแวร์ (Malware) ที่พัฒนาโดยบริษัท Microsoft และติดตั้งมาพร้อมกับระบบปฏิบัติการ Windows 10 และ Windows 11 โดยไม่ต้องติดตั้งเพิ่ม

คุณสมบัติหลักของ Microsoft Defender Antivirus

1. ป้องกันไวรัสและมัลแวร์

- ตรวจจับและลบไวรัส, สปายแวร์, โทรจัน, แรนซัมแวร์ ฯลฯ ได้แบบเรียลไทม์

2. ทำงานอัตโนมัติ

- สแกนระบบเป็นระยะ ๆ และอัปเดตฐานข้อมูลไวรัสอัตโนมัติผ่าน Windows Update

3. สแกนตามคำสั่ง

- ผู้ใช้สามารถสแกนไฟล์หรือโฟลเดอร์แบบเฉพาะเจาะจงได้

4. Integration กับระบบ

- ทำงานร่วมกับ Windows Security Center ช่วยจัดการการตั้งค่าความปลอดภัยได้จากศูนย์กลาง

5. Cloud-delivered Protection

- ใช้ข้อมูลจากระบบคลาวด์ของ Microsoft เพื่อวิเคราะห์ภัยคุกคามได้เร็วและแม่นยำยิ่งขึ้น

6. การกักกันไฟล์อันตราย

- ไฟล์ต้องสงสัยจะถูกกักไว้ใน quarantine ก่อนจะลบหรือยอมรับ

จุดเด่นของ Microsoft Defender

📌 จุดเด่น :

- ฟรี ไม่ต้องเสียเงินเพิ่ม
- ประสิทธิภาพดีขึ้นมากในเวอร์ชันหลัง ๆ
- ทำงานเบาเครื่อง
- ไม่ขัดแย้งกับ Windows Updates หรือฟีเจอร์อื่น ๆ

❗ ข้อควรรู้

- ถ้าคุณติดตั้ง Antivirus อื่น (เช่น Avast, Bitdefender, Kaspersky ฯลฯ) Microsoft Defender จะปิดตัวเองโดยอัตโนมัติ
- เหมาะกับการใช้งานทั่วไป แต่ถ้าเป็นองค์กรที่มีข้อมูลสำคัญมาก อาจพิจารณาใช้โซลูชันความปลอดภัยขั้นสูงร่วมด้วย

Microsoft Defender Antivirus

📌 ข้อดี

ติดตั้งมาพร้อมกับ Windows : ไม่ต้องติดตั้งเพิ่มเติมและไม่มีค่าใช้จ่ายเพิ่มเติม

การป้องกันพื้นฐานที่ดี : ปรับปรุงอย่างต่อเนื่องและให้การป้องกันที่น่าเชื่อถือสำหรับผู้ใช้ทั่วไป

ไม่รบกวนการทำงาน : ทำงานเบื้องหลังโดยไม่ทำให้ระบบช้าลงอย่างมีนัยสำคัญ

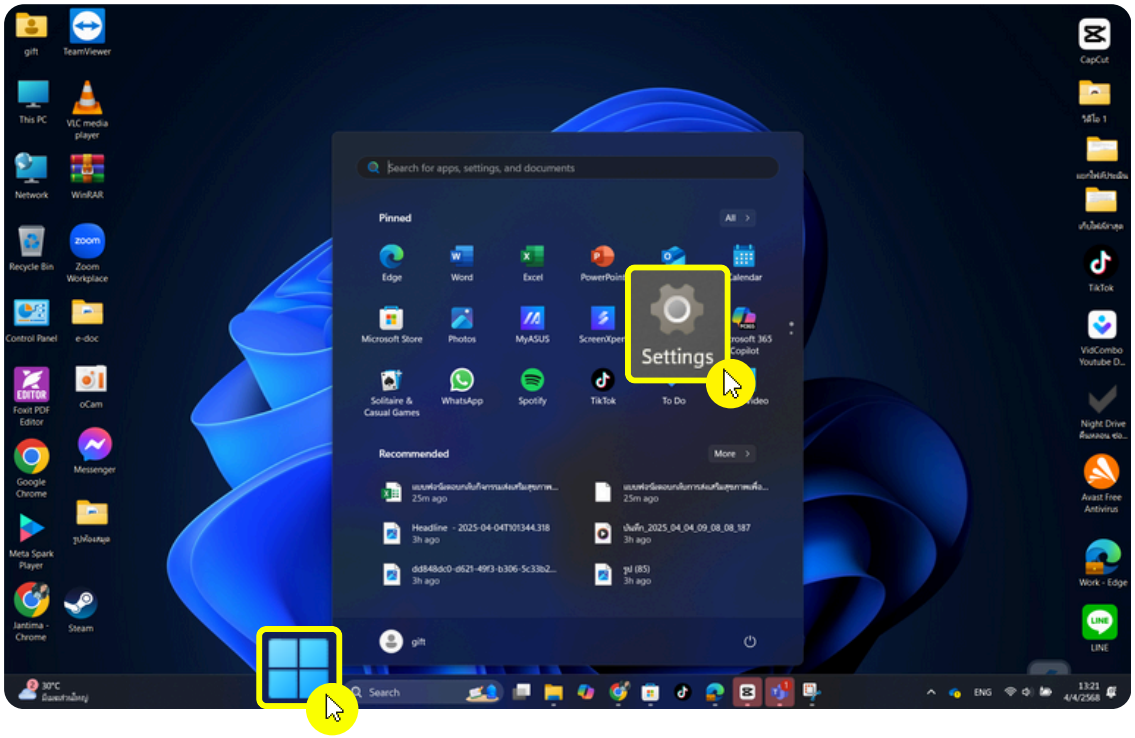
📌 ข้อจำกัด

ฟีเจอร์เพิ่มเติมจำกัด : ไม่มีฟีเจอร์ขั้นสูงเช่น VPN, ตัวจัดการรหัสผ่าน หรือการป้องกันการขโมยข้อมูลส่วนบุคคล

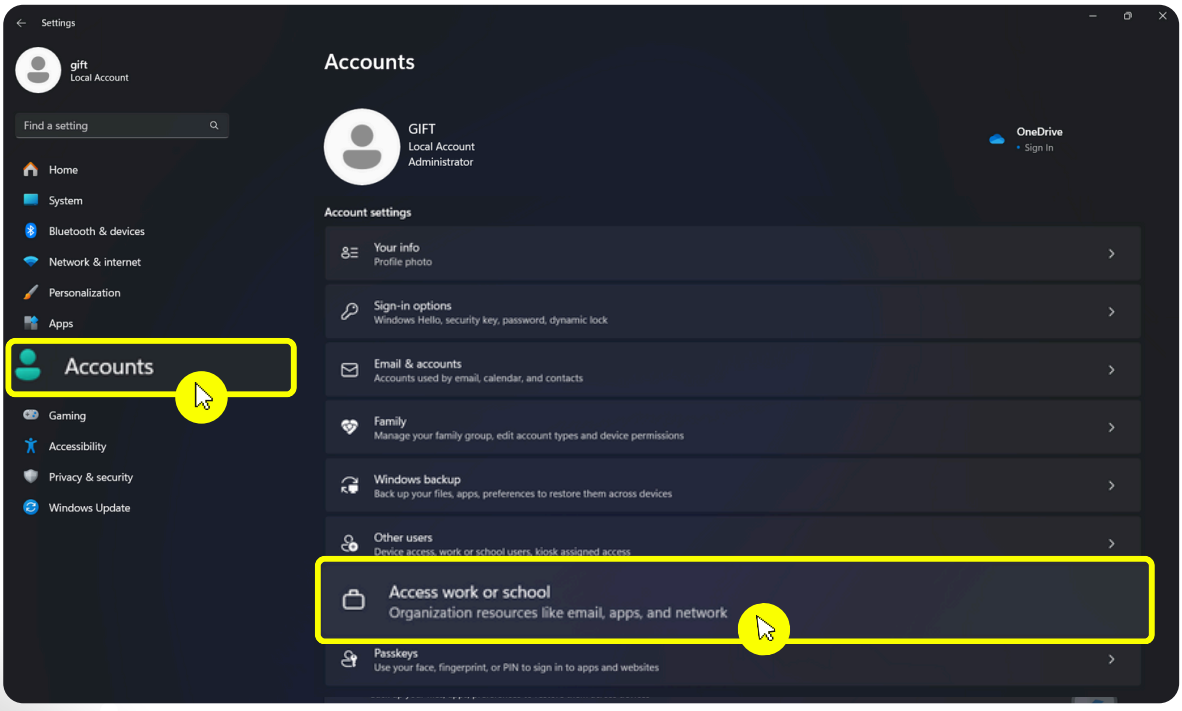
การป้องกันมัลแวร์ขั้นสูง : อาจไม่เพียงพอสำหรับผู้ใช้ที่ต้องการการป้องกันระดับสูงหรือสำหรับองค์กร

ขั้นตอนการเปิดใช้งาน

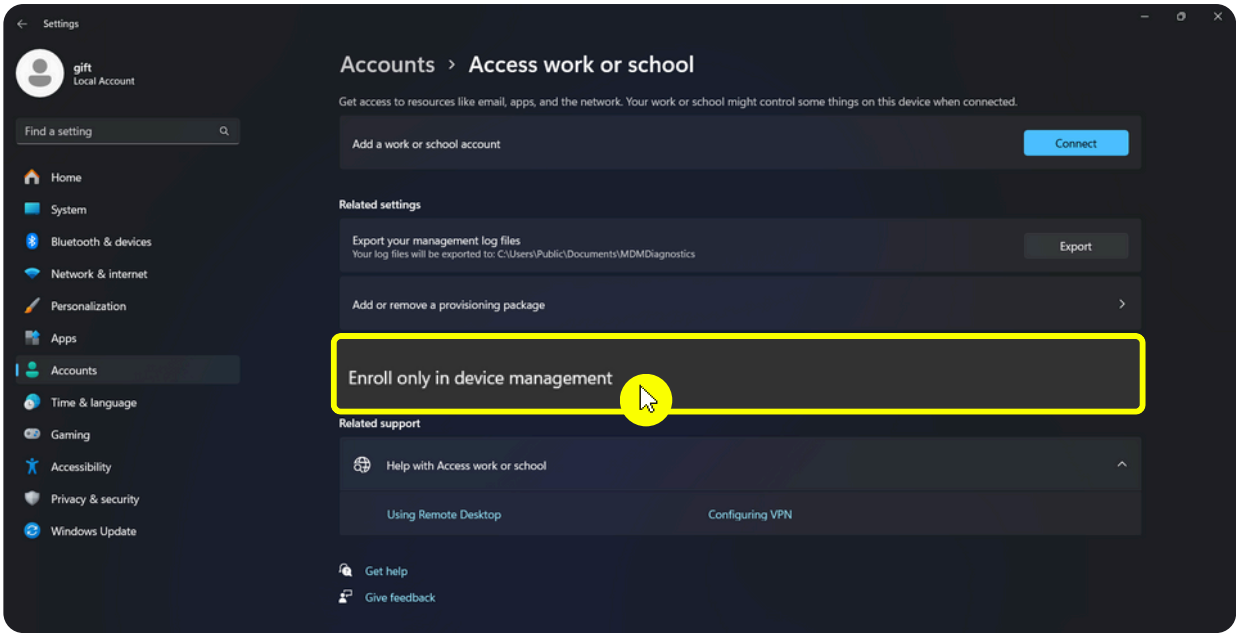
1.กดปุ่ม Start  เลือก Setting 



2. เลือกเมนู Accounts เลือก Access work or school



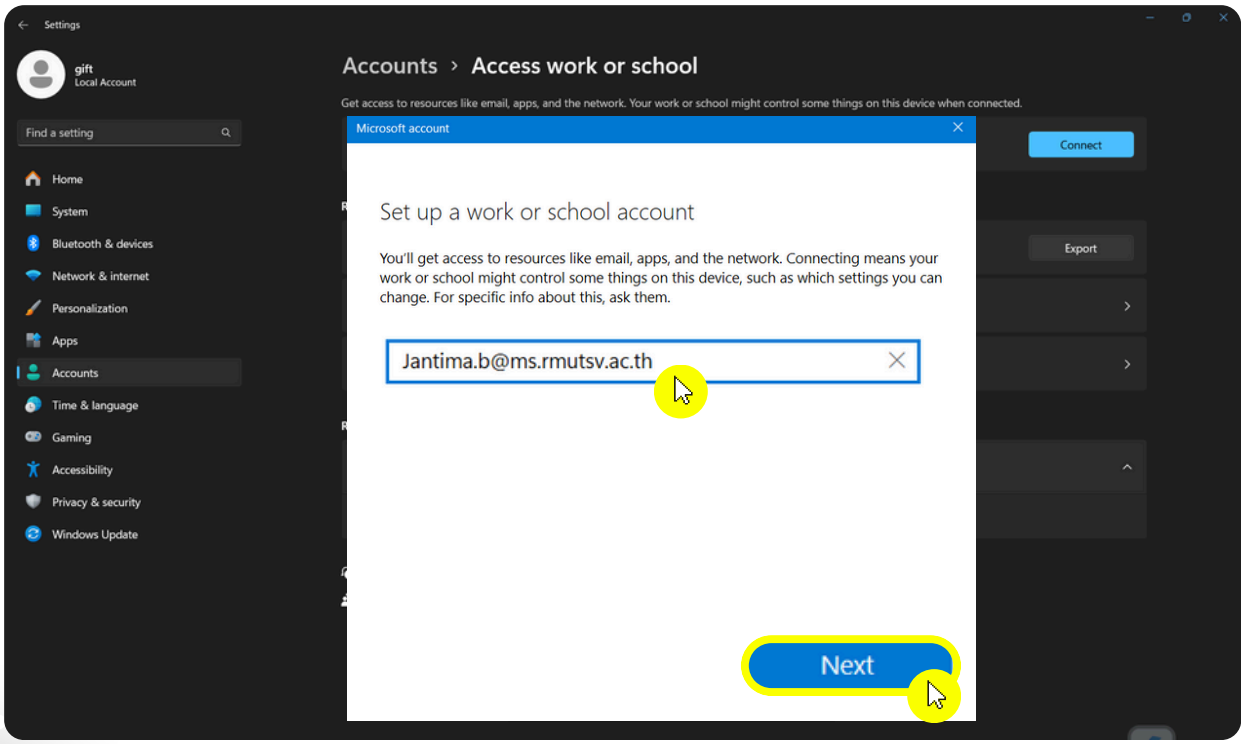
3. เลือก Enrill only in device management



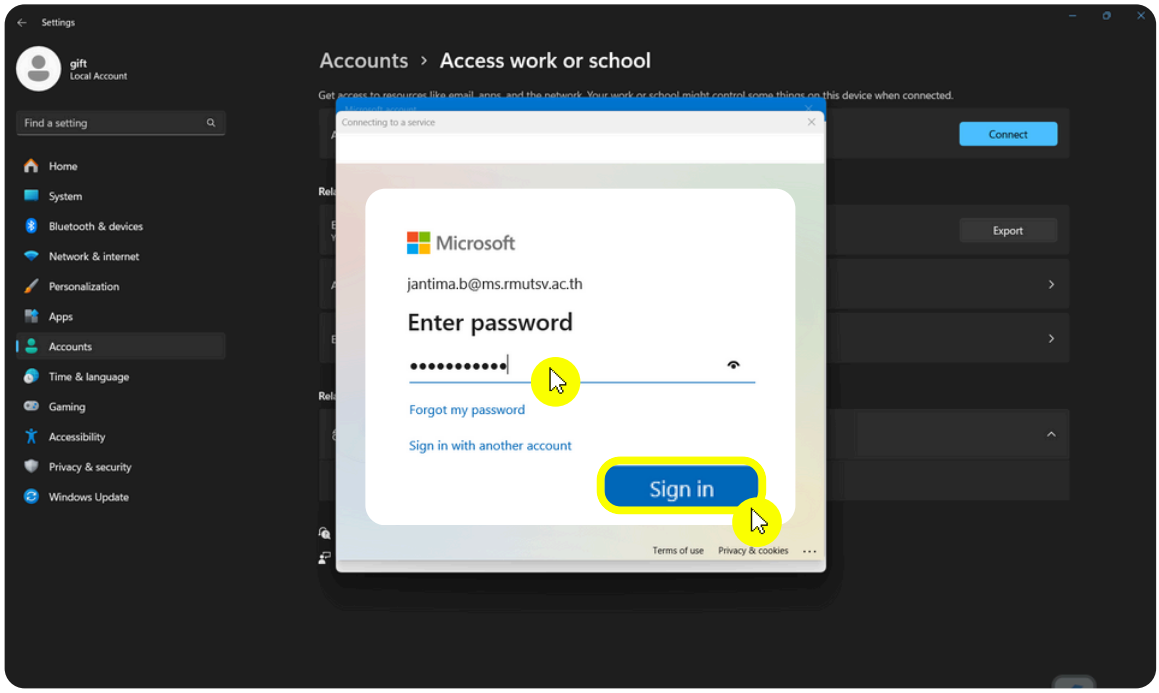
4. ระบุอีเมลของ Microsoft กดปุ่ม Next

ตัวอย่างอีเมลบุคลากร : Jantima.b@ms.rmutsv.ac.th

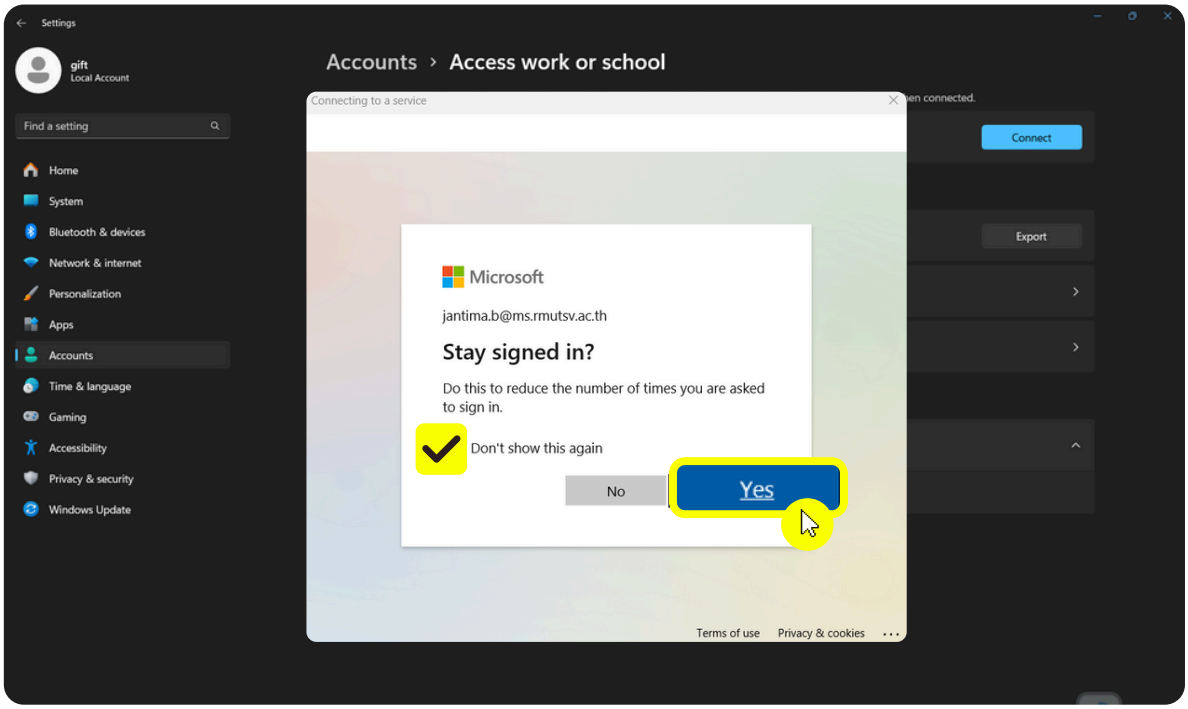
ตัวอย่างอีเมลนักศึกษา : ชื่อบัญชีผู้ใช้งาน e-Passport @ms.rmutsv.ac.th



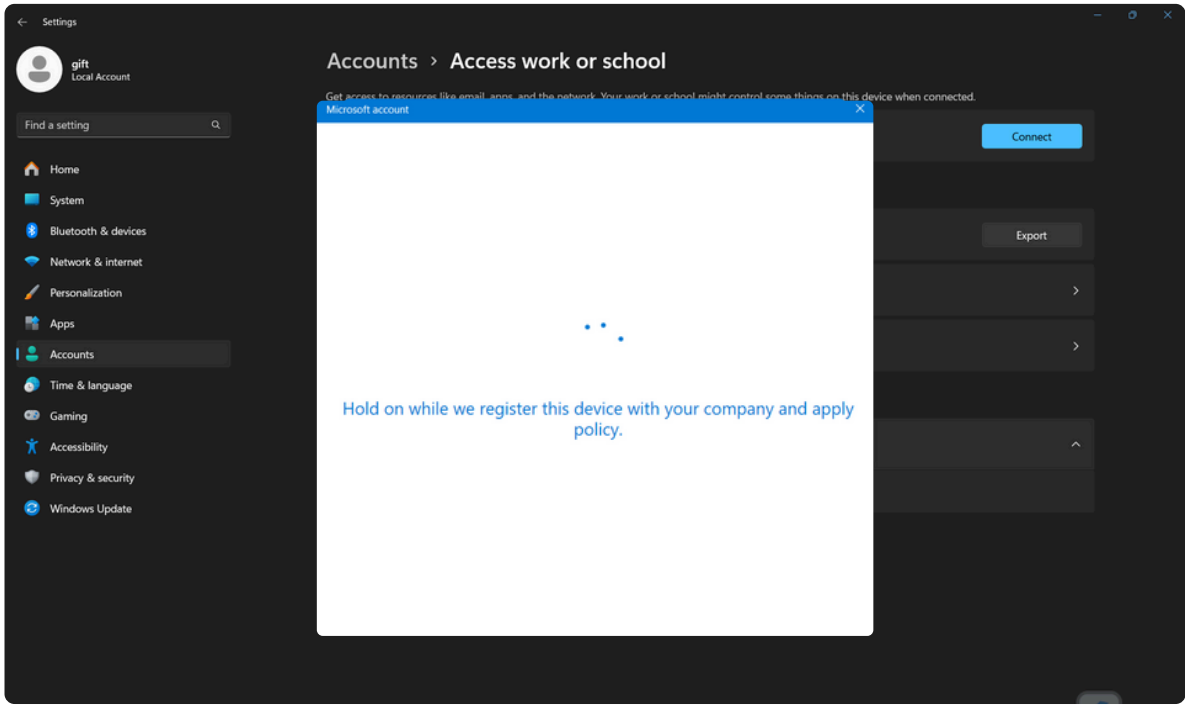
5. ระบุรหัสผ่าน e-Passport และกด Sign in



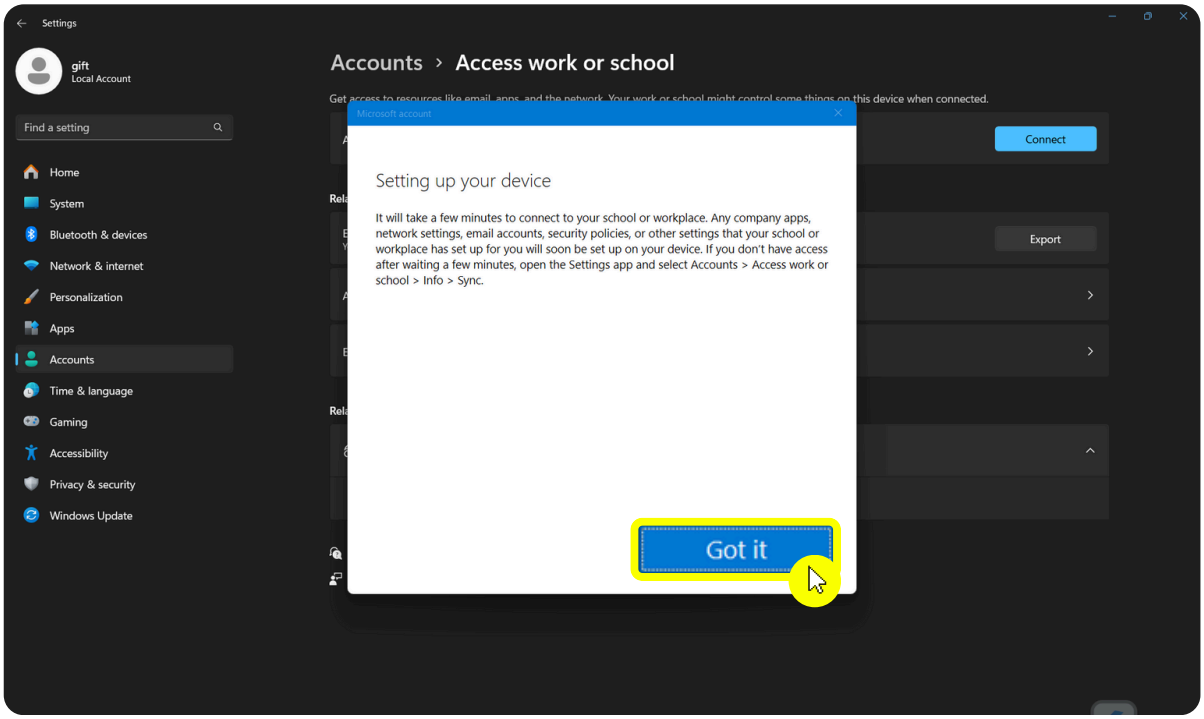
6. ติ๊กถูก หน้าข้อความ " Don't show this again" และคลิก " Yes"



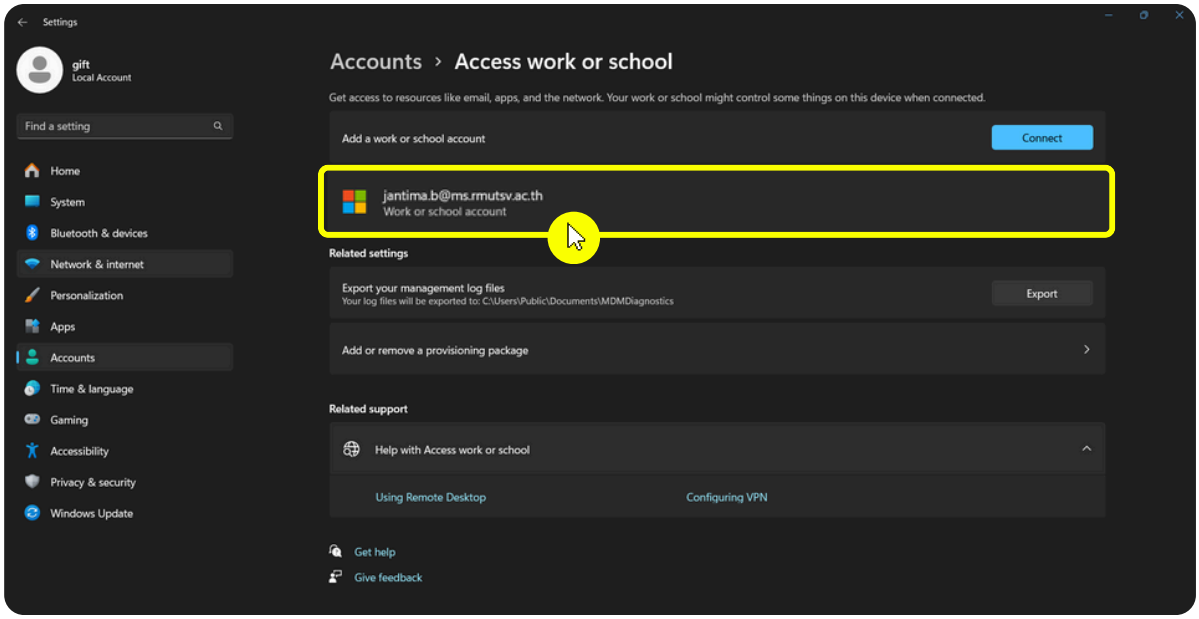
7. รอระบบดำเนินการ



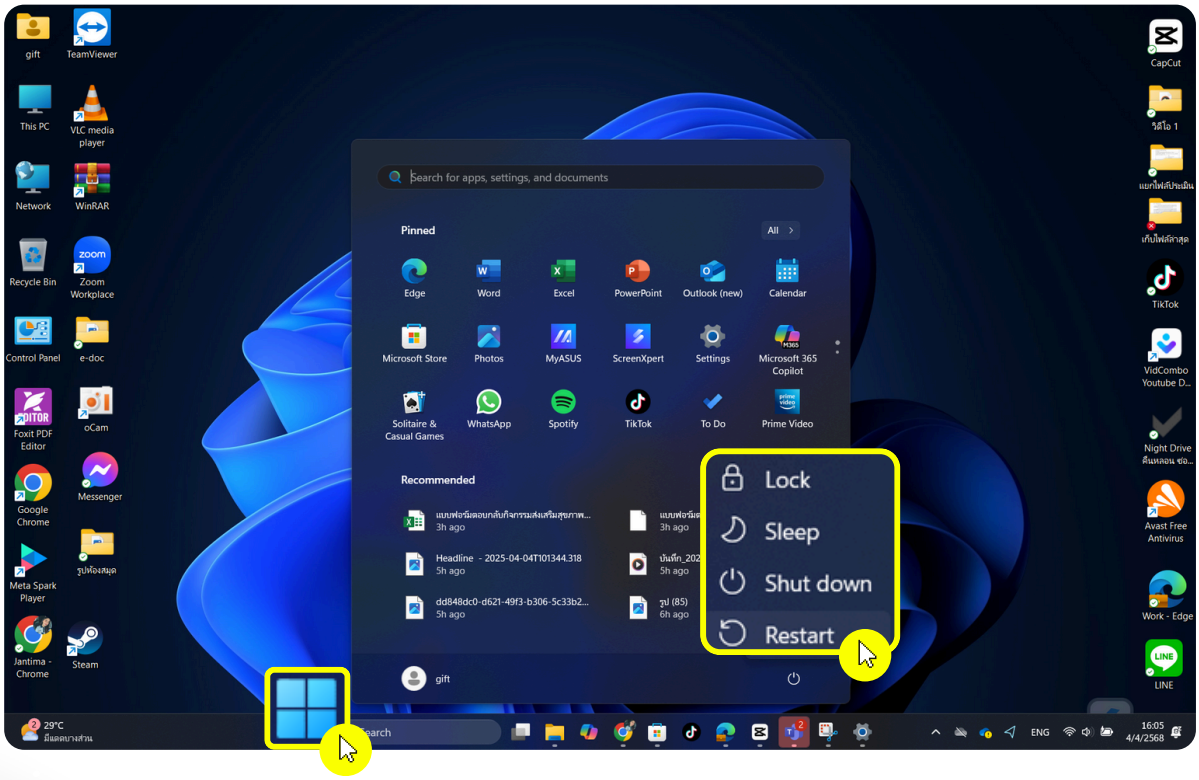
8. คลิก “Got it”



9. จะปรากฏอีเมล Microsoft ของมหาวิทยาลัย จะถือว่าเสร็จสิ้นขั้นตอน

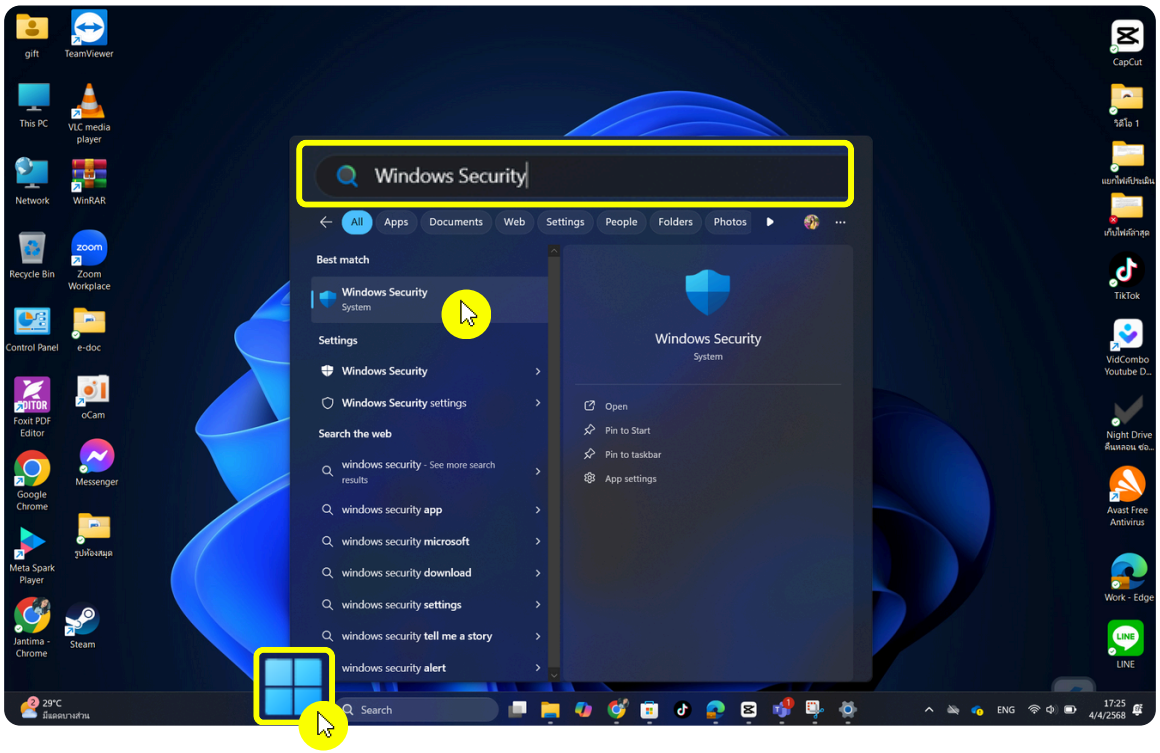


10. กลับไปยังหน้า Dektop คลิกปุ่ม Start เลือก “Restart ” 1 ครั้ง

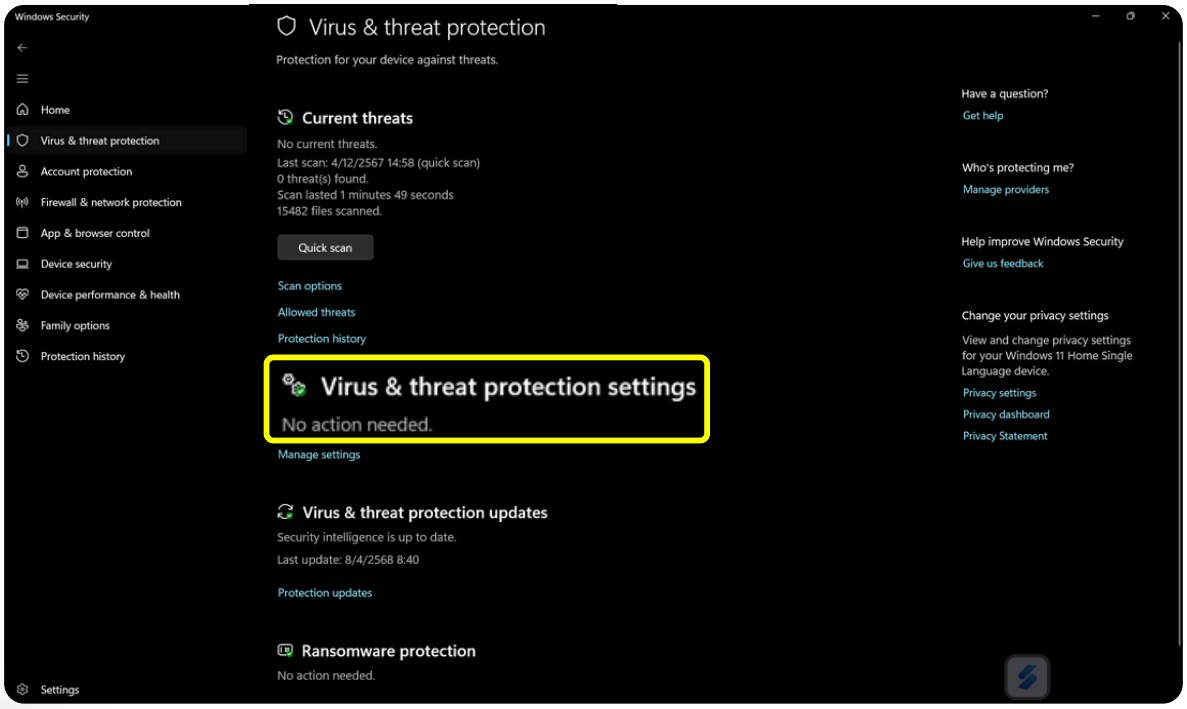


ขั้นตอนการตรวจสอบการเปิดการใช้งาน

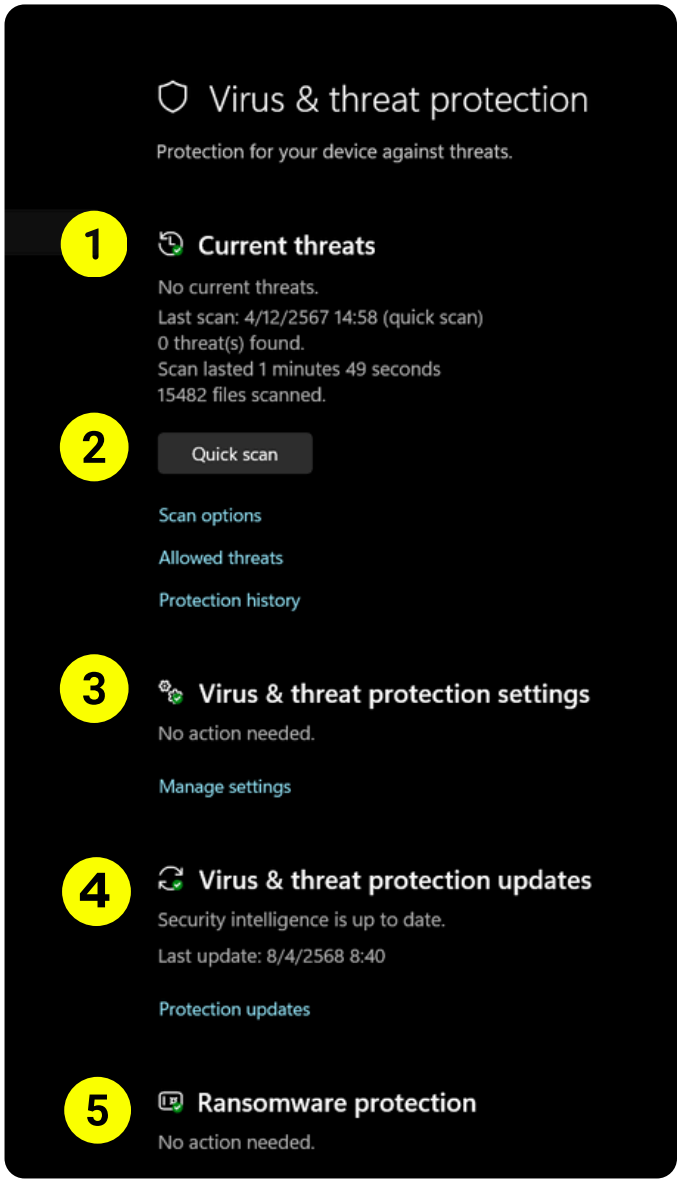
1. คลิก Start พิมพ์ “ Windows Security” คลิกเปิด



2. ตรวจสอบหน้า Virus & Threat Protection จะปรากฏสัญลักษณ์



ตัวอย่างหน้าจอการตรวจสอบสถานะของระบบป้องกันไวรัสในเครื่อง



1. Current threats : แสดงผลการสแกนล่าสุด (ในภาพคือสแกนเมื่อ 3/4/2568 เวลา 12:16 และไม่พบภัยคุกคาม)

2. Quick scan : ปุ่มสำหรับเริ่มการสแกนแบบเร็วทันที

3. Virus & threat protection settings การตั้งค่าการป้องกัน (ยังไม่ต้องดำเนินการใด ๆ)

4. Virus & threat protection updates : แจ้งว่าอัปเดตฐานข้อมูลไวรัสล่าสุดแล้ว (อัปเดตล่าสุดเมื่อ 4/4/2568 เวลา 8:44)

5. Ransomware protection : สถานะการป้องกัน Ransomware ซึ่งในภาพระบุว่าไม่มีการดำเนินการที่ต้องทำ

ถ้าเปิดอยู่และปกติจะเห็น **สัญลักษณ์โล่สีเขียว** พร้อมข้อความว่า :

- "No action needed"
- หรือ "Your device is being protected"
- บางครั้งจะมีวงกลมเขียวมีเครื่องหมาย ✓ ขึ้นอยู่กับเวอร์ชันของ Windows

ถ้าไม่ได้เปิด หรือมีปัญหาจะเปลี่ยนเป็น **สัญลักษณ์โล่สีเหลือง/แดง**

- โล่สีเหลือง/แดง พร้อมเครื่องหมาย ! หรือ X
- มีข้อความแจ้งเตือน เช่น "Turn on virus protection" หรือ "Threats found"

การสแกนไวรัส

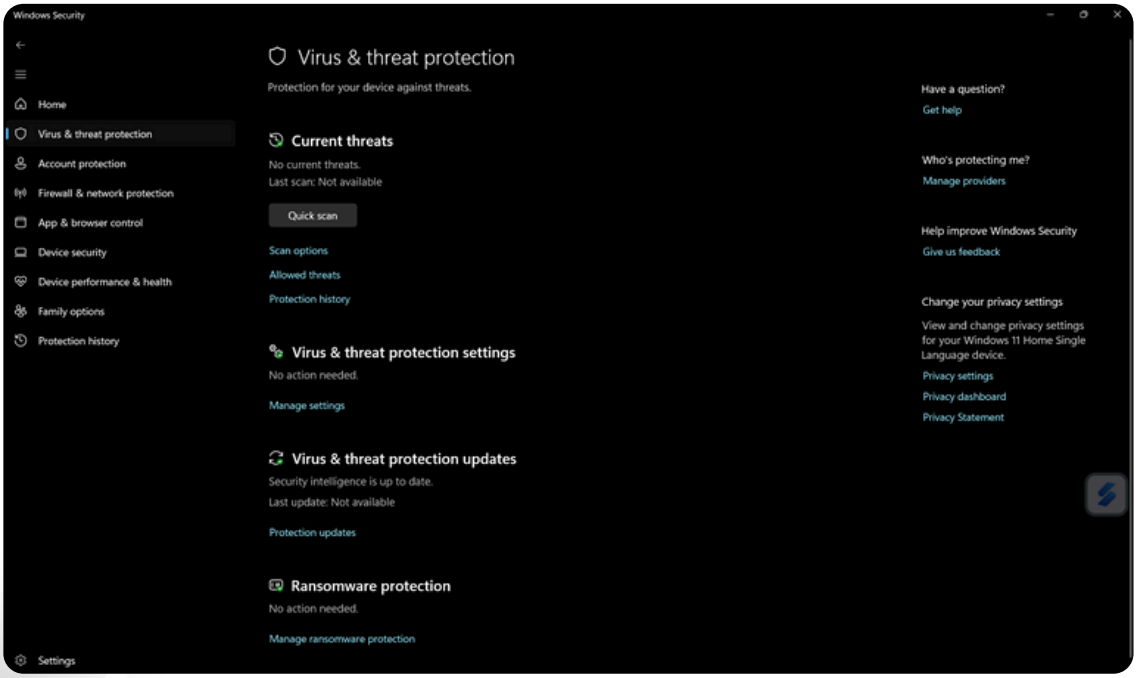
ขั้นตอนการสแกนไฟล์ไวรัสด้วย Microsoft Defender Antivirus **จะมี 2 แบบ**

1. การสแกนไวรัสผ่าน Windows Security 2. การสแกนไวรัสไฟล์หรือโฟลเดอร์แบบเจาะจง

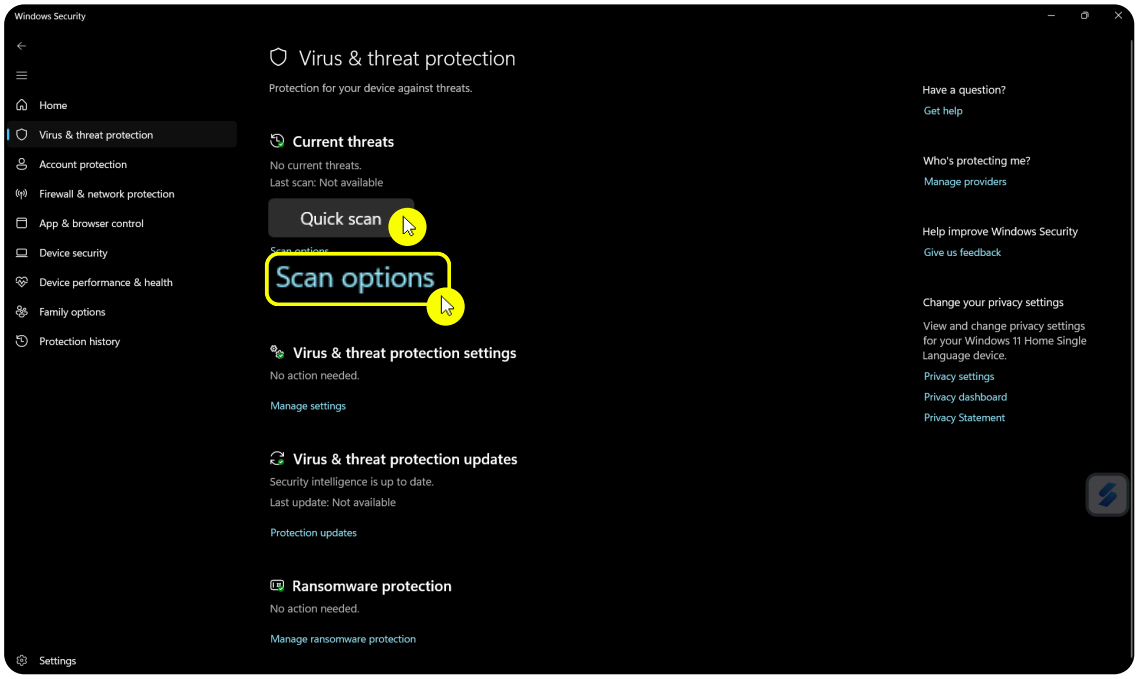
ขั้นตอนการสแกนไวรัสผ่าน Windows Security

1. คลิก Start พิมพ์ “Windown Security”

2. ไปที่เมนู Virus & Threat Protection (การป้องกันไวรัสและภัยคุกคาม)

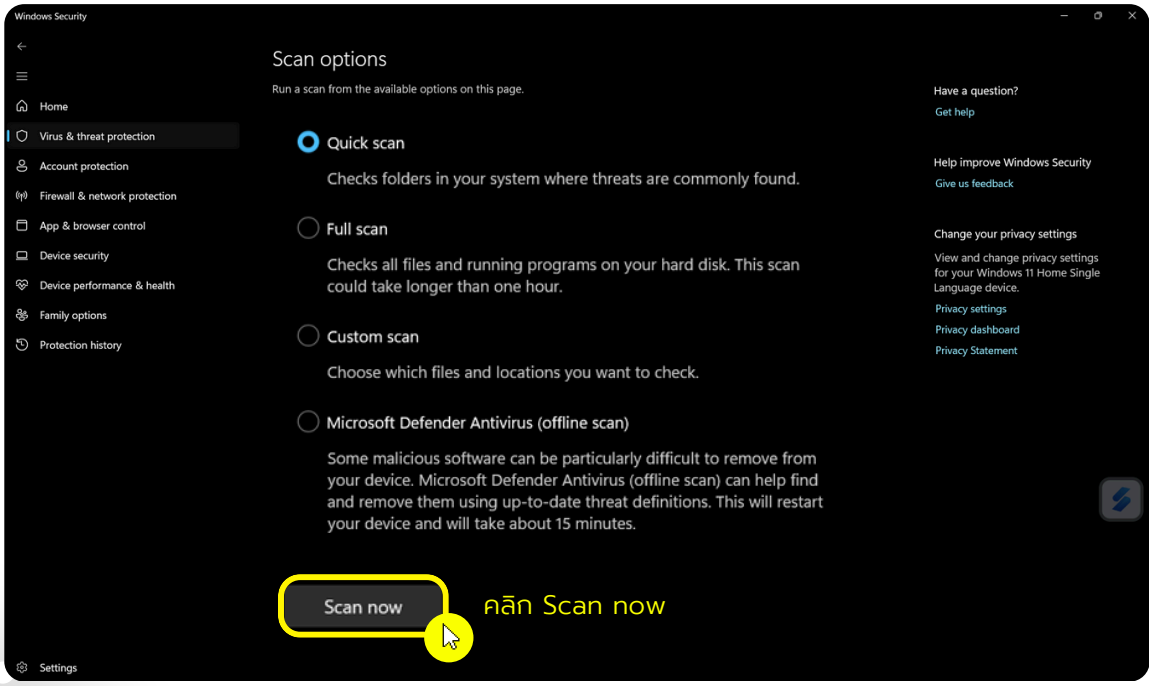


3. คลิกปุ่ม "Quick scan" เพื่อเริ่มการสแกน หากต้องการสแกนละเอียดให้คลิก “Scan options”



4. คลิกเลือกการสแกนแบบละเอียด Scan Options แบ่งออกเป็นประเภทดังนี้
   - Quick Scan สแกนเฉพาะตำแหน่งที่มักมีมัลแวร์
   - Full Scan สแกนทั้งระบบ (ระยะเวลานาน)
   - Custom scan สแกนเฉพาะโฟลเดอร์ หรือไดร์ฟเฉพาะ
   - Microsoft Defender Antivirus (offline scan) รีบูตและสแกนก่อนระบบทำงาน

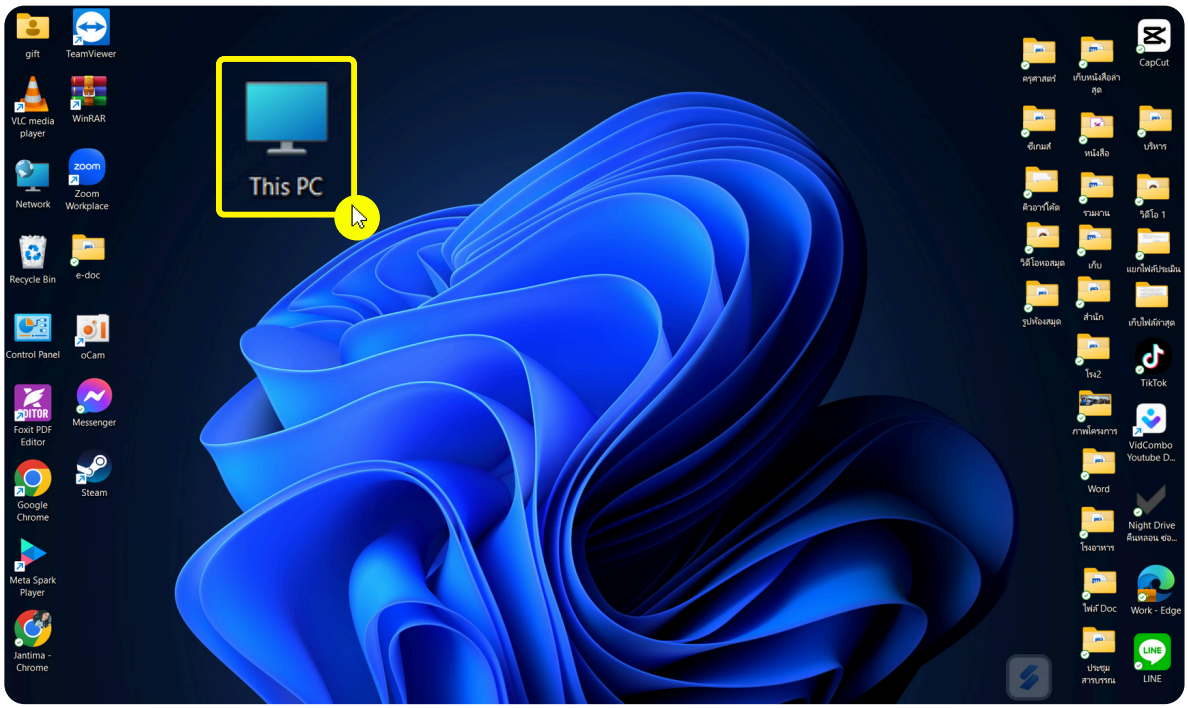
เหมาะกับมัลแวร์ซับซ้อน



การสแกนไวรัส

ขั้นตอนการสแกนไวรัสไฟล์หรือโฟลเดอร์แบบเจาะจง

1.คลิกที่ This PC เพื่อเปิด “File Explorer”

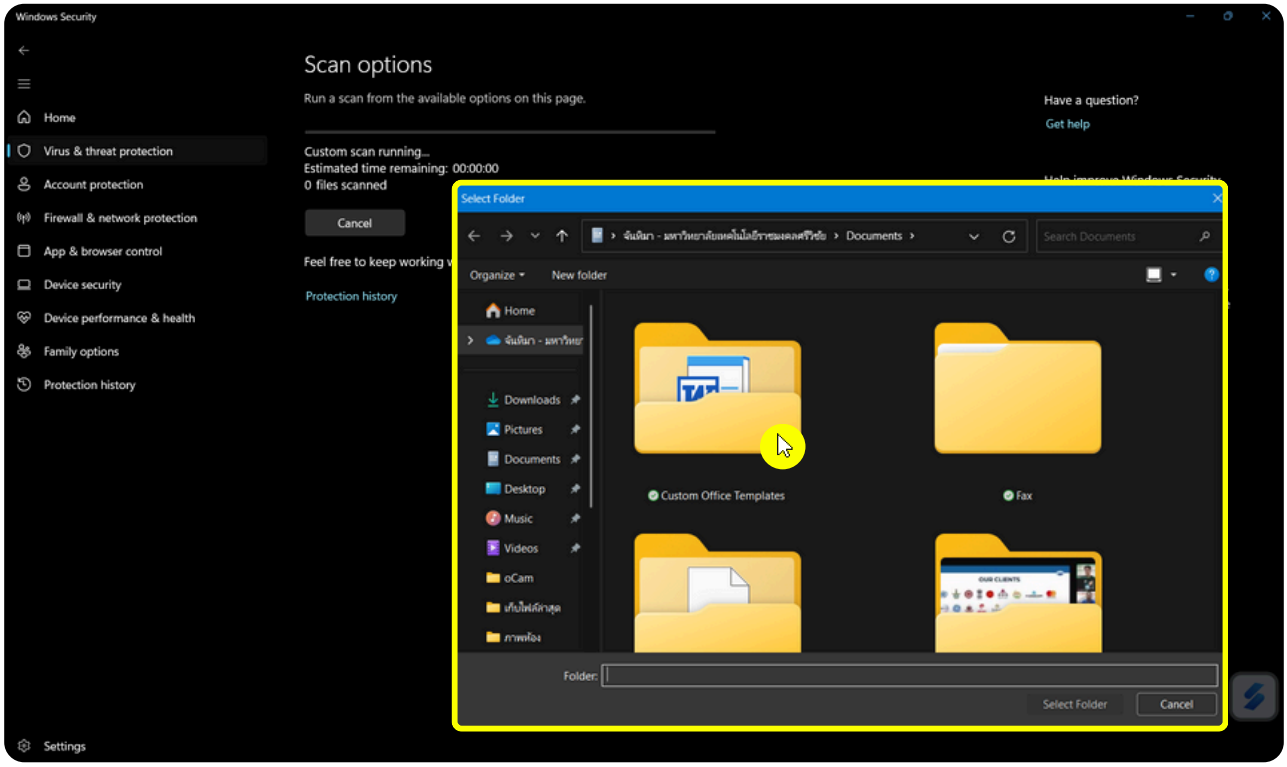


2. จะปรากฏไดร์ฟจัดเก็บข้อมูลต่าง ๆ

จากภาพตัวอย่างจะทำการสแกนไวรัส Local Disk (D:)

หากเป็นที่เก็บข้อมูลจากแฟลชไดร์ฟก็จะปรากฏชื่อแฟลชไดร์ฟนั้น ๆ ขึ้นมายังหน้าจอนี้

5. จะปรากฏหน้าจอให้ทำการเลือกโฟลเดอร์ที่ต้องการสแกน แล้วคลิก “Select Folder”



6. จากนั้น Microsoft Defender จะเริ่มทำการสแกนเฉพาะพื้นที่ที่เลือก