



## คู่มือและข้อปฏิบัติสำหรับ USER สป.สธ.

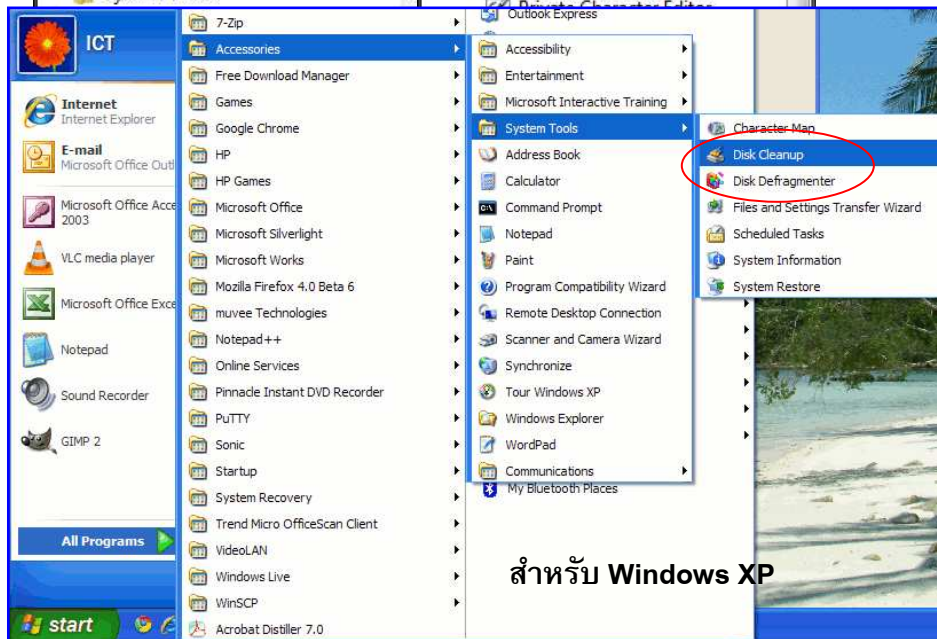
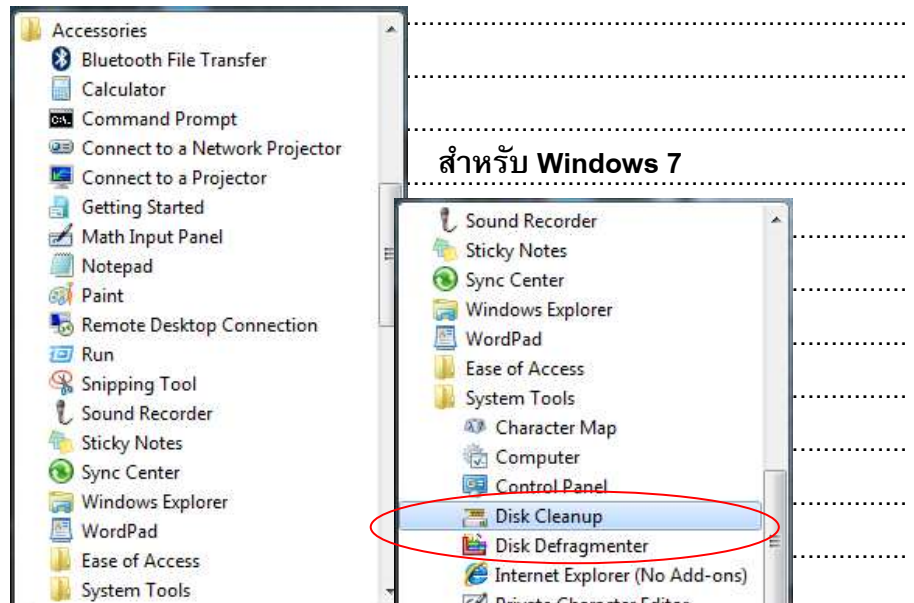


ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร  
สำนักงานปลัดกระทรวงสาธารณสุข

<http://ict.moph.go.th>

[ มีนาคม 2554 ]

## ภาพการเข้าสู่เมนูเพื่อทำ Disk Cleanup และ Disk Defragmenter



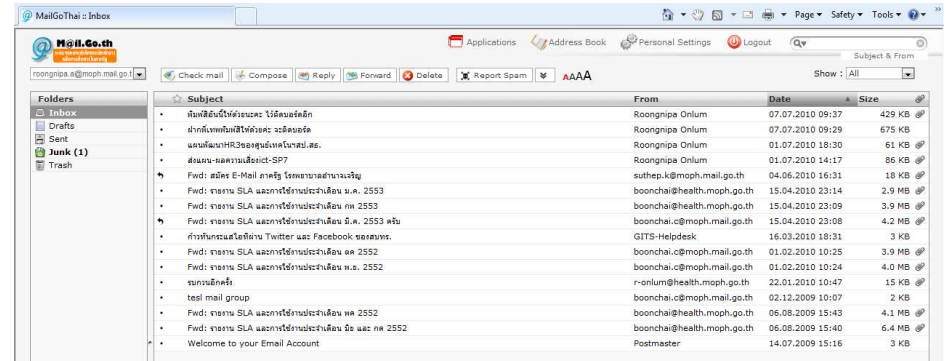
## สารบัญ

	หน้า
ข้อปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์	1
สิ่งที่ต้องปฏิบัติเพื่อป้องกันภัยคุกคามทาง Internet	3
คู่มือการใช้งานโปรแกรม Anti Virus TrendMicro OfficeScan	6
การตรวจสอบการเชื่อมต่อกับระบบเครือข่าย	9
การใช้งาน Internet ผ่าน Wireless LAN สป.สธ.	13
การตั้งชื่อเครื่องคอมพิวเตอร์	18
แนะนำบริการของ ศทส.สป.สธ.	19

อย่าลืม !! ตรวจสอบอายุสมาชิก Internet นะคะ !!



สอบถาม โทร 2198



มีพื้นที่ให้ใช้ 3GB : เชิญ Download ไปสมัครได้ในหน้าเว็บไซต์ศูนย์เทคโนโลยี  
 “สมัครใช้ E-mail ภาครัฐ” ค่ะ

เว็บไซต์ศูนย์ข้อมูลข่าวสาร สป.สธ.

<http://www.moph.go.th/ops/oic/>



เว็บไซต์ e-Conference เข้าสู่ระบบประชุมทางไกล(web Conference)

<http://ict.moph.go.th:8080/conference/>



ระบบ e-Mail ใหม่ของกระทรวงสาธารณสุข



กระทรวง ICT และ สบทร. เป็นผู้ให้บริการนี้

### ข้อปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์

#### ปฏิบัติประจำวัน :-

1. ทำความสะอาดตัวเครื่องและจอภาพ (ขณะยังไม่เปิดเครื่อง)
  - 1.1 ตัวเครื่อง ใช้ผ้าแห้งเช็ดฝุ่น ใช้แปรงขนนุ่มปัดฝุ่นที่คีย์บอร์ด และใช้ผ้าชุบน้ำหมาดๆ เกือบแห้งเช็ดคีย์บอร์ดและเมาส์
  - 1.2 จอภาพแบบLCD ใช้ผ้านุ่มๆเช็ดเท่านั้น หรือใช้ผ้าใยไมโครไฟเบอร์
  - 1.3 จอภาพแบบธรรมดา ใช้ผ้าชุบน้ำหมาดๆ เกือบแห้ง เช็ดก่อนแล้วเช็ดตามทันทีด้วยผ้าแห้ง หรือใช้ผ้าชุบน้ำยาสำหรับเช็ดจอภาพเท่านั้น (ไม่ผสมแอมโมเนีย)
2. เมื่อเปิดเครื่องเข้าสู่ระบบปฏิบัติการ (OS) เช่น MS Windows, Ubuntu
  - 2.1 ตรวจสอบโปรแกรม Anti Virus ที่มีในเครื่องจะต้องไม่หมดอายุ
  - 2.2 Login เข้าสู่ระบบเพื่อเชื่อมต่อ Internet (ระบุ Username และ Password ของตนเองให้ถูกต้อง)
  - 2.3 Update Definition File Virus ให้เป็นวันที่ปัจจุบัน
  - 2.4 ตรวจสอบประกาศ/ข่าวสารด้านไอที ที่ <http://ict.moph.go.th>
3. เมื่อมีการเชื่อมต่อ Removable Drive เช่น thumb drive ให้ทำการ Scan Virus ก่อน Open และ/หรือ Explore เพื่อ copy ไฟล์ หรือ เปิดไฟล์ใช้งาน
4. ควรปฏิบัติงานกับไฟล์ต่างๆ บน Hard drive ของเครื่อง ไม่ควรเปิดไฟล์จาก thumb drive และแก้ไขเปลี่ยนแปลง แนะนำให้ copy ไฟล์นั้นๆ วางไว้ใน C: หรือ MyDocuments ก่อน แล้วจึงเปิดแก้ไขเปลี่ยนแปลง ป้องกัน thumb drive เสียเร็วและข้อมูลสูญหาย
5. ทำการ Copy ไฟล์งานสำคัญๆ จากเครื่อง เก็บไว้ที่ Removable Drive เพื่อเป็นการสำรองข้อมูล (Backup)

### ปฏิบัติประจำสัปดาห์ :-

1. ลบไฟล์จาก **Recycle Bin** บนหน้าจอ Desktop ทั่วไปของวินโดวส์จะมี Icon เป็นรูปถังขยะที่ชื่อว่า Recycle Bin ให้เปิด Folder นั้นขึ้นมา จะมี Menu ด้านซ้ายมือให้เลือก Click ที่ Empty the Recycle Bin และยืนยัน การลบด้วย Yes เพื่อเป็นการลบไฟล์ข้อมูลถาวร



2. ลบไฟล์ที่ไม่จำเป็นด้วย **Disk Cleanup** ที่มากับวินโดวส์ ซึ่งอยู่ที่ Start Menu -> All Programs -> Accessories -> System Tools -> Disk Cleanup เลือก ไดรฟ์ที่ต้องการแล้ว Click OK ระบบจะประมวลผลว่ามีไฟล์ใดบ้างที่สมควรจะลบ เมื่อประมวลผลแล้วระบบจะแจ้งว่ามีพื้นที่ในไดรฟ์นั้นที่ควรลบเท่าใด จากนั้นให้ Click OK เพื่อให้ระบบเริ่มดำเนินการ หมายเหตุ หากเป็นการใช้ Disk Cleanup ครั้งแรก หรือไม่ได้ดำเนินการมานานแล้ว จะทำให้ต้องใช้เวลานานระบบจึงจะ ดำเนินการเสร็จ อาจใช้เวลานานถึง 1/2 ชั่วโมงได้ (ดูภาพท้ายเล่ม)

3. จัดเรียงข้อมูลในดิสก์(Hard disk) ด้วย **Disk Defragment** ซึ่งอยู่ที่ Start Menu -> All Programs -> Accessories -> System Tools -> Disk Defragment เลือกไดรฟ์ที่ต้องการ แล้ว Click ที่ Defragment ระบบจะจัดเรียง ข้อมูลในไดรฟ์นั้นใหม่ เพื่อให้เกิดความรวดเร็วในการเปิดไฟล์ข้อมูล หรือ โปรแกรมต่างๆในไดรฟ์นั้น หมายเหตุ หากเป็นการใช้ Disk Defragment ครั้งแรก หรือไม่ได้ดำเนินการมานานแล้ว จะทำให้ต้องใช้เวลานานระบบจึงจะ ดำเนินการเสร็จ อาจใช้เวลานานถึง 1 ชั่วโมงได้ (ดูภาพท้ายเล่ม)

4. สั่ง **Scan Virus** แบบ **Full System Scan** หรือ Deep Scan เพื่อตรวจหา ไวรัสคอมพิวเตอร์ที่แฝงตัวในครั้งทั้ง C: และ Local Drive

### :: แนะนำบริการของ ศทส.สป.สร. ::

เว็บไซต์ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (http://ict.moph.go.th)

The screenshot shows the ICT-MOPH website interface. At the top, there are navigation links for 'ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร' (ICT Center) and 'สำนักงานปลัดกระทรวงสาธารณสุข' (Ministry of Public Health). Below this, there are links for 'e-Conference', 'Download', and 'KM Blog'. The main content area features a 'ข่าวประชาสัมพันธ์' (Public Information) section with several news items, including announcements about CIO appointments, e-auction procedures, and ICT service updates. There is also a 'บริการ ICT เป็นเลิศและเข้าถึงได้' (Excellent and Accessible ICT Services) section. At the bottom, there is a 'คู่มือและแนวทางดำเนินงานด้าน IT' (IT Workbooks and Guidelines) section with a table listing various IT services and their contact information.

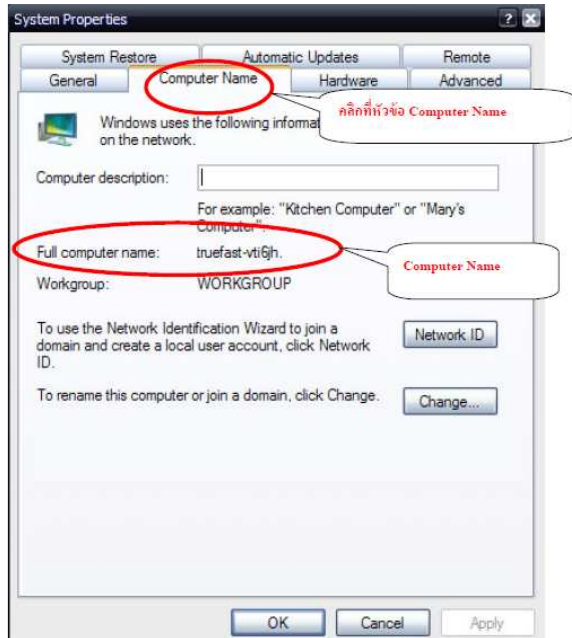
### เว็บไซต์ ICT-MOPH KM BLOG แบ่งปันความรู้ ICT

The screenshot shows the ICT-MOPH KM BLOG website. The main heading is 'เคล็ดลับไม่ลับประจำบ้าน(1)' (Secrets of the Home (1)). The content includes a list of tips for home users, such as 'เคล็ดลับไม่ลับประจำบ้าน(1)', 'เคล็ดลับไม่ลับประจำบ้าน(2)', and 'เคล็ดลับไม่ลับประจำบ้าน(3)'. The page also features a sidebar with a 'เลือกภาษา' (Select Language) dropdown menu and a 'Subscribe via RSS' button. The footer contains contact information for the ICT-MOPH center.

### การตั้งชื่อเครื่องคอมพิวเตอร์

การตั้งชื่อเครื่องมีประโยชน์มากในการใช้งานทรัพยากรร่วมกันบนเครือข่าย เช่น ใช้งาน Printer ร่วมกัน เป็นต้น มีวิธีการตรวจสอบและตั้งค่าดังนี้

1. คลิกขวาที่ My Computer ในหน้า Desktop -> เลือก Properties
2. เลือกแท็บ Computer Name



3. ถ้าต้องการแก้ไข ให้คลิกปุ่ม Change เข้าไปแก้ไขเสร็จแล้ว Apply -> OK ชื่อเครื่องจะเปลี่ยนตามที่แก้ไขเมื่อ Restart เครื่องใหม่
- ควรตั้งชื่อเป็นภาษาอังกฤษ ไม่ยาวมาก ส่วน Workgroup ก็เช่นกัน ควรใช้เป็นตัวอักษรย่อของหน่วยงาน เพื่อสื่อความหมายได้ชัดเจน

\*\*\*\*\*

### สิ่งที่ต้องปฏิบัติเพื่อป้องกันภัยคุกคามทาง Internet

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สช. ขอแนะนำแนวทางปฏิบัติเพื่อรับมือกับภัยอาชญากรรมทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ซึ่งสรุปเป็น 10 วิธีป้องกันตนให้ปลอดภัย มาให้รับทราบและปฏิบัติกัน ดังนี้

1. **ตั้งสติก่อนเปิดเครื่อง** ต้องไม่ให้ใครแอบดู Password เข้าเครื่อง และควรรลือคหน้าจอ(Screen Saver)ให้อยู่ในสถานะที่ต้องใส่ Password ก่อน
2. **กำหนด Password ที่ยากแก่การคาดเดา** ความยาวไม่ควรต่ำกว่า 8 ตัวอักษรและใช้อักษรพิเศษผสมด้วย ไม่ควรเป็นคำที่มีความหมายหรือศัพท์ใดๆ เช่น s0mCh@i หรือตั้งเป็นภาษาไทยแต่พิมพ์ด้วยแป้นภาษาอังกฤษ เช่น คำว่า สมชาย เมื่อพิมพ์ด้วยแป้นภาษาอังกฤษจะตรงกับตัวอักษร "l,=kp" ทำให้คาดเดายากขึ้น ช่วยเพิ่มความปลอดภัย
3. **สังเกตขณะเปิดเครื่องว่ามีโปรแกรมแปลกๆ** ทำงานทันทีพร้อมกับ การเปิดเครื่องหรือไม่ สังเกตระยะเวลาบูตเครื่องว่านานผิดปกติหรือไม่ เพราะถ้าใช่ อาจเป็นได้ว่าเครื่องติดไวรัส หรือมัลแวร์ตัวอื่นๆ
4. **ตรวจสอบและ Update OS หรือ Software** ที่ใช้ ให้เป็นเวอร์ชันปัจจุบันอย่างสม่ำเสมอ โดยเฉพาะโปรแกรมป้องกันภัยจากมัลแวร์ ไวรัสคอมพิวเตอร์ โปรแกรมไฟร์วอลล์ และควรใช้ที่ถูกลิขสิทธิ์ โปรแกรมสำคัญยิ่งอีกโปรแกรมที่ต้อง update ให้ทันสมัยอยู่เสมอคือ Internet Browser เพราะอาจเกิดช่องโหว่ใหม่ๆ ได้ตลอดเวลา
5. **ไม่ลง Software มากเกินจำเป็น** เกินศักยภาพการทำงานของเครื่อง ซึ่ง Software ที่จำเป็นต้องลงในเครื่องได้แก่

5.1 Internet Browser เพื่อใช้เปิดเว็บไซต์ต่างๆ

5.2 โปรแกรมสำหรับงานด้านเอกสาร โปรแกรมตกแต่งภาพ เสียง และ วิดีโอ

5.3 โปรแกรมป้องกันไวรัสคอมพิวเตอร์ และ/หรือ โปรแกรมไฟร์วอลล์ หากจำเป็นต้องใช้โปรแกรมอื่นๆ ควรพิจารณาใช้โปรแกรมที่ผ่าน Web Application เช่น Chat, VoIP เป็นต้น หรืออาจบันทึกโปรแกรมนั้นๆ ลงบน Thumb Drive เพื่อ Run (สั่งทำงาน) จากภายนอกเครื่อง

6. **ไม่ควรเข้าเว็บไซต์เสี่ยงภัย** ได้แก่

6.1 ลามกอนาจาร การพนัน เกี่ยวกับยาเสพติด

6.2 เว็บไซต์ที่มีหัวเรื่องว่า Free แม้กระทั่ง Free Wi-Fi ให้คิดเสมอว่า “ไม่มีของฟรีในโลก”

6.3 เว็บไซต์ที่ให้ Download โปรแกรมไฟล์นามสกุล .exe .dll .vbs เป็นต้น หรือเครื่องมือในการเจาะระบบ (Hacking Tools)

6.4 เว็บไซต์ที่แจก Serial Number เพื่อใช้ Crack โปรแกรม

6.5 เว็บไซต์ที่มี Link ไม่ตรงกับชื่อ Domain โดยทำการ Redirect

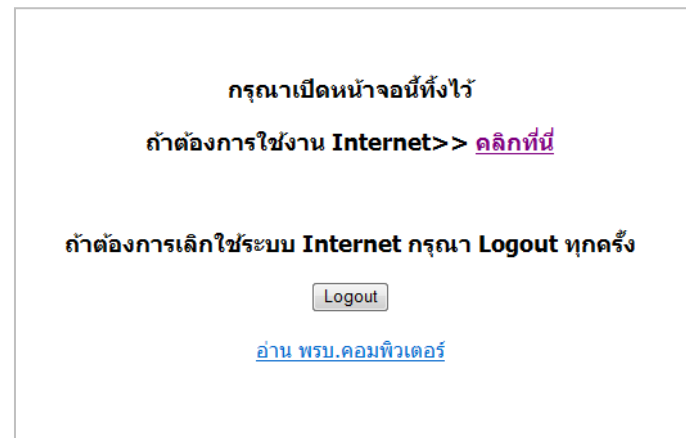
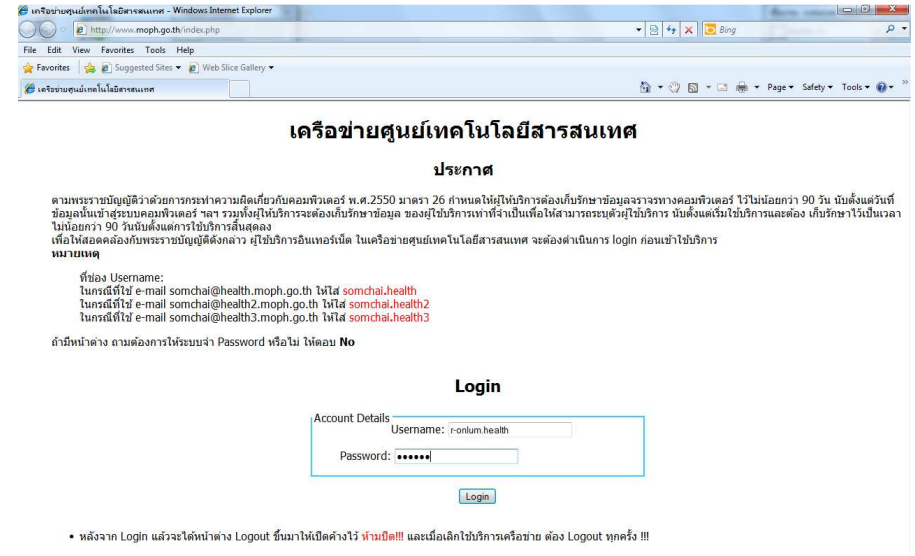
6.6 เว็บไซต์ที่มี pop-up ขึ้นหลายๆ หน้า

6.7 เว็บไซต์ที่มีชื่อ Domain ยาวๆ และมีเครื่องหมายมากเกินปกติ หรือใช้ชื่อที่ไม่เหมาะสมแก่การตั้งชื่อ เช่น www.jsx-abc-xxx-kmd.com

7. สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์ ควรใช้ URL ที่มี HTTPS เพื่อเข้ารหัสข้อมูล ป้องกันการดัก Username และ Password ในเวลาที่เราทำการ Login

8. **ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network** ควรใช้เป็นชื่อเล่น หรือฉายาที่กลุ่มเพื่อนรู้จัก ห้ามเปิดเผยเลขประจำตัวประชาชน เบอร์โทรศัพท์

3.3 เมื่อ Login ผ่านแล้วจะปรากฏหน้าจอถัดไป “กรุณาเปิดหน้าจอนี้ทิ้งไว้” เป็นข้อกำหนดว่า User จะต้องเปิดหน้าจอนี้ค้างไว้ตลอดเวลาที่มีการใช้งาน Internet และเมื่อเลิกใช้งาน Internet แล้วให้ทำการ Logout ทันที



2.2 เมื่อกดปุ่ม Connect เครื่องจะทำการติดต่อกับเครือข่าย MOPH

2.3 เมื่อ Connect เสร็จ จะมีคำเตือนขึ้นมา ให้เลือก Connect Anyway




2.4 เป็นอันเสร็จวิธีเปิดใช้งาน Wireless Network สังเกตถ้าเปิดใช้งานสำเร็จ ไอคอน Wireless Connection (อยู่มุมล่างขวาของ Task bar) จะไม่มีกากบาท



<< ขอขอบคุณวิธีการและภาพตัวอย่างจาก [http://www.it.chula.ac.th/Wireless\\_Network](http://www.it.chula.ac.th/Wireless_Network) >>

### 3. ใช้งาน Internet

3.1 เปิด Internet Browser เช่น Internet Explorer 

3.2 Login ด้วย Username และ Password ของตนเองให้ถูกต้อง เช่น ได้รับ Account จาก ศทส. ในชื่อ somchai@health2.moph.go.th จะใช้ชื่อ Username ว่า somchai.health2 เป็นต้น กรุณาอ่านข้อความในหน้าให้ละเอียด และควรอ่านทุกครั้ง เพราะอาจมีการเปลี่ยนแปลงวิธีการหรือประกาศด่วนเกี่ยวกับความปลอดภัยในการใช้งาน Internet

ส่วนตัว ข้อมูลที่พักอาศัย หมายเลขบัตรเครดิต หมายเลขหนังสือเดินทาง ข้อมูลทางการแพทย์ ประวัติการทำงาน เป็นต้น

**9. ศึกษาข้อกำหนดเกี่ยวกับการใช้สื่อ Internet** ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และควรคำนึงถึง “ใจเขาใจเรา” หากเราไม่ชอบสิ่งใด ก็ไม่ควรทำสิ่งนั้นกับผู้อื่น

**10. ไม่หลงเชื่อโดยง่าย** อย่าเชื่อในสิ่งที่เห็น และอย่ามกมายกับข้อมูลบน Internet ควรศึกษาข้อมูลให้รอบด้าน จากหลายแหล่งข้อมูลมาประกอบกันและใช้วิจารณญาณและประสบการณ์ในการตัดสินใจ

ควรระลึกไว้เสมอว่า “ความมั่นคงปลอดภัยข้อมูลจะเกิดขึ้นได้ ต้องเริ่มจากตัวเองก่อน” หากผู้ใช้งานปลอดภัย ระบบเครือข่ายภายในองค์กรนั้นก็จะเป็นที่ปลอดภัย เครือข่ายองค์กรอื่นๆที่มาร่วมใช้งานด้วยก็จะปลอดภัย เกิดเป็นห่วงโซ่แห่งความปลอดภัย จากระดับเล็กสู่ระดับใหญ่ ไปถึงระดับชาติ ช่วยให้ประเทศไทยของเราปลอดภัยจากการใช้ระบบสารสนเทศได้

\*\*\*\*\*

ที่มา : เอกสารประกอบการสัมมนาเรื่อง แนวทางการรับมือกับภัยไอซีที เมื่อวันที่ 13 กรกฎาคม 2553 ณ โรงแรมมิราเคิล แกรนด์ โดย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

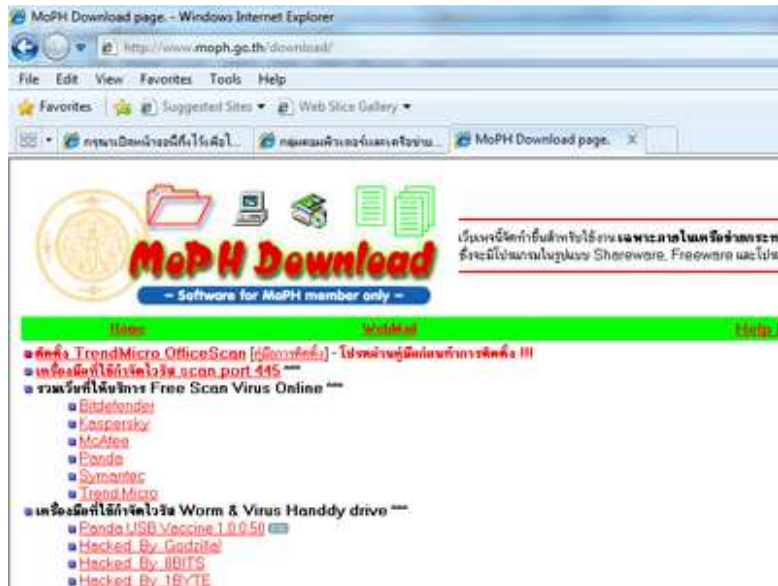
### คู่มือการใช้งานโปรแกรม Anti Virus TrendMicro OfficeScan



โปรแกรมนี้เป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้อง ซึ่งสำนักงานปลัดกระทรวงสาธารณสุข จัดหาเอาไว้เพื่อให้บริการแก่เครื่องลูกข่าย(Clients) ภายในอาคาร สป.สธ. เท่านั้น และโปรแกรมจะ Update อัปเดตโมติผ่าน Internet มายัง TrendMicro Server ณ ศทส.สป.สธ.

ท่านสามารถติดตั้งโปรแกรมนี้ได้โดย

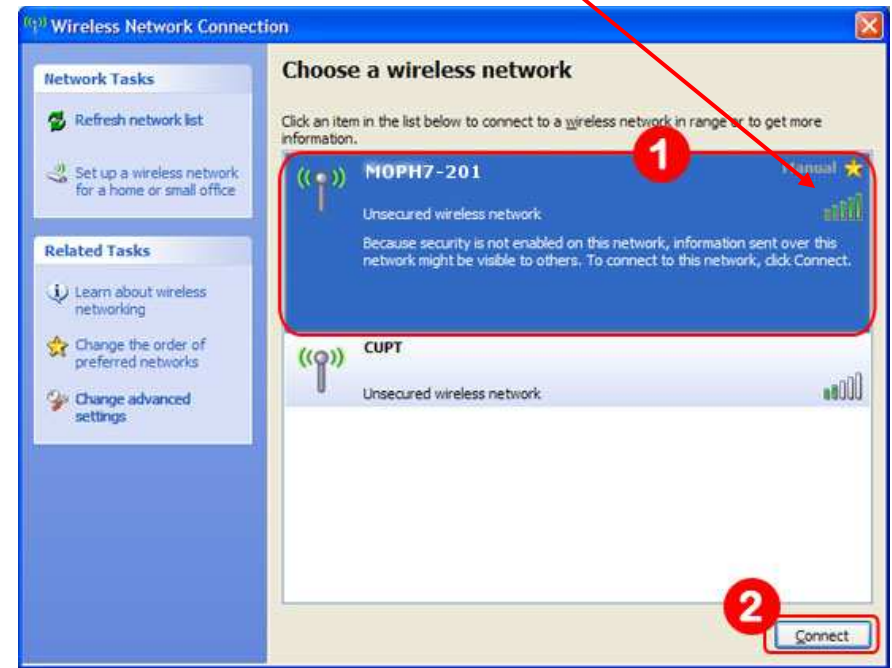
1. เปิดเว็บไซต์ MoPHDownload ที่<http://www.moph.go.th/download/>
2. คลิก "ติดตั้ง TrendMicro OfficeScan" ทำตามคู่มือการติดตั้ง



### 2. การเลือกใช้งานเครือข่าย MOPH

เมื่อกดเลือก View Available Wireless Networks จะมีหน้า Wireless Network Connection ขึ้นมา เป็นหน้าที่ใช้จัดการทำงานของ Wireless Network ซึ่งมีวิธีการเปิดใช้งานเครือข่าย MOPH ดังนี้

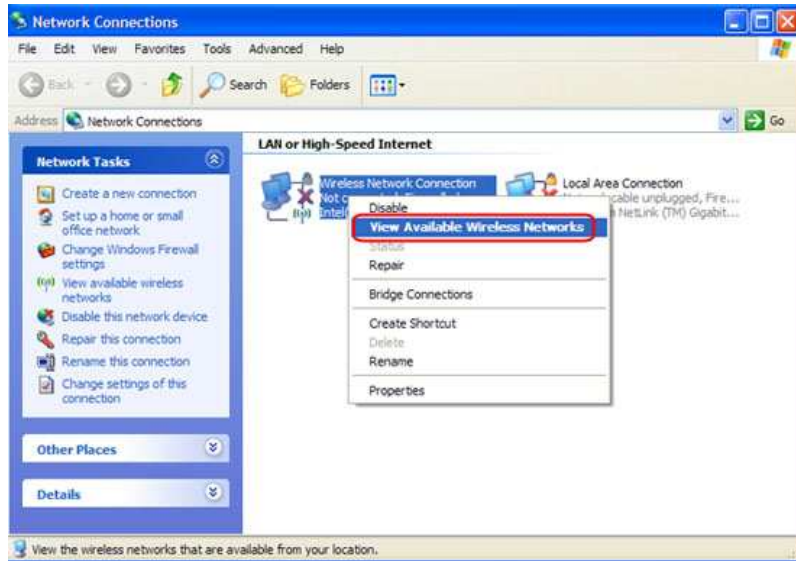
2.1 กดเลือกเครือข่ายที่แสดงคุณภาพสัญญาณดีที่สุด แล้วกดปุ่ม Connect



ศทส. ได้ตั้งชื่อ Access Point สอดคล้องกับตำแหน่งที่ตั้ง แสดงความหมายว่าอุปกรณ์ตัวนั้นติดตั้งอยู่ที่ อาคารใด ชั้นใด และเป็นตัวที่ทำไหระ : MOPH(ตึก)-(ชั้น)(ตัวที่) ดังภาพตัวอย่าง แสดงว่า อาคาร 7 ชั้น 2 ตัวที่ 1

\* ถ้าส่วน Choose a Wireless Network ไม่มีตัวเลือก ให้กดปุ่ม Refresh Network List เพื่อทำการค้นหาเครือข่าย

- มีหน้า Network Connections ขึ้นมา ให้คลิกขวาที่ Wireless Network Connection แล้วเลือก View Available Wireless Networks




วิธีที่ 2 • คลิกขวาที่ไอคอน Wireless Connection (อยู่มุมล่างขวาของ Task bar) กดเลือก View Available Wireless Networks



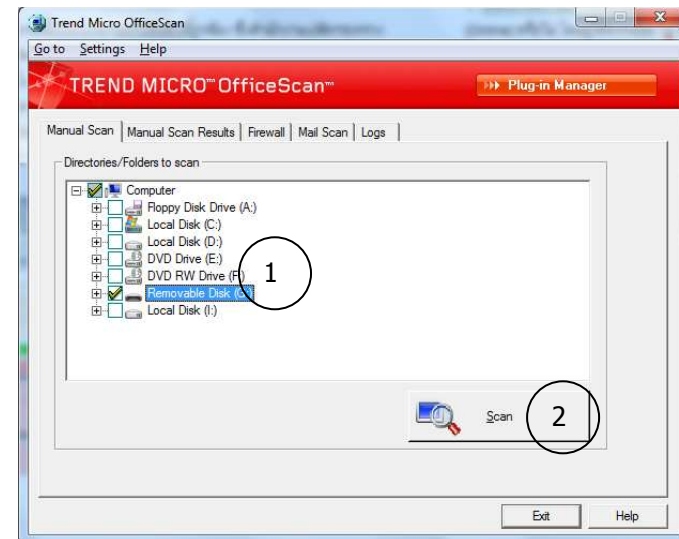
:: การใช้งานโปรแกรม TrendMicro OfficeScan ::

1. ให้สังเกตสถานะการทำงานของโปรแกรมว่าทำงานเป็นปกติตลอดเวลา (Online) หรือไม่ โดยดูได้จากicon ใน task bar ด้านล่างขวา

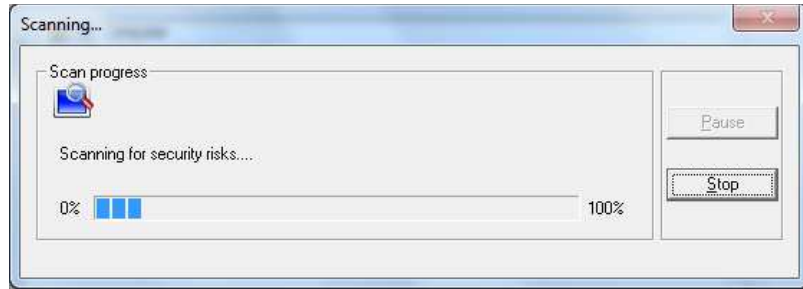


2. เปิดโปรแกรม  OfficeScan Client จากเมนู Start -> All Programs -> Trend Micro OfficeScan Client

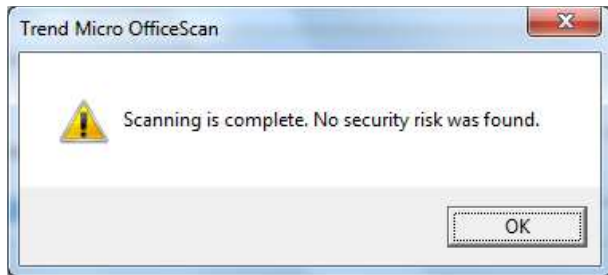
3. เลือก Drive โดยการคลิกให้มีเครื่องหมายถูก เพื่อสั่ง Scan Drive นั้นๆ



4. โปรแกรมจะทำการ Scan และทำการกำจัดไวรัสทันทีที่พบแบบอัตโนมัติ



5. เมื่อเสร็จโปรแกรมจะแจ้งว่าพบไวรัส (Infects) จำนวนเท่าไร และกำจัด (Clean) สำเร็จจำนวนเท่าไร หรือไม่พบไวรัส และความเสียหายใดๆเลย



6. คลิก Exit ปิดโปรแกรม

7. ทุกครั้งที่มีการเชื่อมต่อ Removable Drive เช่น Thumb Drive ที่ผ่านการใช้งานมาจากเครื่องอื่นๆ ต้องทำการ Scan ก่อนเปิดใช้

\*\*\*\*\*

[ สอบถามปัญหาการใช้งานโปรแกรมได้ที่ ศทส.สป.สธ. โทร. 1201 ]

การใช้งาน Internet ผ่าน Wireless LAN สป.สธ.

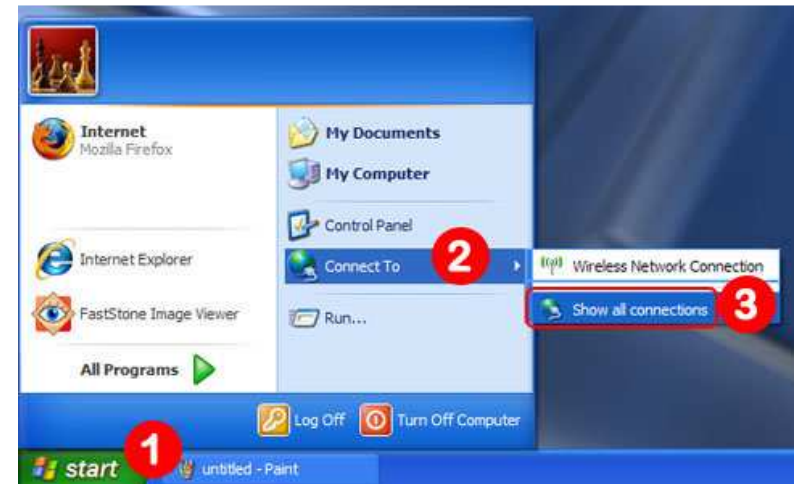
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ติดตั้งอุปกรณ์กระจายสัญญาณ Wireless LAN บริเวณอาคารสำนักงานปลัดกระทรวงสาธารณสุข รวมทั้งสิ้น 50 จุด โดยผู้ที่ใช้งาน Internet ผ่าน Wireless LAN จะต้องสมัครใช้งาน และได้รับ Username, Password ในการ Login เรียบร้อยแล้วจึงปฏิบัติดังต่อไปนี้

**สำหรับผู้ใช้งาน Windows XP**

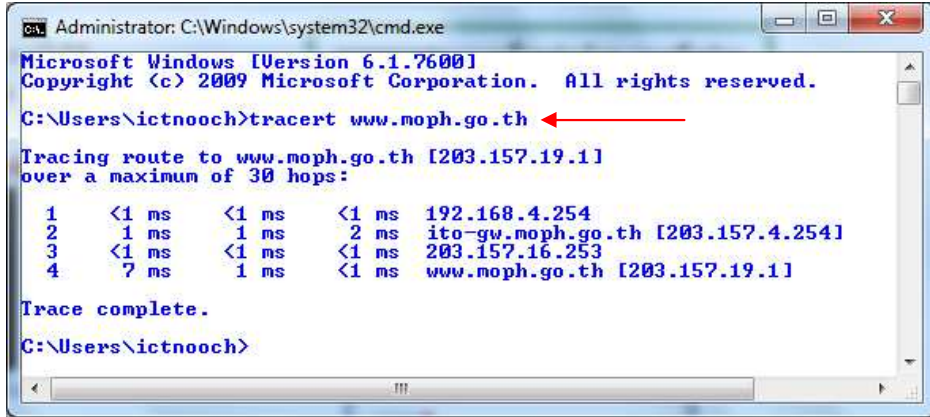
**1. ไปหน้า Wireless Network Connection**

เป็นการเข้าไปที่หน้าที่ใช้จัดการทำงาน Wireless Network ในเครื่องคอมพิวเตอร์ ซึ่งมีวิธีเข้า 2 วิธี คือ

วิธีที่ 1 • คลิกปุ่ม Start ไปที่ Connect TO แล้วคลิก Show all connections



4. กรณี ping เจอ Gateway แล้วแต่ยังเปิดหน้าเว็บไซต์ที่ต้องการไม่ได้ ให้ใช้คำสั่ง “tracert” ใน Dos Prompt เพื่อตรวจสอบเส้นทาง Network เช่น C:\>tracert -d www.moph.go.th



แต่ถ้า tracert ไม่เจอ จะแสดงข้อความเป็น \* \* \* Request time out ให้แจ้ง หมายเลข IP Address บรรทัดสุดท้าย แก่ผู้ดูแลระบบเพื่อเป็นข้อมูลในการตรวจสอบต่อไป

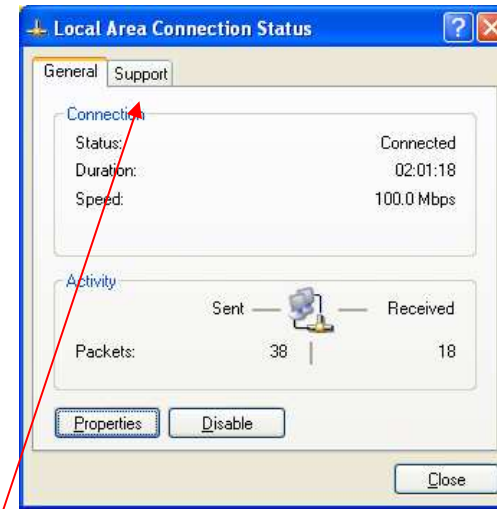
การตรวจสอบดังกล่าวข้างต้น เป็นเพียงวิธีการอย่างง่ายที่ User สามารถทำได้เอง เพื่อช่วยให้ช่างหรือเจ้าหน้าที่ ศทส. วิเคราะห์ปัญหาและแก้ไขได้อย่างถูกต้อง รวดเร็ว

\*\*\*\*\*

### การตรวจสอบการเชื่อมต่อกับระบบเครือข่าย

ในการตรวจสอบว่าเครื่องลูกข่ายที่ใช้งานอยู่นั้นเชื่อมต่อกับเครือข่ายเป็นปกติหรือไม่ จะใช้งาน Internet ได้หรือไม่นั้น มีวิธีการ ดังนี้

- สังเกตจากสัญลักษณ์ LAN ที่ Task bar ด้านล่างขวา ต้องไม่มีกากบาทแบบนี้ ถ้ามีกากบาท อาจเป็นไปได้ว่า สาย UTP(LAN) ที่เสียบต่อกับตัวเครื่องหลุดออก ให้ลองขยับแล้วเสียบกลับเข้าไปใหม่
- ตรวจสอบ IP Address ที่ได้รับ โดยดับเบิลคลิกที่ จะปรากฏหน้าต่าง



คลิกที่แท็บ Support จะแสดงหน้าต่าง บอกหมายเลข IP Address หมายเลข Subnet Mask และ หมายเลข Default Gateway ซึ่งหมายเลข IP Address ที่แจกอัตโนมัติ ให้ใช้ภายในอาคารสำนักงานปลัด ชั้นต้นด้วยเลข 172.2x.xx.xx แตกต่างกันไปตามแต่ละอาคาร ที่สำคัญ !! แต่ละเครื่องห้ามมีเลข IP Address ซ้ำกันเด็ดขาด !!

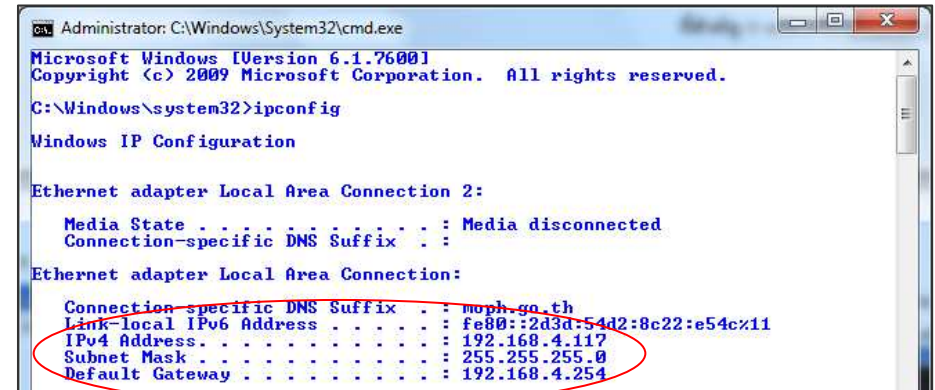
(10)



ตัวอย่าง เช่น

IP : 172.21.1.33  
 Subnet : 255.255.255.0  
 Gateway : 172.21.0.1

จากนั้นจะปรากฏหน้าจอ Dos Prompt แล้ว  
 -> พิมพ์คำสั่ง "ipconfig" และกดปุ่ม Enter



-> ดังภาพตัวอย่าง จะแสดงหมายเลขชุด IP Address

3. กรณีได้รับ IP แล้วแต่ยังใช้งาน Internet ไม่ได้ ให้ทำการตรวจสอบการเชื่อมต่อไปยัง Gateway ด้วยคำสั่ง "ping" ใน Dos Prompt

เช่น C:>ping 172.21.1.254

ถ้า ping เจอจะแสดงข้อความ Reply from เช่น

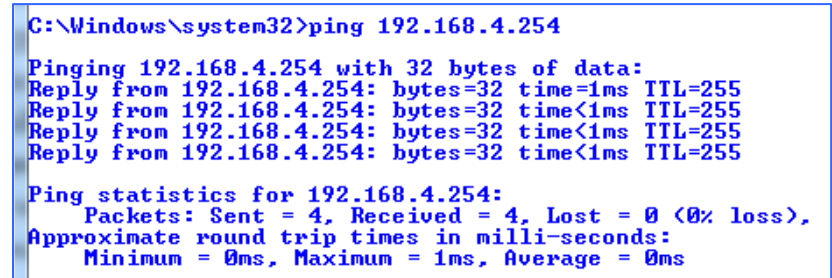
Reply from 172.21.1.254 bytes=33 time=1ms TTL=64 เป็นต้น แสดงว่า

เครือข่าย

ภายใน

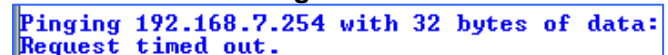
หน่วยงาน

เป็นปกติ



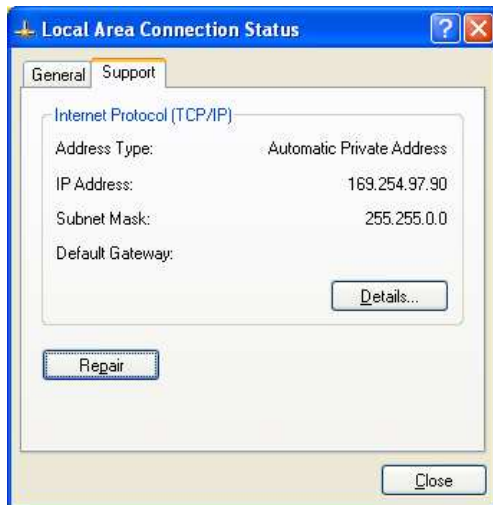
ถ้า ping ไม่เจอจะแสดงข้อความ Request time out แสดงว่าเครือข่ายภายใน

หน่วยงานขัดข้อง เช่น Switch Hang หรือสาย LAN ไม่ปกติ



ดังนั้น User จึงไม่ควรใส่ค่าหมายเลข IP Address เอง เพราะหากซ้ำกันจะส่งผลกระทบต่อการใช้งาน Network ของทั้งองค์กร

หากปรากฏหน้าต่างที่ไม่ได้รับหมายเลขชุดที่แจกให้ และไม่มีค่า Gateway ดังเช่นภาพนี้ แสดงว่า ไม่ได้รับ IP Address อาจต้อง ขยับสาย LAN เสียบใหม่ แล้วสั่ง Repair



เราสามารถตรวจสอบ IP Address ได้อีกวิธีหนึ่งโดยการใช้คำสั่ง ipconfig

-> คลิกปุ่ม Start -> Run -> พิมพ์คำสั่ง "cmd" แล้วกดปุ่ม Enter