

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดหาโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีลิขสิทธิ์ถูกต้อง ไว้ให้เครื่องลูกข่ายภายในสำนักงานปลัดกระทรวงสาธารณสุขติดตั้ง

MoPH Download page. - Windows Internet Explorer
 http://www.moph.go.th/download/

MoPH Download page.

MoPH Download
 - Software for MoPH member only -

Home WebMail Help

- 13 ฟอนต์แห่งชาติ (TH SarabunPSK Regular)
 - รวม font ทั้งหมด 13 fonts
 - เฉพาะชุด TH Sarabun font เท่านั้น
 - คู่มือการติดตั้ง การใช้งาน Font TH
 - ตัวอย่าง Font TH ได้ดังนี้
 - **ติดตั้ง TrendMicro OfficeScan [คู่มือการติดตั้ง] - โปรดอ่านคู่มือก่อนทำการติดตั้ง !!!**
 - เครื่องมือที่ใช้กำจัดไวรัส scan port 445 ***
 - รวมเว็บที่ให้บริการ Free Scan Virus Online ***
 - Bitdefender
 - Kaspersky
 - McAfee
 - Panda
 - Symantec
 - Trend Micro
 - เครื่องมือที่ใช้กำจัดไวรัส Worm & Virus Handdy drive ***
 - Panda USB Vaccine 1.0.0.50
 - Hacked By Godzilla!
 - Hacked By 8BITS
 - Hacked By 1BYTE
 - AVG Anti-Virus Free Edition 8.5.0.409 [65.3 MB]
 - AVG Anti-Virus Free Edition 7.5.472 [21.7 MB]
 - เครื่องมือที่ใช้กำจัดไวรัส Opaserv, Opasoft ***
 - เครื่องมือที่ใช้กำจัดไวรัสจาก Symantec
 - W32.Dumar@mm Removal Tool.
 - W32.Welchia.Worm Removal Tool. - remove ping bomb!!!
 - W32.Blastor.Worm Removal Tool.
 - W32.Mumu.B.Worm Removal Tool.
 - W32.Nimda.A@mm Removal Tool.
 - W32.Nimda.E@mm Removal Tool.
 - W32.Klez.gen@mm Removal Tool.
 - W32.Bugbear@mm Removal Tool.
 - W32.Brid.A@mm/W32.Funlove.4099 Removal Tool.
 - Other Removal Tool from Symantec.
 - ข้อมูลไวรัสจาก ThaiCERT(NECTEC).
 - Windows 2000 Service Pack 4
 - SQL Server 2000 Service Pack 3
 - Windows XP Service Pack 1a
 - Sasser Worm: Critical Security Patch for Windows XP / 2000 ถ้าถูกโจมตีเครื่องของคุณจะปิดเองอัตโนมัติภายใน 60 วินาที
 - Blaster Worm: Critical Security Patch for Windows XP ถ้าถูกโจมตีเครื่องของคุณจะปิดเองอัตโนมัติภายใน 60 วินาที เมื่อติดตั้ง patch เสร็จแล้วจะต้อง run fix W32.Blastor.Worm Removal Tool. ของ symantec ด้วย

และจัดทำคู่มือปฏิบัติสำหรับ User ในการใช้งานโปรแกรม Anti Virus ดังกล่าว

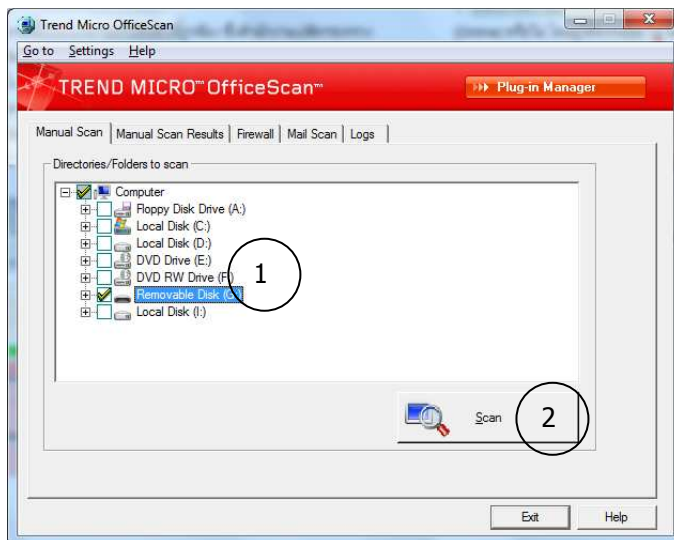
:: การใช้งานโปรแกรม TrendMicro OfficeScan ::

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

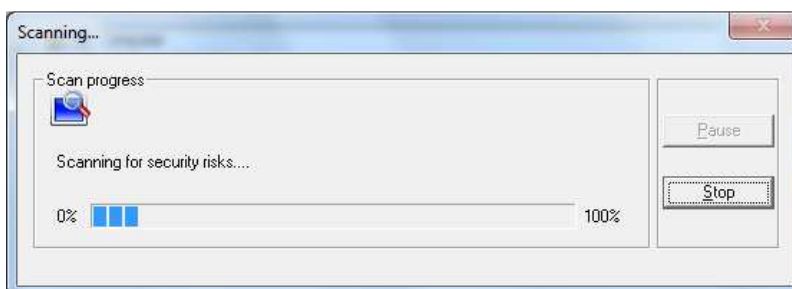


2. เปิดโปรแกรม OfficeScan Client จากเมนู Start -> All Programs -> Trend Micro OfficeScan Client

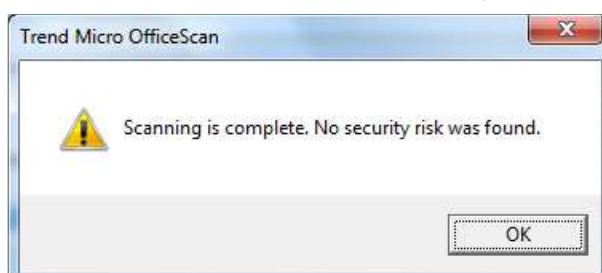
3. เลือก Drive โดยการคลิกให้มีเครื่องหมายถูก เพื่อสั่ง Scan Drive นั้นๆ



4. โปรแกรมจะทำการ Scan และทำการกำจัดไวรัสทันทีที่พบแบบอัตโนมัติ



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



6. คลิก Exit ปิดโปรแกรม

7. ทุกครั้งที่มีการเชื่อมต่อ Removable Drive เช่น Thumb Drive ที่ผ่านการใช้งานมาจากเครื่องอื่น ๆ ต้องทำการ Scan ก่อนเปิดใช้

การตรวจสอบการทำงานของโปรแกรม TREND MICRO OfficeScan

The screenshot displays the Trend Micro OfficeScan console. The main area shows a 'Summary' section with 'Activated services: Desktop/Server Antivirus, Desktop/Server Web Threat Protection, Firewall, Damage Cleanup Services'. Below this is an 'Outbreak Status' table:

Type	Current Outbreak	Last Outbreak	Reset
Virus/Malware	None	None	Reset
Spyware/Grayware	None	None	Reset
Firewall Violation	4/5/2010 14:14:54	4/5/2010 11:14:36	Reset

Next is the 'Networked Computers' section, which includes a 'Connection Status' pie chart (Online: 49, Offline: 74, Roaming: 0, Total: 123) and a 'Detection Status' table:

Type	Detections	Infected Computers
Virus/Malware	1852428	104
Spyware/Grayware	646	50

The bottom section, 'Update Status for Networked Computers (Online Clients: 49)', provides a detailed update progress table:

Category	Item	Current Version	Updated	Outdated	Update Rate
Antivirus	Virus Pattern	6.971.00	48	1	97%
	IntelliTrap Pattern	0.131.00	48	1	97%
	IntelliTrap Exception Pattern	0.527.00	48	1	97%
	Virus Scan Engine (32-bit)	9.100.1001	49	0	100%
	Virus Scan Engine (64-bit)	9.100.1001	0	0	0%
Anti-spyware	Spyware Pattern	9.13	48	1	97%
	Spyware Active-monitoring Pattern	0.913.00	48	1	97%
	Spyware Scan Engine (32-bit)	6.2.3010	49	0	100%
	Spyware Scan Engine (64-bit)	6.2.3010	0	0	0%
Damage Cleanup Services	Virus Cleanup Template	1076	48	1	97%
	Virus Cleanup Engine (32-bit)	6.2.1016	49	0	100%
	Virus Cleanup Engine (64-bit)	6.2.1016	0	0	0%

เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะทำการ Login Admin เข้าสู่โปรแกรมส่วนบริหารจัดการ เพื่อตรวจสอบดูว่า โปรแกรมยังทำงานเป็นปกติอยู่หรือไม่ มีการ Update รายชื่อไวรัสชนิดใหม่ๆ อย่างต่อเนื่องและเป็นปัจจุบันหรือไม่ และจำนวนเครื่องลูกข่ายที่ใช้งานมีจำนวนเท่าไร ยังคงเข้ามา Update ได้เป็นปกติหรือไม่

ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มอบหมายให้เจ้าหน้าที่ดำเนินการตรวจสอบอย่างน้อยสัปดาห์ละ 1 ครั้งตามแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายเทคโนโลยีสารสนเทศ ปีงบประมาณ พ.ศ.2553
