วิธีการเลี่ยงไวรัสจากการใช้งานอุปกรณ์ประเภท

USB Mass Storage Device

เทคโนโลยีทางด้านการจัดเก็บข้อมูลแบบส่วนบุคคล คงจะเลี่ยงไม่ได้ที่จะต้องพูดถึงอุปกรณ์จัดเก็บมูลที่เรียกกันว่า USB Mass Storage Device หรือที่แปลตรงตัวก็คือ อุปกรณ์ที่ใช้จัดเก็บข้อมูลจำนวนมากผ่านทางช่อง USB ของเครื่องคอมพิวเตอร์หรือแล็บทอป ชื่อที่ใช้เรียก อาจแตกต่างกันไปตามผู้ผลิตที่ต้องการสร้างให้ชื่อเป็นเหมือนตัวแทนของอุปกรณ์ประเภทนี้ เช่น Thumb Drive, Handy Drive หรือ USB Flash Drive เป็นต้น อุปกรณ์เหล่านี้ ได้ให้ความสะดวกสบายแก่ผู้ใช้งานระบบคอมพิวเตอร์เป็นอย่างมาก และหากเทียบกับอุปกรณ์ที่ใช้จัดเก็บข้อมูลส่วนบุคคลเช่นเดียวกันอย่างแผ่น Diskette ที่เคยเป็นที่นิยมและเป็นทางเลือกเดียวในการจัดเก็บข้อมูลเพื่อพกพาในอดีต ก็จะพบว่า USB Storage Disk จะให้ความจุข้อมูลและความเร็วในการคัดลอกไฟล์งานต่าง ๆ ได้เร็วกว่าหลายเท่าตัวทีเดียว อุปกรณ์ที่อยู่ในข่ายนี้มีด้วยกันหลายชนิด เช่น Harddisk ภายนอกที่ต่อเชื่อมกับคอมพิวเตอร์ผ่านช่อง USB หรืออุปกรณ์ที่เรียกว่า USB Flash Disk ซึ่งทำหน้าที่จัดเก็บข้อมูลได้เช่นกัน แต่จะมีขนาดเล็กกว่าและความจุจะน้อยกว่า เป็นต้น

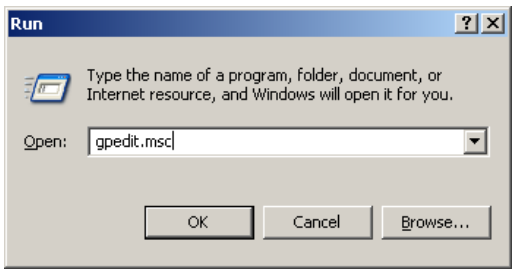
เมื่อมองดูความสะดวกสบายที่ได้รับแล้ว บวกกับราคาที่ไม่สูงนัก กลุ่มคนทำงานหรือนักศึกษาและนักเรียนตามโรงเรียน จึงนิยมหามาใช้งานกันอย่างแพร่หลาย แต่สิ่งที่ตามมาจากความสะดวกสบายดังกล่าว ก็คือ เรื่องของการติดไวรัสคอมพิวเตอร์จากแหล่งที่มาต่าง ๆ ที่ตัว USB Flash Disk ได้ต่อเชื่อม และจากความซับซ้อนของตัวไวรัสใหม่ ๆ ที่มีการแพร่ระบาดอย่างรุนแรงในปัจจุบัน ทำให้เราไม่สามารถล่วงรู้ได้เลยว่ามีการติดไวรัสเข้ามาใน USB Flash Drive ของเราแล้ว และด้วยความไม่รู้นี่เอง ทำให้เราอาจเป็นได้ทั้งเหยื่อของไวรัสและเป็นผู้แพร่กระจายไวรัสโดยรู้เท่าไม่ถึงการถึงแม้ว่าในปัจจุบัน โปรแกรมสำหรับตรวจจับไวรัสจะมีหลายรายที่ออกผลิตภัณฑ์ที่สามารถตรวจจับไวรัสที่ติดมากับ USB Flash Disk ของเราได้ แต่เราจะไว้ใจระบบป้องกันไวรัสที่เรามีอยู่ได้มากน้อยซักแค่ไหน และเราจะฝากความหวังเรื่องความปลอดภัยเพียงอย่างเดียวไม่ได้ ฉะนั้น เราจึงควรเรียนรู้และจำจดวิธีการหลีกเลี่ยงไวรัสที่ติดมากับอุปกรณ์ USB Flash Disk ไว้ เพื่อป้องกันภัยก่อนที่ความเสียหายจะมาถึงเรา

วิธีการปิดการทำงานอัตโนมัติของอุปกรณ์ USB Flash Disk

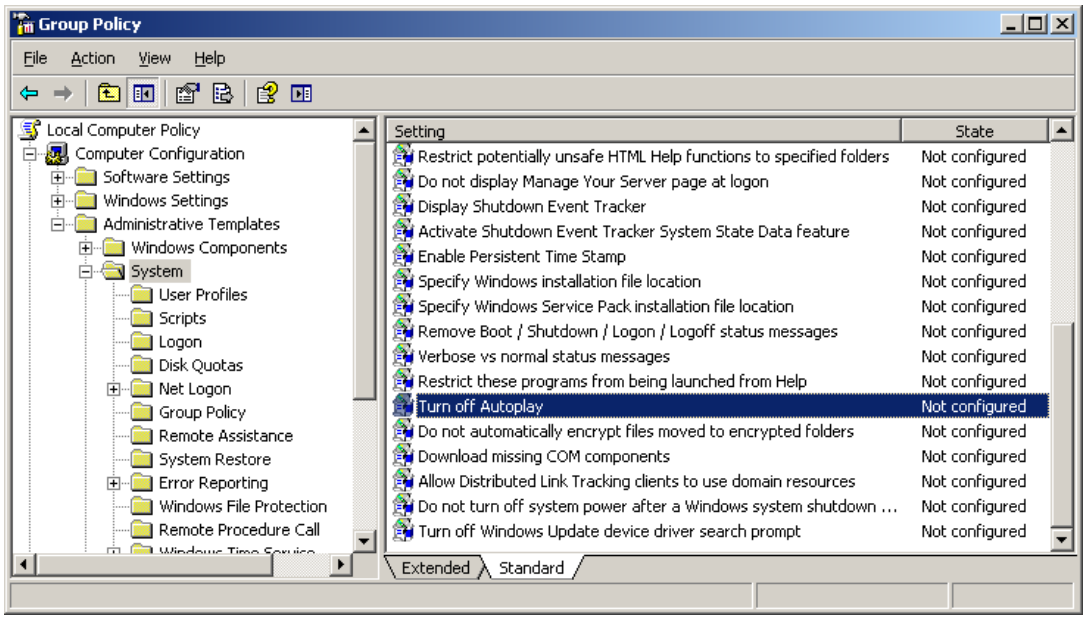
เครื่องคอมพิวเตอร์เกือบทั้งหมดที่ใช้ระบบปฏิบัติการ Windows 98, ME, XP, 2000, 2003 หรือใหม่กว่า มักจะอนุญาตให้เรียกใช้โปรแกรมโดยอัตโนมัติเมื่อนำอุปกรณ์ USB Flash Disk มาต่อเชื่อมกับ

คอมพิวเตอร์ของเรา ซึ่งผลเสียที่ตามมาคือ การเรียกโปรแกรมที่อาจเป็นไวรัสให้ทำงานโดยไม่รู้ตัว วิธีที่ดีที่สุดและได้ผลตรงประเด็นคือ การปิดการทำงานอัตโนมัติดังกล่าวเสีย ซึ่งสามารถทำได้หลายวิธีด้วยกัน ดังนี้

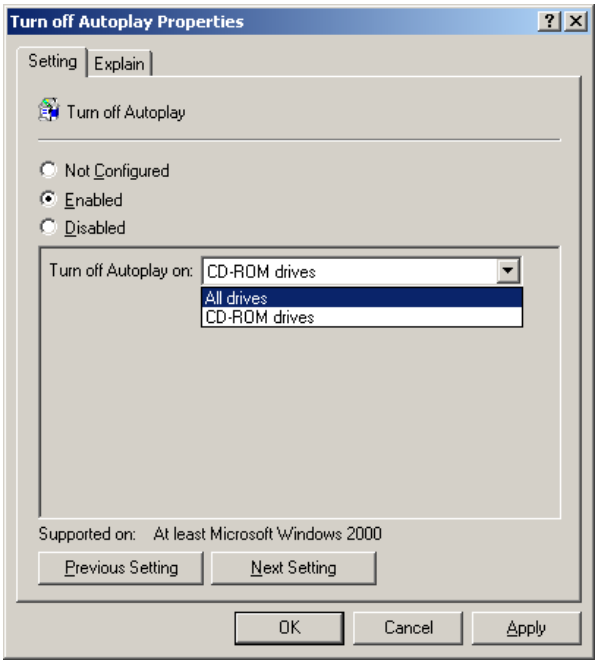
1. ปิดด้วย GPEDIT
   - คลิกที่ปุ่มเมนู Start -> Run
   - พิมพ์คำสั่ง gpedit.msc



   - ที่หน้าต่าง Group Policy สังเกตที่ด้านซ้าย แล้วเลือกไปที่เมนู Computer Configuration ->Administrative Templates -> System



   - ดับเบิลคลิกที่ Turn off Autoplay เพื่อเข้าสู่หน้าต่าง Turn off Autoplay properties และเลือก Enable จากนั้น ในกรอบที่อยู่ด้านล่าง หัวข้อ Turn off Autoplay On: แล้วจึงเลือกเป็น All Drive

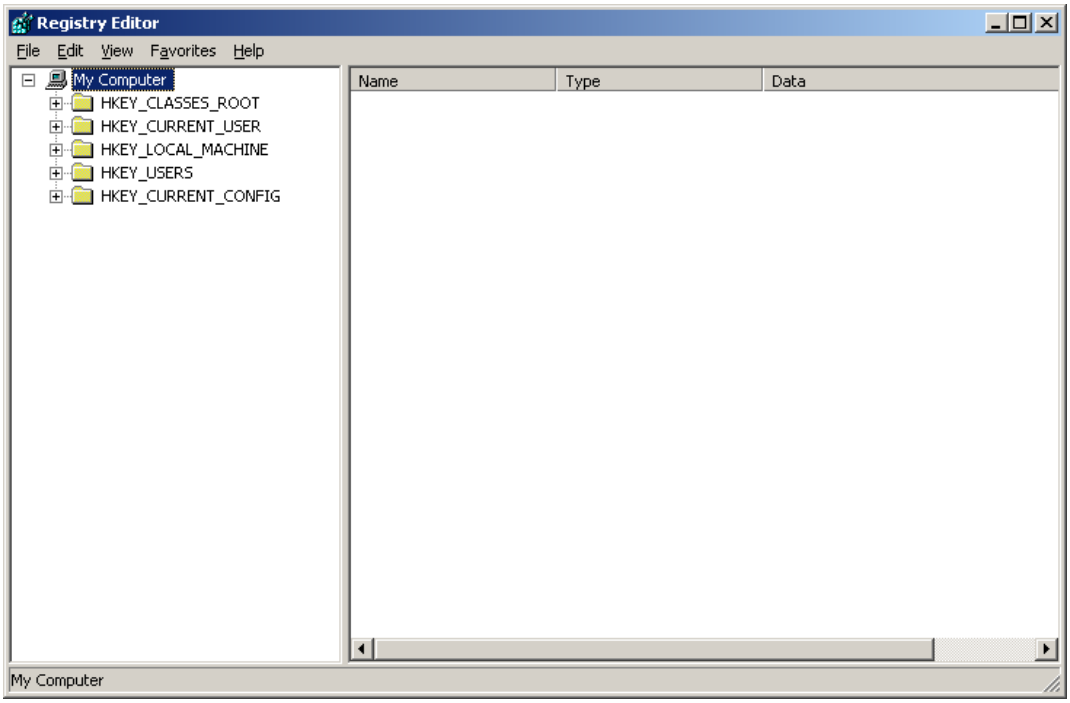


- จากนั้น คลิกปุ่ม OK แล้วปิดหน้าต่างของ Group Policy Editor

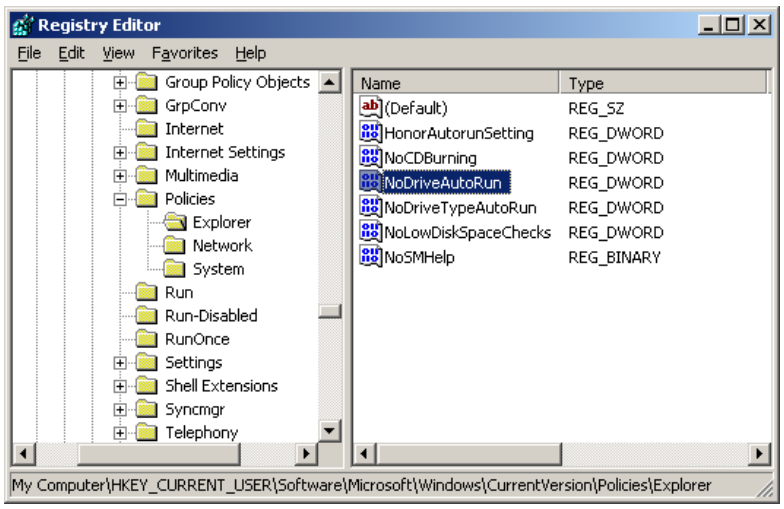
2. ปิดด้วย registry

   วิธีนี้ จะค่อนข้างยุ่งยากและมีความเสี่ยงหากเกิดความผิดพลาดในขั้นตอนการทำ จึงควรดำเนินขั้นตอนต่าง ๆ อย่างรอบคอบรัดกุม

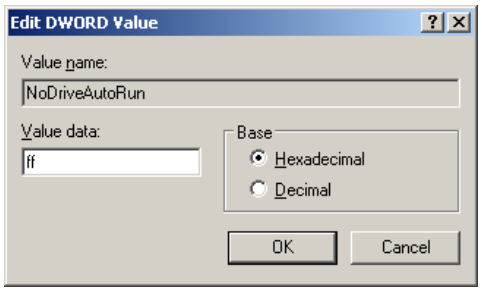
   - คลิกที่ ปุ่มเมนู Start->Run
   - พิมพ์คำสั่ง regedit จะปรากฏหน้าต่าง Registry Edit ดังรูป



- ที่ panel ด้านซ้าย เลือก HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer



- ดับเบิลคลิกที่ key “NoDriveAutoRun” เพื่อกรอกค่า ff (เลขฐานสิบหก)

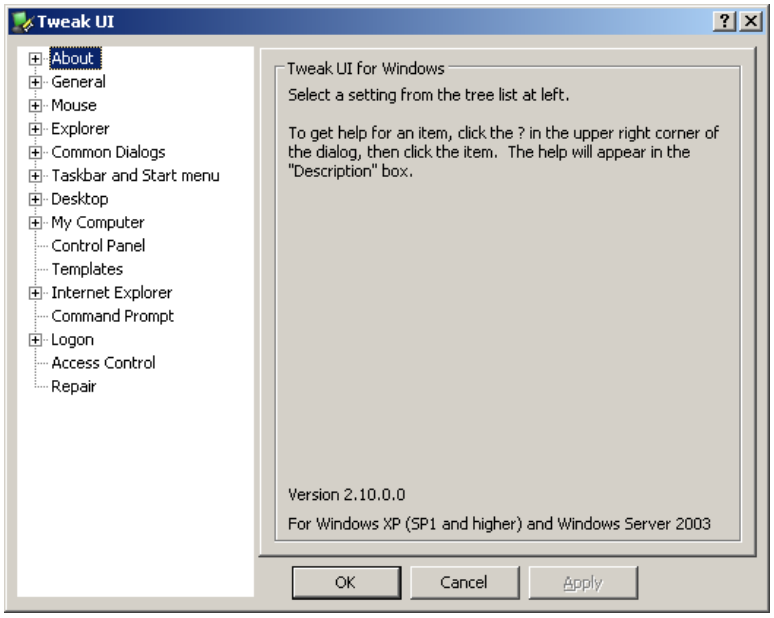


- คลิก OK และปิดหน้าต่างโปรแกรม Registry Editor จากนั้นจึง restart Windows เพื่อทดลองผล

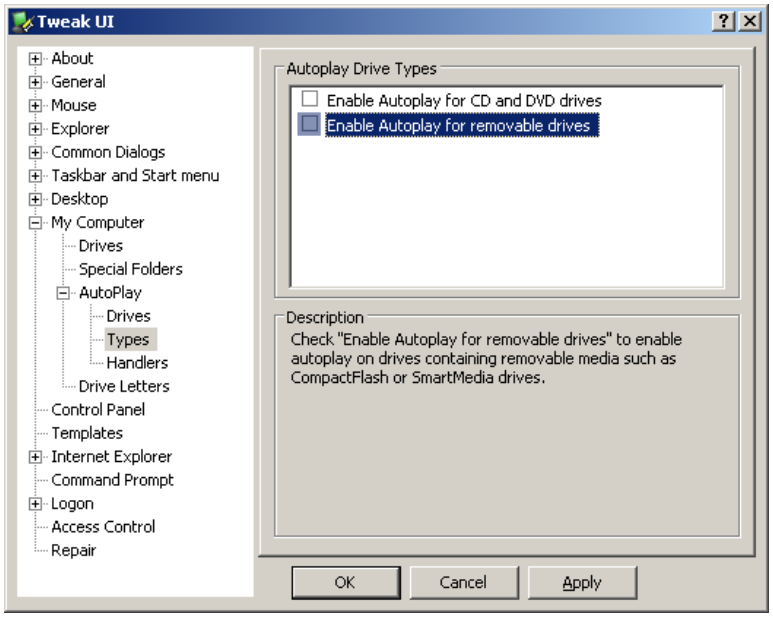
3. ปิดโดยใช้โปรแกรม TweakUI

โปรแกรม TweakUI เป็นโปรแกรมที่ทางบริษัท Microsoft ได้เผยแพร่ให้สามารถ download ใช้งานได้ฟรี และใช้งานได้ไม่ยาก ทำความเข้าใจได้ง่ายกว่ามาก ตัว TweakUI เองได้รวมวิธีการปรับแต่ง Windows อย่างง่าย ๆ ไว้มากมาย หนึ่งในนั้นคือ ความสามารถในการปิดการทำงานแบบอัตโนมัติเมื่อใส่แผ่นซีดีและอุปกรณ์ USB Flash Disk ด้วย ซึ่งการใช้โปรแกรม TweakUI จะช่วยลดขั้นตอนที่ยุ่งยากได้มาก และมีความเสี่ยงต่อความผิดพลาดได้น้อยกว่าสองวิธีข้างต้น สำหรับขั้นตอนในการปิดการทำงานแบบอัตโนมัติ มีดังนี้

- คลิกที่เมนู Start->Program->Power Toys For Windows XP
- เลือก TweakUI จะปรากฏหน้าต่าง TweakUI ขึ้นมา



- ที่ panel ด้านซ้ายมือ เลือก My Computer->AutoPlay->Types ที่ด้านขวามือจะปรากฏกรอบ Autoplay Drive Types ให้คลิกซ้ำเพื่อไม่เลือก Enable Autoplay for CD and DVD Drives ถ้าไม่ต้องการให้แผ่น CD DVD ทำงานแบบอัตโนมัติเมื่อใส่แผ่น Enable Autoplay for removable drives ถ้าไม่ต้องการให้อุปกรณ์ USB Flash Disk ทำงานโดยอัตโนมัติเมื่อใส่แผ่น



- จากนั้นกดปุ่ม OK เพื่อปิดหน้าต่างนี้

<u>ตรวจจับไวรัสด้วยโปรแกรมป้องกัน autorun.inf</u>

อีกสิ่งหนึ่งนอกเหนือจากที่กล่าวมาในข้างต้น หากเราจำเป็นจะต้องเชื่อมต่ออุปกรณ์ USB Flash Disk แล้ว เราควรติดตั้งโปรแกรมที่ทำหน้าที่ตรวจจับไวรัสหรือเตือนเรากรณีที่มีไวรัสฝังตัวอยู่ในอุปกรณ์ โปรแกรมตัวหนึ่งที่ขอแนะนำคือ USB 1.3 ซึ่งคอยทำหน้าที่ตรวจหาไฟล์ที่ชื่อ autorun.inf ที่ไวรัสส่วนใหญ่นิยมฝังตัวไฟล์นี้ไว้เพื่อให้ผู้ใช้เรียกไวรัสโดยไม่รู้ตัว โปรแกรม USB เป็นโปรแกรมที่ใช้งานง่าย ไม่รบกวนผู้ใช้ สามารถหา download ได้ที่ www.sputnik70.narod.ru ส่วนวิธีการใช้งานง่าย ๆ มีดังนี้

1. เมื่อ download ไฟล์มาแล้ว ให้คลาย zip ไฟล์ เก็บไว้ใน folder ชื่อ USB เช่น C:\USB

2. เรียกใช้ไฟล์ชื่อ USB.exe จะปรากฏไอคอนที่ system tray ดังนี้
3. คลิกเมาส์ปุ่มขวาที่ไอคอน เลือกเมนู Setting->Autostart เพื่อให้โปรแกรมทำงานทันทีที่เปิดเครื่องคอมพิวเตอร์
4. คลิกเมาส์ปุ่มขวาอีกครั้งที่ไอคอนเดิม เลือกเมนู Action->Disable Autorun for all system drive เพื่อให้โปรแกรมทำการยกเลิกการทำงานแบบอัตโนมัติทั้งหมดของทั้ง USB Flash Drive และ CD/DVD Drive
5. คลิกเมาส์ปุ่มขวาอีกครั้ง และไปที่เมนู Action->Check Local Drives เป็นการสั่งให้โปรแกรมตรวจหาไฟล์ autorun.inf ซึ่งถ้าตรวจเจอก็จะทำการเปลี่ยนชื่อ ไม่ให้ใช้งานได้อีก

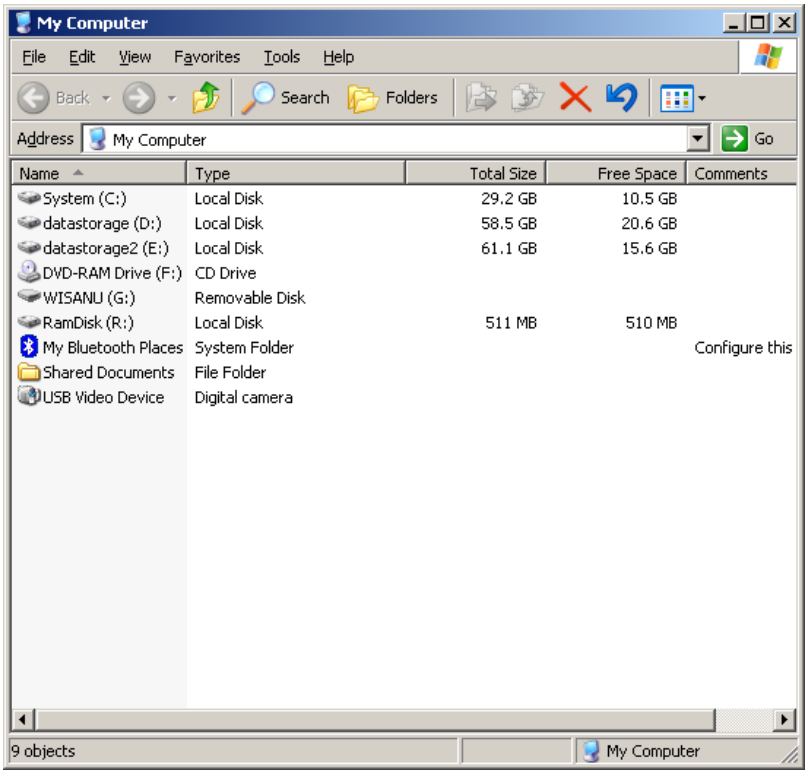
นอกจากนี้ ยังมีโปรแกรมที่ทำหน้าที่ป้องกันไวรัสจากอุปกรณ์ USB Flash Disk อีกมากมาย เช่น Panda USB Vaccine เป็นต้น ซึ่งมีให้ download ฟรี ในอินเตอร์เน็ต ทั้งนี้ ควรศึกษาโปรแกรมต่าง ๆ หลาย ๆ โปรแกรม เพื่อให้ได้โปรแกรมที่เหมาะกับการใช้งานของเราและเหมาะสมกับคอมพิวเตอร์ให้มากที่สุดด้วย

<u>ตรวจจับไวรัสที่แฝงมากับอุปกรณ์ USB Flash Disk ด้วยโปรแกรมตรวจจับไวรัส</u>

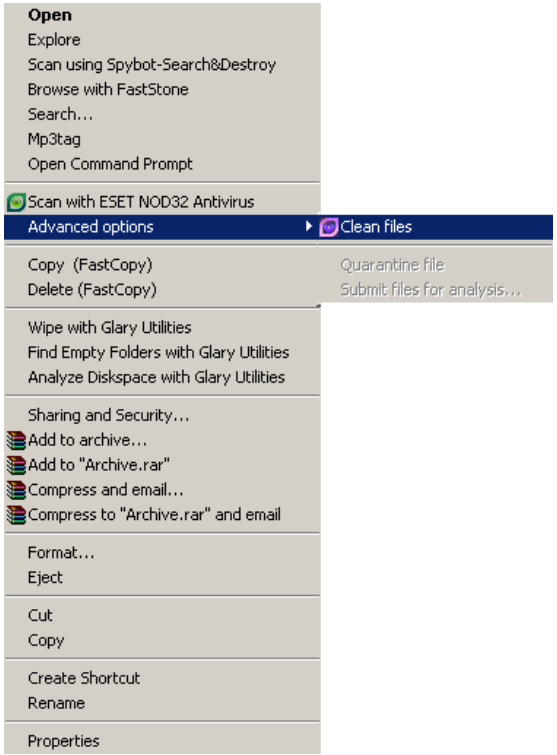
การป้องกันด้วยวิธีปิดการทำงานอัตโนมัติด้วยวิธีต่าง ๆ ที่กล่าวมาข้างต้น ก็เป็นขั้นตอนที่ช่วยเสริมไม่ให้ไวรัสเข้ามาก่อความเสียหายให้แก่ระบบของเรา แต่ถ้าการแพร่ระบาดของไวรัสและความซับซ้อนมากขึ้น ยังมีอยู่อย่างต่อเนื่อง เราก็จำเป็นจะต้องพึ่งพาเครื่องมืออย่างโปรแกรมตรวจจับและป้องกันไวรัสเข้ามาช่วยเหลือ เพื่อเพิ่มความรัดกุม ให้กับการป้องกันตัวจากภัยของไวรัส การใช้งานโปรแกรมตรวจจับไวรัสเพื่อตรวจหาไวรัสที่แฝงตัวมากับอุปกรณ์ USB Flash Disk นั้น มีขั้นตอนและวิธีการที่แตกต่างกันไปตามแต่

ผู้ผลิตจะกำหนด ดังนั้น จึงของยกตัวอย่างโปรแกรมที่ได้รับความนิยมตัวหนึ่ง นั่นคือ NOD32 โดยขั้นตอนการใช้งานก็ไม่ยุ่งยากนัก คือ

1. เมื่อเชื่อมต่ออุปกรณ์ USB Flash Disk เข้ากับคอมพิวเตอร์ของเราแล้ว ให้ดับเบิลคลิกที่ My

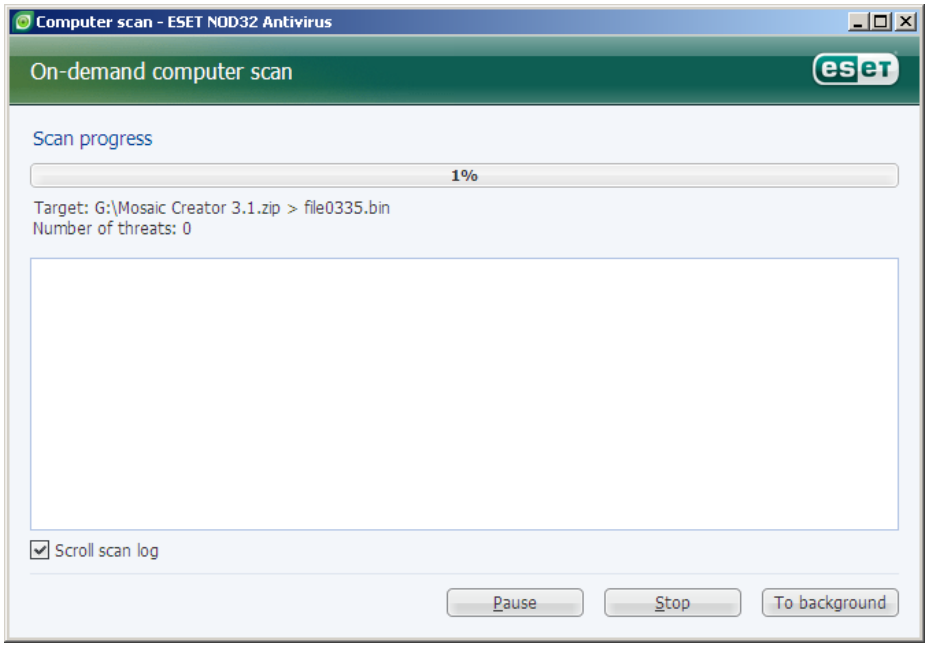


Computer



1. คลิกเมาส์ปุ่มขวาเพื่อเลือกเมนู Advanced options->Clean Files

4. จากนั้น จะปรากฏหน้าต่าง ของโปรแกรม NOD32 และจะทำการตรวจจับไวรัสให้เราโดย

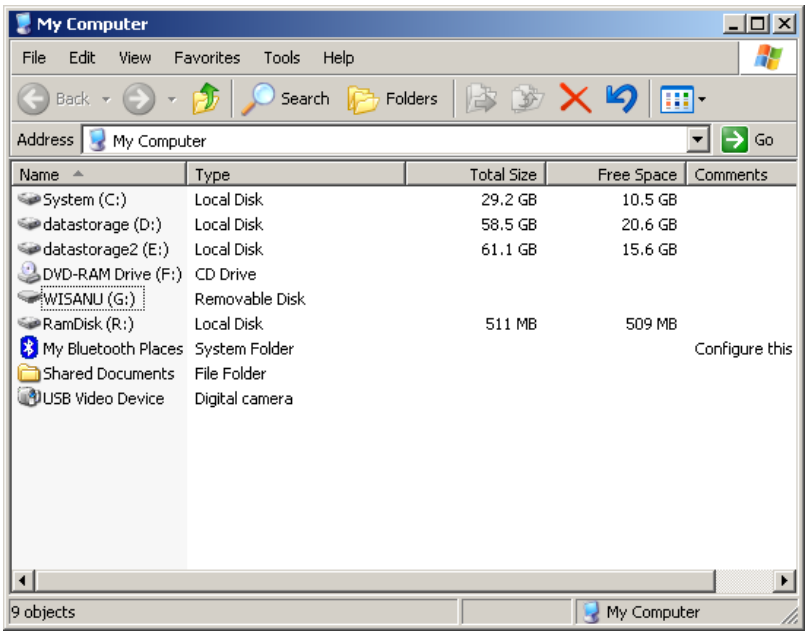


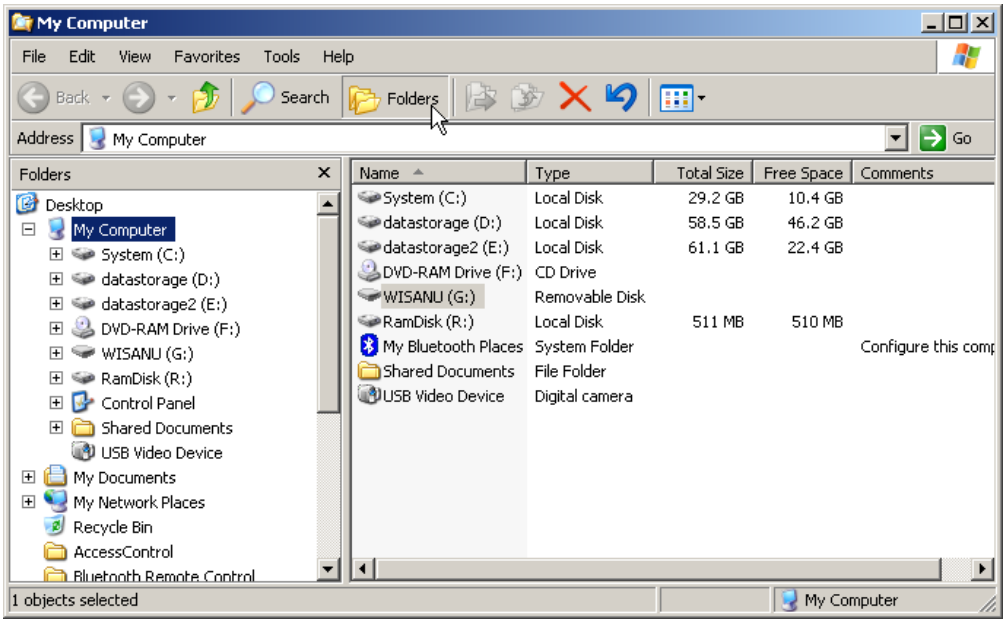
อัตโนมัติ

<u>วิธีการเปิด flash drive ด้วย explorer ให้ปลอดภัย</u>

ในบางครั้ง หากมีความจำเป็นจะต้องใช้งาน USB Flash Disk ของบุคคลอื่นกับเครื่องคอมพิวเตอร์ของเรา และเราไม่สามารถที่จะทำการตรวจจับไวรัสที่อาจมีอยู่ในอุปกรณ์ USB Flash Disk ของบุคคลด้วยโปรแกรมใด ๆ ได้ เรายังมีอีกวิธีหนึ่งที่จะสามารถเลี่ยงการติดไวรัสจากอุปกรณ์ USB Flash Disk ที่ไม่น่าไว้วางใจนั้นได้ ซึ่งทำได้ไม่ยากแต่ได้ผล ดังนี้

1. เมื่อต่อเชื่อมอุปกรณ์ USB Flash Disk กับเครื่องคอมพิวเตอร์แล้ว ให้ดับเบิลคลิกที่ My Computer

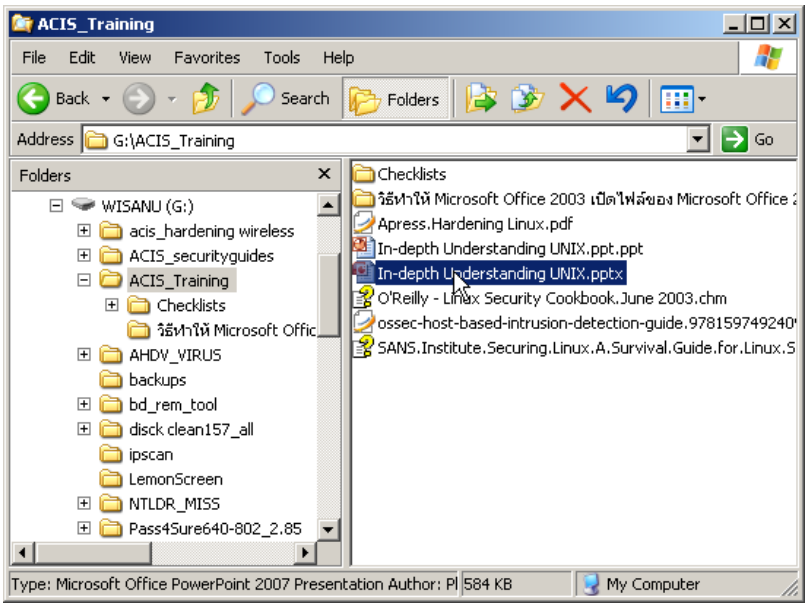




2. คลิกที่ปุ่ม Folder ที่อยู่ด้านบน จะปรากฏ panel ด้านซ้ายมือขึ้นมา

3. ที่ panel ด้านซ้ายมือ จะแสดงชื่อ ไดร์ฟ และ folder ย่อย ๆ ลงไปตามลำดับ และด้านขวามือ จะแสดง folder ย่อย ที่อยู่ภายใต้ไดร์ฟและ folder ที่เราเลือกด้านซ้ายมือ

4. ให้ใช้วิธีการเลือก ไดร์ฟหรือ folder ย่อย ที่ด้านซ้ายมือ แทนการดับเบิลคลิกที่ไดร์ฟหรือ folder ที่ panel ด้านขวามือ โดยเราจะดับเบิลคลิกใน panel ด้านขวามือก็ต่อเมื่อ เราพบไฟล์ที่เราต้องการแล้วจริง ๆ ซึ่งวิธีนี้ จะเลี่ยงการเผลอดับเบิลคลิกเพื่อเรียกให้ไวรัสทำงานโดยไม่ได้ตั้งใจได้



จากขั้นตอนทั้งหมดที่ได้กล่าวมา ถึงแม้ว่าจะมีขั้นตอนและวิธีมากมาย ที่เราสามารถเลี่ยงการติดไวรัสจากอุปกรณ์ USB Flash Disk ได้ก็ตาม แต่พึงระลึกไว้เสมอว่า ขั้นตอนดังที่กล่าวมาในข้างต้น เป็นเพียงวิธีในการหลีกเลี่ยงจากติดไวรัสจากอุปกรณ์ USB Flash Disk เท่านั้น ไม่ใช่วิธีการทำให้เครื่องคอมพิวเตอร์ของเราและอุปกรณ์ของเราปราศจากไวรัสโดยสิ้นเชิง ทั้งนี้ เนื่องจากไวรัสมีวิวัฒนาการไปตามเทคโนโลยีที่เปลี่ยนแปลงอยู่ตลอดเวลา หมายความว่า ความซับซ้อนของปัญหาไวรัสก็จะยิ่งมีมากขึ้นเป็นลำดับเช่นกัน ความจำเป็นที่จะต้องปรับเปลี่ยนพฤติกรรมของผู้ใช้จึงเป็นสิ่งที่เลี่ยงไม่ได้ และไม่ว่าการปรับเปลี่ยนพฤติกรรมนั้นจะออกมาในรูปแบบใด สิ่งที่เราจำเป็นต้องระลึกไว้ เพื่อจะได้ปรับใช้ให้สอดรับกับการเปลี่ยนแปลงของปัญหาไวรัส สามารถสรุปได้พอสังเขปดังนี้

1. ให้คิดเสมอว่า Flash Drive ไม่ว่าจะของใครก็ตามไม่ปลอดภัย และอาจแพร่กระจายไวรัสมาสู่เราได้ทุกเมื่อ
2. หมั่น update โปรแกรมตรวจจับไวรัสของเราให้ทันสมัยเสมอ รองรับไวรัสใหม่ ๆ ที่แพร่ระบาดอยู่ในปัจจุบัน
3. พยายามไม่อนุญาตให้ผู้อื่นเข้ามาใช้เครื่องคอมพิวเตอร์ของเราโดยไม่ที่เราไม่ได้รับรู้ และต้องบังคับให้ผู้ที่จะเข้ามาใช้เครื่องคอมพิวเตอร์ของเราร่วมกับอุปกรณ์ USB Flash Disk ต้อง scan virus ด้วยโปรแกรมตรวจจับไวรัสก่อนเสมอ

4. หมั่น scan virus ของเครื่องเราเองเป็นประจำ เพื่อให้มั่นใจว่า คอมพิวเตอร์ของเราก็จะไม่เป็นแหล่งแพร่ระบาดของไวรัสไปสู่ภายนอกเช่นกัน
5. หมั่นสังเกตความเปลี่ยนแปลงและจดบันทึกความผิดปกติใด ๆ ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ของเรา เพราะหากเป็นอาการของไวรัส จะได้สามารถนำข้อมูลที่จดบันทึกไปเป็นเบาะแสในการระวังและป้องกันปัญหาที่เกิดจากไวรัสได้ในคราวต่อ ๆ ไป
6. ควรจดจำและปฏิบัติตามวิธีหลีกเลี่ยงไวรัสที่เกิดจาก USB Flash Disk จนเป็นนิสัย เพราะจะช่วยให้เครื่องคอมพิวเตอร์ของเราปราศจากไวรัส และลดการแพร่ระบาดของไวรัสในวงกว้างได้อีกด้วย
7. ติดตามข่าวสารการแพร่ระบาดของไวรัสอย่างต่อเนื่อง เพื่อที่จะได้รู้เท่าทันปัญหาไวรัสก่อนปัญหาจะมาถึงเรา

แม้ว่าเราจะไม่ใช่คนในสายไอที แต่เรื่องของไอทีเป็นเรื่องที่ใกล้ตัว และจะกลายเป็นส่วนหนึ่งของชีวิตเรา ตราบใดที่เรายังใช้คอมพิวเตอร์อยู่สม่ำเสมอ ฉะนั้น อย่าปล่อยให้ไอทีเป็นที่ถกเถียงกัน ว่าเป็นเรื่องของคนยุคไหน แต่จงจับตาดูอย่างเข้าใจ เพื่อไม่ให้ยุคของเราถูกกลืนไปกับกาลเวลา

<u>ที่มา</u>

"How to disable the Autorun functionality in Windows", Microsoft,
http://support.microsoft.com/kb/967715