บทที่ ๒
รู้ให้เท่าทันเพื่อป้องกันไวรัสคอมพิวเตอร์

จากที่ได้ทำความรู้จักกับโปรแกรมที่ประสงค์ร้ายต่อคอมพิวเตอร์มาแล้ว และทำความเข้าใจกันแล้วว่าต่อไปนี้ขอเรียกว่าไวรัสคอมพิวเตอร์ เพื่อให้ไปในทิศทางเดียวกัน เพราะไม่เช่นนั้นเวลาจะกล่าวถึงการป้องกันและกำจัดไวรัสคอมพิวเตอร์ ก็ต้องเป็นการป้องกันและกำจัดหนอนคอมพิวเตอร์ การป้องกันและกำจัดสปายแวร์คอมพิวเตอร์ หรือการป้องกันและกำจัดโทรจันคอมพิวเตอร์ ซึ่งจะทำให้ยุ่งยากและดูสับสน เพราะการเรียนรู้นี้ก็เพื่อที่จะป้องกันและกำจัดโปรแกรมที่ประสงค์ร้ายจำพวกนี้ออกจากคอมพิวเตอร์อยู่แล้ว

คำพูดที่ว่า “รู้เขารู้เรารบร้อยครั้งชนะทั้งร้อยครั้ง” ยังสามารถใช้ได้เสมอ ถึงแม้เราจะรบกับไวรัสคอมพิวเตอร์ รู้เขารู้เรารบร้อยครั้งชนะสักห้าสิบครั้ง ก็คุ้มแล้ว ที่เหลือถ้าเกินปัญญาและความสามารถก็ฟอร์แมทติดตั้งโปรแกรมใหม่ก็สิ้นเรื่อง ดีกว่าเรารบร้อยครั้งแพ้ทุกครั้งตั้งมากมาย เพราะทุกวันนี้ ปัญหาไวรัสคอมพิวเตอร์เกิดขึ้นกับผู้ใช้คอมพิวเตอร์ทุกคน ดังนั้นการได้เรียนรู้หรือรู้เท่าทันไวรัสคอมพิวเตอร์ แล้วใช้ความสามารถหนึ่งสมองและสองมือ ที่จะได้รับต่อไปนั้น มาใช้ในการป้องกันและกำจัดไวรัสคอมพิวเตอร์ด้วยตนเอง ดีกว่าจะอาศัยโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์เสียอีก (ไม่เสียเงินในการซื้อหาโปรแกรมป้องกันไวรัสทุกปี)

ถ้าเราจะเปรียบเทียบคอมพิวเตอร์กับคน แล้วลองนึกดูว่าคนเรานั้นถ้าอยากให้มีชีวิตยืนยาวมีสุขภาพดี ทั้งร่างกายและจิตใจนั้น ก็ต้องหมั่นดูแลสุขภาพและร่างกาย เช่น การออกกำลังกาย การเลือกรับประทานอาหารที่ดีต่อสุขภาพและร่างกาย ชีวิตคนเราก็สามารถมีชีวิตที่ยืนยาวได้แล้ว และถ้าเราอยากให้คอมพิวเตอร์มีสภาพของเครื่องที่ดี และการใช้งานที่ยืนยาว เราก็ต้องทำคล้ายกับคนเรา ถึงแม้เราจะให้คอมพิวเตอร์มาออกกำลังกายไม่ได้ แต่เราก็สามารถดูแลและป้องกันคอมพิวเตอร์ได้เพื่อที่จะได้มีภูมิคุ้มกันไวรัสคอมพิวเตอร์ เช่นเราสามารถดูแลคอมพิวเตอร์โดยไม่ลงโปรแกรมที่ไม่น่าไว้ใจ เข้าไปในคอมพิวเตอร์ *(ส่วนมากโปรแกรมละเมิดลิขสิทธิ์ที่ต้อง Crack ซึ่งโปรแกรมพวกนี้จะมีไวรัสคอมพิวเตอร์มาด้วย)* ก็สามารถทำให้คอมพิวเตอร์มีสุขภาพที่ดีได้ เพราะการลงโปรแกรมเข้าไปในคอมพิวเตอร์ก็เปรียบเสมือนคอมพิวเตอร์ได้อาหารเข้าไป ถ้าโปรแกรมที่ลงเชื่อถือได้คอมพิวเตอร์ของเราก็จะมีสุขภาพที่ดี แต่ถ้าโปรแกรมที่ลงไปในคอมพิวเตอร์ไม่ดีเมื่อเข้าไปอยู่ในคอมพิวเตอร์ก็จะทำให้คอมพิวเตอร์มีสภาพที่อ่อนแอได้ หรืออาจจะมีสภาพเหมือนคนอมโรคที่พร้อมจะแพร่เชื้อได้อีกด้วย

ดังนั้นในบทนี้จะแนะนำวิธีการที่ผู้เขียนใช้เป็นเทคนิคในการต่อกรกับไวรัสคอมพิวเตอร์

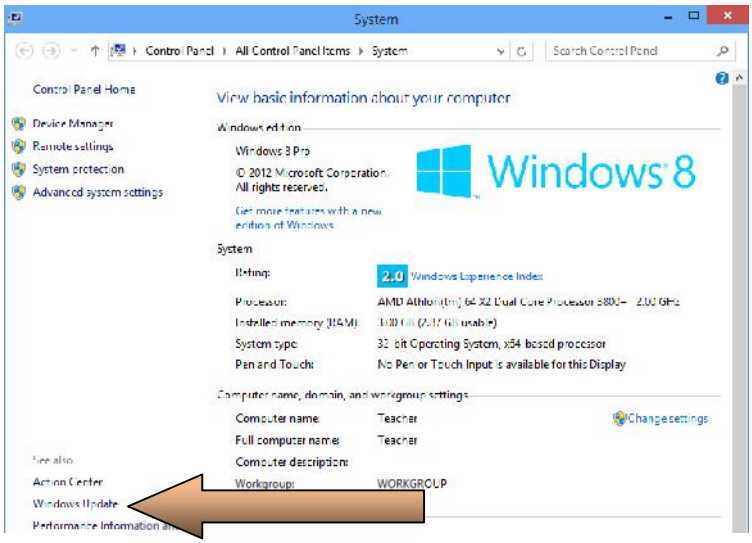
๑. เตรียมพร้อมสถานการณ์

๑.๑ การทำ Image โปรแกรม

การใช้คอมพิวเตอร์ของผู้ใช้แต่ละคนย่อมมีความแตกต่างกัน ขึ้นอยู่กับว่าแต่ละคนซื้อคอมพิวเตอร์มาใช้เพื่องานอะไรบ้าง แต่โดยภาพรวมๆ ของการใช้คอมพิวเตอร์ของคนทั่วไปโดยส่วนใหญ่ก็คือ การใช้ในโปรแกรมชุด Microsoft Office และเชื่อมต่อคอมพิวเตอร์เข้าสู่เครือข่ายอินเทอร์เน็ต เพื่อท่องโลกอินเทอร์เน็ตต่างๆ จะดูหนัง ฟังเพลง ดูทีวีหรือละครย้อนหลัง Facebook, Twitter , Line ก็แล้วแต่ตัวบุคคล ซึ่งคือลักษณะของคนที่ใช้คอมพิวเตอร์ส่วนมาก

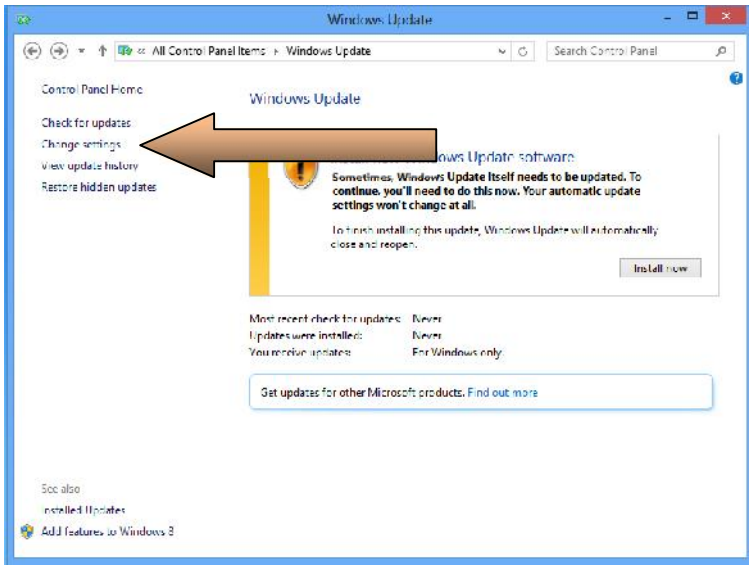
เทคนิคหนึ่งที่ผู้เขียนใช้ก็คือการสร้าง Image File ไว้เพื่อที่กรณี เมื่อเครื่องมีปัญหาสุดๆ หรือเบื่อที่จะค้นหาไวรัสคอมพิวเตอร์ เพื่อที่จะกำจัดมันออกไป ก็จะใช้วิธีการ Image File ที่เก็บไว้กลับมาเหมือนเดิมตอนติดตั้งโปรแกรมไว้ในครั้งแรก แต่ท่านต้องถามตัวเองก่อนนะว่าเครื่องของท่านควรจะมีโปรแกรมอะไรอยู่บ้าง แล้วก็ลงโปรแกรมตามที่ต้องการลงไปให้หมด เช่น ระบบปฏิบัติการวินโดวส์ ไมโครซอฟต์ออฟฟิศ พร้อมทั้งทำการ Activated ผลิตภัณฑ์ต่างๆ ให้สมบูรณ์แบบด้วย (ผู้เขียนสนับสนุนให้ใช้โปรแกรมที่ถูกต้องตามกฎหมายและลิขสิทธิ์นะครับ)

อีกอย่างหนึ่งที่ผู้เขียนใช้ก็คือ เมื่อทำการลงระบบปฏิบัติการวินโดวส์เสร็จเรียบร้อยแล้ว พร้อมทั้งทำการ Activated เรียบร้อยแล้วนั้น ผู้เขียนจะปิด Windows Update ดังนี้



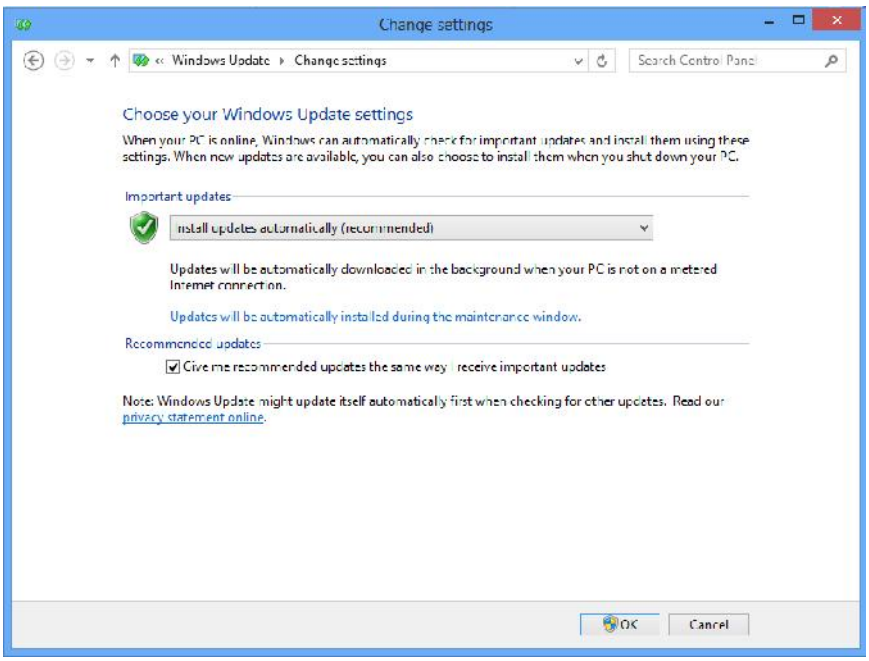
รูป ๒.๑ เมนู Windows Update ที่หน้าต่าง System ของ Windows ๗ และ Windows ๘

๑. คลิกที่ Windows Update บนหน้าต่าง System จะได้หน้าต่าง Windows Update ขึ้นมาตามรูป ๒.๒



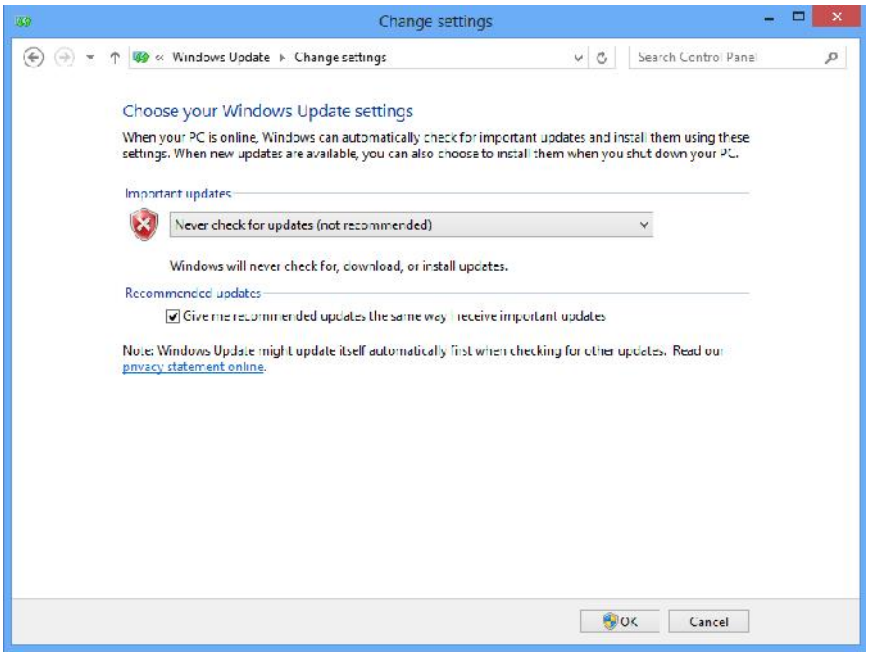
รูป ๒.๒ หน้าต่าง Windows Update

๒. จากนั้นคลิกที่ Change settings ตามลูกศร จะได้หน้าต่าง Change settings ตามรูป ๒.๓



รูป ๒.๓ หน้าต่าง Change settings

๓. ที่ Important updates จะอยู่ที่ Install updates automatically (recommended) ให้คลิกเลือกเป็น Never check for updates (not recommended) ตามรูป ๒.๔ แล้วคลิก OK



รูป ๒.๔ หน้าต่าง Change settings ที่เปลี่ยนไม่ต้องให้ Update

เพราะผู้เขียนมีประสบการณ์จากการใช้ระบบปฏิบัติการวินโดวส์มาตั้งแต่ Windows ยุคแรกคือ ๑.๐ จนถึงปัจจุบัน Windows ๘ ไม่เคยเห็นมีใครใช้ประสิทธิภาพสูงสุดของระบบปฏิบัติการวินโดวส์เลย ดังนั้น ผู้เขียนจึงปิด Windows update เสียเลยจะได้ไม่ต้องมาคอยถามเราบ่อย หรือแม้แต่จะปิดเครื่อง บ้างทีก็ให้เรารอเพื่อจะทำการ update โปรแกรม

หลังจากลงโปรแกรมตามที่ต้องการเสร็จเรียบร้อย ก็ให้ทำการ Image File เก็บไว้ ซึ่งผู้เขียนใช้ Norton ghost ๑๑.๕ ในการทำ Image File (บางทีก็จะเรียกว่าไฟล์ ghost) เก็บไว้ในไดรฟ์ อีกพาร์ติชั่นหนึ่ง เช่น ไดรฟ์ D: เป็นต้น แต่ทั้งนี้ ผู้อ่านท่านใดจะใช้โปรแกรมใดในการสร้าง Image File เก็บไว้ก็แล้วแต่เทคนิคของแต่ละคนนะครับ ผู้เขียนเชื่อว่า หลายคนทำได้และทำเป็น ถ้าไม่ได้ลองศึกษาใน youtube นะครับ เพราะถ้าจะอธิบายเทคนิคการทำ Image File เข้าไปในหนังสือเล่มนี้ จะเป็นการยืดเยื้อ และทำให้หนังสือเล่มนี้มีจำนวนหน้ามากเกินความจำเป็น เพราะถ้าทำ Image File เป็นด้วยวิธีการใดวิธีการหนึ่งแล้วก็สามารถใช้ได้ตลอดไป

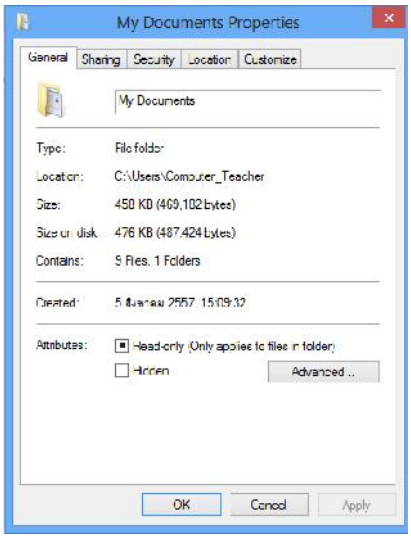
๑.๒ ย้ายการเก็บข้อมูลไปไว้อีกไดรฟ์

ดังที่เคยกล่าวไว้แล้วว่าถ้าเรารบกับไวรัสคอมพิวเตอร์สักร้อยครั้ง ชนะห้าสิบครั้งก็คุ้มแล้วนั้น ก็เพื่อวิธีการที่จะกล่าวต่อไปนี้ เปรียบเสมือนในสมรภูมิรบ แน่นอนว่าย่อมไม่มีขุนศึกใดที่จะไม่มีบาดแผลในการสู้รบ การต่อสู้กับไวรัสคอมพิวเตอร์ก็เหมือนการสู้รบเช่นเดียวกัน เพราะในบางครั้งเมื่อเราสู้กับไวรัสคอมพิวเตอร์ เราไม่สามารถเอาชนะได้ หรือชนะได้ แต่ระบบปฏิบัติการวินโดวส์ก็โดนเล่นงานจนทำงานต่อไปไม่ได้ เพราะไวรัสคอมพิวเตอร์เข้าไปทำลายรีจิสตรี้ (Registry) ซึ่งเปรียบเสมือนยีนส์ของร่างกายมนุษย์นั้นจนเสียหาย หนทางเดียวก็คือต้องฟอร์แมท (Format) ลงโปรแกรมใหม่ (***แต่ผู้เขียนใช้การ ghost กลับจาก Image File ที่เก็บไว้***) ซึ่งปัญหาที่ตามมาก็คือข้อมูลต่างๆ ที่เราจำเป็นต้องใช้ซึ่งอยู่บนหน้า Desktop บ้าง หรืออยู่ใน My Documents เราต้องเสียเวลามาจัดการเก็บสำรองข้อมูลไว้ ซึ่งถ้าระบบปฏิบัติการวินโดวส์สามารถเปิดใช้งานได้ปัญหาก็น้อย แต่ถ้าระบบปฏิบัติการวินโดวส์ ไม่สามารถเปิดขึ้นมาได้แล้ว ปัญหาก็จะใหญ่ตามมา ดังนั้นวิธีที่แนะนำที่ควรทำก็คือ เนื่องจากในปัจจุบันอุปกรณ์ที่ใช้สำหรับสำรองข้อมูลที่เรียกว่าฮาร์ดดิสก์ มีขนาดความจุใหญ่มาก ดังนั้น ควรแบ่งฮาร์ดดิสก์ไว้มากกว่า ๑ พาร์ติชั่น ที่นอกเหนือจากพาร์ติชั่นที่มีระบบปฏิบัติการวินโดวส์ ในพาร์ติชั่นที่ไม่ได้ติดตั้งระบบปฏิบัติการวินโดวส์นั้น ควรเป็นที่บันทึกข้อมูลต่างๆ ไว้ เมื่อจำเป็นต้องฟอร์แมทเพื่อลงระบบปฏิบัติการวินโดวส์ใหม่ จะได้ไม่ยุ่งยากในการสำรองข้อมูล

สำหรับตัวผู้เขียนเองนั้นเวลาจะบันทึกข้อมูลใดๆ หรือสำรองข้อมูล จะไปสร้างโฟลเดอร์ไว้ใน ไดรฟ์ D: ตลอด ถ้าเครื่องมีปัญหาจะได้ไม่เสียเวลายุ่งยากในการสำรองข้อมูล

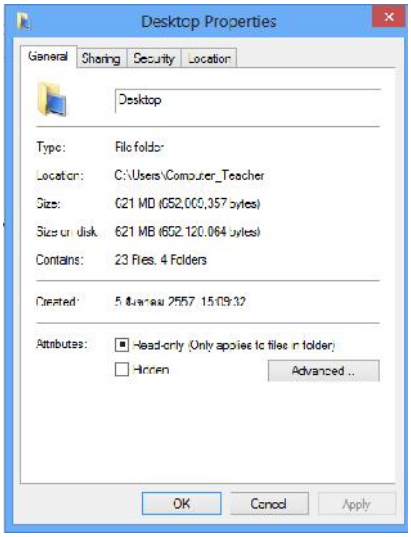
แต่สำหรับผู้ที่ชอบบันทึกข้อมูลไว้ใน My Documents หรือ Desktop มีวิธีการที่สามารถย้ายข้อมูลที่สำคัญไปไว้อีกพาร์ติชั่นหนึ่งได้ตลอดเวลา ถึงแม้จะบันทึกข้อมูลต่างๆ ไว้ใน My Documents หรือบนหน้า Desktop ก็ตาม

โดยค่าปกติของระบบปฏิบัติการวินโดวส์นั้น ใน Windows ๘ เมื่อบันทึกข้อมูลลงไปใน My Documents ข้อมูลจะไปถูกบันทึกใน C:\Users\ชื่อของผู้ใช้ที่ตั้งไว้\My Documents ตามรูป ๒.๕



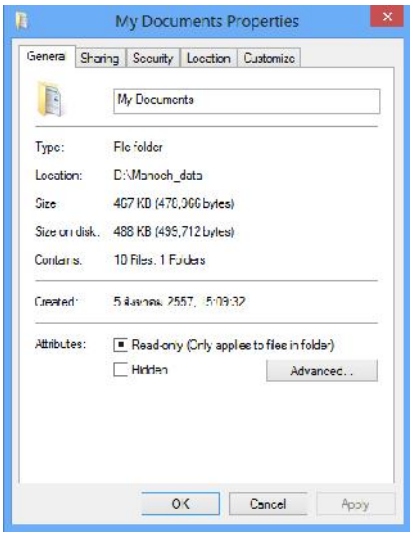
รูป ๒.๕ หน้าต่าง My Documents Properties จากการคลิกขวาที่ My Documents และเลือก Properties

ซึ่งจะเห็นได้ว่าข้อมูลที่จัดเก็บไว้ใน My Documents จะถูกจัดเก็บไว้ที่ Location: C:\users\Computer_teacher (ชื่อ Computer_Teacher คือชื่อของผู้ใช้ที่ตั้งไว้นั่นเอง) และเช่นเดียวกันข้อมูลใน Desktop ก็จะอยู่ใน Location: ดังรูป ๒.๖



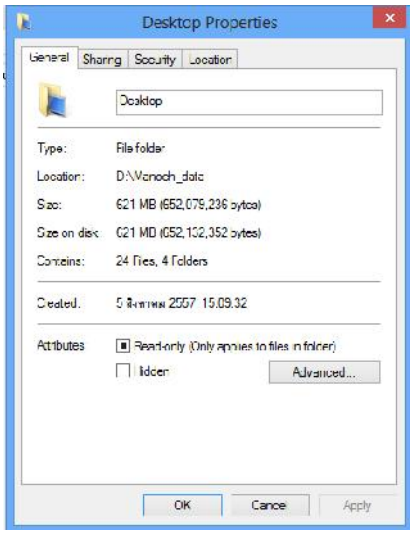
รูป ๒.๖ หน้าต่าง Desktop Properties จากการคลิกขวาที่ Desktop และเลือก Properties

ดังนั้นถ้าหากเราต้องการที่จะบันทึกข้อมูลลงไปใน My Documents หรือบนหน้า Desktop เหมือนเดิม แต่ให้ข้อมูลไปอยู่อีกพาร์ติชั่นสามารถทำได้โดยการย้ายสองโฟลเดอร์ดังกล่าวออกไปไว้ในที่ต้องการ เช่นในกรณีของผู้เขียนมีอีกพาร์ติชั่นหนึ่งชื่อ ไดรฟ์ D: โดยผู้เขียนไปสร้างโฟลเดอร์ชื่อ Manoch_data (ผู้อ่านจะตั้งชื่ออะไรก็ได้) แล้วผู้เขียนได้ Cut เอาโฟลเดอร์ทั้ง My Documents และ Desktop ไปไว้ยังโฟลเดอร์ที่สร้างไว้ชื่อ Manoch_data ใน ไดรฟ์ D: หลังจากนั้นให้นำเมาส์มาคลิกขวาที่โฟลเดอร์ My Documents ใหม่ แล้วเลือก Properties จะเห็นว่าเป็นไปตามรูป ๒.๗ คือ Location: จะเป็น D:\Manoch_data



รูป ๒.๗ แสดงให้เห็นว่าปลายทางของ My Documents หลังจากย้ายแล้วจะอยู่ใน D:\Manoch_data

และในทำนองเดียวกันที่ Desktop เมื่อคลิกขวาเลือก Properties ที่ Location: จะเป็น D:\Manoch_data นั่นคือปลายทางของข้อมูลบนหน้า Desktop จะอยู่ใน D:\Manoch_data เหมือนกัน ดังรูป ๒.๘



รูป ๒.๘ แสดงให้เห็นว่าปลายทางของไฟล์ที่บันทึกบนหน้า Desktop หลังจากย้ายแล้วจะอยู่ใน D:\Manoch_data

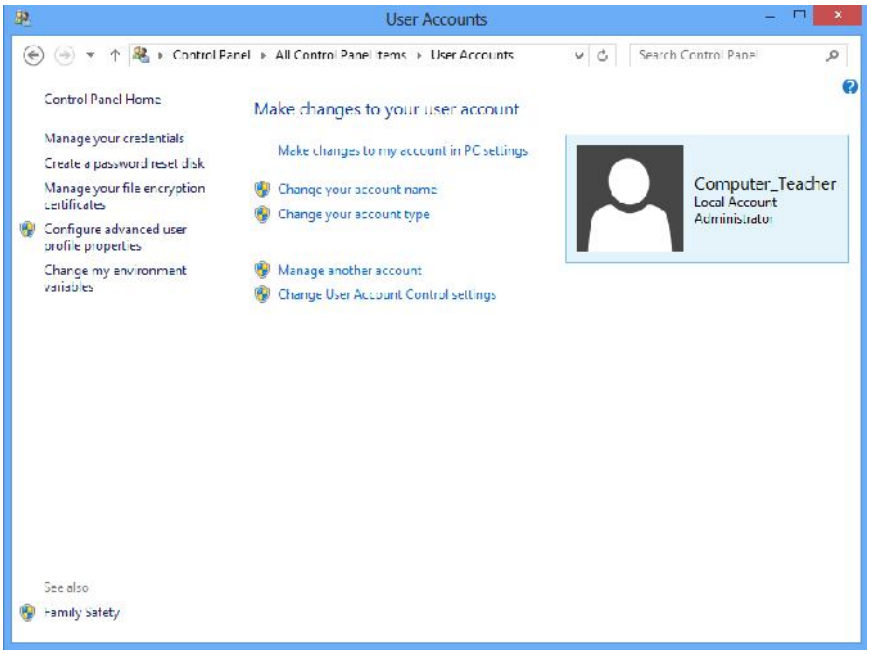
จากที่กล่าวมาในส่วนของการย้ายการเก็บข้อมูลไปไว้อีกไดรฟ์นั้น อยู่ที่ว่าถ้าผู้อ่านสามารถจะเก็บข้อมูลต่างๆ ไปไว้อีกไดรฟ์หนึ่งโดยไม่คิดว่ายุ่งยากก็ไม่ต้องทำตามวิธีการย้ายโฟลเดอร์ทั้งสองคือ My Documents กับ Desktop ก็ได้ ทั้งนี้อยู่ที่ผู้ใช้เอง เจตนาของส่วนนี้ก็เผื่อไว้หากต้องการฟอร์แมท (Format) เครื่องเพื่อติดตั้งระบบปฏิบัติการวินโดวส์และโปรแกรมอื่นๆ ใหม่ จะได้ไม่เสียเวลามาเก็บข้อมูลต่างๆ แต่ถ้าไม่ทำไว้เมื่อมีปัญหาก็สามารถคัดลอกมาได้ซึ่งจะกล่าวไว้ในบทที่ ๔

๒. รู้จักกับ User Accout Control (UAC)

คือ การควบคุมบัญชีผู้ใช้ เป็นลักษณะหนึ่งที่ช่วยให้ผู้ใช้ Wndows ๗ และ Windows ๘ ได้ทราบว่ามีโปรแกรมใดโปรแกรมหนึ่งต้องการติดตั้งลงไปในเครื่องคอมพิวเตอร์ ซึ่งจะต้องได้รับการอนุญาตก่อน แต่ถ้าผู้ใช้คอมพิวเตอร์กำลังทำงานที่สามารถดำเนินการในฐานะผู้ใช้มาตรฐานทั่วไป เช่น การอ่านอีเมล การดูหนังฟังเพลง การใช้อินเทอร์เน็ต การสร้างเอกสารต่างๆ ถือเป็นเรื่องปกติ แต่ถ้าจะทำการเปลี่ยนแปลงต่างๆ ในคอมพิวเตอร์ที่ต้องใช้สิทธิระดับผู้ดูแล UAC จะแจ้งให้ทราบ ถ้าเราแน่ใจว่าการเปลี่ยนแปลงนั้นไม่ใช่ตัวไวรัสคอมพิวเตอร์ เราก็สามารถคลิกใช่ เพื่อดำเนินการต่อไปได้ ที่เป็นเช่นนี้ก็เพราะ UAC เป็นตัวคอยไม่ให้มีสิ่งใดสามารถทำการเปลี่ยนแปลงต่างๆ ในคอมพิวเตอร์ได้ โดยที่เราไม่ทราบ ซึ่งจะช่วยป้องกันไม่ให้ซอฟต์แวร์ที่เป็นอันตราย มาทำการติดตั้งหรือทำการเปลี่ยนแปลงต่างๆ ในคอมพิวเตอร์ของเราได้

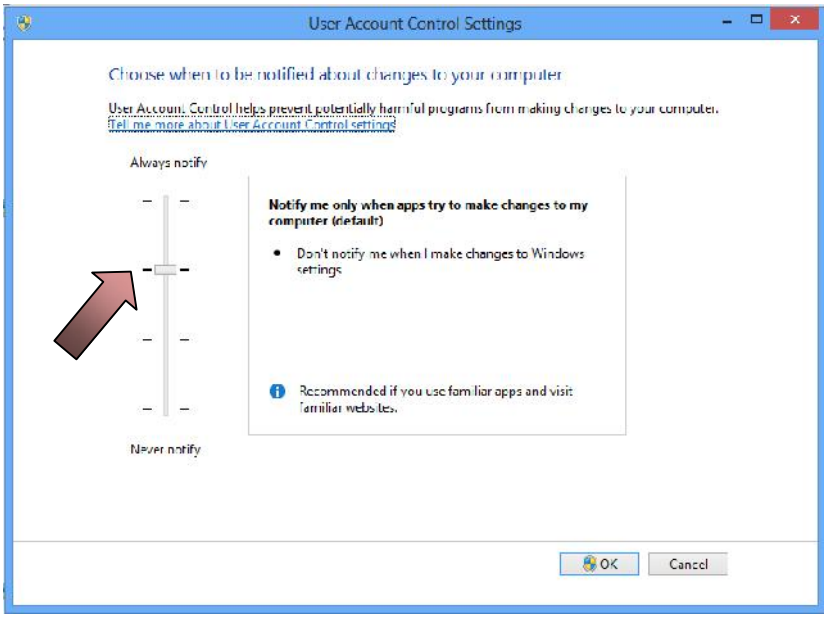
User Account Control (UAC) อยู่ตรงไหนหรือ ? เราสามารถเข้าไปสู่ UAC ได้หลายวิธี แต่วิธีง่ายๆ สัก ๒ วิธี มีดังนี้

วิธีที่ ๑ เข้าที่ Control Panel →User Accounts จะได้หน้าต่าง User Accounts ตามรูป ๒.๙



รูป ๒.๙ หน้าต่าง User Accounts

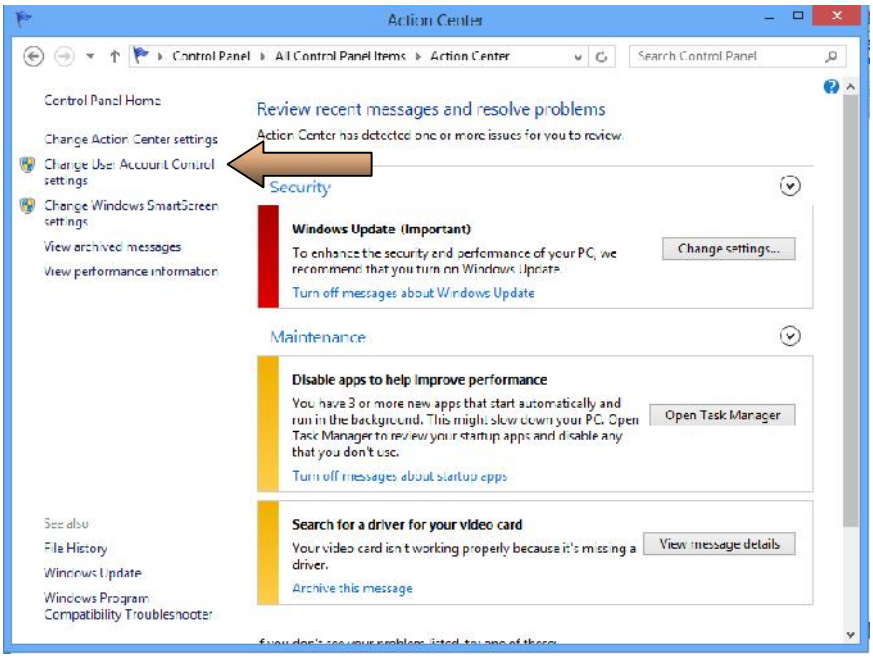
ให้นำเมาส์ไปคลิกที่ Change User Account Control settings จะได้หน้าต่าง User Account Control Settings ตามรูป ๒.๑๐ ซึ่งค่ามาตรฐานที่ปลอดภัยและ Windows แนะนำจะเป็นไปตามรูปนี้ โดยที่สเกลของระดับ (ที่ลูกศรชี้) จะต้องไม่อยู่ที่ Never notify เพราะถ้าอยู่ที่ Never notify แล้ว UAC ก็จะไม่เกิดประโยชน์ใดๆ เลย ใน Windows ๗ ถ้าตั้งค่า เป็น Never notify จะทำให้ใน ไดรฟ์ C: และโฟลเดอร์ System๓๒ สามารถสร้างไฟล์ได้ ซึ่งเป็นอันตรายที่จะทำให้ไวรัสคอมพิวเตอร์สามารถไปฝังตัวในตำแหน่งดังกล่าวได้ ซึ่งเป็นอันตรายอย่างยิ่ง ที่เป็นเช่นนี้ก็คือถ้าไฟล์ไวรัสคอมพิวเตอร์ตัวใดไปฝังในตำแหน่งดังกล่าวได้ การเรียกหรือสั่งให้โปรแกรม



รูป ๒.๑๐ หน้าต่าง User Account Control Settings

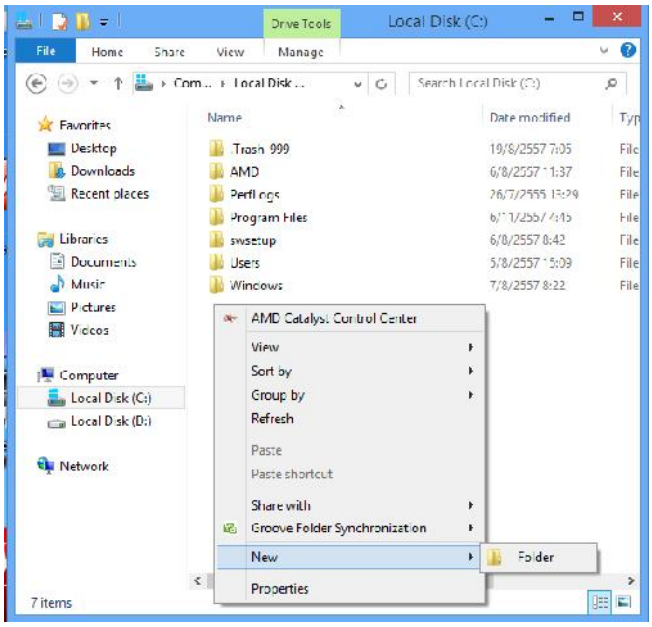
ไวรัสคอมพิวเตอร์ทำงานไม่จำเป็นต้องบอก path หรือตำแหน่งเลย โปรแกรมจะเรียกตรงไหนก็ได้ ยิ่งถ้าไปฝังในรีจิสตรี้แล้วยิ่งสบายไวรัสคอมพิวเตอร์เลย ลองนึกถึงท่านเรียกใช้ Notepad โดยพิมพ์ที่ตำแหน่ง Search ดูจะพบว่า notepad จะทำงานได้เลย หรือพิมพ์ calc เครื่องคิดเลขก็จะมีหน้าต่างมาทำงานให้เลย เพราะทั้ง notepad และ calc เป็นโปรแกรมอยู่ในโฟลเดอร์ system๓๒

วิธีที่ ๒ เข้าที่ Control Panel → System →Action Center (อยู่ทางด้านล่างซ้ายของหน้าต่าง System) จะได้หน้าต่าง Action Center ตามรูป ๒.๑๑ ให้เมาส์คลิกที่ Change User Account Control settings (ลูกศรชี้) จะได้หน้าต่าง User Account Control settings เช่นเดียวกับรูป ๒.๑๐

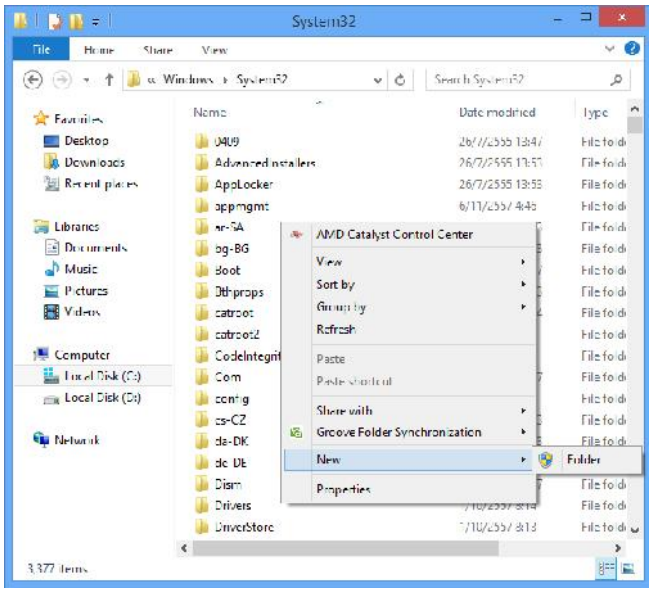


รูป ๒.๑๑ หน้าต่าง Action Center

ดังนั้นการกำหนดให้ UAC อยู่ในตำแหน่งดังกล่าวนั้นจะทำให้เราไม่สามารถสร้างไฟล์ใดๆ ลงไปในไดรฟ์ C: และโฟลเดอร์ System๓๒ ได้เป็นอันขาด นอกจากโฟลเดอร์ (โฟลเดอร์ไม่ใช่โปรแกรมไฟล์ที่ execute จึงไม่เป็นอันตรายใดๆ) นี่คือคุณสมบัติที่มีมาให้ใน Windows ๗ และ Windows ๘ ซึ่งเป็นเรื่องของ security เพราะฉะนั้น ถ้าผู้อ่านตั้ง UAC เป็น Never notify ใน Windows ๗ แล้ว ท่านก็เปรียบเสมือนได้ Windows XP บนธีมของ Windows ๗ เท่านั้น แต่ใน Windows ๘ ถึงแม้จะปรับ UAC เป็น Never notify เราก็ไม่สามารถสร้างไฟล์ใดๆ ลงบนไดรฟ์ C: และโฟลเดอร์ System๓๒ ได้ ดังรูป ๒.๑๒ และ ๒.๑๓

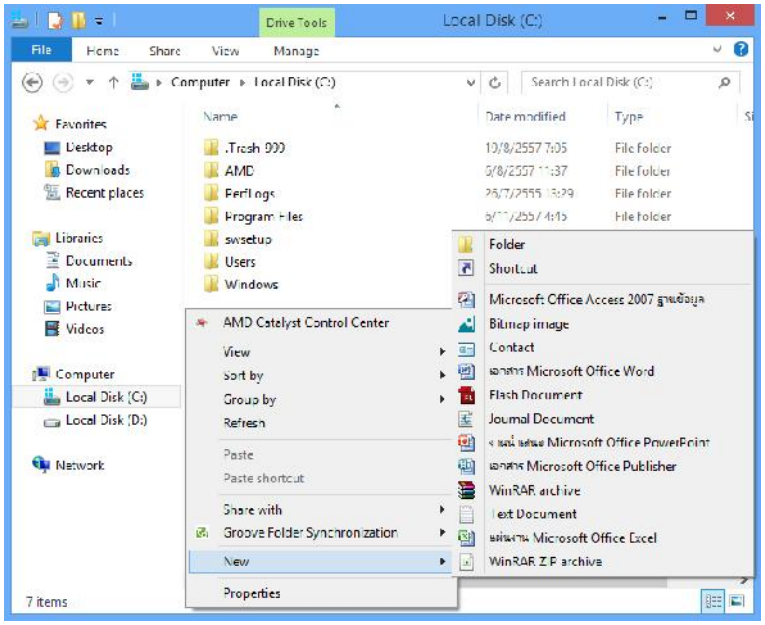


รูป ๒.๑๒ ไม่สามารถสร้างไฟล์ใดๆ ลงในไดรฟ์ C: ได้



รูป ๒.๑๓ ไม่สามารถสร้างไฟล์ใดๆ ลงใน System๓๒ ได้

แต่ถ้าทำการแก้ไขในรีจิสตรี้แล้วก็สามารถที่จะทำการสร้างไฟล์ในไดรฟ์ C: และโฟลเดอร์ System๓๒ ได้ ดังรูป ๒.๑๔ (ต้องการชี้ให้เห็นว่าถ้าแก้ในรีจิสตรี้แล้วก็ทำได้ แต่ไม่ต้องการให้ผู้อ่านเข้าไปยุ่งในรีจิสตรี้ เพราะเราต้องการให้ใช้งาน UAC ให้เกิดประโยชน์ต่อการต่อกรกับไวรัสคอมพิวเตอร์)



รูป ๒.๑๔ สามารถสร้างไฟล์ในไดรฟ์ C: ได้ถ้ามีความรู้เข้าไปแก้ในรีจิสตรี้

๓. ค้นระบบพบสิ่งแปลกๆ

ในระบบปฏิบัติการวินโดวส์จะมีอีกหลายสิ่งหลายอย่างที่ผู้อ่านยังอาจจะไม่เคยเห็นหรือไม่เคยรู้มาก่อนว่า ในระบบปฏิบัติการวินโดวส์มีสิ่งนี้อยู่ด้วยหรือ แล้วมันคืออะไร? มีประโยชน์หรือโทษอย่างไร? มีความจำเป็นแค่ไหนที่ต้องมี? คำถามต่างๆ เหล่านี้ก็จะเกิดขึ้นในใจของผู้อ่านแน่นอน

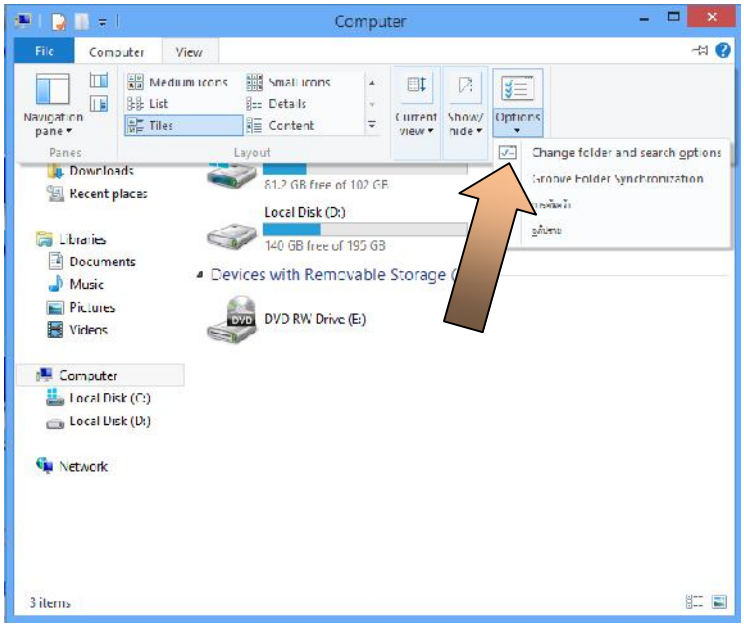
ดังนั้นก่อนที่จะเรียนรู้เทคนิคในการต่อกรกับไวรัสคอมพิวเตอร์ เรามาค้นระบบและรู้จักสิ่งแปลกๆ ที่เราไม่เคยเห็น แต่ว่าเป็นของระบบปฏิบัติการวินโดวส์ก่อน ซึ่งผู้อ่านจะได้ไม่เข้าใจผิดคิดว่าเป็นไวรัสคอมพิวเตอร์กันเสียก่อนเพราะในการต่อกรกับไวรัสคอมพิวเตอร์เมื่อเราเห็นระบบปฏิบัติการวินโดวส์แล้วเราอาจจะตกใจนึกว่าเป็นไวรัสคอมพิวเตอร์ทั้งหมด เพราะว่าบางครั้งมันก็อยู่ก้ำกึ่งกันระหว่างคำว่า **“ใช่”** กับคำว่า **“ไม่ใช่”** ไวรัสคอมพิวเตอร์ เพราะลักษณะอาการบางอย่างก็อาจจะเป็นเพราะฝีมือของไวรัสคอมพิวเตอร์ก็ได้

๓.๑ การกำหนดให้ระบบปฏิบัติการวินโดวส์แสดงไฟล์และโฟลเดอร์ที่ถูกซ่อน

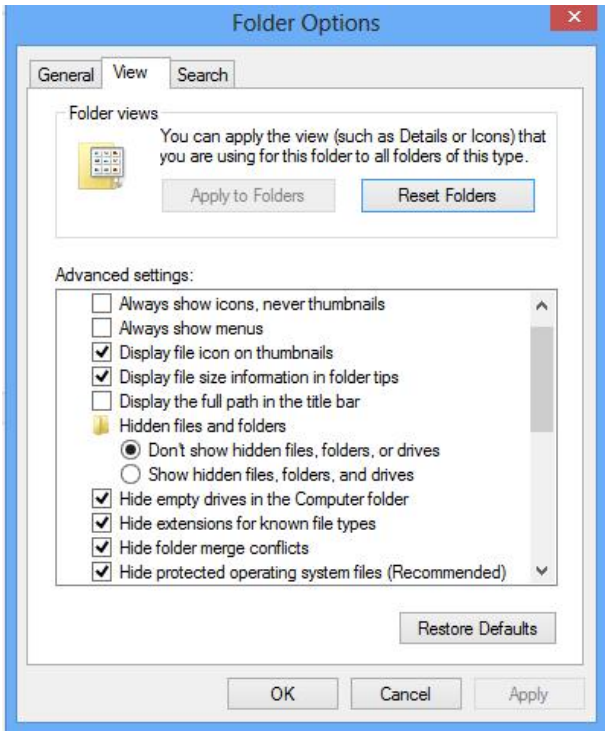
ในระบบปฏิบัติการวินโดวส์นั้นปกติจะมีไฟล์และโฟลเดอร์ที่ระบบปฏิบัติการวินโดวส์ไม่ต้องการให้มองเห็น ซึ่งอาจเป็นไฟล์หรือโฟลเดอร์ของระบบที่ไม่ต้องการให้มองเห็นเพื่อป้องกันไม่ให้ผู้ใช้ลบ อันจะทำให้ระบบปฏิบัติการวินโดวส์มีปัญหาจนถึงอาจจะใช้ไม่ได้ และไวรัสคอมพิวเตอร์ก็อาศัยจุดนี้ในการที่จะซ่อนตัวเองไว้ไม่ให้มองเห็นด้วย แต่ระบบปฏิบัติการวินโดวส์ก็มิได้ปิดกั้นที่จะไม่ให้แสดงไฟล์และโฟลเดอร์ที่ซ่อนไว้ โดยที่เราสามารถเปิดการซ่อนไฟล์และโฟลเดอร์ด้วยวิธีดังนี้

๑. ที่หน้าต่าง Computer (บน Windows ๘) ไปที่เมนู View เลือกริบบอน Option จะปรากฏเมนู Change Folder and search options ขึ้นมาตามรูป ๒.๑๕ (ลูกศรชี้)

๒. คลิกที่ Change Folder and search options จะปรากฏหน้าต่าง Folder Options คลิกที่แท็บ View จะปรากฏตามรูป ๒.๑๖



รูป ๒.๑๕



รูป ๒.๑๖ หน้าต่าง Folder Options

๓. ที่ Hidden files and folders ให้คลิกเลือกที่ Show hidden files, folders, and drives และที่ช่อง

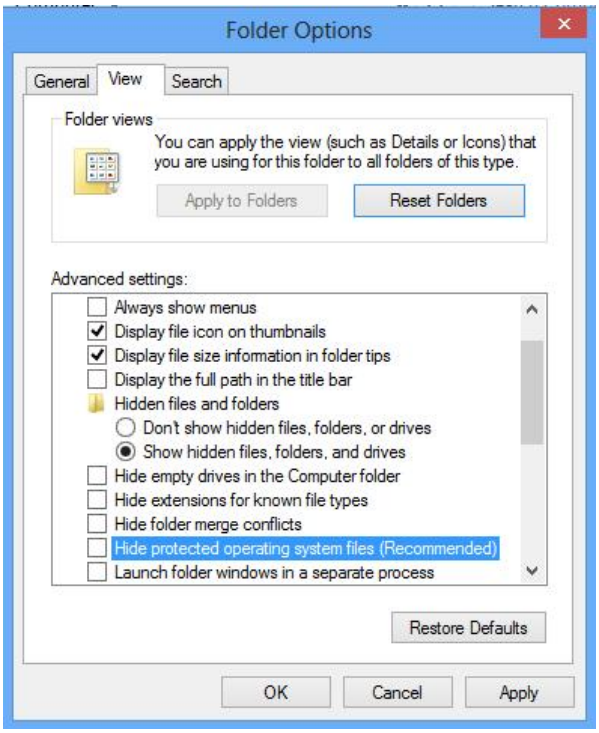
☑ Hide empty drives in the Computer folder

☑ Hide extensions for known file types

☑ Hide folder merge conflicts

☑ Hide protected operating system files (Recommended)

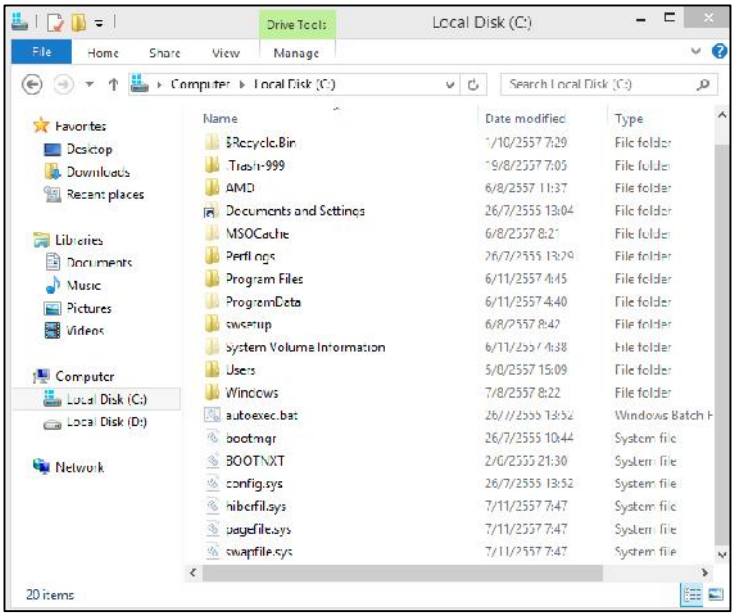
ให้คลิกเอาเครื่องหมาย ✓ ออก ตามรูป ๒.๑๗ แล้วคลิก Apply → OK



รูป ๒.๑๗ วิธีการให้ระบบปฏิบัติการวินโดวส์แสดงนามสกุลของไฟล์และแสดงไฟล์ระบบ

๓.๒ รู้จักไฟล์และโฟลเดอร์ของระบบจะได้ไม่ลบผิด

โดยทั่วไปแล้วในการติดตั้งระบบปฏิบัติการวินโดวส์นั้น ส่วนใหญ่หรือจะเกือบทั้งหมดมักติดตั้งลงบนไดรฟ์ C: ซึ่งเมื่อเรากำหนดให้ระบบปฏิบัติการวินโดวส์แสดงไฟล์ที่ถูกซ่อนขึ้นมาดังที่ได้อธิบายในหัวข้อ ๓.๑ มาแล้วนั้น จะพบว่า ที่ไดรฟ์ C: มีไฟล์และโฟลเดอร์ที่แสดงขึ้นมาเป็นสีจางๆ ปรากฏขึ้นมา หลายคนอาจจะตกใจว่าเป็นไวรัสคอมพิวเตอร์ แต่ขอกล่าวเพียงสั้นๆ ในที่นี้ก่อนว่า *ส่วนใหญ่* ไม่ใช่ไวรัสคอมพิวเตอร์ แต่เป็นคุณสมบัติของไฟล์ ซึ่งในระบบปฏิบัติการวินโดวส์ จะต้องมี และที่เห็นก็คือของ Windows ๘ ตามรูป ๒.๑๘



รูป ๒.๑๘ ไฟล์และโฟลเดอร์ของระบบปฏิบัติการที่ถูกซ่อนไว้ในไดรฟ์ C:

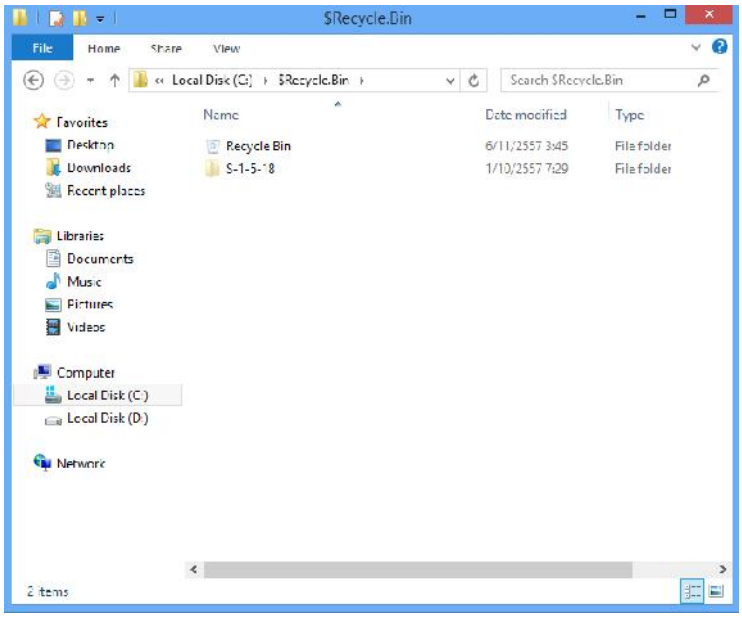
ถ้านำมาจำแนกสิ่งที่ Windows ๘ ซ่อนไว้จะได้ดังนี้

ส่วนที่เป็นไฟล์	**ส่วนที่เป็นโฟลเดอร์**
- autoexec.bat	- $Recycle.Bin
- bootMGR	- Documents and Settings
- BOOTNXT	- MSOCache
- config.sys	- ProgramData
- hiberfil.sys	- System Volume Information
- pagefile.sys	
- swapfile.sys	

จากที่กล่าวมานี้เป็นไฟล์และโฟลเดอร์ของระบบ ไม่ควรยุ่งหรือลบ เพราะถ้าไปลบเข้าบางตัว จะทำให้เข้าใช้ระบบปฏิบัติการวินโดวส์ไม่ได้เลย แต่ถ้าผู้อ่านตั้ง UAC ไว้ การพยายามเขียนไฟล์ลงบนไดรฟ์ C: จะทำไม่ได้อยู่แล้วถ้าผู้อ่านไม่อนุญาต

๓.๓ โฟลเดอร์จางๆ ชื่อ $Recycle.Bin

โฟลเดอร์ชื่อ $Recycle.Bin เป็นที่เก็บข้อมูลของไฟล์ หรือสิ่งที่ถูกลบไว้ (*ขอย้ำว่าเก็บข้อมูลของไฟล์ที่ถูกลบเท่านั้น เพราะไฟล์หรือโฟลเดอร์ที่ถูกลบก็ยังอยู่ที่เดิม แต่ในส่วนของข้อมูลที่อยู่ในโฟลเดอร์ $Recycle.Bin นั้น จะเป็นรายละเอียดของไฟล์หรือโฟลเดอร์ที่ถูกลบว่าอยู่ตรงไหน*) ส่วนไอคอน Recycle Bin ที่อยู่บนหน้า Desktop เป็นเพียงแค่ชอร์ตคัทเท่านั้น ไม่ได้เป็นที่เก็บไฟล์ที่ลบจริง เพราะข้อมูลของไฟล์ที่ถูกลบจะไปอยู่ในโฟลเดอร์ $Recycle.Bin เท่านั้น ซึ่งในโฟลเดอร์ $Recycle.Bin จะประกอบด้วยโฟลเดอร์ ๒ โฟลเดอร์ คือโฟลเดอร์ Recycle Bin กับโฟลเดอร์ S-๑-๕-๑๘ ตามรูป ๒.๑๙



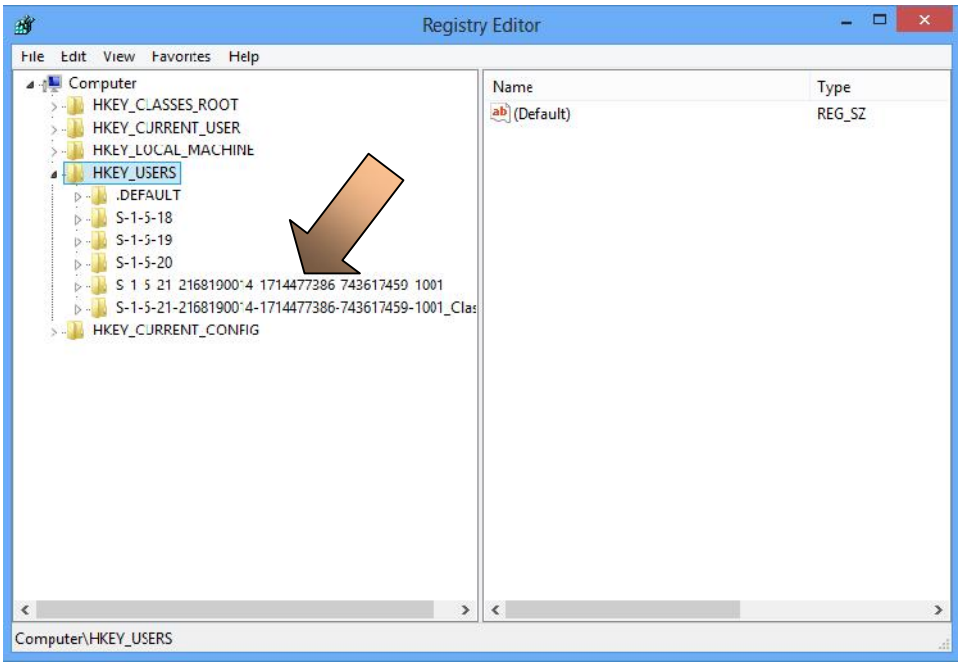
รูป ๒.๑๙ หน้าต่างโฟลเดอร์ $Recycle.Bin ที่ถูกซ่อนไว้

และการที่เราให้ระบบปฏิบัติการวินโดวส์แสดงไฟล์และโฟลเดอร์ที่ถูกซ่อนไว้เมื่อเรานำ External Harddisk หรือแฟลชไดรฟ์ มาเชื่อมต่อ ผู้อ่านก็อาจจะพบกับโฟลเดอร์ที่ชื่อ Recycler บ้าง หรือ Recycled บ้าง ให้ลบทิ้งไปเลย (ส่วนมากเป็นที่ซ่อนตัวของไวรัสคอมพิวเตอร์) ยิ่งถ้าในแฟลชไดรฟ์ จะต้องไม่มีทั้ง Recycler และ Recycled ไม่ว่ากรณีใดๆ ทั้งสิ้น ถ้ามี นั่นคือไวรัสคอมพิวเตอร์แน่นอน

ในโฟลเดอร์ชื่อ Recycle.Bin (โฟลเดอร์ใน $Recycle.Bin) จริงๆ แล้วมีชื่อเฉพาะของตัวเองคือ จะมีชื่อขึ้นด้วย S-X-X-XX-XXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX อยู่ (แต่เรามองในระบบปฏิบัติการ Windows ๘ เราจะเห็นเป็นโฟลเดอร์ชื่อ Recycle.Bin) โดย X คือ ตัวเลข ๐-๙ เราเรียกค่านี้ว่า SID (Security Identifier) ซึ่งไวรัสคอมพิวเตอร์ชอบเข้ามาซ่อนตัวอยู่ในนี้ ถ้าเราแน่ใจว่าเราไม่ต้องการ Restore สิ่งที่เราลบไปแล้วกลับมาใหม่ ก็สามารถลบได้เลย เพราะเมื่อเราปิดแล้วเปิดเครื่องขึ้นมาใหม่ Windows ๘ ก็จะสร้างโฟลเดอร์นี้เปล่าๆ ขึ้นมารองรับการทำงานใหม่

ปัญหาอยู่ที่ว่าแล้วผู้อ่านจะรู้ได้อย่างไรว่าหลายเลข SID ที่ใช้คือหมายเลขอะไร ซึ่งถ้าเครื่องที่เราใช้มีเพียงเราคนเดียว ค่าหมายเลข SID จะมีอยู่ ๑ ชุดเท่านั้น โดยมีวิธีการดูดังนี้

๑. ไปที่ Search พิมพ์คำว่า regedit แล้ว Enter
๒. จะปรากฏหน้าต่าง User Account Control ให้เราอนุญาตก่อนโดยคลิกปุ่ม Yes
๓. จะปรากฏหน้าต่าง Registry Editor ขึ้นมาตามรูป ๒.๒๐
๔. คลิกที่เครื่องหมาย ▷ หน้า HKEY_USERS จะปรากฏหมายเลข SID ของผู้ใช้ขึ้นมา ดูลูกศรชี้ในรูป ๒.๒๐



รูป ๒.๒๐ หน้าต่าง Registry Editor เพื่อดูค่า SID

ซึ่งผู้เขียนต้องการชี้ให้เห็นเท่านั้นนะครับ ถ้าไม่สนใจอะไร ผู้อ่านสามารถลบได้ตลอดเวลา (การจะลบ $Recycle.Bin ในขณะที่อยู่ในระบบปฏิบัติการวินโดวส์นั้นลบได้ไม่หมด) โดยจะกล่าวถึงวิธีการลบในบทต่อไป

๓.๔ ไฟล์ที่ชื่อ Desktop.ini

โดยส่วนมากที่มีอยู่ในระบบปฏิบัติการวินโดวส์นั้นเป็นไฟล์ที่เรียกใช้ทรัพยากรในระบบปฏิบัติการวินโดวส์ร่วมกัน โดยรูปแบบคำสั่งในไฟล์ Desktop.ini ส่วนมากจะมีลักษณะดังนี้

```
[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21769
```

จะพบว่ามีการอ้างอิงไฟล์ shell๓๒.dll ซึ่งไฟล์ shell๓๒.dll เป็นที่เก็บทรัพยากรหลายๆ อย่างของระบบปฏิบัติการวินโดวส์ที่มีการใช้งานร่วมกันไว้ ไม่ว่าจะเป็นข้อความ เมนู รูปภาพ และไอคอน

แต่มีไวรัสคอมพิวเตอร์บางตัวจะจำลองการทำงานเป็น shell๓๒.dll ซึ่ง shell๓๒.dll จะอยู่ที่ C:\WINDOWS\system๓๒\shell๓๒.dll เท่านั้น ถ้าอยู่ที่อื่นลบทิ้งได้หมด

๓.๕ โฟลเดอร์ที่ชื่อ System Volume Information

เป็นโฟลเดอร์ที่ผู้อ่านจะมองไม่เห็น ผู้อ่านจะมองเห็นได้ก็ต่อเมื่อเราเปิดการซ่อนของระบบปฏิบัติการวินโดวส์เท่านั้น System Volume Information เป็นที่เก็บค่าต่างๆ ที่เกิดการเปลี่ยนแปลงขึ้นเมื่อเปิดการทำงานของ System Restore ผู้อ่านจะเข้าไปดูว่าภายในมีอะไรหรือจะลบในขณะที่อยู่ในระบบปฏิบัติการวินโดวส์ไม่ได้ และ ณ สถานที่นี้พวกไวรัสคอมพิวเตอร์ชอบทำตัวเป็นอีแอบมาฝังตัวใน System Volume Information มากเป็นพิเศษ เพราะว่าเราเข้าไปดูว่าภายในมีอะไรอยู่บ้างไม่ได้

๔. สรุป

จากที่กล่าวมาในบทที่ ๒ ทั้งหมดนี้ ผู้อ่านควรจะทำตามก็คือการตั้งค่า UAC ตามที่กำหนด ส่วนไฟล์ระบบปฏิบัติการให้จำไว้เราไม่ควรไปยุ่งหรือลบ ส่วนไฟล์หรือโฟลเดอร์ที่นอกเหนือจากนั้นที่ชอบเป็นที่อยู่ของไวรัสคอมพิวเตอร์ เช่น $Recycle.Bin Recycler Recycled Desktop.ini หรือ System Volume Information เราสามารถลบได้ดังที่ได้อธิบายมาแล้ว แต่วิธีการลบจะกล่าวถึงในบทที่ ๓ ต่อไป

หลังจากที่ผู้อ่านได้เปิดการซ่อนไฟล์และโฟลเดอร์ที่เราได้นำเสนอในหัวข้อ ๓.๑ หน้า ๑๕-๑๗ ไปแล้ว หากจะทำกลับไปเป็นแบบเดิมก็ได้ เพราะว่าวิธีการที่จะลบในบทที่ ๓ ต่อไป ถึงแม้เราจะซ่อนไฟล์และโฟลเดอร์ไว้ก็สามารถมองเห็นได้หมด (ผู้เขียนจะเปิดเฉพาะการแสดงไฟล์และโฟลเดอรไว้เท่านั้น ไว้สำหรับสังเกตถ้ามีสิ่งแปลกปลอมเกิดขึ้นจะได้รู้ตัวก่อน)