เรื่อง : สปายแวร์และวิธีการป้องกัน
เรียบเรียงโดย : ดวงกมล ทรัพย์พิทยากร
เผยแพร่เมื่อ : 30 สิงหาคม 2547
ปรับปรุงล่าสุดเมื่อ : 31 สิงหาคม 2547

ทำความรู้จักกับสปายแวร์

ปัจจุบันการใช้งานอินเทอร์เน็ตนี้เป็นที่นิยมและแพร่หลายมากขึ้น อินเทอร์เน็ตจึงกลายเป็นแหล่งโฆษณาสินค้าและบริการแหล่งใหญ่ และผลที่ตามมาอีกประการหนึ่งคือ สปายแวร์ หรือ แอดแวร์ กลายมาเป็นสิ่งที่เป็นปัญหาตามมามากขึ้น ในบางครั้งที่เครื่องของคุณเกิดปัญหาขึ้น คุณจะพบว่ามันอาจเกิดจากสปายแวร์ที่เข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์โดยที่คุณไม่รู้ตัวเลย

สปายแวร์คืออะไร

แม้จะชื่อว่า สปายแวร์ แต่ไม่ได้มีความหมายลึกลับเหมือนอย่างชื่อ แต่กลับถูกใช้สำหรับการโฆษณาประชาสัมพันธ์เสียมากกว่า ในอันที่จริง สปายแวร์จะได้รับความรู้จักในชื่อของ แอดแวร์ ด้วย ดังนั้นคำว่าสปายแวร์จึงเป็นเพียงการระบุประเภทของซอฟต์แวร์เท่านั้น ส่วนความหมายที่แท้จริง สปายแวร์ หมายถึงโปรแกรมที่แอบเข้ามาติดตั้งในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้อาจไม่ได้เจตนา แล้วเป็นผลให้สปายแวร์กระทำสิ่งต่อไปนี้ เช่น

- อาจส่งหน้าต่างโฆษณาเล็กๆ ปรากฏขึ้นมา(ป๊อบอัพ) ขณะที่คุณใช้งานเครื่องคอมพิวเตอร์อยู่
- เมื่อคุณเปิดเว็บบราวเซอร์ เว็บบราวเซอร์จะทำการต่อตรงไปยังเว็บไซต์หลักของตัวสปายแวร์ที่ถูกตั้งค่าให้ลิ้งก์ไป
- สปายแวร์อาจทำการติดตามเว็บไซต์ที่คุณเข้าไปเยี่ยมชมบ่อยๆ
- สปายแวร์บางเวอร์ชั่นที่มีลักษณะรุกรานระบบจะทำการติดตามค้นหา คีย์ หรือ รหัสผ่าน ที่คุณพิมพ์ลงไปเมื่อทำการ log in เข้าแอคเคาน์ต่างๆ

สปายแวร์สร้างปัญหาอะไรกับเครื่องคอมพิวเตอร์ของคุณบ้าง

เมื่อสปายแวร์ได้แอบเข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของคุณแล้ว มันจะพยายามรัน process พิเศษบางอย่างซึ่งจะเป็นผลให้เครื่องคอมพิวเตอร์ของคุณทำงานช้าลงหรืออาจทำการเข้าสู่เว็บไซต์ต่างๆ ได้ช้า หรืออาจเข้าสู่เว็บไซต์ที่ต้องการไม่ได้เลย นอกจากนี้ ยังส่งผลเกี่ยวเนื่องกับเรื่องของข้อมูลส่วนบุคคล (privacy) ในประเด็นต่อไปนี้ด้วย

- คุณไม่สามารถทราบได้เลยว่าข้อมูลที่ถูกนำไปมีอะไรบ้าง
- คุณไม่อาจทราบได้เลยว่าใครเป็นผู้นำข้อมูลเหล่านั้นของคุณไป
- และคุณก็จะไม่ทราบเช่นกันว่า ข้อมูลเหล่านั้นจะถูกนำไปใช้อย่างไรบ้าง

คุณจะทราบได้อย่างไรว่ามีสปายแวร์เข้ามาแอบติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของคุณ

โดยทั่วไปสามารถสังเกตได้จากอาการผิดปกติดังนี้ (หากมีอาการใดอาการหนึ่งปรากฏ ก็สามารถระบุได้ว่าเครื่องคอมพิวเตอร์ของคุณติดสปายแวร์เข้าแล้ว)

- คุณจะพบว่ามีหน้าต่างเล็กๆ ที่เป็นโฆษณาป๊อบอัพขึ้นมาเองบ่อยครั้งจนนับไม่ถ้วน
- เมื่อคุณต้องการเข้าสู่เว็บไซต์ใดเว็บไซต์หนึ่งและพิมพ์ที่อยู่แอคเคาน์ (URL) ลงไปอย่างถูกต้องแล้ว แต่เว็บบราวเซอร์จะเข้าสู่เว็บไซต์ที่สปายแวร์ได้ตั้งไว้ และแสดงหน้าเว็บเหล่านั้น แทนที่จะเข้าไปยังเว็บไซต์ที่คุณต้องการ
- คุณจะสังเกตเห็นว่ามีแถบเครื่องมือใหม่ๆ ที่ไม่เคยเห็น หรือไม่คุ้นเคยเกิดขึ้นบนเว็บบราวเซอร์ของคุณ
- บริเวณ task tray ในส่วนแสดงการเปิดโปรแกรมที่กำลังรันอยู่ด้านล่างของหน้าต่างวินโดว์จะปรากฏแถบแสดงเครื่องมือหรือไอคอนที่ไม่เคยเห็นมาก่อน หรือไอคอนแปลกๆ
- หน้าหลักของบราวเซอร์ที่คุณเซ็ตค่าไว้ถูกเปลี่ยนไปในทันที
- เมื่อคุณเรียก search engine ที่คุณเคยใช้ในการค้นหาขึ้นมา และทำการค้นหา หรือทันทีที่คลิ้กปุ่ม search เว็บบราวเซอร์จะไปเรียกหน้าเว็บที่แตกต่างไปจากเดิม

- ฟังก์ชั่นบนคีย์บอร์ดบางอย่างที่เคยใช้งานจะเกิดอาการผิดปกติ เช่น เคยกดปุ่ม tab เพื่อเลื่อนไปยังช่องกรอกข้อความในฟิลด์ถัดไปบนหน้าเว็บจะไม่สามารถใช้ในการเลื่อนตำแหน่งได้เหมือนเดิม เป็นต้น
- ข้อความแสดงความผิดพลาดของซอฟต์แวร์วินส์โดว์จะเริ่มปรากฏบ่อยมากขึ้น
- เครื่องคอมพิวเตอร์ของคุณจะทำงานช้าลงอย่างเห็นได้ชัดเมื่อสั่งเปิดโปรแกรมหลายโปรแกรม หรือทำงานหลายอย่าง โดยเฉพาะในระหว่างการบันทึกแฟ้มข้อมูล เป็นต้น

การป้องกันสปายแวร์ไม่ให้แอบเข้ามาติดตั้งในเครื่องคอมพิวเตอร์ของคุณ

เพื่อที่จะป้องกันการเข้ามาติดตั้งสปายแวร์อย่างไม่ได้ตั้งใจ แนะนำให้ปฏิบัติตามวิธีการ ดังนี้

1.ไม่คลิ้กลิ้งบนหน้าต่างเล็กๆ ที่ปรากฏขึ้นมาอัตโนมัติหรือโฆษณาที่ป๊อบอัพขึ้นมา เพราะป๊อบอัพเหล่านั้นมักจะมีตัวสปายแวร์ฝังอยู่ การคลิ้กลิ้งเหล่านั้นจะทำให้สปายแวร์ถูกนำเข้ามาติดตั้งบนเครื่องของคุณผ่านวินโดวส์ได้ในทันที ส่วนวิธีการปิดหน้าต่างป๊อบอัพเหล่านั้นควรคลิ้กที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar)

ตัวอย่าง ไดอะล็อกบ็อกซ์ที่ควรปิดด้วยการกด ปุ่ม "X"

2.ควรเลือกที่คำตอบ "No" ทุกครั้งที่มีคำถามต่างๆ ถามขึ้นมาจากป๊อบอัพเหล่านั้น คุณต้องระมัดระวังเป็นอย่างมากกับคำถามที่ปรากฏขึ้นมาเป็นไดอะล็อกบ็อกซ์ต่างๆ แม้ว่าไดอะล็อกบ๊อกซ์เหล่านั้นจะเกิดขึ้นตอนคุณกำลังรันโปรแกรมเฉพาะที่คุณจะใช้งาน หรือใช้โปรแกรมอื่นอยู่ก็ตาม ควรปิดหน้าต่างป๊อบอัพเหล่านั้นด้วยวิธีคลิ้กที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar)

3.ควรระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี เพราะมีหลายเว็บไซต์ที่จัดหาแถบเครื่องมือแบบที่ให้ผู้ใช้ปรับแต่งเองหรือมีคุณสมบัติอื่นๆ ที่เหมาะสำหรับผู้ใช้ให้ปรับแต่งเองไว้ให้ดาวน์โหลดบนอินเทอร์เน็ต สำหรับท่านที่ต้องการใช้คุณสมบัติของเครื่องมือเหล่านี้ ไม่ควรจะดาวน์โหลดเครื่องมือเหล่านี้มาจากเว็บไซต์ที่ไม่น่าเชื่อถือ และต้องตระหนักเสมอว่ามันเป็นการปล่อยให้สปายแวร์ผ่านเข้ามายังเครื่องคุณได้ด้วย

4.ไม่ควรติดตามอีเมล์ลิ้งที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันสปายแวร์ เหมือนกับอีเมล์ที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันไวรัส ซึ่งอันที่จริงลิ้งเหล่านั้นจะนำไปสู่แนวทางที่ตรงกันข้าม คือเป็นการถามเพื่อให้คุณคลิ้กอนุญาตให้สปายแวร์เข้ามาดำเนินการติดตั้งในเครื่องโดยไม่ถูกขัดขวาง

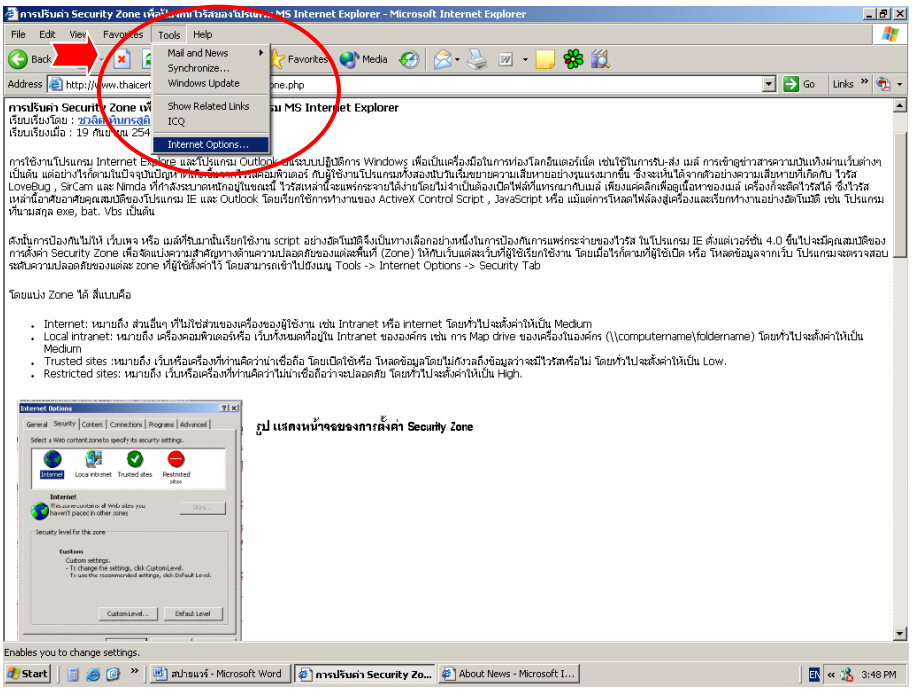
เพิ่มความปลอดภัยให้กับเครื่องคอมพิวเตอร์ของคุณเพื่อลดความเสี่ยงต่อการติดสปายแวร์

โดยเฉพาะอย่างยิ่งหากคุณรู้สึกว่าเครื่องของคุณเสี่ยงต่อการติดสปายแวร์ควรปฏิบัติตามวิธีการต่อไปนี้เพื่อเป็นการลดความเสียงในการติดสปายแวร์

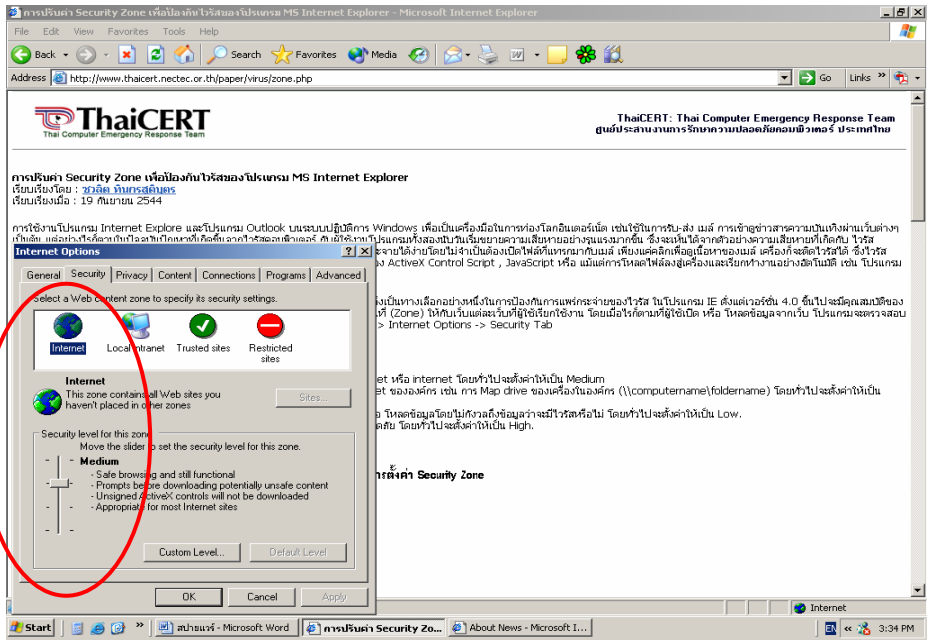
ปรับแต่งบราวเซอร์ไม่ให้อนุญาตให้รันป๊อบอัพ และคุกกี้ไฟล์ เนื่องจากป๊อบอัพเหล่านี้มักเกิดจากสคริปต์ที่รันโดยวินโดว์หรือเนื้อหาที่มีการรันอัตโนมัติ การปรับแต่งภายในบราวเซอร์เป็นไปเพื่อลดหรือป้องกันไม่ให้สคริบต์หรือแอคทีฟคอนเทนต์ (Active Content) หรือลดจำนวนป๊อบอัพที่มักปรากฏขึ้นเองบ่อยๆ บางบราวเซอร์จะมีเครื่องมือปรับแต่งหรือปิดกั้น หรือจำกัดการป๊อบอัพของวินโดว์ ไฟล์คุกกี้ถาวรบางประเภทก็

จัดเป็นสปายแวร์เช่นกัน เพราะมันจะเปิดเผยว่าคุณเข้าสู่เว็บเพจอะไรบ้าง คุณสามารถปรับแต่งค่าความปลอดภัยบนบราวเซอร์ให้อยู่ในระดับที่มีความปลอดภัยสูง หรืออนุญาตเฉพาะไฟล์คุกกี้ของเว็บที่กำลังจะเข้าถึงเท่านั้น (ดูเพิ่มเติมได้ที่ browsing safely: Understanding active content and cookies for more information) หรือ ดูได้จากบทความเผยแพร่ไวรัส เรื่องการปรับค่า Security Zone เพื่อป้องกันไวรัสของโปรแกรม MS Internet Explorer เรียบเรียงโดย : ชวลิต ทินกรสูติบุตร เรียบเรียงเมื่อ : 19 กันยายน 2544 หรือปฏิบัติตามขั้นตอนต่อไปนี้

ขั้นที่ 1 ไปที่ Tool -> Internet option -> Security tab

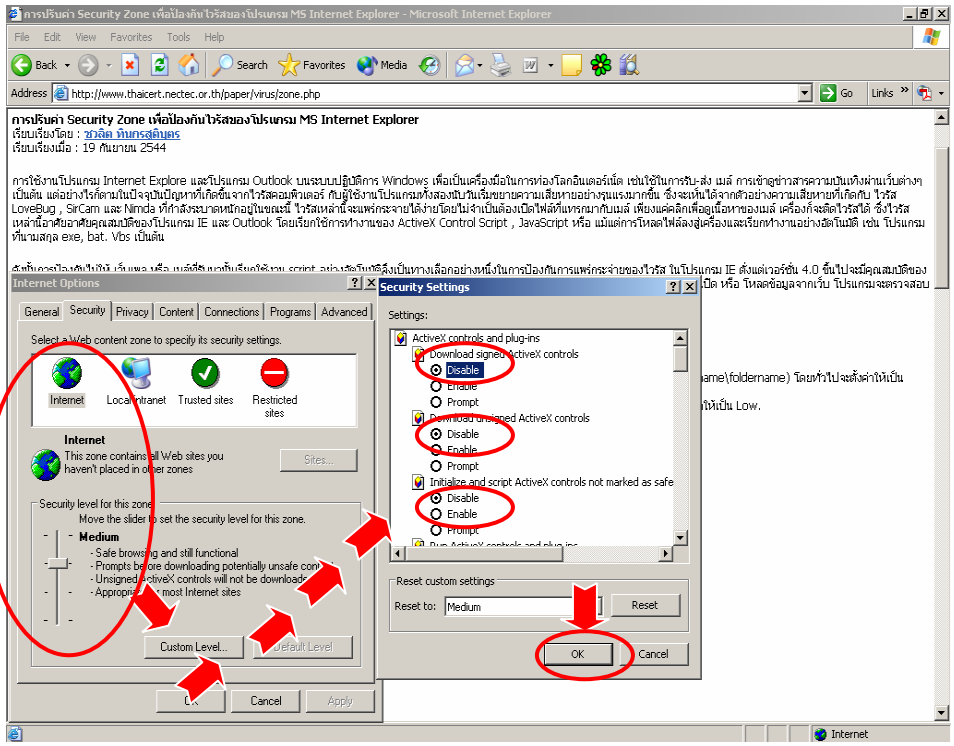


ขั้นที่ 2 เมื่อเลือกแถบ Security แล้ว คลิ้กเลือก internet (ดังภาพ)



ขั้นที่ 3 คลิ้กที่แถบ Custom Level บริเวณด้านล่างของบ็อกซ์ (ดังภาพ) จากนั้นให้คลิ้ก Disable ActiveX Active script , Java Script และ File Download และกดปุ่ม OK

หมายเหตุ คุณต้องแน่ใจก่อนว่าผลที่เกิดจากการยกเลิกคุณสมบัติเหล่านี้จะไม่กระทบต่อการเรียกใช้งานระบบผ่านเว็บโดยผู้พัฒนาขององค์กร หากมีกรณีดังกล่าวเกิดขึ้นขอให้คุณติดต่อฝ่ายไอทีขององค์กรเป็นผู้ปรับแต่งค่าเหล่านี้ให้แทน



วิธีกำจัดสปายแวร์

- ทำการสแกนเครื่องคอมพิวเตอร์อย่างถี่ถ้วน ด้วยโปรแกรมแอนติไวรัส ซึ่งแอนติไวรัสบางยี่ห้อจะมีคุณสมบัติในการค้นหาและกำจัดสปายแวร์ แต่แอนติไวรัสอาจไม่สามารถมองหาสปายแวร์พบแบบ real time ได้ ดังนั้นควรกำหนดให้โปรแกรมแอนติไวรัสของคุณทำการสแกนหาไวรัสเมื่อเครื่องอยู่ในสภาวะปลอดจากการใช้งานใดๆ และควรทำการสแกนอย่างถี่ถ้วนและสม่ำเสมอ เช่น วันละครั้งหลังเลิกงาน เป็นต้น
- ทำการติดตั้งโปรแกรมแอนติสปายแวร์ที่มีลิขสิทธิ์และถูกออกแบบมาเพื่อกำจัดสปายแวร์โดยเฉพาะมีผู้ผลิตหลายรายที่เสนอผลิตภัณฑ์ที่มีคุณสมบัตินี้ซึ่งจะสแกนหาสปายแวร์บนเครื่องและกำจัดสปายแวร์ออกจากเครื่องได้ สำหรับผลิตภัณฑ์แอนติสปายแวร์ที่เป็นที่นิยม ได้แก่ LavaSoft'Adaware, Webroot's SpySweeper, PestPatrol, Spybot Search and Destroy (ตามลิ้งก์ด้านล่าง)
- หรือเข้าอ่านในเว็บไซต์ ThaiCERT เรื่องวิธีการใช้งานโปรแกรม Ad-aware เขียนโดย คุณกิติศักดิ์ จิรวรรณกูล (http://www.thaicert.nectec.or.th/paper/spyware/AdawareHowToEliminateSpyware.pdf)

แหล่งข้อมูลเพิ่มเติม

http://www.lavasoftusa.com/software/adaware/
http://www.spywarewarrior.com/
http://www.spysweeper.com/
http://www.pestpatrol.com/
http://www.safer-networking.org/en/index.html

แหล่งข้อมูลอ้างอิง

Mindi McDowell, Matt Lyte, http://www.us-cert.gov/cas/tips/ST04-016.html

ผู้เรียบเรียง น.ส.ดวงกมล ทรัพย์พิทยากร
ผู้ตรวจสอบ นายบรรจง หะรังษี(ดร.)