การกำจัดและป้องกันไวรัส

ไวรัสคอมพิวเตอร์(Virus) คืออะไร

ไวรัสคอมพิวเตอร์เป็นโปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้ และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการ นำเอายูเอสบีแฟลชไดร์ฟที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสาร

สปายแวร์ (Spyware) คืออะไร

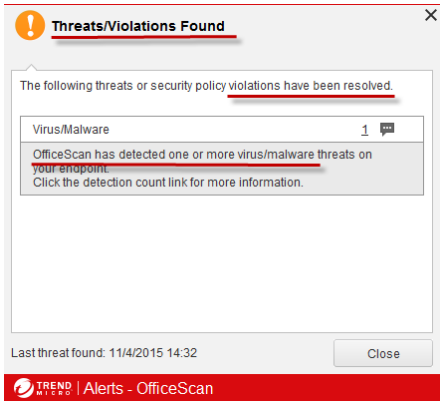
สปายแวร์คือ โปรแกรมที่แฝงเข้ามาในคอมพิวเตอร์ขณะที่คุณท่องอินเตอร์เน็ต เป็นโปรแกรมที่ถูกเขียนขึ้นมาสอดส่อง (สปาย) หรือดักจับข้อมูลการใช้งานเครื่องคอมพิวเตอร์ของคุณ สปายแวร์ อาจเข้ามาเพื่อโฆษณาสินค้าต่าง ๆ บางตัวก็สร้างความรำคาญเพราะจะเปิดหน้าต่างโฆษณาบ่อย ๆ แต่บางตัว ร้ายกว่านั้น คือ ทำให้คุณใช้อินเตอร์เน็ทไม่ได้เลย

อาการติดไวรัสเบื้องต้น

1. เครื่องมีการรีสตาร์ทหรือเครื่องปิดตัวเองลงขณะที่กำลังใช้งานอยู่หรือเมื่อเปิดเครื่องแล้วไม่ สามารถบูตเข้าสู่วินโดวส์ได้
2. เกิดไฟล์ขึ้นเองโดยไม่ได้สร้างขึ้น เช่น Autorun.inf หรือไฟล์นามสกุล .vbs ปรากฏตามไดร์ฟต่างๆ
3. เนื้อที่ในฮาร์ดดิสก์ลดลงโดยไม่ทราบสาเหตุโดยไม่ได้ติดตั้งโปรแกรม หรือนำข้อมูลมาลงไว้
4. วินโดวส์แสดงไดอะลอกบ๊อกซ์ข้อความโดยไม่ทราบสาเหตุ หรือมีโปรแกรมบางตัวทำงานเองโดยไม่ได้เรียกใช้งาน
5. คอมพิวเตอร์ทำงานช้าอย่างผิดปกติทั้งๆ ที่ไม่ได้เปิดใช้โปรแกรมใดๆ
6. ไฟล์ข้อมูลมีขนาดใหญ่ขึ้นมากแบบผิดปกติทุกครั้งที่ใช้งาน
7. เครื่องคอมพิวเตอร์เกิดอาการแฮงค์ (Hang) โดยไม่ทราบสาเหตุ
8. โปรแกรมป้องกันไวรัสไม่สามารถเปิดได้หรือเปิดโปรแกรมต่างๆ ไม่ได้หรือบางครั้งโปรแกรมที่ใช้ประจำหายไป
9. มี Pop up ขึ้นมาบ่อยๆ ในขณะที่เราเข้าเว็บ หรือถึงแม้จะไม่ได้ต่อ internet
10. Toolbar ของ browser มีแถบปุ่มเครื่องมือเพิ่มขึ้น โดยที่เราไม่ได้ติดตั้งอะไรเสริมเลย
11. หน้า Desktop มีไอคอนประหลาดๆ เพิ่มขึ้น

การแสกน และกำจัดไวรัส

โปรแกรมป้องกันไวรัสหลายๆ ยี่ห้อจะมีระบบป้องกันเปิดอยู่ตลอดเวลาที่เปิดเครื่อง (real time protect) เมื่อมีไวรัสเข้ามาโปรแกรมจะตรวจจับและกำจัดไวรัสทันที พร้อมทั้งแจ้งให้ผู้ใช้ทราบ



รูปที่ 1 real time protect ของโปรแกรม Trend micro

รูปที่ 2 real time protect ของโปรแกรม ESET NOD32

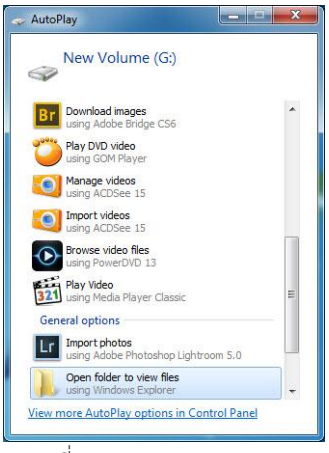
รูปที่ 3 real time protect ของโปรแกรม AVG

บางโปรแกรมอาจไม่กำจัดไวรัสเอง จะแจ้งข้อความ และให้เราเลือกว่าจะจัดการกับตัวไวรัสเอง เช่นรูปที่ 3 โปรแกรม AVG จะแจ้งว่าเจอไวรัส จะให้เลือกวิธีการ 3 หัวข้อ คือ

- Move to Vault กักไวรัส
- Go to file เปิดเข้าไปดูไฟล์ตัวปัญหา
- Ignore the threat ละเว้นไฟล์ที่เจอ

การสแกนไวรัส

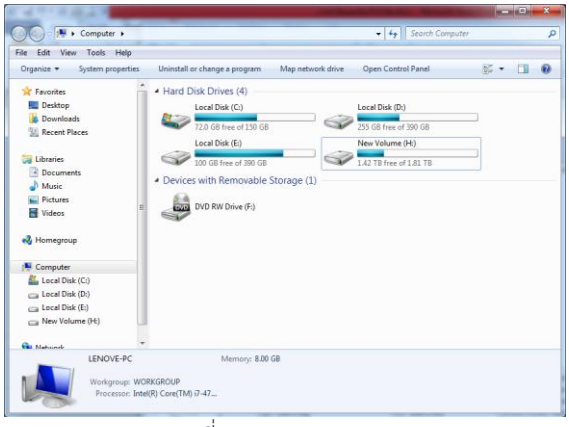
กรณีที่เสียบ USB Flash Drive บางเครื่องจะมี Auto play pop up ขึ้นมาให้เลือกว่าจะทำอะไรกับ Flash Drive ดังรูปที่ 4 ถ้าขึ้นแบบนี้มา ให้คลิกปิดไป ถ้าเราคลิกตัวเลือกใด ตัวเลือกหนึ่ง และบังเอิญ Flash Drive ตัวนั้นมีไวรัส อาจจะทำให้เราติดไวรัสที่ชื่อ Autorun ได้



รูปที่ 4 Auto play pop up

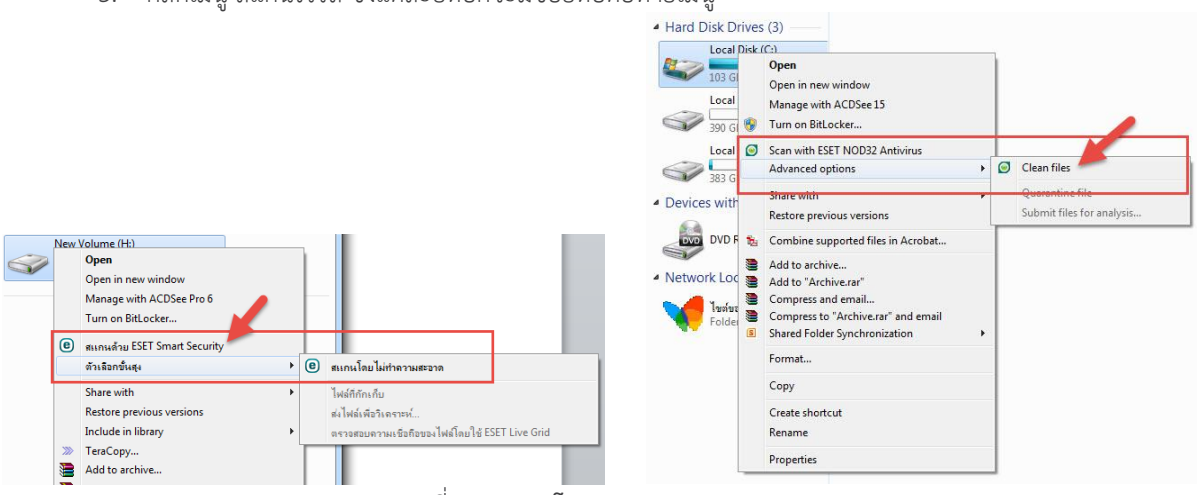
หลังจากปิด Auto play แล้วให้สแกนหาไวรัส ซึ่งโปรแกรมป้องกันไวรัสหลายๆ ยี่ห้อ มีขั้นตอนการสแกนไวรัสคล้ายๆกัน ดังนี้

1. เปิด My Computer ขึ้นมา

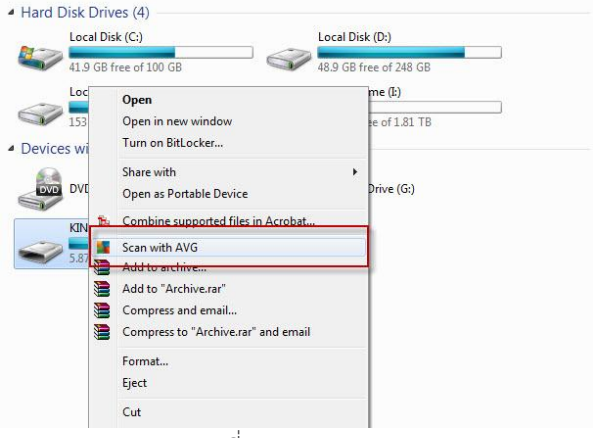


รูปที่ 5 My Computer

2. คลิกขวาที่ไดร์ฟที่ต้องการสแกน โดยจะมีเมนูสแกนไวรัสให้เลือก
3. คลิกเมนู สแกนไวรัส ซึ่งแต่ละยี่ห้อก็จะมีชื่อยี่ห้อต่อท้ายเมนู



รูปที่ 6 เมนูของ**โปรแกรม ESET NOD32**



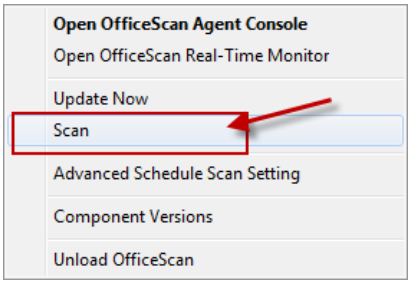
รูปที่ 7 เมนูของ AVG

โปรแกรม Trend Micro จะไม่มีเมนูตอนคลิกขวาที่ไดร์ฟ เราต้องเปิดตัวโปรแกรมแล้วสั่งสแกน ดังนี้

1. คลิกขวาที่ไอคอนของโปรแกรม ซึ่งจะอยู่ตรงมุมล่างขวาของจอ

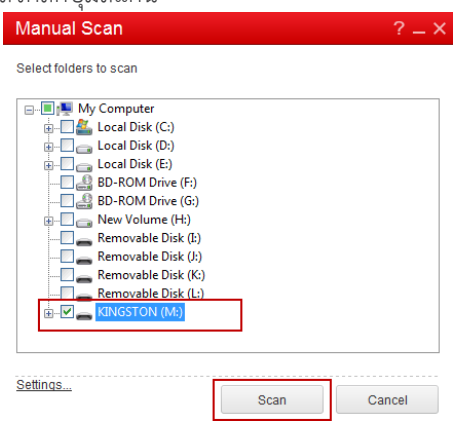
รูปที่ 8 ไอคอน Trend Micro

2. เลือกเมนู Scan เพื่อเปิดหน้าการทำงานของ Trend Micro ขึ้นมา



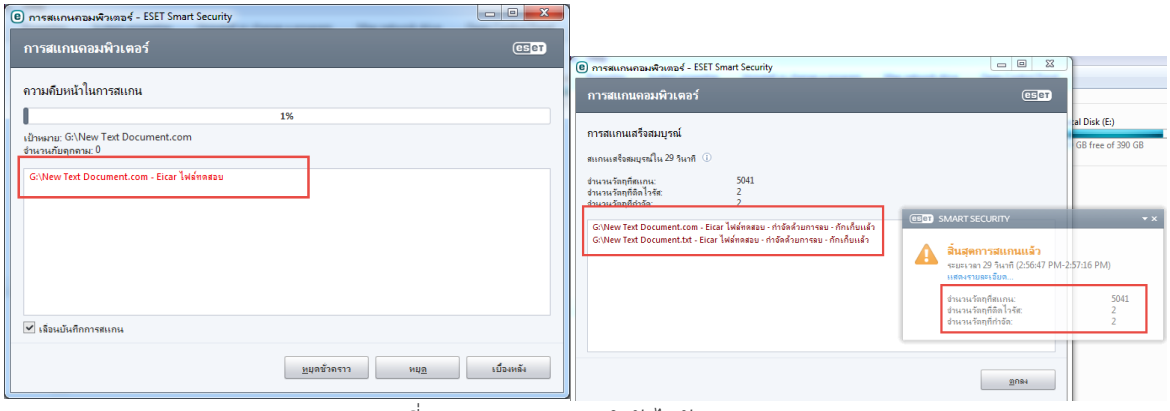
รูปที่ 9 เลือกเมนู Scan

3. เลือกไดร์ฟที่ต้องการสแกน แล้วคลิกปุ่มสแกน

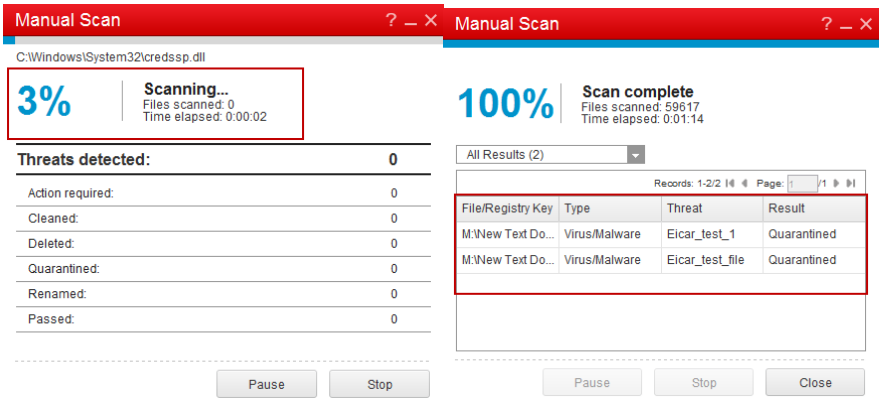


รูปที่ 10 เลือกไดร์ฟ และคลิก Scan

จากนั้นโปรแกรมจะทำการสแกนหาไวรัส รอจนกว่าจะสแกนเสร็จ ถ้าหากเจอไวรัสก็จะกำจัดไวรัสให้เองอยู่แล้ว และแสดงรายการไวรัส พร้อมทั้งบอกสถานการณ์กำจัดจะมี Cleaned กับ Quarantined หากไม่สามารถกำจัดได้ จะให้เราเลือกการกำจัดเอง เช่นโปรแกรม AVG



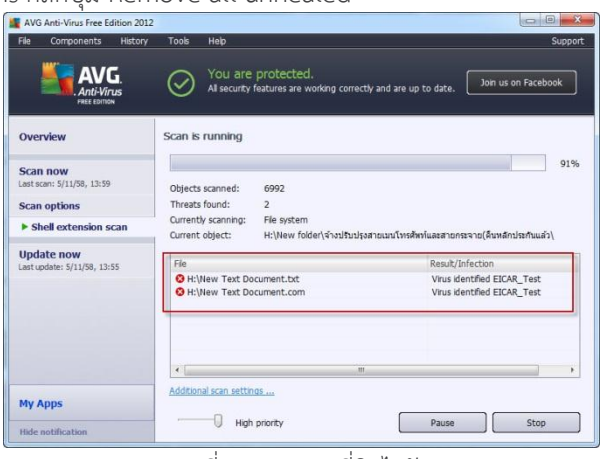
รูปที่ 11 การสแกนและกำจัดไวรัสของ ESET NOD32



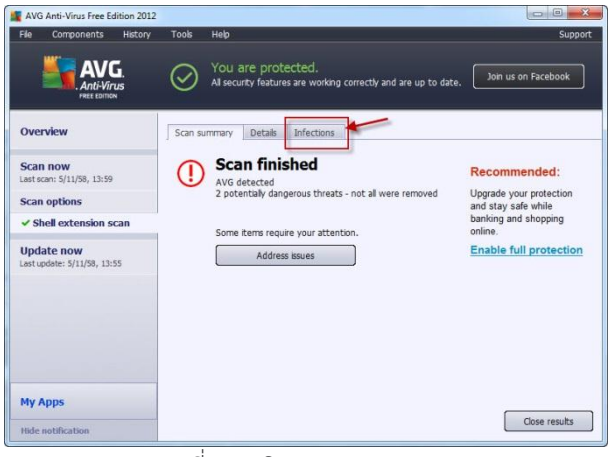
รูปที่ 12 การสแกนและกำจัดไวรัสของ Trend Micro

ส่วน AVG จะไม่กำจัดไวรัสให้ เราต้องเลือกการกำจัดเอง

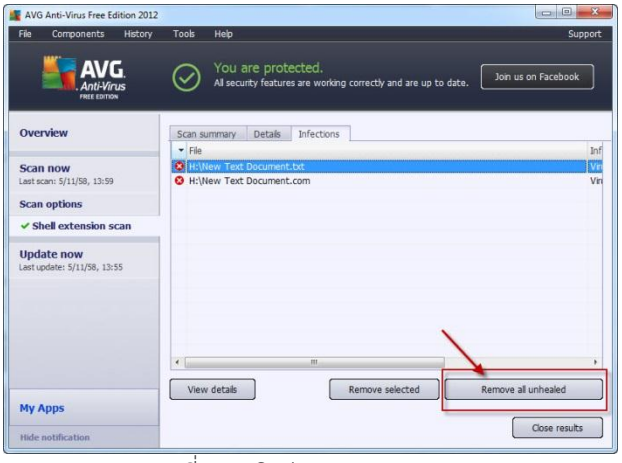
- คลิกแทบ infections
- ที่หน้า infections คลิกปุ่ม Remove all unhealed



รูปที่ 13 รายการที่ติดไวรัส



รูปที่ 14 คลิกแทบ Infections



รูปที่ 15 คลิกปุ่ม Remove all unhealed

วิธีสแกนไวรัสที่กล่าวมา สามารถใช้ได้กับ Flash Drive และ ไดร์ฟ ต่างๆ ของเครื่องคอมพิวเตอร์

แนวทางการป้องกันไวรัสและสปายแวร์

การติดไวรัสคอมพิวเตอร์สามารถได้มาจากหลายทางดังนี้

1. ไวรัสจากอินเตอร์เน็ต
2. USB Flash Drive
3. ไวรัสจากการเชื่อมต่อเครือข่าย
4. ติดตั้งซอฟท์แวร์ผิดลิขสิทธิ์แล้วโดนโปรแกรมประสงค์ร้ายแถมมา
5. ถูกหลอก หรือรู้เท่าไม่ถึงการณ์ติดตั้งโปรแกรมที่ไม่รู้จัก หรือคลิกลิงค์ที่เชื่อมต่อกับเว็บไซต์ที่เป็น ไวรัส
6. ติดไวรัสผ่านทางจดหมายอิเล็กทรอนิกส์ (e-mail) เนื่องจากตั้งรหัสผ่านที่สามารถเดาได้ง่าย เสี่ยงต่อการถูกแฮ็ค

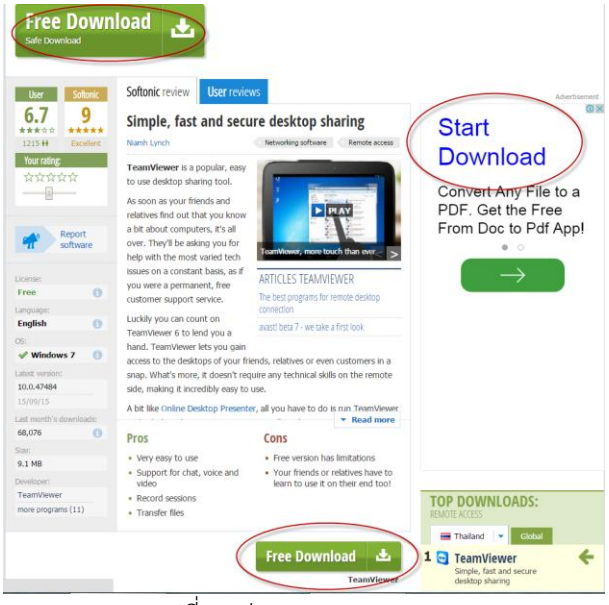
วิธีการป้องกัน สปายแวร์

เพื่อที่จะป้องกันการเข้ามาติดตั้งสปายแวร์อย่างไม่ได้ตั้งใจ แนะนำให้ปฏิบัติตามวิธีการ ดังนี้

1. เมื่อเข้าเว็บไซต์ต่างๆ ไม่คลิกลิ้งค์บนหน้าต่างเล็กๆ ที่ปรากฏขึ้นมาอัตโนมัติหรือโฆษณาที่ป๊อบอัพขึ้นมา เพราะป๊อบอัพเหล่านั้นมักจะมีตัวสปายแวร์ฝังอยู่ การคลิ้กลิ้งเหล่านั้นจะทำให้สปายแวร์ถูกนำเข้ามาติดตั้งบนเครื่องของคุณผ่านวินโดวส์ได้ในทันที

รูปที่ 16 โฆษณา ที่ล่อหลอกให้คลิกเข้าไป

2. กรณีที่ไม่มีปุ่มปิด ควรเลือกที่คำตอบ "No" ทุกครั้งที่มีคำถามต่างๆ ถามขึ้นมาจากป๊อบอัพเหล่านั้น ต้องระมัดระวังเป็นอย่างมากกับคำถามที่ปรากฏขึ้นมาเป็นไดอะล็อกบ็อกซ์ต่างๆ แม้ว่าไดอะล็อกบ๊อกซ์เหล่านั้นจะเกิดขึ้นตอนคุณกำลังรันโปรแกรมเฉพาะที่คุณจะใช้งาน หรือใช้โปรแกรมอื่นอยู่ก็ตาม ควรปิดหน้าต่างป๊อบอัพเหล่านั้นด้วยวิธีคลิ้กที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar)
3. ควรระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี เพราะมีหลายเว็บไซต์ จะมีปุ่มหลอกให้คลิก โดยเฉพาะปุ่ม Download หากเป็นเว็บไซต์ที่ไม่น่าเชื่อถือต้องตระหนักเสมอว่ามันเป็นการปล่อยให้สปายแวร์ผ่านเข้ามายังเครื่องคุณได้ด้วย



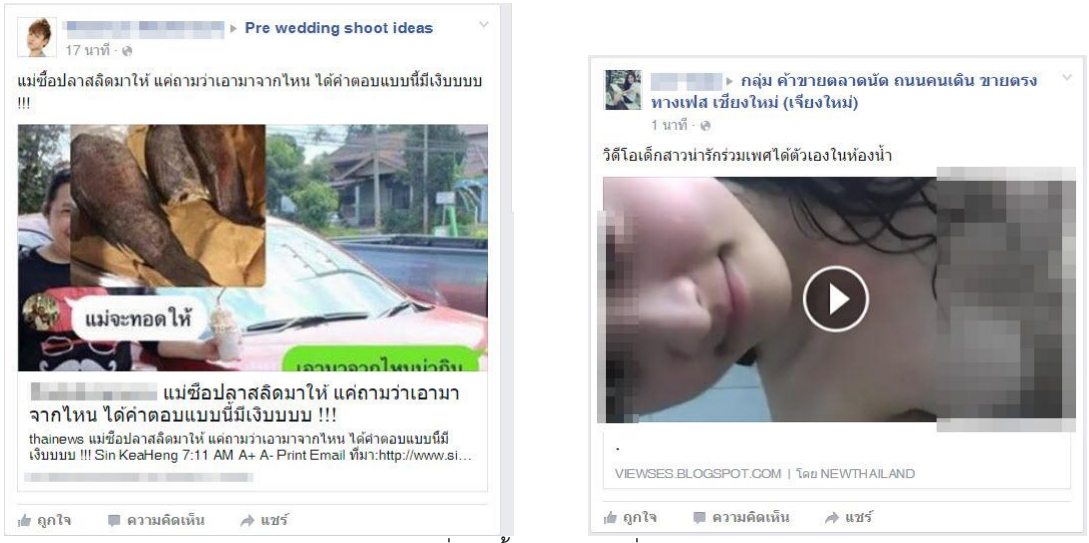
รูปที่ 17 ปุ่มหลอก Download

ใช้ความระมัดระวังในการเปิดอ่าน E-mail

1. อย่าเปิดไฟล์ที่แนบมากับ E-mail จนกว่าจะรู้ที่มา
2. อย่าเปิดอ่าน E-mail ที่มีชื่อเรื่อง ที่เป็นข้อความจูงใจ
3. ลบ E-mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที เพื่อตัดปัญหาทั้งปวง

ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเตอร์เน็ต

1. ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา Social Network เช่น skype, facebook, twitter เป็นต้น หรือการแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่มีนามสกุล .exe , .pif , .com , .bat , .vbsเป็นต้นโดยไม่ได้ตรวจสอบแหล่งที่มาก่อน
2. ไม่ควรเข้าเว็บไซต์ที่มากับ E-mail หรือโปรแกรมสนทนาต่าง ๆรวมทั้งโฆษณาชวนเชื่อ หรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ตั้งใจ



รูปที่ 18 ลิ้งค์อันตราย ที่แฝงมากับเฟซบุ๊ค

3. ไม่ดาวน์โหลดไฟล์ต่าง ๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
4. หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ถ้าต้องการแชร์ไฟล์ ควรแชร์แบบอ่านอย่างเดียว