**मैलवेयर से बचाव**

1. ऑपरेटिंग सिस्टम, एंटी-वायरस और एप्लिकेशन के लिए हमेशा ऑटोमेटिक अपडेट सेट करके रखें। (माई कंप्यूटर -> प्रापर्टी-> ऑटोमेटिक अपडेट के लिए ऑटोमेटिक और टाइम पर क्लिक करें)

2. किसी भी असामान्य या हिडन फ़ाइल को ढूंढने के लिए हिडन फ़ाइल और सिस्टम फ़ाइल अवलोकन को इनेबल करें। (माई कंप्यूटर -> टूल -> फ़ोल्डर विकल्प -> अवलोकन ->"हिडन फ़ाइल और फ़ोल्डर्स देखें" विकल्प के साथ चयन करें और "हाइड संरक्षित ऑपरेटिंग सिस्टम फ़ाइलों" को डिसेबल करें)

3. ऑटो प्ले बंद करें (स्टार्ट -> रन -> gpedit.msc टाइप करें -> कंप्यूटर कॉन्फ़िगरेशन -> एडमिनिस्ट्रेटिव टेम्प्लेट -> विंडोज कंपोनेंट्स ->"ऑटोप्ले पोलिसी " चुनें ->"टर्न ऑफ ऑटो प्ले " पर डबल क्लिक करें -> इंनबेल क्लिक करें ->"टर्न ऑफ ऑटो प्ले" को "सभी ड्राइव" पर सेट करें और ओके पर क्लिक करें।)

4. %temp% को "रन" टाइप करें और किसी भी संदिग्ध अटैचमेंट को ओपन करने के बाद सभी एन्ट्रीयों को हटा दें।

5. रन में cmd टाइप करें और Netstat –na टाइप करें। फोरन इस्टेबलिश्ड कनेक्शन और आईपी अड्रैस की जांच करें। इसके स्वामित्व के लिए आईपी पते की जाँच करें।

6. "रन" में "msconfig" टाइप करें और किसी भी ऑटोमेटिक रनिंग अनयुजवल एक्जुक्यूटेबल की जांच करें।

7. नेटवर्क आइकन की जांच करें (प्राप्त और भेजे गए पैकेट के लिए) I गैर-ब्राउज़िंग मोड में डेटा के लिए एडीएसएल लाइट का उपयोग करे। यदि आउटगोइंग असामान्य रूप से अधिक है, तो यह संभव है कि सिस्टम से हैक हो गया है।

8. Cmd प्रॉम्प्ट में "ipconfig/displaydns" टाइप करें और किसी भी यूआरएल को देखें जिसे आपने हाल ही में एक्सेस नहीं किया है।

9. ज्ञात स्रोतों से भी अटैचमेंट खोलते समय हमेशा सतर्क रहें। अटैचमेंट खोलने के लिए नॉन-नेटिव एप्लिकेशन का उपयोग करने का प्रयास करें। उदाहरण के लिए वर्ड दस्तावेज़ उपयोग, अटैचमेंट ओपन के लिए वर्डपैड का उपयोग।

10. जब संदेह हो, तो कुछ "पैच वर्क" करने के बजाय इंटरनेट से जुड़े कंप्यूटर को फॉरमैट करना बेहतर होगा।

11. लोकल एडमिनिस्ट्रेटर्स के लिए सिस्टम (आरडीपी, एसएमबी, आरपीसी) में किसी भी दूरस्थ लॉगऑन को प्रतिबंधित करें।

12. सभी एंडपॉइंट वर्कस्टेशनों पर एप्लिकेशन व्हाइटलिस्टिंग 'सॉफ़्टवेयर प्रतिबंध नीतियों को लागू करें। यह मैलवेयर ड्रॉपर्स या अनधिकृत सॉफ़्टवेयर को एंडपॉइंट पर निष्पादन करने से रोकेगा।

13. नेटवर्क पर वेब और ईमेल फ़िल्टर तैनात करें। ज्ञात ख़राब डोमेन, स्रोतों और पतों को स्कैन करने के लिए इन उपकरणों को कॉन्फ़िगर करें; संदेश प्राप्त करने और डाउनलोड करने से पहले इन्हें ब्लॉक करें।

14. फ़ाइल और प्रिंटर शेयरिंग सेवाओं को हटाए। यदि इन सेवाओं की आवश्यकता है, तो मजबूत पासवर्ड या सक्रिय निर्देशिका प्रमाणीकरण का उपयोग करें।

15. माइक्रोसॉफ्ट ऑफिस दस्तावेज़ों में मैक्रोज़ को डिसेबल करे (doc/docx, xls/xlsx, ppt/pptx और mdb/accdb), डिफ़ॉल्ट रूप से, Microsoft उत्पाद VBS मैक्रो डिसेबल के साथ आते हैं। ऑफिस बटन-> वर्ड विकल्प ट्रस्ट सेंटर-> ट्रस्ट सेंटर सेटिंग्स -> मैक्रोज़ सेटिंग्स।

16. पीडीएफ फाइलों के लिए एडोब एक्रोबैट रीडर में जावा स्क्रिप्ट या समान स्क्रिप्टिंग फ़ंक्शन को डिसेबल करें।

17. माइक्रोसॉफ्ट ऑफिस वर्ड दस्तावेजों को संरक्षित अवलोकन में खोलने के लिए माइक्रोसॉफ्ट ऑफिस 2010 में "संरक्षित अवलोकन" सेटिंग्स के लिए अंतर्निहित सुविधा को कॉन्फ़िगर करें: ऑफिस बटन -> वर्ड विकल्प -> ट्रस्ट सेंटर -> ट्रस्ट सेंटर सेटिंग्स -> संरक्षित दृश्य