পেন ড্রাইভ ভাইরাস (ওয়ার্ম) প্রতিরোধের উপায়

পেন ড্রাইভ পিসিতে লাগিয়ে ড্রাইভ আইকনে ডাবল-ক্লিক করা মাত্রই ওয়ার্ম (যদি থাকে) সক্রিয় হয়ে যায়। তাই পেন ড্রাইভ প্রবেশ করিয়ে কোন অবস্থাতেই ড্রাইভ আইকনে ডাবল-ক্লিক করা যাবে না। এমনকি পেন ড্রাইভ আইকনে রাইট ক্লিক করে সেখান থেকে Open, Explore, Search প্রভৃতি মেনু সিলেক্ট করে পেন ড্রাইভে ঢুকার চেষ্টা করলেও ওয়ার্ম সক্রিয় হয়ে উঠতে পারে। তাহলে কিভাবে পেন ড্রাইভে অ্যাকসেস করা যাবে? এর বিভিন্ন পদ্ধতি রয়েছে। তবে সবচেয়ে সহজ ও নিশ্চিত কার্যকর পদ্ধতি নিম্নরূপ: (উল্লেখ্য, ধরে নেওয়া হচ্ছে যে, আপনার পিসিতে কোন ধরনের ওয়ার্ম সক্রিয় অবস্থায় নেই। আপনার পিসিতে ওয়ার্ম সক্রিয় অবস্থায় রয়েছে কি না তা জানার জন্য ‘‘ওয়ার্ম প্রতিকারের উপায়’’ অনুচ্ছেদটি দেখুন, যা এ প্রবন্ধটির বৃহত্তর সংস্করণে রয়েছে। প্রবন্ধটির বৃহত্তর সংস্করণটি ডাউনলোড করার জন্য নিচের লিংকটি ভিজিট করুন: http://www.islaamlib.com/softwares/Malware_Cleaning.pdf)

১. পেন ড্রাইভ প্রবেশ করিয়ে মাই কম্পিউটারে রাইট-ক্লিক করুন। মেনু থেকে Explore-এ ক্লিক করুন।

২. Tools মেনু থেকে Folder Options-এ ক্লিক করুন।

৩. View ট্যাবে ক্লিক করুন।

৪. নিচের Advanced settings অপশনগুলো থেকে Hidden files and folders অপশনের অন্তর্গত Show hidden files and folders অপশনে ক্লিক করুন।

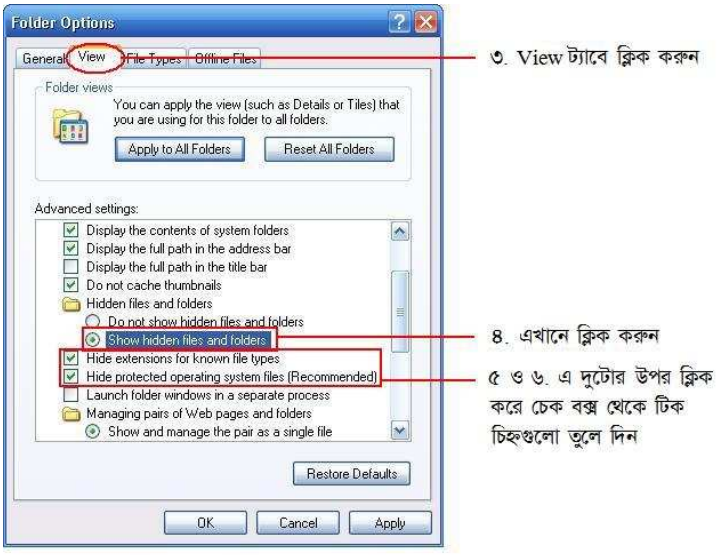
চিত্র: ওয়ার্ম প্রতিরোধের পদ্ধতি (১ম ও ২য় ধাপ)।

৫. ঠিক নিচে অবস্থিত Hide extensions for known file types অপশনের বাম পাশের চেক বক্স থেকে টিক চিহ্ন তুলে দিন।

৬. তার ঠিক নিচে অবস্থিত Hide protected operating system files (Recommended) অপশনের বাম পাশের চেক বক্স থেকেও টিক চিহ্ন তুলে দিন। পর্দায় আগত সতর্ক বার্তার Yes বোতামে ক্লিক করুন।

৭. OK বোতামে ক্লিক করুন।

সামনে অগ্রসর হওয়ার পূর্বে এতক্ষণ কী করা হল তা জেনে নেওয়া দরকার।



চিত্র: ওয়ার্ম প্রতিরোধের পদ্ধতি (৩য় থেকে ৬ষ্ঠ ধাপ)।

Show hidden files and folders অপশনটি সিলেক্ট করা থাকলে আপনার পিসির সকল hidden ফাইল প্রদর্শিত হবে। ওয়ার্ম ফাইলগুলো হিডেন থাকে। তাই সেগুলোকে ডিটেক্ট করতে হলে এ অপশনটি অবশ্যই সিলেক্ট করতে হবে।

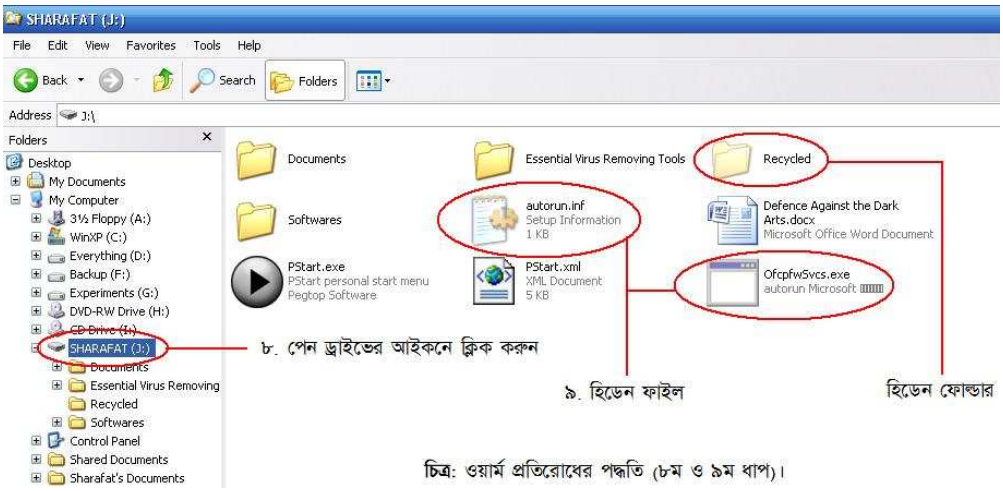
Hide protected operating system files - অপারেটিং সিস্টেমের গুরুত্বপূর্ণ ফাইলগুলো সর্বদা লুকোনো অবস্থায় থাকে। Show hidden files and folders অপশনটি সিলেক্ট করা থাকলেও এ সকল সিস্টেম ফাইল প্রদর্শিত হবে না। কেননা, যদি ভুলবশত এসব ফাইলের কোনটি মুছে যায়, তাহলে অপারেটিং সিস্টেম ঠিকমত বুট হবে না। ফলে উইন্ডোজ নতুন করে রি-ইন্সটল করার প্রয়োজন হতে পারে। তাই অতিরিক্ত সতর্কতার জন্য Show hidden files and folders অপশনটি সিলেক্ট করা থাকা সত্ত্বেও সেগুলো প্রদর্শিত হয় না। সমস্যা হল ওয়ার্ম ফাইলগুলোও সিস্টেম ফাইল হিসেবে থাকে। তাই Hide

protected operating system files -এর পাশ থেকে টিক চিহ্ন তুলে দিয়ে সিস্টেম ফাইলগুলো প্রদর্শনের ব্যবস্থাও করতে হবে।

Hide extensions for known file types অপশনটি থেকে টিক চিহ্ন তুলে দিলে সকল ফাইলের এক্সটেনশন দেখা যাবে। ফাইলের এক্সটেনশন প্রকাশ করে যে, ফাইলটি কোন্ প্রকারের। যেমন, মাইক্রোসফট ওয়ার্ডের একটি ফাইলের এক্সটেনশন হল doc । এক্সটেনশনকে ফাইলের নাম থেকে আলাদা করা হয় একটি ডট (.) দ্বারা। উদাহরণস্বরূপ, ঐ ওয়ার্ড ফাইলের নাম যদি হয় abc, তাহলে এক্সটেনশন সহ ফাইলটির নাম হবে abc.doc । এখানে abc হল ফাইলের নাম এবং doc হল ফাইলের এক্সটেনশন। অপারেটিং সিস্টেম doc অংশটি দেখলেই বুঝতে পারবে যে, এটি মাইক্রোসফট ওয়ার্ড ডকুমেন্ট ফাইল (যদি পিসিতে ওয়ার্ড ইন্সটল করা থাকে)। ভাইরাসের ক্ষেত্রে এক্সটেনশন প্রদর্শন কী কাজে দেয়, তা আমরা একটু পরেই দেখব।

এবার বাকি পদক্ষেপগুলো দেখা যাক:

৮. বাম দিকের প্যানেল থেকে পেন ড্রাইভের আইকনে ক্লিক করুন।



চিত্র: ওয়ার্ম প্রতিরোধের পদ্ধতি (৮ম ও ৯ম ধাপ)।

৯. এবার ডান দিকের প্যানেলে ফাইল-ফোল্ডারের তালিকা দেখুন। লক্ষ্য করুন যে, সেখানে autorun.inf নামে কোন ফাইল আছে না কি। যদি থাকে, তাহলে নিশ্চিতভাবে পেন ড্রাইভে ওয়ার্ম রয়েছে। এবার লক্ষ্য করুন আশ-পাশে কোন হিডেন ফাইল দেখা যায় কি না। হিডেন ফাইল-ফোল্ডারগুলো সাধারণ ফাইল-ফোল্ডারের তুলনায় আবছাভাবে প্রদর্শিত হয়। সাধারণভাবে পেন ড্রাইভের স্বত্বাধিকারীর জানা থাকার কথা তাঁর পেন ড্রাইভে কী কী ফাইল-ফোল্ডার রয়েছে। তাই সন্দেহজনক কোন ফাইল-ফোল্ডার (বিশেষত হিডেন অবস্থায়) পেলে সহজেই ধরে নেওয়া যায় যে, তা ওয়ার্ম ফাইল বা ফোল্ডার।

১০. autorun.inf সহ সেসব আবছাভাবে প্রদর্শিত ফাইল-ফোল্ডারগুলো সিলেক্ট করে Shift+Delete চাপুন। তাহলে সেগুলো রিসাইকেল বিনে জমা না হয়ে সরাসরি মুছে যাবে। সিলেক্ট করার সময় লক্ষ্য রাখবেন যেন exe এক্সটেনশন যুক্ত ওয়ার্ম ফাইলে ডাবল-ক্লিক পড়ে না যায়। তাহলে কিন্তু ওয়ার্ম পিসিকে আক্রমণ করে ফেলবে।

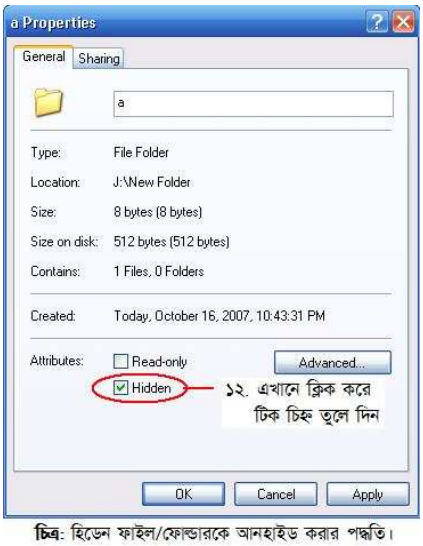
অনেক ক্ষেত্রেই দেখা যায় যে, Recycled নামে একটি হিডেন ফোল্ডার থাকে। এর ভিতর সাধারণত driveinfo.exe নামে একটি ওয়ার্ম ফাইল থাকে। সেক্ষেত্রে পুরো ফোল্ডারটিই মুছে ফেলতে হবে।

১১. এবার আরও লক্ষ্য করুন যে, এমন কোন ফাইল পাওয়া যায় কি না, যার আইকন ফোল্ডারের আইকনের মত, কিন্তু এক্সটেনশন exe । উল্লেখ্য, ফোল্ডারের কোন এক্সটেনশন থাকে না। সুতরাং, ফোল্ডারের আইকন সম্বলিত exe এক্সটেনশন যুক্ত ফাইল অবশ্যই ওয়ার্ম ফাইল। একইভাবে, টেক্সট ফাইলের আইকন সম্বলিত, অথচ txt এক্সটেনশনের পরিবর্তে exe এক্সটেনশন যুক্ত ফাইল; এবং ইমেজ ফাইলের আইকন সম্বলিত, অথচ jpeg, jpg, png, bmp বা gif ইত্যাদি এক্সটেনশনের পরিবর্তে exe এক্সটেনশন যুক্ত ফাইল নিঃসন্দেহে ওয়ার্ম ফাইল। এ সকল ফাইলও Shift+Delete চেপে মুছে ফেলুন।

চিত্র: বিভিন্ন ফাইল টাইপের আইকন সম্বলিত, অথচ exe এক্সটেনশন যুক্ত ওয়ার্ম ফাইল।

১২. একটি বিশেষ ক্ষেত্রে দেখা যায় যে, পেন ড্রাইভে যেসব ফোল্ডার রয়েছে, সেগুলো হিডেন হয়ে গেছে এবং একই নামের কতগুলো ফাইল রয়েছে যেগুলো ফোল্ডারের আইকন সম্বলিত এবং exe এক্সটেনশন যুক্ত। পাশের চিত্রটি লক্ষ্য করুন। এখানে a, b ও c ফোল্ডারগুলো হল মূল ফোল্ডার এবং a.exe, b.exe ও c.exe হল ওয়ার্ম ফাইল। এক্ষেত্রে exe ফাইলগুলো মুছে ফেলুন। মূল ফোল্ডারগুলো স্বাভাবিক অবস্থায় ফিরিয়ে আনার জন্য ফোল্ডারগুলো সিলেক্ট করে Alt+Enter চাপুন। Hidden অপশনের পাশের চেক বক্স থেকে টিক চিহ্ন তুলে দিন। OK করুন। যদি স্ক্রীনে Confirm Attribute Changes নামে কোন ডায়ালগ বক্স আসে, তাহলে সেখান থেকে নিচের অপশনটি (Apply changes to this folder, subfolders and files) সিলেক্ট করে OK করুন।

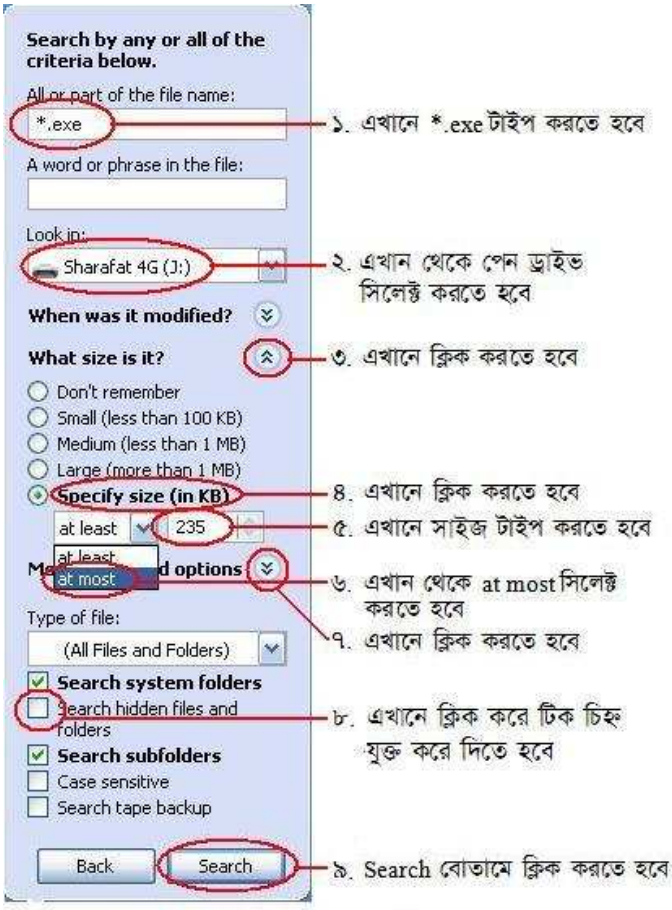
চিত্র: মূল ফোল্ডার ও ওয়ার্ম ফাইল।



চিত্র: হিডেন ফাইল/ফোল্ডারকে আনহাইড করার পদ্ধতি।

১৩. এবার সর্বশেষ আরেকটি বিষয় লক্ষ্য করুন। ধরুন, আপনার পেন ড্রাইভে a নামে কোন ফোল্ডার রয়েছে। a ফোল্ডারটিতে ডাবল-ক্লিক করুন। ভিতরে যদি a.exe নামে ফোল্ডারের আইকন সম্বলিত কোন ফাইল পান, তাহলে তা নিশ্চিতভাবে ওয়ার্ম ফাইল। অর্থাৎ, কোন ফোল্ডারের ভেতর যদি ঐ ফোল্ডারের নামে কোন exe ফাইল থাকে, যার আইকন ফোল্ডারের আইকনের মত, তাহলে ঐ exe ফাইলটি হল ওয়ার্ম ফাইল। এক্ষেত্রেও exe ফাইলটি Shift+Delete চেপে মুছে ফেলতে হবে। যদি পেন ড্রাইভের কোন একটি ফোল্ডারের ভিতর এরকম ফাইল পান, তাহলে বুঝতে হবে যে, বাকি ফোল্ডারগুলোর ভিতরেও এরকম ওয়ার্ম ফাইল রয়েছে। অতএব, প্রতিটি ফোল্ডারের ভেতর ঢুকে চেক করুন ঐ ফোল্ডারের ভিতর ঐ ফোল্ডারের নামে কোন exe ফাইল আছে কি না এবং থাকলে মুছে ফেলুন।

যদি পেন ড্রাইভে ফোল্ডারের সংখ্যা অত্যধিক হয়, তখন কী করবেন? একটি একটি করে চেক করতে তো সারা দিন লেগে যাবে। এজন্য প্রথমে যে কোন একটি ওয়ার্ম exe ফাইলের সাইজ দেখে নিন (ফাইল সাইজ দেখার জন্য ফাইলটিতে রাইট-ক্লিক করে Properties মেনুতে ক্লিক করুন)। এবার Start মেনু থেকে Search মেনুতে ক্লিক করুন। All files and folders –এ ক্লিক করুন। All or part of the file name –এ টাইপ করুন *.exe । *.exe দ্বারা বুঝানো হচ্ছে যে, কেবল exe এক্সটেনশন যুক্ত ফাইলের তালিকা আমরা চাচ্ছি। এরপর Look in –এর ড্রপ-ডাউন লিস্টে ক্লিক করে সেখান থেকে আপনার পেন ড্রাইভের ড্রাইভ আইকন সিলেক্ট করুন। নিচের দিকে What size is it? –এর ডান পাশের তীর চিহ্নতে ক্লিক করুন। নিচের Specify size (in KB) –এ ক্লিক করুন। তার ঠিক নিচের অপশন থেকে at most –এ ক্লিক করুন। ডান পাশের বক্সের 0 মুছে সেখানে টাইপ করুন ঐ ওয়ার্ম ফাইলের সাইজ + ১। অধিকাংশ ক্ষেত্রেই দেখা যায় যে, পেন ড্রাইভে SSVICHOSST.exe নামক একটি common ওয়ার্ম থাকে, যার ফাইল সাইজ হয় 234 কিলোবাইট (ফাইল সাইজ দেখার জন্য ফাইলটিতে রাইট-ক্লিক করে Properties মেনুতে ক্লিক করুন)। সুতরাং, এক্ষেত্রে সার্চের সময় বক্সটিতে টাইপ করতে হবে (234+1) বা 235 । যদি আপনি এমন কোন ওয়ার্ম exe ফাইল পান যার



চিত্র: ওয়ার্মের প্রতিলিপি সার্চ করা।

সাইজ ধরুন 428 কিলোবাইট হয়, তাহলে উক্ত বক্সটিতে টাইপ করবেন 429 । ফাইল সাইজ নির্দিষ্ট করে দেওয়ার মাধ্যমে আমরা সার্চ ফাংশনটিকে বুঝাতে চাচ্ছি যে, আমরা সর্বোচ্চ (at most) এত কিলোবাইট ফাইল চাচ্ছি। এখন More advanced options –এর ডান পাশের তীর চিহ্নতে ক্লিক করুন। নিচে Search hidden files and folders বক্সে ক্লিক করে তাতে টিক চিহ্ন যুক্ত করে দিন। এবার Search বোতামে ক্লিক করুন।

সার্চ শেষ হলে ডান দিকের প্যানেলে লক্ষ্য করুন। এখান থেকে Size কলামের হেডিংয়ের উপর একবার ক্লিক করুন। কিছুক্ষণ অপেক্ষা করুন। দেখবেন যে, সাইজের উচ্চক্রমানুসারে (১, ২, ৩, ...) পুরো তালিকাটি সাজানো হয়ে গেছে। এবার ঐ কলামের হেডিংয়ের উপরে আবারও ক্লিক করুন ও কিছুক্ষণ অপেক্ষা করুন। দেখবেন যে, সাইজের নিম্নক্রমানুসারে (২৩৫, ২৩৪, ২৩৩, ...) পুরো তালিকাটি সাজানো হয়ে গেছে। এবার Name কলামের অধীনের ফাইলগুলো লক্ষ্য করুন। যতগুলো ফাইলের আইকন ফোল্ডারের আইকনের মত পাবেন (যদি আদৌ থাকে), সবগুলো সিলেক্ট করে Shift+Delete চাপুন। ফোল্ডারের আইকন ছাড়াও কয়েকটি ফাইলের আইকন পাশের চিত্রের মত হতে পারে। আপনি যদি নিশ্চিত হন যে, ফাইলগুলো আপনার কোন প্রয়োজনীয় প্রোগ্রামের ফাইল নয় (নিশ্চিত হওয়ার জন্য In Folder কলাম থেকে ঐ ফাইলটির পাথ দেখুন এবং নিশ্চিত করুন যে, ঐ স্থান বা পাথে এরকম কোন exe ফাইল থাকার কোন সম্ভাবনা আছে কি না), তাহলে সেগুলোও Shift+Delete চেপে মুছে ফেলুন। এবার পুনরায় সার্চ দিয়ে একইভাবে তালিকাটি নিম্নক্রমানুসারে সাজান। লক্ষ্য করুন যে, Name কলামের অধীনে ফোল্ডারের আইকন যুক্ত কোন ফাইল রয়ে গেছে কি না। যখন নিশ্চিত হবেন যে, এরকম আর কোন ফাইল নেই, তখন বুঝা যাবে যে, পেন ড্রাইভ থেকে এ ওয়ার্মটি পুরোপুরি দূর হয়ে গেছে।

ব্যস, পেন ড্রাইভ এখন ওয়ার্মমুক্ত। পেন ড্রাইভটি বের করে পুনরায় লাগান। এবার আপনি নিশ্চিন্তে ড্রাইভ আইকনে ডাবল-ক্লিক করতে পারেন।

[বি. দ্র.: আপনি এ প্রবন্ধের কোন অংশ বুঝতে না পারলে বা এখানে উল্লেখিত কোন প্রক্রিয়া সম্পন্ন করতে গিয়ে কোন সমস্যায় পড়লে, অথবা ভাইরাস সম্পর্কিত আপনার যে কোন প্রশ্ন থাকলে অনুগ্রহপূর্বক আমার ই-মেইলে যোগাযোগ করুন:

শারাফাত ইবনে মোল্লা মোশাররফ
sharafat_8271@yahoo.co.uk
www.sharafat.info]