VI'S R' US

Author: Dale Neumann

05/07/2009

SOMETHING SLOWING YOUR COMPUTER AND YOU DO NOT KNOW WHAT IT IS?

TRY UNINSTALLING YOUR VIRUS PROTECTION PROGRAMS...

CHANCES ARE THEY ARE QUARANTEENING GOOD FILES AND THE VIRUS THAT COULD
BE ON YOUR COMPUTER IS NEWER OR OF RANDOM NAME THAT YOUR VIRUS PROTECTION PROGRAM
IS NOT HELPING YOU AT ALL. THE REAL-TIME SCANNER WILL SIGNIFICANTLY SLOW
PROCESSING.
AT LEAST TURN THAT OFF, BUT I WOULD UNINSTALL COMPLETELY.
OH YES, AND IF THE SOFTWARE UNINSTALLER ASKS IF YOU WISH TO DELETE
THE QUARANTEENED FILES, "JUST SAY 'NO'".

NOW THE MOST IMPORTANT THING YOU NEED TO ENABLE, NOW THAT YOU
ARE NOT USING "VIRUS PROTECTION " SOFTWARE, IS THE WINDOWS FIREWALL.
TURN THIS *ON* IMMEDIATELY. BY DEFAULT, THIS MAY BE OFF, SO
DO NOT TRUST THAT WINDOWS PUT IT ON FOR YOU AUTOMATICALLY.
THERE IS ALSO AN EXCEPTION TAB WHERE YOU CAN UNCHECK THINGS LIKE REMOTE
ASSISTANCE, ETC. WHERE SOMEONE MIGHT BE LOOKING AT YOUR COMPUTER
WHEN YOU THOUGHT ONLY YOUR EYES WERE ON IT.

ALSO, *PLEASE* TURN OFF WINDOWS UPDATES. THEN YOU WILL NOT BE RECEIVING
RANDOM CHANGES TO YOUR OPERATING SYSTEM LIKE "SECURITY" UPDATES
WHICH WILL, AGAIN, SLOW YOUR COMPUTER DOWN AND POSSIBLY BREAK SOME
FEATURE OF SOME PROGRAM THAT YOU LOVE AND DEPEND ON.

AUTOMATED REGISTRY FIXERS ARE ANOTHER NOTORIOUS DEMON.
UNINSTALL THESE AS WELL. CHANCES ARE THEY ARE GOING TO CHANGE
A GOOD REGISTRY ENTRY OR ADD UNNECESSARY ONES. WHAT YOU SHOULD
DO IS OPEN THE REGISTRY (BEST WHEN YOU JUST BUY THE COMPUTER OR AFTER
INSTALLING A NEW PROGRAM) AND DO FILE->EXPORT AND SELECT "ALL".
SAVE THE FILE IN MY DOCUMENTS OR ELSEWHERE AS ALL.REG.
NOW IF THERE IS A DESCREPANCY, YOU HAVE THE ORIGINAL REGISTRY.

OTHER PLACES TO LOOK FOR COMPUTER "DEMONS":

STARTUP FOLDER UNDER START PROGRAMS.
MOVE OUT ANY PROGRAMS THAT YOU DO NOT NEED TO HAVE START
WHEN THE COMPUTER BOOTS TO A NEW FOLDER CALLED
"STARTUP BACKUP". THAT WAY YOU ARE NOT PERMANENTLY DELETING ANY THAT
MAY HAVE TO BE THERE.

REGISTRY:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run
FIRST EXPORT THIS FOLDER AS THE "SELECTED" FOLDER TO A FILE
CALLED RUN.REG SO YOU HAVE A BACKUP. BY COPYING THIS FILE AND REMOVING
ITEMS THAT YOU DO NOT WISH TO IMPORT, YOU CAN DOUBLE-CLICK THE FILE
AND IT WILL RESTORE ANY REGISTRY ENTRY THAT YOU LATER FOUND
OUT THAT YOU REALLY NEEDED, AFTER YOU DELETED IT FROM THE REGISTRY.
NOW THAT IT IS BACKED UP, YOU CAN DELETE ANY REGISTRY KEY VALUES
OF ITEMS IN THE "RUN" FOLDER THAT LOOK SUSPICIOUSLY TAKING UP YOUR
PROCESSING POWER WITH YOU GAINING LITTLE, NO VALUE, OR NEGATIVE VALUE.
JUST BE CAREFUL NOT TO DELETE ENTRIES THAT ARE OPERATING SYSTEM RELATED
LIKE TOUCHPAD MOUSE DRIVER DLL LOADINGS AND PRINTER DRIVER DLL LOADINGS,
ETC.

MSN MESSENGER:
THIS IS ALSO NOTORIOUS FOR SLOWING STARTUP. IF YOU DO NOT *ALWAYS* WISH

TO START USING THIS PROGRAM WHEN YOU BOOT UP, YOU ARE BETTER OFF
TAKING IT OUT OF THE "RUN" IN THE REGISTRY, AND CLICKING ON IT
MANUALLY YOURSELF "ON DEMAND". YOU MIGHT WISH TO PUT A SHORTCUT TO
MSN MESSENGER CLOSE, LIKE ON YOUR DESKTOP, IF IT IS NOT ALREADY THERE,
SO, AT LEAST, YOU CAN GET TO IT EASILY.

ORGANIZING YOUR DESKTOP:
THIS WILL DRAMATICALLY IMPROVE YOUR ABILITY TO GET TO THE THINGS
YOU NEED QUICKLY AND REDUCE YOUR NUMBER OF DESKTOP ICONS WHICH ALSO
SLOW PROCESSING ON BOOT UP WHEN NUMEROUS.

PROCEDURE:

CREATE A FOLDER ON YOUR DESKTOP CALLED "Desktop".

CREATE MEANINGFUL SUBFOLDERS LIKE:

Computer - for computer related shortcuts
Document Shortcuts - obvious
Games - gaming related links
Internet - Internet browser programs and favorites
Media - Music, Pictures, and Video programs and data shortcuts
Office - Microsoft Office, Editors, Business Activities
Programming - For developers ONLY.

NOW MOVE ALL YOUR DESKTOP ICONS THAT ARE MOVEABLE (SOME LIKE INTERNET EXPLORER
ARE DESIGNED TO REMAIN ON THE DESKTOP, BUT YOU CAN DO "PASTE SHORTCUT" TO GET A COPY
IN YOUR INTERNET FOLDER/)
BE SURE YOU *ONLY* PUT *SHORTCUTS* IN THESE FOLDERS AND NOT "REAL"
FOLDERS OR ELSE YOU WILL BE DUPLICATING THE FOLDER AND DOUBLING YOUR
HARD DISK USAGE WHICH IS TOTALLY UNNECESSARY! (AND THE TWO FOLDERS WOULD
GET OUT-OF-SYNC OVER TIME WHILE YOU ADD ENTRIES TO ONE AND NOT THE OTHER.)
I.E. IF YOU WISH THE C DRIVE BE IN YOUR COMPUTER FOLDER, YOU CAN
GO TO LOCAL DRIVE C: ON YOUR WINDOWS EXPLORER AND RIGHT-CLICK "COPY"
BUT, FOR HEAVEN SAKES, WHEN YOU PASTE IT IN THE COMPUTER FOLDER, DO
NOT ACCIDENTLY CLICK "PASTE"! YOU MUST CLICK "PASTE SHORTCUT", SO
BE VVVVERYYYY CAREFUL (OR ELSE YOU WILL BE DUPLICATING THE CONTENTS
OF YOUR ENTIRE COMPUTER) !

FOR ADDING MICROSOFT OFFICE TO YOUR OFFICE FOLDER, YOU NEED TO RIGHT-CLICK
EXPLORE ON THE START MENU TO THE LOCATION OF THE MICROSOFT OFFICE FOLDER
IN THE START MENU. THEN, JUST DO RIGHT-CLICK COPY ON THE FOLDER AND
PASTE TO THE OFFICE FOLDER. IF THEY ARE ALREADY SHORTCUTS, AS THESE ARE,
FOR EXAMPLE, "PASTE" OR "PASTE SHORTCUT" WILL DO THE SAME THING,
BUT IT IS MUCH BETTER TO GET IN THE HABIT OF DOING "PASTE SHORTCUT" EXCEPT
FOR WHEN YOU *REALLY* WISH TO COPY DATA FOR BACKUP PURPOSES.

NOW THAT YOU HAVE A CLEAN DESKTOP WITH JUST A DESKTOP FOLDER AND
A FEW NON-MOVABLE LINKS OR "EMERGENCY FAVORITES",
RIGHT-CLICK ON THE DESKTOP FOLDER AND CLICK "COPY".
THEN RIGHT-CLICK EXPLORE ON THE START MENU AND "PASTE SHORTCUT"
( NOT PASTE, PLEASE ! ) INTO THE PROGRAMS FOLDER OF THE START MENU.
THIS WILL GIVE YOU A START MENU ACCESS TO YOUR DESKTOP FOLDER.
BUT DO NOT STOP THERE: BEFORE CLOSING THE WINDOWS EXPLORER, CLICK
ON THE NEW DESKTOP FOLDER SHORTCUT IN THE START MENU->PROGRAMS FOLDER OF
THAT WINDOWS EXPLORER WHILE HOLDING THE CTRL KEY. KEEP THE CTRL
KEY DOWN (WHICH IS A "COPY" ACTION INSTEAD OF A "MOVE" ACTION) AND DRAG
WHILE HOLDING THE LEFT MOUSE BUTTON AND THE CTRL BUTTON OVER TO THE
START MENU BUTTON WHICH SHOULD BE IN THE LOWER LEFT-HAND CORNER.
HOVER OVER THE START BUTTON UNTIL THE START MENU OPENS AUTOMATICALLY.
THEN DRAG THE SHOFTCUT INTO A SLOT ON THE PINUP LIST NEXT TO WHERE
THE INTERNET EXPLORER OR OUTLOOK SHORTCUT IS LOCATED IN THE PINUP LIST.
WHEN COMFORTABLE THAT YOU ARE IN THE RIGHT LOCATION, RELEASE

THE MOUSE BUTTON FIRST, THEN THE CTRL BUTTON, AND LET GO.
THIS SHOULD DROP ANOTHER SHORTCUT TO YOUR DESKTOP FOLDER ONTO
THE PINUP LIST OF THE START MENU.  NOW YOU HAVE *REAL* EASY ACCESS.
IF YOU DID IT RIGHT, NOW WHEN YOU ADD A SHORTCUT TO THE DESKTOP FOLDER ON
THE DESKTOP, IT WILL AUTOMATICALLY SHOW UP IN THE OTHER TWO LOCATIONS
OF THE START MENU->PROGRAMS AND THE START MENU->PINUP AREAS.

TYPICAL VIRUS SCENARIO:

VIRUS IS DOWNLOADED BY CLICKING ON A LINK OR OPENING AN EMAIL THAT YOU
SHOULD NOT HAVE OPENED - THIS IS WHY YOU SHOULD ALWAYS BE CAREFUL WHERE YOU GO
AND WHAT YOU CLICK ON WHEN YOU ARE ON THE WORLD WIDE WEB.
VIRUS EXECUTES INSTALLING AN .EXE SOMEWHERE,
USUALLY IN THE C:\WINDOWS\SYSTEM32 FOLDER.  THIS .EXE IS USUALLY LAUNCHED
FROM THE "RUN" REGISTRY.  THERE ARE OTHER RUN REGISTRIES IN THE OTHER
"HKEY" FOLDERS WHICH YOU SHOULD EXPORT AND CHECK AS WELL.  THIS .EXE SPAWNS
ONE OR MORE DLLs WITH A RANDOM NAME LIKE ABCDEFG123456.DLL.
IF YOU MANAGE TO DELETE THIS DLL FROM YOUR C:\WINDOWS\SYSTEM32 FOLDER,
CHANCES ARE ANOTHER WILL BE SPAWNED AS SOON AS THE VIRUS FIGURES OUT
THAT THE OLD ONE IS NOT RUNNING, AND WITH A NEW RANDOM NAME.  A NEW
"RUN" REGISTRY ENTRY WILL HAVE BEEN MADE TO LAUNCH THE NEW DLL.
THIS VIRUS MAY DO STRANGE THINGS LIKE REDIRECT YOU TO A PORN SITE OR
DISPLAY THAT YOU NEED TO DOWNLOAD VIRUS PROTECTION SOFTWARE WHICH IS
REALLY JUST ANOTHER VIRUS ONLY MORE FORMALLY DESIGNED.
MICROSOFT HAS A PROGRAM CALLED "ERD" (EMERGENCY REPAIR DISK) THAT
ALLOWS YOU TO BOOT THE OPERATING SYSTEM WITHOUT STARTING REGISTRY ENTRIES
THAT WILL "LOCK" THE VIRUS' .EXE AND .DLL FILES FROM BEING DELETED
DIRECTLY WITH NORMAL COMPUTER OPERATIONS.  IT IS DEFINITELY WORTH
GETTING FOR EMERGENCIES.  (IN THE OLD DAYS, IT WAS EASY TO ACCESS ANY
FILE ON YOUR COMPUTER, BUT NOW THINGS ARE A LITTLE MORE COMPLICATED.)
ANYWAY, OF COURSE, ONCE YOU DETECT THE VIRUS' .EXE AND .DLL FILES AND
THE REGISTRY ENTRIES, YOU CAN PROPERLY REMOVE THE VIRUS WITH TRICKS LIKE
ERD.

ANOTHER GOOD HABIT IS TO GENERATE A SYSTEM RESTORE POINT EVERY ONCE IN A WHILE,
LIKE BEFORE AND AFTER INSTALLING A NEW PROGRAM.  DO NOT ASSUME
WINDOWS WILL DO THIS AUTOMATICALLY FOR YOU.  THEN, YOU CAN REVERT TO
THE OLD WINDOWS CONFIGURATION (BACKUP ALL YOUR DATA FIRST, JUST TO BE SAFE!)
EITHER FROM WINDOWS OR FROM ERD, IF YOUR WINDOWS CANNOT BOOT.
WHEN YOU BUY A NEW COMPUTER, YOU SHOULD DEFINITELY CREATE A RESTORE
POINT RIGHT AWAY.

FIREWALLS, WINDOWS UPDATES, WINDOWS DEFENDER, AND SYSTEM RESTORE ARE ALL
FOUND IN YOUR CONTROL PANEL.  WINDOWS DEFENDER IS YET ANOTHER VIRUS PROTECTION
SYSTEM
THAT YOU CAN CHOOSE TO UNINSTALL TO SPEED UP THINGS.

SOME QUOTE "ANTI-VIRUS" SOFTWARE ALSO TURN OFF YOUR WINDOWS FIREWALL,
INVOKING THERE OWN FIREWALL.  PERSONALLY, I WOULD PREFER THE SIMPLE
WINDOWS FIREWALL TO HAVING SOME STRANGE FIREWALL THAT COULD HAVE "CRACKS"
IN IT.

SOME BUSINESS VPN ACCOUNTS SAY THEY REQUIRE THE WINDOWS FIREWALL
TO BE TURNED OFF, BUT I HAPPEN TO BELIEVE THIS IS JUST ANOTHER LIE.
I WOULD TRY IT WITH THE FIREWALL ON FIRST.  (IT WORKED OK FOR ME.)
NOW FOR SOME VERY, VERY, SPECIALIZED CONNECTIONS, THEY DO USE FIREWALLS
IN THE OFF STATE, *BUT* THERE IS USUALLY ALWAYS SOME OTHER PIECE
OF INTERNET HARDWARE IN BETWEEN TO DO THOROUGH FIREWALL PROTECTION
IN PLACE OF THE WINDOWS FIREWALL.  EVEN SO, YOU SHOULD NOT BE
AFRAID TO CHANGE THE FIREWALL SETTING BACK TO "ON" AND RE-TEST
FUNCTIONALITY TO SEE IF THINGS STILL WORK PERFECTLY.  IF NOT,
I AM QUITE CERTAIN THAT BY TURNING THE FIREWALL BACK OFF,
YOUR COMMUNICATIONS WILL RETURN TO THE WAY THE INSTALLER SET UP

YOUR HARDWARE FIREWALL.  IF THE HARDWARE FIREWALL CANNOT HANDLE
YOU FLIP-FLOPPING THE WINDOWS FIREWALL, YOU SHOULD REALLY RECONSIDER
THE SOURCE OF YOUR HELP.  AT WORST, A REBOOT OR LOG OFF/LOG ON SHOULD
GET YOU BACK UP AND RUNNING.  I CERTAINLY WOULD NOT HAVE ANY UNSAVED
WORK ON YOUR DESKTOP BEFORE ATTEMPTING THIS NO MATTER HOW SAFE THE
TEST IS.

INTERNET EXPLORER - WHICH IS THE ORIGINAL BROWSER DESIGNED
BY MICROSOFT *FOR* WINDOWS, THE EARLIER A VERSION,
THE SIMPLER - CAN SOMETIMES BE CONFIGURED BY A VIRUS TO
NOT DISPLAY A LINK OR WEB PAGE THAT YOU THOUGHT WAS UP AND RUNNING.
IE, SHORT FOR INTERNET EXPLORER, ENHANCEMENTS LIKE GOOGLE TOOLBAR, ETC.
TEND TO CLUTTER UP YOUR BROWSER, SLOW IT DOWN, AND SELECTIVELY CHANGE
YOUR ACCESS RIGHTS TO SOME WEB PAGES AND LINKS.  NOW SOME ADD-ONS
LIKE "JAVA", ETC. ARE NECESSARY TO VIEW CERTAIN THINGS THAT ARE
IMPORTANT, BUT FOR THE MOST PART, THE FRIVOLOUS BELLS AND WHISTLES
YOU ADD TO YOUR BROWSER WILL ONLY HARM YOU IN THE LONG RUN.
SO, WHEN YOU FIND OUT THAT YOU CANNOT ACCESS A PAGE OR LINK
THAT YOU *KNOW* IS AVAILABLE, THE BEST AND EASIEST THING TO DO
IS TO GO TO INTERNET OPTIONS (AVAILABLE FROM IE->TOOLS
OR FROM CONTROL PANEL) AND CLICK THE BUTTON TO "RESET WEB SETTINGS".
YOU WILL HAVE A CHOICE TO ADDITIONALLY RESET YOUR HOME PAGE,
BUT YOU DO NOT NEED TO CHECK THAT BOX.  I RECOMMEND ALWAYS STARTING
YOUR BROWSER WITH THE "BLANK" HOME PAGE, AND THEN GOING TO YOUR
MOST FAVORITE SITE BY CLICKING A FAVORITES LINK.  THIS WAY
YOU MIGHT SAVE SOME INTERNET ENERGY WHEN YOU WERE OPENING UP
YOUR BROWSER TO GO SOME PLACE OTHER THAN THAT MOST FAVORITE
WEB PAGE, AND YOU DO NOT EXPOSE YOURSELF TO THE INTERNET WORLD
UNTIL *YOU* SELECT A DESTINATION.  BUT, BACK TO RESETTING
YOUR WEB SETTINGS: DEPENDING ON YOUR VERSION OF IE, THE BUTTON
WILL EITHER BE FOUND ON THE "PROGRAMS" TAB OR THE "ADVANCED" TAB.
AND ON ANOTHER NOTE, IF THE VERSION OF IE YOU CURRENTLY HAVE INSTALLED
IS WORKING EXCELLENT FOR YOU, PLEASE DO ME A FAVOR AND DO *NOT*
UPGRADE.  YOU ONLY RISK GETTING MORE UNPREDICTABLE BEHAVIOR
FROM YOUR BROWSER.  AS BROWSERS GET MORE COMPLEX, MORE SECURITY
FEATURES, ETC. ARE ADDED WHICH USUALLY MAKE FOR A SLOWER BROWSER
AND ONE THAT IS MORE RESTRICTIVE.  IF YOU CANNOT ACCESS A WEB PAGE,
MORE THAN LIKELY, RESETTING YOUR WEB SETTINGS TO CREATE A
CLEAN AND *SIMPLER* BROWSER WILL WIN THE GAME FOR YOU, RATHER THAN
UPGRADE TO THE NEXT RISKY VERSION AND GET INTO HOT WATER DEEPER.
OH, AND DELETING YOUR TEMPORARY INTERNET FILES, COOKIES, ETC.
FROM INTERNET OPTIONS->GENERAL TAB->SETTINGS->VIEW FILES->
[CTRL-A] (TO SELECT ALL)->[DELETE KEY] (TO DELETE THEM ALL) -
I RECOMMEND DOING IT THIS WAY AS OPPOSED TO "DELETE COOKIES"
AND "DELETE FILES" - CAN ALSO MAKE PAGES MAGICALLY START TO WORK AGAIN.
IF NONE OF THESE TRICKS WORK, AS A LAST RESORT, YOU CAN DO THE UPGRADE,
BUT GENERALLY SPEAKING, THE VERSION THAT CAME WITH YOUR COMPUTER
SHOULD BE SUFFICIENT FOR ANY INTERNET ACTIVITY (UNLESS YOU HAVE A REALLY,
REALLY OLD COMPUTER AND NEVER UPGRADED IE).  CERTAINLY, DO NOT UPGRADE
AS THE FIRST IDEA IN A STREAK OF PANIC.  AND, DO NOT LISTEN TO ALL THE
ADVERTISING HYPE ON THE NET ABOUT UPGRADING NOW, SWITCHING
TO A DIFFERENT BROWSER, OR ADDING ANY UNNECESSARY FEATURES AND
ENHANCEMENTS.