Using SANDBOXIE to Safely Browse the Internet ©

(verified with ver 5.20) Jim McKnight www.jimopi.net Sandboxie.lwp revised 6-25-2017

- **GENERAL NOTES:**
  - ✓ These tips are based on my personal experience using Sandboxie. I feel Sandboxie is the best available "Safety Net" for protection against infections while Web Browsing. This sheet will continue to be updated as I learn more about using Sandboxie. Feedback is welcome.*You can find my email address at: www.jimopi.net*
  - ✓ Once Sandboxie is set up, all you have to do is double-click the Sandboxie Icon on the desktop and your regular (Default) Internet Browser opens safely in a sandbox.
  - ✓ Sandboxie uses your regular Internet Browser to go on the Internet without the fear that you will be tricked into infecting your PC by malicious websites, or by infected downloads.
  - ✓ Although Sandboxie does some amazing things with many kinds of programs, this article focuses on making your Internet browsing safe from malware infections.
  - ✓ This article addresses features in the FREE version of Sandboxie. The paid version offers many bells and whistles, but for safe Internet browsing, the FREE version is adequate.
  - ✓ DEFAULT SANDBOX: The free version of Sandboxie only offers one sandbox: the Default Box. Although the paid version offers the ability to use multiple sandboxes running at once, I just use the "Default Box" for everything. Even if you use the paid version, I do not recommend using multiple sandboxes.
  - ✓ CONFLICTS: Be aware that some programs do not play well with Sandboxie. If you are still using XP, I recommend using Avira for your anti-virus, since Avast! does not play will with Sandboxie. I have also had issues with Kaspersky causing SBIE errors when the browser is opened. For more conflict info, see: http://www.sandboxie.com/index.php?KnownConflicts
  - ✓ Nag Screen: The only downside to the FREE version of Sandboxie is that 30 days after installation, a Nag screen pops up most every time you use it with a 5 second delay telling you that the Nag delay will go away permanently if you buy a registered license for Sandboxie. *Cost is currently about $20.00 per year (15 Euros) for a single PC license. Well worth the money in my opinion. It protects you much better than any antivirus program.*
  - ✓ I highly recommend sandboxing your email client. *See the last page of this write-up.*
- **HELP AND TUTORIALS:**
  - ✓ For an overview of what a "sandbox" is, go to the http://www.sandboxie.com home page.
  - ✓ Also see the Sandboxie Help pages at: http://www.sandboxie.com/index.php?HelpTopics
  - ✓ See this Video Tutorial (3 parts; About 20 minutes total). It is very good: http://www.securitytube.net/video/578
  - ✓ You can get to the 6-part "Getting Started" tutorial for the Sandboxie program at any time as follows: *(Double-click the Sandboxie Control Icon on the Task bar > Help > Getting Started Tutorial)*
- **DOWNLOADING AND INSTALLING SANDBOXIE**
  - ✓ You can download the SANDBOXIE program from: http://www.sandboxie.com
  - ✓ During the installation, you may be notified of software compatibility conflicts between Sandboxie and some other program/s. You will be asked to give permission to automatically change some configuration settings to fix it. Just click OK. *Note: You can get to this screen anytime: (click Sandbox > Configure > Software Compatibility).*

- **CONFIGURATION SETUPS AFTER INSTALL**
  1) YELLOW BORDER: Set it up to ALWAYS Display: I like to have the YELLOW border always visible whenever a program is running sandboxed. To set this up, double-click the Sandboxie Control Icon in the System Notification area, then: *(click Sandbox > Default Box > Sandbox Settings > Appearance).* Un-check the box for "☐ Display the border only when the mouse cursor is in the Window Title", click Apply.

  2) "AUTO-DELETE" FILES:
     a) By default, Sandboxie does NOT Auto-delete anything. Everything is saved in the sandbox until you manually delete it.

     b) I highly recommend setting up Sandboxie to "Automatically delete contents of sandbox" when the sandboxed browser is closed. This will delete all browser changes, add-ons, downloads, and program installs *(including malware)* each time you close Sandboxie. To set up Sandboxie to always Auto-Delete:
        1. Double-click the Sandboxie Control Icon in the System Notification area.
        2. In the Sandboxie window; *(click Sandbox > Default Box > Sandbox Settings > Delete > Delete Invocation)*.
        3. Click to check the box for ☑ Automatically delete contents of sandbox, and click OK.

     c) NOTE: *"Auto-delete" usually does not include manually downloaded files. They are kept in the sandbox until you manually either "Recover" them or "Delete" them.*

  3) AUTO-UPDATING: Set up Sandboxie for Automatic update checking: *(Click Help > Check for Updates). In the "Check for Updates" box, check the box "☑ In the future check for updates without asking", then click the Now button, then OK.*

  4) PRINTING PERMISSIONS: Open Sandboxie Control *(Configure > Edit Configuration)*.
     1. Scroll down to "DefaultBox" settings
     2. At the end of the DefaultBox settings, add the line: AllowSpoolerPrintToFile=y
     3. Click Save, then exit Sandboxie Control

- **UNDERSTANDING THE SANDBOXIE CONTROL CENTER ICON:**
  - ✓ The Sandboxie Control Icon looks like a Yellow Kite and is in the System Notificaton Area.
  - ✓ If the Kite is solid Yellow, then the Sandbox is empty.
  - ✓ If the Kite is Yellow with Red dots, then the Sandbox has files or programs in it.
  - ✓ When you close the last running Sandboxed program, Sandboxie may take a few seconds to empty the sandbox during which time you may see a Red X flash in the area, then it goes solid Yellow. *This is with Auto-delete turned on (as shown above).*

- **HOW TO MANUALLY DELETE EVERYTHING IN THE SANDBOX**:
  - ✓ If the yellow "Sandboxie Control" system tray Icon has little red dots in it, that means there is still something in the sandbox that should be deleted. It could be programs or files.
  - ✓ Double-click the "Sandboxie Control" system tray Icon, then; *(click Sandbox > Default Box > Delete Contents)*. Close the Sandboxie Control window.

- **HOW TO SAVE *(RECOVER)* DOWNLOADED FILES:**
  - ✓ Sandboxie offers you the opportunity to save "for real" any downloaded files both after you download the file and when you close the browser. If you do not save them, they disappear when you close Sandboxie (but by default stay in the sandbox for you to recover or delete later). Saving for real is called Quick Recovery.
  - ✓ Each time you download files to the Downloads Folder or the Desktop, you are usually (but not always) prompted to "Quick Recover" that file *(save for real).*
  - ✓ If you download files to places other than the Downloads Folder or the Desktop, you may NOT be prompted for "Quick Recovery". If you do not get the prompt to recover the file, then go to the

Quick Recovery *(save for real)* screen by double-clicking the Sandboxie Control Icon in the notification area, then select *(Sandbox > Default Box > Quick Recovery)*. Click on the desired Item/s (to highlight them), then click either "Recover to Same Folder" or "Recover to Any Folder".

- ✓ Last resort: If you are still having trouble saving a file "for real", AND if you trust the download website, AND if you trust the file: First copy the website URL, close Sandboxie, browse to that site without Sandboxie, and download your file. Be sure to manually scan it for malware before using.

- **EXPLORING DOWNLOADED FILES**
  - ✓ It is best to explore downloaded files that are in the sandbox by using the "Sandboxed" version of Windows Explorer:
    1) Open the Sandboxie Control program by double-clicking its Icon in the System Tray.
    2) Click *(Sandbox > Default Box > Run Sandboxed > Run Windows Explorer)*.
    3) Locate the downloaded file (Usually in the Downloads folder)
    4) Right-click on the file and click on Scan with Windows Defender (or your default AV program).
  - ✓ Now as you explore the system using the sandboxed Windows Explorer, you will see your downloaded (and sandboxed) files right along side regular files in the same folder where you downloaded them. *Note: If you navigate to that folder with the regular (Non-Sandboxed) Windows Explorer, you will NOT see the downloaded files. This can be confusing so hang in there.*

- **HOW TO CHECK DOWNLOADED FILES FOR MALWARE**
  - ✓ There are two ways to scan downloaded files for malware:
    1) You can get to the file using the sandboxed Windows Explorer shown above, then right-click the file and run your normal Anti-malware program scan on it to make sure it is safe before "Saving it for real".
    2) Everything that is sandboxed is actually hidden in a folder called C:\Sandbox. Your antivirus scanner can be run against that folder and will inspect all the files in it for malware. It should then be safe to save those downloaded files "for real".

- **HOW TO KNOW IF YOU ARE RUNNING IN THE SANDBOX -** Two ways:
  - ✓ Look for # (pound signs) before and after the Browser's name in the Title Bar. Note: Internet Explorer no longer has a name/title so there are no pound signs visible with a sandboxed IE.
  - ✓ YELLOW Border:
    1. By default, you can hover the mouse pointer near the top of the active browser window. If you are running in the sandbox, the window frame will be outlined in a YELLOW border.
    2. Optionally, you can have the YELLOW border always display when a program is sandboxed: *(Click Sandbox > Default Box > Sandbox Settings > Appearance)* Uncheck the box for "☐ Display the border only when the mouse cursor is in the Window Title". *(I prefer this)*.

- **HOW TO ENSURE THAT E-MAIL HOT-LINKS OPEN IN A SANDBOXED BROWSER**:
  - ✓ This section assumes your e-mail is NOT set up to run sandboxed. If your e-mail is set up to run sandboxed then all attachments will open the necessary program/browser in the Sandbox. To run your e-mail sandboxed, see the SUPPLEMENT PAGE at the end of this document.
  - ✓ My preferred way is to first open your default browser in the sandbox. Then if you click any links in your e-mail, they will open a new tab in the already open and sandboxed browser.
  - ✓ *Warning: If the default browser is not already open in the sandbox when you click an e-mail link, then the link will open the default browser WITHOUT being sandboxed*.

- **HOW TO RUN A DIFFERENT BROWSER USING SANDBOXIE**
  - ✓ The Sandboxie Icon (Free version) always uses the system's "Default" browser. You cannot specify different browsers for the Sandboxie "Sandboxed Web Browser" Icon.
  - ✓ If you want to use a different browser with Sandboxie, you have 3 choices:
    1) Right-click the desired browser Icon *(Context Menu)*, then select "Run Sandboxed". *Note: Depending on your Operating System, the context menu option for Sandboxie may not show up. (IE: Quicklaunch Icons or the Start Menu Favorites Icons). It does always work with the Desktop Icons.*
    2) Change the Default browser:
       a. Close the sandboxed browser.
       b. Change the default browsing program to the Browser you desire. *The method varies depending on your operating system.*
       c. Double-click the Sandboxie "Sandboxed Web Browser" Icon. The new default browser should now open.
    3) Create a new Desktop Icon that will use Sandboxie to open a specific Browser program other than your default browser:
       a. Open the Sandboxie Control program by double-clicking its Icon in the System Tray. Click *(Configure > Windows Shell Integration > click the "Add Shortcut Icons" button.).*
       b. Click OK a couple times until you get to the window titled "Sandboxie Start Menu Default box" and select "Programs".
       c. Click to highlight the Browser Program Icon you want to open. The new Icon will immediately appear on the Desktop.
       d. I suggest renaming the Icon after you create it.
- **MAKING PERMANENT CHANGES TO THE BROWSER:** *(This includes adding/removing/updating "add-ons", browsing history, adding bookmarks (Favorites), etc.)*
  - ✓ With Auto-Delete turned ON: *(RECOMMENDED)*
    - BROWSER CHANGES: Sandboxie will NOT save your Browsing History or any added Bookmarks, or any other changes to the Browser when Sandboxie closes.
    - "ADD-ON" UPDATES: When you open a browser in Sandboxie and you see that one of your add-ons has auto-updated, note that it will update over and over each time you open the browser via Sandboxie. You need to open the browser without Sandboxie so the update can permanently install itself.
  - ✓ With Auto-Delete turned OFF: *(NOT RECOMMENDED)*
    1. BROWSER CHANGES: Your Browser changes will be remembered, but only within the Sandboxie browsing sessions. If you open the Browser without Sandboxie, the changes will not be visible.
    2. "ADD-ON" UPDATES: When you open a browser in Sandboxie and you see that one of your add-ons has auto-updated, note that it is NOT permanently installed. It will only show up inside the Sandboxed browser. You need to open the browser without Sandboxie so the update can permanently install itself.
  - ✓ TO MAKE PERMANENT BROWSER CHANGES: Any Browser updates or customizations *(Add-ons, Favorites, Bookmarks, Toolbars, etc.)* that you want to be <u>permanently</u> changed in your Browser, must be installed by opening the Browser WITHOUT using Sandboxie, and then making the changes. *Otherwise, any changes you make will be sandboxed and will disappear.*

- **PRINTING:**
  - ✓ Yes, you can print stuff as usual from your Browser.
    a. NOTE: On version 4.20 or higher, you may get error SBIE1320 when trying to print. The message asks you to double click the message to permit printing to continue. To make this message go away permanently, follow this procedure.
    - Close all Sandboxed programs.
    - Double-click the Sandboxie Control tray icon.
    - Click Configure > Edit Configuration
    - Scroll down to the sandbox that you want to add that setting, usually [DefaultBox]
    - Add the setting: "AllowSpoolerPrintToFile=y" , like this:

```
[DefaultBox]

ConfigLevel=7
AutoRecover=y
Template=Thunderbird
Template=WindowsFontCache
Template=BlockPorts
Template=LingerPrograms
Template=Chrome_Phishing_DirectAccess
Template=Firefox_Phishing_DirectAccess
Template=AutoRecoverIgnore
RecoverFolder=D:\A_DigiPHOTOS
RecoverFolder=%{374DE290-123F-4565-9164-39C4925E467B}%
RecoverFolder=%Personal%
RecoverFolder=%Favorites%
RecoverFolder=%Desktop%
BorderColor=#00FFFF
Enabled=y
BoxNameTitle=n
AutoDelete=y
NeverDelete=n
AllowSpoolerPrintToFile=y
```

    - ***Make sure there's one blank line after that entry, then click: File > Save > OK***

  - ✓ PDF's: If you have trouble printing with Adobe Reader (where it may be very slow to respond), I suggest you turn off the Adobe Reader's "Protected Mode" *(Adobe Reader > Edit > Preferences > General > Uncheck "☐ Enable Protected Mode at Startup").* Obviously this removes the malware protection built into Adobe Reader X. *Note: Adobe Reader 9 works fine and has no Protected Mode.*

- **BROWSER PROGRAM IS SLOW TO CLOSE**: This is normal from time to time. Make sure there are no open windows hidden behind the main browser window awaiting user action.
- **DESKTOP "INTERNET LINKS" SHORTCUT ICONS. CREATE SANDBOXED ICONS THAT WILL START YOUR BROWSER IN A SANDBOX:** Be aware that your regular Desktop "Internet" shortcut Icons do NOT use Sandboxie when they open your Browser. To create new Desktop Internet Shortcut Icons that WILL use Sandboxie to open your Browser program, try this:
  - ✓ Open the Sandboxie Control program by double-clicking its Icon in the System Tray. Click *(Configure > Windows Shell Integration > click the "Add Shortcut Icons" button.).*
  - ✓ Click OK a couple times until you get to the window titled "Sandboxie Start Menu Default box" and select "Desktop".
  - ✓ Click to highlight the desktop Icon you want to duplicate. The new Icon will immediately appear on the Desktop.
  - ✓ Be sure to rename each Icon after you create it. *This is so Sandboxie will not overwrite it when you create another Icon***.**
- **E-MAIL LINKS**:
  - ✓ If you click a link in your e-mail client to go to a webpage, your default browser will NOT open in Sandboxie. Your Browser will open but not in Sandboxie, therefore you are at risk.
  - ✓ If your browser is already open in Sandboxie, then the link will open a new tab in the already open sandboxed browser. This is what you want, so before you click any links in your e-mail client, make sure your sandboxed browser is already open.

- **WEBSITES ACT WEIRD OR DO NOT "AUTOMATICALLY LOG YOU ON" PROPERLY**:
  - ✓ If you experience any weird behavior with websites, close down Sandboxie. Make sure the Sandbox is totally empty, then restart the Sandboxed Web Browser. *If you are also running your e-mail client or any other program sandboxed, you will have to close all sandboxed programs.*
  - ✓ I have experienced strange behavior with Internet Explorer sometimes not remembering my log-in to a site. If I open the IE without Sandboxie, the login is remembered. I am not sure which sites or circumstances this occurs because I never use Internet Explorer. I use Firefox and it works perfectly with Sandboxie.

==========

E-MAIL SUPPLEMENT

SET UP YOUR E-MAIL CLIENT TO RUN IN A SANDBOX

- **WEBMAIL:** If you use Webmail for your E-Mail, this section does not apply. just use Sandboxie to start your Browser to access your mail.
- **GENERAL NOTES AND TIPS:**
  - ✓ **Clicking "Browser Hot-Links" in your emails:** With your email client sandboxed, clicking a link to a website will open a new incidence of your Browser in the sandbox and then safely open the link**.**
  - ✓ **Opening E-Mail Attachments:** Any attachments such as a .PDF, .DOC, .PPS, .ZIP, etc. will open in a sandboxed version of the proper program, thus protecting your system from malware.
  - ✓ **Saving E-Mail Attachments:** This is the same as in the section: SAVE *(RECOVER)* DOWNLOADED FILES above. *Do not allow Sandboxie to "Recover" an attachment unless you are 100% certain the attachment is clean and safe*.
  - ✓ **E-Mail Client Program Updates**: Remember that Email Client program updates cannot be installed while in the Sandbox. You have to open the E-mail client without Sandboxie and as an Administrator, then download and install the updates.
  - ✓ **MORE TIPS:** http://www.sandboxie.com/index.php?EmailProtection
- **FIRST, PREPARE SANDBOXIE TO WORK WITH YOUR E-MAIL CLIENT:**
  - ✓ **CONFIGURE YOUR E-MAIL READER:**
    1. Open the Sandboxie Control program by double-clicking its Icon in the System Tray.
    2. Click: *(Sandbox > Default Box > Sandbox Settings > Applications > E-mail Reader)* .
    3. Click on your preferred E-mail Client, then click "Add", then "Apply" or "OK".
  - ✓ **TEST your Sandboxie/E-mail Configuration to make sure it is working properly before going live:** http://www.sandboxie.com/index.php?TestEmailConfiguration
  - ✓ **Tutorial**: http://www.sandboxie.com/index.php?ApplicationsSettings#email
- **SECOND, CREATE A DESKTOP ICON TO OPEN YOUR E-MAIL IN THE SANDBOX**:
  - ✓ **Create and name the new Icon:**
    1. Open the Sandboxie Control program by double-clicking its Icon in the System Tray. Click *(Configure > Windows Shell Integration > click the "Add Shortcut Icons" button.).*
    2. Click OK a couple times until you get to the window titled "Sandboxie Start Menu Default box" and select "Desktop" or "Program".
    3. Click to highlight the E-mail Program Icon you want to create for Sandboxie. The new Icon will immediately appear on the Desktop.
    4. Be sure to rename the Icon after you create it, to something like "Sandboxed E-Mail". *This is so Sandboxie will not overwrite it if or when you create another Desktop Icon.*
  - ✓ I suggest moving your original e-mail Icon off the Desktop to avoid accidently opening your email without the sandbox.