

# PC SECURITY FOR BANKING

A [Ciphers By Ritter](#) Page

Terry Ritter

A = ritter B = ciphersby  
A@BA.com

2010 January 24

---

## SUMMARY

Almost everyone has poor on-line security, but free approaches do exist to fix the problem:

1. *Avoid malware by using Linux for on-line browsing.*
2. *Avoid infections by booting Puppy Linux from DVD.*
3. *Avoid browser weakness by using Firefox and security add-ons.*
4. *Avoid account hacking by using long random passwords and LastPass.*
5. *Avoid snooping by using SSL ([HTTPS://](#)).*

## INTRODUCTION

The major banking security problem is malware.

**Microsoft has put their users in a bind.**

1. First, malware is real, does frequently infect Windows systems, and can be a serious danger for banking security.
2. Next, Microsoft provides no tool to certify that a Windows installation remains clean. While anti-virus and anti-malware scanners may detect malware, they cannot detect *all* malware.
3. Last, once Windows is infected, it commonly remains infected, session after session, until the infection is somehow detected and Windows is re-installed from CD. Unfortunately, Microsoft has made Windows installation an ordeal ordinary users should avoid.

So malware is a serious danger, we cannot tell if we have it, and making sure the system is clean requires a re-install ordeal. Way to go Microsoft!

**How can PC's be secured for on-line banking?**

1. **First, do not use Windows online**, and especially do not use Windows for banking. Using Linux defeats almost all malware, because malware is designed to attack Windows, not Linux.
2. **Next, boot Puppy Linux from DVD.** Booting from DVD avoids existing Windows infections because the boot does not use the Windows hard drive. Other Linux distributions offer a "Live CD" or "Live DVD" but those are often slow and hard to update. Puppy Linux is the only known Linux which allows the frequent browser security updates to be burned to new sessions on the existing boot DVD.

**But Microsoft Windows is professional!**

Puppy Linux from DVD may not be best at everything, but right now it is best for secure browsing. A Windows hard drive is easily infected, and then it *stays* infected, whereas a Puppy DVD is hard to infect and easy to clean. Booting Puppy Linux from DVD loads a clean system and avoids existing Windows infections.

**Linux can have malware too!**

Linux does not make malware impossible, but it does mean getting out of the malware line of fire. Criminals have little reason to strike at Linux when they can make vastly larger profits targeting Windows. It is a fact that Mac and Linux users have for years enjoyed the advantage of few malware attacks.

Someday, Linux malware may become an issue, but right now Windows is vastly riskier than Linux. Someday, BIOS infections may become an issue too, just not now.

**For secure browsing, use Firefox with security add-ons.**

No other browser has anywhere near the security features produced by these add-ons:

- "LastPass" is a secure cross-platform password manager which allows the user to make and easily use a different long random password for every device and every site and every account.
- "Safe" puts a colored border around each page where SSL has been established, thus clearly announcing snooping protection.
- "NoScript" converts the usual and dangerous "run any scripts from any page" to "only run scripts from specific trusted pages."
- "Perspectives" provides a way to check web page authentication and expose SSL man-in-the-middle attacks.
- The add-ons "WOT" and "PhishTankSiteChecker" help expose phishing sites.
- and there are many more.

Until another browser has these features, the choice for secure browsing must be Firefox.

## QUESTIONS

**What can be done about malware?**

Most attacks can be avoided simply by using some OS other than Microsoft Windows when on the Web. An attack designed to exploit the faults or use the services of a *particular* OS is unlikely to succeed on a *different* OS.

### Why avoid Microsoft Windows?

Criminals design attacks which encounter users at random. Since most users have Windows, most attacks target Windows. We can avoid most attacks by using something else.

### Why not protect Microsoft Windows?

Finding ways to harden Windows was the original goal of this research, but no solution was found. Malware can and does infect Windows, but users will not know, so users will expose their account numbers and passwords. Microsoft does not provide a tool that will certify a Windows installation as uninfected. Because of the risk of having been infected in some past session and remaining infected, Windows simply cannot be trusted with account information.

### Why not do something simple?

Using Puppy Linux is about as simple as an effective solution can get (especially if somebody sets it up for you, or tells you how). Puppy Linux is a very small operating system taking up only a small part of one DVD. Much of the apparent setup complexity is just configuring the OS and Firefox. The supposed alternative of trying to harden Windows enough for banking simply cannot work.

### What are the alternatives?

For secure banking, it is crucial to not use a system infected by malware. Since we cannot really know whether our Microsoft Windows system is infected, we are forced to find a way to load a clean system. Booting Puppy Linux from DVD is that way.

If you have a Mac, use that, but you still have an easily infected hard drive.

It is possible to subscribe to a personal VPN encryption service (like WiTopia), but that will not protect us from malware. Encryption cannot hide information when malware is in charge. Any Linux distribution should resist malware, but booting Puppy Linux from DVD also resists infection.

### Will Puppy Linux affect my existing system?

No. Since we boot Puppy Linux from a DVD, we do not have to change anything on the Windows hard drive. Unless we work at it, the only thing we can screw up is the DVD. And, with a DVD+RW, we can re-use the same disc and try again.

### Why choose Puppy Linux?

In theory, any Linux distribution can support good security simply by having a "Live" boot DVD which supports the Firefox browser. Booting from DVD avoids hard drive installation and any effect on the existing system. Booting from DVD also avoids any existing malware infections on the hard drive.

In practice, live DVD design and implementation issues make a big difference in different distributions. Some distributions may load code from CD or DVD as needed, so the DVD must remain in place, and operation is very slow. Puppy Linux loads completely into RAM and runs from RAM, which is *faster* than a hard drive. The Puppy boot DVD can be removed in operation. The computer does not even need to *have* a hard drive, even to produce an updated Puppy. When there is no hard drive, there is no hard drive information to be exposed, and there is no hard drive to infect.

In practice, supporting Firefox means supporting browser and add-on updates which quickly become a way of life. Some distributions force the user to make a new CD or DVD for each new update, which means once or twice a week. Only Puppy Linux actually burns new or changed files to new sessions (directories) on the original boot DVD. When Puppy boots, new file versions load instead of old ones, but the old versions are still there and can be read from the DVD under either Windows or Linux.

Currently, alone among all known Linux distributions, only Puppy Linux makes updates practical for a "Live" boot DVD.

### What are Puppy advantages?

- Puppy Linux is easy to use from DVD without hard drive installation.
- Puppy Linux on DVD avoids any malware already hiding on the PC hard drive.
- Puppy Linux supports the Firefox browser which has many security add-ons.
- Puppy Linux can save program updates back to a (writable) boot DVD.
- Puppy Linux gives everyone their own private PC for the cost of a DVD.

### How do we use it?

When we want to access on-line accounts, we put our Puppy DVD in the optical drive and restart the system. Puppy comes up, we start Firefox, and are back in familiar territory. We do our banking, remove the Puppy DVD, and restart the system back to Windows. Even if our main OS is infected, booting the Puppy OS from DVD avoids the infection.

### What are the Puppy Linux security features?

- Linux prevents almost all current malware from running and *exposing* anything.
- Linux prevents almost all current malware from running and *infecting* anything.
- A DVD boot avoids any malware already on the hard drive.
- A DVD boot disk generally defeats attempts to infect the OS files on the DVD.
- A DVD boot disk is easily replaced without a tedious OS re-install.
- Puppy Linux supports security updates by writing them to the boot DVD.

### Why use Firefox?

- Firefox generally is patched much faster than other browsers when security flaws are found.
- Firefox provides incredibly easy updates for itself and add-ons.
- Firefox used with security add-ons has many important security features not available in other browsers.

### What features do the Firefox add-ons provide?

- **NoScript** stops JavaScript, Java, Flash, SilverLight, etc., unless allowed for that web page.

- **NoScript** protects against XSS, IFrame and Clickjacking attacks.
- **NoScript** can prevent snooping by forcing SSL on particular web pages.
- **Safe** shows when a page does (or does not) have SSL active.
- **Perspectives** uses notaries to expose a false certificate or SSL man-in-the-middle.
- **SSL Blacklist** exposes Debian flaw bad certificates and MD5 poor authentication.
- **SSLPasswdWarning** announces when password entry is not SSL protected.
- **Facebooksecurelogin** forces SSL for Facebook login (only).
- **LastPass** Password Manager handles long, random passwords for web site login.
- **LastPass** encrypts the password database locally before saving it anywhere.
- **LastPass** allows password database access via SSL from any computer.
- **URL Tooltip** displays link URL for inspection before clicking.
- **Long URL Please** expands short URLs for inspection before clicking.
- **PhishTank SiteChecker** warns when page is a known phishing site.
- **WOT** warns when page has a bad reputation from other users.
- **BetterPrivacy** deletes Flash-cookies (Local Shared Objects, LSO).
- **BetterPrivacy** disallows Document Object Model (DOM) browser storage.
- **ShowIP** displays the page IP address and supports whois and other lookups.

#### What about passwords?

- Even the most basic security requires us to use long random values for passwords.
- We need to make and use a different long random password for every device and every site and every account.
- We need a password manager, and it needs to run both in Windows and Puppy Linux.
- The easiest way to do that is with LastPass.com and the Firefox add-on.
- Do not email passwords to anyone, including yourself.
- Delete all on-line emails containing passwords.
- Install passwords in your LastPass.com account (or save as Secure Notes).
- Avoid entering a password on a web page until after SSL has been established.
- If forced to enter a password without SSL, consider the account public.

#### What about email?

- We should use on-line email (try Google Gmail), since they can scan better than we can.
- Always connect to on-line email via SSL encrypted connection. (Set the Gmail option.)
- Do not click on a link in unexpected email. If necessary, copy the address, paste it to the browser, and inspect it before going.
- Do not download unexpected attachments, since a malware email can pretend to be from one of your friends.
- In Gmail, view .PDF files online without downloading.
- Never supply or confirm User ID, Password, or any private data via email. *Never email passwords!*
- Emails which do not address you by name are probably not really from accounts that do have your name.

#### What about browsing?

- Do not download browser toolbars.
- Any alert that claims your system has malware probably is itself malware.
- Any page which wants you to download and install something may be distributing malware.
- If you need an update or a player, go to the manufacturer's page and download it from there.
- Even respected companies can have their pages invaded and used to distribute malware.
- NoScript is our friend even in Linux since JavaScript code will run on any browser.

#### What about snooping?

- Currently, most information on the web is sent unencrypted, in the open.
- For wireless, anybody nearby can read what you send unless WPA2 security has been established.
- But WPA2 security only extends through the air to your router, with the data unprotected on wired broadband.
- With wired CAT5 connections, anybody on the same sub-network (e.g., any room in a motel) might read what you send.
- Avoid wired and broadband snooping by establishing an SSL (<https://>) encrypted connection.
- SSL uses a cryptographic certificate to link a web site to an issuer whose certificate is included in your browser.
- *Never approve a certificate*, especially in a "Free Wi-Fi" coffee shop or other open Wi-Fi hotspots.
- Secrecy requires establishing an SSL connection before entering a password.
- Instead of establishing SSL with each account, one might subscribe to a personal VPN service (like WiTopia).

## PUPPY LINUX

Puppy Linux is a free alternate operating system that most ordinary Windows users can use quickly. Puppy Linux supports the Firefox browser and most Firefox add-ons, thus delivering a browsing experience similar to Windows. There are various advantages:

- **Puppy Linux is not Windows.** Malware that infests Windows generally assumes the presence of Windows services, data structures and program code. When Windows is not present, the malware generally cannot operate successfully.
- **Puppy Linux can boot from DVD.** If an infection is acquired during operation, even in Linux, a simple DVD re-boot solves the problem.
- **Puppy Linux updates the boot DVD.** A modern browser is updated frequently to patch security flaws. With a DVD OS, updates would normally mean burning a new DVD and doing a new configuration. In contrast, Puppy Linux allows writing file changes from browser and add-on updates as another session on a multisession boot DVD. The next time we boot we have the updated browser just like we would with a hard drive OS. If a work session seemed strange, we do not have to save it. If Puppy starts acting funny, we can void the previous session and restart to a session before the problem.
- **Puppy Linux does not need a hard drive.** When there is no hard drive, there is no hard drive to infect. Browsing without a hard drive is surprisingly normal. We have many options to save information beyond relying on a vulnerable hard drive:
  - Save files with the session to the DVD.
  - Save files to a USB flash drive.
  - Save files as Gmail attachments in email.
  - Copy and paste text into an email.

**Bookmarks are a self-made burden.** For synchronizing bookmarks between Windows and Puppy I had been using Xmarks with great success. Eventually, though, my rapidly-expanding bookmark list made that intrusive by needing a ponderous download for every sync operation. Now, by exporting bookmarks as HTML then sending that file to myself as an email attachment, I can have all the old and obscure bookmarks available by viewing email. I save important new

bookmarks to Google bookmarks "in the cloud," to avoid extending the DVD on every session. I do keep a few everyday bookmarks (tabs) locally.

**Puppy Linux is not the whole security solution.** Using a different OS can protect the computing environment from malware, including viruses, key-loggers and bot-nets. Browser, password, and connection security issues remain, although Firefox add-ons can be a big help. In addition to using Puppy Linux, users should:

- Use an external router firewall and the Linux firewall.
- Use on-line email and do not download unexpected attachments (try Gmail).
- Use the Firefox browser and keep it up to date.
- Use Firefox security add-ons, especially to support secure (SSL).
- Have and use different long, random passwords for each site account (try LastPass).
- Force SSL (<https://>) page connections whenever entering anything private, especially on social sites.
- Only enter passwords on clearly SSL-protected pages, particularly when using an unsecured wireless connection or free Wi-Fi.
- Never approve new SSL certificates.

**Puppy Linux is free, voluntary software.** New versions have been coming out every few months, although none are oriented specifically toward secure use. Apparently Puppy has had multi-session DVD operation for years, and may be the only live-DVD Linux supporting browser updates.

## The Linux Development Environment

The reality of free Linux can be a shock to Windows users. Microsoft has a few basic flavors of Windows, all of professional quality, which stay basically the same for years. Puppy Linux has any number of different versions, often going in different directions with a few part-time developers, which may last a few months to the next version, or just die out. The way to assess the new work is to download a likely .iso, burn it to DVD and see what it does.

Business users may point to the lesser quality in the free Linux distributions, but if Microsoft was really doing a quality job, we would not be here. Reasonable people can disagree about which OS is better and yet still prefer Linux to Windows for on-line security. In most cases, we can take an ordinary PC, boot Puppy Linux in a couple of minutes, do our online work in much greater safety, then reboot Windows.

Those who do most of their work in the browser may not have as much need to reboot Windows as they first expect. However, when it comes to devices that are in any way unusual or specialized or new, Windows always has a driver, and Puppy generally does not.

In free systems, it is common for things to not work as smoothly as in a professional product. In the case of Puppy Linux, usually there are work-arounds, since many other people have to do the same things as you anyway. Or there may be a new fixed version in a few weeks or a month. On the whole, Puppy Linux is very usable.

## Puppy Linux Resources

A surprising amount of information is available, although some of it is dated and some is hard to find. Here are some starting points:

- A remarkable visual .PDF introduction: [Introduction to Puppy Linux: Installation on a USB Flash Disk](#).
- Various video tutorials: [TutorialYouTube](#)
- A basic starting point: [Puppy Linux](#)
- Another starting point: [Basic info - getting started](#)
- The Wiki home page: [HomePage](#)
- A Wikibooks presentation: [Puppy Linux](#)
- A manual: [English Manual for Puppy 4.0](#)
- FAQ: [Puppy Linux FAQ](#)
- More: [More On Puppy Linux](#)
- The Barry Kauler site: [Puppy Linux](#)
- Puppy itself includes help, which brings up a little HTML viewer linking to some of these pages and a whole list of internal how-to's and applications documentation.
- The Puppy on a CD (or DVD) page: [Puppy on a CD](#)
- The multisession DVD page: [multisession live-DVD \(and CD\)](#)

## Write Puppy to DVD+RW as Multi-Session

For best security, Puppy should be booted from DVD and **not** installed to a USB flash drive or hard drive. Any boot medium that is immediately writable can be easily infected. To freeze out malware, we need to not provide an easily infectable boot storage. While a DVD+RW obviously can be written, writing to DVD is nontrivial, should be obvious to the user, can be absolutely prevented by removing the DVD, and is easily voided in any case. The following instructions are for Puppy 4.3.1 and similar.

Although the documentation recommends DVD-R, I think the results depend upon the particular burner drive the user has and particular types of DVD, which seem to vary a lot. I have had better luck with DVD+RW, and I can erase those and start over.

1. In Windows and Firefox, from:
  - <ftp://ftp.oss.cc.gatech.edu/pub/linux/distributions/puppylinux/>, or
  - <http://puppylinux.com/>, or
  - <http://puppylinux.org/wikka/HomePage>, or
  - <ftp://ibiblio.org/pub/linux/distributions/puppylinux/> (very slow).
2. Look around to find pup-431.iso (105MB) and download. If there is a newer version, use 4.3.1 until you get familiar with it, and only then update to the new version.
3. Burn the .iso to a DVD+RW, using special software if necessary (try CDBurnerXP). Use session-at-once and unselect "finalize" or select "Mode 2 XA multisession". (We want a "closed" session, but not a "closed" disc. If you find that Puppy cannot write to that disc with a "save", use Puppy Menu / Multimedia / Burniso2cd to burn another .iso copy using the Puppy burner software.)
4. An .iso file is just a drive-image of a CD or DVD. An .iso should not be burned as a normal file, because it already has a file structure, with files in place.

## Tell the BIOS to Boot a CD

The BIOS is the part of the computer which is in charge before a major operating system is loaded or "booted." Basically, the BIOS goes down a list of devices to see if they hold a bootable OS to load. The first thing found that can be loaded, is loaded, and becomes the computer OS for that session. Normally, we want the "first boot device" to be "CDROM". The idea is to boot from a CD or DVD when one is present, and otherwise boot from the hard drive.

To enter the BIOS, restart the computer and watch for the message about which key to press to enter the BIOS. Often this will be Del (the delete key), but may be something else. Press the key very quickly, or restart and try again until a BIOS configuration screen opens. Find "Boot / Boot Device Priority" or "Advanced BIOS Features / First Boot Device" or "Boot Sequence", and change the first entry to CDROM. Move subsequent entries down, including the hard drive entry, "HDD" or "Hard Drive" or "Hard Disk". Then save changes and exit, which will start a reboot.

For BIOS help, see: [Puppy on a CD](#), or [How To Access the BIOS Setup Utility](#), or [How to Set BIOS to Boot from CDRROM](#).

## Download Extra Programs

We want Firefox, and it need not be the latest version because it is so easy to update. We do want the latest possible Flash Player, which is harder to update. Some Puppy versions (e.g., puppies-431.iso) include Firefox and an updated Flash Player, and so do not need .pet installs. The main Puppy version (e.g., pup-431.iso) does not have Firefox, and Flash Player quickly becomes outdated. Firefox and Flash can be installed (or re-installed) by finding and downloading .PET files. To install a .PET, copy / paste it into Puppy memory (perhaps /tmp), click it to install, then delete that file.

1. Go to a .PET download site like:
  - o <http://www.puppylinux.ca/tpp/bugs/> (user: puppy, password: linux, twice) or
  - o <http://puppylover.netsons.org/dokupuppy/> or
  - o <http://dotpups.de/puppy4/dotpups/> or
  - o <http://petstore.puppyspace.org/> or
  - o <http://www.wisdom-seekers.com/puppy.html> or
  - o <http://qposil.com/pets/>.
2. Depending on what your Puppy version contains, possibly download .PET files to USB flash (then copy them to the Puppy drive before clicking to install):
  1. Firefox – firefox-3.5.6.pet or later (easily updated on-line)
  2. Adobe Flash Player – adobe\_flash\_player-10.0.42.34.pet or later

There is a Linux program called Wine which emulates Windows and allows some Windows programs to run in Linux. You may be tempted to install Wine, but DO NOT DO IT! Wine has gotten good enough to support a range of Windows malware, which is precisely what we are trying to avoid. If we need to run Windows programs, we probably should stop browsing and re-boot into Windows.

## Example Puppy Install

When used for improved security, Puppy Linux should **not** be installed to a hard drive but should instead boot from DVD on every session. As programs and configurations are added to Puppy, the changes should be saved to the Puppy DVD, provided nothing strange has happened in that session. If any attack files actually do make it into the RAM file system and are backed up on the DVD, the session can be voided later. This example install is limited by my ancient monitor. **This is a tested, working example for my particular equipment—do not follow it blindly!**

### A. Startup

1. Boot the Puppy DVD
2. confirm US keyboard layout
3. confirm English, USA language and country
4. select US/Central timezone
5. tab and select X/VESA display (preferred on my equipment)
6. for video changes, follow Menu / Setup to Xvesa Video Wizard and click
7. select 1024x768x24 or 1280x800x16 and CHANGE to try it
8. use control-alt-backspace to recover, if necessary
9. confirm OKAY for video mode

### B. Access .PET Files

1. insert USB drive with .PET files (e.g., Firefox and Flash)
2. USB flash icon appears named sda1
3. single-click on sda1 icon
4. green dot indicates flash drive mounted
5. (right-click and hold and select "Unmount sda1" before removing)
6. file manager window opens with flash root
7. single-click to navigate to downloaded .PET files

### C. Install PET Packages

1. (run .pet packages from Puppy RAM instead of USB flash)
2. single-click on desktop "file" icon
3. file manager window opens into "~" and subdirectories
4. single-click the green up-arrow
5. file manager window changes to deeper directory level
6. control-click to highlight each desired .pet file in flash
7. click and hold to drag all highlighted into "tmp"
8. select "copy" so the source version is not erased
9. single-click on "tmp" to open subdirectory
10. for each .pet file, single-click on file, click "OK" to install
11. right-click and hold on USB drive icon, select "Unmount sda1" and release
12. remove USB drive
13. close file manager windows to move on

### D. Set Up Firewall

1. follow Menu / Network to Linux-Firewall firewall and click
2. select OK, press Enter
3. press Enter to move on

### E. Configure Internet

1. on the desktop, click connect
2. click on internet by network or wireless LAN
3. click on eth0
4. click on Auto DHCP, connection succeeds
5. possibly save configuration, which gives an easier startup, but may cause problems when DVD boots on a different computer
6. click Done to move on

### F. Update Firefox

1. on desktop, click browse to start Firefox
2. in Firefox, follow Help to select "Check for Updates"
3. click "Update Firefox"
4. click "Restart Firefox"
5. close Firefox

### G. Save Changes to DVD+RW, then Reboot

1. on desktop, find "save" button and click
2. click "SAVE"
3. reboot computer by hardware reset button, power OFF then ON, or Menu / Shutdown / Reboot

4. Puppy comes back up
5. if network configuration not saved, on desktop click connect and set up internet connection as before
6. on desktop click Browse to start Firefox
7. in Firefox, follow Help to select "About Mozilla Firefox"
8. confirm updated version now on DVD

#### H. Install Firefox Extensions

1. in Firefox, follow Tools to "Add-ons" and click
2. select "Get Add-ons" and click "Browse All Add-ons"
3. Mozilla "Add-ons for Firefox" page opens in browser
4. search for and select each desired add-on and download into Firefox (if not updated on Mozilla, go to author's site for latest version) (if apparently unavailable, search "Firefox addons" and the add-on name to find the add-on generally hidden on the Mozilla site)
5. at least get important / security add-ons, shown in **bold**
  - **Adblock Plus** – hide ads to improve speed
  - **BetterPrivacy** – clear Flash cookies and DOM storage
  - CertViewerPlus – certificate viewer enhancements
  - Down Them All – fast download manager
  - **Facebook Secure Login** – SSL for Facebook login only
  - FEBE – backup Firefox configuration
  - FireFTP – FTP client
  - **Force-TLS** – remembers to use SSL on some sites
  - JSView – expose external stylesheets and JavaScripts
  - **LastPass** – encrypted passwords in the cloud
  - **Long URL Please** – exposes target of short URL's
  - MD5 Reborned Hasher – check hash in normal downloads
  - MultipleTabHandler – close multiple tabs
  - **NoScript** – whitelist for scripts, XSS protect, etc.  
Options / Advanced / HTTPS:
    - Force: mail.google.com www.google.com/calendar
    - www.google.com/ig www.google.com/bookmarks
    - \*.bankofamerica.com
    - Never: www.google.com/search www.google.com/support www.google.com/url\*
  - NoSquint – page and text sizing per site
  - PDF Download – better PDF control
  - PageDiff – show differences between HTML pages
  - **Permit Cookies** – whitelist for cookies
  - **Perspectives** – notaries expose SSL man-in-the-middle
  - **PhishTankSiteChecker** – announce known phishing sites
  - **Safe** – colored outline around SSL pages
  - Save Complete – File / Save Page As... improved
  - SearchMenu – fast dictionary, thesaurus (keep disabled)
  - Shooter – capture screen or entire page as graphic
  - **ShowIP** – show page IP addresses
  - **SSLBlacklist** – expose bad certificates
  - **SSLPasswdWarning** – warns when sending password w/o SSL
  - **Tab Mix Plus** – tab setup / crash protect (also Bookmark All Tabs)
  - Uppity – URL up-one-level
  - **URL Tooltip** – expose link URL with mouse
  - **WOT (Web Of Trust)** – danger colors on search result links
6. each can be uninstalled or disabled later from Tools / Add-ons...
7. when done, on the Add-ons panel, select "Restart Firefox"
8. when Firefox comes up, use Tab Mix Plus Session Manager, accept everything
9. remember to use desktop "save" button before ending session

#### I. Configuring Firefox for Windows and Linux

1. if you can configure Firefox on your own, do so.
2. Follow View / Toolbars to deselect "Bookmarks Toolbar"
3. In Windows, follow Tools to Options and select.
4. In Linux, follow Edit to Preferences and select.
5. Set up a Home Page URL.
6. In the Main tab, Downloads,
  - for Windows select "Always ask me where to save files"
  - for Linux select "Save files to" and browse to the bottom of the file system to select "/archive".

#### J. Configuring Firefox

1. In the Tabs tab, unselect all warnings.
2. In the Content tab, unselect "Enable Java".
3. In the Privacy tab,
  - at "Firefox will:" choose "Use custom settings for history".
  - Unselect "Accept third-party cookies"
  - Select "Clear history when Firefox closes", click "Settings..." and select everything except "Site Preferences" and "Tab Mix Plus Saved Sessions" and click "OK".
4. In the Security tab,
  1. unselect "Remember passwords for sites" (never allow any browser to manage passwords).
  2. at "Warning Messages" click "Settings...", check only "I submit information that's not encrypted."
5. Click "Close" to move on.

#### K. Configure Tab Mix Plus

1. In Firefox, follow "Tools" to "Tab Mix Plus Options" and select.
2. In the "Events" tab,
  - under "Tab Closing", for "When closing current tab, focus", select "Last selected tab".
  - under "Tab Features", "Max number of closed tabs to remember" enter 50 and select.
3. In the "Display" tab, under "Tab Bar"
  - Select "New tab button" and "on Left Side".
  - Select "Close tab button".
  - Unselect "All..." and "Extra..." options.
  - For Hide the tab bar, select "Never".
  - For When tabs don't fit width, select "Multi-row".
  - For Max number of rows to display, select "5".

4. In the "Display" tab, under "Tab"
  - under "Highlight" select "Current tab" only.
  - under "Show on Tab" unselect "Close tab button".
  - for "Tab width" use 25 to 250.
5. In the "Session" tab,
  - select "Enable Session Manager" and "Enable Crash Recovery" only.
  - On "Start/Exit", for "When Browser Starts", select "Ask Before Restoring".
  - For "When Browser Exits", select "Save Session".
  - For "Startup Session", select "Last Session".
  - In Preserve tab, select everything.
6. Click "OK" to move on.

#### L. Save Changes

1. close any open windows
2. right-click on and unmount any USB flash and remove
3. on desktop, find "save" button and click
4. click "SAVE"

### Using Windows Drives

When Puppy comes up it will look for system drives (hard drives, floppies, CD's, etc.). The drive names will be unfamiliar, but it is easy to see what files are on any drive. A single click on a drive "mounts" that drive, and a directory window will appear. A mounted drive will have a green on-screen dot or "LED" indicator as a reminder. Right-click-and-hold to select "Unmount" when done using the drive.

### Using NoScript

NoScript is a browser add-on that disables JavaScript and most other scripting languages, but allows scripting to be enabled for any particular page and remembered for future use. Scripting is a problem because scripts are executable program code which the browser downloads and runs as part of a displayed page. Not enabling scripts can cause awkward page problems, but enabling a malware script can cause security problems. For sites you go to once, you might enable them temporarily, provided they look like respectable sites, meaning that WOT and PhishTank do not go crazy. Click the S button on the Status Bar to show alternatives.

### Using LastPass

The user is responsible for having good passwords. A good password cannot be short and it cannot be words or names. The best password is a machine-generated sequence of random characters. A good 15-character password is probably stronger than every other part of the system. We cannot remember such passwords, so we need a password manager to save them for us. Passwords are saved in a little database protected by cryptography done right.

The password manager LastPass.com works either as a local program or a website. The contents of many other password managers can be imported into LastPass. Users can access their passwords from the website using any uninfected computer. Booting Puppy Linux from DVD is the best approach to get a believably uninfected OS. Saving the encrypted database on the Web provides both off-site backup and synchronization for use with multiple computers. LastPass has a Firefox add-on both for Linux and Windows.

Starting to use password management can seem like being out of control. Only the password manager knows the actual passwords, and if it dies, what then? First, there is a copy of the encrypted password database saved on the LastPass website. Next, the browser add-on stores a copy of the database locally, for use if the web site is down. And the database can be exported for backup or use by a stand-alone LastPass program.

Using LastPass can seem scary, because it tries to be automatic. New sites are included by signing in and letting LastPass create an entry. Sometimes the automatic way fails, and sometimes the web site changes their login page. A manual login option is available by clicking on the LastPass icon, and then selecting the current site. The Username or Password can be copied to the clipboard, which then can be pasted into the desired location.

Correcting a login sequence can seem daunting, but there are relaxing options. When I edited an entry and changed the name, the old entry was not lost but the new entry was added. That meant I could change the new entry as desired without losing the password.

LastPass also has a "Secure Notes" feature which saves little text files in the encrypted database. Secure Notes can be used to save Username and Password, just to make sure nothing is lost. Secure Notes also is a good way to save the security questions and answers which will be needed if the owner becomes incapacitated. Since emergencies are inevitable, your spouse or someone responsible should have your LastPass password.

### Saving Files to DVD+RW

New or modified files can be saved to the DVD. For some reason, the desktop "save" button seems more reliable than an update triggered by Menu / Shutdown. The "save" button copies all changed files to a new session or directory on the DVD, but does not mark them as saved, so clicking "save" again will save all the same files again! Then ending the session by Menu / Shutdown will try to save those same files again! Just say no! Each boot after a "save" will complain about an "unclean exit" for "x" but just select "Ignore" and move on.

I try to limit my DVD saves to once a week or so.

Files in the /tmp directory are not saved to DVD. Files in the /archive directory are saved to DVD, but not recovered in the next boot. Changed files are saved to DVD without overwriting the older versions, and only the most recent version recovered on boot.

In most file systems, a new file replaces the old one. But each time Puppy Linux saves to DVD, it creates a new DVD directory for that save. So the DVD can contain the file as it was each time it was saved. This will automatically archive the progress of a writing or programming project over time in a way that does not occur in normal computer file systems. Each DVD session, and each archived file version, can be read from DVD under Linux or Windows.

### DVD Issues

As a banking security system, Puppy Linux should be booted from DVD, and run in memory. The unique Puppy Linux ability to update the DVD is what makes a DVD boot practical. But updates do need to be written to the DVD, and optical storage simply is not as reliable as hard drive storage.

Since all storage systems are somewhat unreliable, our Puppy response is just to be more rigorous than usual. For example, I manually back up an important local work (like this article, during development) before the end of every session. I may copy my file to a USB flash drive (1 minute), or send the file to myself as an email attachment (2 minutes), and save it to a Windows drive (1 minute), if present. Even if I work "in the cloud" using Google Docs, I still "Download as" the file and attach it to an email to myself, thus creating a project archive without writing to the DVD.

Sometimes upon restart Puppy comes up (the splash screen shows), but then fails upon reading the last saved session. We can void the last session by starting Puppy again and entering the command "puppy pfix=1" at the splash screen input.

Rarely, we can find that the last session save has made the disc completely unreadable, at least for boot purposes. Then we need to start over with a new disc we have cleverly made in advance.

### **Making a configured boot DVD**

Perhaps the best way to "copy" a configured Puppy DVD is to first boot from a fully-configured DVD. Then download and burn (and verify) the current .iso to a blank DVD using Menu / Multimedia / Burniso2cd. There will be a lot of drive door opening and closing going on, and I have found it important after any door closing to watch the burner LED and wait for it to settle down before issuing a command. Then clicking "save" will burn the current configuration, effectively making a copy, probably with fewer saved DVD sessions. This may be a good common base for DVDs used by a group, a class, or a family.

Since Puppy essentially selects a video configuration when it first runs (as opposed to making a new selection on each boot), moving the already-video-configured disk to a new machine can be an adventure. By comparison to another Puppy system, it may be possible to select Menu / Setup / Xvesa Video Wizard (or whatever) and choose a reasonable mode *without being able to read the selections*. Once everything is configured for a particular computer, click "save" and you will have the same thing on the next boot. Eventually it would be a good idea to burn a new .iso DVD and use "save" to make a standby copy configured for that computer.

### **LET ME KNOW!**

Also see:

- [PC Banking Security Q&A \(18K\)](#)
- [Basic PC Security \(150K\)](#)
- [Simplified PC Security \(26K\)](#)

If you find errors or problems, let me know!

If you think changes are needed, let me know!

If something else needs to be covered, let me know!

If you try it with success, let me know!

If you try it and have problems, tell me about your technical level, what you tried, and what went wrong, but let me know!