# *E-Government* Services in Florida Public Libraries:

## *Best Practices for Patron Computers*

Mickey Boyd

Revised June 2014

# Best Practice Summary for Libraries and Library Staff

Florida Libraries are experiencing high usage of public access computing resources for *E-Government* activities. Therefore, it is imperative to offer a safe computer environment for *E-Government* and other public access activities.

Best practices include:

- Equipping computers used for *E-Government* with a windows lockdown program and a hard drive protection program.
- Creating library policy mandating proper operation of hard drive protection programs.
- Being aware of security concerns pertaining to *E-Government*.
- Educating staff and patrons on safe use of the Web for *E-Government*.
- Providing patrons easy access to a privacy mode Web browser.
- Being familiar with legal concerns associated with delivering *E-Government* services in the library.

# Configuring Public Access Computers for *E-Government* Services

The most common approach used by libraries to provide patrons with a safe computing environment is to use consumer-grade PC computers, running either Windows 7 or 8 operating systems as a base. Other useful software is installed, and then the computer is protected with several security products. This is the approach described within this document.

There are alternate choices to providing a safe computing environment within libraries. They include sophisticated, managed Windows environments, and the use of computers with a non-Microsoft Operating System (OS).

There are many economic advantages to using standard consumer-grade Microsoft Windows 7 or 8 computers for public access. Such computers are cheap and readily available, often at a steep discount for non-profit organizations. Specialized public access software products are used to provide protection against patron vandalism, both intentional and accidental, and malicious attacks by computer criminals. This strategy can produce reliable public access computers that are relatively simple to maintain.

Within libraries, patron computers are set up to "forget" the changes that individual users generate during their sessions. Typically, library computers used for *E-Government* and public access are continuously being "reset" to a known safe configuration through the use of hard drive protection products. Also, library computers usually minimize the features exposed to patrons through the use of windows lockdown programs.

# Alternate Choices

There are other alternate approaches to providing a safe computing environment within libraries. They include sophisticated, managed Windows environments, and the use of computers with a non-Microsoft OS.

**Computers That Use A Non-Microsoft OS**

Most malicious attacks are targeted at Microsoft Windows operating systems. Therefore, a large amount of computer risk can be avoided by choosing a non-Microsoft OS for public access computers.

Macintosh computers can effectively be used in libraries for *E-Government* and public access. The guest account features of OSX can work well for public access and *E-Government* use. To further enhance patron safety and security, hard drive protection products are available for OSX with capabilities similar to Windows hard drive protection products.

Linux based products are another option. There is at least one Linux based operating system environment specifically designed for libraries, *Userful Desktop*. This product is in use by at least one Florida library system, and numerous libraries in other US states and Canada. The product can be evaluated for free. It provides a user experience that is in some ways much more secure than a Windows session.

**Sophisticated, Managed Windows Environments**

Highly managed Windows environments are among the most flexible and customizable public access computing solutions. However, they require highly trained IT staff, and significant support infrastructure. In such environments, administrators can decide just what Windows functionality is exposed to public users. These decisions are often implemented using *Group Policy*, a Microsoft OS feature that allows the precise definition of rules to control the environment of user accounts. While *Group Policy* is endlessly flexible, it is also easy to make a mistake, or omission, when trying to provide a safe computing environment. Many commercial Windows lockdown

programs are essentially simplified interfaces to the types of changes that can be made with *Group Policy*.

Such environments might include specialized client models, such as Remote Desktop Services, thin clients or virtual desktops. These client models use the computers at each public access seat as remote keyboard/video/mouse units, with most of the "work" for each user session being performed by a central server, or set of servers.

# Windows Lockdown Programs

Windows lockdown programs allow staff to turn off unwanted features on patron computers. There are many commercial Windows lockdown programs to choose from. Choosing a specific lockdown program involves a compromise between cost, features, integration with other public access software and ease of use.

Most Windows lockdown programs offer the following features:

- Disable or restrict start menu.
- Disable or restrict control panel.
- Disable or restrict printer changes.
- Disable or restrict desktop changes.
- Disable run button.
- Disable command prompt.
- Control access to USB/Firewire devices.

In addition to these basic functions, lockdown programs often include the ability to customize the way various common applications behave. For example, most such programs allow staff to configure the features that *Internet Explorer* provides. Some lockdown programs allow for customization of any application, and the ability to rigidly define what applications are allowed to run at all.

Sample Windows Lockdown Programs:

- *Winselect* by Faronics.
- *Fortres 101* by Fortres Grand.

# Hard Drive Protection Programs

In a library setting, it is important to guarantee as much as possible that patrons cannot affect each other with their computer sessions, particularly those engaged in *E-Government* work. In other words, each patron should have a "fresh" computer environment that is completely free of any changes made by past patrons. Fortunately, it is easy and inexpensive to add this capability to a computer.

Hard drive protection programs form the core security for library computers used for public access and *E-Government*. These products not only protect patrons from each other, they also save staff time and effort that would otherwise be needed to fix computer problems. When properly deployed, a computer using a hard drive protection program can simply be rebooted to fix most issues, as it will go back to a known good state.

These programs work by "tricking" Windows into seeing a hard drive that is actually simulated in software. This software hard drive pretends to work normally while Windows is being used, allowing changes as expected. However, these changes are not actually being recorded on the real hard drive, they are instead a part of the simulation. When the computer is rebooted, the simulated changes are discarded, and the computer boots back up to a known good state.

To set up a new computer for *E-Government* and public access use, one begins with a freshly installed and updated Windows operating system. Commonly used software, such as Microsoft Office or Adobe Reader, should be installed and updated, including antivirus or other security software. A Windows Protection Program should be installed and configured. At this point, the computer is in a known good state, before it has been used for any type of general computer tasks. This would be a great time to install and activate a hard drive protection program. After activation, unwanted changes to the computer will simply go away upon reboot.

All hard drive protection programs provide the ability to turn their protection on and off, both by hand and automatically, via a schedule. Most libraries will want to take advantage of both types of control. There are some permanent hard drive changes that are desirable. Common examples include: Windows updates; Office updates; Adobe updates; and security updates, such as antivirus. In other words, the portions of the computer that protect patrons from security and reliability problems should be allowed to make changes to the hard drive.

Typically, this is done in a scheduled fashion. The hard drive protection program is configured to disable protection at a certain time in the evening, usually after the library is closed. The operating system and security programs are then given an opportunity to download and install their updates. After completing the updates, the computer either resets or turns itself off. The next time it is turned on, it will boot up in protected mode, freshly updated for security and reliability.

Most hard drive protection programs offer the following features.

- Enable/Disable Hard Drive Protection via password.
- Enable/Disable Hard Drive Protection via time schedule.
- Create a Temporary Writeable Drive.
- Create a Persistent Writeable Drive.
- Enterprise Console Capability.

Writeable drive features allow library staff to define drive letters on the computer (for example, D: or E:) where changes are allowed to occur. These writeable drives can either be temporary, and thus erased on every reboot, or persistent. These features can be useful in some situations. Any use of such features should be carefully considered with respect to risk.

Most commercial hard drive protection products can be used either in a standalone fashion, where each computer must be visited to make changes, or from an enterprise console. An enterprise console is a, “master control program,” for all the library's computers on the network that are using the correct hard drive protection program. From the enterprise console, a staff member can see the status of all library computers intended for patron

use. That staff member can also reboot any computer, or enable/disable the hard drive protection. Enterprise console capability is very useful when a large number of computers are being managed. The importance of that feature should be considered when evaluating hard drive protection programs. Some vendors include this capability at no extra charge, while others require a more expensive version of the product license.

**Sample Hard Drive Protection Programs:**

- *Deep Freeze* by Faronics
- *Clean Slate* by Fortres Grand
- *SmartShield* by Centurion Technologies

# Importance of Per-User Reboots

Sadly, it is not uncommon to encounter library systems that have deployed hard drive protection products, but do not use them to their full advantage. Most hard drive protection products function using a, "reboot and restore," method, where a computer reboot is necessary to erase all changes. A computer reboot will also destroy any memory resident copies of malicious software, and generally resets everything completely for each user.

**When using a, "reboot and restore," hard drive protection program, it is very important to reboot between every user!**

This simple point cannot be stressed enough. Unfortunately, some libraries misunderstand how the products work, or do not realize how easily users can affect each other when the computers are not reset. The result is compromised security, and ultimately, reduced safety for patrons.

A common way that hard drive protection products are misused is to leave library computers booted up all day, without any reboots. The hard drive protection product erases all changes that occur within that day when the computer is turned off in the evening, which does help both security and reliability. However, this means that every user of that computer for an entire day may have accidentally left privacy information or malicious software behind. Other users during that day might find this privacy information, or be attacked by the malicious software. Indeed, each user could potentially be both a source, and a victim, of various malicious attacks. Library computers are often heavily used, sometimes serving dozens of people each day. Failing to reset computers between each user creates significant risk for patrons.

Simply put, it is a best practice for library computers used for *E-Government* and public access to be rebooted between users, thus allowing a hard drive protection product to completely reset the system. Libraries should develop computer policies that include a mandatory reboot between each patron, either initiated or verified by a staff member.

# Reboot Optimization

One way to encourage compliance of a mandatory, “reboot between each patron,” policy is to make the reboot process as quick and easy as possible.

There are many technical websites that have tips on how to reduce reboot time; try search terms like, "speed up windows boot," to find them. Most modern computers can be configured to boot Windows 7 or 8 in approximately 20-30 seconds. There are also techniques to speed up the Windows shutdown process, which must also be endured during a reboot. Common reboot speed-up techniques include:

- Configuring the BIOS to eliminate timeouts, default to hard drive and enabling the quickboot feature.
- Using free Microsoft boot optimization tools, such as msconfig.

In addition to improving the boot speed of the computer, one can also reduce the effort that goes into the chore of actually initiating the reboot. It is easy to create a super fast reboot button on the desktop of each library computer. Just one click, and the computer will reboot, which is much better than the several clicks, and waiting for the start menu, that are usually required.

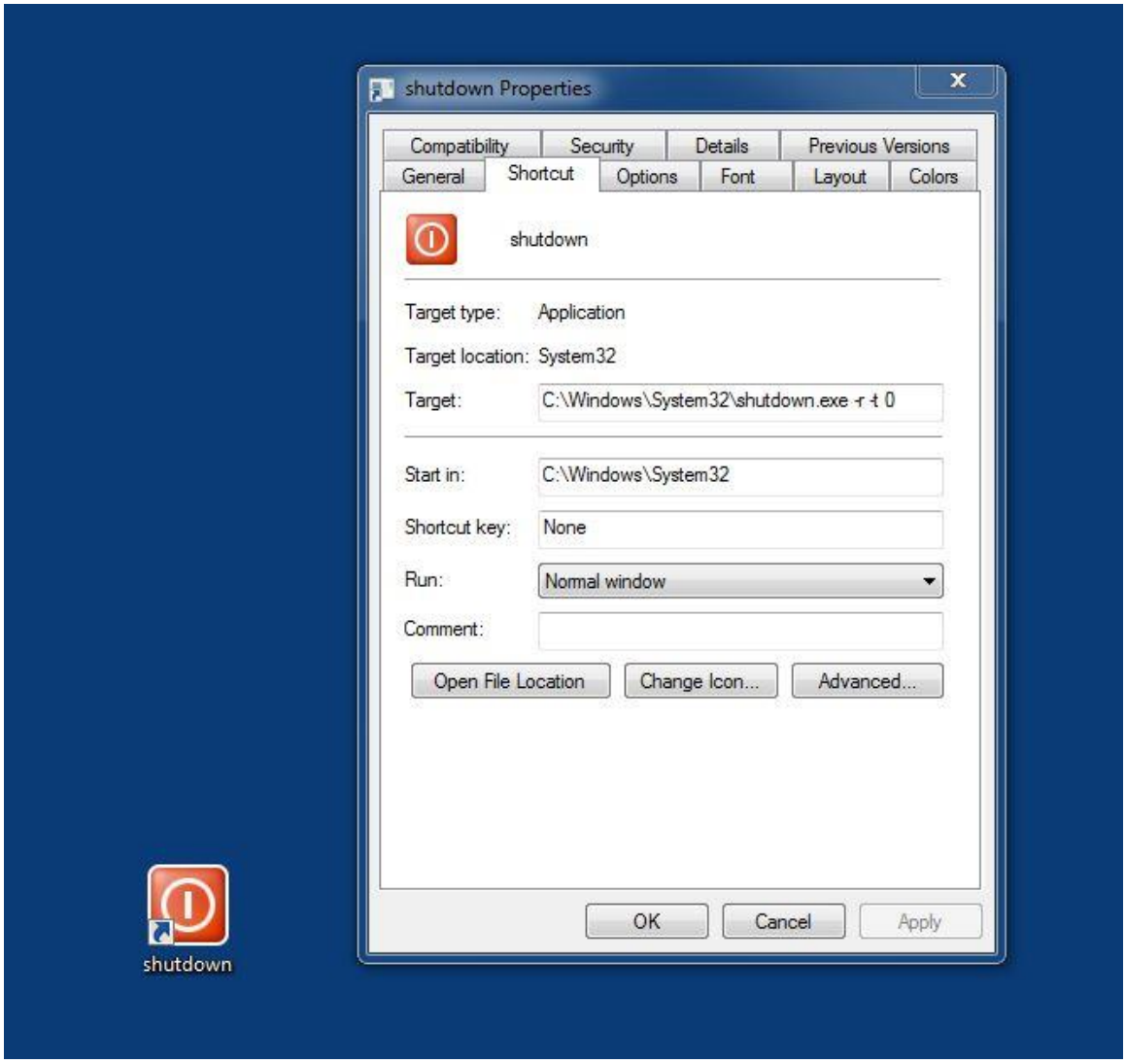
It is important to clearly label the super fast reboot icon, as patrons can lose their work if it is accidentally clicked. An easy way to do this is to put it in the middle of the desktop. A sticker on the monitor could suggest that patrons, “Close all windows and click REBOOT when done.” Library staff should verify that each patron computer is rebooted as the patron departs.

# Super Fast Reboot Icon

In Windows 7 or 8, follow these steps to create a Super Fast Reboot Icon:

1. Right click on the Desktop; choose New; then Shortcut. A window will appear with a box labeled, "What item would you like to create a shortcut for?"
2. Click the Browse button; then Computer; then navigate to C:\Windows\System32\shutdown.exe. Depending on your settings, it may be shown as just, "Shutdown," with no .exe extension. Click OK.
3. You should be back at the window with the box labeled, "What item would you like to create a shortcut for?" The box should now contain C:\Windows\System32\shutdown.exe. Click Next.
4. A window will appear with a box labeled, "Type a name for this shortcut."
5. Type in REBOOT; Click Finish.
6. A plain icon named REBOOT will appear on the desktop. Right click the icon; then click Properties.
7. You should be looking at the Shortcut tab. One box will be labeled, "Target:" and will contain, "C:\Windows\System32\shutdown.exe."
8. Click at the end of this box, and add, "-r –t 0" to the end of the line. It should be, "C:\Windows\System32\shutdown.exe –r –t 0." There must be a space before and after the "-r." There must be a space between "t" and "0." That is a numeric zero, not the letter "o."
9. Click, "Change Icon" in the lower part of the window, and choose a good icon. The square red shutdown button icon is a common choice.
10. Click OK.

The super fast reboot icon is simply a shortcut to the standard Windows shutdown program. The "-r" change instructs the shutdown program to reboot, and the "-t 0" instructs the program to wait zero seconds. Using such an icon is much quicker than rebooting via the start menu, and will assist in compliance with a, "reboot between each patron," policy.


shutdown Properties
Compatibility
Security
Details
Previous Versions
General
Shortcut
Options
Font
Layout
Colors
shutdown
Target type: Application
Target location: System32
Target: C:\Windows\System32\shutdown.exe -r -t 0
Start in: C:\Windows\System32
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply
shutdown

# Computer Security Concerns

The security environment present on today's Windows computers is high risk to innocent users. While some computer vulnerabilities are fixed before they are exploited, computer criminals seem to be able to find an endless stream of new vulnerabilities. Unfortunately, it is common for computer criminals to possess many effective Web exploits at any given moment. These exploits are mixed with malicious payloads in endlessly changing combinations, and then delivered to victim computers by many different means. If a particular patron makes poor, or gullible, choices while browsing the Web, or if they are successfully tricked by one of the many Web scams present on the Internet, the chances are high that malicious software will be present on that computer, no matter what security software is present.

Unfortunately, even a careful user with a fully updated computer can be successfully attacked by malicious software on the Web. There have been many documented cases of innocent websites being subverted by computer criminals into sources of malicious software. Subsequent visitors to these innocent websites are attacked with, “drive-by download,” methods that deliver malicious software to their computers without their knowledge.

There are best practices that can help reduce the risk of computer and Web interactions, but there is no way to guarantee complete safety. This is why it is critically important to completely erase all of the changes caused by a particular patron before the next patron uses the computer. Any previous patron could have infected the computer with malicious software, either intentionally or not. While the library cannot protect patrons from themselves, it can effectively protect patrons from each other through the proper use of security software, in particular, a hard drive protection program.

Windows computers accrue damage, malicious software and personal information, with time and use. This is a bad combination. Hard drive protection products allow library staff to effectively, “turn back the clock,” on patron computers. Properly used, they are powerful tools that mitigate significant risk. By simply rebooting a computer equipped with a hard drive

protection product, all changes made since the last reboot are discarded. Doing so between each patron will help ensure that *E-Government*, and other private activities remain private. For example, temporary Web browser files created during patron Web sessions can contain private information. These files would be completely expunged upon reboot.

The additional security software installed on patron computers will vary based on the specific needs of each library system. There are many vendors that offer such products. If possible, libraries should avoid the most common security products. Computer criminals have become adept at concealing their malicious software from the most popular security products. To do so requires tricks specific to each security product. In other words, criminals generally cannot hide their malicious software from all security products, but they can hide it from specific products if they make the effort. Of course, they pick the most popular examples of security software for this special treatment. The conclusion is that the best security products are those that have excellent features, but not much market share. Fortunately, the security marketplace is rich with good choices.

An interesting trend that is beneficial to libraries is the inclusion of security software within popular hard drive protection programs. Several vendors now offer integrated antivirus and security features within their hard drive protection product. This is a convenient combination of functionality, as it allows for easier coordination of security updates on machines using a hard drive protection program.

# Physical Security

Library patron computers should be protected from physical mischief and vandalism. This contributes not only to the reliability of the equipment, but also to patron safety and privacy. Special furniture can be used to protect patron computers, essentially locking away the vulnerable areas of the computer. Alternately, keeping computers completely exposed, and in easy view, is another approach to discourage tampering. The areas where cables plug into the computer are particularly important.

Keystroke logging devices (or "keyloggers") are a serious physical threat to library patron computers. These devices are cheap and easy to obtain. They appear to be cable adapters, and often blend right in when connected to a computer. They are available in both PS/2 and USB versions, and plug in where the keyboard normally connects to the computer. These devices are essentially small computers, with their own memory and other resources. Keyloggers "listen" in on the keystrokes coming from the keyboard, recording usernames, passwords, URLs, and any other information input by the keyboard. The keyloggers record these keystrokes into their own memory. When the keylogger is retrieved and connected to another computer, the memory contents can be examined. In other words, the devices must be placed on computers, time goes by while the computers are used, and finally the keyloggers are retrieved by the criminals and taken to some other location.

Pictured below are example PS/2 and USB keyloggers:

Keylogging devices cannot be detected by software, and must be discovered via physical inspection. It is important to regularly inspect patron computers for foreign devices. Any suspicious activity associated with the cabling areas of the computers should be noted and investigated. It would be logical for criminals to use minors to place and retrieve keylogger devices.

Libraries should develop a set of procedures to be followed in the event of a keylogger discovery. Involve law enforcement in the discussion if possible, as there may be special resources that can be deployed for computer crime.

# Web Browser Security

Web browsers are the workhorses of modern computers. They are also under continuous scrutiny and attack by computer criminals. Some browsers are perceived to be more secure than others. This is a continuously changing situation, and to some degree is a game of numbers. For example, even if a careful user uses a browser that is considered highly secure, and does so in a conservative and cautious way, that user could still be successfully attacked by malicious software. It would be bad luck, but it could happen. However, the odds of that careful person and secure browser being a victim are much lower than that of a careless user running an old and poorly updated version of *Internet Explorer*.

*Internet Explorer* gets a lot of bad press. It is a program that many love to hate, or at least criticize. It is important to note that the newest version of *Internet Explorer* is an excellent modern browser with many new safety features. However, there are many millions of users on the Internet that use old versions of *Internet Explorer*. To understand why this is a serious concern requires a bit of history.

In the early 2000s, the Internet was a very different place. *Internet Explorer* 5 and 6 commanded 95% of the browser market. Both of these browsers had their own idea of how webpages should work. In other words, they did not adhere well to Internet standards. Often, webpages required many nonstandard tricks and workarounds to appear correctly on these browsers. Since alternative browsers only made up a tiny percentage of the market during that time, many websites only worked correctly with *Internet Explorer*.

As time went on, more alternate browser choices appeared and matured. These alternate browsers offered powerful features that were not present in *Internet Explorer*. Some of these features include, Browser Tabs, Popup Blockers and the ability to install add-ons. As the market share for alternate browsers increased, businesses and organizations began to publish webpages that would work well with them. For the most part, alternate browsers tend to follow Internet standards closely, so fewer special

exceptions are needed for webpages to display properly. This has led to an Internet that is based more on standards, which is a good thing for compatibility and security.

Unfortunately, there are still plenty of people using old versions of *Internet Explorer*. These old browsers lack the advanced security features built into modern browsers. *Internet Explorer* is one of the most popular Web browsers in the world, particularly for nontechnical users. As a result, a large percentage of the Web-based malicious software is aimed specifically at weaknesses within *Internet Explorer*, particularly older versions. Entire classes of malicious software will only work against *Internet Explorer*. In other words, avoiding the use of *Internet Explorer* is a way to sidestep a lot of potential danger.

That is not to say that alternate browsers do not have their own malicious software concerns. Because of their popularity, *Firefox* and *Chrome* have also become popular targets for criminals. As a particular browser grows in popularity, malicious software attacks targeted at that browser grow as well. This leads to the conclusion that the safest Web browser to use for *E-Government*, and other activities involving privacy information, is one that has excellent security features and modest browser market share.

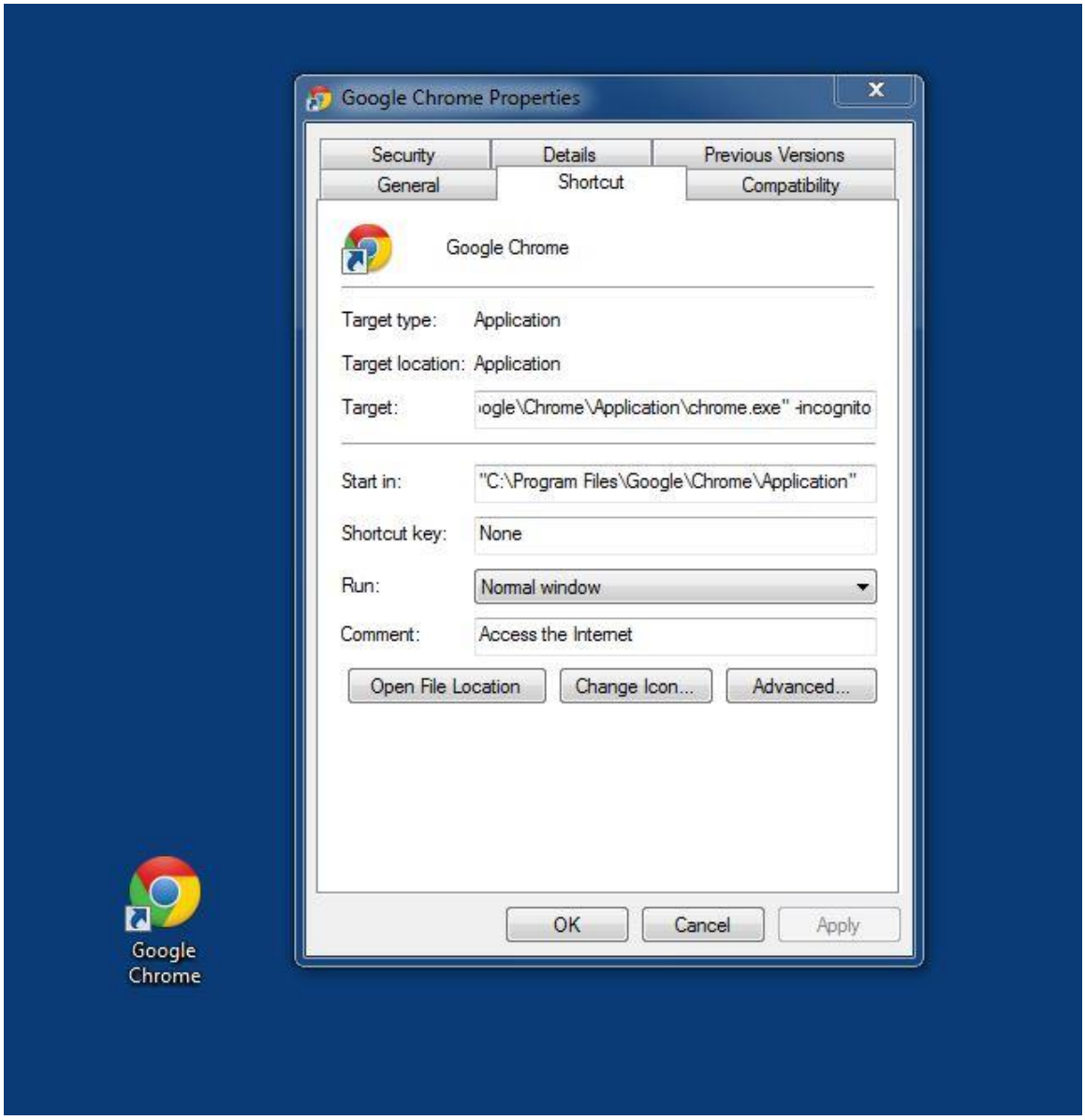
One important caveat is that there are still websites that require a particular version of *Internet Explorer* to work correctly. This can sometimes be a problem with *E-Government* websites, particularly those that have not been updated recently. Because of this, it is important for libraries to retain the capability to run *Internet Explorer* as a last resort. However, patron safety will be enhanced if *Internet Explorer* is not the default recommended Web browser on the computer.

# Configuring a Private Mode Web Browser

Many modern Web browsers have a privacy mode that can be used for private activities. When the browser is in this mode, it behaves in ways that increase security and privacy. No history is recorded during a privacy mode session, nor are temporary files or Web cookies saved. When the Web session ends and the browser is exited, all traces of the session are expunged. This behavior is ideal for *E-Government* use. Patrons who wish to engage in *E-Government* activities on library computers should be encouraged to use a browser in privacy mode.

At the time of this writing, the *Google Chrome* browser is a strong recommendation. It has powerful security features. *Chrome* calls its privacy mode, "Incognito Mode." It is easy to modify the *Chrome* desktop shortcut so that it brings up *Chrome* in Incognito Mode every time. To do this:

1. Download and install *Google Chrome*.
2. Find the *Google Chrome* icon on the desktop. Right click the icon and select Properties.
5. You should be looking at the Shortcut tab. One box will be labeled "Target:" and will contain a long line of text that ends in chrome.exe.
6. Click at the end of this box, and add the text, "-incognito" to the end of the line. Then click OK to close the window.


Google Chrome Properties
Security
Details
Previous Versions
General
Shortcut
Compatibility
Google Chrome
Target type: Application
Target location: Application
Target: ogle\Chrome\Application\chrome.exe" -incognito
Start in: "C:\Program Files\Google\Chrome\Application"
Shortcut key: None
Run: Normal window
Comment: Access the Internet
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply
Google Chrome

# Secure Web Browsing Strategies

The World Wide Web contains many websites that will attempt to infect visitors with malicious software, in a variety of direct and indirect ways. In some cases, such websites are obviously seedy or questionable. In other cases, such websites appear to be entirely innocent, and may even radiate legitimacy or a sense of security. It is best to assume that the chance of encountering malicious software during a typical Internet session is quite high. Such software can come from unexpected sources. Even security conscious users can be successfully attacked, as there have been many examples of highly trusted websites being tricked into distributing malicious software. An obvious observation is that as the number of websites visited during a session grows, so does the risk of being infected with malicious code.

In other words, the scope of a malicious software attack is restricted to the amount of Internet activity in a particular computer session. If the computer is using a hard drive protection product, then each time the computer is rebooted, all private data will be erased, including any that may have been left behind after performing an *E-Government* task. The ability to completely erase all changes is an advantage that patron computers in libraries have over typical home computers.

Put simply, patrons should be advised to not mix tasks for which security is important with recreational Web browsing. The safest approach is to perform secure work on a freshly reset computer, then log out and reset it again before engaging in other activities. The idea is to minimize the chance of malicious software having access to privacy information that may be present in the memory of the computer, within temporary files or even on other tabs of the Web browser.

Some situations might not allow patron computers to be reset more than once per user. For example, extra reboots might not integrate well with the computer reservation system. In such cases, the recommended approach is to use a Web browser in privacy mode to perform *E-Government* and other

secure work. The work should be performed, and then the browser should be completely exited. Doing so will trigger the privacy mode behavior, erasing any temporary data associated with that Internet session. Afterward, the user can run a fresh browser and continue using the Internet.

# *E-Government* Services on Home Computers

Home computers must be configured in a secure fashion if they are to be used for *E-Government* services. Install security software on the computer, and check often to make sure the security software is updating regularly. For most commercial security products, this implies a recurring fee. Many new computers come with commercial security software that receives updates for a short time, and then begins to request payment for more updates. It is very important for security software to receive updates.

As an alternative, Microsoft offers free security software for Windows, called *Security Essentials*. Updates are also free.

Make sure the operating system is up to date. Activating Automatic Updates for Windows is recommended.

Understand what a Web browser is, and is not. Tutorial movies are available that explain this clearly.

Avoid using *Internet Explorer*. If *Internet Explorer* is required, update to a new version.

Install a Web browser that offers a privacy mode. A recommended choice is *Google Chrome*. Within *Chrome*, the privacy mode is called Incognito Mode. Incognito Mode is designed for privacy, and will safely erase all history and temporary data associated with a Web session each time the browser is exited.

Do not mix private Web tasks that require private information, such as *E-Government* activities, with recreational Web browsing. Doing so increases exposure of private data to malicious software attacks. Perform private Web tasks separately, and then completely exit the browser.

While privacy mode is ideal for secure activities, it can be inconvenient for general Web browsing. For example, many websites use cookies in useful ways, such as to remember what has already been seen during a previous visit. Such websites usually work best with a Web browser that is not in privacy mode.

Use good passwords. Passwords should be at least eight (8) characters long, use letters and numbers and ideally have at least one symbol character. Longer passwords are more secure, so use the greatest number of password characters you are comfortable memorizing. In general, it is better to use a small number of good passwords rather than a large number of poor passwords.

Avoid using the password save feature within Web browsers. These features can be attacked by malicious software, in the worst case resulting in the compromise of all saved passwords.