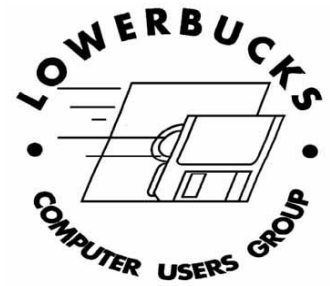


The ASCIIriber

THE JOURNAL OF THE LOWER BUCKS COMPUTER USERS GROUP

Volume 28 • Issue 8, October 2009



Using Your PC As A Media Center

This month we'll look at some of the media server software you can use to create a link between your PC, gaming system and television. For example, how about using your WII to view HULU video feeds? Or starting your PS3 and then watching movies or listening to music that you have stored on your computer?

There are a number of programs. Some are free, some cost a little money. We'll look at some of them and talk about the others.

One that I have been evaluating is called playon and can be found here:

<http://www.themediamall.com/playon>.

It cost \$40 but I think it is well worth the money. At the next meeting I will tell you why.

See you on Sunday.

NEXT MEETING:

SUNDAY, October 4, 2 P.M.

Free software and ways to help your computer. You can't ask for more and it's all provided by Jim McGorry

- AMP Font Viewer
- Control Ill Behave Applications
- Daemon tools
- Stop Key logging software
- Key loggers can read from clipboard
- More tricks to evade key loggers
- Object dock
- Opera 10

Weekly Download Section from Jim McGorry

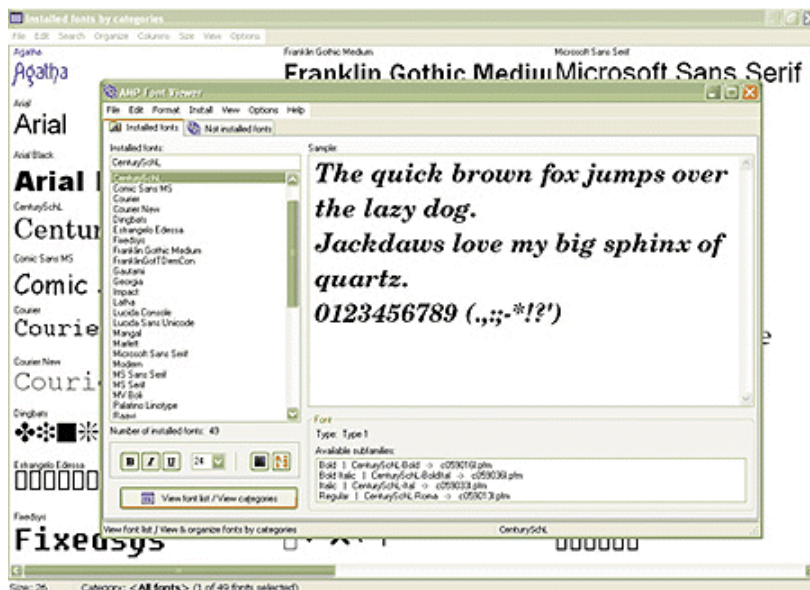
Welcome members and visitors alike to this new section I hope it will be of interest and use to you. Each month I will try and have interesting and useful programs for you to download and try on your systems as you see fit. Some are free and some may have a nominal fee.

A brief write-up and link to download page will be displayed here so you can determine if you wish to get it and use it.

ALSO NOTE: Some web addresses may not be a direct link. If not, then just copy and paste the address into the "Address Location" window and hit enter.

AMP FONT VIEWER

The other day, I received an e-mail from a reader, asking if there was a program that would allow for a quick look at all of the fonts on their system, without having to open a big program such as MS Word. I started looking around and I happened upon a great free download that does just that! It's called **AMP Font Viewer** and it's very simple to install and use. Just install the program, open it and you'll be good to go! Here's what it looks like:



As you can see from the image above, all you need to do is click on the name of the font and it will show you what the font looks like. This little program now saves me a ton of time when I'm searching for new fonts! You can download the AMP Font Viewer right here:

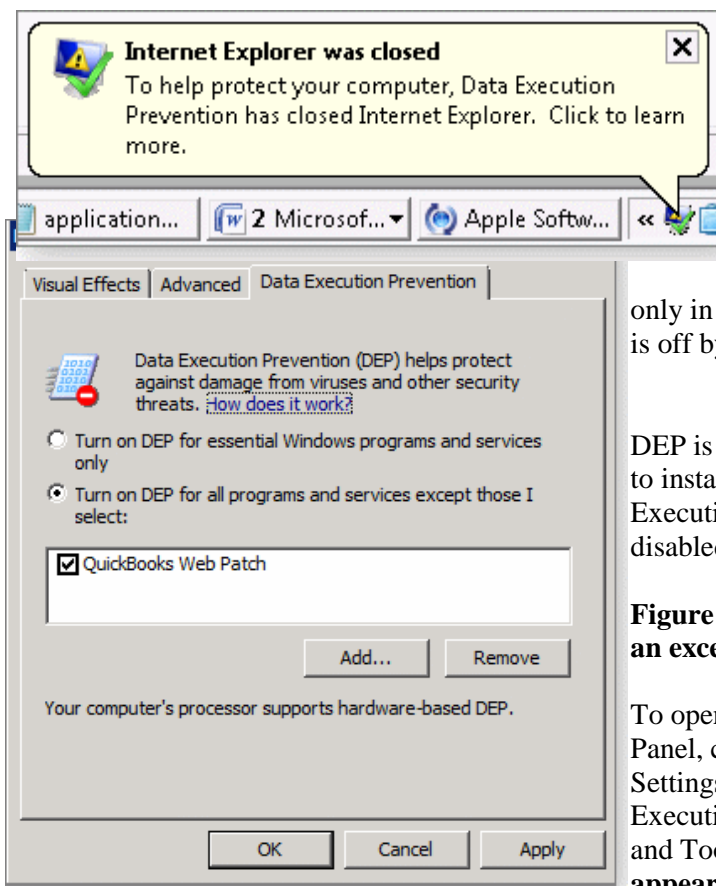
<http://www.ampsoft.net/utilities/FontViewer.php>

Simply click on the **Download** button at the top of the page and then click on the **Installer** button. Enjoy!

From: The Desk of Jim McGorry
Excerpts taken from the Windows Secrets Periodical

CONTROL ILL-BEHAVED APPS WITH DEP IN IE

Internet Explorer 8 includes a security feature that shuts down misbehaving applications before they can harm your system.



This capability, known as Data Execution Prevention (DEP), runs by default when IE 8 is installed on XP SP3 and Vista SP1 or later, but it may not always be clear to you why DEP has put the brakes on one of your PC's applications.

DEP is the best reason I know for updating to Internet Explorer 8 and Vista SP1. For many years, Microsoft has included DEP — which is also called No-Execute (NX) — only in parts of Windows. For example, DEP is available in IE 7 but is off by default to avoid conflicts with old, incompatible programs.

DEP is now a key part of Vista and Internet Explorer 8. When I try to install older software on newer machines, I must configure Data Execution Prevention to allow the software installer to run with DEP disabled. (See Figure 1.)

Figure 1. You can configure Data Execution Prevention to create an exception for an application.

To open the Data Execution Prevention dialog in XP, open Control Panel, choose System, and then select the Advanced tab. Click the Settings button in the Performance section and select the Data Execution Prevention tab. In Vista, choose Performance Information and Tools, click Advanced Tools in the left pane, select **Adjust the appearance and performance of Windows**, and click the Data Execution Prevention tab. For instance, when I install

QuickBooks 2007 on Windows Server 2008, I have to exclude under the DEP tab the QuickBooks updating tool in order to install it on the server.

Keep in mind that the only reason I'm doing so is because I trust Intuit, the publisher of QuickBooks. If I didn't change the settings, DEP would prevent me from installing an older version of this software on the newer system.

If I didn't already trust the vendor, I'd look for valid reasons why DEP was blocking the installation before I took the step of changing any DEP settings. In most instances, good, up-to-date software shouldn't need to be excluded from DEP.

DEP helps block malware in Internet Explorer

Since IE 7, Microsoft has used DEP to help thwart online attacks in the browser itself. What the company didn't do until IE 8, though, was to enable DEP by default. Prior to IE 8, DEP was disabled by default for compatibility reasons, as documented on the [IE blog](#). Many older IE add-ons were built using earlier versions of the Active Template Libraries (ATL). They aren't compatible with DEP, therefore, and crash when IE loads them.

When DEP is enabled and combined with Address Space Layout Randomization (ASLR), IE's ability to protect against Web-based attacks improves considerably. In a nutshell, ASLR is designed to make it harder for automatic attacks to occur. You can read more about ASLR in the [MSDN blog](#).

Specifically, ASLR helps prevent exploits both in IE *and* in any add-ons that are loaded. Even with the new security protections in IE 7 and 8, the browser is still targeted more often by malware authors than other browsers. This has caused security pundits to state, as Wired's Brian X. Chen does on the [Gadget Lab blog](#), that Apple's new Snow Leopard operating system is "less secure than Windows, but safer."

(If you use Snow Leopard, I encourage you to update your system to OS X version 10.6.1. This includes a patch for the insecure Adobe Flash Player that Snow Leopard shipped with, as documented in an Apple [security update](#).) There are many protections built into Internet Explorer 8 that may be considered just another annoying browser crash when seen in action. (See Figure 2.)

Figure 2. When DEP prevents bad code from executing in IE, it closes the browser and pops up an alert.

Unfortunately, it's not always obvious that IE is actually protecting you when in fact it is.

Find the source of DEP-related browser crashes

Some PC support sites, such as the [Tech Support Forum](#), recommend that you disable DEP to prevent it from closing IE whenever an unauthorized memory access is detected. However, once you understand why the browser is shutting down, it becomes clear why disabling DEP is a bad idea.

Generally, DEP errors in IE are due to an add-on, a hardware conflict, or a corrupted IE installation. If DEP continually shuts down IE on your system, find the cause of the failures instead of disabling DEP. For example, there are reports that stealthy toolbars from the Chinese search engine Baidu are the source of many DEP closures.

If DEP is closing IE 8 on a regular basis, first try opening the browser with all add-ons disabled. To do so, click Start, All Programs, Accessories, System Tools, Internet Explorer (No Add-ons).

If the DEP closures stop, this indicates that an add-on is causing the problem. Disable each add-on and then enable them one by one until the crashes return. At that time, you've found the culprit. To review the processes DEP has enabled by default, press Ctrl+Alt+Del and click Start Task Manager. Click the Processes tab, select View, and choose Select Columns. Scroll to the bottom of the resulting dialog box, check the Data Execution Prevention option, and click OK.

A new column appears in the Processes window that shows which processes on your PC are natively protected by DEP. The more processes for which DEP is enabled, the better your system is protected from buffer overflows and the other memory-related vulnerabilities DEP shields you from.

If you decide that you *must* disable DEP, you can easily do so in the 32-bit versions of IE 7 and IE 8. To find this setting in IE 7, click Tools, Internet Options, Advanced, and scroll to the Security section, as shown in Figure 3. (Press the Alt key if IE's standard menu isn't visible.)

In IE 8, first right-click the IE shortcut, select **Run as administrator**, and then enter the browser's Advanced options.

In both IE 7 and IE 8, uncheck **Enable memory protection to help mitigate online attacks** to disable DEP.

On 32-bit systems, DEP is enabled by the "Enable memory protection" option, which is fourth from the bottom in this screen shot.

The 64-bit version of IE 8 lacks a DEP option on the Advanced tab. The reason it's not visible in the 64-bit version of IE is that DEP is enabled automatically and can't be disabled. If you're running a 64-bit operating system, you probably want the protections that DEP gives you.

Weekly Download Section from Jim McGorry

Welcome members and visitors alike to this new section I hope it will be of interest and use to you. Each month I will try and have interesting and useful programs for you to download and try on your systems as you see fit. Some are free and some may have a nominal fee.

A brief write-up and link to download page will be displayed here so you can determine if you wish to get it and use it.

ALSO NOTE: Some web addresses may not be a direct link. If not, then just copy and paste the address into the "Address Location" window and hit enter.

DAEMON TOOLS

Have you ever purchased software on a CD, installed it on your computer and ran it, only to find that you have to keep the disk in for it to work right? I hate that!

Well, today I have found a free program that will solve that little problem forever! The program is called Daemon Tools and it allows you to create virtual drives so you never have to hunt down those pesky disks!

I love how easy this program is to use! After installing Daemon Tools, you can simply open the tools panel and choose "**disk imaging**". From there, point the program to your troublesome, required cd rom and have it start copying. Daemon Tools will create an exact image of the disk so you can use it whenever you want without having to actually insert the CD ever again!

Here's a quick shot of the toolbar. It sits above your start menu so it doesn't get in the way:



Daemon Tools will create up to 4 virtual drives at once, but you can swap images between them for truly unlimited virtual disks at your disposal. Instead of having to hunt down a disk, just click the "mount'n'drive manager" and select the disk you want to use. Its as simple as that! If you want to download daemon Tools, you can get it right here:

http://download.cnet.com/Daemon-Tools-Lite/3000-2646_4-10778842.html?tag=mncol

Enjoy!

From: The Desk of Jim McGorry

Excerpts taken from the Windows Secrets Periodical

PREVENT KEYLOGGERS FROM GRABBING YOUR PASSWORDS

Strong passwords are important, but even the best password won't keep you safe from keyloggers — hardware and software that's designed to secretly record your keystrokes.

Fortunately, there's a way you can enter sensitive data so it's extremely difficult for snoops to extract your passwords from keylogger files.

In her [Aug. 6](#) Top Story, WS contributing editor Becky Waring reported that Google's Gmail service allows hackers to try to guess your password 1,200 times per day. She provided some useful tips for making strong passwords that are easy to remember but hard to crack. The bad news? Even the strongest passwords can be recorded by keyloggers. These are software and hardware products designed to capture computer events and store them in a log file.

Keyloggers can have legitimate uses in business, or they can be perverted into collecting passwords for identity theft. For more information on how these products work, see my [Oct. 9, 2008](#) review of free software keyloggers.

Windows' On-Screen Keyboard app is also logged

If you're using a computer you aren't sure is keylogger-free, how do you protect any passwords to sensitive Web accounts you may need to access? A reader named K. recently submitted the following suggestion:

"I use a simple existing tool in Windows called **osk.exe** (On-Screen Keyboard).

This program, as you may know, resides in the **C:\WINDOWS\system32** directory, but there's no shortcut or link to it, so most people don't know it exists! You can launch it by entering **osk** in the Run command.

"Anytime I need to log in to any sensitive sites (banking, etc.), I launch **osk.exe** first and use this on-screen keyboard to click and enter my user name and password, even on my own home computer. This way, I feel confident that my credentials can never be captured."

K's suggestion may be useful to prevent some types of hardware keyloggers from detecting signals from the physical keyboard. Unfortunately, the program provides no defense against software keyloggers. Windows' On-Screen Keyboard sends information to applications as keystrokes, just as though you'd pressed the keys on a keyboard.

The first keylogger program I tested with the OSK workaround — All in One Keylogger from RelyTec — easily captured my keystrokes as I signed in to a Web site. (For more information about the All in One program, see the [vendor's site](#).)

Holes in anti-keylogging software protection

Another alternative that's often touted to protect your passwords is to use anti-keylogging software. The [Antispy Software](#) site lists several such products, but I can't vouch for them.

Anti-keylogging software — even if it were effective in its stated mission — wouldn't prevent your password from being intercepted by a hardware keylogger. The sad fact is, if a keylogger is deployed effectively, you can't detect whether a public or unsecured computer has a hardware or software keylogger — or any keylogger at all, for that matter.

The universal defense against password snoops

Your best defense is not to use any untrusted computer to sign in to any site that contains banking or sensitive personal information. When you simply *must* take a chance on using a random PC, however, you can minimize the risk — if not eliminate it.

Security blogger Ian Saxon publishes an approach that may not be 100% foolproof but should provide some reasonable protection when entering passwords. Writing on his [Defending the Kingdom](#) site, S. outlines what he calls the "revised Vesik method" for entering passwords:

Step 1. Click in the password box and type three random characters, mixing upper and lower case, numbers, etc.

Step 2. Use your mouse or the Shift and arrow keys to select the characters you just typed. Then type three more random characters or a portion of your password, replacing the characters you typed previously. (Mixing random characters with actual parts of the password makes it more difficult for keyloggers to identify your password.)

Step 3. Repeat steps 1 and 2 a few times. The more often you repeat the process, the harder it will be for an intruder to discern your password when examining the keylogger file.

Step 4. Click to the left or right of your password segment and follow steps 1 to 3 to add a few more characters.

Step 5. Repeat the process, adding a few more characters of your password on each cycle until your entire password is in the password box. Then sign in to the site.

This procedure clutters the keylogger's log file with a series of click events and characters. There's no easy way for the intruder to know which characters are your password and which are random.

The key is to select and gradually overtype gibberish characters with your actual password characters. Don't simply type some garbage, backspace over it, and then enter your real password. Most keyloggers compensate for backspacing but can't keep track of characters you select and overtype.

As S. points out, this method isn't foolproof. For example, if you use an untrusted PC to sign in to the same site twice — and you don't use identical gibberish each time — a hacker could compare the two captured keystroke sequences and possibly figure out which characters constitute your actual password.

However, most crooks are looking for "low-hanging fruit." They'll move on to another victim rather than spend a lot of time trying to filter your password out of the noise.

Of course, if we all used the Vesik method to obscure our passwords, hackers might develop keyloggers that track this kind of data entry, too. But most people don't conceal their passwords in noise, so keyloggers don't compensate for it.

If you have no choice but to sign in to a site on a PC you aren't sure of, protecting your password is a difficult problem with no perfect solution. Many software programs, such as RoboForm2Go, offer password-protection schemes that vary from the no-cost Vesik technique. WS senior editor Gizmo Richards recently reviewed these methods in an [analysis](#) at his Tech Support Alert site. Just be aware that accessing the Internet using your own laptop — on which you run up-to-date antivirus software — protects your passwords better than using a public Internet terminal or a friend's PC.

From: The Desk of Jim McGorry
Excerpts taken from the Windows Secrets Periodical

SOME KEYLOGGERS CAN READ THE CLIPBOARD, TOO

Several dozen readers responded to WS contributing editor Scott Dunn's [Sept. 10 Top Story](#) on keeping your passwords out of the hands of sneaky keyloggers on untrusted PCs you may be forced to use while traveling.

The most frequent suggestion was to copy passwords from a text file and paste them into password boxes, but many keyloggers — unfortunately — capture any text you paste from the Clipboard. Crooks with computers are experts at raiding online bank accounts and making a profit from personal information. Every time you think you've outsmarted them with a new defense, hackers find a way around or through it.

Scott described the "revised Vesik method," which involves typing nonsense characters and mousing them into place to form a real password. It's admittedly a convoluted way to hide data from keyloggers when you need to sign in to a Web site using a PC that might be infected. Scott acknowledged that the trick is time-consuming and prone to error.

Many readers recommended other programs and techniques to thwart either hardware or software keyloggers. C. M. points out the advantages of authentication techniques used by banks in Europe:

"I don't know the position in the U.S., but here in Europe, sensitive Web sites such as [those for] Internet banking are usually configured to defeat keyloggers.

"The best way is for the bank to supply a token — similar in concept to the SecurID or Vasco two-factor authentication systems that readers working in IT departments may be familiar with — that requires you to insert a bankcard and enter your usual PIN number before it generates a unique key that will allow logon.

"Even if this is read by a keylogger, it won't work for any subsequent logon attempts. The drawback is obviously that you need to carry it with you and be able to attach it (via USB) to any public computer you want to use.

"Alternatively, banks require you to select a long password — say, 12 characters— and then ask at logon for a random subset: e.g., 'Please enter the 8th, 3rd, and 10th character of your password.'

"For further protection, these characters may be selected by using drop-down menus, which should defeat most keyloggers.

"The drawback is a slight weakening against brute-force guessing — you have a chance of guessing correctly if you can make many tens of thousands of attempts— but there are strong limitations on the number of incorrect logon attempts that are allowed before the account is locked (typically three), requiring a phone call to reset the procedure.

"Simpler still is for the bank to issue a 'one-time pad' of randomly generated passwords that you use once and then discard. Obviously, a written pad can be lost, but as long as you don't keep it with other identifying information — e.g., your account number — this should not be a problem.

"I think one of the reasons for the different systems in Europe is that here the onus is on the banks to provide security. If your bank account or credit card is 'hacked,' any resultant loss is the responsibility of the bank, unless they can demonstrate collusion on the account holder's part. I understand this doesn't apply in the U.S."

Some keylogger software can, in fact, record the choices in drop-down menus. And there are reports of man-in-the-middle attacks that exploit one-time passwords only momentarily, as explained in a [blog item](#) by the Washington Post's Brian Krebs. But it's clear that European banks, due to tighter regulation, are ahead of American financial institutions in security practices that defeat run-of-the-mill keyloggers. In the U.S., the Electronic Funds Transfer Act limits consumer liability when someone is the victim of an online theft. There remains little uniformity, however, in online banking. Scott will discuss additional password-management utilities and techniques in a follow-up article about keyloggers on Sept. 24. Stay tuned!

From: The Desk of Jim McGorry
Excerpts taken from the Windows Secrets Periodical

MORE TRICKS TO EVADE KEYLOGGERS ON PUBLIC PCS

Dozens of readers responded to my [Sept. 10 Top Story](#), many of them proposing alternative ways to evade keyloggers other than the "revised Vesik method" I described.

No method can make you completely safe when using a public computer, so you must balance convenience with the level of risk that's acceptable to you.

The Clipboard's no safer than the keyboard

The revised Vesik method involves typing nonsense characters into a password input box when using a public PC and then rearranging some of the letters to form your actual password with the mouse. If the PC contains a hardware keylogger or is infected with a software keylogger, rearranging a password in this way will usually suffice to obscure your credentials. Most hackers will concentrate on the 99% of users who type in their passwords at Internet cafés in the usual way. One proposal sent in by many, many, *many* readers was a variation on a single theme. Namely, keep your sign-in information on a USB flash drive or memory stick, then copy and paste the info into the appropriate fields when you're required to use a public PC or other unsecured computer.

Unfortunately, many keyloggers capture any information you place into the Windows Clipboard. I tested the copy-and-paste technique using the All In One Keylogger from RelyTec. For more info, see the [vendor's site](#). The program easily captured the sign-in IDs and passwords entered, whether I used the standard menu options (Edit, Copy and Edit, Paste) or the keyboard shortcuts Ctrl+C and Ctrl+V.

In my tests, the All In One Keylogger wasn't able to capture the information when I performed a copy-paste operation using a context (right-click) menu. But that's not much to rest one's hopes on. Other keyloggers do succeed at capturing data copied via context-menu options.

Note that many password-manager products require you to copy and paste your passwords from their database to an input box. (See my [Sept. 18, 2008](#), review of password managers.) Any product using the Clipboard in this manner is vulnerable to a keylogger that captures data from the Clipboard.

Other strategies for blocking keyloggers

Readers suggested various ways of carrying one's passwords on a flash drive. J. H. asked, for example:

"What about surfing from suspect PCs using only Firefox Portable running off a USB drive, with all your passwords stored in the browser?"

If you store passwords in a portable version of Firefox, make sure you set a "master password" first. This encrypts your passwords so they're not readable on the USB device for any malware to scan. To establish a master password in Firefox, pull down the Tools menu, click Options, select the Security tab, and turn on

Use a master password.

After doing this, you must enter your master password once per browser session. Another reader, Val Ingraham, proposed signing in using a tool such as the portable version of Siber Systems' free RoboForm password manager, available on the company's [download page](#).

Both of these approaches were able to evade the keylogger I tested them with and would likely confound other keyloggers as well. However, any method that permits automatic sign-in from a flash drive poses a risk of physical security. A flash drive is easy to lose. When you misplace one, you could be handing over your passwords to whoever finds the device — if you don't enable a master password.

Can freeware provide the privacy you need?

Several readers like products that are specifically designed to defeat keyloggers. Simon Bleasdale recommends Neo's SafeKeys 2008, available for free on the [Alpin Software site](#). The program promises the same functionality as the Windows On-Screen Keyboard (OSK) utility described in the original tip — but without OSK's security risks. (OSK sends keystrokes in a way that keyloggers can see and record. To use OSK if you need it for entering something other than a password, open the software by clicking Start, All Programs, Accessories, Accessibility, On-Screen Keyboard.)

Neo's SafeKeys 2008 displays a small window with a simulated keyboard on which you can type your sign-in, password, and other information — just as with OSK. But unlike the Microsoft utility, Neo's SafeKeys 2008 doesn't transmit information in a way that can be picked up by keyloggers. Nor does the program use the Clipboard. Instead, you type your info in the SafeKeys 2008 window and then drag the data to the appropriate text box in your browser.

Neo's SafeKeys 2008 successfully evaded the All In One Keylogger product in my tests. Other options help you foil keyloggers that regularly take screen captures to record your PC activities. According to the Alpin Software site, however, the utility's drag-and-drop methods don't work with all products — including the Opera browser. No product will ever be able to guarantee your safety from snoops when you use a public computer. Fortunately, the techniques and products described here and in the previous article can reduce your risk substantially.

You're the only person, however, who can decide what constitutes an acceptable risk level for your data. That may mean never signing in to Web sites using PCs at Internet cafés — or wherever you're not sure adequate security precautions have been taken.

Weekly Download Section from Jim McGorry

Welcome members and visitors alike to this new section I hope it will be of interest and use to you. Each month I will try and have interesting and useful programs for you to download and try on your systems as you see fit.

Some are free and some may have a nominal fee.

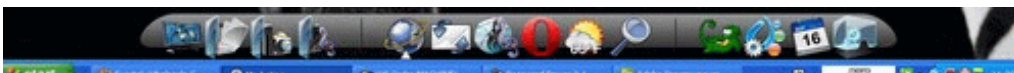
A brief write-up and link to download page will be displayed here so you can determine if you wish to get it and use it.

ALSO NOTE: Some web addresses may not be a direct link. If not, then just copy and paste the address into the "Address Location" window and hit enter.

OBJECT DOCK

I'm sure that many of you use the quick launch bar that comes with windows. It's the little part of your task bar that you can use to launch programs that you use all of the time and it definately comes in handy. For me, the quick launch bar is just too small. As a matter of fact, I would like it if my quick launch had larger icons and stretched across my entire screen! Just think about it for a second... If you could have a bar that had all of the main programs, folders and utilities you use, you wouldn't need to clutter up your desktop and there would be less need to hunt around in the start menu, right?

Well, Today's free download has all of those features and more. Today's program is called **Object Dock** and it will allow you to do everything I described above, plus a couple extra goodies. My favorite "extra" is the weather feature. It tells me the weather in an easy to read format right on my object dock. Here is what it looks like:



As you can see, it automatically adds dock items like "my documents", "my computer", "date", "weather" and "internet". If you want to add something else, just drag it on and you are set. I love this program! If you want to check out Object Dock, you can get it by clicking here:

http://download.cnet.com/ObjectDock/3000-2072_4-10210264.html?tag=mncol
Enjoy!

Weekly Download Section from Jim McGorry

Welcome members and visitors alike to this new section I hope it will be of interest and use to you. Each month I will try and have interesting and useful programs for you to download and try on your systems as you see fit. Some are free and some may have a nominal fee.

A brief write-up and link to download page will be displayed here so you can determine if you wish to get it and use it.

ALSO NOTE: Some web addresses may not be a direct link. If not, then just copy and paste the address into the "Address Location" window and hit enter.

OPERA 10

It seems that the more advanced the Internet gets, the longer it takes for pages to load in your browser. Whether you use Internet Explorer, Firefox or Safari, if your connection isn't performing at it's peak, the time it takes to load your favorite web pages can take forever.

Well, it seems that a browser company has finally thought about that problem and has come up with a solution. The Opera Software Company just released their newest browser, Opera 10, a few days ago. For those of you that have never heard of Opera, I'll explain a little bit. You see, Opera is just another browser like Internet Explorer or Firefox. It pulls up the same internet web pages and even looks similar to other browsers. It is just made by a different company and uses different technologies that the others don't. Here is a shot of what opera looks like:



Looks familiar, right?

This new version of Opera comes with some new technology that they call "Opera 10 with Turbo". According to Opera, Turbo technology "keeps Web pages loading lightning fast, even if your connection slows down". Doesn't that sound awesome?

I downloaded and installed Opera 10 with Turbo. It was a quick and painless download with a simple install. I cruised around with it a bit and honestly, I'm impressed with its speed.

The best thing about Opera 10 is that, you guessed it, it's free! So, if you want to give it a shot, you can download it here:

<http://www.opera.com/>

Enjoy!