

If you connect to the Internet via DSL or cable modem, your high-speed connection makes a tempting target for hackers as you are "on line" at all times. For this reason you should have a good firewall program installed. Personal firewalls protect your computer system from external attack and provide warning of nefarious activity. A computer using a national broadband provider receives an amazing number of scans on a daily basis. Once you install a personal firewall, you can see what kind of scans your system gets. Even if you run a personal firewall, never share your drive or folders with other users on the Internet.

Firewall programs can be gotten from McAfee, Norton, and Symantec to name a few. Most newer computers come with some type of firewall software already included.

Gone Wireless?

If you are a user of the new wireless Internet connection, your neighbors several houses away may be able to see what you are doing on your computer. Encryption programs can keep hackers out. They come with your wireless unit, so take an extra 5 minutes to load the program and use it.

If you access wireless service in a café or outside, keep in mind that the people around you may be able to access your computer as well, so refrain from doing any banking, paying bills, etc. — anything that requires your password or personal information — when using a public wireless service.

If you have a home network there are a few simple things you can do to reduce the likelihood that someone will snoop your data: 1. **Don't call attention to yourself.** Turn off the broadcast SSID function. 2. **Change your name.** Don't make your network name obvious; change the default name and then change it every few months. 3. **Scramble your data.** Use an encryption tool (i.e. WEP - Wired Equivalent Privacy). 4. **Telecommute through a tunnel.** Use a

Virtual Private Network (VPN) which creates a "tunnel" between your laptop and your office only. The tunnel is fortified with better encryption than WEP. All versions of Windows XP include the desktop software required to connect a VPN.

Other suggestions

- Don't store credit card information or online bank account information on your computer.
- Install and use Anti-virus and firewall software.
- Set your anti-virus software to scan for phishing web sites.
- Turn off file-sharing.
- Scan for spyware and adware with software such as "Spybot Search & Destroy" and/or "AdAware" which can be downloaded for free from the Internet.
- Change passwords frequently, using upper and lower case letters, numbers and special characters (punctuation, etc.).



**SNOOP
PROOF**

Your Computer



Mesa Police Department
Crime Prevention
(480) 644-2300
www.mesaaz.gov/police

Your PC is ready and willing to reveal what you've been up to. Give nosy types just a few hours to dig around, and they can unearth plenty: incoming and outgoing mail you've deleted, Internet sites you've visited, search criteria and data you've entered on web forms, even phrases you've included in a document (then thought better of and deleted). Fortunately, you can protect yourself with a few tricks. Here's how to keep your personal PC information hidden.



Recycle

Get rid of files you think you've already nixed from your system. We're talking about all the trash you banished to your Recycle Bin. Sure, you can empty it out whenever you remember, but a better way is to turn off the Recycle Bin. To truly delete your files the first time around, right click on the Recycle Bin and choose Properties, then Global. Check the box called "Do not move files to the Recycle Bin. Remove files immediately on delete."

Clean up and lock down

Even if snoops can't view your documents directly, they can get an idea of what you've been doing by scanning your list of recently used files in the Microsoft Word or Excel File menu. This temporary menu lists even files you've recently deleted, so it's best to turn off the option. In Word or Excel, select Tools>Options, then General. Uncheck the box labeled Recently Used File List. In Word 2007, select the Office Button, Word Options, then Advance. Set "Show this number of recent documents" to "0."

Next, cover the tracks of your current documents. Pop up the Start menu and select Documents. It shows a list of the last 15 or so files you had open, making it too easy for someone to browse through your work or personal files without even searching your hard drive.

To hide your work, clear the menu by clicking going to Control Panel>Task Bar and Start Menu. Then click on the Start Menu tab, click Customize, and then click the Clear or Clear List button.

Now it's time to clean out your temp files. All applications usually save temporary copies of your work in progress to guard against system crashes. Many also save text you've deleted, moved, or copied, even if you haven't saved the file you're working on. Get rid of those bits by routinely deleting the temporary files that each application saves in the TEMP folder. Also, be sure to delete all files within its subdirectories, such as those labeled FAX and WORDXX. Many of the files have extensions such as TMP, but they are actually complete versions of DOCX, HTML, or even image files.

Passwords protect

Newer computers usually provide some basic security. You can make your computer completely inaccessible while you're away from it by setting a password for your computer access and to exit from your screensaver.

When your screen saver runs, only someone who knows the password will be able to reactivate the computer.

Check with your individual computer manual for instructions on how to set passwords.

You can also add password protection to specific files, such as a Word document. With the program, click Save As and then select the Options button to set the password option for each file.

The best passwords aren't real words or dates. Use a combination of letters, numbers, and punctuation for a password that's hard to guess. You'll have to type your password each time you open and save the document.

Search Engines & Browsers

Search engines (Google, Yahoo, Bing, Ask, etc.) record your search data; your search terms, the time of your visit, the links you choose, your IP address and your User ID cookies, which all get stored in a database. Identity profiles can be constructed from this information, which is a goldmine for marketers and other shady characters. Ixquick is one search engine that does not record your IP address and deletes users' privacy data within 48 hours. There are many free downloads to help you surf undetected. Simply do a search on "surf web undetected" to find them. Make sure you are downloading from a reputable site.

Your browser (Netscape, Explorer, Firefox, AOL) is the next area to safe-guard. Most browsers also keep lists of all the places you've been, including the specific pages you've visited, searches you've done, and data you've entered.

With most browsers, if you go to Tools and then Options, there are Privacy and/or Security tabs. Check both out and set them to delete cookies, your browsing history, passwords, etc. when you exit the browser.

You should also clean out your cache. Browsers keep caches of recently visited web pages on your hard drive. This speeds up web access when you revisit the pages, but it also leaves you open to snoops. You can set your security/privacy settings to delete your cache when you exit the browser as well.

