Computer Safety

You may diligently lock your car, the doors/windows of your home, and even keep your personal papers in very secure place, **but an identity thief** won't need to set a foot in your house to steal your key personal information if you're lax with your personal computer security. SSN #, birthdays, financial account information, tax records and more may be stored in your computer which is a veritable treasure-chest to an identity thief.

These computer-security tips can help you keep your computer(s) (and any personal information on it) safe:

Update your virus protection software regularly, or when a new virus alert is announced. With more than 500 new computer viruses discovered each month, it's **critical** that you keep your anti-virus software up-to-date.

- Computer viruses can have a variety of damaging effects, including introducing program code that causes your computer to send out files or other stored information.
- Also, be on the alert for security repairs and patches that you can download from your operating system's (OS) website. Some anti-virus software *(and updates)* won't function properly without also having the latest OS updates installed.

Keep your Operating System *(OS)* **software updated.**
There's a constant, ongoing security-battle between hackers and OS vendors.

- Every time a new exploit/vulnerability is discovered, your system OS vendor makes a "patch" available to fix the potential security hole. To do YOU any good, you need to know about these patches, and install them as soon as they are available.
- The most recent versions of both the Microsoft and Apple operating systems have an "automatic update" feature for their security upgrades. Make sure your system is set to auto-update security upgrades, or you will need to make a special effort to take time, frequently, and manually check the OS websites for the availability of new security patches.

Run anti-virus software (and install OS updates) on all your computers —even those you don't use to surf/access the Internet.

- Even computers on a home/office network that aren't ever used to access the Internet can become infected with some types of computer "viruses". Computer "worms" can move/multiply across network "shares" of write-enabled, shared directories that contain executables or crucial system documents. Avoid write-enabling any directory that contains anything but your user documents.

Install, keep up-to-date, and run spy ware monitoring software. You might be surprised how many people what to know about you and what you do on your computer, and use legal or illegal means to get that information.

Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.

Use a firewall program, especially if you're using a high-speed Internet connection like satellite, cable-modem, DSL, or T1, which leaves your computer connected to the Internet 24 hours a day. A firewall program will allow you to stop hackers/thieves from accessing your computer. Without it, hackers can take over your computer and steal all of your key personal information stored on it. For even better protection, consider complementing your firewall software by installing a **hardware** firewall.

Be aware of Internet Scams such as Fraudulent Ebay, Pay Pal, or Nigerian Money Scam.

If you have any questions call the Community Services unit of the KU Public Safety Office at 864-5900, email us at kupso@ku.edu or visit our home page at: http://publicsafety.ku.edu/

The annual security report about KU safety policies, crime statistics, and campus resources is available online at www.ku.edu/safety, or on paper by contacting the Office of the Vice Provost for Student Affairs, 133 Strong Hall, (785) 864-4060.

KU prohibits discrimination and harassment. Report discrimination and harassment to the Office of Institutional Opportunity and Access at IOA@ku.edu or (785) 864-6414, 711 TTY

THE UNIVERSITY OF KU KANSAS
Office of Public Safety

Revised 04/14