Keeping Your Computer Safe

In order to keep your computer as safe as possible, you should consider using anti-virus software and a firewall. Anti-virus software is used to scan incoming e-mails and files. You can download anti-virus software from Internet websites of software companies, or you can buy it from a retail store. When selecting anti-virus software, make sure it recognizes both current and old viruses, will effectively reverse any damage caused by any found virus, and receives updates automatically. If your anti-virus software does not automatically update, you will need to run updates at least once a week. If your software has an expiration date, you will need to remember to download new software when your existing software expires.

Firewalls are used to prevent hackers from hacking into your computer, accessing your personal information, and sharing it with others. The purpose of a firewall is to safeguard your system from outside attempts to access your system, and to block communications to and from websites you don't permit. Some PC's come with a firewall installed, but may be shipped in the "off" mode. You will need to turn the firewall on when setting up your computer. Your online "Help" instructions can assist with this set up. If your computer doesn't come with a firewall, you will need to get separate firewall software. There are several free firewall software programs available online. Another option is to install a hardware firewall, an external device including firewall software. No matter which firewall you select, be sure it is set up correctly and keep it updated regularly.

If you do not have up-to-date anti-virus protection and a firewall, spammers could install software on your computer, allowing them to send e-mails via your computer to thousands of other computer users. Those e-mails look like they are coming from you. If this should happen, you may receive a great number of complaints from those receiving the e-mails, and because of this, your Internet Service Provider may close your e-mail account. The name given to these spammers are "zombie drones".

Protecting Your Web Browser

Computer hackers can also take advantage of your web browser(Internet Explorer, or Netscape) and also operating systems, such as Windows or Linux. You can help minimize this risk by taking advantage of the built-in security features on your PC. Check your "Tools" or "Options" menus for these features. For further help understanding how to use these features, use your "Help" function.

Your operating system may offer free software "patches" to close holes in the system hackers could exploit. Some systems can be set to automatically update and install these patches for you. If your system is not capable of this, you will need to visit your PC's manufacturing website and update your system on a regular basis.

If you do not use your PC for an extended period of time, it is a good idea, to turn off the computer, or unplug it from the phone or cable line. If the computer is not on, it cannot send or retrieve data over the Internet, and is less likely to be hacked.

Password Protection

Protect yourself and your information by keeping your passwords in a secure place. Never give your password information to anyone for any reason. Your Internet Service Provider should never ask you for your password, nor should anyone else for that matter. If your computer system asks to remember your password, at any given time, please tell it no. Change your password , regularly, at least every 90 days. When choosing a passcode, use at least 8 characters, including numbers and symbols. Avoid using everyday words. Some hackers have been known to use programs capable of trying every word in the dictionary. Personal information should not be used when selecting a password. You should not use the same password for all your online accounts. In order to create a strong password, it is suggested you use a song title, or a phrase you like. Take the first letter of each word in the song title or the phrase and use those letters to create a password. Whenever, possible replace the letter with a character or a number. Here is an example: Four Score and Seven Years Ago could be **4S&7yrsAGO**.

By following the steps mentioned above, you can create a safer and secure environment on your PC. Unfortunately, no system is completely secure. If your computer should fall victim to hacking, immediately verify that your Anti-Virus software, your anti-spyware, and your firewall are all updated. Run each one of these programs to scan for any viruses, spyware, malware, or signs of intrusion on your computer. Unplug the phone or cable line to your PC, and immediately contact your Internet Service Provider. It would be beneficial to the ISP if you would include your firewall log information regarding the incident. This will help the ISP prevent similar problems of this nature in the future.

You should also visit the FBI website, www.ic3.gov and file a complaint. They need to be made aware of the problem, in order to prevent such occurrences in the future, and to fight these types of computer hackers.

We hope this information will be beneficial to each of you and helps you understand the importance of being safe online. For more details about the information contained in this pamphlet, ask for the booklet titled "OnGuard Online" inside any of our bank lobbies or you can visit
http://onguardonline.gov/index.html
Remember: "**STOP-THINK-CLICK!**"

Next month look for a brochure on Skimming and the Nigerian Advance Fee Fraud scam.

Bank of New Madrid

A REAL COMMUNITY BANK

Phishing/ Pharming

Bank of New Madrid

Mailing Address & Telephone Numbers
PO Box 10, New Madrid, MO 63869
573-748-5551
PO Box 607, Lilbourn, MO 63862
573-688-2111
PO Box 325, Portageville, MO 63873
573-379-5551

www.bankofnewmadrid.com

MEMBER FDIC

PHISHING attacks use "spoofed"(hoax) e-mails and fraudulent websites to divulge personal financial data such as credit card numbers, checking/savings account numbers, account usernames and passwords, social security numbers and other personal information from consumers.

If you get an e-mail or pop-up message asking for personal or financial information, do not reply and do not click on any link that may be in the message. Legitimate organizations do not send out e-mails to their customers requesting personal information they normally have on file for that customer. If you are concerned about an e-mail you have received from an organization you do business with, call the organization via a telephone number you know to be a valid number or open a separate browser and type in the organization's web address as you know it. Do not ever copy and paste a website address received from a possible spoof e-mail into your Internet browser. It may look like you are going to the correct site, but in reality you are going to a different site with the sole-purpose being to fraudulently obtain your personal information. Some phishing e-mails can cause damage to your computer or may even track the sites and the activities you perform on the computer, and can do this without your knowledge.

DO NOT E-MAIL your personal or financial information, as regular e-mail channels are not secure enough to transmit your personal information. If you are on a site and you need to enter your personal information in order to complete a transaction on the site, check for the " lock icon" on the status bar, (see picture below). This lock signifies the site you are on uses encryption to protect your personal information, such as your account number, credit card number, Social Security number and other payment information. If the lock is closed, the site uses encryption. You can double-click on the lock to display the certificate for the site. Check the **Issued to.** The name should match the site you are on. If it does not, you may be on a "spoofed" site.

You can also check to be sure the URL address you are using begins with https. The "s" indicates the site is secure. Anytime you are on a site and the lock is in the locked position, the URL address should always start with https. Unfortunately, no indicator is foolproof as some scammers have forged security icons. You should also read website privacy policies. The policies should tell you what information is being collected from you, how it is being used, and if it is shared with third party sites. If you do not see a privacy policy on the site you are viewing, or you do not understand their policy, it would be in your best interest to not use the site.

PHARMING uses the same kind of "spoofed" sites as "phishing", but uses malware/spyware to redirect users from the real websites to fraudulent sites. Pharming involves the use of Trojan programs, worms and other type viruses to attack your Internet browser address bar. Pharming is much more sophisticated than "phishing", as when a customer types in a valid URL address, they are redirected to a fraudulent site instead of the intended website.

In order to prevent malicious software from getting into your PC, you should be aware of the different types of malware that are out there.

Adware: Software displaying advertising windows on your screen, either as pop-up ads on top of your active windows, or underneath your active windows.

Dialer: An application secretly using your modem to call 900 numbers or to make other international phone calls.

Keylogger: A program recording every button you push on your keyboard.

Spam: Unsolicited commercial e-mails from companies you've never dealt with before.

Spyware: Software created to retrieve your own personal information from your PC, and share with other third-party websites.

Tracing Cookie: Spyware records websites you visit and shares with other third-party websites.

Trojan program: A program masquerading as a legitimate program your firewall will allow to upload and download data, however it neither replicates nor copies itself. The program stays in your computer doing damage in the process, or it allows someone from a remote site to take over your computer.

Worm: A self-contained program, or it can be a set of programs, that are able to spread copies of itself to other computer systems. This usually takes place through e-mail attachments or through network connections.

Virus: A program or code attaching itself to a legitimate, executable program, and then reproduces itself when the program is ran. This usually takes place through e-mail attachments or IM attachments, like a screensaver or a Word document in the DOC format.

If you happen to receive an e-mail that appears to be "phishing" or "pharming" for information, forward the e-mail to spam@uce.gov, and to the company being impersonated by the e-mail. You can find other information to help avoid e-mail scams and deal with deceptive spam at ftc.gov/spam.

File Sharing
Every day, millions of computer users share files online. Although file sharing can give us access to an extreme amount of information, including games, music, and software, it also has a number of risks. If you do not have the proper settings on your computer, you could be sharing your own personal information with others. You may also be downloading questionable material labeled as something else, or material protected by copyright laws, which means you could be breaking the law. If you use file sharing software, make sure it is configured correctly and read all software agreements to be sure you understand the side effects of any free downloads.

Some side effects from free downloads, such as spyware, affects your ability to use your computer, sometimes by monitoring or controlling how you use it. Some anti-virus software allows the capability to activate anti-spyware. If yours does not, it would be a good idea to install a separate anti-spyware software, and run it regularly to scan and delete any spyware programs found on your computer.

Another side effect of file sharing can be virus-laden e-mails. The e-mail itself is not harmful until you actually open it. However, a hacker (person who uses the Internet to access computers without permission) will often lie to get you to open an e-mail. The e-mail in question may appear to come from a friend or a known acquaintance, or may have a file name like "Fwd: FUNNY or "Per your request!". Some even promise to clean a virus from your computer if you open it or follow a link. Do not open an e-mail attachment unless you are expecting it or know what it contains. When you send e-mails with attachments, include a message in the text of the e-mail informing others of the contents of the attachment.

Remember to always save your important files to a disc and store them in a safe place.