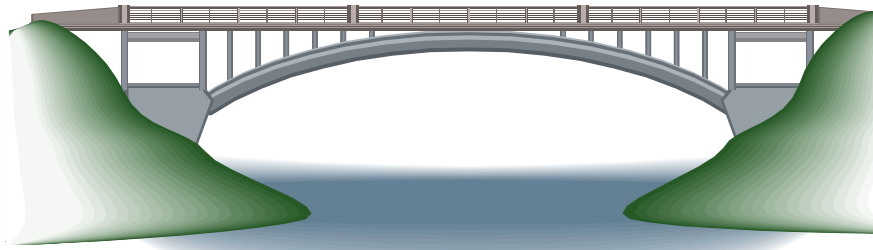


MHASI Matters



“Building Bridges Between Mental Health and Aging”

Fall 2009

Somebody out there wants to be exactly like you

Practices for Safer Computing

Being on guard online helps you protect your information, your computer, even yourself. To be safer and more secure online, adopt these seven practices.

1. **Protect your personal information.** *It's valuable.* To minimize your risk of identity theft, don't share your personal information unless you know how it will be used and protected. Don't reply to or click on links in any email asking for your personal information.
2. **Know who you're dealing with.** When shopping online, look for a seller's physical address and a working telephone number. Before downloading free software, read the fine print—some downloads come with spyware.
3. **Use anti-virus and anti-spyware software, as well as a firewall.** Update them all regularly; many update automatically. Look for anti-virus software that removes or quarantines viruses, and for anti-spyware software that can undo changes spyware makes to your system. Make sure your firewall is on and set up properly.
4. **Be sure to set up your operating system and Web browser software properly, and update them regularly.** Select security settings high enough to reduce your risk of being hacked. Make sure to regularly update your system with the latest patches.
5. **Protect your passwords.** Keep your passwords in a secure place, and don't share them on the Internet, over email, or on the phone.
6. **Back up important files.** If you have important files stored on your computer, copy them onto a removable disc, and store it in a safe place.
7. **Learn who to contact if something goes wrong online.** Visit OnGuardOnline.gov and click on “File a Complaint” to learn how to respond if problems occur when you're online.

OnGuardOnline, Your Safety Net

Credit Card Fraud Steps to Protect Yourself

- Photocopy both sides of each license, credit card, and important document in your wallet.
- Keep the photocopy in a safe place
- If credit card fraud happens to you, cancel your credit cards immediately.
- File a police report in the jurisdiction where the theft occurred immediately.
- Notify three credit reporting organizations.

Numbers of National Credit Reporting Organizations

Equifax	800-525-6285
Experian	888-397-3742
Trans Union	800-680-7289
Social Security Administration Fraud Line	800-269-0271

Clues that Spyware is on a Computer

- A barrage of pop-up ads
- A hijacked browser—that is, a browser that takes you to sites other than those you type into the address box
- A sudden or repeated change in your computer's internet home page
- New and unexpected toolbars
- Unexpected icons on the system tray at the bottom of your computer screen
- Keys that don't work
- Random error messages
- Sluggish or downright slow performance when opening programs or saving files.

Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to the theft of your personal information.

What You Can Do to Limit Vulnerability

- Update your operating system and Web browser software. Your operating system may offer free software "patches" to close holes in the system that spyware could exploit. Make sure to set your browser security high enough to detect unauthorized downloads.
- Download free software only from sites you know and trust. It can be appealing to download free software like games, file-sharing programs, customized toolbars, or other programs that may change or customize the functioning of your computer. Be aware, however, that many free software applications bundle other software, including spyware.
- If you're not using your computer for an extended period, disconnect it from the Internet. When it's disconnected, the computer doesn't send or receive information from the Internet and isn't vulnerable to hackers.
- Passwords—use passwords that have at least 8 characters and include numbers or symbols. The longer the password, the tougher it is to crack. Avoid common words—hackers can try every word in the dictionary.
- Change your passwords regularly—every 90 days. Don't use the same password for each online account. Don't use personal information, login name, or adjacent keys on the keyboard. Convert letters into numbers that resemble letters.

Keep your passwords in a secure place, and out of plain view. Don't share your passwords on the Internet, over email, or on the phone. Your Internet Service Provider (ISP) should never ask for your password.

FRAUD

Recognize It. Report It. Stop It.

Scammers don't care about your age, race, income, or geographic location. They just want your money. They use professional marketing materials and well-crafted and researched telephone scripts, which are traded among criminals. They will use a friendly tone and a "generous" offer to put you at ease. They give believable answers to your tough questions. They have an ability to impersonate legitimate businesses, charities, and causes. They expertly will use your own emotions against you. They are professional **CRIMINALS**: They know what they're doing and they do it well.

Don't fall for the **BIG PRIZE SCAM**. A caller or internet ad says you won a big lottery prize but you must send money before you collect. It is fraud and you will lose your money! Legitimate lottery and sweepstakes administrators never charge fees to deliver your prize. If you send money, you will never get it back.

Automatically entered into a **FOREIGN LOTTERY**?—you've automatically won, but you must send fees to cover taxes and handling. The fact is most legitimate lotteries do not call winners. It's a **SCAM**. You will not get your money back, once it goes out of the country.

A caller offers a **low-interest credit card** but you must send money before the card can be activated. It is a **FRAUD**, you will lose your money. **Pre-qualified never means pre-pay** to get a low-interest loan or credit card or to repair your bad credit even though banks have turned you down. They want you to provide your Social Security Number, driver's license number, bank account numbers **AND** a processing fee of several hundred dollars.

An employment advertisement offers a **work-at-home opportunity**, multi-level marketing plan or other way to "be your own boss," increase your income. The fact is sending fees for job guarantees is risky. In many cases, scammers advertise all kinds of job opportunities from envelope stuffing to craft assembly, and all too often, the ads make promises they can't keep. You will be losing more money instead of making more money.

Contact the FTC at ftc.gov or 1-877-FTC-HELP

Federal Trade Commission and Competition Bureau Canada

Questions or Comments? Contact the Gero-Psych Specialist in your area.

Heartland Human Services (Green)

Contact Person: Linda Warner, EdM, QMHP
P.O. Box 1047, 1200 N. Fourth St.
Effingham, IL 62401
217.347.7179 x 1046
Email: lwarner@heartlandhs.org
Website: www.heartlandhs.org

Southeastern Illinois Counseling Centers, Inc. (Blue)

Contact Person: Juanita Suro, MA, LCPC
P.O. Drawer M, 504 Micah Drive
Olney, IL 62450
618.395.4309 x 230
Email: jjuro@msn.com
Website: www.seicc.org

The H Group (Peach)

Contact Person: Lynn Tadda, LCSW
902 West Main Street
West Frankfort, IL 62896
618.937.6483 x7504
Email: lynn.tadda@Hgroup.org

