

# Money for Life

May 2006

Dear Readers,

Thanks to the Internet, you can order books, clothes, or appliances online; reserve a hotel room; download music and games; check your bank balance 24 hours a day; or access your workplace from thousands of miles away.

However, the Internet — and the anonymity it affords — also can give online scammers, hackers, and identity thieves access to your computer, personal information, finances, and more.

Being on guard online helps you protect your information, your computer, even yourself. To be safer and more secure online, adopt these practices recommended by the Federal Trade Commission.

## Protect Personal Information



If you're asked for your personal information — your name, email or home address, phone number, account numbers, or Social Security number — find out how it's going to be used and how it will be protected before you share it. If you have children, teach them to not give out your last name, your home address, or your phone number on the Internet.

If you get an email or pop-up message asking for personal information, don't reply or click on the link in the message. The safest course of action is not to respond to requests for your personal or financial information. If you believe there may be a need for such information by a company with whom you have an account or placed an order, contact that company directly in a way you know to be genuine.

In any case, don't send your personal information via email because email is not a secure transmission method.



If you are shopping online, don't provide your personal or financial information through a company's website until you have checked for indicators that the site is secure, like a lock icon on the browser's status bar or a website URL that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some scammers have forged security icons.

Read website privacy policies. They should explain what personal information the website collects, how the information is used, and whether it is provided to third parties. The privacy policy also should tell you whether you have the right to see what information the website has about you and what security measures the company takes to protect your information.

## Protect Passwords

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.

In addition, hackers may try to figure out your passwords to gain access to your computer. You can make it tougher for them by:

- Using passwords that have at least eight characters and include numbers or symbols.

- Avoiding common words: some hackers use programs that can try every word in the dictionary.
- Not using your personal information, your login name, or adjacent keys on the keyboard as passwords.
- Changing your passwords regularly (at a minimum, every 90 days).
- Not using the same password for each online account you access.

One way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "How much wood could a woodchuck chuck" would become HmWc@wC.

## Operating System and Web Browser



Hackers also take advantage of Web browsers (like Internet Explorer or Netscape) and operating system software (like Windows or Linux) that are unsecured. Lessen your risk by changing the settings in your browser or operating system and increasing your online security. Check the "Tools" or "Options" menus for built-in security features. If you need help understanding your choices, use your "Help" function.

Your operating system also may offer free software "patches" that close holes in the system that hackers could exploit. In fact, some common operating systems can be set to automatically retrieve and install patches for you. If your system does not do this, bookmark the website for your system's manufacturer so you can regularly visit and update.

Your email software may help you avoid viruses by giving you the ability to filter certain types of spam. It's up to you to activate the filter. If you're not using your computer for an extended period, turn it off or unplug it from the phone or cable line. When it's off, the computer doesn't send or receive information from the Internet and isn't vulnerable to hackers

## Anti-Virus Software and Firewall



Anti-virus software scans your computer and your incoming email for viruses, and then deletes them. To be effective, your anti-virus software should update routinely. Most commercial anti-virus software includes a feature to download updates automatically when you are on the Internet. Look for anti-virus software that:

- Recognizes current viruses, as well as older ones.
- Effectively reverses the damage.
- Updates automatically.

A firewall watches for outside attempts to access your system and blocks communications to and from sources you don't permit. For your firewall to be effective, it needs to be set up properly and updated regularly. Check your online "Help" feature for specific instructions.

If your operating system doesn't include a firewall, get a separate software firewall that runs in the background while you work, or install a hardware firewall — an external device that includes firewall software. Several free firewall software programs are available on the Internet.

### Newsletter contact information:

Phyllis Zalenski  
 605 E. Main  
 Anamosa, IA 52205  
 319-462-2791  
 319-462-4572 (FAX)  
[zalenski@iastate.edu](mailto:zalenski@iastate.edu)

**IOWA STATE UNIVERSITY**  
 University Extension

*... and justice for all*

The U.S. Department of Agriculture (USDA) prohibits discrimination in all its programs and activities on the basis of race, color, national origin, gender, religion, age, disability, political beliefs, sexual orientation, and marital or family status. (Not all prohibited bases apply to all programs.) Many materials can be made available in alternative formats for ADA clients. To file a complaint of discrimination, write USDA, Office of Civil Rights, Room 326-W, Whitten Building, 14th and Independence Avenue, SW, Washington, DC 20250-9410 or call 202-720-5964.