

# Fraud and the Internet: Online Shopping

*Consumer education is the process of gaining the knowledge and skills needed to manage consumer resources and taking appropriate action to influence the factors that affect consumer decisions.*

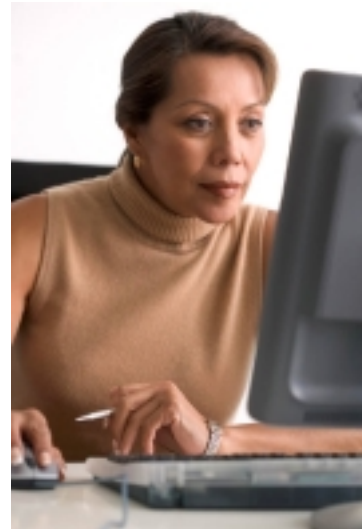
## Know the Facts

Internet shopping can be convenient, economical, safe, and perhaps fun. Shopping on the Internet offers many purchasing opportunities that are as varied as there are products to be sold. Nevertheless, just as in any other shopping venue where there are unscrupulous dealings, the Internet has crooks just waiting to take your money.

The National Consumers League (NCL) reported that the average victim loss in 2007 remained steady for Internet fraud. The average loss per person for Internet scams was \$1,507.62, which was nearly consistent with 2006's average of \$1,512. Additionally, in 2005, NCL indicated that the number of crooks from outside the United States targeting American consumers had also climbed. Within Internet fraud, 35 percent of the reports came from foreign countries, up from 30 percent in 2004. One quarter of fraudulent telemarketers were off shore, while among the 26 percent of reported Internet scams, the victims had no idea where the crooks were located.

"Paying with a credit card is the safest way to shop online. Federal law protects credit card users if they do not get what the seller promised them or if unauthorized charges are made on their accounts," said Susan Grant, director of NCL's Internet Fraud Watch (IFW). Fraud victims are more likely to have paid with a check or money order.

The NCL offers the following information to help consumers avoid Internet fraud.



## An Advantage to Shopping Online

The Internet offers numerous opportunities to shop online even outside our local communities. Nevertheless online shopping has the advantage of giving us a nearly hassle free way of doing comparison shopping among several vendors. Internet shopping can provide an adventurous shopping experience. You can shop online, find bargains, and save money while browsing stores in places you will never travel to or visit physically. Notwithstanding, the convenience of being able to shop anytime you want, 24 hours a day, seven days a week. Internet shopping also offers the availability of locating hard-to-find gifts, books, and other novelty items you will not be able to buy in your local community without ever having to leave the comfort of your home or location.

## Risks Associated with Online Shopping

However, Internet shopping brings certain security risks. Personal information provided over the Internet can be retrieved by crooks if the vendor's website is not a secure site. Practice precaution when shopping from one site to another. Do not be tempted to click on other pop-up windows that are not a part of a

secure vendor's site. Remember to protect your personal and financial information from such things as scams and other unscrupulous financial tricks.

### **Financial Fraud**

A concern for the security and protection of your personal and financial information is very important. Scams and other unscrupulous financial tricks can result from entering credit or debit card information, or any other method of payment that is required for online shopping that uses personal information. Crooks and people who are dishonest can intercept and steal your personal information and force you to encounter other financial issues or problems associated with identity theft. Personal information that is stored in computer databases could be stolen by dishonest employees or people who hack into a computer to violate the financial privacies of others. They can use this information in a negative way to cause financial ruin to online shoppers.

### **Dishonest Vendors**

While the Internet has many legitimate vendors doing business online, there are also people online that are dishonest. These so-called businesses are online to scam the consumer. It is very easy for a dishonest and fraudulent business to appear reputable simply by designing an attractive website. Usually these types of businesses misrepresent their goods or merchandise. They take your payments and never send the goods or merchandise you paid for, thus leaving you with an unresolved problem. They even go further with their misrepresentations by sending e-mails to solicit donations as if they are genuine charity agencies or organizations. Using e-mail to pull off such fraudulent tactics is cost effective and very easy to do.

### **Invasions of Privacy**

Often websites ask for personal information before you are allowed to enter their website. This type of action should be looked upon with some skepticism. Other times you may be asked to provide personal information you believe is necessary to complete a shopping transaction, or for some other reason that seems legitimate, but could prove to be harmful to you. Your personal information could be gathered and given to thieves for the purpose of causing you financial harm and irreparable damage to your financial well-being.

## **Consumer Protection**

### **Financial Privacy Rule**

The Federal Trade Commission (FTC) has published a rule as required by section 504(a) of the Gramm-Leach-Bliley (GLB) Act. The GLB Act, enacted on November 12, 1999, places certain restrictions on financial institutions when disclosing non-public consumer information to third parties. The Act directed the FTC and other federal agencies to develop rules to enforce the requirements set forth in the legislation.

According to the FTC, the GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some, but not all, sharing of their information. In other words, if companies want to sell a consumer's personal information to non-affiliated businesses, they must give the consumer a chance to say no to this practice. This is referred to as "opting out."

Currently, a financial institution is required under the GLB Act to provide consumers with a privacy policy at the time of establishing a customer relationship. The Act defines a customer relationship as a continuing relationship between a consumer and a financial institution whereby the institution provides a financial product or service to a consumer that is to be used primarily for personal, family or household purposes. The Act also describes the conditions under which a financial institution may disclose non-public personal information about a consumer; whether or not it has established a customer relationship with that consumer to a non-affiliated third party. Under the GLB Act, such information cannot be shown without providing the consumer with the institution's privacy policy and the opportunity to opt out of the information sharing. This policy is subject to certain exceptions. Despite the broad notion of financial institutions dictated by the Act, the notice states that many entities that come within the broad definition of financial institutions will unlikely be subject to the disclosure requirements of the Act because not all financial institutions have consumers or establish customer relationships. For example, management consulting is a financial activity, but it is unlikely that any individual obtains management consulting services for personal, family or household purposes.

Similarly, not every product or service that a financial institution provides to an individual is a financial product or service that establishes the individual's status as a consumer entitled to the required notice and opt out agreement. A product or service that does not result from a financial activity is not within the scope of the Act. Therefore, "a department store that issues its own credit card directly to consumers provides a financial service (credit) to consumers who use the card, but when it sells merchandise, it provides a non-financial product or service," said Grant.

## Reducing Internet Risk

### Internet Security

Check to be sure you are using a secured browser. This can be determined from the letters <https://> that appear first in the URL or address in the browser.

### Internet Privacy

Do the following when using Internet information relating to you that can be collected by companies and others.

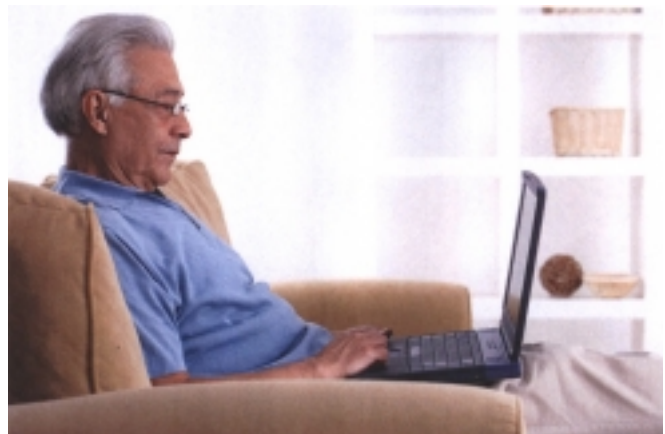
- Keep your personal information private.
- Shop with businesses and people you know and trust.
- Do not share your password.
- Use a credit card or charge card to pay for your purchases and your transaction will be protected by the Fair Credit Billing Act.
- Keep a record of your transaction for your protection.
- If you pay bills online, do not give out any personal information unless you know the business or company collecting the information.
- Check to see if the company has an online privacy policy. This policy should tell you what kind of information is being collected on the website and how such information will be used. If no privacy policy exist e-mail or write and ask the company about the privacy policy and also ask them to post the policy on their web site.

## Internet Fraud and Internet Investment

- Watch out for bogus online investment newsletters they could be a tool used fraudulently against you.
- Watch out for bogus electronic bulletin boards.
- Be on the look out for e-mail spam. Spam is junk e-mail. Crooks use it to find investors who may be lured into bogus investment schemes or to spread false information about a company.

## Phishing

Phishing is a fraud that happens through the use of e-mail. It closely resembles an authentic and legitimate looking message sent for the purpose of getting your personal and financial information. The intent of this message is to commit identity theft and make bogus purchases in your name. Most often such e-mail resembles legitimate banks, businesses, or government agencies. The e-mail asks you to confirm personal information as well as account number and password. There are also links to bogus websites. You are asked to click these sites and to provide requested information. Know that legitimate companies do not ask for personal and financial information via e-mail. Sherry (2008) suggests that you forward phishing e-mails and other suspicious e-mails to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov) and to the company that is being impersonated.



## IMPORTANT CONTACT INFORMATION

The IRS opened the Identity Protection Specialized Unit on October 1, 2008, to help taxpayers deal with the burdens caused by identity theft. Victims are advised to call 1-800-908-4490 between the hours of 8:00 a.m. and 8:00 p.m. local time.

National Fraud Information Center (NFIC) ..... 1-800-876-7060  
*Although they specialize in telemarketing and Internet fraud, NFIC also makes referrals for other types of fraud.*

### References

- Federal Citizen Information Center. (1999). *Shop safely online*. Retrieved December 10, 2008, from [http://www.pueblo.gsa.gov/cic\\_text/computers/shoonline/shoonline.htm](http://www.pueblo.gsa.gov/cic_text/computers/shoonline/shoonline.htm).
- Federal Trade Commission. (2007, June). *In brief: The financial privacy requirement of the Gramm-Leach-Bliley Act*. Facts for Business. Retrieved December 10, 2008, from <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm>.
- National Consumers League. (n.d.). *2007 top ten internet scams*. Retrieved December 10, 2008, from <http://www.fraud.org/internet/2007internet.pdf>.
- National Consumers League. (n.d.) *Why shop online*. Retrieved December 10, 2008, from <http://www.nclnet.org/eWise2.pdf>.
- National Consumers League (2005, August). *Mid-year fraud stats reveal alarming trends in telemarketing, internet scams*. NCL News. Retrieved June 25, 2008, from [http://www.nclnet.org/news/2005/fraud\\_trends\\_june2005.htm](http://www.nclnet.org/news/2005/fraud_trends_june2005.htm).
- National Consumers League (2008, February). *Con artists prey on consumer vulnerability, lurk online, make deceptive pitch via phone, email*. NCL News. Retrieved July 2, 2008, from [http://www.nclnet.org/news/2008/top\\_ten\\_scams\\_02222008.htm](http://www.nclnet.org/news/2008/top_ten_scams_02222008.htm).
- Sherry, L. (2008, Spring). *Make safety first online*. Consumer Action News. Retrieved December 10, 2008, from [http://www.consumer-action.org/news/articles/internet\\_commerce\\_issue\\_spring\\_2008/#Topic\\_02](http://www.consumer-action.org/news/articles/internet_commerce_issue_spring_2008/#Topic_02).
- United States Securities and Exchange Commission. (2007, August). *Internet fraud: How to avoid internet investment*. Retrieved December 10, 2008, from <http://www.sec.gov/investor/pubs/cyberfraud.htm>.



*Alabama A&M and Auburn Universities*

**UNP-37**

**Bernice B. Wilson, Ph.D.,** *Extension Resource Management Specialist,*  
Alabama A&M University

---

**For more information,** call your county Extension office. Look in your telephone directory under your county's name to find the number.

---

Published by the Alabama Cooperative Extension System (Alabama A&M and Auburn Universities) in cooperation with the U.S. Department of Agriculture. An Equal Opportunity Educator and Employer.

Updated December 2008; UNP-0037

© 2008 by Alabama Cooperative Extension System. All rights reserved.