

# Identity Theft Protection & Prevention: Prevent ID Internet Fraud

---

*Article by: James Banks*

Online identity theft is a serious crime that can clean out your life savings and leave you with a damaged credit history that may take years to repair. In the interim, obtaining loans, renting apartments, and even applying for work can become increasingly difficult. Here is what you can do to protect yourself:

## **Internet and computer safeguards:**

Before you shop online, install and Update spyware and virus protection utilities to prevent a worm, virus or spyware program from sending out files or other stored information from your computer. Install a firewall on your home computer to prevent hackers from obtaining personal identifying and financial data from your hard drive. Encrypt sensitive files.

Before discarding your computer, use a strong "wipe" utility to remove all recoverable data.

## **Find Out About the Company**

If you are unfamiliar with the company, research it before buying from them. If you decide to purchase something from an unknown retailer, start out with an inexpensive test order to see if the company comes through.

Trustworthy companies advertise their real business address and phone number, or customer service line. See if they are listed on the Internet yellow pages.

Call the company directly to determine if their business is genuine. Find out how the merchant handles returns.

## **Read their Privacy Policy**

Reputable e-commerce sites should offer a Privacy Policy explaining how your personal information may be shared with third parties. To prevent unwanted e-mail ("spam"), junk mail, or phone calls, read their privacy policies before submitting your personal information.

## **Verify the Web Site Address**

Cyber-criminals have been known to create counterfeit sites that look like authentic, well-established companies. Check the website address at the top of the screen, when you first visit an online store and check if it is the same as the real company's.

## **Shop on Secured Transaction Protected Sites**

A secure site uses encryption technology to transfer information from your computer to the online merchant's computer. There are a couple of ways to discern whether a site is secure.

At the time of entering personal credit card information, look at the address bar to see https://. The "s" after "http" indicates secure. Often, you will not see the "s" until time of check out.

Another way to know if a web site is secure is to look for a closed padlock displayed at the bottom of your screen. If that lock is open, you should assume it is not a secure site. Some browsers indicate a secure site with an unbroken key.

## **Shop in the USA**

By shopping in the U.S., you are protected by both federal and state consumer laws. Consumer protection is often unavailable in other countries.

## **Seal of Approval**

For peace of mind, find out if the online store voluntarily belongs to a seal-of-approval program that sets privacy-related guidelines; such as, the Better Business Bureau Online ([www.bbbonline.org](http://www.bbbonline.org)) or TRUSTe ([www.truste.org](http://www.truste.org)).

## **Credit Cards VS. Debit Cards, Cash VS. Checks**

Because of the federal Fair Credit Billing Act, credit cards are the safest way to shop online. Under this law you have the right to withhold payments on disputed charges. It is good practice to use one credit card when purchasing online to more readily track fraudulent charges.

Personal checks make you susceptible to bank fraud. Money orders may prevent this but do not offer additional protection in the event of problems with your order.

Use an actual credit card, not an ATM debit or check card. As with checks, an ATM card may open your personal banking information to criminals. Debit cards are not protected to the same extent as credit cards. If you have to use a debit card, consider using one with a limited balance that you use solely for online purchases.

**Keep Your Password Private**

Reputable e-commerce sites may require the shopper to log-in by creating a username and a password before placing or viewing an order. Never reveal your password to anyone. When selecting a password, do not use commonly known information, such as your birth date, or driver's license number. Do not reuse the same password for other sites. A good password has at least eight characters and includes both letters and numbers.

**Do NOT Give Out Your Social Security Number**

There is no reason for any merchant to ask for your Social Security number. It is not a requirement for purchasing online.

**Disclose as Little Information as Possible**

Merchants often try to obtain more information about you than necessary. They may want to know your leisurely activities, income or interests. This information may be used for marketing purposes and can lead to "spam", junk mail and telemarketers.

Only answer questions you deem are required to process your order. Often, required questions will be marked with an asterisk (\*).

**Print a Hard Copy of Your Order**

After placing an order, you should be directed to a confirmation page that reviews your entire order along with customer service information and a confirmation number. Keep it for your records for at least the period covered by the return/warranty policy.

Often you will also receive a confirmation e-mail. Be sure to keep it in your inbox along with any other correspondence until you are satisfied with your purchase.

For more on Identity Theft, visit SpyFind's ID Theft Center, [http://www.spyfind.com/credit/identity\\_theft.html](http://www.spyfind.com/credit/identity_theft.html).

James Banks serves as valuable team contributor to the SpyFind Information Network. For more related articles, visit SpyFind.com, <http://www.spyfind.com/>