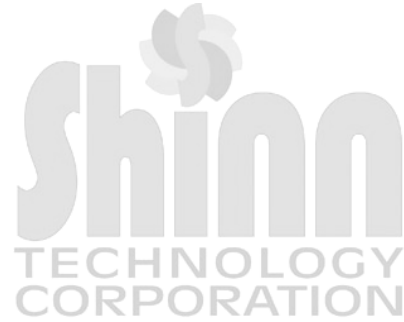


# Shinn Technology Corporation

P.O. Box 173  
Fishers , IN 46038

(317) 545-3650  
<http://www.ShinnTechnology.com>



**TITLE:           Using Your Credit Card on the Internet**

---

The Internet can be used for more than playing games or finding and retrieving information. Other uses of the Internet can include:

1. Online banking
2. Buying items from retail establishments
3. Paying utility bills
4. Handling investment decisions
5. Ordering items from catalogs

There are literally thousands of things the Internet user can do online, from making purchases to accessing your private financial information. This can all be done safely over the Internet, but a few precautions need to be taken to ensure that your information is safe. To better protect your information, you need to see how the information is sent over the Internet.

## **How Information is Sent on the Internet**

To "surf the Internet" (or to go from one site to another on the World Wide Web), you use a web browser such as Internet Explorer. Typing in web addresses, otherwise known as URLs (Uniform Resource Locators), will take you to different websites on the Internet. For example, typing in "<http://www.ShinnTechnology.com>" will take you to the Shinn Technology Corp website.

Some sites require usernames and passwords to access that particular website. On other websites, you may encounter form fields that ask you to enter information. Such fields may ask for your name, address, credit card information, telephone number, or other private information. Retail websites will require financial information such as a credit card number in order to make online purchases.

The information you type into the browser is transmitted over the Internet in what is known as "packets". Packets are like small "envelopes" that contain the information you have typed in. These packets are directed through the Internet pipelines until they reach the server of the company you are accessing.

## **What Can Happen When Your Private Information is Unprotected**

We used the analogy of the data being transmitted in packets, much like information is sent in envelopes through

the postal service. Between your computer and the computer to which you are sending the data over the Internet, there are literally hundreds of mechanical devices that route your packets to the appropriate destination.

On the Internet, there can be malicious individuals that could attempt to steal packets of data so they can view the content inside them. While nearly every Internet service in the world attempts to secure their networks, people who steal information are still present due to loopholes in hardware and software security on the Internet. There are many things that can be done to prevent these malicious people from stealing your private information.

## **How You Can Protect Your Credit Card and Personal Information**

There are a number of things that you can do to protect your private information -- such as your credit card numbers, addresses, and identity -- when using the Internet. Shinn Technology Corporation offers the following recommendations so that your online experience can be both safe and enjoyable:

1. When you are on a web page that asks for personal information about your identity, or for your credit card number, simply look for a small yellow padlock that is locked at the bottom right of the Internet Explorer browser window. The padlock looks like this:



This padlock means that the website that is asking for your personal information is using SSL encryption. SSL encryption is a process of securing the personal information that is being transmitted into packets of coded data that only the receiving computer can translate. So, if a hacker were to steal the encrypted data packet going out of your computer, they cannot read the information inside.

SSL encryption uses what is known as a 128-bit encryption scheme. To make it easily understood without going through the complete technical explanation, it would take the fastest computer in the world  $8.77 \times 10$  (to the 17th power) years to decode the information sent with 128-bit encryption protection. This translates to 876,530,835,323,573,935 years needed to decode all the possible encryption methods used by 128-bit encryption.

If the yellow padlock is present, all of your information should be secure when traveling through the Internet.

2. Make sure that you only give your credit card information to trusted retailers and people that you know. It does no good to use 128-bit encryption on your trusted data when you are sending the credit card information directly to a malicious person. If you have never heard of the company or individual to whom you are sending your personal information, ask plenty of questions, review their policies for protection of credit card data, and research the validity of their business BEFORE giving out credit card information. Also, be sure to keep records of any online credit card transactions.
3. There are many "scams" on the Internet. Some users of the Internet have received direct emails which appeared to come from some sites such as eBay.com, Microsoft.com, and Amazon.com. These emails express that the user's account on that website has been compromised, and they have asked the user to

"resend" their personal information, including credit card numbers, full names, date of birth, and so on.

NEVER send personal information in response to an email that you have received, EVEN if it looks like one of the site's web pages are automatically built into the email. In less than two minutes, a malicious person that knows how to create a webpage can take a page from a retail site, and reformat it to make it look like a "legitimate" request for information.

If you receive an email that appears to be from a legitimate request for personal information, you should call the retailer for confirmation before submitting personal information. NEVER use the "provided" number in the email. Use resources such as 800-555-1212 to get the real number of the retailer and call them directly to check the validity of the email.