

1INTERNET SHOPPING SAFETY FOR THE HOLIDAYS

Some consumer spending experts are estimating that Americans will do more than 30% of their shopping online this year. We are big fans of the online experience as well. Shopping online is a great way to save time and money. You can avoid the crowds, avoid the cold weather, and avoid the people with colds. When you are in front of the computer, it is easy to compare prices and conduct product research. But you have to be careful when shopping online, and here are some tips for doing it safely:

Shop only secure SSL web sites.

SSL stands for Secure Sockets Layer technology. This technology encrypts your sensitive information that is being exchanged on the site and it is sent through a private channel. What are the risks if the site doesn't have SSL security? You are potentially exposing your personal information to hackers and criminals. If the website does not offer SSL security, then you should probably shop elsewhere online.

How can I tell if the website is secure?

- (1) Check the webpage url:

The URL is the webpage address. It normally starts with "http:"

When you click on a link within the website to start a secure transaction, the URL should now change to "https:"

- (2) Check to make sure there is a LOCK icon that appears in the browser window. This lock icon is not just a picture. When you click on it you should see details about the sites security.

The website should post a notice or certificate with the words "Secure Transaction" or something to the effect of "Our site uses SSL technology." Veri-sign is one of the companies that offers this certification to websites.

Don't get Phished or Pharmed:

Phishing and pharming are 2 techniques used by scammers to get you to reveal your personal financial information, like your credit card numbers.

PHISHING: A scam email that appears to be legitimate from a store, bank, or credit card company that asks you to take various actions - verify your credit card information, your password, etc.

Here is a **RULE TO NEVER FORGET:** Legitimate companies will never ask you to verify any personal information via email.

PHARMING: This is a little harder to detect. This is when a fake web page has been created by a scammer that appears to be a checkout page on a shopping site. The best way to protect yourself from pharming sites is to make sure you have up to date internet security software, like Norton Internet Security. In addition, don't click on a link from an email that appears to be from a store for you to check out and purchase an item. Be on the safe side and enter in the store's web address in your browser.

Use credit cards not debit cards:

Always use your credit cards when shopping online and NEVER your debit card. Why? Most credit card companies now offer buyer protection against fraud, lost shipments, broken merchandise, etc. The big problem with a debit card is that it is a DIRECT line to your banking account.

Look at the risk of credit cards vs. debit:

If a scammer gets your credit cards, they can create havoc and hassle for you, but the loss will not be catastrophic. If they get to your bank account, they can empty it. Imagine the financial turmoil of not having money in the bank while you try and sort out that mess.

Don't buy gift cards:

We are really not fans of gift cards. Some companies have monthly fees that eat away at the balance you originally placed on the card. Most have expiration dates. And what happens if the company goes into Chapter 11 bankruptcy? There are several companies in dire financial straits that are still selling these gift cards. Will you be able to use your card when they are in bankruptcy? What happens if the company goes out of business completely?