(nv) money, inc.

By Sharon J. Ritchey and Katie Wilmeth Illustration by Matt Mignanelli

BUSINESS

Cyber Security

Pay Close Attention When Shopping Online This Holiday Season

The holiday shopping season will soon be in full swing along with the grind of circling the parking lots at Tysons Corner, Pentagon City and Potomac Mills. But there is an alternative. Shoppers are paying closer attention to online offers from "everything" retailers like Amazon.com, Buy.com and specialty boutiques flooding their inboxes. As a nation, America is gleefully embracing the ease and convenience of shopping online.

The U.S. Department of Commerce reports online sales now account for 3 percent of total retail sales in this country—$119.4 billion in 2006.

But as technology becomes easier to use, we tend to take it for granted. When it comes to online shopping, there are some risks.

Inno Eroraha, a cyber security expert and owner of Netsecurity, an information security consulting firm in Sterling, says that unfortunately, "There is really no way to determine if a merchant has a secure site. Thankfully though, Visa and MasterCard are now requiring that merchants perform annual security assessments depending on the volume of credit card transactions they do each year."

Eroraha says the first step to online security starts with good physical security. Shred your sensitive data. Educate yourself about new security threats, and know who you share your personal information with.

» Consider the computer you are using, how many people with whom you share it and the websites where you are shopping.

» Protect or secure your computer

PERRUSH/SHUTTERSTOCK (GIFT)

with a firewall, anti-virus and anti-spyware tools. Keep up to date on system patches and upgrade your software packages.

» Create passwords for your computers and log out of your system when you are done.

» Clear the browser's temporary files and close the browser when you are finished shopping. If you are using a public access machine, log off your account, clear the cache of the browser, delete temporary files, close the browser and log off the machine.

George Stafford, owner of Fairmont Studios in Clarksburg, Md., a web-design firm with an emphasis on back-end systems like online shopping carts and inventory systems, agrees with Eroraha. "Even if a company has security measures, there's a chance your data could be stolen. They may have excellent information on the front of the site, the part that you use to order your products, but they can mishandle it after they receive it."

Both Eroraha and Stafford point out that though there are potential security pitfalls, there are ways that consumers can be safer. They offer some additional hot cyber security tips:

» Never trust a site that doesn't display contact information. Additionally, if you contact a merchant via e-mail, they should answer within a reasonable amount of time.

» If you are not comfortable with a site, type the vendor's name into a search engine with the keyword "reviews" and see if there is any user feedback.

» Don't opt to store your credit card or other personal information on the merchant's computer.

» Look for a merchant's online privacy policy. Read it and see if you agree with it.

» Make sure that your transaction is secured using Secure Socket Layer (SSL) or Transport Layer Security (TSL) before entering a credit card or pin number.

» Don't give out personal information or passwords, and create different passwords for different accounts.—*SR*