Online Shopping Security Tips for the Holiday Season

More shoppers than ever are turning to mobile devices and computers to do their holiday shopping. However, internet shopping has unique risks for consumers, so shoppers need to take steps to protect themselves from fraud and scams. Here are a few tips for novice and veteran internet shoppers.

Avoid using public Wi-Fi
Any purchases made online require transmitting your credit card and/or bank account information over the internet. Using a public Wi-Fi connection to do so puts that sensitive information at risk. Hackers can tap into unsecured Wi-Fi connections at hotspots like coffee shops and airport terminals to capture that information. If you're using a wireless connection to shop, be sure that it requires a password or WEP key.

Don't respond to text solicitations
During the holiday shopping season, scammers will send out hundreds of fake deals or gift card offers via text message. If you respond, you'll likely be prompted to divulge sensitive financial information (such as a credit card number). Responding also puts you on the "sucker list" which means you'll receive even more unsolicited scam texts.

Monitor your accounts
Proactively monitoring your financial accounts (such as bank and credit card statements) can help you catch errors and spot potential fraud at the first sign. To simplify this process, use a single credit card for all your online purchases. That way you only have one statement to check instead of several.

Do not click links on social networking sites
To avoid infecting your computer or mobile device with malicious software, never click on a link to a deal or special savings on a social networking site or in an unsolicited email. Scammers will often disguise a social media post or email to make it seem as if it's coming from a known retailer, but the link will take you to a fake site and infect your device. If you see a link that supposedly leads to a sale you want to take advantage of, visit the retailer's website directly rather than clicking the link. From there you can verify if the sale is legit.

Finally, if you do notice suspicious charges on your credit card or transfers from your banking account, contact your credit card company and bank right away to notify them. They will put a freeze on the account, preventing further fraud. Remember, whenever you're online: think before you click.

BankFirst
NATIONAL
For Better Banking, Think First.

More Consumer Column articles are available at www.BankFirstNational.com under the About tab.

Article courtesy of the Wisconsin Bankers Association / Consumer Column