12/02/2014

By: Mark Pribish, Special for The Arizona Republic, November 6, 2014, used by permission of the author

If you want to help ensure a happy holiday season — whether you own a business or are a consumer — it's time to boost your Identity Theft Aptitude because identity-theft criminals are especially active from Thanksgiving to New Year's Eve.

Businesses — and really all of us — will be prime targets for deceit and deception by ID-theft criminals during the busiest selling season of the year.

To help you grow your Identity Theft Aptitude, I've assembled a checklist of tips to help you reduce your risk of identity theft and fraud.

• Computer security software. Regularly update the security software (e.g. anti-virus, firewall and anti-malware) on your computer(s).

• Contests. Be careful when entering contests to win cash, cars, computers, and tickets, etc., as they can be a source of computer viruses. Remember also that every contest site will use your personal information for marketing purposes and sell your personal information to third party marketers.

• E-mails and attachments. Do not open e-mails and attachments from individuals or organizations that you do not know and trust.

• Holiday packages. Be aware of thieves stealing packages delivered to your doorstep, where the thief follows United Parcel Service or FedEx trucks, waits for a delivery and then grabs the

package(s) before you can retrieve them.

• Online shopping. Do business with companies you know and trust. If you are unfamiliar with a website, research the company, its website and privacy policies. Use a credit card instead of a debit card or checking account, as your credit card is protected under the Fair Credit Billing Act.

• Password management. Always create complex passwords using a combination of mixed-case words, numbers, punctuation, symbols and letters, with a minimum of 10 characters.

• Personally identifiable information. Take extra care in protecting personal information such as your name, bank account, birthddate, driver's license, home address, passwords, phone number, photos, and Social Security number.

• Phishing and vishing scams. Learn how to identify phishing scams by paying close attention to e-mails from financial institutions and retail marketing organizations asking for personal information. No credible company will ask for your personal or sensitive information via email and/or phone calls.

• Privacy policies. Learn and understand the privacy policies of any application that you use and use you discretion in downloading apps.

• Privacy settings. Learn, understand, and use the privacy settings of the social media sites that you are on.

• Shredding. Purchase and use a shredder to shred your documents containing personal information.

• Social media. Review, update and confirm the personal and professional information that you have on any social network. Do not communicate to the world where you are and when, as

criminals want to know when you are not home.

• Wireless internet. Be careful of wireless Internet use and make sure that the wireless network you are using is password protected. Be aware of the fact that hackers can hack into wireless Internet networks and can view what you are viewing, such as bank account information.

Mark's most important: Do all you can to raise your Identity Theft Aptitude for the holidays so you can be the Grinch to ID-theft criminals.

Mark Pribish is vice president and ID-theft practice leader at Merchants Information Solutions Inc., a national ID-theft and background-screening provider based in Phoenix.