

From: Roy Paz [<mailto:Roy.Paz@ci.tampa.fl.us>]  
Sent: 2009-11-03 12:10  
Subject: Fwd: Information Security Advisory

FYI

>>> SecurityOffice 11/3/2009 10:04 AM >>>

### **Holiday Scams: Think Twice Before Giving**

As the holiday season draws near, scammers are gearing up to separate you from your cash by pretending to represent a charity. Don't fall for it.

You'd like to know your precious charity dollars will be well spent. With pressing needs all around and more than a million charities to choose from, how can philanthropists ensure that they're getting a decent bang for their buck? Here are some tips from experts:

The Charity Navigator website ([www.charitynavigator.org](http://www.charitynavigator.org)) allows you to search for a regional, national or global organization you might like to help. Charity Navigator, itself a nonprofit, rates the financial health and efficiency of 5,300 large charities on a four-star scale.

You may be inclined to spread your money around to as many worthy organizations as you can, but experts advise limiting the number of groups you support. Why? Well, the more organizations that you give to, the smaller the amount that goes to each group. That has some unfortunate side effects. For starters, small donations increase a charity's administrative costs. Much more of your money will benefit the actual charitable programs if you give \$500 to one organization, rather than \$5 to 100 groups.

Not only that, but giving less than \$100 or so also will sharply increase the amount of requests you get for donations. Charities commonly sell the names and addresses of their small donors to brokers who peddle lists of generous people. But charities rarely share the information on those who give, say, \$1,000 - they want to keep those donors for themselves.

Q&A: Millions Tricked by Rogue  
Security Software

Cyber-criminals are using fear and anxiety to convince users to buy rogue security software. Indeed, security firm Symantec says more than 40 million people have fallen victim to the "scareware" scam in the past 12 months.

So we thought it an opportune time to answer some common questions about the insidious practice, with an eye toward helping you safeguard your data - and your wallet.

Q: For starters, what exactly is this "scareware"?

A: It's a scam in which users are presented alarming popup windows claiming their computer security has been breached.

Q: Is this a widespread issue?

A: Yes; Symantec has identified 250 versions of scareware, and some of the criminals who run these rackets are thought to earn well over a million dollars a year.

Q: How does it work?

A: Scareware sellers use pop-up ads deliberately designed to look legitimate - for example, they often use the same typefaces and designs as Microsoft or other well-known software providers. The popups, which typically appear when a user is switching between websites, falsely warn that the computer's security has been compromised. If the user then clicks on the message, he is directed to another site where he can download the (fake) anti-virus software he supposedly needs for a fee ranging from \$29.95 to \$100.

Q: Any other risks associated with this scam?

A: Yes. Since the scareware artists are crooks to begin with, it will come as no surprise that they can't be trusted with victims' credit-card information - they often use it to commit identity fraud. Not only that, but in the insult-to-injury department, the scareware downloads themselves tend to swarm with malware, such as keyloggers, Trojans or other viruses