9 Charitable Disaster Scams

When disaster strikes not only are the lives of those involved at stake, but often the pocket books of donors are also threatened. Disaster relief efforts for hurricanes, earthquakes, fires and floods are costly and legitimate organizations depend on charitable donations and urgent fundraising. Scammers use fake phone numbers, websites, emails, text messages and social media accounts to lure donors into giving away money and personal information.

CONSUMER TIP: Do your research before donating to any organization. Whenever possible seek out the charity you wish to donate to yourself. Always independently verify the charity's name, address, phone number and contact information and learn as much as you can about the charity before donating. When donating via the web or by text message make sure you understand the terms and conditions, and total dollar value of your contribution. Visit the CRA Charities Directory (cr.arc.gc.ca) for a list of registered charities in Canada.

10 Business Directory Scams

Local companies were aggressively targeted via fax and email to advertise in a business directory that at first glance appeared to be the Yellow Pages, but was in reality no way related. An unsolicited order form was sent to local businesses containing an inverted Yellow pages logo, by a company using a similar business name. Local businesses that filled out the form contractually agreed to purchase costly advertising in a less popular online directory.

CONSUMER TIP: Both businesses and individuals need to carefully review every invoice and bill received to ensure they are from legitimate companies you wish to do business with. When signing any document or making any payment carefully read the fine print to make sure you understand the terms and conditions of the sale. Businesses, like individuals, need to be extremely cautious as to whom they give their private information.

BBB
vi.bbb.org

2010: TOP 10 SCAMS

1 Door-to-Door Sales

Beware door-to-door sales people using aggressive sales tactics to bully consumers into unnecessary purchases. Disreputable door-to-door sales people have been reported making promises they could not keep, failing to give consumers any personal or business contact information, refusing to leave the premises without closing the sale and refusing to leave copies of a written contract with the consumer.

CONSUMER TIP: Don't fall victim to high-pressure sales tactics. If you are uncomfortable with a sales person ask them to leave your home and call the police if they do not leave immediately. Before signing a contract or making a payment, ask the sales person for copies of a sample contract, warranty details and their contact information. Tell them you will research their offer and get back to them if you are interested.

2 Auto Rental Scams

Car rental companies often employ a number of tactics to increase your bill. BBB has received complaints about one low advertised rate being offered to get customers in the door, and one extremely high contract rate riddled with hidden fees and unnecessary add-ons being reality. When it comes to auto rentals be aware of overcharges related to insurance, gas, damages and additional fees.

CONSUMER TIP: Before purchasing rental insurance from a car rental company check your pre-existing coverage via your personal auto insurance, credit card coverage and home or life insurance policies. It is also more cost effective if you refill the car with gas yourself, immediately before returning it. Prior to leaving the lot with your rental car be sure you carefully go over the vehicle with a rental attendant to document any dings, dents, scratches or damage that exist.

Top 10 Scams of 2010 - *Protect Yourself*

3 Overcharges

Watch for tiny overcharges on your receipts, bank and credit card statements. Scammers quickly make a small fortune robbing you of pennies or dollars at a time. Unscrupulous cashiers and or online fraudsters are responsible for adding additional small charges to your bills under the guise of legitimate products and services.

CONSUMER TIP: Protect yourself by checking your receipt before you leave the store to make sure you have not been charged any additional funds for products you did not purchase. Review your bank and credit card statements on a monthly basis and compare your statements with your purchase receipts to make sure they match. If you see any fraudulent charges report them immediately to the store, bank or credit card company.

4 Smishing

Smishing is the newest twist on phishing (via email) and vishing (via voice over IP) Smishing is when scammers use SMS text messaging to contact you pretending to be a trustworthy source (like your bank) and claim that there is an issue with your account. You are then asked go to a website or to phone a certain number where you are duped into updating your personal and account information for the purposes of identity theft.

CONSUMER TIP: Legitimate financial organizations will not contact you via email, voice messaging or text messaging if there is a problem with your account. If there is a legitimate problem you will most likely be asked to visit your nearest financial institution to remedy the issue. If you are contacted via email, phone or text about your account, contact your financial institution directly via contact numbers you yourself have found and ask if there is a problem with your account.

5 Social Media Scams

Social media scammers employ the same tactics common to traditional scams, but take advantage of social networking technology to target mass groups of users quickly. Common elements of social media scams include: offers of cash, a prize, or a gift to entice people to participate; you are asked to become a fan or follower and to invite others on your contact lists to get involved; personal information is requested; or you are lured away from the original social media site to outside web links.

CONSUMER TIP: Always be aware of unsolicited opportunities to win cash, a prize or take advantage of a too-good-to-be-true opportunity. Be extremely cautious about giving out personal information to anyone, under any circumstances. Be sure you understand and regularly review your personal privacy settings on social media sites that you visit. Never download something unless you are sure it is coming from a well-known, trusted source.

6 SPLOGS

Also known as spam blog, a SPLOG is essentially a fake blog often composed of stolen content that has been created for the purposes of search engine spamming. Most SPLOGS contain a high number of web links to sites that are disreputable in order to promote affiliated websites, increase search engine rankings or to simply sell links and ads. SPLOGs proliferate the Internet. It is estimated that as many as 1 in 5 blogs are fake.

CONSUMER TIP: The existence of SPLOGs threatens the credibility of legitimate bloggers. People who blog must be aware of the very real likelihood that someone is stealing their original content and passing it off as their own. SPLOG's are typically identifiable by the fact that the content, title and links do not match up. Often embedded links to additional content end up just being links to irrelevant ads. If you come across a SPLOG report it to the blog administrator (i.e. WordPress, Google etc.)

7 Pyramid Schemes

A pyramid scheme is a non-sustainable business model in which the focus is based on recruiting people to participate or invest in a business opportunity, rather than on delivering a legitimate product or service. Pyramid schemes eventually lead to a point where no new investors exist and the pyramid collapses. Those on the bottom lose their money.

CONSUMER TIP: Before getting involved in any business opportunity you need to understand it fully. Ask for written documentation regarding the company's officers, products, business plan, marketing plan, contracts, sales materials and prospectus. Review these materials with your lawyer. Do your research to ensure that there is a market for the products or services the business sells. Be wary of opportunities with large start up costs and in which the primary focus is the recruitment of new members. If it sounds too good to be true, it usually is.

8 Online Job Scams

Job scams posted online are fairly similar to those posted in traditional classified ads, however the number of online job scams is exploding with the increased use of Internet and social networking sites. There are hundreds of different online job scams in existence. The common thread is that job seekers are required to give out excessive amounts of personal information and typically are charged some type of fee to participate.

CONSUMER TIP: Be aware of jobs that require: money up front in order for you to purchase materials to get started; you to wire, forward or transfer money through personal bank accounts; you to provide detailed personal and financial information in order to apply for the position; you to download applications from unsecure sources. Before applying for any online job opportunity do some research first, and visit vi.bbb.org to look up the company's BBB Business Review.