How to Protect Yourself from Fake Charities and Donation Scams

Giving the gift of a donation to charity is a great way to lend a helping hand to our community. But it's important to be on the watch for fake charities and donation scams. Arm yourself with the skills and tools to be able to tell if a charity is legitimate as well as find cause to donate to.

Signs of Fake Charities and Donation Scams:

Being Pressured to Donate

It's okay if your heart strings are tugged, but you should never feel like your arm is being twisted. If you are feeling pressured, are faced with aggression, or are having an emergency deadline put on your donation, this might be a scam.

A legitimate charity is going to provide an opportunity for a paper trail and receipts. If you are being told any of the following, do some more investigating:

- They can only accept **cash** donations
- That a check needs to be made out to them personally because it will help accounting
- That they can't provide an official receipt

A few questions you can ask:

- For an explanation to the relief that will be offered
- How funds will be distributed
- Who will benefit
- When funds will be allocated
- What percentage of donations directly benefit the cause

There are so many amazing non-profit organizations in our community and any one of them who are receiving an in-kind gift would be happy to answer your questions.

Abnormal behavior

If you already have a relationship with a charity and receive an email or phone call that is completely out of character for them, question the validity. This may be an example of **spoofing**, where scammers use a legitimate business' profiles to get more information.

Before committing or giving any information, follow-up with a number or email you know and have used before to check the validity of the request. Do not use the contact information that is given to you.

Maybe you've worked with a local charity, and they are now sending you a request to support a "partner organization" overseas. This is a great example of a legitimate business, and their reputation, being used for a scam.

Online solicitations

If you've received an email, text message or social post from unknown senders, this could be a **Phishing attempt**. Don't get hooked!

Ignore any links, click thru to videos, or even unsubscribes which could trick you into giving a valid email to their database. Instead, add it to your own spam filter so future attempts will be ignored.

Cheney Federal Credit Union's free real-time fraud monitoring service monitors members' debit and credit cards for fraudulent activity and might text you if fraud is suspected. Unless you have just activated a new product or service, **CFCU would never reach out to you for your personal account information, including Social Security Number or credit card information, by email, text, or over the phone.**

If you receive a suspicious email, text, or phone call, **DO NOT** give out any information and immediately call CFCU at 509-235-6533.

Charity Checklist

Maybe you already have your favorite charities, but if you are looking to give to a new non-profit, there are some things you should do to make sure the **charity is legitimate.**

- Ask for detailed information. Beyond name, address, and telephone, ask for their Annual Report or area of funding.
- Do some research. Use the internet or call the organization with contact information that was not provided in the initial phone call.
- Check to see if the charity or fundraiser is registered to receive tax deductible contributions
- How long has the charity been around? Be cautious of those that spring up suddenly in response to current events and natural disasters.

What to do if you feel like you've fallen victim to a scam

Don't panic. Scammers are relying on you to make hasty decisions. You'll be better able to avoid their traps if you don't rush.

Change your passwords

- First change the password to any account or machine the scammer has or could access.
- Change the passwords on any account that you were logged in to on your machine.
- Change the passwords for any accounts that use the same or similar login credentials.

Protect your computer, click carefully, and guard personal data. Ensure that anti-virus software, security patches and firewalls are installed, active and up-to-date.

We understand that a situation like this creates stress and anxiety about the safety of your account information. If you have further questions about this or any other correspondence that looks suspicious, please come in and visit with a Member Service Specialist or call us at 509-235-6533.