

SCAM #11 ALERT

Protect yourself when donating money online

In the wake of recent natural disasters, you may have considered how you can help those most affected by the tragedies.

Donating money online is a convenient way that you can lend a hand, unfortunately it's also a simple way for scammers to divert your money to them. Here are a few easy tips to remember to make sure your gift is sent to the intended recipient.

- **Give to legitimate charities.**

Ask to see the organization's 990 IRS Form. Charities must file this document with the Internal Revenue Service.

- **Type the Web address of the charity you'd like to give to.**

Don't simply click a link because it might lead you right to a fraudulent Web site, which may look a lot like the charity you'd like to donate to.

- **Check the privacy policy.**

Don't disclose personal or financial information unless you know how this data will be used.

- **Print a copy of the donation confirmation page.**

If you do not receive a confirmation, then ask for one.

- **Look for contact information.**

Most reputable charities will include an e-mail address as well as their phone number and address on their Web site.

When you give to a charity online, you want to ensure that your contribution is making a difference, not making a scammer rich. By following these basic guidelines, you can make sure your gift is doing the good you intended it to... help those in need!



SEFCU is committed to helping members protect themselves against fraud. This is the eleventh in a series of SCAM ALERTS to educate members about deceptive activities that could harm members' financial security. While we cannot advise members of every scam, we hope the series will advance awareness of privacy and security issues.

©SEFCU, October 2005