Consumer Federation of America
1620 I Street, NW Suite 200 * Washington, DC 20006

PROTECT YOURSELF FROM THE "GRANDPARENT SCAM"

You get a call or an email unexpectedly from someone who claims to be a friend or relative. This often happens to grandparents with the caller claiming to be their grandson or granddaughter. The caller says there's an emergency and asks you to send money immediately. But beware, there's a good chance this is an imposter trying to steal your money! Follow these tips to avoid becoming a victim of fraud.

- **How do these scammers choose you to contact?** Sometimes they contact people randomly. They also use marketing lists, telephone listings, and information from social networking sites, obituaries and other sources. Sometimes they hack into people's email accounts and send messages to everyone in their contact list.

- **How do these scammers know the names of your friends or relatives?** In some cases they don't. For instance, the scammer may say "Hi grandma," hoping that you actually have a grandson. If you ask, "David, is that you?" the scammer will say "Yes!" Often these crooks will call in the middle of the night and take advantage of the fact that you may not be awake enough to ask more questions and you may not want to disturb other people by calling them to confirm the information. Sometimes the scammers *do* know the names of your friends or relatives. They can get that information from a variety of sources. Your relatives may be mentioned in an obituary or on a social networking site. Your email contact list may contain the names of friends and relatives.

- **What do these scammers usually say?** They might say something like, "I'm in Canada and I'm trying to get home but my car broke down and I need money right away to get it fixed." Or they may claim to have been mugged, or been in a car accident, or need money for bail or to pay customs fees to get back into the United States from another country. They may also pose as an attorney or law enforcement official contacting you on behalf of a friend or relative. No matter the story, they always want you to send money immediately.

- **If you realize you've been scammed, what can you do?** These scammers ask you to send money through services such as Western Union and MoneyGram because they can pick it up quickly, in cash. They often use phony IDs, so it's impossible to trace them. Contact the money transfer service immediately to report the scam. If the money hasn't been picked up yet, you can retrieve it, but if it has, it's not like a check that you can stop – the money is gone.

- **How can you protect your email account from being used by scammers?** Use a firewall and anti-virus and anti-spyware software. Many computers come with these features already built-in. They are also easy to find on the Internet. Keep your software updated. Don't open attachments in emails from strangers, since they can contain programs that enable crooks to get into your computer remotely.

- **What else can you do to protect yourself?** If you get a call or email from someone claiming to know you and asking for help, check to confirm that it's legitimate before you send any money. Ask some questions that would be hard for an imposter to answer correctly – the name of the person's pet, for example, or the date of their mother's birthday. Contact the person who they claim to be directly. If you can't reach the person, contact someone else – a friend or relative of the person. Don't send money unless you're sure it's the real person you know. For more information about protecting yourself from fraud, go to www.consumerfed.org/fraud.