

## Scam E-Mails That Require Action or Lack Thereof

If you have had an e-mail account, you are familiar with having “unwanted” solicitation e-mails for “free” things that are **never** really free and things that you never signed-up for begin to appear in your mailbox.

That problem continues to happen every day to almost everyone....in fact it happens more often than we realize. Have you ever had an email promoting a free iPad that if you only “*Click Here*” and sign up for the free drawing, you could own one tomorrow? The reality is that by signing up for the “free” promotional item, you have just provided “someone” with your name, email address, telephone number, and mailing address. You have also given permission for your email account to be solicited to - which means that the number of “Junk” emails in your Inbox will only increase.

Similar emails about people you know being stranded in foreign countries also circulate quite a bit. Unfortunately once the contact list of someone you know has been compromised, you are very likely to be contacted and asked for immediate financial assistance. There are emails that pretend to be your financial institution (bank) and request your account number for verification...**never** reply or give out any personal information unless you were directed to contact the bank directly by someone in our Finance Department.

In all these cases, the first thing to do is

1. **STAY CALM** and never fall victim to an alerting email that your computer has a virus and needs immediate repair or that someone you know has been badly hurt/stranded and needs money.
2. **DO NOT RESPOND** to any emails with suspicious websites or links on it.
3. **CONTACT the SSND CP IT Staff** as soon as possible if you have any questions. We will be more than happy to assist.

Contact us directly at 1-800-373-7521 or [helpdesk@ssndcp.org](mailto:helpdesk@ssndcp.org)