Those infamous online crooks who notify us we've won sweepstakes or inherited millions from forgotten relatives have come up with a travel-related scam. Apparently they're targeting seniors who've been frequent cruise and resort passengers.

Where they got the email addresses is suspect, possibly from greedy cruise ship crews and/or resort and travel agency employees. The scam works simply. You're notified that you've won an all-expense-paid luxury cruise or hotel vacation at one of the popular lines or resorts, such as Club Med, Princess, Royal Caribbean, Cunard and others.

Sounds wonderful, doesn't it. The scam email says the cruise or vacation is worth $10,000, sometimes more. In order to qualify, all you need to do is fill out a questionnaire giving all personal information, name, address and three numbers: social security, bank account and credit card. Some of the scams will ask for a check as an advance deposit fee of from $100 to $1,000, telling you the fee is necessary for "processing expenses" or "good faith" to reserve your absolutely free $10,000 vacation.

Here's what you do: NOTHING! If the subject line words on the email look like a scam, don't open the email. If you open it, DO NOT fill in the information on the questionnaire. DO NOT give out any personal ID numbers. With those in their possession, the thieves can empty out your bank account or charge thousands to your credit card, all in a matter of hours. And, of course, DO NOT send any deposit money.

Just a week or so ago, we received an email supposedly from our online money processing organization. It had the realistic-looking company logo on it, and a questionnaire. The instructions told us our account needed updating, and we needed to list all of our current bank and credit card numbers on the form. The letter said if we did not submit the completed questionnaire within 10 days, the company could cancel our account.

That last paragraph gave it away as a scam. No organization, under law, can just kill our account. We called the company trouble line and it was confirmed that the email was a fraud. Sorry to say, that wasn't an isolated case. In our offices, we get two or three obvious scam emails a day, and staff members get several a week on their home computers.

In summary: If an email subject line words look suspicious, DO NOT open the email. Some of the words on the subject line often list familiar bank, cruise or charity names. That attracts many people to open the emails. If you do, and the content looks phony, DO NOT respond in any way, and just ERASE the email.

One more note. If the phony email uses familiar business names, such as Bank of America, U.S. Treasury Department, Princess Cruise Lines, Bank of England or others, take a few moments to phone or email the legitimate companies and report details of the scam.