Beware of Internet Emails from Overseas

The Hook
Emails addressed to your account informing you of winning the lottery or other prize claims.

The Scam
These individuals are “phishing” for information about you that can result in a loss of thousands of dollars or even identity theft.

Play it Safe
Do not respond to individuals through email that you do not know. If you receive an email from another country, chances are it is a scam and you should delete it right away. Be very cautious on who you send information to.

The Whole Story
These emails are an example of "phishing" for detailed personal information over the internet by notifying you of attractive free offers, or lottery winnings. It is, however, merely a numbers game. If you send enough teasers over the internet notifying the recipient they are the winners of a lottery or drawing, there will always be people who respond. To prevent getting caught, or at least minimize the chance of prosecution, the fraudsters usually send these emails from hard to trace accounts on servers located overseas. It used to be that anything you saw originating from Africa (particularly Nigeria) or Eastern Europe was suspicious; but the most recent spate of emails comes from Brussels, Belgium and London, England.

Here is how it works. You get an email from an organization that you don’t recognize, addressed to your email account but not addressing you by your first name. In other words, there is no salutation such as "Dear Jenny" on the email (because they don’t know your name, they just have your email address). It simply says you have just won a lottery prize worth a substantial sum of money (sometimes in the millions). All you have to do to collect the prize, for example, is fly to Brussels on a certain date to receive the award and participate in an awards ceremony and a press conference. The email says the organization will make arrangements for travel (hotel and plane) if you simply will send them a confirmation with your proper name on it and your willingness to accept the prize on certain promotional conditions. They give the telephone number of the person to call if you have questions. Over the phone they will convincingly ask other pertinent, plausible questions that make you think they are going to purchase your plane ticket, such as address, social security number, credit card number, expiration date on your card, and the special three digit code on the back of the card.

By giving out this critical information, you are enabling identity theft and giving immediate access to your credit card allowing the fraudsters to ring up plenty of charges. The worst part is the possibility of identity theft. With this information they will be able to go beyond just one credit card and can cause detrimental damage to credit scores as well as have access to your mailing address and bank accounts. It may take months to get everything cleared up, in addition to the hassle with creditors.

Lesson
Never, never, give out your social security number to someone you don’t know (especially over the phone or the internet). When you buy something using your credit card over the phone you have to give out the card number, but your safeguard against misuse of your card is the monthly billing statement to make sure you recognize every charge on the monthly bill. When you give out additional information such as home phone number, address, or social security number you are simply putting frosting on the cake and increasing the risk of identity theft. In the time period that elapses until you get your monthly billing a fraudster can rack up incredible charges, and even print a bogus plastic card since he has you name, number, expiration date, and three digit code. The fraudster can keep buying until the card limit is reached or you call to cancel your card. And remember, misuse of your credit card enhances the chance of subsequent damage to you bank accounts and your credit rating.