

# Lotto Scam Alert

**Are you receiving e-mails** and letters from legitimate sounding lottery organizations or claim winning businesses that assure you are a winner in a lottery drawing or insurance claim? Are these lottery drawings/claims held in distant countries? Well, so have many people! This is a **scam**, an old one that comes around every year or so. This is what Fox Valley Savings Bank found out regarding this scam.

**Each lottery e-mail or letter** is rich in detail about when and where the drawing was held, the lucky ticket numbers, how the fortunate person or company name was included in the drawing, who was to pay out the funds, the payer's phone number and fax numbers, plus their web site information and how much money is supposed to be coming. The winner of an insurance windfall letter usually has a cashier's check attached along with a phone number to contact regarding how to obtain the rest of your claim money. Most often, all the "supporting" information is false. In some cases, the names of the real lotteries and banks are involved, however, the financial institutions have no relationship to them.

**So far we've seen versions** of this fraud come in from "De Lotto Netherlands," "Diamond Lotto South America," "Alpha Lottery International," "Lotto Canada", and many fraudulent cashier's checks – just to name a few. They are all the same scam. The scam artist changes the names of the lottery handing out the winnings. Those who try to collect their "winnings" soon find themselves receiving e-mails or letters informing them that they have to pay facilitation fees before the big pay outs will come to them. There are no lottery winnings waiting, but rather scam artists ready to trick people into wiring "handling fees" directly into their accounts. The "lucky" winners scramble to pay the fees while the clock is ticking, but they never receive any winnings.

**Be careful if you receive** any e-mails or letters similar to these. Ask yourself these questions: Did you buy a lottery ticket? Did you give them your name? Did you provide it when you purchased the lottery ticket? If you answer NO to these questions – DON'T SEND ANY MONEY – IT IS A SCAM!

CONTINUED ON NEXT PAGE »

# Phishing - Don't Get Caught

Phishing (pronounced like fishing) is an internet scam whereby the scammer creates a replica of an existing Web page to fool a user into submitting personal, financial or password data. For example, you may get an Email that looks like it is from your credit card company. It may ask you to supply your credit card number in order to keep your card active. **When you respond to any such requests for information, you are giving the scammers what they need to defraud you.** Likewise, it is possible for scammers to duplicate the look of a bank's web page and send you an email asking you to supply your account numbers and password in order to keep your internet banking account active. Never, ever respond to a request like this. Your bank would not send you a request for that type of information.

## Tips on how to avoid the internet scam known as "phishing".

1. If you receive an unexpected Email saying your account will be shut down unless you confirm your billing information, do not reply or click any links in the Email body. Never provide your personal information over the phone (unless you have placed the call to a known entity); never respond to an unsolicited internet request.
2. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It means your information is secure during transmission.
3. If you are uncertain about the information, contact the company through an address or telephone number you know to be genuine.
4. If you unknowingly supplied personal or financial information, contact your bank and credit card company immediately.
5. Suspicious Email can be forwarded to [uce@ftc.gov](mailto:uce@ftc.gov), and complaints should be filed with the state attorney general's office or through the FTC at [www.ftc.gov](http://www.ftc.gov).