



Scams Mimic Government Stimulus Package

February 11, 2009

Identity thieves posing as representatives of the Internal Revenue Service (IRS) are sending spam emails promising government economic stimulus packages. The message tells the user to download an attachment that is masked as a form they must fill out and send to the IRS to receive their check. However, the document is really an identity theft tool that steals the personal information entered.

Another scam being used promises more information on how to get “economic stimulus grants.” They tempt users with fake testimonials such as, “I found the grant I needed and filled out the forms and sent them in, and in about two weeks I received a check in my hand for \$100,000.” It leads to a marketing-type site in which you enter personal information such as salary range, email address, mailing address, and date of birth purportedly to get a free CD that shows you how to claim one of these grants. To order the CD, you must enter credit card information for the postage and handling costs. You never get the CD—only a stolen identity.

Unfortunately, the threat of fraud due to phishing attempts continues to be very active. Fraudsters are increasing in sophistication, and this type of activity shows no sign of slowing down.

Never respond to any email, telephone call, voice message, text message, or letter received through the mail that requests personal and financial information, including the three-digit number on the back of the card unless you have initiated the transaction.

If you have any questions, or feel that your information may have been compromised, please contact the credit union immediately at 217-278-7700 or toll-free at 877-678 -4328.