Cerritos Neighborhood Watch Report

April 2008

Hardening the Target

IRS warns taxpayers to be on the lookout for scams

The Internal Revenue Service (IRS) is warning taxpayers to beware of several current e-mail and telephone scams that use the IRS name as a lure.

Specifically, the scams involve the stimulus payments.

The goal of the scams is to trick people into revealing personal and financial information, such as Social Security, bank account or credit card numbers, which the scammers can use to commit identity theft.

Typically, identity thieves use a victim's personal and financial data to empty the victim's financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name, file fraudulent tax returns or even commit crimes. Most of these fraudulent activities can be committed electronically from a remote location. Committing these activities in cyberspace allows scammers to act quickly and cover their tracks before the victim becomes aware of the theft.

The most recent scams brought to the IRS's attention are described below.

Rebate phone call

At least one scheme using the word "rebate" as part of the lure has been identified. In this scam, consumers receive a phone call from someone claiming to be an IRS employee. The caller tells the targeted victim that he is eligible for a sizable rebate if he files his taxes early. The caller then states that he needs the target's bank account information for the direct deposit of the rebate. If the target refuses, he is told that he cannot receive the rebate.

This phone call is a scam. The IRS does not force taxpayers to use direct deposit. Those who opt for direct deposit do so by completing the appropriate section of their tax return, with bank routing and account information, when they file their taxes; the IRS never gathers this information by telephone.

Refund e-mail

The IRS has also seen several variations of a refund-related e-mail which falsely claims to come from the IRS. The e-mail tells the recipient that he or she is eligible for a tax refund for a specific amount, and instructs the recipient to click on a link in the e-mail to access a refund claim form. The form asks the recipient to enter personal information that the scammers can then use to access the e-mail recipient's bank or credit card account.

In a new wrinkle, the current version of the refund scam includes two paragraphs that appear to be directed toward tax-exempt organizations that distribute funds to other organizations or individuals. The e-mail contains the name and supposed signature of the Director of the IRS's Exempt Organizations business division.

This e-mail is also phony. The IRS does not send unsolicited e-mail about tax account matters to individual, business, tax-exempt or other taxpayers.

Filing a tax return is the only way to apply for a tax refund; there is no separate application form. The only official IRS website is located at www.irs.gov.

Audit e-mail

Another new scam brought to the IRS's attention contains features not seen before by the IRS. This phony e-mail notifies the recipient that his or her tax return will be audited.

Also unusual for a scam e-mail, it may contain a salutation addressed to the specific recipient.

This e-mail instructs the recipient to click on links to complete forms with personal and account information, which the scammers will use to commit identity theft.

Again, this is another phony e-mail; the IRS does not send unsolicited, tax-account related e-mails to taxpayers.

Changes to tax law e-mail

This bogus e-mail is addressed to businesses, accountants and "Treasury" managers. It instructs them to download information on tax law changes by clicking on a series of links to publications on businesses, estate taxes, excise taxes, exempt organizations and IRAs and other retirement plans. The IRS believes that clicking on a link downloads "malware" onto the recipient's computer. Malware is malicious code that can take over the victim's computer hard drive, possibly giving someone remote access to the computer.

Paper check phone call

In a current telephone scam, a caller claiming to be an IRS employee says that the IRS sent a check to the individual being called. The caller states that because the check has not been cashed, the IRS wants to verify the individual's bank account number.

The IRS leaves it entirely up to the individual to choose to cash or not cash a paper check, and will not call a person to verify whether their check has been cashed.

Continued on the other side

Monthly Crime Summary: March 2008

There were 123 Part I felony investigations initiated by Cerritos Sheriff's Station personnel in March. An adjusted figure of 140 cases was logged in February 2008. Robberies, residential burglaries, vehicle burglaries and vehicle thefts decreased in March. Field deputies were handling an average of 309 calls for service per week at the end of March.

Robberies

There were 10 robbery incidents investigated by Cerritos deputies in March, compared to 11 incidents in February.

On Wednesday, March 5 at 1:00 a.m. a male adult was riding his bicycle on Pioneer Boulevard near South Street when he was surrounded by seven males. One produced a knife and the victim was robbed of his cash.

A male was exiting his vehicle in a lot at Gridley Road and South Street on Thursday, March 6 at 11:00 p.m. when he was attacked by two males. When the victim was on the ground, one of the two suspects removed his wallet and the suspects fled.

On Thursday, March 20 at 10:08 p.m. a female was walking in the 19200 block of Ely Avenue when a vehicle containing three male juveniles pulled up beside her. One exited the vehicle and grabbed the victim's purse, then returned to the car and drove away.

At 7:30 p.m. on Friday, March 21, another vehicle stopped near a male juvenile on Gridley Road north of South Street and one of the three teens in that vehicle exited and demanded the victim's cell phone.

A woman was robbed of cash in the 12100 block of Napoli Drive on Saturday, March 22 at 11:30 a.m. by what appeared to be a residential burglar that reacted to an opportunity (the victim) and committed a robbery.

A shoplifting incident turned into a robbery on Wednesday, March 26 at 7:00 p.m. when two juveniles fought with loss prevention personnel at a store in the 11500 block of South Street. One was arrested and the other fled, but was identified.

A juvenile victim reported being robbed by two male juveniles in the 11100 block of Artesia Boulevard on Monday, March 17 at 7:00 a.m. A small amount of cash was taken in the crime, which was reported more than ten days later.

Juveniles were involved in yet another robbery as three teens confronted three teen victims on Thursday, March 27 at 4:30 p.m. in the 12400 block of Ashcreek Road.

An attempted robbery occurred on Friday, March 28 at 9:55 a.m. when a male tried to grab a deposit bag from a merchant in the 17500 block of Bloomfield Avenue.

The final incident occurred on Saturday, March 29 at 4:30 p.m. in the 19300 block of Vickie Avenue when a teen took a laptop computer from a male juvenile.

Residential Burglaries

Seventeen residential burglaries were reported in March, down from 18 in February. Open/unlocked doors or windows were involved in six entries. Seven windows were shattered and four were pried open. Cameras, bicycles, video games, jewelry, laptop computers, wallets, cash and a vehicle were among the items reported stolen. The 2008 weekly average in residential burglaries was 3.2 at the end of March.

Neighborhood Watch Town Hall Meeting set for May 14

The next Neighborhood Watch Town Hall Meeting is scheduled for Wednesday, May 14 at 7 p.m. at the Senior Center located at 12340 South Street. Representatives from the Cerritos Sheriff's Station/Community Safety Center will offer an in-depth presentation on crime in Cerritos.

Vehicle Burglaries

Vehicle burglaries also decreased by one case compared to February as 29 were investigated in March. High-volume commercial parking lots were the crime scenes in 15 of the break-ins. Twenty-two of the incidents involved SUVs, and two victims reported car stereo items stolen. Other items reported stolen included laptop computers, MP3 players, gym bags, briefcases, flashlights, backpacks, tools and GPS units. The weekly average in vehicle burglaries at the end of March was 8.4.

Vehicle Thefts

Fourteen vehicle thefts were reported in March, down from an adjusted figure of 22 in February. Nine of the vehicles were stolen from high-volume commercial parking lots. Eight SUVs were taken, along with two Hondas and four Toyotas. The weekly average in vehicle theft at the end of March was 4.6.

IRS warns of scams

Continued from the other side

What to do

Anyone wishing to access the IRS website should type the address into their Internet address window, rather than clicking on a link in an e-mail or opening an attachment.

Those who have received a questionable e-mail claiming to come from the IRS may forward it to the IRS at phishing@irs.gov, using instructions contained in an article titled "How to Protect Yourself from Suspicious E-Mails or Phishing Schemes." (The article is available on the IRS website by searching for the words "suspicious e-mails".) Following the instructions will help the IRS track the suspicious e-mail to its origins and shut down the scam.

Those who have received a questionable phone call that claims to come from the IRS may also use the e-mail above to notify the IRS of the scam.