INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS
OCTOBER 17, 2011

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

TRAFFIC TICKET SPAM

The IC3 has received over 70 complaints since July 2011 reporting fraudulent e-mails claiming the recipient had been issued a traffic ticket. The spam, which spoofed a nyc.gov e-mail address, claimed to be from the New York State Police (NYSP). Complainants, throughout the U.S. and internationally, reported that the e-mail indicated a traffic ticket had been issued against them as a result of a moving violation. None of the complainants reported any monetary loss. The e-mail, as noted in the sample below, instructed them to print the ticket and mail it to a town court in Chatam Hall to plead.

> *Subject: Uniform traffic ticket*
> *New York State Department of Motor Vehicles*
> ***UNIFORM TRAFFIC TICKET***
> *POLICE AGENCY*
> *NEW YORK STATE POLICE*
> *Local Police Code*
> ***THE PERSON DESCRIBED ABOVE IS CHARGED AS FOLLOWS***
> *Time* *Date of Offense* *IN VIOLATION OF*
> *7:25 AM* *07/05/2011* *NYS V AND T LAW*
> *Description of Violation*
> ***SPEED OVER 55 ZONE***
> ***TO PLEAD, PRINT OUT THE ENCLOSED TICKET AND SEND IT TO TOWN COURT, CHATAM HALL., PO BOX 117***

The attached file contained in the e-mail was called Ticket-064-211.zip and some of the recipients reported that their anti-virus software detected that it contained malware.

The NYSP has posted the following two alerts on their site warning consumers of this scam:

http://troopers.ny.gov/Public_Information/2011_News_Releases/07-06-11_Hoax_E-mail_Alert.cfm

http://troopers.ny.gov/Public_Information/2011_News_Releases/08-17-11_UTT_Hoax_E-mail_Returns.cfm

FRAUDSTER DOUBLE-DIPPING

Most of us are familiar with fraud involving automobiles being sold over the Internet. A fraudster will post a nonexistent vehicle for sale on the Internet, typically a luxury or sports car. The details of the vehicle, including photos and description, are typically lifted from legitimate websites. An interested buyer, hopeful for a bargain, responds and is told that the vehicle is located overseas. The fraudster then instructs the victim to send a deposit via wire transfer to initiate the shipping process.

In a new twist to this scam, the fraudster advised there was an issue with the initial wire transfer and sent the victim a cashier's check. The victim was instructed to cash the check and resend a second wire to a different account. Unaware that the check was counterfeit, the

victim followed through as instructed by the fraudster. This resulted in the victim getting duped two times and the fraudster accomplishing his "double-dipping" strategy.

Victims should be vigilant when an Internet transaction involves wire transfers and cashier's checks. Most individuals believe that cashier's checks are as good as cash and they clear the day after they are deposited. However, banks are required to make the funds "available" in the individual's account within 48 hours, which can be days before the cashier's check clears or bounces. Once the bank makes the funds available, the counterfeit check circulates to incorrect Federal Reserve locations. Generally, the average cashier's check takes up to two weeks to clear, not two days. The bottom line: fraudsters understand the U.S. banking system process and capitalize on victims' misconceptions of the term "available funds."

The IC3 has posted multiple alerts warning consumers of various types of counterfeit check scams. The most recent warning was in the IC3 Scam Alert, May 10, 2011, which is available at: https://www.ic3.gov/media/2011/110510.aspx.

To learn more on this scam, prevention tips, and available resources, consumers can visit LooksTooGoodToBeTrue's Types of Fraud page on counterfeit checks at the following link: http://www.lookstoogoodtobetrue.com/fraudtypes/counterfeitcheck.aspx.

ONLINE VEHICLE SCAM USING KELLEY BLUE BOOK'S NAME

The IC3 has received complaints reporting fraudsters for misrepresenting themselves as Kelley Blue Book (KBB) agents to swindle victims out of thousands of dollars in online vehicle purchases. Upon finding a vehicle and making an inquiry to the seller, the complainant was told that the transaction must go through KBB's escrow-based buyer-protection plan to protect both of them. The fraudster claimed that the protection plan would hold the buyer's money for a five-day period while they could receive and inspect the vehicle. The fraudster then sent the complainant a link, which was purportedly to the KBB website, providing details of the process. Some complainants reported that the fraudster sent pictures of the vehicle as well. Once the purchase was agreed upon, the fraudster sent the complainant an official-looking e-mail, purportedly from KBB, instructing them to wire the payment to a KBB agent.

Upon contacting the actual KBB company, complainants were advised that it was a scam and that KBB does not offer an escrow-based buyer-protection plan. Recent articles have been posted on the KBB website warning consumers of this particular scam.

RADIO SPOTS ADVERTISING FOR A MYSTERY SHOPPER

Some retailers hire marketing research companies to evaluate the quality of service in their stores. These research companies, in turn, use mystery shoppers to make a particular purchase in a store or restaurant and then report on the experience.

Another version of mystery shopping involves consumers being "hired" to evaluate the speed and efficiency of a specified money transfer service. In this process, the shopper receives a check with instructions to deposit it in a personal bank account, withdraw the amount in cash, and wire it to a third party. After wiring the cash to a third party, the victim learns that the check was counterfeit, and loses the amount of money involved. Generally, such opportunities are posted on reputable websites, television stations, and publications, hoping this will give them credibility. In reality, these media outlets are unable to verify the legitimacy of the job opportunity.

Recently, the IC3 received information from radio stations, reporting they had been contacted via e-mail by an individual wanting to run advertising on their radio stations. The individual wanted to purchase radio spots to promote a mystery shopper program. The radio stations received signed confirmations and payments, via credit cards, which cleared. The radio stations ran the ads and, shortly after, began receiving complaints from listeners who had been scammed by the offer. Listeners advised they received a check and were instructed to cash it immediately. After deducting $450 for their commission, they were told to wire the difference to a third party. Later, the check was identified as counterfeit by the financial institution. In addition, the credit card used to pay for the ads was later identified as being compromised.

GOVERNMENT OFFICIALS' IDENTITIES BEING USED ON SOCIAL NETWORKING SITES

The IC3 has seen an increase of the use of names and photos of U.S. government officials by fraudsters to set-up fraudulent social networking profiles. The scam entails the fraudster creating an account by using the government official's name and a copy of the official's portrait image available online. The fraudsters then use these accounts to appear reputable and successfully befriend potential victims. Then, the fraudster expresses a romantic interest and begins to ask for money. Often the fraudster implies that they are overseas for important work and that a family member has fallen ill. Sometimes, the victims are encouraged to apply for work-at-home jobs posted online. Victims end up repeatedly wiring funds to the fraudster, believing they are involved in a genuine relationship.

The IC3 has released several Public Service Announcements (PSA) warning consumers that U.S. government officials have been repeated targets of spam and identity theft. To address the volume of these particular scams, which use the FBI and government agencies and officials' names, the IC3 added a link titled "FBI E-mail Scam Alert" to the LooksTooGoodToBeTrue.com home page a few years ago. The link contains several IC3 PSA's addressing these particular scams.

MODELING SCAM

The IC3 has received several complaints from individuals reporting modeling scams. Complainants reported receiving unsolicited e-mails offering them a modeling position, while others reportedly responded to advertisements offering modeling jobs from what appeared to be reputable modeling agencies.

Those who received the unsolicited e-mails reported that the e-mail contained a link to what appeared to be a website for a legitimate modeling agency. The recipient was instructed to click the link to log on and create an account. Afterwards, the recipient reportedly realized the link was to a fraudulent website and that their computer was possibly infected with a keylogger as a result.

Other complainants reported they were told they would make $7,000 for a photo shoot. However, they were asked to first pay "fees" up front which covered registration, licensing, clothes, photos, etc. Victims were instructed to wire their fees. Once the fees were wired, complainants were requested to pay additional fees, but were promised they would be paid half of their salary up front before the photo shoot.

E-MAIL PURPORTEDLY FROM THE FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

The IC3 has received several complaints from individuals who reported they received an unsolicited e-mail claiming to be from the FDIC. The e-mail notifies the recipient that their ACH and wire transactions have been suspended due to expiration, and instructs the recipient to download and install the newest updates by clicking on a link. Clicking the link actually downloads malicious software onto the user's computer.

The FDIC has posted the following two alerts:

http://www.fdic.gov/consumers/consumer/alerts/index.html

> ***E-mail Claiming to Be From the FDIC - August 30, 2011***
>
> *The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent e-mails that have the appearance of being from the FDIC.*
>
> *The e-mails appear to be sent from a "no.reply@fdic.gov" e-mail address.*
>
> *The e-mails have a subject line that read: "FDIC Notification."*

The fraudulent e-mails are addressed to "Dear customer" and state "Your account ACH and Wire transactions have been temporarily suspended for security reasons due to the expiration of your security version. To download and install the newest installations read the document(pdf) attached below. As soon as it is set up, your transaction abilities will be fully restored."

The message concludes with, "Best regards, Online security department, Federal Deposit Insurance Corporation."

The e-mails include an attachment named "FDIC_document.zip." The e-mails and attachments are fraudulent and were not sent by the FDIC. Recipients should consider the intent as an attempt to collect personal or confidential information, or to load malicious software onto end users' computers. Recipients should NOT open the attachment.

Financial institutions and consumers should be aware that other subject lines and modifications to the e-mails may occur over time. The FDIC does not directly contact consumers in this manner nor does the FDIC request personal financial information from consumers.

E-mail Claiming to Be From the FDIC - July 14, 2011

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent e-mails that have the appearance of being from the FDIC.

The e-mails appear to be sent from various "@fdic.gov" e-mail addresses, such as "protection@fdic.gov," "admin@administration.fdic.gov," or "service@admin.fdic.gov."

The messages have various subject lines that read: "Update for your banking account" or "ACH and Wire transfers disabled," and "Banking security update."

*The fraudulent e-mails are addressed to "Dear clients" and state "Your account **ACH and Wire transactions** have been **temporarily suspended** for your Security, due to the expiration of your security version. To download and install the newest Updates, follow this **link**. As soon as it is set up, your transaction abilities will be fully restored."*

The message concludes with, "Best regards, Online security department, Federal Deposit Insurance Corporation."

These e-mails and links are fraudulent and were not sent by the FDIC. Recipients should consider the intent of these e-mails as an attempt to collect personal or confidential information, or to load malicious software onto end users' computers. Recipients should NOT access the link provided within the body of the e-mails and should NOT, under any circumstances, provide any personal financial information through this media.

Financial institutions and consumers should be aware that other subject lines and modifications to the e-mails may occur over time. The FDIC does not directly contact consumers in this manner nor does the FDIC request personal financial information from consumers.