INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
SEPTEMBER 1, 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.

"MASS JOINDER LAWSUITS" PROMISING HOME MORTGAGE RELIEF

The IC3 has received several complaints from individuals who reported they received a letter stating they were a potential plaintiff in a "Mass Joinder" lawsuit being filed by a law firm located in California, against their mortgage companies. Consumers stated they were requested to pay non-refundable, upfront fees of $2,000 to $5,000. The law firm made a wide variety of claims and sales pitches and offered legal and litigation services, with the goal of taking money from the victim.

Lawyers seeking plaintiffs to join a class for a class action lawsuit do not seek up front commission from their class clients. Class action lawyers are typically paid on a contingency basis. In a contingency fee arrangement, an attorney receives approximately 40% of any judgment or settlement amount obtained on the client's behalf.

Warnings have been posted on-line regarding "Mass Joinder" by the California Department of Real Estate; the Better Business Bureau; as well as consumers who have been scammed and posted their experiences, insights, and warnings.

ON-LINE AUCTION SITE PLAYSTATION BUNDLE AD SCAM

The IC3 has received several complaints from individuals who reported they received an unsolicited e-mail stating their ad for a Sony Playstation 3 Metal Gear Solid 4 PS3 80 GB Bundle has been posted and a confirmation number was enclosed for the posting. In each instance the victim claimed they did not place an ad on an on-line auction site for the Sony Playstation Bundle. Some victims stated they did not even have an on-line auction account.

Warnings have been posted on-line to beware of auction site phishing e-mail scams and specifically mention the above-mentioned scam. One warning indicated the scam was first reported in January 2009.

FRAUD TRENDS AFFECTING THE ECOMMERCE COMMUNITY

Ethoca recently provided the IC3 information pertaining to the increase in fraud attempts incurred by on-line merchants. Ethoca was founded under the concept of safely sharing transaction data to fight on-line credit card fraud. The company serves as a data sharing platform for merchants to stop on-line fraud and is partnered with the National Cyber Forensics and Training Alliance (NCFTA). The data received by Ethoca remains private and is only used for fraud prevention. The following information is based on Ethoca's data collection and information sharing process.

ADVISORY ON MILITARY ADDRESSES

On 07/11/2011, the hacker group Anonymous posted 90,000 e-mail addresses and passwords. As a result of this posting, merchants have reported some orders containing military e-mail addresses have been identified as fraudulent. Until this time, military e-mail addresses typically meant an order was less likely to be fraudulent. The increase in fraud orders has happened within the last 30 days.

E-MAIL ADDRESS TUMBLING

E-mail address tumbling has been around for awhile and fraudsters have used it for many years. On the other side, good consumers utilize address tagging to identify orders.

The purpose of e-mail tagging is to allow consumers to have one e-mail address for every purpose. The attractive feature of e-mail tagging is it allows the consumer to vary their e-mail address to help differentiate when placing orders, shopping, working, schooling, etc., but automatically forwards to the primary e-mail address. This feature on Gmail works in two ways, either with a period or a plus sign. The period works by allowing the consumer to take an e-mail address, JohnDoe@gmail.com, and add as many periods as the consumer wants to the e-mail address, JohnDoe.....@gmail.com, J.o.h.n.D.o.e@gmail.com, etc.

The feature most often used is the + feature, which allows a user to add additional tags to their e-mail address to easily identify how someone obtained their name. Using the above example, when shopping on-line, a consumer can tag their e-mail as JohnDoe+081811OnlineRetailerName@gmail.com. This allows the user to know they shopped on-line with a merchant on that specific day.

These features can be used in combination with rules to route e-mails into different boxes, keeping inbox e-mail volume down, and helping users be more efficient.

Fraudsters have figured out this tip and use what has been termed e-mail address tumbling, so the fraudster does not have to create unique user accounts for their many fraud attempts. So far these features have only been found to work with Gmail accounts.