INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
FEBRUARY 17, 2012

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

MYSTERY SHOPPER SCAM TO EVALUATE WIRE TRANSFER SERVICES

The IC3 has recently received over 250 complaints reporting a new twist to the online employment scam. The scam involves individuals who responded to online ads or were contacted via e-mail as a result of their resume being posted on job websites. The perpetrator posed as a research company and requested participants to complete a paid survey regarding services provided at wire transfer locations to improve the effectiveness of the company's money-transfer services.

Complainants were hired and then mailed a cashier's check or money order. They received instructions to cash the check/money order at their local bank, keep a portion as payment, and wire the remaining amount via wire transfer to a designated recipient. Victims were then asked to immediately e-mail their employer with the transfer number, amount wired, recipient's name and address, and the name of the wire transfer location evaluated. Upon sending the information, victims received a questionnaire form regarding their overall wire transfer experience to complete and return. Those who did not promptly follow through with the instructions received threatening e-mails stating if they did not respond within 24 hours, their information would be forwarded to the FBI and they could face 25 years in jail.

Shortly after the transactions, victims were informed by their banks that the checks were counterfeit and were held responsible for reimbursing their banks. Most victims owed their bank over $2,500.

SPAM REFERENCING U.S. MILITARY MEMBERS AND GADDAFI

Criminals continue to explore new avenues to lure victims, most recently by claiming to be a US military contractor, who was performing reconstruction work in Libya. Fraudsters sent unsolicited e-mails claiming that several metal boxes were found in cellars of high-rise buildings built and occupied by Muammar Gaddafi. Each box purportedly contained large sums of money, in addition to guns, armor, bullets, and drugs. The e-mails requested the recipient’s assistance with transferring the money out of Libya. The fraudsters also told the e-mail recipients that they were expected to receive, secure, and protect the boxes until the overseas assignment elapsed and promised the victims a 30 percent profit.

Often times in online scams, once communication with the fraudsters begins, they will request personal information, including but not limited to bank account details, claiming funds are needed to cover various expenses.

Be wary of any unsolicited e-mail, especially those requesting personal information or soliciting the submission of money for any reason. Unsolicited e-mails should not be opened, as they often contain viruses or other malicious software.

POX PARTY ONLINE ADVERTISEMENTS

Recently, the IC3 received a complaint from an individual reporting an advertisement on a social media site that offered ways to obtain "natural immunity" from the chickenpox by sharing lollipops licked by children infected with the virus. Parents have been known to take their child to a "Pox Party" as an alternative to vaccinating children from varicella, otherwise

known as chickenpox, but sending virus-covered lollipops through the mail is against Federal law.

One individual posted a message stating "fresh batch of pox in Nashville shipping of suckers, spit, and Q-tips available tomorrow 50 dollars."

As a disclaimer, the social media site posted the following notice on their page:

> "This page has never condoned the mailing of infectious diseases. For our members: The mailing of infectious items, such as lollipops, rags, etc, is a federal offense. This page is not private and can been seen by members and non members alike. You may post on the page that you have the pox and are willing to share in YOUR AREA but please keep your specifics in private messages between members. Again, this page can be seen by anyone and mailing is a federal offense. We are all intelligent adults but these guidelines will help protect your privacy."

According to the Center for Disease Control's (CDC) website, www.cdc.gov, chickenpox is spread in the air when an infected person coughs or sneezes. It can also be spread by touching or breathing in the virus particles that come from the chickenpox blisters. The CDC also discourages chickenpox parties because the disease can be serious. Dangerous diseases like hepatitis A and strep can be transmitted via saliva according to the CDC's website. Therefore, not only is the contaminated candy not likely to provide exposure to chickenpox, it could expose children to an entirely different disease.