INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
MAY 26, 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.

FRAUD SURROUNDING THE LATEST NEWS EVENTS OF THE MOMENT

When a major news story breaks, it is typical for fraudsters to attempt to capitalize on the event. As a result, the IC3 has been monitoring its complaint database for possible scams related to the recent death of Osama bin Laden. Various scams have been identified; however, many complainants are becoming more aware of such scams and not participating in these schemes.

One such scam identified is cross-site scripting (XSS), which allows an attacker to execute code on the target website from a user's browser via crafted values in the target site's URL, web forms, or in cases where sites allow users to place material directly in posted content. Recently, social networking site users have fallen victim to "self" infecting XSS attacks where they actually perform the attack themselves by following directions to view the latest Osama bin Laden video. Before users can view the video, they must complete a "5 second security check." A few keyboard shortcuts allow users to cut and paste malicious code directly into their browser's URL without any indications it is a viral scam.

SCAMS MISREPRESENTING THE FINANCIAL CRIMES ENFORCEMENT NETWORK OF THE UNITED STATES (U.S.) DEPARTMENT OF THE TREASURY

Perpetrators commonly use various government agencies or officials to legitimize their scams. Most recently, the IC3 has received several complaints which fraudulently represent the Financial Crimes Enforcement Network of the U.S. Department of the Treasury.

Victims reported they received an e-mail claiming to be from the U.S. Department of the Treasury stating their lost funds, which were stolen and diverted to a foreign account registered in their name, have been recovered. The e-mail advised to cease all money transactions, especially overseas, and to respond to the e-mail so the lost funds could be returned. The e-mail further stated the U.S. government is making adequate arrangements to ensure outstanding beneficiaries receive their funds. The e-mail is signed by James H. Freis, Deputy Director of the Financial Crimes Enforcement Network, and requires victims to provide personally identifiable information that could potentially result in identity theft.

The U.S. Department of the Treasury posted a scam alert on their website on April 13, 2011, stating they do not send unsolicited requests and do not seek personal or financial information from members of the public by e-mail and recommending that recipients not respond to such messages. The alert further provides links for victims to report solicitations claiming to be from the U.S. Treasury.