INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS

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.

ROMANCE SCAMMERS CLAIMING AFFILIATION WITH THE IC3

The IC3 has received several complaints regarding a romance scam originating via a dating website. Generally, in romance scams, the subject claims to be out of the country for a business trip and in need of money. The subject asks potential victims to wire funds for various reasons including paying for a hotel, returning to the states, or paying for a lawyer.

Recently, the scammers have added a layer of supposed law enforcement involvement in an attempt to convince the victim the scam is legitimate. In one such IC3 complaint, the "investigator" says he is using his private e-mail because the IC3 database is under maintenance. To convince the victim to wire the requested funds, he claims to be assigned to the case and assures the victim that the subject has been "interrogated and investigated" and that he is a safe, "legit business man."

Other complainants reported having difficulty canceling their membership to the particular dating site, which reportedly offers a "3-day free membership" for their service. The membership is reportedly "automatically" renewed after the three days unless canceled. Complainants reported that the website renewed their membership and charged their credit card over $59 despite the complainant's attempts to cancel the membership. Some complainants said the company did not answer their calls, e-mails, or voice mail messages, while others claimed the company admitted the "error" and offered them free service, but refused to refund the charges.

PHISHING E-MAIL CLAIMS "YOUR FEDERAL TAX PAYMENT WAS REJECTED"

In October 2010, articles were posted online warning consumers about phishing e-mails purportedly from the Electronic Federal Tax Payment System (EFTPS) claiming the recipient's federal tax payment was rejected. The IC3 has received over 150 complaints reporting this matter. Although different versions of this spam campaign exist, many complainants reported that the e-mails they received were titled "*LAST NOTICE: Your Federal Tax Payment has been rejected.*" E-mails stated, "*the problem is that system doesn't process your company ID on holidays and we moved your tax payment batch to a waiting list.*" Recipients were then directed to click on the link provided to obtain more details about their company's status and tax payment batch file. Some complainants reportedly use the electronic system to pay their estimated quarterly taxes, so the e-mail appeared relevant.

Other related phishing e-mails claimed, "*the identification number used in the Company Identification Field is not valid.*" Recipients were directed to visit hxxp://eftps.gov/r21 and "*check the information and refer to Code R21 to get details about your company payment in transaction contacts section.*"

A recent complaint filed with the IC3 reported the same type of phishing e-mail except this time, the e-mail directed the recipient to open an attachment contained in the e-mail. The e-mail was titled "*Your Federal Tax Payment Notice.*" Like the others, it claimed, "*the identification number used in the Company Identification Field is not valid.*" To entice the recipient to open the attachment, the e-mail stated, "*check the attached information and refer to Code R21 to get details about your company payment in transaction contacts section.*"

TELEPHONE SCAM OFFERING VIRUS REMOVAL SERVICES TO GAIN REMOTE ACCESS TO VICTIMS' COMPUTERS

The IC3 has received several complaints from victims who reported a telephone scam in which the caller purports to be an employee of a major online company, which develops, manufactures, and supports software along with other products and services. Victims reported that a caller with an Indian accent claimed their computers were infected with viruses. The caller advised the victims they were sending the viruses to others via the Internet, and instructed victims to go to websites such as hxxp://www.irssupport.net, hxxp://www.go4support.org, hxxp://www.teche4pc.com, and hxxp://www.ammyy.com. When the victims navigated to one of the websites, they were further instructed to click on live support or live connect for assistance in removing the viruses. Some victims were instructed to download a program once they were on the hxxp://www.ammyy.com website. After the victim clicked on the link or downloaded the program, the caller gained control of the victim's computer. Victims watched as the caller explored personal files, pointing out files that were infected. Some victims reportedly believe the caller copied their files and obtained their personal information. In some cases, the caller tried to sell the victims' software. Many victims reported loud background noise during the call, indicating a possible boiler room-type operation. Some victims reported the scam to the online software company. The company has an alert on their website warning consumers about this matter.

For more information regarding online scams visit our Press Room page for the most current Public Service Announcements.

https://www.ic3.gov/media/default.aspx