

## Investigative Programs Cyber Investigations

How to Report E-Scams and Hoaxes to the FBI

### New E-Scams & Warnings

#### RENTAL AND REAL ESTATE SCAMS

03/12/10—Individuals need to be cautious when posting rental properties and real estate on-line. The IC3 continues to receive numerous complaints from individuals who have fallen victim to scams involving rentals of apartments and houses, as well as postings of real estate online.

Rental scams occur when the victim has rental property advertised and is contacted by an interested party. Once the rental price is agreed-upon, the scammer forwards a check for the deposit on the rental property to the victim. The check is to cover housing expenses and is, either written in excess of the amount required, with the scammer asking for the remainder to be remitted back, or the check is written for the correct amount, but the scammer backs out of the rental agreement and asks for a refund. Since the banks do not usually place a hold on the funds, the victim has immediate access to them and believes the check has cleared. In the end, the check is found to be counterfeit and the victim is held responsible by the bank for all losses.

Another type of scam involves real estate that is posted via classified advertisement websites. The scammer duplicates postings from legitimate real estate websites and reposts these ads, after altering them. Often, the scammers use the broker's real name to create a fake e-mail, which gives the fraud more legitimacy. When the victim sends an e-mail through the classified advertisement website inquiring about the home, they receive a response from someone claiming to be the owner. The "owner" claims he and his wife are currently on missionary work in a foreign country. Therefore, he needs someone to rent their home while they are away. If the victim is interested in renting the home, they are asked to send money to the owner in the foreign country.

If you have been a victim of Internet crime, please file a complaint at <http://www.IC3.gov/>.

---

#### NEW TWIST ON COUNTERFEIT CHECK SCHEMES TARGETING U.S. LAW FIRMS

01/21/10—The FBI continues to receive reports of counterfeit check schemes targeting U.S. law firms. As previously reported, scammers send e-mails to lawyers, claiming to be overseas and seeking legal representation to collect delinquent payments from third parties in the U.S. The law firm receives a retainer agreement, invoices reflecting the amount owed, and a check payable to the law firm. The firm is instructed to extract the retainer fee, including any other fees associated with the transaction, and wire the remaining funds to banks in Korea, China, Ireland, or Canada. By the time the check is determined to be counterfeit, the funds have already been wired overseas.

In a new twist, the fraudulent client seeking legal representation is an ex-wife "on assignment" in an Asian country, and she claims to be pursuing a collection of divorce settlement monies from her ex-husband in the U.S. The law firm agrees to represent the ex-wife, sends an e-mail to the ex-husband, and receives a "certified" check for the settlement via delivery service. The ex-wife instructs the firm to wire the funds, less the retainer fee, to an overseas bank account. When the scam is executed successfully, the law firm wires the money before discovering the check is counterfeit.

All Internet users need to be cautious when they receive unsolicited e-mails. Law firms are advised to conduct as much due diligence as possible before engaging in transactions with parties who are

handling their business solely via e-mail, particularly those parties claiming to reside overseas.

Please view an additional public service announcement posted to the IC3 web site regarding a similar Asian extortion scheme located at the following link, <http://www.ic3.gov/media/2009/090610.aspx>. Individuals who receive information pertaining to counterfeit check schemes are encouraged to file a complaint at [www.IC3.gov](http://www.IC3.gov).