



United States Department of Justice Federal Bureau of Investigation

October 16, 2006

FBI, SPRINGFIELD DIVISION
<http://springfield.fbi.gov>

Internet Fraud and other forms of Cyber Crime are a growing problem for consumers and law enforcement. The Internet Crimes Complaint Center (IC3), receives more than 18,000 complaints each month from consumers. Whether they are new scams, or old scams with a new twist, these attempts to separate consumers from their hard earned money are circulating in cyberspace with increased regularity. Therefore, it is important for law enforcement to increase and maintain public awareness regarding the types of scams which are prevalent and provide consumers with the tools to identify scams and avoid being victimized.

COUNTERFEIT CHECK SCHEMES

One of the more common scams currently being reported is the counterfeit check scam. This scam is often committed in conjunction with the buying and selling of goods over the internet. The scammer will express an interest in buying something that the victim is advertising for sale. The victim will receive a cashier's check or money order as payment for the merchandise. However, the check is payable for an amount above the sale price of the merchandise. The scammer will fabricate an explanation for why the check is for an amount above and beyond the price of the merchandise, such as to pay shipping costs through a third party. The scammer asks the victim to deposit the check and wire the excess funds to the scammer, or another person. The victim feels comfortable doing this for two reasons:

1. Consumers and banks treat cashier's checks like cash, without waiting for the check to clear before utilizing the funds; and
2. The victims believe they are only wiring the "excess" funds, while keeping the amount necessary to pay for the merchandise which was sold.

However, the fact that the bank may release the funds before the check clears does not mean that the check is authentic. These scams involve counterfeit checks, which may not be apparent by examining the check. By the time the bank determines that the check is counterfeit, the victim has already wired money to the scammer. Or worse, the scammer may attempt to cancel the transaction and convince the victim to

wire the entire amount of the check back to the scammer.

This counterfeit check scheme has also been used in conjunction with the sweepstakes or lottery scheme. Instead of asking the victim to pay certain fees for the purpose of receiving their “winnings,” as in the traditional sweepstakes/lottery scam, the scammer will send the counterfeit check and ask the victim to deposit the check and wire the fees or taxes back to the scammer.

Protecting Yourself

The success of this scam is dependant on the scammer convincing the victim to wire money before the check is discovered to be fraudulent.

- There is no legitimate reason for someone who is buying something to send a check for an amount above the sale price. This is a red flag.
- *Urgency* is a common theme used by scammers. The scammer needs the victim to act before taking the time to carefully analyze the situation and verify the authenticity of the check. Urgency is a red flag.
- Consumers can *verify* the authenticity of a cashier’s check by contacting the financial institution on which the check is drawn. However, do not rely on information printed on the check. Some criminal groups are creating toll free telephone numbers and using legitimate bank logos for the purpose of check verification. If the check appears to be drawn on the ABC Bank, locate a telephone number for ABC Bank from a reliable source to verify the check.

PHISHING

Phishing is a form of identity theft which uses e-mail and malicious web sites to obtain personal information. Phishing has become the leading type of internet-based fraud. The typical phishing attack involves the scammer sending the victim an e-mail message, which appears to be from a legitimate business. The e-mail message requests the victim to update, or verify, personal information by clicking on a link in the e-mail message. This link will take the victim to what appears to be a legitimate company web page. However, the web page is actually a well designed phony web page, which only looks authentic . When the victim enters personal information into the web page, the victim is actually supplying information directly to the scammer.

The most frequently targeted industry by phishing schemes continues to be financial institutions, accounting for approximately 90% of all phishing attacks. The scammer e-mail message offers what may sound like a plausible explanation for why the victim needs to update, or verify, account information. Reasons used in the past by phishing scams include a warning of fraudulent activity on the customer’s account which necessitates account verification, or a scheduled software upgrade. A recent

phishing scam offered a \$50.00 account credit to the victim for simply participating in a short online survey. The scammers are copying and using official bank logos to make the e-mail messages and fake web pages appear authentic. Some of the phishing schemes are providing a telephone number for account verification, rather than a web page link. This is simply another means of obtaining the victim's personal information. Customers of internet service providers, eBay, and PayPal have also been targeted by phishing scams.

Scammers are always trying to find new ways to steal personal information, including a new form of phishing called vishing. Vishing schemes are using voice over internet protocol (VoIP) to obtain personal information. Instead of directing consumers to a fake web site to electronically enter their personal information, the scammer provides a telephone number (VoIP) for the victim to use to update, or verify, account information. The vishing scheme is relying on the fact that it is not unusual for consumers to conduct business transactions over the telephone. Banking by phone has been available for years.

Protecting Yourself

The success of phishing schemes is dependent on tricking victims into providing personal information to the scammer. This is typically accomplished by tricking the victim into following a web link supplied by the scammer in the e-mail message, which takes the victim to a fake webpage, where the victim may enter personal information. In the alternative, the phishing e-mail message may contain a telephone number, possibly even a toll free number, which the victim is tricked into calling to provide personal information.

- Internet users should not utilize links or telephone numbers contained within an e-mail message for the purpose of providing personal information, whether under the guise of account verification or otherwise. Financial institutions and other businesses already have their customers' account numbers, and will never ask for that type of information electronically;
- Consumers may verify that e-mail messages or telephone calls are authentic by contacting the company directly, using a telephone number known to be legitimate. Consumers should contact their financial institution using the telephone number on their bank statement. Consumers should contact their credit card company using the telephone number on the back of their credit card;
- Protect your computer with anti-virus software and a firewall. Keep them up to date.

Other Resources

- **Internet Crime Complaint Center (IC3):** www.ic3.gov
 - IC3 is a centralized complaint center for all federal internet related criminal complaints, including fraud, computer intrusions, and crimes against children. These complaints are forwarded to the appropriate local, state, or federal agency for action.

- **Identity Theft Hotline:** www.consumer.gov/idtheft
[1-877-ID-THEFT \(1-877-438-4338\)](tel:1-877-ID-THEFT)
 - The Federal Trade Commission (FTC) offers a hotline specifically for Identity Theft complaints.

- **Phonebusters:** www.phonebusters.com
[1-888-495-8501](tel:1-888-495-8501)
 - Phonebusters is a centralized complaint center for Canadian based telemarketing fraud complaints. Lottery/sweepstakes scams are a common Canadian based fraud complaint. The victims, often elderly, are advised they have won money, but need to pay certain fees or taxes before receiving their winnings. No legitimate lottery or sweepstakes requires a winner to pay money as a condition of receiving a prize.

- **“Do Not Call” Registry:** www.donotcall.gov
[1-888-382-1222](tel:1-888-382-1222)
 - The National Do Not Call Registry is free and easy to use. Anyone who wants to reduce the number of telemarketing calls received at home may register online, or over the telephone. If registering by telephone, make the call from the telephone line you want registered.

- **Opt Out:** [1-888-5-OPTOUT \(1-888-567-8688\)](tel:1-888-5-OPTOUT)
 - The credit bureaus offer a toll-free number that enables consumers to opt out of pre-approved credit offers, for a period of two years. Also, many businesses and organizations offer an opt out feature which limits the amount of personal information that will be shared with other businesses for promotional purposes.

Contact:

Marshall Stone, FBI, Springfield
Supervisory Special Agent/Media Coordinator
(217)522-9675