New E-Scams & Warnings

To report potential e-scams, please go the **Internet Crime Complaint Center and file a report**. Note: the FBI does not send mass e-mails to private citizens about cyber scams, so if you received an e-mail that claims to be from the FBI Director or other top official, it is most likely a scam.

If you receive unsolicited e-mail offers or spam, you can forward the messages to the Federal Trade Commission at spam@uce.gov.

Below are some recent scams and warnings.

Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money

11/30/12—A new extortion technique is being deployed by cyber criminals using the Citadel malware platform to deliver Reveton ransomware. The latest version of the ransomware uses the name of the Internet Crime Complaint Center to frighten victims into sending money to the perpetrators. In addition to instilling a fear of prosecution, this version of the malware also claims that the user's computer activity is being recorded using audio, video, and other devices.

As described in prior alerts on this malware, it lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States Federal Law. The message further declares that a law enforcement agency has determined that a computer using the victim's IP address has accessed child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine using prepaid money card services. The geographic location of the user's PC determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud.

This is not a legitimate communication from the IC3, but rather is an attempt to extort money from the victim. If you have received this or something similar do not follow payment instruction.

It is suggested that you:

- File a complaint at www.IC3.gov;
- Keep operating systems and legitimate antivirus and antispyware software updated; and
- Contact a reputable computer expert to assist with removing the malware.

Smartphone Users Should be Aware of Malware Targeting Mobile Devices and Safety Measures to Help Avoid Compromise

10/12/12—The IC3 has been made aware of various malware attacking Android operating systems for mobile devices. Some of the latest known versions of this type of malware are Loozfon and FinFisher. Loozfon is an information-stealing piece of malware. Criminals use different variants to lure the victims. One version is a work-at-home opportunity that promises a profitable payday just for sending out e-mail. A link within these advertisements leads to a website that is designed to push Loozfon on the user's device. The malicious application steals contact details from the user's address book and the infected device's phone number.

FinFisher is a spyware capable of taking over the components of a mobile device. When installed the mobile device can be remotely controlled and monitored no matter where the Target is located. FinFisher can be easily transmitted to a smartphone when the user visits a specific web link or opens a text message masquerading as a system update.

Loozfon and FinFisher are just two examples of malware used by criminals to lure users into compromising their devices.

Safety tips to protect your mobile device:

- When purchasing a smartphone, know the features of the device, including the default settings. Turn off features of the device not needed to minimize the attack surface of the device.
- Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in the case of loss or theft.
- With the growth of the application market for mobile devices, users should look at the reviews of the developer/company who published the application.
- Review and understand the permissions you are giving when you download applications.
- Passcode protect your mobile device. This is the first layer of physical security to protect the contents of the device. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
- Obtain malware protection for your mobile device. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that enable geo-location. The application will track the user's location anywhere. This application can be used for marketing, but can also be used by malicious actors, raising concerns of assisting a possible stalker and/or burglaries.
- Jailbreak or rooting is used to remove certain restrictions imposed by the device manufacturer or cell phone carrier. This allows the user nearly unregulated control over what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the attack surface of the device. Anytime an application or service runs in "unrestricted" or "system" level within an operation system, it allows any compromise to take full control of the device.
- Do not allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Smartphones require updates to run applications and firmware. If users neglect this, it increases the risk of having their device hacked or compromised.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.

If you have been a victim of an Internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at www.IC3.gov.

Lawyers' Identities Being Used for Fake Websites and Solicitations

09/14/12—A recent scam has surfaced in which the identify of a Texas attorney, who had not practiced in years, was used to set up a fake law firm website using the attorney's maiden name, former office address, and portions of her professional biography. Other attorneys have complained about the use of their names and professional information to solicit legal work. All attorneys should be on the alert to this scam. If you become aware of the same or a similar situation involving your name and/or law firm, you should immediately report the incident to local authorities, your state Bar, and the FBI at the Internet Crime Complaint Center. Additionally, be sure to closely monitor your credit report or bank accounts to ensure that your identity is not the only thing being stolen. If you have been a victim of an Internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at www.IC3.gov.

Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money

08/07/12—The IC3 has been made aware of a new Citadel malware platform used to deliver ransomware named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States federal law. The message further declares the user's IP address has been identified by the Federal Bureau of Investigation as visiting websites that feature child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the U.S. Department of Justice using a prepaid money card service. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar, do not follow payment instructions. Infected computers may not operate normally. If your computer is infected, you may need to contact a local computer expert for assistance to remove the malware.

It is suggested that you:

- File a complaint at www.IC3.gov.
- Seek out a local computer expert to assist with removing the malware.

Related story
New Internet Scam: Ransomware Locks Computers, Demands Payment

---

Citadel Malware Delivers Reveton Ransomware in Attempts to Extort Money

05/30/12—The IC3 has been made aware of a new Citadel malware platform used to deliver ransomware, named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States federal law. The message further declares the user's IP address was identified by the Computer Crime & Intellectual Property Section as visiting child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a $100 fine to the U.S. Department of Justice using prepaid money card services. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar, do not follow payment instructions.

It is suggested that you:

- Contact your banking institutions.
- File a complaint at www.IC3.gov.

Malware Installed on Travelers' Laptops Through Software Updates on Hotel Internet Connections

05/08/12—Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while they are establishing an Internet connection in their hotel rooms.

Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to set up the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

The FBI recommends that all government, private industry, and academic personnel who travel abroad take extra caution before updating software products through their hotel Internet connection. Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor may reveal an attempted attack. The FBI also recommends that travelers perform software updates on laptops immediately before traveling, and that they download software updates directly from the software vendor's website if updates are necessary while abroad.

Anyone who believes they have been a target of this type of attack should immediately contact their local FBI office and promptly report it to the IC3's website at www.IC3.gov. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The complaint information is also used to identify emerging trends and patterns.

U.S. Law Firms Continue to be the Target of Counterfeit Check Scheme

03/12/12—The IC3 continues to receive reports of counterfeit check schemes targeting U.S. law firms. The scammers contact lawyers via e-mail, claiming to be overseas and requesting legal representation in collecting a debt from third parties located in the U.S. The law firms receive a retainer agreement and a check payable to the law firm. The firms are instructed to deposit the check, take out retainer fees, and wire the remaining funds to banks in China, Korea, Ireland, or Canada. After the funds are wired overseas, the checks are determined to be counterfeit.

In a slight variation of the scheme's execution, the victim law firm receives an e-mail from what appears to be an attorney located in another state requesting assistance for a client. The client needs aid in collecting a debt from a company located in the victim law firm's state. In some cases, the name of the referring attorney and the debtor company used in the e-mail were verified as legitimate entities and were being used as part of the scheme. The law firm receives a signed retainer agreement and a check made payable to the law firm from the alleged debtor. The client instructs the law firm to deposit the check and to wire the funds, minus all fees, to an overseas bank account. The law firm discovers after the funds are wired that the check is counterfeit.

Law firms should use caution when engaging in transactions with parties who are handling their business solely via e-mail, particularly those parties claiming to reside overseas. Attorneys who agree to represent a client in circumstances similar to those described above should consider incorporating a provision into their retainer agreement that allows the attorney to hold funds received from a debtor for a sufficient period of time to verify the validity of the check.

If you have been a victim of an internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at www.IC3.gov.

New Variation on Telephone Collection Scam Related to Delinquent Payday Loans

02/21/12—The Internet Crime Complaint Center (IC3) continues to receive complaints from victims of payday loan telephone collection scams. As previously reported in December 2010, the typical payday loan scam involves a caller who claims the victim is delinquent on a payday loan and must make payment to avoid legal consequences.

Callers pose as representatives of the FBI, "Federal Legislative Department," various law firms, or other legitimate-sounding agencies and claim to be collecting debts for companies such as United Cash Advance, U.S. Cash Advance, U.S. Cash Net, or other Internet check-cashing services. The fraudsters relentlessly call the victim's home, cell phone, and place of employment in attempts to obtain payment. The callers refuse to provide information regarding the alleged payday loan or any documentation and become verbally abusive when questioned.

The IC3 has observed variations of this scam in which the caller tells the victim that there are outstanding warrants for the victim's arrest. The caller claims that the basis of the warrants is non-payment of the underlying loan and/or hacking. If it's the latter, the caller tells the victim that he or she is wanted for hacking into a business' computer system to steal customer information. The caller will then demand payment via debit/credit card; in other cases, the caller further instructs victims to obtain a prepaid card to cover the payment.

The high-pressure collection tactics used by the fraudsters have also evolved. In one recent complaint, a person posed as a process server and appeared at the victim's job. In another instance, a phony process server came to a victim's home. In both cases, after claiming to be serving a court summons, the alleged process server said the victim could avoid going to court if he or she provided a debit card number for repayment of the loan.

If you are contacted by someone who is trying to collect a debt that you do not owe, you should:

- Contact your local law enforcement agencies if you feel you are in immediate danger;
- Contact your bank(s) and credit card companies;
- Contact the three major credit bureaus and request an alert be put on your file;
- If you have received a legitimate loan and want to verify that you do not have any outstanding obligation, contact the loan company directly;
- File a complaint at www.IC3.gov.

Timeshare Marketing Scams

01/25/12—Timeshare owners across the country are being scammed out of millions of dollars by unscrupulous companies that promise to sell or rent the unsuspecting victims' timeshares. In the typical scam, timeshare owners receive unexpected or uninvited telephone calls or e-mails from criminals posing as sales representatives for a timeshare resale company. The representative promises a quick sale, often within 60-90 days. The sales representatives often use high-pressure sales tactics to add a sense of urgency to the deal. Some victims have reported that sales representatives pressured them by claiming there was a buyer waiting in the wings, either on the other line or even present in the office.

Timeshare owners who agree to sell are told that they must pay an upfront fee to cover anything from listing and advertising fees to closing costs. Many victims have provided credit cards to pay the fees ranging from a few hundred to a few thousand dollars. Once the fee is paid, timeshare owners report that the company becomes evasive—calls go unanswered, numbers are disconnected, and websites are inaccessible.

In some cases, timeshare owners who have been defrauded by a timeshare sales scheme have been subsequently contacted by an unscrupulous timeshare fraud recovery company as well. The representative from the recovery company promises assistance in recovering money lost in the sales scam. Some recovery companies require an up-front fee for services rendered, while others promise no fees will be paid unless a refund is obtained for the timeshare owner. The IC3 has identified some instances where people involved with the recovery company also have a connection to the resale company, raising the possibility that timeshare owners are being scammed twice by the same people.

If you are contacted by someone offering to sell or rent your timeshare, the IC3 recommends using caution. Listed below are tips you can use to avoid becoming a victim of a timeshare scheme:

- Be wary if a company asks you for up-front fees to sell or rent your timeshare.
- Read the fine print of any sales contract or rental agreement provided.
- Check with the Better Business Bureau to ensure the company is reputable.

To obtain more information on Internet schemes, visit www.LooksTooGoodToBeTrue.com.

Anyone who believes they have been a victim of this type of scam should promptly report it to the IC3's website at www.IC3.gov. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration.

Situational Alert Regarding Charitable Contribution Schemes

08/26/11—In light of Hurricane Irene, the public is reminded to beware of fraudulent e-mails and websites claiming to conduct charitable relief efforts. To learn more about avoiding online fraud, please see "Tips on Avoiding Fraudulent Charitable Contribution Schemes" at: http://www.ic3.gov/media/2011/110311.aspx.

Malicious Software Features Usama bin Laden Links to Ensnare Unsuspecting Computer Users

The Internet Crime Complaint Center (IC3) urges computer users to not open unsolicited (spam) e-mails, including clicking links contained within those messages. Even if the sender is familiar, the public should exercise due diligence. Computer owners must ensure they have up-to-date firewall and anti-virus software running on their machines to detect and deflect malicious software.

The IC3 recommends the public do the following:

- Adjust the privacy settings on social networking sites you frequent to make it more difficult for people you know and do not know to post content to your page. Even a "friend" can unknowingly pass on multimedia that's actually malicious software.
- Do not agree to download software to view videos. These applications can infect your computer.
- Read e-mails you receive carefully. Fraudulent messages often feature misspellings, poor grammar, and nonstandard English.
- Report e-mails you receive that purport to be from the FBI. Criminals often use the FBI's name and seal to add legitimacy to their fraudulent schemes. In fact, the FBI does not send unsolicited e -mails to the public. Should you receive unsolicited messages that feature the FBI's name, seal, or that reference a division or unit within the FBI or an individual employee, report it to the Internet Crime Complaint Center at www.ic3.gov.

E-Mails Containing Malware Sent to Businesses Concerning Their Online Job Postings

01/19/2011—Recent FBI analysis reveals that cyber criminals engaging in ACH/wire transfer fraud have targeted businesses by responding via e-mail to employment opportunities posted online.

Recently, more than $150,000 was stolen from a U.S. business via unauthorized wire transfer as a result of an e-mail the business received that contained malware. The malware was embedded in an e-mail response to a job posting the business placed on an employment website and allowed the attacker to obtain the online banking credentials of the person who was authorized to conduct financial transactions within the company. The malicious actor changed the account settings to allow the sending of wire transfers, one to the Ukraine and two to domestic accounts. The malware was identified as a Bredolab variant, svrwsc.exe. This malware was connected to the ZeuS/Zbot Trojan, which is commonly used by cyber criminals to defraud U.S. businesses.

The FBI recommends that potential employers remain vigilant in opening the e-mails of prospective employees. Running a virus scan prior to opening any e-mail attachments may provide an added layer of security against this type of attack. The FBI also recommends that businesses use separate computer systems to conduct financial transactions.

For more information on this type of fraud and prevention tips, please refer to previous public service announcements at the links below:

- http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf
- http://www.ic3.gov/media/2010/WorkAtHome.pdf
- http://www.ic3.gov/media/2009/091103.aspx

Anyone who believes they have been a target this type of attack should immediately contact their financial institutions and local FBI office and promptly report it to the IC3's website at www.ic3.gov. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The IC3 also uses complaint information to identify emerging trends and patterns.

Telephone Collection Scam Related to Delinquent Payday Loans

12/01/2010—The IC3 receives a high volume of complaints from victims of payday loan telephone collection scams. In these scams, a caller claims that the victim is delinquent in a payday loan and must repay the loan to avoid legal consequences. The callers purport to be representatives of the FBI, Federal Legislative Department, various law firms, or other legitimate-sounding agencies. They claim to be collecting debts for companies such as United Cash Advance, U.S. Cash Advance, U.S. Cash Net, and other Internet check cashing services.

One of the most insidious aspects of this scam is that the callers have accurate information about the victims, including Social Security numbers, dates of birth, addresses, employer information, bank account numbers, and names and telephone numbers of relatives and friends. The method by which the fraudsters obtained the personal information is unclear, but victims often relay that they had completed online applications for other loans or credit cards before the calls began.

The fraudsters relentlessly call the victim's home, cell phone, and place of employment. They refuse to provide to the victims any details of the alleged payday loans and become abusive when questioned. The callers threaten victims with legal actions, arrests, and in some cases physical violence if they refuse to pay. In many cases, the callers even resort to harassment of the victim's relatives, friends, and employers.

Some fraudsters instruct victims to fax a statement agreeing to pay a certain dollar amount, on a specific date, via prepaid visa card. The statement further declares that the victim would never dispute the debt.

These telephone calls are an attempt to obtain payment by instilling fear in the victims. Do not follow the instructions of the caller.

If you receive telephone calls such as these, you should:

- Contact your banking institutions;
- Contact the three major credit bureaus and request an alert be put on your file;
- Contact your local law enforcement agencies if you feel you are in immediate danger;
- File a complaint at www.IC3.gov.

Fraudulent Notification Deceives Consumers Out of Thousands of Dollars

11/29/2010—The IC3 continues to receive reports of letters and e-mails being distributed pursuant to prize sweepstakes or lottery schemes. These schemes use counterfeit checks that bear legitimate-looking logos of various financial institutions to fool victims into sending money to the fraudsters.

Fraudsters tell victims they won a sweepstakes or lottery, but to receive a lump sum payout, they must pay the taxes and processing fees upfront. Fraudsters direct individuals to call a telephone number to initiate a letter of instructions. The letter alleges that the victim may elect to take an advance on the winnings to make the required upfront payment. The letter includes a check in the amount of the alleged taxes and fees, along with processing instructions. Ultimately, victims believe they are using the advance to make the required upfront payment, but in reality they are falling prey to the scheme.

The victim deposits the check into their own bank, which credits the account for the amount of the check before the check clears. The victim immediately withdraws the money and wires it to the fraudsters. Afterwards, the check proves to be counterfeit and the bank pulls the respective funds from the victim's account, leaving the victim liable for the amount of the counterfeit check plus any additional fees the bank may charge.

Persons may fall victim to this scheme due to the allure of easy money and the apparent legitimacy of the check the fraudsters include in the letter of instruction. The alleged cash prizes and locations of the financial institutions vary.

Tips to avoid being scammed:

- A federal statute prohibits mailing lottery tickets, advertisements, or payments to purchase tickets in a foreign lottery.
- Be leery if you do not remember entering a lottery or sweepstakes.
- Beware of lotteries or sweepstakes that charge a fee prior to delivering your prize.
- Be wary of demands to send additional money as a requirement to be eligible for future winnings.

If you have been a victim of this type of scam or any other cyber crime, you can report it to the IC3 at www.IC3.gov. The IC3 complaint database links complaints for potential referral to law enforcement for case consideration. Complaint information is also used to identify emerging trends and patterns to alert the public to new criminal schemes.

Holiday Shopping Tips

11/15/2010—This holiday season, the FBI reminds shoppers that cyber criminals aggressively create new ways to steal money and personal information. Scammers use many techniques to fool potential victims, including conducting fraudulent auction sales, reshipping merchandise purchased with stolen credit cards, and selling fraudulent or stolen gift cards through auction sites at discounted prices.

Fraudulent Classified Ads and Auction Sales

Internet criminals post classified ads and auctions for products they do not have and make the scam work by using stolen credit cards. Fraudsters receive an order from a victim, charge the victim's credit card for the amount of the order, then use a separate, stolen credit card for the actual purchase. They pocket the purchase price obtained from the victim's credit card and have the merchant ship the item directly to the victim. Consequently, an item purchased from an online auction but received directly from the merchant is a strong indication of fraud. Victims of such a scam not only lose the money paid to the fraudster, but may be liable for receiving stolen goods.

Shoppers may help avoid these scams by using caution and not providing financial information directly to the seller, as fraudulent sellers will use this information to purchase items for their schemes. Always use a legitimate payment service to ensure a safe, legitimate purchase.

As for product delivery, fraudsters posing as legitimate delivery services offer reduced or free shipping to customers through auction sites. They perpetuate this scam by providing fake shipping labels to the

intercept the packages for nonpayment and the victim loses the money paid for the purchase of the product.

Diligently check each seller's rating and feedback along with their number of sales and the dates on which feedback was posted. Be wary of a seller with 100 percent positive feedback, with a low total number of feedback postings, or with all feedback posted around the same date and time.

Gift Card Scam

Be careful when purchasing gift cards through auction sites or classified ads. It is safest to purchase gift cards directly from the merchant or retail store. If the gift card merchant discovers that your card is fraudulent, the merchant will deactivate the gift card and refuse to honor it for purchases. Victims of this scam lose the money paid for the gift card purchase.

Phishing and Smishing Schemes

In phishing schemes, a fraudster poses as a legitimate entity and uses e-mail and scam websites to obtain victims' personal information, such as account numbers, user names, passwords, etc. Smishing is the act of sending fraudulent text messages to bait a victim into revealing personal information.

Be leery of e-mails or text messages that indicate a problem or question regarding your financial accounts. In this scam, fraudsters direct victims to follow a link or call a number to update an account or correct a purported problem. The link directs the victim to a fraudulent website or message that appears legitimate. Instead, the site allows the fraudster to steal any personal information the victim provides.

Current smishing schemes involve fraudsters calling victims' cell phones offering to lower the interest rates for credit cards the victims do not even possess. If a victim asserts that they do not own the credit card, the caller hangs up. These fraudsters call from TRAC cell phones that do not have voicemail, or the phone provides a constant busy signal when called, rendering these calls virtually untraceable.

Another scam involves fraudsters directing victims, via e-mail, to a spoofed website. A spoofed website is a fake site that misleads the victim into providing personal information, which is routed to the scammer's computer.

Phishing schemes related to deliveries are also rampant. Legitimate delivery service providers neither e-mail shippers regarding scheduled deliveries nor state when a package is intercepted or being temporarily held. Consequently, e-mails informing of such delivery issues are phishing scams that can lead to personal information breaches and financial losses.

Tips

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail with the link to which you are directed and determine if they match and will lead you to a legitimate site.
- Log directly onto the official website for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.
- If you are asked to act quickly, or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.
- Remember if it looks too good to be true, it probably is.

To receive the latest information about cyber scams, sign up for e-mail alerts on this website. If you have received a scam e-mail, please notify the IC3 by filing a complaint at www.ic3.gov.

Involvement in Criminal Activity Through Work-From-Home Scams

10/20/10—Consumers continue to lose money from work-from-home scams that assist cyber criminals move stolen funds. Worse yet, due to their deliberate or unknowing participation in the scams, these individuals may face criminal charges. Work-from-home scam victims are often recruited by organized cyber criminals through newspaper ads, online employment services, unsolicited emails or "spam" ,one and social networking sites advertising work-from-home opportunities. Once recruited, however, rather than becoming an employee of a legitimate business, the consumer is actually a "mule" for cyber criminals who use the consumer's or other victim's accounts to steal and launder money. In addition, the consumer's own identity or account may be compromised by the cyber criminals. More

---

Cyber Criminals Take Over Corporate Accounts

10/20/10—Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered. More

---

Claims of Being Stranded Swindle Consumers Out of Thousands of Dollars

07/01/10—The IC3 continues to receive reports of individuals' e-mail or social networking accounts being compromised and used in a social engineering scam to swindle consumers out of thousands of dollars. Portraying to be the victim, the hacker uses the victim's account to send a notice to their contacts. The notice claims the victim is in immediate need of money due to being robbed of their credit cards, passport, money, and cell phone; leaving them stranded in London or some other location. Some claim they only have a few days to pay their hotel bill and promise to reimburse upon their return home. A sense of urgency to help their friend/contact may cause the recipient to fail to validate the claim, increasing the likelihood of them falling for this scam.

If you receive a similar notice and are not sure it is a scam, you should always verify the information before sending any money.

If you have been a victim of this type of scam or any other Cyber crime, you can report it to the IC3 website at www.IC3.gov. The IC3 complaint database links complaints for potential referral to the appropriate law enforcement agency for case consideration. Complaint information is also used to identity emerging trends and patterns.

Fraudulent Telephone Calls Allow Fraudsters Access to Consumer Financial and Brokerage Accounts

06/21/10—The FBI Newark Division released a warning to consumers concerning a new scheme using telecommunications denial-of-service (TDoS) attacks.

The FBI determined fraudsters compromised victim accounts and contacted financial institutions to change the victim profile information (i.e., e-mail addresses, telephone numbers, and bank account numbers).

The TDoS attacks used automated dialing programs and multiple accounts to overwhelm victims' cell phones and land lines with thousands of calls. When victims answered the calls they heard dead air (nothing on the other end), an innocuous recorded message, advertisement, or a telephone sex menu. Calls were typically short in duration but so numerous that victims changed their phone numbers to terminate the attack.

These TDoS attacks were used as a diversion to prevent financial and brokerage institutions from verifying victim account changes and transactions. Fraudsters were afforded adequate time to transfer funds from victim brokerage and financial online accounts.

Protection from TDoS attacks and other types of fraud requires consumers to be vigilant and proactive. In Newark's Public Service Announcement (PSA), they recommend the following guidelines for consumers to protect themselves:

- Implement security measures for all financial accounts by placing fraud alerts with the major credit bureaus if you believe they were targeted by a TDoS attack or other forms of fraud.
- Use strong passwords for all financial accounts and change them regularly.
- Obtain and review your annual credit report for fraudulent activity.

If you were a target of a TDoS attack, immediately contact your financial institutions, notify your telephone provider, and promptly report it to the IC3 website at www.ic3.gov. The IC3 complaint database links complaints to assist in referrals to the appropriate law enforcement agency for case consideration. The complaint information is also used to identity emerging trends and patterns.

Resources:
- The Latest Phone Scam: Targets Your Bank Account
- FBI Newark Public Service Announcement

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 website regarding a similar Asian extortion scheme. Individuals who receive information pertaining to counterfeit check schemes are encouraged to file a complaint at www.IC3.gov.

Mystery/Secret Shopper Schemes

01/20/10—The IC3 has been alerted to an increase in employment schemes pertaining to mystery/secret shopper positions. Many retail and service corporations hire evaluators to perform secret or random checks on themselves or their competitors, and fraudsters are capitalizing on this employment opportunity.

Victims have reported to the IC3 they were contacted via e-mail and U.S. mail to apply to be a mystery shopper. Applicants are asked to send a resume and are purportedly subject to an extensive background check before being accepted as a mystery shopper. The employees are sent a check with instructions to shop at a specified retailer for a specific length of time and spend a specific amount on merchandise from the store. The employees receive instructions to take note of the store's environment, color, payment procedures, gift items, and shopping/carrier bags and report back to the employer. The second evaluation is the ease and accuracy of wiring money from the retail location. The money to be wired is also included in the check sent to the employee. The remaining balance is the employee's payment for the completion of the assignment. After merchandise is purchased and money is wired, the employees are advised by the bank the check cashed was counterfeit, and they are responsible for the money lost in addition to bank fees incurred.

In other versions of the scheme, applicants are requested to provide bank account information to have money directly deposited into their accounts. The fraudster then has acquired access to these victims' accounts and can withdraw money, which makes the applicant a victim of identity theft.

Tips

Here are some tips you can use to avoid becoming a victim of employment schemes associated with mystery/secret shopping:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Virus scan all attachments, if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- There are legitimate mystery/secret shopper programs available. Research the legitimacy on companies hiring mystery shoppers. Legitimate companies will not charge an application fee and will accept applications online.
- No legitimate mystery/secret shopper program will send payment in advance and ask the employee to send a portion of it back.

Individuals who believe they have information pertaining to mystery/secret shopper schemes are encouraged to file a complaint at www.IC3.gov.

Haitian Earthquake Relief Fraud Alert

01/13/10—The FBI today reminds Internet users who receive appeals to donate money in the aftermath of Tuesday's earthquake in Haiti to apply a critical eye and do their due diligence before responding to those requests. Past tragedies and natural disasters have prompted individuals with criminal intent to solicit contributions purportedly for a charitable organization and/or a good cause.

Therefore, before making a donation of any kind, consumers should adhere to certain guidelines, to include the following:

- Do not respond to any unsolicited (spam) incoming e-mails, including clicking links contained within those messages.
- Be skeptical of individuals representing themselves as surviving victims or officials asking for donations via e-mail or social networking sites.
- Verify the legitimacy of nonprofit organizations by utilizing various Internet-based resources that may assist in confirming the group's existence and its nonprofit status rather than following a purported link to the site.
- Be cautious of e-mails that claim to show pictures of the disaster areas in attached files because the files may contain viruses. Only open attachments from known senders.
- Make contributions directly to known organizations rather than relying on others to make the donation on your behalf to ensure contributions are received and used for intended purposes.
- Do not give your personal or financial information to anyone who solicits contributions: Providing such information may compromise your identity and make you vulnerable to identity theft.

Anyone who has received an e-mail referencing the above information or anyone who may have been a victim of this or a similar incident should notify the IC3 via www.ic3.gov.

Archived E-Scams & Warnings