

FEDERAL BUREAU OF INVESTIGATION

New E-Scams & Warnings

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 identify 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 identify emerging trends and patterns.

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.

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.

POP-UP ADVERTISEMENTS OFFERING ANTI-VIRUS SOFTWARE POSE THREAT TO INTERNET USERS

12/11/09—An ongoing threat exists for computer users who, while browsing the Internet, began receiving pop-up security warnings that state their computers are infected with numerous viruses.

These pop-ups known as scareware, fake, or rogue anti-virus software look authentic and may even display what appears to be real-time anti-virus scanning of the user's hard drive. The scareware will show a list of reputable software icons; however, the user cannot click a link to go to the actual site to review or see recommendations. The scareware is intimidating to most users and extremely aggressive in its attempt to lure the user into purchasing the rogue software that will allegedly remove the viruses from their computer. It is possible that these threats are received as a result of clicking on advertisements contained on a website. Cyber criminals use botnets to push the software and use advertisements on websites to deliver it. This is known as malicious advertising or malvertising.

Once the pop-up appears it cannot be easily closed by clicking "close" or the "X" button. If the user clicks on the pop-up to purchase the software, a form is provided that collects payment information and the user is charged for the bogus product. In some instances, whether the user clicks on the pop-up or not, the scareware can install malicious code onto the computer. By running your computer with an account that has rights to install software, this issue is more likely to occur.

Downloading the software could result in viruses, Trojans, and/or keyloggers being installed on the user's computer. The repercussions of downloading the malicious software could prove further financial loss to the victim due to computer repair, as well as, cost to the user and/or financial institutions due to identity theft. The assertive tactics of the scareware has caused significant losses to users. The FBI is aware of an estimated loss to victims in excess of \$150 million.

Be cautious—Cyber criminals use easy to remember names and associate them with known applications. Beware of pop-ups that offer a variation of recognized security software. It is recommended that the user research the exact name of the software being offered.

Take precautions to ensure operating systems are updated and security software is current. If a user receives these anti-virus pop-ups, it is recommended to close the browser or shut the system down. It is suggested that the user run a full, anti-virus scan whenever the computer is turned back on. If you have experienced the anti-virus pop-ups or a similar scam, please notify the IC3 by filing a complaint at www.ic3.gov.

HOLIDAY SHOPPING TIPS

11/30/09—This holiday season the Federal Bureau of Investigation (FBI) is reminding people that cyber criminals continue to aggressively create new ways to steal money and personal information. Scammers use many techniques to fool potential victims including fraudulent auction sales, reshipping merchandise purchased with a stolen credit card, and selling fraudulent or stolen gift cards through auction sites at a discounted price.

Fraudulent Classified Ads or Auction Sales

Internet criminals post classified ads or auctions for products they do not have. If you receive an auction product from a merchant or retail store, rather than directly from the auction seller, the item may have been purchased with someone else's stolen credit card number. Contact the merchant to verify the account used to pay for the item actually belongs to you.

Shoppers should be cautious and not provide financial information directly to the seller, as fraudulent sellers will use this information to purchase items for their scheme from the provided financial account. Always use a legitimate payment service to protect purchases.

As for product delivery, unfamiliar Web sites or individuals selling reduced or free shipping to customers through auction sites many times are deemed to be fraudulent. In many instances, these websites or sellers provide shipping labels to their customers as a service. However, the delivery service providers are ultimately not being paid to deliver the package; therefore, packages shipped by the victims using these labels are intercepted by delivery service providers because they are identified as fraudulent.

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, if they have a low total number of feedback postings and all feedback was posted around the same date and time.

Gift Card Scam

Be careful about purchasing gift cards from auction sites or through classified ads. If you need a gift card, it is safest to purchase it directly from the merchant or another authorized retail store. If the gift card merchant discovers the card you received from another source or auction was initially obtained fraudulently, the merchant will deactivate the gift card number and it will not be honored for purchases.

Phishing and Smishing Schemes

Be leery of e-mails or text messages you receive indicating a problem or question regarding your financial accounts. In this scam, you are directed to follow a link or call the number provided in the message to update your account or correct the problem. The link actually directs the individuals to a fraudulent website or message that appears legitimate where any personal information you provide, such as account number and PIN, will be stolen.

Another scam involves victims receiving an e-mail message directing the recipient to a spoofed website. A spoofed website is a fake site or copy of a real website and misleads the recipient into providing personal information, which is routed to the scammer's computers.

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. Virus scan the 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 actually match and will lead you to a legitimate site.
- Log on directly to 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.

To receive the latest information about cyber scams, please go to the FBI website and sign up for e-mail alerts by clicking on one of the red envelopes. If you have received a scam e-mail, please notify the IC3 by filing a complaint at www.IC3.gov. For more information on e-scams, please visit the FBI's New E-Scams and Warnings webpage at <http://www.fbi.gov/cyberinvest/escams.htm>.

SPEAR PHISHING E-MAILS TARGET U.S. LAW FIRMS AND PUBLIC RELATIONS FIRMS

11/17/09—The FBI assesses with high confidence that hackers are using spear phishing e-mails with malicious payloads to exploit U.S. law firms and public relations firms. During the course of ongoing investigations, the FBI identified noticeable increases in computer exploitation attempts against these entities. The specific intrusion vector used against the firms is a spear phishing or targeted socially engineered e-mail designed to compromise a network by bypassing technological network defenses and exploiting the person at the keyboard. Hackers exploit the ability of end users to launch the malicious payloads from within the network by attaching a file to the message or including a link to the domain housing the file and enticing users to click the attachment or link.

Network defense against these attacks is difficult as the subject lines are spoofed, or crafted, in such a way to uniquely engage recipients with content appropriate to their specific business interests. In addition to appearing to originate from a trusted source based on the relevance of the subject line, the attachment name and message body are also crafted to associate with the same specific business interests. Opening a message will not directly compromise the system or network because the malicious payload lies in the attachment or linked domain.

Infection occurs once someone opens the attachment or clicks the link, which launches a self-executing file and, through a variety of malicious processes, attempts to download another file.

Indicators are unreliable to flag in-bound messages; however, indicators are available to determine an existing compromise. Once executed, the malicious payload will attempt to download and execute the file 'srhost.exe' from the domain 'http://d.ueopen.com'; e.g. <http://d.ueopen.com/srhost.exe>. Any traffic associated with 'ueopen.com' should be considered as an indication of an existing network compromise and addressed appropriately.

The malicious file does not necessarily appear as an 'exe' file in each incident. On occasion, the self-executing file has appeared as other file types, e.g., '.zip', '.jpeg', etc.

Please contact your local field office if you experience this network activity and direct incident response notifications to DHS and U.S. CERT.

FRAUDULENT AUTOMATED CLEARING HOUSE (ACH) TRANSFERS CONNECTED TO MALWARE AND WORK-AT-HOME SCAMS

11/03/09—Within the last several months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts. In a typical scenario, the targeted entity receives a "spear phishing" e-mail which either contains an infected attachment, or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware is installed on their computer. The malware contains a key logger which will harvest the recipients business or corporate bank account log-in information. Shortly thereafter, the perpetrator either creates another user account with the stolen log-in information, or directly initiates funds transfers by masquerading as the legitimate user. These transfers have occurred as both traditional wire transfers and as ACH transfers.

Further reporting has shown that the transfers are directed to the bank accounts of willing or unwitting individuals within the United States. Most of these individuals have been recruited via work-at-home advertisements, or have been contacted after placing resumes on well-known job search websites. These persons are often hired to "process payments", or "transfer funds". They are told they will receive wire transfers into their bank accounts. Shortly after funds are received, they are directed to immediately forward most of the money overseas via wire transfer services such as Western Union and Moneygram.

Customers who use online banking services are advised to contact their financial institution to ensure they are employing all the appropriate security and fraud prevention services their institution offers. The United States Computer Emergency Readiness Team (US-CERT) has made information on banking securely online available at http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf

Protecting your computer against malicious software is an ongoing activity and, at minimum, all computer systems need to be regularly patched, have up to date anti-virus software, and a personal firewall installed. Further information is available at <http://www.us-cert.gov/nav/nt01/>

If you have experienced unauthorized funds transfers from your bank accounts, or if you have been recruited via a work-at-home opportunity to receive transfers and forward money overseas, please notify the IC3 by filing a complaint at www.ic3.gov.

For a detailed analysis of this scam please visit <http://www.ic3.gov/media/2009/091103-1.aspx>

SPAMMERS CONTINUE TO ABUSE THE NAMES OF TOP GOVERNMENT EXECUTIVES BY MISUSING THE NAME OF THE UNITED STATES ATTORNEY GENERAL

10/27/09—As with previous spam attacks, which have included the names of high-ranking FBI executives and names of various government agencies, a new version misuses the name of the United States Attorney General, Eric Holder.

The current spam alleges that the Department of Homeland Security and the Federal Bureau of Investigation were informed the e-mail recipient is allegedly involved in money laundering and terrorist-related activities. To

avoid legal prosecution, the recipient must obtain a certificate from the Economic Financial Crimes Commission (EFCC) Chairman at a cost of \$370. The spam provides the name of the EFCC Chairman and an e-mail address from which the recipient can obtain the required certificate.

DO NOT RESPOND. THESE E-MAILS ARE A HOAX.

Government agencies do not send unsolicited e-mails of this nature. The FBI, Department of Justice, and other United States government executives are briefed on numerous investigations, but do not personally contact consumers regarding such matters. In addition, United States government agencies use the legal process to contact individuals. These agencies do not send threatening letters/e-mails to consumers demanding payments for Internet crimes.

Consumers should not respond to any unsolicited e-mails or click on any embedded links associated with such e-mails, as they may contain viruses or malware.

It is imperative consumers guard their Personally Identifiable Information (PII). Providing your PII will compromise your identity!

If you have been a victim of Internet crime, please file a complaint at www.IC3.gov.

FRAUDULENT E-MAIL CLAIMING TO CONTAIN FBI "INTELLIGENCE BULLETIN NO. 267"

10/05/09—A fraudulent e-mail message claiming to contain a confidential FBI report titled "New Patterns in Al-Qaeda Financing" has been circulating since August 15, 2009. The e-mail has the subject line "Intelligence Bulletin No. 267," and contains an attachment titled "bulletin.exe." This message, or similar messages, may contain files that are harmful to the recipient's system and may try to steal user credentials.

DO NOT CLICK ON ANY LINKS ASSOCIATED WITH THIS E-MAIL OR SIMILAR E-MAILS, IT IS A HOAX.

The FBI does not send unsolicited e-mails or email official reports. Consumers should not respond to any unsolicited e-mails or click on any embedded links, as they may contain viruses or other malicious software. Below is an example of the fraudulent e-mail message:

INTELLIGENCE BULLETIN No. 267

Title: New Patterns in Al-Qaeda Financing

Date: August 15, 2009

THREAT LEVEL: YELLOW (ELEVATED)

THE INTELLIGENCE BULLETIN PROVIDES LAW ENFORCEMENT AND OTHER PUBLIC SAFETY OFFICIALS WITH SITUATIONAL AWARENESS CONCERNING INTERNATIONAL AND DOMESTIC TERRORIST GROUPS AND TACTICS.

HANDLING NOTICE: Recipients are reminded that FBI Intelligence Bulletins contain sensitive terrorism and counterterrorism information meant for use primarily within the law enforcement community. Such bulletins are not to be released either in written or oral form to the media, the general public, or other personnel who do not have a need-to-know without prior approval from an authorized FBI official, as such release could jeopardize national security.

As with many fraudulent e-mail messages, this message contains multiple spelling errors and poor grammar.

If you have been a victim of Internet crime, please file a complaint at www.IC3.gov.

FRAUDULENT E-MAIL CLAIMING TO BE FROM DHS AND THE FBI COUNTERTERRORISM DIVISION

10/05/09—Fraudulent e-mails containing the subject line "New DHS Report" have been circulating since August 15, 2009. The e-mails claim to be from the Department of Homeland Security (DHS) and the FBI Counterterrorism Division. The e-mail text contains information about "New Usama Bin Ladin Speech Directed to the People of Europe," and has an attachment titled "audio.exe." The attachment is purportedly an audio speech from Bin Ladin; however, it actually contains malicious software intended to steal information from the recipient's system.

DO NOT CLICK ON ANY LINKS ASSOCIATED WITH THIS E-MAIL OR SIMILAR E-MAILS, IT IS A HOAX.

The FBI does not send unsolicited e-mails or e-mail official reports. Consumers should not respond to any unsolicited e-mails or click on any embedded links, as they may contain viruses or malware. One example of this fraudulent e-mail message is as follows:

Subject: New DHS Report

New Usama Bin Ladin Speech Directed to the People of Europe

Prepared by DHS/I&A Intelligence Watch and Warning Division and the FBI Counter Terrorism Division

(U//FOUO) Media outlets are reporting the release of a new audio tape on Al Jazeera today from Usama Bin Ladin, in which he states that all European countries involved in the Afghanistan war should end their support of American oppression in Afghanistan. In the audio message, Bin Ladin claims direct responsibility for the 11 September 2001 attacks and emphasizes that neither the Afghan people nor the Afghan government had foreknowledge of the attacks.

////Signed////

Charlie Allen

Chief Intelligence Officer

Department of Homeland Security

As with many fraudulent e-mail messages, this message contains multiple spelling errors and poor grammar. If you have been a victim of Internet crime, please file a complaint at www.IC3.gov.

FRAUDULENT E-MAIL CLAIMING TO CONTAIN AN FBI INTELLIGENCE BULLETIN FROM THE WEAPONS OF MASS DESTRUCTION DIRECTORATE

10/05/09—A fraudulent e-mail, initially appearing around June 16, 2009, claims to contain a confidential FBI report from the FBI "Weapons of Mass Destruction Directorate." The subject line of the email is "RE: Weapons of Mass Destruction Directorate," and contains an attachment "reports.exe." This message and similar messages may contain a file related to the "W32.Waledac" trojan software, which is designed to steal user authentication credentials or send spam messages.

DO NOT CLICK ON ANY LINKS ASSOCIATED WITH THIS E-MAIL OR SIMILAR E-MAILS, IT IS A HOAX.

The FBI does not send unsolicited e-mails or e-mail official reports. Consumers should not respond to any unsolicited e-mails or click on any embedded links, as they may contain viruses or malicious software. Below is an example of the fraudulent e-mail:

CLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

INTELLIGENCE BULLETIN

Weapons of Mass Destruction Directorate

HANDLING NOTICE: Recipients are reminded that FBI Intelligence Bulletins contain sensitive terrorism and counterterrorism information meant for use primarily within the law enforcement and homeland security communities. Such bulletins shall not be released, either in written or oral form, to the media, the general public, or other personnel who do not have a valid need-to-know without prior approval from an authorized FBI official, as such release could jeopardize national security.

[Link to malicious software \(report.exe\)](#)

If you have been a victim of Internet crime, please file a complaint at www.IC3.gov.

TECHNIQUES USED BY FRAUDSTERS ON SOCIAL NETWORKING SITES

10/01/09—Fraudsters continue to hijack accounts on social networking sites and spread malicious software by using various techniques. One technique involves the use of spam to promote phishing sites, claiming there has been a violation of the terms of agreement or some other type of issue which needs to be resolved. Other spam entices users to download an application or view a video. Some spam appears to be sent from users' "friends", giving the perception of being legitimate. Once the user responds to the phishing site, downloads the application, or clicks on the video link, their computer, telephone or other digital device becomes infected.

Another technique used by fraudsters involves applications advertised on social networking sites, which appear legitimate; however, some of these applications install malicious code or rogue anti-virus software. Other

malicious software gives the fraudsters access to your profile and personal information. These programs will automatically send messages to your "friends" list, instructing them to download the new application too. Infected users are often unknowingly spreading additional malware by having infected websites posted on their webpage without their knowledge. Friends are then more apt to click on these sites since they appear to be endorsed by their contacts.

Tips on avoiding these tactics:

- Adjust website privacy settings. Some networking sites have provided useful options to assist in adjusting these settings to help protect your identity.
- Be selective of your friends. Once selected, your "friends" can access any information marked as "viewable by all friends."
- You can select those who have "limited" access to your profile. This is for those whom you do not wish to give full friend status to or with whom you feel uncomfortable sharing personal information.
- Disable options and then open them one by one such as texting and photo sharing capabilities. Users should consider how they want to use the social networking site. If it is only to keep in touch with people then perhaps it would be better to turn off the extra options which will not be used.
- Be careful what you click on. Just because someone posts a link or video to their "wall" does not mean it is safe.

Those interested in becoming a user of a social networking site and/or current users are recommended to familiarize themselves with the site's policies and procedures before encountering such a problem. Each social networking site may have different procedures on how to handle a hijacked or infected account; therefore, you may want to reference their help or FAQ page for instructions. Individuals who experienced such incidents are encouraged to file a complaint at www.IC3.gov reporting the incident.

FRAUDSTERS CONTINUE TO EXPLOIT TELECOMMUNICATIONS RELAY SERVICES (TRS)

07/08/09—The IC3 continues to receive complaints pertaining to scam artists using Telecommunications Relay Services (TRS) to defraud U.S. businesses and consumers. Under Title IV of the Americans with Disabilities Act, all telephone companies must provide TRS for individuals with hearing impairments or speech impairments. This IC3 alert is to make the public aware of the continuing abuse of TRS to exploit U.S. businesses. Recent reports indicate scam artists are using TRS to exploit auto repair shops. The scam entails the fraudster using TRS to request services for a vehicle. The fraudster claims the vehicle has to be shipped to the auto repair business and requests the repairs and shipping fees be charged to a credit card. Unbeknownst to the business, the credit card is fraudulent or stolen; however, the charges initially go through without any complications. The business is then directed to wire the money to the shipper to cover the shipping costs. It is not until the shipper's money is wired that the business is notified of the fraudulent credit card; therefore, the business bears the loss.

A previous PSA titled *Notorious "Reshipper Scam" Transforms* was released on February 9, 2004, covering this exploit. To view the PSA in its entirety, please visit the following link: <http://www.ic3.gov/media/2004/040209.aspx>. Individuals who receive a communication, such as the one described above, are encouraged to file a complaint at www.ic3.gov reporting the incident

ASIAN EXTORTION SCHEME

06/10/09—The FBI is currently aware of a nationwide attempt to extort ethnic business owners, mostly of Asian decent, through telephonic threats of violence. The telephone calls appear to be originating from foreign countries. The caller acquires an adequate amount of open source information about the victim through Internet searches. This misleads the victim into believing the subject has personal knowledge about the victim. There have been no reported incidents of violence actually perpetrated to date.

Individuals who receive phone calls or e-mails containing threats of violence and their personally identifiable information (PII) are encouraged to contact law enforcement as well as file a complaint at www.ic3.gov.

CIRCULATION OF FRAUDULENT E-MAIL CLAIMING TO BE FROM U.S. CUSTOMS AND BORDER PROTECTION (CBP)

04/27/09—A spam e-mail claiming to be from former CBP Assistant Commissioner Thomas S. Winkowski is currently being circulated. This attempt to defraud is the typical e-mail scam using the name and reputation of a federal government official to create an air of authenticity.

The spam e-mail indicates the CBP has stopped a Diplomat who is carrying a consignment to be delivered to the recipient's residence. This consignment allegedly contains millions of dollars, which is revealed to be an inheritance for the e-mail recipient.

As with many other scams, this e-mail advises the recipient they will be permitted to access this inheritance once the recipient has given the sender of the e-mail their personal information.

This e-mail is a hoax. Do not respond.

The U.S. CBP does not send unsolicited e-mails. Consumers should not respond to unsolicited e-mails or click on any embedded links, as they may contain viruses or malware.

It is imperative consumers guard their personally identifiable information (PII). Examples of a person's PII include, but are not limited to: date of birth; social security number; and bank account numbers. Providing your PII will compromise your identity.

If you have received this e-mail, or a similar e-mail, please file a complaint at www.ic3.gov.

SCHEME PURPORTEDLY ANNOUNCING A MILLIONAIRE CONTEST

04/07/09—The IC3 has been alerted to the circulation of a fraudulent e-mail, purportedly from *The Oprah Winfrey Show*, notifying recipients of their nomination for the "Oprah Millionaire Contest Show." To participate, recipients are requested to mail their contact information such as full name, address, telephone number, and e-mail address; however, no mailing address was provided. Verified contestants are then required to purchase airfare and a ticket to attend *The Oprah Winfrey Show*, as well as complete a forthcoming contest form containing personal questions. The contestants are then promised a seat for *The Oprah Winfrey Show* in April and asked to provide their responses to the personal questions for a chance to win a million dollars.

Consumers always need to be alert to unsolicited e-mails. Do not open unsolicited e-mails or click on any embedded links, as they may contain viruses or malware. Providing your personally identifiable information will compromise your identity!

Individuals who receive such e-mails are encouraged to file a complaint at www.ic3.gov.

FAKE MILITARY TWIST ON VEHICLE SALE SCAMS

03/05/09—The FBI continues to receive reports of individuals victimized while attempting to purchase vehicles via the Internet. Victims find attractively priced vehicles advertised at different Internet classified ad sites. Most of the scams include some type of third-party vehicle protection program to ensure a safe transaction. After receiving convincing e-mails from the phony vehicle protection program, the victims are directed to send either the full payment, or a percentage of the payment, to the third-party agent via a wire payment service. No vehicles are delivered to the victims.

In a new twist, scammers are posing as members of the United States military. The fictitious military personnel in the scam have either been sent to a foreign country to improve military relations, or they need to sell a vehicle quickly and cheaply because of their upcoming deployment to either Iraq or Afghanistan.

Consumers are advised to do as much due diligence as possible before engaging in transactions to purchase vehicles advertised online. Consumers are also cautioned to be aware of the rules of or warnings posted by the Internet sites they visit. If someone is asking you as a consumer to break or avoid the rules of the website, it is possible that person is trying to scam you.

If you have fallen victim to this type of scam, please notify the IC3 by filing a complaint at www.ic3.gov.

WORK-AT-HOME SCAMS

02/04/09—Consumers need to be vigilant when seeking employment online. The IC3 continues to receive numerous complaints from individuals who have fallen victim to work-at-home scams.

Victims are often hired to "process payments," "transfer funds," or "reship products." These job scams involve the victims receiving and cashing fraudulent checks, transferring illegally obtained funds for the criminals, or receiving stolen merchandise and shipping it to the criminals.

Other victims sign up to be a “mystery shopper,” receiving fraudulent checks with instructions to cash the checks and wire the funds to “test” a company’s services. Victims are told they will be compensated with a portion of the merchandise or funds.

Work-at-home schemes attract otherwise innocent individuals, causing them to become part of criminal schemes without realizing they are engaging in illegal behavior.

Job scams often provide criminals the opportunity to commit identity theft when victims provide their personal information, sometimes even bank account information, to their potential “employer.” The criminal/employer can then use the victim’s information to open credit cards, post on-line auctions, register websites, etc., in the victim’s name to commit additional crimes.

If you have been a victim of Internet crime, please file a complaint at www.ic3.gov.

FLURRY OF SPAM TARGETING THE FEDERAL BUREAU OF INVESTIGATION

12/11/08—Consumers continue to be inundated by spam purportedly from the FBI. As with previous spam attacks, the latest versions use the names of several high ranking executives within the FBI and even the IC3 to attempt to defraud consumers.

Many of the spam e-mails currently in circulation claim to be an “official order” from the FBI’s Anti-Terrorist and Monetary Crimes Division, from an alleged FBI unit in Nigeria, confirm an inheritance, or contain a lottery notification, all informing recipients they have been named the beneficiary of millions of dollars. To claim the large sum, recipients are instructed to furnish their personally identifiable information (PII) and are often threatened with some type of penalty, such as prosecution, if they fail to do so. Specific PII information requested includes, but is not limited to, the recipient’s name, banking information, telephone number, and a copy of their passport. The spam e-mail allegedly from the IC3 states that the recipient has extorted money and will be given a limited amount of time to refund the money or face prosecution.

Do not respond. These e-mails are a hoax.

The FBI does not send unsolicited e-mails of this nature. FBI executives are briefed on numerous investigations but do not personally contact consumers regarding such matters. In addition, the IC3 does not send threatening letters to consumers demanding payments for Internet crimes.

Consumers should not respond to any unsolicited e-mails or click on any embedded links associated with such e-mails, as they may contain viruses or malware.

It is imperative consumers guard their PII. Providing your PII will compromise your identity.

If you have been a victim of Internet crime, please file a complaint at www.ic3.gov.

NEW TECHNIQUE UTILIZING PRIVATE BRANCH EXCHANGE (PBX) SYSTEMS TO CONDUCT VISHING ATTACKS

12/09/08—The FBI has received information concerning a new technique used to conduct vishing (1) attacks. The recent attacks were conducted by hackers exploiting a security vulnerability in Asterisk software. Asterisk is free and widely used software developed to integrate PBX (2) systems with Voice over Internet Protocol (VoIP) digital Internet voice calling services; however, early versions of the Asterisk software are known to have a vulnerability. The vulnerability can be exploited by cyber criminals to use the system as an auto dialer, generating thousands of vishing telephone calls to consumers within one hour.

The vulnerability referred to in this alert is a known vulnerability. Digium, the original creator and primary developer of Asterisk, released a Security Advisory, AST-2008-003, in March of 2008, which contains the information necessary for users to configure a system, patch the software, or upgrade the software to protect against this vulnerability.

If a consumer falls victim to this exploit, their personally identifiable information (PII) will be compromised. To prevent further loss of consumers’ PII and to reduce the spread of this new technique, it is imperative that businesses using Asterisk upgrade their software to a version that has had the vulnerability fixed. Further, consumers should not release personal information in response to unsolicited telephone calls. Providing your PII will compromise your identity!

If you have been a victim of Internet crime, please file a complaint at www.ic3.gov.

(1) *Vishing utilizes caller ID spoofing via VoIP to contact potential victims in order to gain access to their PII by convincing the victim that the criminal is associated with a legitimate business with a need to know the victim's PII.*

(2) *PBX Systems are used by companies to allow telephone calls between VoIP enterprise users on local lines while allowing all users to share a limited number of external lines*

FRAUDULENT SPAM E-MAIL PURPORTEDLY FROM FBI DEPUTY DIRECTOR JOHN S. PISTOLE

10/16/08—A spam e-mail claiming to be from FBI Deputy Director John S. Pistole is currently being circulated. This attempt to defraud is the typical e-mail scam using the name and reputation of an FBI official to create an air of authenticity.

As with many scams, the e-mail advises the recipient that they are the beneficiary of a large sum of money which they will be permitted to access once fees are paid and personal banking information is provided. The appearance of the e-mail leads the reader to believe that it is from FBI Deputy Director John S. Pistole.

This e-mail is a hoax. Do not respond.

The IC3 continues to receive and develop intelligence regarding fraud schemes misrepresenting the FBI and/or FBI officials. The scam e-mails give the appearance of legitimacy through the use of pictures of FBI officials, seal, letterhead, and/or banners.

These fraud schemes claim to be from domestic as well as international FBI offices. The typical types of schemes utilizing the names of FBI officials and/or the FBI are lottery endorsements and inheritance notifications, but can cover a range of scams from threats and malicious computer program attachments (malware) to online auction scams.

These scams use the social engineering technique of employing the FBI's name to intimidate and convince the recipient the e-mail is legitimate.

Please be cautious of any unsolicited e-mail referencing the FBI, Director Mueller, Deputy Director Pistole, or any other FBI official claiming that the FBI is endorsing any type of Internet activity.

Always be cautious when responding to requests or special offers delivered through unsolicited e-mail:

- Guard your personal information and your account information carefully.
- You should never give any personal, credit, or banking information in response to unsolicited e-mails.

If you have received this e-mail, or a similar e-mail, please file a complaint at www.ic3.gov.

HIT MAN E-MAIL SCAM RETURNS

08/28/08—The IC3 continues to receive thousands of reports concerning the hit man e-mail scheme. The e-mail content has evolved since late 2006; however, the messages remain similar in nature, claiming the sender has been hired to kill the recipient.

Two new versions of the scheme began appearing in July 2008. One instructed the recipient to contact a telephone number contained in the e-mail and the other claimed the recipient or a "loved one" was going to be kidnapped unless a ransom was paid. Recipients of the kidnapping threat were told to respond via e-mail within 48 hours. The sender was to provide the location of the wire transfer five minutes before the deadline and was threatened with bodily harm if the ransom was not received within 30 minutes of the time frame given. The recipients' personally identifiable information (PII) was included in the e-mail to promote the appearance that the sender actually knew the recipient and their location.

Perpetrators of Internet crimes often use fictitious names, addresses, telephone numbers, and threats or warnings regarding the failure to comply to further their schemes.

In some instances, the use of names, titles, addresses, and telephone numbers of government officials and business executives, and/or the victims' PII are used in an attempt to make the fraud appear more authentic. Below are links for the two previous public service announcements published by the IC3 concerning the hit man scheme:

- <http://www.ic3.gov/media/2007/070109.aspx>
- <http://www.ic3.gov/media/2006/061207.aspx>

Consumers always need to be alert to unsolicited e-mails. Do not open unsolicited e-mails or click on any embedded links, as they may contain viruses or malware. Providing your PII will compromise your identity! Individuals who receive e-mails containing threats of violence and their PII are encouraged to contact law enforcement as well as file a complaint at www.ic3.gov.

STORM WORM VIRUS

07/30/08—Be on the lookout for spam e-mail spreading malicious software (malware) which mentions “F.B.I. vs. facebook.” The e-mail directs the recipient to click on a link to view an article about the FBI and Facebook. Once the user clicks on the link, the “Storm Worm”malware is downloaded to the Internet-connected device, causing it to become infected with the virus and part of the Storm Worm botnet. A botnet is a network of compromised machines under the control of a single user. Botnets are typically set up to facilitate criminal activity such as spam e-mail, identity theft, denial of service attacks, and spreading malware to other machines on the Internet. The Storm Worm virus has capitalized on various holidays and fictitious world events in the last year by sending millions of e-mails advertising an e-card link within the text of the spam e-mail.

Be wary of any e-mail received from an unknown sender. Do not open any unsolicited e-mail and do not click on any links provided.

If you have received this, or a similar e-mail, please file a complaint at www.ic3.gov.

TIPS ON AVOIDING FRAUDULENT CHARITABLE CONTRIBUTION SCHEMES

07/08/08—Since late May and early June 2008, there have been several natural disasters throughout the country—including tornadoes, wildfires, and floods—that have devastated lives and property. In the wake of these events, which cause emotional distress and great financial loss to numerous victims, individuals across the nation often feel a desire to help, frequently through monetary donations.

Tragic incidents such as 9/11, Hurricanes Katrina and Rita, and the recent earthquake in China 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 unsolicited (spam) e-mail.
- Be skeptical of individuals representing themselves as officials soliciting via e-mail for donations.
- 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.
- To ensure contributions are received and used for intended purposes, make contributions directly to known organizations rather than relying on others to make the donation on your behalf.
- Validate the legitimacy of the organization by directly accessing the recognized charity or aid organization's website rather than following an alleged link to the site.
- Attempt to verify the legitimacy of the non-profit status of the organization by using various Internet-based resources, which also may assist in confirming the actual existence of the organization.
- Do not provide personal or financial information to anyone who solicits contributions: providing such information may compromise your identity and make you vulnerable to identity theft.

To obtain more information on charitable contribution schemes and other types of online schemes, visit www.lookstoogoodtobetrue.com. If you are a victim of an online scheme, please notify the IC3 by filing a complaint at www.ic3.gov.

PHISHING AND VISHING ATTACKS TARGETING USERS OF EPPICARDS

06/13/08—The IC3 has received reports of phishing attacks targeting users of EPPICards. The EPPICard is similar to a debit card. EPPICards are issued by a state agency for the purpose of receiving child-support payments. The cards are currently used in 15 states.

Individuals have reported receiving e-mail or text messages indicating a problem with their account. They are directed to follow the link provided in the message to update their account or correct the problem. The link actually directs the individuals to a fraudulent web site where their personal information, such as account number and PIN, is compromised.

Individuals have also reported receiving an e-mail message asking them to complete an online survey. At the end of the survey, they are asked for their EPPICard account information to allow funds to be credited to the account in appreciation for completing the survey. Providing this information will allow criminals to compromise the account.

EPPICard providers indicate they are not affiliated with survey web sites and do not solicit personal information via email or text messages.

Please be cautious of unsolicited e-mails. Do not open e-mails from unknown senders because they often contain viruses or other malicious software. Also, avoid clicking links in e-mails received from unknown senders as this is a popular method of directing victims to phishing websites.

If you have received an e-mail similar to this, please notify the IC3 by filing a complaint at www.ic3.gov.

FRAUDULENT REFUND NOTIFICATION PURPORTEDLY FROM THE IC3

06/06/08—Consumers need to be aware of e-mail schemes containing various versions of fraudulent refund notifications purportedly from the IC3 and the government of the United Kingdom. The e-mails claim the refunds are being made to compensate the recipients for their losses as victims of Internet fraud.

The perpetrators of this fraud use the names of people not associated with the IC3 but give them titles in an attempt to make the e-mails appear official. The perpetrators use the IC3's logo and the former name of the IC3, the Internet Fraud Complaint Center (IFCC), as well as the names of the Bank of England and the Metropolitan Police in the e-mails.

The e-mails promise refunds of thousands of dollars which are to be sent via bank wire transfer from the "bank of England" once the victim signs a "fund release order." The e-mails contain warnings that failure to sign the order will place the funds on hold and a penalty will be applied.

As with most spam, the content contains elements which are evidence of fraud such as: multiple spelling errors, poor grammar, agency names, signatures of officials and titles to appear authentic, and a warning for failure to comply. In some of the e-mails, the names of the officials do not match the signatures.

Consumers always need to be alert when they receive an unsolicited e-mail. Remember: do not open unsolicited e-mail or click on any links embedded in the e-mail, as they may contain a virus or malware.

If you have received an e-mail similar to this, please file a complaint at www.ic3.gov.

PHISHING RELATED TO ISSUANCE OF ECONOMIC STIMULUS CHECKS

05/08/08—The FBI warns consumers of recently reported spam e-mail purportedly from the Internal Revenue Service (IRS) which is actually an attempt to steal consumer information. The e-mail advises the recipient that direct deposit is the fastest and easiest way to receive their economic stimulus tax rebate. The message contains a hyperlink to a fraudulent form which requests the recipient's personally identifiable information, including bank account information. To convince consumers to reply, the e-mail warns that a failure to complete the form in a timely manner will delay the issuance of the rebate check.

One example of this IRS spam e-mail message is as follows:

"Over 130 million Americans will receive refunds as part of President Bush's program to jumpstart the economy.

Our records indicate that you are qualified to receive the 2008 Economic Stimulus Refund.

The fastest and easiest way to receive your refund is by direct deposit to your checking/savings account.

Please follow the link and fill out the form and submit before May 10th, 2008 to ensure that your refund will be processed as soon as possible.

Submitting your form on May 10th, 2008 or later means that your refund will be delayed due to the volume of requests we anticipate for the Economic Stimulus Refund.

To access **Economic Stimulus refund**, please **click here**."

Consumers are advised that the IRS does not initiate taxpayer communications via e-mail. In addition, the IRS does not request detailed personal information via e-mail or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

Please be cautious of unsolicited e-mails. It is recommended not to open e-mails from unknown senders because they often contain viruses or other malicious software. It is also recommended to avoid clicking links in e-mails received from unknown senders as this is a popular method of directing victims to phishing websites.

If you have received an e-mail similar to this, please notify the IC3 by filing a complaint at www.ic3.gov.

FRAUDULENT GRAND JURY SUMMONS CONTAINING MALWARE

04/17/08—The IC3 warns consumers of recently reported spam e-mail containing a fraudulent subpoena notifying recipients they are commanded to appear and testify before a Grand Jury. The e-mail attempts to appear authentic by containing a court case number, federal code, name and address of a California federal court, court room number, issuing officers' names, and a court seal. Recipients are directed to click the link provided in the e-mail in order to download and print associated information for their records. If the recipient clicks the link, malicious code is downloaded onto their computer.

The e-mail also contains language threatening recipients with contempt of court charges if they fail to appear. Recipients are also told the subpoena will remain in effect until the court grants a release. As with most spam, the content contains multiple spelling errors.

If you receive this type of notification and are unsure of its authenticity, you should contact the issuing court for validation.

Be aware; if you receive an unsolicited e-mail, especially from an unknown sender, it is recommended you do not open it. If you do open the e-mail, do not click any embedded links, as they may contain a virus or malware.

If you have received an e-mail similar to this, please file a complaint at www.ic3.gov.

STORM WORM VIRUS

02/11/08—With the Valentine's Day holiday approaching, be on the lookout for spam e-mails spreading the Storm Worm malicious software (malware). The e-mail directs the recipient to click on a link to retrieve the electronic greeting card (e-card). Once the user clicks on the link, malware is downloaded to the Internet-connected device and causes it to become infected and part of the Storm Worm botnet. A botnet is a network of compromised machines under the control of a single user. Botnets are typically set up to facilitate criminal activity such as spam e-mail, identity theft, denial of service attacks, and spreading malware to other machines on the Internet.

The Storm Worm virus has capitalized on various holidays in the last year by sending millions of e-mails advertising an e-card link within the text of the spam e-mail. Valentine's Day has been identified as the next target.

Be wary of any e-mail received from an unknown sender. Do not open any unsolicited e-mail and do not click on any links provided.

If you have received this, or a similar e-mail, please file a complaint at www.ic3.gov.

FBI IDENTIFIES RECURRING FRAUDULENT E-MAIL SCAM

02/01/08—The FBI has recently developed information indicating cyber criminals are attempting to once again send fraudulent e-mails to unsuspecting recipients stating that someone has filed a complaint against them or their company with the Department of Justice or another organization such as the Internal Revenue Service, Social Security Administration, or the Better Business Bureau.

Information obtained during the FBI investigation has been provided to the Department of Homeland Security (DHS). DHS has taken steps to alert their public and private sector partners with the release of a Critical Infrastructure Information Notice (CIIN).

The e-mails are intended to appear as legitimate messages from the above departments, and they address the recipients by name, and other personal information may be contained within the e-mail. Consistent with previous efforts, the scam will likely be an effort to secure Personally Identifiable Information. The nature of these types of scams is to create a sense of urgency for the recipient to provide a response through clicking on a hyperlink, opening an attachment, or initiating a telephone call.

It is believed this e-mail refers to a complaint that is in the form of an attachment, which actually contains virus software designed to steal passwords from the recipient. The virus is wrapped in a screensaver file wherein most anti-virus programs are unable to detect its malicious intent. Once downloaded, the virus is designed to monitor username and password logins, and record the activity, as well as other password-type information, entered on the compromised machine.

Be wary of any e-mail received from an unknown sender. Do not open any unsolicited e-mail and do not click on any links provided. If you have received a scam e-mail please notify the IC3 by filing a complaint at www.ic3.gov.

VISHING ATTACKS INCREASE

01/17/08—Are you one of many who have received an e-mail, text message, or telephone call, supposedly from your credit card/debit card company directing you to contact a telephone number to re-activate your card due to a security issue? The IC3 has received multiple reports of different variations of this scheme known as "vishing".

These attacks against US financial institutions and consumers continue to rise at an alarming rate.

Vishing operates like phishing by persuading consumers to divulge their Personally Identifiable Information (PII), claiming their account was suspended, deactivated, or terminated. Recipients are directed to contact their bank via a telephone number provided in the e-mail or by an automated recording. Upon calling the telephone number, the recipient is greeted with "Welcome to the bank of" and then requested to enter their card number in order to resolve a pending security issue.

For authenticity, some fraudulent e-mails claim the bank would never contact customers to obtain their PII by any means, including e-mail, mail, or instant messenger. These e-mails further warn recipients not to provide sensitive information when requested in an e-mail and not to click on embedded links, claiming they could contain "malicious software aimed at capturing login credentials."

Please beware—spam e-mails may actually contain malicious code (malware) which can harm your computer. Do not open any unsolicited e-mail and do not click on any links provided.

A new version recently reported involves the sending of text messages to cell phones claiming the recipient's on-line bank account has expired. The message instructs the recipient to renew their on-line bank account by using the link provided.

Due to rapidly evolving criminal methodologies, it is impossible to include every scenario. Therefore, be cognizant and protect your PII. Beware of e-mails, telephone calls, or text messages requesting your PII.

If you have a question concerning your account or credit/debit card, you should contact your bank using a telephone number obtained independently, such as from your statement, a telephone book, or other independent means.

If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.

AN INCREASE IN INTERNET SCHEMES CLAIMING TO BE FROM THE FBI

01/04/08—We have increasingly received reports of fraudulent schemes misrepresenting FBI agents, officials, and/or FBI Director Robert S. Mueller, III. The fraudulent e-mails give the appearance of legitimacy due to the usage of pictures of the FBI Director, seal, letterhead, and/or banners. The e-mails may also claim to come from our domestic or overseas offices.

The types of schemes utilizing the names of FBI agents, officials, or the Director's name are typically lottery endorsements and inheritance notifications. However, other fraudulent schemes include threat and extortion e-mails, website monitoring containing malicious computer program attachments (malware), and online auction scams.

The social engineering technique of utilizing the FBI's name is to intimidate and convince the recipient the e-mail is legitimate.

The FBI does not send out emails soliciting information from citizens.

Please be cautious of any unsolicited e-mail referencing the FBI, FBI Director Mueller, or any other FBI official endorsing any type of Internet activity.

If you have experienced this situation please notify the IC3 by filing a complaint at www.ic3.gov.

NEW TWIST CONCERNING THREAT AND EXTORTION E-MAILS

01/09/07—There is a new twist to the IC3 alert posted on December 7, 2006 regarding e-mails claiming that the sender has been paid to kill the recipient and will cancel the contract on the recipient's life if that person pays a large sum of money. Now e-mails are surfacing that claim to be from the FBI in London. These e-mails note the following information:

- An individual was recently arrested for the murders of several United States and United Kingdom citizens in relation to this matter.
- The recipient's information was found on the subject identifying the recipient as the next victim.
- The recipient is requested to contact the FBI in London to assist with the investigation.

It is not uncommon for an Internet fraud scheme to have the same overall intent but be transmitted containing variations in the e-mail content, e.g., different names, e-mail addresses, and/or agencies reportedly involved. [See our related top story on the hitman scam.](#)

Please note, providing any personal information in response to an unsolicited e-mail can compromise your identity and open you to identity theft.

If you have experienced this situation please notify the IC3 by filing a complaint at www.ic3.gov.

Due to the threat of violence inherent in these extortion e-mails, if you receive an e-mail that contains personally identifiable information that might differentiate your e-mail from the general e-mail spam campaign, we encourage you to contact the police.

E-MAILS CONTAINING THREATS AND EXTORTION

12/07/06—We have recently received information concerning spam e-mails threatening to assassinate the recipient unless the individual pays several thousand dollars to the sender of the e-mail.

The subject claims to have been following the victim for some time and was supposedly hired to kill the victim by a friend of the victim. The subject threatens to carry out the assassination if the victim goes to the police and requests the victim to respond quickly and provide their telephone number.

Warning! Providing any personal information can compromise your identify and open you to identity theft. If you have experienced this situation, please notify your local, state, or federal law enforcement agency immediately. Also, please notify the IC3 by filing a complaint at www.ic3.gov.