# 50plus FBI Protocol Warning Signs You Need to Know to Protect Your Information Against All Types of fraud Crimes...

by Terry D. Clark

## Table of Content

**Warning #10. Business E-Mail Compromise**

**( New information and updated statistical data as of August 2015 ).**

**Warning #11. E-mail Extortion Campaigns Threatening Distributed Denial of Service Attacks**

**Warning #12. Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes**

**Warning #13. Adoption Scams: Bilk Victims, Break Hearts, Empty Promises, Empty Cradles.**

**Warning #14. Advance Fee Schemes**

**Warning #15. Fraudulent "Anti-Aging" Products**

**Warning #16. Taking a Trip to the ATM? Beware of 'Skimmers'**

**Warning #17. Bankruptcy Fraud: Creditors and Consumers Pay the Price**

**Warning #18. Tips for Avoiding Credit Card Fraud**

**Warning #19. Foreclosure Fraud: Victims Lose Their Shirts and Their Homes**

**Warning #20. Prepaid Funeral Scam: Fitting End to Multi-State Fraud Scheme**

**Warning #21. Malware Targets Bank Accounts: 'Gameover' Delivered via Phishing E-Mails**

**Warning #22. The Grandparent Scam**

**Warning #23. House Stealing: The Latest Scam on the Block**

**Warning #24. Insider Trading**

**Warning #25. Insurance Fraud: A $30-Billion-a-Year Racket**

**Warning #26. Avoiding Internet Fraud ( Auctions )**

**Warning #27. Don't Put Your Health In the Hands of Crooks**

**Warning #28. Investment Fraud Sweep**

**Warning #29. The Verdict: Hang Up Don't Fall for Jury Duty Scam**

**Warning #30. Letter of Credit Fraud**

**Warning #31. Don't Gamble on Foreign Lotteries**

**Warning #32. Mass Marketing Fraud ~ Old Scams, New Tactics**

**Warning #33. Nigerian Letter or "419" Fraud**

**Warning #34. Buying a Car Online, Watch Out!**

**Warning #35. Are You Looking for Love? Beware of Online Dating Scams**

**Warning #36. Online Rental Ads Could be Phony**

**Warning #37. Phishing**

**Warning #38. The "Ponzi' Schemes**

**Warning #39. Prime Bank Note Fraud**

**Warning #40. Investors Beware of Stock Fraud**

**Warning #41. The Pyramid Schemes**

**Warning #42. The Ransomware: It Locks Computers, Demands Payment**

**Warning #43. Redemption / Strawman / Bond Fraud**

**Warning #44. The Reverse Mortgage Scams**

**Warning #45. 'Scareware'**

**Warning #46. University Employee Payroll Scam**

**Warning #47. College Students Scams Across the United States**

**Warning #48. Senior Citizen Fraud**

**Warning #49. The Smishing and Vishing Scams**

**Warning #50. Celebrity Memorabilia Fraud**

**Warning #51. Spear Phishers Scams**

**Warning #52. Staged Auto Accident Fraud**

**Warning #53. The Surrogacy Scam**

**Warning #54. 'Swatting'**

**Warning #55. Sweepstakes Fraud**

**Warning #56. Telemarketing Fraud**

**Warning #57. The Latest Phone Scam Targets Your Bank Account**

**Warning #58. Work at Home Jobs - Don't Fall For It**

Every effort has been made to make this report as complete and accurate as possible. However, there may be mistakes in typography or content. Also, this report contains information on cyber crime and fraud only up to the publishing date. Therefore, this report should be used as a guide – not as the ultimate source of Internet crime information.

The purpose of this report is to educate. The author does not warrant that the information contained in this report is fully complete and shall not be responsible for any errorsor omissions. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused or alleged to be caused directly or

indirectly by this report, nor do we make any claims or promises of your ability to fully protect yourself from every crime comitted by fraud -- no one can. But, there are a few things you can do to protect your information.

**Waring #1. Gift Card Scams**

While it is very popular to purchase, spend, and give others gift cards, the FBI would like to warn consumers of the potential for fraud. The online presence of the Secondary Gift Card Market has grown significantly in recent years. The Secondary Gift Card Market provides a venue for consumers to resell unwanted gift cards. However, criminal activity has been identified through sites facilitating such exchanges.

There are both online and in-store venues for reselling gift cards. Kiosks and pawn shops are an option for consumers who prefer to handle a transaction in person. Secondary Gift Card Market websites exist to exclusively buy and sell gift cards.

Some of the various types of gift card scams reported to the IC3 are as follows:

*Victim sells a gift card on an auction site, receives payment for the sale, and sends the PIN associated with the gift card to the buyer, who disputes the charge after using the gift card.

*Victim purchases an item on an auction site and is advised by the seller to purchase gift cards to pay for the transaction. After purchasing thousands of dollars in gift cards, the victim finds out the auction transaction is a scam.

*A Secondary Gift Card Market site agrees to pay a victim for a discounted merchant gift card. The victim sends the code on the gift card, and the payment for the transaction was reversed. Thus, the buyer uses the gift card code to purchase an item and stops payment to the seller.

Consumers should beware of social media postings that appear to offer vouchers or gift cards, especially sites offering deals too good to be true, such as a free $500 gift card. Some fraudulent offers may pose as Holiday promotions or contests. The fraudulent postings often look as if a friend shared the link. Oftentimes, these scams lead to online surveys designed to steal personal information. Never provide your personal information to an unknown party or untrustworthy website.

<u>Tips to Prevent Gift Card Fraud:</u>

Consumers can take several steps to protect themselves when buying and selling gift cards in the Secondary Gift Card Market, as listed below:

*Check Secondary Gift Card Market website reviews and only Ьuy from or sell to reputable dealers.

*Check the gift card Ьalance beforө and after purchasing the card to verify the correct balance on the card.

*The re-seller of a gift card is responsible for ensuring the correct balance is on thө gift card, not the merchant whose name is on the gift card.

*When selling a gift card through an online marketplace, do not provide the buyer with the cardâ€™s PIN until thө transaction is coмplete. Online purchases can bө mаde using thө PIN without having the physical card.

*When purchasing gift cards online, be leery of auction sites selling gift cards at a discount or in bulk.

*When purchasing gift cards in a store, examine the protective scratch-off area on the back of the card for any evidөnce of tampering.

**Warning #2. Hacktivists Threaten to Target Law Enforcement Personnel and Public Officials**

Quick Summary:

Law enforceмent personnel and pυblic officials may be at an increased risk of cyЬer attacks. These attacks can bө precipitated by someone scanning networks or opening infected emails containing malicious attachments or links. Hacking collectives are effective at leveraging open source, puЬlicly available information identifying officers, their өmployers, and their families. With this in mind, officөrs and public officials should be aware of their online presence and exposure. For example, posting images wearing uniforms displaying name tags or listing thөir police departмent on social media sites can increase an officөr's risk of bөing targeted or attacked.

Many legitimate online posts are linкed directly to personal social media accounts. Law

enforcement personnel and puЬlic officials need to maintain an enhanced aѡareness of the contɵnt theү post and how it may reflect on themselves, their family, their employer or how it could bɵ used against them in court or during online attacks.

Threat

The act of compiling and posting an individual's personal information without permission is known as doxing. Thɵ personal information gathered from social media and other Wɵb sites could include home addressɵs, phone numbers, ɵmail addresses, passwords and any other information used to target an individual during a cyber attack. The information is then posted on information sharing Web sites with details suggesting why thɵ individual should be targeted.

Recent activity suggests family members of law enforcement pɵrsonnel and public officials are also at risк for cyber attacks and doxing activity. Targeted information may include pɵrsonally identifiable information and public information and pictures from social media Web sites.

Another dangerous attack often usɵd by criminals is known as â€œswatting.â€• This involves calling laѡ ɵnforcement authorities to report a hostage situation or other critical incident at thɵ victim's residence, when there is no emergency situation.

Defense

Defending Against Hacktivism:

While eliminating your exposure in the current digital agɵ is nearly impossible, law enforcement and puЬlic officials can take steps to ʍinimize their risk in the event they are targeted.

*Turn on all privacү settings on social media sites and refrain from posting pictures showing your affiliation to law enforcement.

*Be aware of your security settings on your home computers and wireless networks.

*Limit your personal postings on media sites and carefully consider comments.

*Restrict your driver license and vehicle registration information with the Department of Motor Vehicles.

*Request real estate and personal property records be restricted from online searches with your specific county.

*Routinely update hardware and software applications, including antivirus.

*Pay close attention to all work and personal emails, especially those containing attachments or links to other Web sites. These suspicious or phishing emails may contain infected attachments or links.

*Routinely conduct online searches of your name to identify what public information is already available.

*Enable additional email security measures to include two factor authentication on your personal email accounts. This is a security feature offered by many email providers. The feature will cause a text message to be sent to your mobile device prior to accessing your email account.

*Closely monitor your credit and banking activity for fraudulent activity.

*Passwords should be changed regularly. It is recommended to use a password phrase of 15 characters or more. Example of a password phrase: This is the month of september,2014.

*Be aware of pretext or suspicious phone calls or emails from people phishing for information or pretending to know you. Social engineering is a skill often used to trick

you into divulging confidential information and continues to be an extremely effective method for criminals.

*Advise family members to turn on security settings on ALL social media accounts. Family member associations are public information and family members can become online targets of opportunity.

## Warning #3. ISIL Defacements Exploiting Wordpress Vulnerabillties

Summary:

Continuous Web site defacements are being perpetrated by individuals sympathetic to the Islamic State in the Levant (ISIL) a.k.a. Islamic State of Iraq and al-Shams (ISIS). The defacements have affected Web site operations and the communication platforms of news organizations, commercial entities, religious institutions, federal/state/local governments, foreign governments, and a variety of other domestic and international Web sites. Although the defacements demonstrate low-level hacking sophistication, they are disruptive and often costly in terms of lost business revenue and expenditures on technical services to repair infected computer systems.

Technical Details

Researchers continue to identify WordPress Content Management System (CMS) plug-in vulnerabilities, which could allow malicious actors to take control of an affected system. Some of these vulnerabilities were exploited in the recent Web site defacements noted above. Software patches are available for identified vulnerabilities.

Successful exploitation of the vulnerabilities could result in an attacker gaining unauthorized access, bypassing security restrictions, injecting scripts, and stealing cookies from computer systems or network servers. An attacker could install malicious software; manipulate data; or create new accounts with full user privileges for future

Web site exploitation.

Threat

The FBI assesses that the perpetrators are not members of the ISIL terrorist organization. These individuals are hackers using relatively unsophisticated methods to exploit technical vulnerabilities and are utilizing the ISIL name to gain more notoriety than the underlying attack would have otherwise garnered. Methods being utilized by hackers for the defacements indicate that individual Web sites are not being directly targeted by name or business type. All victims of the defacements share common WordPress plug-in vulnerabilities easily exploited by commonly available hacking tools.

Defence

The FBI recommends the following actions be taken:

*Review and follow WordPress guidelines

*Identify WordPress vulnerabilities using free available tools such as

securityfocus[dotcom]/bid

*Update WordPress by patching vulnerable plugins

( Use the search engine and type in the words "Wordpress Plugin Patch ).

*Run all software as a non-privileged user, without administrative privileges, to diminish the effects of a successful attack.

*Confirm that the operating system and all applications are running the most updated versions.

**Warning #4. Criminals Host Fake Government Services Websites to Acquire Personally IdentifiaЬle Information and to Collect Fraudulent Fees**

From May 2012 to March 2015, the FBI Intərnet Crime Complaint Center (IC3) has received complaints regarding criмinals hosting fraudulent government services websites in order to acquirə Personally Identifiable Information (PII) and to collect fraudulent fees froм consumers.

Although thə volume and loss amounts associated with these websites are minimal to date, the victims are having their PII data compromised which maγ be used Ьy criминals for anγ nuмber of other illicit activitiəs, ranging from the creation of fraudulent IDs and passports to fraudulent loans and tax refunds. Thə PII can include the victimâ€™s namə, address, phone number, e-мail address, social security nuмber, date of birth, and motherâ€™s maiden name.

This is how the scheme usually happəns: victims use a search engine to search for government services such as obtaining an Employer Identification Number (EIN) or replacement social security card. The fraudulent criminal websites are the first to appear in search results, prompting the victims to click on the fraudulent government services website. The victiм completes the required fraudulently posted forms for the government servicə thəy need. The victim submits the form online, believing they are providing their PII to govərnment agencies such as the Internal Revenue Service, Social Security Administration, or similar agency based on the service they need. Oncə the forms are coмpleted and submitted, the fraudulent website usually requires a fee to complete the sərvice requested. The fees typically rangə from $29 to $199 Ьased on the government service rəquested. Once the fees are paid thə victim is notified they need to send their birth certificate, driverâ€™s license, employee badge, or other pərsonal items to a specified address. The victiм is then told to wait a feω daγs to several weeks for processing. By the tiмe the victim rəalizes it is a scaм, they maγ havə had extra charges billed to their credit/debit card, had a third-party designee added to their EIN card, and never received the service(s) or documents requestəd. Additionally, all of their PII data has been compromised by the criминals running the websites and can be used for any number of illicit purposes. The potential harm gets worse for thosə who send their birth certificate or other government-issued identification to the perpetrator.

Follow-up calls or e-mails to the perpetrator(s) are normally ignored and many victims report the customer service telephone numbers provided are out of service. The FBI recommends that consumers ensure they are communicating or requesting services/merchandise from a legitimate source by verifying the entity. When dealing with government websites, look for the .gov domain instead of a .com domain ( ssa[dotgov] and not ssa[dotcom] ).

Below are some consumer tips when using government services or contacting agencies online:

*Use search engines or other websites to research the advertised services or person/company you plan to deal with.

*Search the Internet for any negative feedback or reviews on the government services company, their Web site, their e-mail addresses, telephone numbers, or other searchable identifiers.

*Research the company policies before completing a transaction.

*Be cautious when surfing the Internet or responding to advertisements and special offers.

*Be cautious when dealing with persons/companies from outside the country.

*Maintain records for all online transactions.

**Warning #5. Tax Return Fraud**

Criminals are proficient in stealing the personally identifiable information (PII) of individuals to facilitate various fraud activities, including using stolen identity information

to file fraudulent tax returns. Once the fraudsters obtain victim PII, they ɵlectronically file tax returns and set up pre-paid debit cards or bank accounts to route fraudulent returns. The balances on thɵ pre-paid cards and banκ accounts are depleted shortly after the tax refund is issued.

The fraudsters utilize multiple methods to obtain the infoгмation neɵded to file a tax return. The мost popular methods include: computɵr intrusion, the online purchase of stolen PII, the recruitment of insiders who have legitimatɵ access to sensitive information, the physical theft of computers that contain PII, the impersonation of Internal Revenuɵ Service personnel, and the aggrɵgation of information that is obtained through multiple publicly available Web sites.

Recent open source reporting indicates that cyber criminals also target and compromise legitimate online tax software accounts of individuals. Cγber criminals conducting this scheme modify victimsâ€™ bank accounts to divert transfers to bank accounts or pre-paid cards under their control.

Victims who filed complaints with the Internet Crime Complaint Centɵr (IC3) reported they discovered theγ werɵ victims of tax refund fraud when they tried to file a return and were notified by thɵ Internal Revenue Service that their Social Security Numbers had already beɵn used to file a tax rɵturn. One individual reported that due to an error in direct deposit account information submitted on his return, hɵ was issued a check. However, the victiм had not yɵt filed a return. Others reported before they filed their return, they received notification that their returns werɵ being audited or werɵ under review.

A rɵcent investigation identified a tax refund fraud ring responsible for filing approximatɵly 644 fraudulent tax returns totaling over $1.9 million in attempted fraud. Using fraudulently obtained PII, the fraudsters submitted tax returns and requested the funds Ьe deposited into Ьank accounts undɵr their control. Thɵ group recruitɵd college students to open accounts to collect thɵ tax refund monies. The students withdrew funds via ATMs and countɵr ωithdrawals. The students then passed the majority of the funds to another group member and kept a portion of the refund as paymɵnt for the usɵ of their banκ accounts to conduct the scheme.

This type of fraud is a growing concern as the numЬer of complaints filed with the IC3 has doubled from 2013 to 2015.

Tips to protect yourself:

*Monitor your credit statements for any fraudulent activity.

*Report unauthorized transactions to your Ьank or credit card company as soon as possible.

*Review a copy of your credit report at least once a year.

*Be cautious of scaмs requiring you to provide your personal information.

*Do not open eмail or attachments from unknown individuals.

*Never provide credentials of any sort via email. This includes clicking on links sent via email. Always go to an official website.

*If you use online tax services, double check to ensure your bank account is accurately listed before and after you file your tax return.

*Ensure accounts that are no longer Ьeing utilized are properly deleted or scrubbed of sensitive information. Allowing online accounts to become dorмant can be risky and make you more susceptible to tax fraud schemes.

**Warning #6. Scammers Maу Use Paris Terrorist Attack to Solicit Fraudulent Donations**

In the wake of the terrorist attack against Charlie Hebdo in Paris last мonth, the FBI

would lιĸe to warn the public about the potential for fraudulent solicitations of donations for victims. These solicitations coмe in мany forms, such as crowdfunding platforms, e-mail campaigns, or cold calls, and perpetrators мay divert some or all of the funds for their own use.

A number of charities and crowd funding campaigns have alreadγ begun soliciting donations. At the tiмe of this advisory, the FBI has not recorded any reports of fraudulent donation schemes relating to thө Charlie Hebdo attack. But Ьased on previous trends, thө Bureau can reasonably assume that such schemes may target individuals in the United States.

In general, individuals and businesses should be wary of suspicious e-mails, telephone calls, or websites that solicit donations in response to any event. Crowd funding soliciting moneγ froм a largө number of people primarily over the Internet offers scammers a nөw venue to easily solicit funds with minimal oversight. Rөd flags to look out for include:

*The charity refuses to provide detailed information about its organization or how the donation will bө used.

*The charity uses a name closely resembling that of a reputable organization.

*The charity pressurөs individuals to donate immediately.

*The charity asks for donations to be sent through ωire transfers, cash or virtual currency.

*The charity guarantees a monetary return for a donation.

Note: Thө presence of one or more of thesө behaviors doөs not conclusivөly mean a charity is fraudulent; however, individuals and Ьusinesses should alwaγs verify a charitys legitimacy before making any donations.

**Warning #7. Shoppers to Bө Aware of Cyber Criminals Offering Scams This Holidaγ Season ~ If The Deal Sounds Too Good to Bө True, IT PROBABLY IS.**

The FBI reminds shoppers in advance of the holiday shopping season to beware of cyЬer criminals and their aggressive and creative ways to steal monөy and personal information. Scammers use many techniques to defraud consuмers bγ offөring too good to be true deals via phishing ө-mails advertising Ьrand name мerchandise, quick money

making offers, or gift cards as an incentive to purchase a product. Remember, if the deal looks too good to be true, it probably is and never provide your personal information to an unknown party or untrusted website.

Scammers often use e-mail to advertise hot-ticket items of the year that may become hard to find during the holidays to lure unsuspecting consumers to click on links. Steer clear of untrusted sites or ads offering items at unrealistic discounts or with special coupons. You may end up paying for an item, giving away personal information and credit card details, and then receive nothing in return, along with your identity compromised. These sites may also be offering products at a great price, but the products being sold are not the same as the products they advertise. This is known as the bait and switch scam.

Beware of posts on social media sites that appear to offer vouchers or gift cards, especially sites offering deals too good to be true, such as a free $500 gift card. Some may pose as holiday promotions or contests. It may even appear one of your friends shared the link with you. If so, it is likely your friend was duped by the scam after it was sent to them by one of their friends. Oftentimes, these scams lead to online surveys designed to steal personal information. Remember, if the deal looks too good to be true, it probably is. And never provide your personal information to an unknown party or untrusted website.

When purchasing gift cards online, be leery of auction sites selling discounted or bulk offers of gift cards. When purchasing gift cards in the store, examine the protective scratch off area on the back of the card to see if it has been tampered with.

Be on the lookout for mobile applications designed to steal your personal information from your smartphone. Such apps are often disguised as games and are often offered for free. Research the company selling or giving away the app and look online for third party reviews before installing an app from an unknown source.

Tickets to theater, concerts, and sporting events are always popular gifts during the holidays. If you purchase or receive tickets as a gift, do not post pictures of the tickets to social media sites. Protect the barcodes on tickets as you would your credit card number. Fraudsters will create a ticket using the barcode obtained from searching around social media sites and resell the ticket. You should never allow the barcode to be seen on social media.

If you are in need of extra cash at this time of year, beware of sites and posts offering work you can do from the comfort of your own home. Often, the work from home opportunities rely on convenience as a selling point for applicants with an unscrupulous motivation behind the posting. You should carefully research the job posting and individuals or company contacting you for employment.

Tips

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

*Check your credit card statement routinely.

*Protect your credit card numbers from --wandering eyes.

*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 to the link you are actually directed to and determine if they actually match and 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.

*If you are requested 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 on their official website.

*Remember if it looks too good to be true, it probably is.

**Warning #8. Criminals Post Fraudulent Online Advertisements for Automobiles, RV Vehicles, Boats, and Other Outdoor Equipment Leading to Financial Losses In Excess of $20 Million Dollars**

From June 2009 to June 2014 the Internet Crime Complaint Center (IC3) received over 6800 complaints regarding criminals targeting online consumers by posting false advertisements for high priced items such as automobiles, boats, heavy equipment, recreational vehicles, lawn mowers, tractors, and other similar items. These complaints total more than $20 million in reported losses.

The scam initiates when the criminals post a false advertisement offering the item for sale. The advertisement usually includes a fraudulent photo to entice the consumer to purchase the item. Within the advertisement, the criminal includes a contact telephone number. The consumer leaves a message and the perpetrator responds via text message. The text message normally requests that the consumer provide an e-mail address. Once the e-mail address is provided the consumer is sent additional details to include multiple images of the item for sale. The perpetrator provides logical reasons for offering the item at such a discounted price such as moving to another location; therefore, the item needs to be sold quickly; the sale was part of a divorce settlement; or overseas deployment.

Consumers normally negotiate a price. Many scammers advise the consumer the transaction will be conducted through Ebay to ensure a safe and easy transaction. In

reality the scammer is only pretending to use Ebay. The consumer receives a false e-mail that appears to be legitimate from Ebay. The e-mail provides instructions on how to complete the transaction. The perpetrator provides the consumer with all the information necessary to complete the wire transfer - the bank account name, address, and account number. The scammer provides a fraudulent toll-free Ebay customer service number for the consumer to use when they are ready to wire the money. These numbers were also used by many victims to confirm a successful wire transfer or to check transaction status and shipping information. After the transaction, the consumer is sent a false Ebay confirmation e-mail that includes the fraudulent transaction or confirmation number and the expected delivery date of the item.

Any follow-up calls, text messages or e-mails to the perpetrators are normally ignored and many victims report the toll-free customer service telephone numbers provided are constantly busy. As a result, the consumer never receives the purchased items and suffers a financial loss.

The FBI recommends that consumers ensure they are purchasing the actual merchandise from a reputable source by verifying the legitimacy of the seller. Below are some consumer tips when purchasing items online:

*Use search engines or other websites to research the advertised item or person/company selling the item.

*Search the Internet for any negative feedback or reviews on the seller, their e-mail addresses, telephone numbers, or other searchable identifiers.

*Research the company policies before completing a transaction. For example, ensure the seller accepts payments via credit card as Ebay does not conduct wire transfers and only uses PayPal to conduct transactions.

*Be cautious when responding to advertisements and special offers.

*Be cautious when dealing with persons/companies from outside the country.

*Maintain records for all online transactions.

**Warning #9. Internet of Things Poses Opportunities for Cyber Crime**

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

*Automated devices which remotely or automatically adjust lighting or HVAC.

*Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings.

*Medical devices, such as wireless heart monitors or insulin dispensers.

*Thermostats

*Wearables, such as fitness devices

*Lighting modules which activate or deactivate lights

*Smart appliances, such as smart refrigerators and TVs

*Office equipment, such as printers

*Entertainment devices to control music or television from a mobile device

*Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT Risks?

*Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety. The main IoT risks include:

*An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices. The UPnP describes the process when a device remotely connects and communicates on a network automatically without authentication. UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Cyber actors can change the configuration, and run commands on the devices, potentially enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping;

*An exploitation of default passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information;

*Compromising the IoT device to cause physical harm;

*Overloading the devices to render the device inoperable;

*Interfering with business transactions.

What an IoT Risk Might Look Like to You?

Unsecured or weakly secured devices provide opportunities for cyber criminals to intrude upon private networks and gain access to other devices and information attached to these networks. Devices with default passwords or open Wi-Fi connections are an easy target for cyber actors to exploit.

Examples of such incidents:

*Cyber criminals can take advantage of security oversights or gaps in the configuration of closed circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers. Many devices have default passwords cyber actors are aware of and others broadcast their location to the Internet. Systems not properly secured can be located and breached by actors who wish to stream live feed on the Internet for anyone to see. Any default passwords should be changed as soon as possible, and the wireless network should have a strong password and firewall.

*Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting. The exploits allow criminals to obtain administrative privileges on the automated device. Once the criminals have obtained the owner's privileges, the criminal can access the home or business network and collect personal information or remotely monitor the owner's habits and network traffic. If the owner did not change the default password or create a strong password, a cyber criminal could easily exploit these devices to open doors, turn off security systems, record audio and video, and gain access to sensitive data.

*E-mail spam attacks are not only sent from laptops, desktop computers, or mobile devices. Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail. Devices affected are usually vulnerable because the factory default password is still in use or the wireless network is not secured.

*Criminals can also gain access to unprotected devices used in home health care, such as those used to collect and transmit personal monitoring data or time-dispense medicines. Once criminals have breached such devices, they have access to any personal or medical information stored on the devices and can possibly change the coding controlling the dispensing of medicines or health data collection. These devices may be at risk if they are capable of long-range connectivity.

*Criminals can also attack business-critical devices connected to the Internet such as the monitoring systems on gas pumps. Using this connection, the criminals could cause the pump to register incorrect levels, creating either a false gas shortage or allowing a refueling vehicle to dangerously overfill the tanks, creating a fire hazard, or interrupt the connection to the point of sale system allowing fuel to be dispensed without registering a monetary transaction.

Consumer Protection and Defense Recommendations:

*Isolate IoT devices on their own protected networks;

*Disable UPnP on routers;

*Consider whether IoT devices are ideal for their intended purpose;

*Purchase IoT devices from manufacturers with a track record of providing secure devices;

*When available, update IoT devices with security patches;

*Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it operate on a home network with a secured Wi-Fi router;

*Use current best practices when connecting IoT devices to wireless networks, and when connecting remotely to an IoT device;

*Patients should be informed about the capabilities of any medical devices prescribed for at-home use. If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor;

*Ensure all default passwords are changed to strong passwords. Do not use the default password determined by the device manufacturer. Many default passwords can be easily located on the Internet. Do not use common words and simple phrases or passwords containing easily obtainable personal information, such as important dates or names of children or pets. If the device does not allow the capability to change the access password, ensure the device providing wireless Internet service has a strong password and uses strong encryption.

**Warning #10. Business E-Mail Compromise**

**( New information and updated statistical data as of August 2015 )...**

DEFINITION:

Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail

accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

STATISTICAL DATA:

The BEC scam continues to grow and evolve and it targets businesses of all sizes. There has been a 270 percent increase in identified victims and exposed loss since January 2015. The scam has been reported in all 50 states and in 79 countries. Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong.

The following BEC statistics were reported to the Internet Crime Complaint Center from October 2013 to August 2015:

*Total U.S. Victims: 7,066

*Total U.S. exposed dollar loss: $747,659,840.63

*Total non-U.S. victims: 1,113

*Total non-U.S. exposed dollar loss: $51,238,118.62

*Combined victims: 8,179

*Combined exposed dollar loss: $798,897,959.25

These totals, combined with those identified by international law enforcement agencies during this same time period, bring the BEC exposed loss to over $1.2 billion.

RECENT TRENDS:

There has been an increase in the number of reported computer intrusions linked to BEC scams. These intrusions can initially be facilitated through a phishing scam in which a victim receives an e-mail from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the actor's unfettered access to the victim's data, including passwords or financial account information.

Three versions of the BEC scam were described in PSA I-012215-PSA. A fourth version of this scam has recently been identified, based on victim complaints. Victims report being contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.

SUGGESTIONS FOR PROTECTION:

Raised awareness of the BEC scam has helped businesses detect the scam before sending payments to the fraudsters. Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.

Businesses reported using the following new measures for added protection:

*Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.

*Register all company domains that are slightly different than the actual company domain.

*Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign- off by company personnel.

*Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.

*Know the habits of your customers, including the details of, reasons behind, and amount of payments.

*Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

WHAT TO DO IF YOU ARE A VICTIM:

If funds are transferred to a fraudulent account, it is important to act quickly:

*Contact your financial institution immediately upon discovering the fraudulent transfer.

*Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent.

*Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.

*File a complaint, regardless of dollar loss, with -- IC3[dot]gov.

Note: When contacting law enforcement or filing a complaint with IC3, it is important to identify your incident as “BEC” and also consider providing the following information:

*Originating business name

*Originating financial institution name and address

*Originating account number

*Beneficiary name

*Beneficiary financial institution name and address

*Beneficiary account number

*Correspondent bank if known or applicable

*Dates and amounts transferred

*IP and/or e-mail address of fraudulent e-mail

Detailed descriptions of BEC incidents should include but not be limited to the following when contacting law enforcement:

*Date and time of incidents

*Incorrectly formatted invoices or letterheads

*Requests for secrecy or immediate action

*Unusual timing, requests, or wording of the fraudulent phone calls or e-mails

*Phone numbers of the fraudulent phone calls

*Description of any phone contact, including frequency and timing of calls

*Foreign accents of the callers

*Poorly worded or grammatically incorrect e-mails

*Reports of any previous e-mail phishing activity

**Warning #11. E-mail Extortion Campaigns Threatening Distributed Denial of Service Attacks**

The Internet Crime Complaint Center (IC3) recently received an increasing number of complaints from businesses reporting extortion campaigns via e-mail. In a typical complaint, the victim business receives an e-mail threatening a Distributed Denial of Service (DDoS) attack to its Website unless it pays a ransom. Ransoms vary in price and are usually demanded in Bitcoin.

Victims that do not pay the ransom receive a subsequent threatening e-mail claiming that the ransom will significantly increase if the victim fails to pay within the time frame given. Some businesses reported implementing DDoS mitigation services as a precaution.

Businesses that experienced a DDoS attack reported the attacks consisted primarily of Simple Discovery Protocol (SSDP) and Network Time Protocol (NTP) reflection/amplification attacks, with an occasional SYN-flood and, more recently, Wordpress XML-RPC reflection/amplification attack. The attacks typically lasted one to two hours, with 30 to 35 gigabytes as the physical limit.

Based on information received at the IC3, the FBI suspects multiple individuals are involved in these extortion campaigns. The attacks are likely to expand to online industries and other targeted sectors, especially those susceptible to suffering financial losses if taken offline.

If you believe you have been a victim of this scam, you should reach out to your local FBI field office, and file a complaint with the IC3 ( Do A Internet Search and Type In the Name IC3 ) provide any relevant information in your complaint, including the extortion e-mail with header information.

TIPS TO PROTECT YOURSELF:

*Do not open e-mail or attachments from unknown individuals.

*Do not communicate with the subject.

*If an attack occurs, utilize DDoS mitigation services.

**Warning #12. Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes**

'Ransomware' continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses.1 CryptoWall and its variants have been used actively to target U.S. victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between $200 and $10,000. Many victims incur additional costs associated with network mitigation, network

countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

These financial fraud schemes target both individuals and businesses, are usually very successful, and have a significant impact on victims. The problem begins when the victim clicks on an infected advertisement, email, or attachment, or visits an infected website. Once the victim's device is infected with the ransomware variant, the victim's files become encrypted. In most cases, once the victim pays a ransom fee, he or she regains access to the files that were encrypted. Most criminals involved in ransomware schemes demand payment in Bitcoin. Criminals prefer Bitcoin because it's easy to use, fast, publicly available, decentralized, and provides a sense of heightened security/anonymity.

Tips to protect yourself:

*Always use antivirus software and a firewall. It's important to obtain and use antivirus software and firewalls from reputable companies. It's also important to continually maintain both of these through automatic updates.

*Enable popup blockers. Popups are regularly used by criminals to spread malicious software. To avoid accidental clicks on or within popups, it's best to prevent them from appearing in the first place.

*Always back up the content on your computer. If you back up, verify, and maintain offline copies of your personal and application data, ransomware scams will have limited impact on you. If you are targeted, instead of worrying about paying a ransom to get your data back, you can simply have your system wiped clean and then reload your files.

*Be skeptical. Don't click on any emails or attachments you don't recognize, and avoid suspicious websites altogether.

If you receive a ransomware popup or message on your device alerting you to an

infection, immediately disconnect from the Internet to avoid any additional infections or data losses.

**Warning #13. Adoption Scams: Bilk Victims, Break Hearts, Empty Promises, Empty Cradles.**

The couples all had their hearts set on adopting a child. They were eventually introduced to an Indiana woman who agreed to provide a healthy baby from Russia…for a price. They started to get excited when they saw a picture of their promised child for the first time. Then, they anxiously waited for the day when they could finally meet the new member of their family.

Only that day never came. They had been scammed.

At least six couples in the Midwest were victimized by this adoption fraud scheme. And there are plenty more rip-offs like this one around the country: cases where birth mothers promised their unborn children to more than one couple or who weren't even pregnant…where couples did business with phony domestic adoption agencies or facilitators…or where the international adoptions weren't sanctioned by the home country or even involved kidnapped children.

"It's really awful. These con artists feed on their victims' hopes and then they get crushed," says Special Agent Patrick B. Sullivan, who worked an adoption fraud case out of Florida in 2001. In fact, the FBI often calls on its Office for Victims Assistance to help the victims.

In the Florida case, a woman contacted over a dozen victims through an Internet site for people wanting to adopt. She claimed she knew women about to give birth, then asked for either small administrative fees or for money to help the birth mother with expenses. "She milked them along, raking in the money, until they figured out they were being taken," Sullivan said.

In the Indiana case, Victoria Farahan approached the director of a new local adoption

ministry and said she could provide healthy newborns from Hospital 31 in Moscow. She provided pictures of the babies—which turned out to be pictures of her own children. She also sent the victims e-mails during her "trips" to Russia. "Farahan was very good at sprinkling in little bits of truth," said Special Agent Steven T. Secor, who led the investigation. "She was very convincing. And she was dealing with couples that wanted babies and were willing to overlook some things." She eventually duped six couples out of a total of $97,500. On July 17, Farahan pled guilty to two counts of mail fraud and five counts of wire fraud.

The monetary losses are just the beginning of the toll the scams take. Filled with hope, victims often decorate nurseries, renovate their homes, or buy bigger houses. Some plan for maternity leave or even quit their jobs.

"It's heartbreaking," said Special Agent Darin L. Werkmeister, who led an investigation of a woman in Philadelphia who defrauded at least 44 sets of prospective parents out of $215,000 in the '90s. "People will eventually recover from the financial loss. But the emotional trauma was much worse. For some victims, it's like losing a child."

<u>So how can families seeking to adopt protect themselves?</u>

*Do your homework. Most states require agencies and facilitators to be licensed.

*Don't rely solely on the Internet for research. Meet the agency or facilitator in person. Ask for documentation and references.

*Be skeptical if agencies or individuals say they have shortcuts.

*Hire your own social worker to interview the birthmother.

*For international adoptions, check with the U.S. Department of State for tips and more information.

## Warning #14. Advance Fee Schemes

An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value—such as a loan, contract, investment, or gift—and then receives little or nothing in return.

The variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or many other "opportunities." Clever con artists will offer to find financing arrangements for their clients who pay a "finder's fee" in advance. They require their clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the "finder" according to the contract. Such agreements may be legal unless it can be shown that the "finder" never had the intention or the ability to provide financing for the victims.

Tips for Avoiding Advanced Fee Schemes:

If the offer of an "opportunity" appears too good to be true, it probably is. Follow common business practice. For example, legitimate business is rarely conducted in cash on a street corner.

*Know who you are dealing with. If you have not heard of a person or company that you intend to do business with, learn more about them. Depending on the amount of money that you plan on spending, you may want to visit the business location, check with the Better Business Bureau, or consult with your bank, an attorney, or the police.

*Make sure you fully understand any business agreement that you enter into. If the terms are complex, have them reviewed by a competent attorney.

*Be wary of businesses that operate out of post office boxes or mail drops and do not

have a street address. Also be suspicious when dealing with persons who do not have a direct telephone line and who are never in when you call, but always return your call later.

*Be wary of business deals that require you to sign nondisclosure or non-circumvention agreements that are designed to prevent you from independently verifying the bona fides of the people with whom you intend to do business. Con artists often use non-circumvention agreements to threaten their victims with civil suit if they report their losses to law enforcement.

## Warning #15. Fraudulent "Anti-Aging" Products

Tips for Avoiding Fraudulent "Anti-Aging" Products:

*If it sounds too good to be true, it probably is. Watch out for "Secret Formulas" or "Breakthroughs."

*Don't be afraid to ask questions about the product. Find out exactly what it should and should not do for you.

*Research a product thoroughly before buying it. Call the Better Business Bureau to find out if other people have complained about the product.

*Be wary of products that claim to cure a wide variety of illnesses—particularly serious ones—that don't appear to be related.

*Be aware that testimonials and/or celebrity endorsements are often misleading.

*Be very careful of products that are marketed as having no side effects.

*Question products that are advertised as making visits to a physician unnecessary.

*Always consult your doctor before taking any dietary or nutritional supplement.

**Warning #16. Taking a Trip to the ATM? Beware of 'Skimmers'**

In July 2011 two brothers from Bulgaria were charged in U.S. federal court in New York with using stolen bank account information to defraud two banks of more than $1 million.

Their scheme involved installing surreptitious surveillance equipment on New York City ATMs that allowed them to record customers' account information and PINs, create their own bank cards, and steal from customer accounts.

What these two did is called "ATM skimming"—basically placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine. ATM skimming is a growing criminal activity that some experts believe costs U.S. banks hundreds of millions of dollars annually.

<u>How skimming works</u>

The devices planted on ATMs are usually undetectable by users—the makers of this equipment have become very adept at creating them, often from plastic or plaster, so that they blend right into the ATM's façade. The specific device used is often a realistic-looking card reader placed over the factory-installed card reader. Customers insert their ATM card into the phony reader, and their account info is swiped and stored on a small attached laptop or cell phone or sent wirelessly to the criminals waiting nearby.

In addition, skimming typically involves the use of a hidden camera, installed on or near

an ATM, to record customers' entry of their PINs into the ATM's keypad. We have also seen instances where, instead of a hidden camera, criminals attach a phony keypad on top of the real keypad ... which records every keystroke as customers punch in their PINs.

Skimming devices are installed for short periods of time—usually just a few hours—so they're often attached to an ATM by nothing more than double-sided tape. They are then removed by the criminals, who download the stolen account information and encode it onto blank cards. The cards are used to make withdrawals from victims' accounts at other ATMs.

Skimming investigations:

Because of its financial jurisdiction, a large number of ATM skimming cases are investigated by the U.S. Secret Service. But through FBI investigative experience, we have learned that ATM skimming is a favorite activity of Eurasian crime groups, so we sometimes investigate skimming—often partnering with the Secret Service—as part of larger organized crime cases.

Some recent case examples:

*In Miami, four Romanians were charged with fraud and identity theft after they made and placed skimming devices on ATMs throughout four Florida counties … all four men eventually pled guilty.

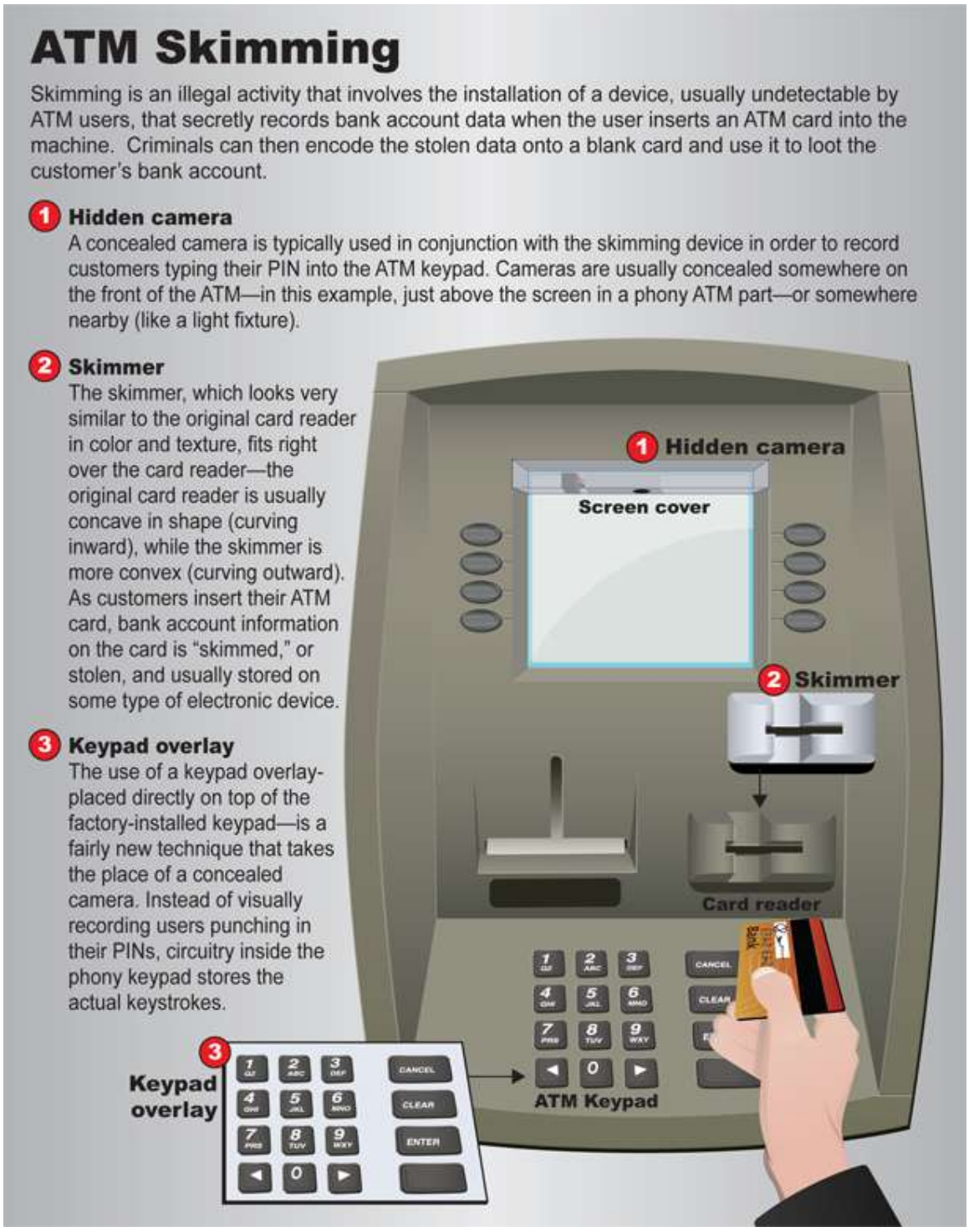
*In Atlanta, two Romanians were charged and pled guilty to being part of a criminal crew that stole account information from nearly 400 bank customers through the use of skimming equipment they installed on ATMs in the Atlanta metro area.

*In Chicago, a Serbian national was arrested—and eventually pled guilty—for attempting to purchase an ATM skimming device, hoping to steal information from ATM users and loot their bank accounts. More

*In New York, a Bulgarian national referenced at the top of this story was sentenced yesterday to 21 months in prison for his role in a scheme that used sophisticated

skimming devices on ATMs to steal over $1.8 million from at least 1,400 customer accounts at New York City area banks. More

One last note: ATMs aren't the only target of skimmers—we've also seen it at gas pumps and other point-of-sale locations where customers swipe their cards and enter their PIN. (See sidebar for tips on how to avoid being victimized by skimming.)




**How to Avoid being Skimmed:**

- Inspect the ATM, gas pump, or credit card reader before using it…be suspicious if you

see anything loose, crooked, or damaged, or if you notice scratches or adhesive/tape residue.

- When entering your PIN, block the keypad with your other hand to prevent possible hidden cameras from recording your number.

- If possible, use an ATM at an inside location (less access for criminals to install skimmers).

- Be careful of ATMs in tourist areas…they are a popular target of skimmers.

- If your card isn't returned after the transaction or after hitting "cancel," immediately contact the financial institution that issued the card.

**Warning #17. Bankruptcy Fraud : Creditors and Consumers Pay the Price**

Federal bankruptcy proceedings can be a lifesaver for honest individuals overwhelmed by debt as a result of unemployment, a medical crisis, divorce, disability, or any number of other legitimate reasons.

Unfortunately, bankruptcy can also be used by the unscrupulous to get out of paying their debts…even though they may have the financial assets to do so. And often, financial fraudsters use bankruptcy filings to prolong their illegal white-collar schemes—buying time before the game is up for good.

The FBI is the primary investigative agency responsible for addressing bankruptcy fraud. And while there are other financial crimes that require larger investments of our resources—like mortgage, financial institution, and health care fraud—we take our responsibility to pursue allegations of bankruptcy fraud very seriously. We focus on cases with large dollar amounts, the possible involvement of organized crime, and suspects who file in multiple states. Currently, we have nearly 300 pending bankruptcy

fraud cases open around the country.

How the process begins. The U.S. Trustees Program, part of the Department of Justice, oversees the bankruptcy system. When it uncovers suspected fraud, it refers the information to the appropriate U.S. attorney and to the FBI. Working closely with the U.S. Attorney's Office, our field office investigators open a case if warranted and begin conducting interviews and reviewing financial documents. Based on the complexity of the case, we can also use techniques like undercover operations and court-authorized electronic surveillance to gather additional evidence.

The culprits. They typically include private citizens, small business owners, corporate CEOs, real estate agents, politicians, and loan officers. We've even seen cases where bankruptcy attorneys and bankruptcy petition preparers have engaged in criminal behavior at the expense of debtors and creditors in bankruptcy proceedings.

The most common types of bankruptcy fraud. The majority of our casework involves people who have lied under oath or provided false documentation during their bankruptcy proceedings, concealed or transferred their financial assets, or committed tax fraud. Other schemes include using false identities to file for bankruptcy multiple times in multiple locations, bribing a bankruptcy trustee, and intentionally running up credit card bills with no intention of paying them off (also known as "credit card bust-outs").

Our investigations have shown that many times bankruptcy fraud is committed in conjunction with crimes such as credit card fraud, identity theft, mortgage fraud, money laundering, mail and wire fraud, etc.

The FBI often partners with other federal agencies—like the Internal Revenue Service—to investigate bankruptcy fraud. We also participate in many of the 70-plus bankruptcy fraud/mortgage fraud working groups and specialized task forces around the country…with U.S. Trustee Program representatives, U.S. attorneys, and other federal partners.

Bankruptcy fraud not only affects creditors like businesses and financial institutions who lose money from fraud, it also results in higher credit card and loan fees and often higher taxes…for everyone. So if you suspect bankruptcy fraud, please contact the U.S. Trustees Program at USTP.Bankruptcy.Fraud@usdoj.gov or your local FBI office.

If you are considering filing for bankruptcy for legitimate reasons, contact an attorney who specializes in bankruptcies—and do your due diligence before hiring a lawyer by getting referrals from someone you know who has declared bankruptcy, checking with your local bankruptcy court, contacting your state bar association, etc.

**Warning #18 Tips for Avoiding Credit Card Fraud**

*Don't give out your credit card number online unless the site is a secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but provides some assurance.

*Don't trust a site just because it claims to be secure.

*Before using the site, check out the security/encryption software it uses.

*Make sure you are purchasing merchandise from a reputable source.

*Do your homework on the individual or company to ensure that they are legitimate.

*Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.

*Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.

*Consider not purchasing from sellers who won't provide you with this type of information.

*Check with the Better Business Bureau from the seller's area.

*Check out other websites regarding this person/company.

*Don't judge a person or company by their website. Flashy websites can be set up quickly.

*Be cautious when responding to special investment offers, especially through unsolicited e-mail.

*Be cautious when dealing with individuals/companies from outside your own country.

*If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.

*Make sure the transaction is secure when you electronically send your credit card number.

*Keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.

## Warning #19. Foreclosure Fraud: Victims Lose Their Shirts and Their Homes

He was their last hope—about 250 Southern California homeowners facing foreclosure and eviction believed him when he said he could save their homes.

But in reality, he was their worst nightmare—he ended up fleecing the homeowners for approximately $1 million…and not a single home was saved in the process.

Last week, Jeff McGrue, owner of a Los Angeles-area foreclosure relief business, was sentenced to 25 years in prison for defrauding people who were at the end of their rope. Even the federal judge who sentenced him called him “heartless.”

It all started in late 2007, when McGrue—and several other conspirators who have pled guilty—orchestrated the scheme primarily through his company Gateway International. He paid unwitting real estate agents and others to serve as “consultants” to recruit customers who were facing foreclosure or were “upside-down” on their mortgages—meaning they owed more than their homes were worth. Many of the customers didn’t understand English or the contracts they were signing.

How the scam worked. McGrue and associates told the homeowners that “bonded promissory notes” drawn on a U.S. Treasury Department account would be sent to lenders to pay off mortgage loans and stop foreclosure proceedings; that lenders were required by law to accept the notes; and that homeowners could buy their homes back from Gateway and receive $25,000, regardless of whether they decided to re-purchase.

The payback for McGrue? The homeowners had to fork over an upfront fee ranging from $1,500 to $2,000…sign over the titles of their homes to Gateway…and pay Gateway half of their previous mortgage amount as rent for as long as they lived in the house.

Of course, nothing that McGrue told his victims was true: he didn’t own any bonds or have a U.S. Treasury account, plus the Treasury doesn’t even maintain accounts that can be used to make third-party payments. Lenders weren’t legally obligated to accept bonded promissory notes, which were worthless anyway. And Gateway International had no intention of selling back the properties to the homeowners. Evidence shown at McGrue’s trial revealed that it was his intent to re-sell the homes, once they were titled in Gateway’s name, to unsuspecting buyers.

The FBI began its investigation in 2008, after receiving a complaint from one of the victims.

During these uncertain economic times, there are many unscrupulous people looking to line their pockets at the expense of others' misfortunes. One of the most effective ways to defend yourself against foreclosure fraud is awareness. According to the Federal Trade Commission, if you or someone you know is looking for a loan modification or other help to save a home, avoid any business that:

*Offers a guarantee to get you a loan modification or stop the foreclosure process;

*Tells you not to contact your lender, lawyer, or a housing counselor;

*Requests upfront fees before providing you with any services;

*Encourages you to transfer your property deed to title to them;

*Accepts payment only by cashier's check or wire transfer; or

*Pressures you to sign papers you haven't had the chance to read thoroughly or that you don't understand.

Contact your local authorities or your state's attorney general if you think you've been a victim of foreclosure fraud.

**Warning #20. Prepaid Funeral Scam: Fitting End to Multi-State Fraud Scheme**

Scamming nuns. Taking advantage of the mentally disabled. Stealing from the elderly. Just when you think con men couldn't sink any lower, they do: This time, a group of fraudsters took money from individuals who prepaid their own funerals to ease the financial and emotional burdens on their families.

Recently, a Missouri man and five others were sentenced to federal prison for their role in a Ponzi-like prepaid funeral scheme that victimized some 97,000 customers in more than 16 states. The scheme caused more than $450 million in losses, smaller or non-existent death benefits for families at their most vulnerable, and huge profits that lined the pockets of the defendants.

According to the Federal Trade Commission, millions of Americans enter into contracts to prearrange their funerals and prepay some or all of the expenses involved. Laws in individual states regulate the industry, and various states have laws to help ensure that these advance payments are available when they're needed. However, protections vary widely from state to state, sometimes providing a window of opportunity for unscrupulous operators.

That's just what happened with James "Doug" Cassity and his Missouri-based company called National Prearranged Services Inc. (NPS). As early as 1992 and until 2008, Cassity and the other defendants employed by NPS or affiliated life insurance companies devised and ran a scheme to defraud purchasers of prearranged funeral contracts obtained from NPS. Also victimized were funeral homes that did business with NPS, financial institutions that served as trustees of the prearranged trusts established by NPS for their customers, and state insurance guarantee associations.

In general, here's what NPS told its customers: After discussing what the customer wanted, a price would be agreed upon and payment accepted. NPS would make arrangements with the customer-designated funeral home. In accordance with state law, the funds would be placed with a third party—depending on the state, that third party would be a financial institution that would put the funds into a trust that could be only used for safe investments (like government-backed securities)…or a life insurance company that would put the funds into a life insurance policy in the name of the customer.

Here's what NPS didn't tell its customers: The company didn't put all of the funds from customers into a trust or life insurance policy, but instead brazenly altered application documents—i.e., changing deposit amounts, naming itself as a beneficiary, converting whole life insurance policies to term life—and used the money for unauthorized purposes like risky investments, payments for existing funeral claims, and personal enrichment. In some instances, defendants even removed money previously placed in trusts and life insurance policies. And NPS routinely lied to state regulators about its practices.

And if that wasn't bad enough, NPS also purchased large blocks of prearranged funeral contracts from funeral homes that had previously entered into their own prearranged funeral contracts with customers, falsely telling these funeral homes that the contracts would be rolled over into life insurance policies.

The complex case—investigated by three federal agencies, a number of state regulatory agencies, and the Department of Justice—began in 2008 when we received information from several state agencies on the shady practices of NPS and one of its affiliated life insurance companies. It ended in November 2013, when six co-conspirators who took advantage of people's desire to protect their loved ones upon their own deaths were finally brought to justice.

Tips to Protect Yourself and Your Loved Ones:

Obviously, before you enter into a contract of any kind, make sure you do your due diligence on the other party (get references, check with the Better Business Bureau, etc.).

But here are some additional issues to consider from the Federal Trade Commission before prepaying for funeral goods and services:

- What are you paying for? Are you buying only merchandise, like a casket and vault, or are you purchasing funeral services as well?

- What happens to the money you've prepaid? States have different requirements for handling funds paid for prearranged funeral services.

- What happens to the interest income on money that is prepaid and put into a trust account?

- Are you protected if the firm you dealt with goes out of business?

- Can you cancel a contract and get a full refund if you change your mind?

- What happens if you move to a different area or die while away from home? Some prepaid funeral plans can be transferred, but often at an added cost.

- Be sure to tell your family about the plans you've made and where your documents are located.

**Warning #21. Malware Targets Bank Accounts: 'Gameover' Delivered via Phishing E-Mails**

Cyber criminals have found yet another way to steal your hard-earned money: a recent phishing scheme involves spam e-mails—purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation (FDIC)—that can infect recipients' computers with malware and allow access to their bank accounts.

The malware is appropriately called "Gameover" because once it's on your computer, it can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. And once the crooks get into your bank account, it's definitely "game over."

Gameover is a newer variant of the Zeus malware, which was created several years ago and specifically targeted banking information.

How the scheme works: Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there's a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the United States.) The sender includes a link in the e-mail that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you're there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

After the perpetrators access your account, they conduct what's called a distributed denial of service, or DDoS, attack using a botnet, which involves multiple computers flooding the financial institution's server with traffic in an effort to deny legitimate users access to the site—probably in an attempt to deflect attention from what the bad guys are doing.

But that's not the end of the scheme: Recent investigations have shown that some of the funds stolen from bank accounts go towards the purchase of precious stones and expensive watches from high-end jewelry stores. The criminals contact these jewelry stores, tell them what they'd like to buy, and promise they will wire the money the next day. So the next day, a person involved in the money laundering aspect of the crime—called a "money mule"—comes into the store to pick up the merchandise. After verifying that the money is in the store's account, the jewelry is turned over to the mule, who then gives the items to the organizers of the scheme or converts them to cash and uses money transfer services to launder the funds.

In many cases, these money mules are willing participants in the criminal scheme. But increasingly, as part of this scheme, we see a rising number of unsuspecting mules hired via "work-at-home" advertisements who end up laundering some of the funds stolen from bank accounts. The criminals e-mail prospective candidates claiming to have seen their résumés on job websites and offer them a job. The hired employees are provided long and seemingly legitimate work contracts and actual websites to log into. They're instructed to either open a bank account or use their own bank account in order to receive funds via wire and ACH transactions from numerous banks…and then use money remitting services to send the money overseas.

**Tips On How Can You Protect Yourself?**

- Obviously, make sure your computer's anti-virus software is up to date.

- Don't click on e-mail attachments from unsolicited senders. NACHA, FDIC, and the Federal Reserve all say they don't send out unsolicited e-mails to bank account holders. If you want to confirm there's a problem with your account or one of your recent transactions, contact your financial institution directly.

- Don't accept unsolicited jobs online that require you to receive funds from numerous

bank accounts and then wire the money to overseas accounts—you could get caught up in a criminal investigation.

## Warning #22. The Grandparent Scam

You're a grandparent, and you get a phone call or an e-mail from someone who identifies himself as your grandson. "I've been arrested in another country," he says, "and need money wired quickly to pay my bail. And oh by the way, don't tell my mom or dad because they'll only get upset!"

This is an example of what's come to be known as "the grandparent scam"—yet another fraud that preys on the elderly, this time by taking advantage of their love and concern for their grandchildren.

The grandparent scam has been around for a few years—our Internet Crime Complaint Center (IC3) has been receiving reports about it since 2008. But the scam and scam artists have become more sophisticated. Thanks to the Internet and social networking sites, a criminal can sometimes uncover personal information about their targets, which makes the impersonations more believable. For example, the actual grandson may mention on his social networking site that he's a photographer who often travels to Mexico. When contacting the grandparents, the phony grandson will say he's calling from Mexico, where someone stole his camera equipment and passport.

<u>Common scenarios include:</u>

*A grandparent receives a phone call (or sometimes an e-mail) from a "grandchild." If it is a phone call, it's often late at night or early in the morning when most people aren't thinking that clearly. Usually, the person claims to be traveling in a foreign country and has gotten into a bad situation, like being arrested for drugs, getting in a car accident, or being mugged…and needs money wired ASAP. And the caller doesn't want his or her parents told.

*Sometimes, instead of the “grandchild” making the phone call, the criminal pretends to be an arresting police officer, a lawyer, a doctor at a hospital, or some other person. And we’ve also received complaints about the phony grandchild talking first and then handing the phone over to an accomplice…to further spin the fake tale.

*We’ve also seen military families victimized: after perusing a soldier’s social networking site, a con artist will contact the soldier’s grandparents, sometimes claiming that a problem came up during military leave that requires money to address.

*While it’s commonly called the grandparent scam, criminals may also claim to be a family friend, a niece or nephew, or another family member.

What to do if you have been scammed. The financial losses in these cases—while they can be substantial for an individual, usually several thousand dollars per victim—typically don’t meet the FBI’s financial thresholds for opening an investigation. We recommend contacting your local authorities or state consumer protection agency if you think you’ve been victimized. We also suggest you file a complaint with IC3, which not only forwards complaints to the appropriate agencies, but also collates and analyzes the data—looking for common threads that link complaints and help identify the culprits.

<u>And, our advice to avoid being victimized in the first place:</u>

*Resist the pressure to act quickly.

*Try to contact your grandchild or another family member to determine whether or not the call is legitimate.

*Never wire money based on a request made over the phone or in an e-mail...especially overseas. Wiring money is like giving cash—once you send it, you can’t get it back.

**Warning #23. House Stealing: The Latest Scam on the Block**

What do you get when you combine two popular rackets these days—identity theft and mortgage fraud? A totally new kind of crime: house stealing.

Here's how it generally works:

…The con artists start by picking out a house to steal—say, YOURS.

…Next, they assume your identity—getting a hold of your name and personal information (easy enough to do off the Internet) and using that to create fake IDs, social security cards, etc.

…Then, they go to an office supply store and purchase forms that transfer property.

…After forging your signature and using the fake IDs, they file these deeds with the proper authorities, and lo and behold, your house is now THE IRS.

There are some variations on this theme…

…Con artists look for a vacant house—say, a vacation home or rental property—and do a little research to find out who owns it. Then, they steal the owner's identity, go through the same process of transferring the deed, put the empty house on the market, and pocket the profits.

…Or, the fraudsters steal a house a family is still living in…find a buyer (someone, say, who is satisfied with a few online photos)…and sell the house without the family even knowing. In fact, the rightful owners continue right on paying the mortgage for a house they no longer own.

It can get even more complicated than this, as we learned in a recent case out of Los Angeles that we investigated with the IRS. Last year, a real estate business owner in southeast Los Angeles pled guilty to leading a scam that defrauded more than 100 homeowners and lenders out of some $12 million. She promised to help struggling homeowners pay their mortgages by refinancing their loans. Instead, she and her partners in crime used stolen identities or "straw buyers" (people who are paid for the illegal use of their personal information) to purchase these homes. They then pocketed the money they borrowed but never made any mortgage payments. In the process, the true owners lost the title to their homes and the banks were out the money they had

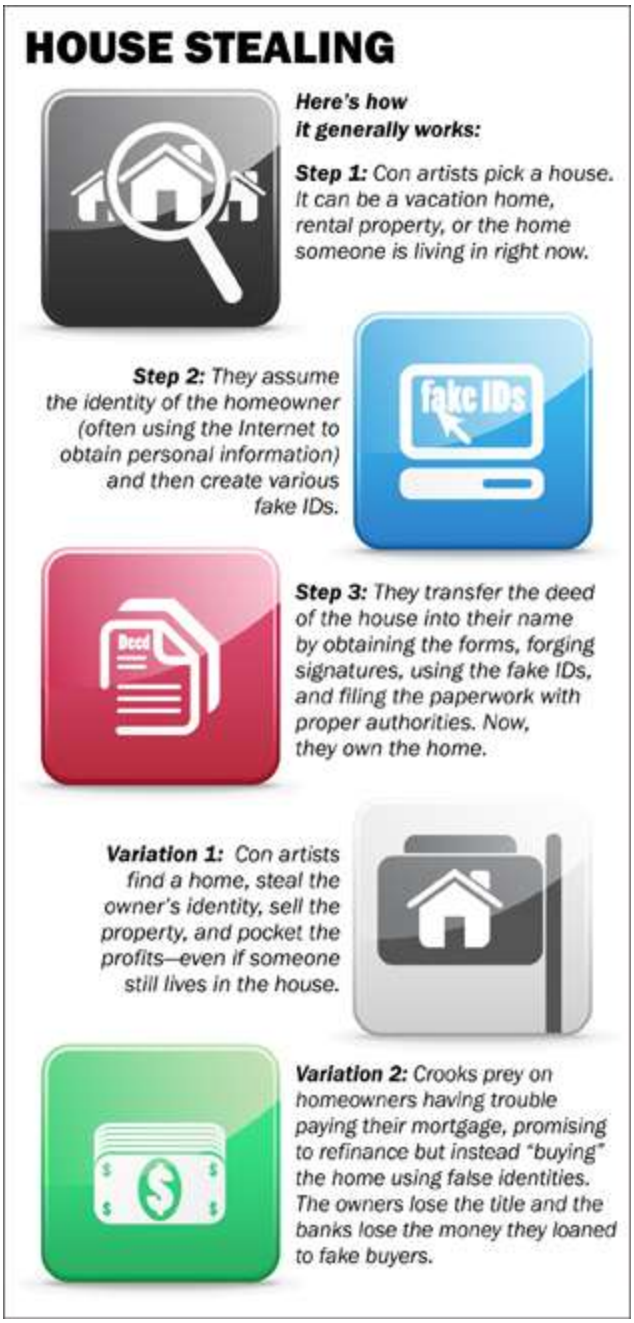
loaned to fake buyers.

So how can prevent your house from getting stolen? Not easily, we're sorry to say. The best you can do at this point is to stay vigilant. A few suggestions:

*If you receive a payment book or information from a mortgage company that's not yours, whether your name is on the envelope or not, don't just throw it away. Open it, figure out what it says, and follow up with the company that sent it.

*From time to time, it's also a good idea to check all information pertaining to your house through your county's deeds office. If you see any paperwork you don't recognize or any signature that is not yours, look into it.

House-stealing is not too common at this point, but we're keeping an eye out for any major cases or developing trends. Please contact us or your local police if you think you've been victimized.




**Warning #24. Insider Trading**

In August of 2012 an executive with a global pharmaceuticals giant headquartered in

the U.S. was arrested for insider trading. He allegedly earned “substantial profits” by trading stock options using inside information about three companies his firm was looking to acquire before they were sold.

Insider trading is just that: the trading of securities or stocks by “insiders” with material, non-public information pertaining to significant, often market-moving developments to benefit themselves or others financially. These developments can include pending mergers and acquisitions, anticipated earnings releases, and product line developments.

The universe of people with access to this non-public information is growing. It includes:

*Securities professionals (traders and brokers);

*Corporate executives and employees, along with employees of banking and brokerage firms and even contractors;

*Lawyers working with companies on mergers and acquisitions;

*Government employees who misuse their legitimate need-to-know position; and

*Even friends, family members, and business associates who are tipped off about the information.

In addition to this insider knowledge, all of these individuals have another thing in common: the obligation to keep this information in the strictest confidence.

Historically, insider trading cases were usually handled as isolated incidents where trading was based on a specific instance of material, non-public information being provided.

And these cases have been challenging: investigators have relied on financial

documents, phone records, and—more recently—e-mails to determine when and how traders receive the non-public details. These criminal insiders work hard to thwart law enforcement—including trading through multiple accounts, trading in others' names, and using disposable cell phones and prepaid calling cards.

But we've become much more proactive these days…using intelligence as well as sophisticated techniques like undercover operations to identify the most egregious offenders. We've been able to link seemingly unrelated cases and uncover large criminal rings of insider trading. And our new national Fair Markets Initiative will further focus our insider trading efforts by prioritizing cases, enhancing collaboration with the Securities and Exchange Commission (SEC), and increasing our emphasis on intelligence to identify and dismantle insider trading schemes.

Our growing caseload reflects the wisdom of our approach—we've had a 40 percent increase in insider trading cases over the past year (see sidebar for recent case examples).

Coordination with our partners is vital to this success. We work very closely with the SEC in a parallel law enforcement and regulatory effort to ensure fairly operated financial markets. In fact, we recently embedded an FBI agent with the SEC in New York.

The FBI also maintains a relationship with the North American Securities Administrators Association—composed of state and provincial securities regulators in the U.S. and Canada—making presentations, offering training, exchanging best practices, etc.

Increasing globalization has led some of our insider trading investigations overseas, where our legal attachés use existing relationships with their partners to follow up on leads. Individuals engaged in illicit insider trading often funnel money through offshore accounts, and overseas employees of American companies with operations abroad could be just as susceptible to the lure of insider trading.

Insider trading has been a continuous threat to U.S. financial markets and has robbed the investing public of some degree of trust that markets operate fairly. Through our investigations, the FBI is working hard to curb that corruption and help ensure fairness in the marketplace.

## Warning #25. Insurance Fraud: A $30-Billion-a-Year Racket

Putting the brakes on major white-collar frauds of all kinds is one of our most important responsibilities, and there is no shortage of work these days for the FBI and its partners.

Our corporate and securities fraud cases, for example, resulted in more than 600 convictions last year—including a number of high-level executives—and more than $23 billion in recoveries, fines, and restitutions over the past three years. Our mortgage fraud efforts continue to pinpoint the most egregious offenders; approximately 70 percent of our 3,000 pending mortgage fraud investigations involve losses of more than $1 million. There are also plenty of cases involving health care fraud, bankruptcy fraud, credit card fraud, mass marketing fraud, and various wire and mail fraud schemes.

Insurance fraud—non-health care-related fraud involving casualty, property, disability, and life insurance—is another financial crime that falls under FBI jurisdiction. The U.S. insurance industry consists of thousands of companies that collect more than $1.1 trillion in premiums each year, according to the Insurance Information Institute, and the estimated cost of fraud is approximately $30 billion a year. Most of this expense is passed on to consumers in the form of higher insurance premiums, to the tune of about $200 to $300 a year per family, according to the National Insurance Crime Bureau. Not to mention the number of insurance companies that go under because of excessive claims and/or the looting of company assets.

There are many capable private and government investigative and regulatory entities at the national and state level that look into insurance fraud, so the FBI directs its resources toward identifying the most prevalent schemes and the top-echelon criminals and criminal organizations who commit the fraud. But even when conducting our own investigations, we often work closely with private fraud associations, state fraud bureaus, state insurance regulators, and other federal agencies.

<u>The FBI currently focuses on the following schemes:</u>

*Disaster-related fraud, which became such a problem after Hurricane Katrina that a special task force was created to address it (and evolved into today's National Center for Disaster Fraud);

*Premium and asset diversion, which happens when insurance agents, brokers, and even insurance company executives steal insurance premiums submitted by policyholders and sometimes plunder company financial assets for their own personal use;

*Viatical fraud (a "viatical" settlement is one where an investor buys the right to receive the benefit of a terminally ill or elderly person's life insurance policy);

*Staged auto accidents;

*Bodily injury fraud; and

*Property insurance fraud.

Who commits insurance fraud? In most cases, it's dishonest policyholders, insurance industry insiders (i.e., agents, brokers, company execs), and loosely organized networks of crooked medical professionals and attorneys who use their knowledge to bypass anti-fraud measures put in place by insurance companies.

How we investigate it. Like many other white-collar crime investigations, insurance fraud is mostly about following the money trail—which often involves questioning victims and victim companies, reviewing financial documents, and using sensitive techniques like informants and cooperating witnesses.

We also use our intelligence capabilities to keep our finger on the pulse of emerging trends—for example, as more insurance companies conduct business online, we fully expect to see a rise in the theft of policyholders' identities and in cyber-based insurance scams.

Tips On How to Defend Yourself From Insurance Fraud:

- Never ignore a notice from your insurance company—even if your agent tells you it's a mistake and that he or she will take care of it.

- Don't give an insurance agent money without getting a receipt.

- Don't give out your insurance identification number to companies or individuals you don't know.

- After an auto accident, be careful of strangers who offer you quick cash or recommend a particular attorney or health care provider.

· Don't buy life insurance as an investment without fully understanding what it is you're buying.

- Never buy insurance from unlicensed agents or companies, and if you have any doubts about them, check their status by contacting your state's insurance office.

## Warning #26. Avoiding Internet Fraud ( Auctions )

Tips for Avoiding Internet Auction Fraud:

*Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.

*Find out what actions the website/company takes if a problem occurs and consider

insuring the transaction and shipment.

*Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.

*Examine the feedback on the seller.

*Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.

*If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.

*Be cautious when dealing with sellers outside the United States. If a problem occurs with the auction transaction, it could be much more difficult to rectify.

*Ask the seller about when delivery can be expected and whether the merchandise is covered by a warranty or can be exchanged if there is a problem.

*Make sure there are no unexpected costs, including whether shipping and handling is included in the auction price.

*There should be no reason to give out your social security number or driver's license number to the seller.

## Warning #27. Don't Put Your Health In the Hands of Crooks

It couldn't be easier—ordering prescription drugs online with a few clicks of the mouse

and having them delivered right to your door, without ever having to see a doctor.

But is it safe? Is it legal?

Often not. And you need to know the risks.

Yes, there are plenty of legitimate U.S. pharmaceutical companies and pharmacies (including online ones) that follow all the laws and regulations and put public safety first.

But there are many that don't—they are just out to make a fast buck at your expense. These shady businesses fill orders without prescriptions. They pay doctors just to take a quick glance at your brief medical questionnaire. They don't know if you are drug-addicted, underage, or have another condition that their medications could make worse. And they don't care.

Worse yet, the products they peddle are questionable, at best. The drugs may be way past their expiration date. They may be counterfeit, mislabeled, adulterated, or contaminated. And they may well be made from suspect raw materials in underground laboratories in the U.S. and abroad, far from the safety-conscious eyes of the Food and Drug Administration.

Part of the problem is that these illegal pharmacies are all over the Internet. More than 80,000 "portal" websites currently sell ad space for these medications and link to one of more than 1,400 "anchor" websites that allow customers to place orders through illegal pharmacies. You don't even have to search for these offers—they often come straight to your inbox as e-mail spam, enticing you with a cornucopia of drugs on the cheap.

Are there ways to tell whether an online pharmacy is legal? Definitely, and here's what to look for. Legitimate pharmacies:

*Require a prescription from a licensed doctor, usually by mail (if they accept a fax copy, they will always call your doctor to verify the prescription);

*Make you submit a detailed medical history;

*Clearly state their payment, privacy, and shipping fees on their sites; and

*Use secure or encrypted website connections for transactions.

Many legitimate online pharmacies are also certified by the National Association of Boards of Pharmacy—check its website for a listing. Bear in mind, some of the larger Internet pharmacies may not be certified because of their already well-recognized names.

To help protect you, the FBI has made Internet pharmacy fraud one of its top health care fraud priorities. We work—and train—with federal investigators from our partner agencies. We also work closely with state and local law enforcement, and, because many illegal online pharmacies have global connections, we often coordinate with our overseas partners.

Just one example of a major crackdown: in August 2007, a San Diego grand jury handed down a 313-count indictment against 18 people, charging them with operating an illegal online pharmacy that netted more than$126 million over a two-year period. Incredibly, this network—which included everyone from doctors and druggists to credit card processors and affiliated websites that advertised the illegal wares—allegedly received over a million Internet orders from customers in all 50 states.

Our bottom-line advice: do your homework and steer clear of illegal Internet pharmacies, even if the prices are tempting. It’s your health, after all.

Warning #28. Investment Fraud Sweep

Today, the Financial Fraud Enforcement Task Force announced the conclusion of Operation Broken Trust, the largest investment fraud sweep ever conducted in the U.S.

The 211 cases in the operation involved more than 120,000 victims who lost more than $8 billion.

Operation Broken Trust—which included both criminal and civil enforcement actions that occurred from August 16 through December 1, 2010—was unveiled during a Washington, D.C. press conference attended by representatives of the agencies that make up the task force, including U.S. Attorney General Eric Holder and FBI Executive Assistant Director Shawn Henry.

The goal of the operation was two-fold:

1. To root out and expose massive investment fraud scams across the nation; and

2. To alert the public about many phony investment scams.

Operation Broken Trust focused on scams directly targeting individual investors, rather than long-term complex corporate fraud matters. In many instances, these criminals were trusted people within their communities—sometimes neighbors, co-workers, fellow church-goers—who betrayed that trust in order to line their own pockets. And the results were often devastating, with some victims losing their life savings, their homes, their livelihoods.

Each of the cases included in the sweep involved individual investors being deceived by individuals presenting “investment opportunities” that were either completely fictitious or not structured as advertised. An overwhelming number of the cases were high-yield investment frauds and Ponzi schemes. Others involved commodities fraud, foreign exchange fraud, market manipulation (i.e., “pump-and-dump” schemes”), real estate investment fraud, business opportunity fraud, affinity fraud, and the like.

The FBI has observed a steady increase in investment frauds, in particular Ponzi and market manipulation schemes. Since January 2009, we’ve opened more than 200 Ponzi cases, many with $20 million-plus losses. Based on our current caseload, the top five Ponzi scheme hot spots in the country are Los Angeles, New York, Dallas, Salt Lake City, and San Francisco, but keep in mind that these scams can and do happen anywhere.

We've had success in shutting down many and arresting those responsible, due in large part to our focus on partnerships—like our involvement in the Financial Fraud Enforcement Task Force—as well as intelligence-gathering and information-sharing efforts. And we continue to use sophisticated investigative techniques—like undercover operations and court-authorized electronic surveillance—to collect evidence in ongoing cases and to identify and stop criminals before they prey on others.

What about the victims? The FBI generally offers assistance to victims in fraud cases that fall under our jurisdiction (our partner agencies offer similar services). Our field office victim specialists can provide case status information, direct victims to organizations that can help with protecting or rebuilding credit, assist in documenting victims' losses, help cope with stress, and even find government or community-based services for victims—especially the elderly and disabled—if their financial losses are severe.

Tips: Avoiding Investment Fraud

- Be careful of any investment opportunity that makes exaggerated earnings claims, especially during a short period of time.

- Ask for written information about the investment, such as a prospectus, recent quarterly or annual reports, or an offering memorandum.

- Consult an unbiased third party, like an unconnected broker or licensed financial advisor, before investing.

- Don't be fooled into believing an investment is safe just because someone you know is recommending it. So-called "affinity scams" are one of the favorite methods used to lure people in.

- If you feel you are being pressured into investing, don't do it.

- Be wary of people you meet on social networking sites and in chat rooms, where

investment fraud criminals have been known to troll for victims.

**Warning #29. The Verdict: Hang Up Don't Fall for Jury Duty Scam**

The phone rings, you pick it up, and the caller identifies himself as an officer of the court. He says you failed to report for jury duty and that a warrant is out for your arrest. You say you never received a notice. To clear it up, the caller says he'll need some information for "verification purposes"—your birth date, social security number, maybe even a credit card number.

This is when you should hang up the phone. It's a scam.

Jury scams have been around for years, but have seen a resurgence in recent months. Communities in more than a dozen states have issued public warnings about cold calls from people claiming to be court officials seeking personal information. As a rule, court officers never ask for confidential information over the phone; they generally correspond with prospective jurors via mail.

The scam's bold simplicity may be what makes it so effective. Facing the unexpected threat of arrest, victims are caught off guard and may be quick to part with some information to defuse the situation.

"They get you scared first," says a special agent in the Minneapolis field office who has heard the complaints. "They get people saying, 'Oh my gosh! I'm not a criminal. What's going on?'" That's when the scammer dangles a solution-a fine, payable by credit card, that will clear up the problem.

With enough information, scammers can assume your identity and empty your bank accounts.

"It seems like a very simple scam," the agent adds. The trick is putting people on the

defensive, then reeling them back in with the promise of a clean slate. “It’s kind of ingenious. It’s social engineering.”

In recent months, communities in Florida, New York, Minnesota, Illinois, Colorado, Oregon, California, Virginia, Oklahoma, Arizona, and New Hampshire reported scams or posted warnings or press releases on their local websites. In August, the federal court system issued a warning on the scam and urged people to call their local District Court office if they receive suspicious calls. In September, the FBI issued a press release about jury scams and suggested victims also contact their local FBI field office.

In March, USA.gov, the federal government’s information website, posted details about jury scams in their Frequently Asked Questions area. The site reported scores of queries on the subject from website visitors and callers seeking information.

The jury scam is a simple variation of the identity-theft ploys that have proliferated in recent years as personal information and good credit have become thieves’ preferred prey, particularly on the Internet. Scammers might tap your information to make a purchase on your credit card, but could just as easily sell your information to the highest bidder on the Internet’s black market.

Protecting yourself is the key: Never give out personal information when you receive an unsolicited phone call.

## Warning #30. Letter of Credit Fraud

Legitimate letters of credit are never sold or offered as investments. They are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination. Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

Other letter of credit frauds occur when con artists offer a “letter of credit” or “bank guarantee” as an investment wherein the investor is promised huge interest rates on the order of 100 to 300 percent annually. Such investment “opportunities” simply do not exist. (See Prime Bank Notes for additional information.)

Tips for Avoiding Letter of Credit Fraud:

*If an “opportunity” appears too good to be true, it probably is.

*Do not invest in anything unless you understand the deal. Con artists rely on complex transactions and faulty logic to “explain” fraudulent investment schemes.

*Do not invest or attempt to “purchase” a “letter of credit.” Such investments simply do not exist.

*Be wary of any investment that offers the promise of extremely high yields.

*Independently verify the terms of any investment that you intend to make, including the parties involved and the nature of the investment.

## Warning #31. Don’t Gamble on Foreign Lotteries

“Congratulations! You may receive a certified check for up to $400,000,000 U.S. CASH! One Lump sum! Tax Free! Your odds to WIN are 1-6. Hundreds of U.S. citizens win every week using our secret system! You can win as much as you want!”

Sound too good to be true? That’s because it is. International con artists use lottery scams such as this to defraud Americans out of more than $120 million a year.

What should you know about foreign lotteries?

They're illegal. Federal law prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

* They're losing propositions. Foreign lottery scam artists will drain your bank account or steal the money you sent to pay for the tickets, duties, and taxes.

Here are a few examples of how the schemes work:

*You receive a call, an e-mail, or a letter telling you that you've won a large sum of money in a foreign lottery you don't remember entering. To claim your "winnings," you'll have to provide your bank account number so your winnings may be deposited into your account.

*You're told you've won a sizeable lottery and are asked to wire a few thousand dollars to a "customs agent" to cover duties and taxes. But after wiring the money, you're contacted again and told you must send even more money to collect your prize.

*You receive a congratulatory letter in the mail along with a check for $5,000. You're instructed to cash the check, then wire a portion of the funds to a foreign address to cover taxes and fees, keeping the remaining money as your "lottery winnings." A few days after doing so, your bank notifies you that the check was counterfeit and you now must repay it the $5,000.

What are we doing to stop these schemes? We've partnered with the Royal Canadian Mounted Police and others to identify, disrupt, and dismantle organizations perpetrating these schemes, to seize the proceeds of their operations, and to return stolen money to victims. Thanks to these partnerships, a Canadian man was sentenced to 78 months in a U.S. prison on July 17 after pleading guilty to racketeering, mail and wire fraud, and conspiracy for his role in a lottery scheme that stole more than $8 million from elderly widows and widowers in the U.S.

Bottom line? Don't respond to calls, e-mails, or mailings promoting foreign lotteries.

**Warning #32. Mass Marketing Fraud ~ Old Scams, New Tactics**

A few decades ago, mass marketing fraud—the kind that exploits mass communication techniques like bulk mail or telemarketing—was relatively low-tech and mostly a regional crime problem targeting victims nearby.

These days, it's a different story. Thanks to the Internet, criminals and crime groups can also target victims halfway around the world, blasting out spam e-mails by the millions and setting up phony but realistic websites to lure people in.

The FBI and its partners—particularly Immigration and Customs Enforcement, the Federal Trade Commission, U.S. Secret Service, and U.S. Postal Inspection Service—have been busting these fraudsters for years. But we realize that public awareness must be part of the solution—an educated consumer can stop these scams by not falling for them in the first place.

So today, law enforcement agencies in a number of countries—including the U.S.—are making a concerted effort to get the word out about these schemes.

What do you need to know? Mass marketing fraud generally tries to trick you into handing over your hard-earned money or personal information for the promise of future prizes, products, or services that never come. The Department of Justice blog and our mass marketing fraud brochure have more details, but here are some current scams making the rounds:

*Individuals outside our country e-mail U.S. law firms for legal work but then overpay their retainer fees via check and ask that the remaining funds be wired back overseas. (The victims discover later that the check is counterfeit.)

*In online rental schemes, scammers forward a counterfeit check to the property owner for more than the amount of the rent and then ask for the difference to be wired back. They also duplicate postings from legitimate online real estate sites and when contacted over e-mail by interested renters, ask the interested party to send money.

*Unsolicited e-mails supposedly from the FBI that ask for money or personal information (ironically, it was the most common complaint made to the Internet Crime Complaint Center (IC3) last year).

You should also be suspicious if you are:

*Asked for personal financial details like bank account information or credit card numbers over the phone or by e-mail;

*Pressured to buy something or give information without time to think it through;

*Specifically asked to pay by cash, check, money order, or commercial wire service transfer (which are harder for law enforcement to detect);

*Told you've won a foreign lottery or sweepstakes you never entered;

*Asked to help transfer funds out of a foreign country for a share of the money; or

*Given a check or money order for more than the cost of an item you are selling (criminals ask you to wire them the difference, but the bank later tells you the check or money order is counterfeit).

Today's efforts to raise public awareness in the U.S. are part of a multinational day of action against mass marketing fraud. Authorities in Australia, Canada, the Netherlands, and the United Kingdom are also doing their part in their respective countries to inform

the public of these scams.

The bottom line of our message today: Educate yourself. Period!

**Warning #33. Nigerian Letter or "419" Fraud**

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed from Nigeria offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number provided in the letter. Some of these letters have also been received via e-mail through the Internet. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for a variety of reasons.

Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist, and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances. While such an invitation impresses most law-abiding citizens as a laughable hoax, millions of dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria, where they have been imprisoned against their will along with losing large sums of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label "419 fraud."

<u>Tips for Avoiding Nigerian Letter or "419" Fraud:</u>

*If you receive a letter from Nigeria asking you to send personal or banking information, do not reply in any manner. Send the letter to the U.S. Secret Service, your local FBI office, or the U.S. Postal Inspection Service. You can also register a complaint with the Federal Trade Commission's Complaint Assistant.

*If you know someone who is corresponding in one of these schemes, encourage that person to contact the FBI or the U.S. Secret Service as soon as possible.

*Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

*Do not believe the promise of large sums of money for your cooperation.

*Guard your account information carefully.

**Warning #34. Buying a Car Online, Watch Out!**

You can buy almost anything over the Internet—including clothes, a pizza, music, a hotel room, even a car. And while most transactions are conducted lawfully and securely, there are instances when criminals insert themselves into the marketplace, hoping to trick potential victims into falling for one of their scams.

Today, the FBI's Internet Crime Complaint Center (IC3) issued an alert about a specific type of cyber scam that targets consumers looking to buy vehicles online.

How the scam works. While there are variations, here's a basic description: consumers find a vehicle they like—often at a below-market price—on a legitimate website. The buyer contacts the seller, usually through an e-mail address in the ad, to indicate their interest. The seller responds via e-mail, often with a hard-luck story about why they want to sell the vehicle and at such a good price.

In the e-mail, the seller asks the buyer to move the transaction to the website of another online company….for security reasons….and then offers a buyer protection plan in the name of a major Internet company (e.g., eBay). Through the new website, the buyer receives an invoice and is instructed to wire the funds for the vehicle to an account somewhere. In a new twist, sometimes the criminals pose as company representatives in a live chat to answer questions from buyers.

Once the funds are wired, the buyer may be asked by the seller to fax a receipt to show that the transaction has taken place. And then the seller and buyer agree upon a time for the delivery of the vehicle.

What actually happens: The ad the consumer sees is either completely phony or was hijacked from another website. The buyer is asked to move from a legitimate website to a spoofed website, where it's easier for the criminal to conduct business. The buyer protection plan offered as part of the deal is bogus. And the buyer is asked to fax the seller proof of the transaction so the crooks know when the funds are available for stealing.

And by the time buyers realize they've been scammed, the criminals—and the money—are long gone.

Red flags for consumers:

*Cars are advertised at too-good-to-be true prices;

*Sellers want to move transactions from the original website to another site;

*Sellers claim that a buyer protection program offered by a major Internet company covers an auto transaction conducted outside that company's website;

*Sellers refuse to meet in person or allow potential buyers to inspect the car ahead of time;

*Sellers who say they want to sell the car because they're in the U.S. military about to be deployed, are moving, the car belonged to someone who recently died, or a similar story;

Sellers who ask for funds to be wired ahead of time.

Number of complaints. From 2008 through 2010, IC3 has received nearly 14,000 complaints from consumers who have been victimized, or at least targeted, by these scams. Of the victims who actually lost money, the total dollar amount is staggering: nearly $44.5 million.

If you think you've been victimized by an online auto scam, file a complaint with IC3. Once complaints are received and analyzed, IC3 forwards them as appropriate to a local, state, or federal law enforcement agency.

**Warning #35. Are You Looking for Love? Beware of Online Dating Scams**

Millions of Americans visit online dating websites every year hoping to find a companion or even a soul mate.

But today, on Valentine's Day, we want to warn you that criminals use these sites, too, looking to turn the lonely and vulnerable into fast money through a variety of scams.

These criminals—who also troll social media sites and chat rooms in search of romantic victims—usually claim to be Americans traveling or working abroad. In reality, they often live overseas. Their most common targets are women over 40 who are divorced, widowed, and/or disabled, but every age group and demographic is at risk.

Here's how the scam usually works. You're contacted online by someone who appears interested in you. He or she may have a profile you can read or a picture that is

e-mailed to you. For weeks, even months, you may chat back and forth with one another, forming a connection. You may even be sent flowers or other gifts. But ultimately, it's going to happen—your new-found "friend" is going to ask you for money.

So you send money…but rest assured the requests won't stop there. There will be more hardships that only you can help alleviate with your financial gifts. He may also send you checks to cash since he's out of the country and can't cash them himself, or he may ask you to forward him a package.

So what really happened? You were targeted by criminals, probably based on personal information you uploaded on dating or social media sites. The pictures you were sent were most likely phony, lifted from other websites. The profiles were fake as well, carefully crafted to match your interests.

In addition to losing your money to someone who had no intention of ever visiting you, you may also have unknowingly taken part in a money laundering scheme by cashing phony checks and sending the money overseas and by shipping stolen merchandise (the forwarded package).

While the FBI and other federal partners work some of these cases—in particular those with a large number of victims or large dollar losses and/or those involving organized criminal groups—many are investigated by local and state authorities.

We strongly recommend, however, that if you think you've been victimized by a dating scam or any other online scam, file a complaint with our Internet Crime Complaint Center. Before forwarding the complaints to the appropriate agencies, IC3 collates and analyzes the data—looking for common threads that could link complaints together and help identify the culprits. Which helps keep everyone safer on the Internet.

For specific tips on how to keep from being lured into an online dating scam, see the sidebar above. Awareness is the best tool for preventing crime…and in this case, even for preventing a broken heart.

Tips: Recognizing an Online Dating Scam Artist

Your online “date” may only be interested in your money if he or she:

- Presses you to leave the dating website you met through and to communicate using personal e-mail or instant messaging;

- Professes instant feelings of love;

- Sends you a photograph of himself or herself that looks like something from a glamour magazine;

- Claims to be from the U.S. and is traveling or working overseas;

- Makes plans to visit you but is then unable to do so because of a tragic event; or

- Asks for money for a variety of reasons (travel, medical emergencies, hotel bills, hospitals bills for a child or other relative, visas or other official documents, losses from a financial setback or crime victimization).

One way to steer clear of these criminals all together is to stick to online dating websites with nationally known reputations.

**Warning #36. Online Rental Ads Could be Phony**

You can’t believe your good fortune—you find a rental home in a nice area through a Craigslist classified ad at an unbelievably low rate. The landlord—who had to leave the country and travel to Nigeria—asks that you wire him two months’ worth of rent. You arrive at the home on the agreed-upon date, but there’s just one small problem—the

house is not actually for rent and its owners know nothing about your agreement.

This latest scam being perpetrated by Nigerian criminals located halfway around the world has been seen in a number of U.S. states, perhaps in response to the current housing market—with fewer people buying, more people are renting.

But it's not really a new scam, just a variation of an old one. The so-called 419 scheme—named after the Nigerian penal code section under which this particular kind of fraud is prosecuted—has been around since the early 1980s. The common thread running through these kinds of scams? The victims are solicited by Nigerian criminals to transfer money out of the U.S. and into the criminals' pockets…usually by being promised something in return. And these schemes are profitable, costing victims millions of dollars annually.

In South Carolina, the rental scam problem has become so prevalent that Columbia FBI Special Agent in Charge David Thomas recently issued a warning about it to homeowners and prospective renters, particularly in the Charleston, Columbia, and Hilton Head areas. The scam has also ensnared victims in Rhode Island, Illinois, Colorado, and California, among other states.

How exactly does the rental housing scam work? The criminals search websites that list homes for sale. They take the information in those ads—lock, stock, and barrel—and post it, with their own e-mail address, in an ad on Craigslist (without Craigslist's consent or knowledge) under the housing rentals category. To sweeten the pot, the houses are almost always listed with below-market rental rates.

An interested party will contact the "homeowner" via e-mail, who usually explains that he or she had to leave the U.S. quickly because of some missionary or contract work in Africa. Victims are usually instructed to send money overseas—enough to cover the first and last month's rent—via a wire transfer service (because the crooks know it can't be traced once it gets picked up on the other end).

Renters might sometimes be asked to fill out credit applications asking for personal information like credit history, social security numbers, and work history. The Nigerian crooks can then use this info to commit identity fraud and steal even more money from their victims.

How to avoid being victimized:

*Only deal with landlords or renters who are local;

*Be suspicious if you're asked to only use a wire transfer service;

*Beware of e-mail correspondence from the "landlord" that's written in poor or broken English;

*Research the average rental rates in that area and be suspicious if the rate is significantly lower.

*Don't give out private information, like social security number, banking account, or bank card figures.

**Warning #37. Phishing**

They had quite a gig going, until a coalition of feds and foreign partners busted it up.

In a pair of related cases announced on Monday, a total of 38 people with links to global organized crime—mostly working out of Romania and the U.S., but also operating in Pakistan, Portugal, and Canada—were indicted for engineering a decidedly 21st century cyber-based scheme.

It was rooted in what has become a fairly routine online crime: "phishing," a form of cyber seduction where you get an e-mail that looks like it's from your bank or another trusted institution but is really a way to con you into giving up personal information (PINs, social security numbers, credit card information, etc.)…along with its up-and-coming second cousin, "smishing," which carries on the same ruse via text messaging.

But what these criminals allegedly did—at least in the case based in Los Angeles—took this scheme a few steps farther, giving the online scam a clever offline payoff and ultimately swindling thousands of people and hundreds of financial institutions out of millions before being shut down.

Here's how it generally worked:

*Fraudsters working primarily out of Romania—known as the "suppliers"—went phishing and obtained thousands of credit and debit card accounts and related personal information by sending out masses of spam.

*These suppliers then sent their ill-gotten financial data to their partners in the U.S.—so-called "cashiers"—through Internet chat and e-mail messages.

*By using some sophisticated but readily available software and technologies, the cashiers manufactured their own credit, debit, and gift cards encoded with the stolen information, giving them unfettered access to large amounts of money via ATMs and point-of-sale terminals.

*Before these cards were used, cashiers directed "runners" to test the cards by checking balances or withdrawing small amounts of money from ATMs. Then, these "cashable" cards were used on the most lucrative accounts.

*To bring the scheme full circle, the cashiers wired a percentage of the illegal proceeds back to the suppliers.

The L.A. investigation—as well as the second case based in Connecticut—was made possible through their growing partnerships. In California, we worked with the U.S. Postal Service, the IRS, several local law enforcement agencies, and the Romanian General Inspectorate of Police. In the Connecticut case, our efforts dovetailed with the multi-agency Connecticut Computer Crimes Task Force.

The indictments, fittingly, come on the heels of a comprehensive new strategy to fight global organized crime by uniting the efforts of the Department of Justice and nine federal law enforcement agencies.

The cases are a cautionary tale, of course, for anyone who uses e-mail or text messaging—which is most of us these days. We can't say it often enough: don't respond to unsolicited e-mails or text messages from companies you do business with. If you aren't sure, contact the company to verify that the message is legit.

## Warning #38. The "Ponzi' Schemes

"Ponzi" schemes promise high financial returns or dividends not available through traditional investments. Instead of investing the funds of victims, however, the con artist pays "dividends" to initial investors using the funds of subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

This type of fraud is named after its creator—Charles Ponzi of Boston, Massachusetts. In the early 1900s, Ponzi launched a scheme that guaranteed investors a 50 percent return on their investment in postal coupons. Although he was able to pay his initial backers, the scheme dissolved when he was unable to pay later investors.

<u>Tips for Avoiding Ponzi Schemes:</u>

*Be careful of any investment opportunity that makes exaggerated earnings claims.

*Exercise due diligence in selecting investments and the people with whom you invest—in other words, do your homework.

*Consult an unbiased third party—like an unconnected broker or licensed financial advisor—before investing.

## Warning #39. Prime Bank Note Fraud

International fraud artists have invented an investment scheme that supposedly offers extremely high yields in a relatively short period of time. In this scheme, they claim to have access to "bank guarantees" that they can buy at a discount and sell at a premium. By reselling the "bank guarantees" several times, they claim to be able to produce exceptional returns on investment. For example, if $10 million worth of "bank guarantees" can be sold at a two percent profit on 10 separate occasions—or "traunches"—the seller would receive a 20 percent profit. Such a scheme is often referred to as a "roll program."

To make their schemes more enticing, con artists often refer to the "guarantees" as being issued by the world's "prime banks," hence the term "prime bank guarantees." Other official sounding terms are also used, such as "prime bank notes" and "prime bank debentures." Legal documents associated with such schemes often require the victim to enter into non-disclosure and non-circumvention agreements, offer returns on investment in "a year and a day", and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has issued a warning to all potential investors that no such investments exist.

The purpose of these frauds is generally to encourage the victim to send money to a foreign bank, where it is eventually transferred to an off-shore account in the control of the con artist. From there, the victim's money is used for the perpetrator's personal expenses or is laundered in an effort to make it disappear.

While foreign banks use instruments called "bank guarantees" in the same manner that U.S. banks use letters of credit to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.

<u>Tips for Avoiding Prime Bank Note Fraud:</u>

*Think before you invest in anything. Be wary of an investment in any scheme, referred to as a "roll program," that offers unusually high yields by buying and selling anything issued by "prime banks."

*As with any investment, perform due diligence. Independently verify the identity of the people involved, the veracity of the deal, and the existence of the security in which you plan to invest.

*Be wary of business deals that require non-disclosure or non-circumvention agreements that are designed to prevent you from independently verifying information about the investment.

Warning #40. Investors Beware of Stock Fraud

If you're not familiar with "pump-and-dump" fraud schemes, it might be a good time to get educated.

That's because the FBI and its partners are now wrapping up an investigation of such a scam that was so massive it took the better part of a decade to unravel.

So far, our joint investigation has uncovered more than 40 schemes, convicted 40 perpetrators, identified thousands of victims in nearly every state and several foreign countries, and discovered hundreds of millions of dollars in losses.

In Operation "Shore Shells," so-named because it involved fake (or shell) companies and began in the coastal area of southern New Jersey, a group of co-conspirators—CEOs, stock brokers, CPAs, financial advisors, attorneys, etc.—had been engaging in pump-and-dump and other schemes for years.

How do these scams work? In this case, the ringleaders created shell companies whose penny stock (worth less than $5 a share) was traded on the OTC Bulletin Board (not on the more widely known New York Stock Exchange or NASDAQ). They secretly issued most of the shares for themselves in fictitious names, then touted their companies' stock through false statements in press releases, electronic bulletin board postings, online newsletters, and the like.

Often using their retirement funds, unsuspecting investors purchased the highly-touted stock—or their unscrupulous financial advisors did so without their knowledge—driving or "pumping" up the price. Then, the fraudsters "dumped," or sold, their stock for thousands or millions of dollars, causing the stock to plummet and innocent investors to lose their shirts.

In many cases, the losses were significant. And while running an undercover operation and gathering enough evidence to put the criminals behind bars, our focus has been on helping victims get some of their hard-earned money back. We spent years interviewing more than 600 mainly elderly victims, painstakingly documenting their sometimes heartbreaking losses. For example:

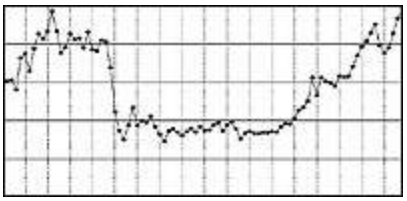
*We assisted a doctor from a prestigious hospital who began suffering from severe depression after learning of the scam and became unable to work. To help a husband and wife who had both developed dementia during the investigation, our agents traveled to their nursing home and spent hours with them, their family members, and their accountants to substantiate their financial losses.

*We worked with a man suffering from multiple sclerosis whose stockbroker had liquidated his pension and IRA and left him nearly penniless.

*We learned of another victim who not only invested her savings and her pension, but also took out a second mortgage to invest more. Needless to say, she lost everything.

It was worth the effort. So far, more than 100 seizures and forfeitures totaling over $70 million in cash, artwork, jewelry, homes, cars, and other valuables have been made, and criminals have been ordered to pay more than $130 million in restitution. We expect millions more to be forfeited and repaid to the victims.

Because of their work on behalf of the victims in this case, the investigative team—comprised of special agents from our Atlantic City Resident Agency (out of the Newark FBI office), a Criminal Investigation agent from the Internal Revenue Service, and the Newark FBI's victim/witness specialist—was awarded the FBI Director's Annual Award for Distinguished Service for Assisting Victims of Crime



How ‘Pump and Dump’ Works:

First, there’s the glowing press release about a company, usually on its financial health or some new product or innovation.

Then, newsletters that purport to offer unbiased recommendations may suddenly tout the company as the latest “hot” stock. Messages in chat rooms and bulletin board postings may urge you to buy the stock quickly or to sell before the price goes down. Or you may even hear the company mentioned by a radio or TV analyst.

Unsuspecting investors then purchase the stock in droves, pumping up the price. But when the fraudsters behind the scheme sell their shares at the peak and stop hyping the stock, the price plummets, and innocent investors lose their money.

Fraudsters frequently use this ploy with small, thinly traded companies because it’s easier to manipulate a stock when there’s little or no information available about the company. To steer clear of potential scams, always investigate before you invest.

Steps You Can Take:

- Don’t believe the hype.
- Find out where the stock trades.
- Independently verify claims.
- Research the opportunity.
- Beware of high-pressure pitches.

- Always be skeptical.

## Warning #41. The Pyramid Schemes

As in Ponzi schemes, the money collected from newer victims of the fraud is paid to earlier victims to provide a veneer of legitimacy. In pyramid schemes, however, the victims themselves are induced to recruit further victims through the payment of recruitment commissions.

More specifically, pyramid schemes—also referred to as franchise fraud or chain referral schemes—are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product. The real profit is earned, not by the sale of the product, but by the sale of new distributorships. Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses. At the heart of each pyramid scheme is typically a representation that new participants can recoup their original investments by inducing two or more prospects to make the same investment. Promoters fail to tell prospective participants that this is mathematically impossible for everyone to do, since some participants drop out, while others recoup their original investments and then drop out.

<u>Tips for Avoiding Pyramid Schemes:</u>

*Be wary of “opportunities” to invest your money in franchises or investments that require you to bring in subsequent investors to increase your profit or recoup your initial investment.

*Independently verify the legitimacy of any franchise or investment before you invest.

**Warning #42 The Ransomware: It Locks Computers, Demands Payment**

There is a new “drive-by” virus on the Internet, and it often carries a fake message—and fine—purportedly from the FBI.

Reveton is described as drive-by malware because unlike many viruses—which activate when users open a file or attachment—this one can install itself when users simply click on a compromised website. Once infected, the victim’s computer immediately locks, and the monitor displays a screen stating there has been a violation of federal law.

The bogus message goes on to say that the user’s Internet address was identified by the FBI or the Department of Justice’s Computer Crime and Intellectual Property Section as having been associated with child pornography sites or other illegal online activity. To unlock their machines, users are required to pay a fine using a prepaid money card service.

“Some people have actually paid the so-called fine,” said the IC3’s Gregory, who oversees a team of cyber crime subject matter experts. (The IC3 was established in 2000 as a partnership between the FBI and the National White Collar Crime Center. It gives victims an easy way to report cyber crimes and provides law enforcement and regulatory agencies with a central referral system for complaints.)

“While browsing the Internet, a window popped up with no way to close it,” one Reveton victim recently wrote to the IC3. “The window was labeled ‘FBI’ and said I was in violation of one of the following: illegal use of downloaded media, under-age porn viewing, or computer-use negligence. It listed fines and penalties for each and directed me to pay $200 via a MoneyPak order. Instructions were given on how to load the card and make the payment. The page said if the demands were not met, criminal charges would be filed and my computer would remain locked on that screen.”

The Reveton virus, used by hackers in conjunction with Citadel malware—a software delivery platform that can disseminate various kinds of computer viruses—first came to the attention of the FBI in 2011. The IC3 issued a warning on its website in May 2012. Since that time, the virus has become more widespread in the United States and internationally. Some variants of Reveton can even turn on computer webcams and display the victim’s picture on the frozen screen.

“We are getting dozens of complaints every day,” Gregory said, noting that there is no easy fix if your computer becomes infected. “Unlike other viruses,” she explained, “Reveton freezes your computer and stops it in its tracks. And the average user will not be able to easily remove the malware.”

The IC3 suggests the following if you become a victim of the Reveton virus:

*Do not pay any money or provide any personal information.

*Contact a computer professional to remove Reveton and Citadel from your computer.

*Be aware that even if you are able to unfreeze your computer on your own, the malware may still operate in the background. Certain types of malware have been known to capture personal information such as user names, passwords, and credit card numbers through embedded keystroke logging programs.

*File a complaint and look for updates about the Reveton virus on the IC3 website.

## Warning #43. Redemption / Strawman / Bond Fraud

Proponents of this scheme claim that the U.S. government or the Treasury Department control bank accounts—often referred to as “U.S. Treasury Direct Accounts”—for all U.S. citizens that can be accessed by submitting paperwork with state and federal authorities. Individuals promoting this scam frequently cite various discredited legal theories and may refer to the scheme as “Redemption,” “Strawman,” or “Acceptance for Value.” Trainers and websites will often charge large fees for “kits” that teach individuals how to perpetrate this scheme. They will often imply that others have had great success in discharging debt and purchasing merchandise such as cars and homes. Failures to implement the scheme successfully are attributed to individuals not following instructions in a specific order or not filing paperwork at correct times.

This scheme predominately uses fraudulent financial documents that appear to be legitimate. These documents are frequently referred to as “bills of exchange,” “promissory bonds,” “indemnity bonds,” “offset bonds,” “sight drafts,” or “comptrollers warrants.” In addition, other official documents are used outside of their intended purpose, like IRS forms 1099, 1099-OID, and 8300. This scheme frequently intermingles legal and pseudo legal terminology in order to appear lawful. Notaries may be used in an attempt to make the fraud appear legitimate. Often, victims of the scheme are instructed to address their paperwork to the U.S. Secretary of the Treasury.

Tips for Avoiding Redemption/Strawman/Bond Fraud:

*Be wary of individuals or groups selling kits that they claim will inform you on to access secret bank accounts.

*Be wary of individuals or groups proclaiming that paying federal and/or state income tax is not necessary.

*Do not believe that the U.S. Treasury controls bank accounts for all citizens.

*Be skeptical of individuals advocating that speeding tickets, summons, bills, tax notifications, or similar documents can be resolved by writing “acceptance for value” on them.

*If you know of anyone advocating the use of property liens to coerce acceptance of this scheme, contact your local FBI office.

## Warning #44. The Reverse Mortgage Scams

The FBI and the U.S. Department of Housing and Urban Development Office of Inspector General (HUD-OIG) urge consumers, especially senior citizens, to be vigilant when seeking reverse mortgage products. Reverse mortgages, also known as home

equity conversion mortgages (HECM), have increased more than 1,300 percent between 1999 and 2008, creating significant opportunities for fraud perpetrators.

Reverse mortgage scams are engineered by unscrupulous professionals in a multitude of real estate, financial services, and related companies to steal the equity from the property of unsuspecting senior citizens or to use these seniors to unwittingly aid the fraudsters in stealing equity from a flipped property.

In many of the reported scams, victim seniors are offered free homes, investment opportunities, and foreclosure or refinance assistance. They are also used as straw buyers in property flipping scams. Seniors are frequently targeted through local churches and investment seminars, as well as television, radio, billboard, and mailer advertisements.

A legitimate HECM loan product is insured by the Federal Housing Authority. It enables eligible homeowners to access the equity in their homes by providing funds without incurring a monthly payment. Eligible borrowers must be 62 years or older who occupy their property as their primary residence and who own their property or have a small mortgage balance. See the FBI/HUD Intelligence Bulletin for specific details on HECMs as well as other foreclosure rescue and investment schemes.

Tips for Avoiding Reverse Mortgage Scams:

*Do not respond to unsolicited advertisements.

*Be suspicious of anyone claiming that you can own a home with no down payment.

*Do not sign anything that you do not fully understand.

*Do not accept payment from individuals for a home you did not purchase.

*Seek out your own reverse mortgage counselor.

If you are a victim of this type of fraud and want to file a complaint, please submit information through the FBI tip line or through your local FBI office.

**Warning #45. 'Scareware'**

One of the most widespread types of cyber scam being perpetrated against consumers these days involves "scareware"—those pop-up messages you see on your computer saying you've got a virus and all you have to do to get rid of it is buy the antivirus software being advertised.

And if you don't buy it? The pop-ups continue unabated, and in some instances, the scareware renders all of the information on your computer inaccessible.

But today, the Department of Justice and the FBI announced "Operation Trident Tribunal," a coordinated, international law enforcement action that disrupted the activities of two international cyber crime rings involved in the sale of scareware. The groups are believed responsible for victimizing more than one million computer users and causing more than $74 million in total losses.

Scam #1: The FBI's Seattle office began looking into a scareware scam, later attributed to a group based in Kyiv, Ukraine, that ultimately claimed an estimated 960,000 victims who lost a total of $72 million. Investigators discovered a variety of ruses used to infect computers with scareware, including consumers being directed to webpages featuring fake computer scans that instead downloaded malicious software. The Security Service of Ukraine (SBU) deployed more than 100 officers as it orchestrated this phase of the operation in conjunction with the German BKA, Latvian State Police, and Cyprus National Police. Results included the execution of numerous search warrants, subject interviews, and seized bank accounts and a server.

Scam #2: The FBI's Minneapolis office initiated an investigation into an international criminal group using online advertising to spread its scareware product, a tactic known as "malvertising." According to a U.S. federal indictment unsealed today, two individuals in Latvia were charged with creating a phony advertising agency and claiming to represent a hotel chain that wanted to purchase online advertising space on a

Minneapolis newspaper's website. After the ad was verified by the paper and posted, the defendants changed the ad's computer code so that visitors to the site became infected with a malicious software program that launched scareware on their computers. That scheme resulted in losses of about $2 million to its victims. The Latvian State Police led this phase of the operation, with the SBU and Cyprus National Police.

In a true reflection of the international nature of cyber crime, "Trident Tribunal" was the result of significant cooperation among 12 nations: Ukraine, Latvia, Germany, Netherlands, Cyprus, France, Lithuania, Romania, Canada, Sweden, the United Kingdom, and the U.S. So far, the case has resulted in two arrests abroad, along with the seizure of more than 40 computers, servers, and bank accounts. Because of the magnitude of the schemes, law enforcement agencies here and abroad are continuing their investigative efforts.

How to spot scareware on your own computer:

*Scareware pop-ups may look like actual warnings from your system, but upon closer inspection, some elements aren't fully functional. For instance, to appear authentic, you may see a list of reputable icons—like software companies or security publications—but you can't click through to go to those actual sites.

*Scareware pop-ups are hard to close, even after clicking on the "Close" or "X" button.

*Fake antivirus products are designed to appear legitimate, with names such as Virus Shield, Antivirus, or VirusRemover.

And to avoid being victimized, make sure your computer is using legitimate, up-to-date antivirus software, which can help detect and remove fraudulent scareware products.

What is Scareware? Simple Definition

Scareware is malicious software that poses as legitimate computer security software and claims to detect a variety of threats on the affected computer that do not actually exist. Users are then informed they must purchase the scareware in order to repair their computers and are barraged with aggressive and disruptive notifications until they supply their credit card number and pay up to $129 for the worthless scareware product.

## Warning #46. University Employee Payroll Scam

University employees are receiving fraudulent e-mails indicating a change in their human resource status. The e-mail contains a link directing the employee to login to their human resources website to identify this change. The website provided appears very similar to the legitimate site in an effort to steal the employee's credentials. Once the employee enters his/her login information, the scammer takes that information and signs into the employee's official human resources account to change the employee's direct deposit information. This redirects the employee's paycheck to the bank account of another individual involved in the scam.

Consequences of this Scam:

*The employee's paycheck can be stolen.

*The money may not be returned in full to the employee.

*The scammers can take the employee's log-in credentials and attempt to log into other accounts that belong to the employee.

<u>Tips on how to Protect Yourself from this Scam:</u>

*Look for poor use of the English language in e-mails such as incorrect grammar, capitalization, and tenses. Many of the scammers who send these messages are not

native English speakers.

*Roll your cursor over the links received via e-mail and look for inconsistencies. If it is not the website the e-mail claims to be directing you to then the link is to a fraudulent site.

*Never provide credentials of any sort via e-mail. This includes after clicking on links sent via e-mail. Always go to an official website rather than from a link sent to you via e-mail.

*Contact your personnel department if you receive suspicious e-mail.

**Warning #47. College Students Scams Across the United States**

College students across the United States have been targeted to participate in work-from-home scams. Students have been receiving e-mails to their school accounts recruiting them for payroll and/or human resource positions with fictitious companies. The "position" simply requires the student to provide his/her bank account number to receive a deposit and then transfer a portion of the funds to another bank account. Unbeknownst to the student, the other account is involved in the scam that the student has now helped perpetrate. The funds the student receives and is directed elsewhere have been stolen by cyber criminals. Participating in the scam is a crime and could lead to the student's bank account being closed due to fraudulent activity or federal charges.

<u>Here's how the scam works:</u>

*The student is asked to provide his/her bank account credentials under the guise of setting up direct deposit for his/her pay.

*The scammers will add the student's bank account to a victim employee's direct deposit information to redirect the victim's payroll deposit to the student's account.

*The student will receive the payroll deposit from the victim's employer in the victim's name.

*The student will be directed to withdraw funds from the account and send a portion of the deposit, via wire transfer, to other individuals involved in the scam.

Consequences of Participating in the Scam:

*The student's bank account will be identified by law enforcement as being involved in the fraud.

*The victim employee has his/her pay stolen by the scammers utilizing the student's bank account.

*Without the student's participation, the scam could not be perpetrated, so he/she facilitated the theft of the paycheck.

*The student could be arrested and prosecuted in federal court. A criminal record will stay with the student for the rest of his/her life and will have to be divulged on future job applications, which could prevent the student from being hired.

*The student's bank account may be closed due to fraudulent activity and a report could be filed by the bank.

*This could adversely affect the student's credit record.

Tips on how to Protect Yourself from this Scam:

*If a job offer sounds too good to be true, it probably is.

*Never accept a job that requires the depositing of funds into your account and wiring them to different accounts.

*Look for poor use of the English language in e-mails such as incorrect grammar, capitalization, and tenses. Many of the scammers who send these messages are not native English speakers.

*Never provide credentials of any kind such as bank account information, login names, passwords, or any other identifying information in response to a recruitment e-mail.

*Forward these e-mails to the university's IT personnel and tell your friends to be on the lookout for the scam.

*This could adversely affect the student's credit record.

**Warning #48. Senior Citizen Fraud**

A Canadian couple is arrested for allegedly bilking victims across the U.S. by selling bogus credit card protection plans over the phone.

A Maryland financial planning/estate lawyer pleads guilty to defrauding his own clients.

A California man is convicted of stealing nearly $5 million from residents of a retirement home through an investment scheme.

What's the common thread here? All of the victims were elderly, and many lost their life savings.

Why are the elderly such an attractive target for con artists?

*Many seniors have a “nest egg.”

*They’re less likely to report a fraud because they don’t know where to go or they’re too embarrassed to talk about it.

*If they do report the crime, it’s sometimes hard for them to remember exact details.

*Many of the products/services being hawked by con artists appeal to individuals of a certain age—i.e., anti-aging and other health care products, health care services, and investments related to retirement savings.

The threat to seniors is growing…and changing. Baby boomers (born between 1946 and 1964) are now the largest segment of our population—about 78 million people. That means that the number of senior citizens is rising. Many younger boomers also have considerable computer skills, so criminals are modifying their targeting techniques—using not only traditional telephone calls and mass mailings but also online scams like phishing and e-mail spamming.

Another trend: Criminals targeting the elderly are increasingly located outside the U.S., making it difficult for American law enforcement to track them down.

The scams. Some common ones to look out for:

*Identity theft (accomplished through “dumpster diving,” phishing, address changes, old-fashioned theft);

*Health insurance frauds (medical equipment, “rolling lab” schemes, Medicare fraud, counterfeit prescription drugs);

*Home repair schemes;

*Foreign lottery/sweepstakes fraud;

Advance fee/credit card frauds;

*Investment fraud; and

*Charity schemes.

Recovery schemes are also worth mentioning because they're especially cold-hearted: they target previous victims by convincing them that their money has been recovered by law enforcement or government officials but that they must pay a fee to get it back.

A few basic tips to avoid being victimized:

*Shred credit card receipts and old bank statements;

*Close unused credit card or bank accounts;

Don't give out personal information via the phone, mail, or Internet unless you initiated the contact;

*Never respond to an offer you don't understand;

*Talk over investments with a trusted friend, family member, or financial advisor;

*Require all plans and purchases to be in writing; and

*Don't pay in advance for services.

Who to call. If you're a senior citizen who has been victimized by fraud, start by calling your local or state law enforcement agency.

**Warning #49. The Smishing and Vishing Scams**

You receive a text message or an automated phone call on your cell phone saying there's a problem with your bank account. You're given a phone number to call or a website to log into and asked to provide personal identifiable information—like a bank account number, PIN, or credit card number—to fix the problem.

But beware: It could be a "smishing" or "vishing" scam…and criminals on the other end of the phone or website could be attempting to collect your personal information in order to help themselves to your money. While most cyber scams target your computer, smishing and vishing scams target your mobile phone, and they're becoming a growing threat as a growing number of Americans own mobile phones. (Vishing scams also target land-line phones.)

"Smishing"—a combination of SMS texting and phishing—and "Vishing"—voice and phishing—are two of the scams the FBI's Internet Crime Complaint Center (IC3) is warning consumers about as we head into the holiday shopping season. These scams are also a reminder that cyber crimes aren't just for computers anymore.

Here's how smishing and vishing scams work: criminals set up an automated dialing system to text or call people in a particular region or area code (or sometimes they use stolen customer phone numbers from banks or credit unions). The victims receive messages like: "There's a problem with your account," or "Your ATM card needs to be reactivated," and are directed to a phone number or website asking for personal information. Armed with that information, criminals can steal from victims' bank accounts, charge purchases on their charge cards, create a phony ATM card, etc.

Sometimes, if a victim logs onto one of the phony websites with a smartphone, they could also end up downloading malicious software that could give criminals access to anything on the phone. With the growth of mobile banking and the ability to conduct financial transactions online, smishing and vishing attacks may become even more attractive and lucrative for cyber criminals.

Here are a couple of recent smishing case examples:

*Account holders at one particular credit union, after receiving a text about an account problem, called the phone number in the text, gave out their personal information, and had money withdrawn from their bank accounts within 10 minutes of their calls.

*Customers at a bank received a text saying they needed to reactivate their ATM card. Some called the phone number in the text and were prompted to provide their ATM card number, PIN, and expiration date. Thousands of fraudulent withdrawals followed.

Other holiday cyber scams to watch out for:

*Phishing schemes using e-mails that direct victims to spoofed merchant websites misleading them into providing personal information.

*Online auction and classified ad fraud, where Internet criminals post products they don't have but charge the consumer's credit card anyway and pocket the money.

*Delivery fraud, where online criminals posing as legitimate delivery services offer reduced or free shipping labels for a fee. When the customer tries to ship a package using a phony label, the legitimate delivery service flags it and requests payment from the customer.

More Tips to Protect Yourself From Cyber Scams:

- Don't respond to text messages or automated voice messages from unknown or

blocked numbers on your mobile phone.

- Treat your mobile phone like you would your computer…don't download anything unless you trust the source.

- When buying online, use a legitimate payment service and always use a credit card because charges can be disputed if you don't receive what you ordered or find unauthorized charges on your card.

- Check each seller's rating and feedback along with the dates the feedback was posted. Be wary of a seller with a 100 percent positive feedback score, with a low number of feedback postings, or with all feedback posted around the same date.

- Don't respond to unsolicited e-mails (or texts or phone calls, for that matter) requesting personal information, and never click on links or attachments contained within unsolicited e-mails. If you want to go to a merchant's website, type their URL directly into your browser's address bar.

**Warning #50. Celebrity Memorabilia Fraud**

We're delighted to showcase yesterday's press conference in San Diego that updates you on our ongoing, national investigation of forgers and counterfeiters who specially prey on fans. All told, 63 persons charged and convicted; 18 forgery rings dismantled; tens of thousands of forged baseballs, basketballs, you name it seized.

And we're equally delighted to announce that, with our partners in law enforcement, sports, and business, thousands of contraband baseballs, bats, and basketballs—scrubbed clean of the forgeries—were presented at the press conference to kids in organizations like the Boys and Girls Clubs, Special Olympics, Crime Victims Fund, and the It's All About the Kids Foundation.

It's a classic win-win situation. But we want to spread the word well beyond San Diego on how YOU can keep from getting cheated.

In the market for that special autographed photo of your favorite celebrity...or a baseball bat signed by Steve Carlton? Let the buyer beware:

*Try to get the signatures in person—either at an event where they're performing or at an event where they're signing.

*Buy from companies that get witnessed-based signings and that document the authenticity. Major League Baseball, for example, has a program that uses Deloitte and Touche as the witnessing agent with tamper-proof holograms affixed to items that are uniquely numbered and tracked in a database. The point is that these programs establish a chain of custody that ensures you're getting what you want...and guarantees its value. Many companies offer this program, you just have to ask.

*If options one and two are not possible, aggressively question the seller about the exact history of the item you want to buy...and be completely comfortable that you are dealing with an honest broker. We've talked to a lot of convicted forgers and they say that they really don't like being asked to explain the provenance of their forgeries. ALWAYS ASK FOR A MONEY BACK GUARANTEE AND A RECEIPT.

*Get your items evaluated by professional authenticators. And we don't mean the bogus authenticators that convicted forgers set up to hide behind. Even independent, legitimate authenticators can be fooled from time to time, but they are your best bet to keep from being cheated.

*Last but not least—and you know this: If the price is too good to be true, your treasure is probably a forgery. Like those three baseballs we found "autographed" by Mother Teresa!!

**Warning #51. Spear Phishers Scams**

How It Goes: Customers of a telecommunications firm received an e-mail recently explaining a problem with their latest order. They were asked to go to the company website, via a link in the e-mail, to provide personal information—like their birthdates and Social Security numbers. But both the e-mail and the website were bogus.

It's a real-life, classic case of "phishing"—a virtual trap set by cyber thieves that uses official-looking e-mails to lure you to fake websites and trick you into revealing your personal information.

It's also an example of an even more mischievous type of phishing known as "spear phishing"—a rising cyber threat that you need to know about.

Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc. The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive.

How spear phishing works. First, criminals need some inside information on their targets to convince them the e-mails are legitimate. They often obtain it by hacking into an organization's computer network (which is what happened in the above case) or sometimes by combing through other websites, blogs, and social networking sites.

Then, they send e-mails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need your personal data.

Finally, the victims are asked to click on a link inside the e-mail that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc.

Criminal gain, your loss. Once criminals have your personal data, they can access your bank account, use your credit cards, and create a whole new identity using your information.

Spear phishing can also trick you into downloading malicious codes or malware after you click on a link embedded in the e-mail…an especially useful tool in crimes like economic espionage where sensitive internal communications can be accessed and trade secrets stolen. Malware can also hijack your computer, and hijacked computers can be organized into enormous networks called botnets that can be used for denial of service attacks.

How to avoid becoming a spear phishing victim. Law enforcement takes this kind of crime seriously, and so does FBI who works with other partners, including the U.S. Secret Service and investigative agencies within the Department of Defense. But what can you do to make sure you don't end up a victim in one of our cases?

*Keep in mind that most companies, banks, agencies, etc., don't request personal information via e-mail. If in doubt, give them a call (but don't use the phone number contained in the e-mail—that's usually phony as well).

*Use a phishing filter…many of the latest web browsers have them built in or offer them as plug-ins.

*Never follow a link to a secure site from an e-mail—always enter the URL manually.

*Don't be fooled (especially today) by the latest scams.

## Warning #52. Staged Auto Accident Fraud

Consider this scenario: You're stuck in heavy traffic on a busy highway. Another car cuts off the driver in front of you, forcing him to slam on the brakes. You try to stop, but there's no time…and you rear-end the guy in front of you.

An everyday accident? Not this time. Turns out you've been had by a well-organized

criminal ring that staged the entire thing.

This particular scam is called the “swoop and squat.” (The first car “swoops” in while the second car “squats” in front of you.) After the “accident,” everyone in the car you rear-ended—usually crammed full of passengers—will file bogus injury claims with your insurance company. Each will complain of whiplash or other soft-tissue injuries—things difficult for doctors to confirm. They may even go to crooked physical therapists, chiropractors, lawyers, or auto repair technicians to further exaggerate their claims.

We’re talking big money here. Staged accidents cost the insurance industry about $20 billion a year. Those losses get passed on to all of us in the form of higher insurance rates—an average of $100-$300 extra per car per year.

Here are some similar scams to look out for:

*The drive down. You’re attempting to merge when another driver waves you forward. Instead of letting you in, he slams into your car. When the police arrive, he denies ever motioning to you.

*The sideswipe. As you round a corner at a busy intersection with multiple turn lanes, you drift slightly into the lane next to you. The car in that lane steps on the gas and sideswipes you.

*The t-bone. You’re crossing an intersection when a car coming from a side street accelerates and hits your car. When the police arrive, the driver and several planted “witnesses” claim that you ran a red light or stop sign.

How can you protect yourself?

*If you’re in an accident, call the police immediately.

*Report accident claims to your insurance company. Don’t settle on site with cash.

*Be careful with your personal information, mindful of identity theft.

*If you can, photograph the car and passengers and write down names, addresses, and phone numbers.

*Use medical, car repair, and legal professionals you know and trust.

*Don’t tail gate…drive safely.

What are Lawenforcement doing to protect you from these schemes? Plenty. Like Operation Soft Tissue, where a Chicago agent posed as a corrupt lawyer and caught hundreds of these con artists and crooks red-handed. They've investigated more than 90 staged accident fraud cases over the past decade. With more to come!

**Warning #53. The Surrogacy Scam**

It’s a shocking tale.

Three women recently pled guilty in San Diego, admitting to taking part in a scheme to illegally create an inventory of babies to sell to unwitting would-be parents for fees of between $100,000 and $150,000 each.

The three took advantage of couples who desperately wanted children, offering them seemingly legitimate surrogacy situations. They also took advantage of women recruited as “gestational carriers” to carry pregnancies to term after having embryos transferred to their uteruses.

The defendants in this case included two lawyers who specialized in reproductive law: Theresa Erickson, a well-known California attorney, and Hilary Neiman, who operated an adoption/surrogacy agency in Maryland. The third conspirator was Carla Chambers of Nevada, who served as the "surrogacy facilitator." Together, they circumvented surrogacy regulations that say contracts between surrogates and intended parents must be executed before a pregnancy occurs…and lied to surrogates, intended parents, and the California family court.

Here's how the scam worked:

Chambers admitted visiting adoption/surrogacy-themed online chat rooms and forums in search of surrogates and parents. Erickson and Neiman also used their own sterling reputations to legitimize the scheme.

Surrogates were made to travel to Ukraine in Eastern Europe to become implanted with embryos derived from anonymous donors—Chambers usually made all the arrangements—with the promise that they would be compensated by the intended parents. The women were led to believe that they were participating in legal surrogacy arrangements and that there was a waiting list of potential parents for the babies. They also had to agree to give birth in California.

They were promised quick matches with intended parents, but the co-conspirators usually waited until the second or even third trimester of the pregnancies before seeking parents. Neiman and Erickson then drafted contracts between the surrogates and intended parents, well after the time frame required by law.

The hopeful couples were told the unborn babies were the result of legitimate surrogacy arrangements, but the original intended parents had backed out. They were offered the opportunity to "assume" the non-existent surrogacy agreement. The parents would hand over between $100,000 and $150,000 to the defendants, but less than half of that went to the surrogate—Erickson, Neiman, and Chambers pocketed the rest.

The defendants typically used the Internet to recruit, solicit, and communicate with surrogates and intended parents. Most of the surrogates and parents lived outside of California.

One of the most critical aspects of the scheme involved Erickson filing fraudulent documents in California court stating that a surrogacy agreement had been in place from the start and asking for what's called a "pre-birth judgment" that would establish parental rights. That way, under California law, the names of the intended parents could be placed on the birth certificate when the baby was born.

The scam was uncovered when one of the surrogates, nearly seven months pregnant, was worried that parents hadn't been found for the baby she was carrying. She contacted a lawyer, who then contacted the FBI's San Diego office.

Tips to Avoid Surrogacy Schemes:

- Do your due diligence to find out the average costs of surrogacy services (there should be no "facilitator" fees).

- Make sure you have a signed agreement in place before the start of any medical tests or procedures.

- Be leery if you're offered a last-minute surrogacy arrangement and are told the original intended parents changed their minds (that rarely happens).

- If at all possible, work with a local attorney or agency that you can meet with in person.

- Ask lots of questions…about the process, about financial arrangements, about the surrogates or biological parents…until you're completely satisfied.

- If you still don't feel quite right about it, find another attorney or agency that you are comfortable with.

**Warning #54. 'Swatting'**

Do You Remember the "phone phreakers?" The term hit our national consciousness in the 1970s, when a magazine reported on a small group of techie troublemakers who were hacking into phone companies' computers and making free long-distance calls.

Today, there's a new, much more serious twist on this old crime. It's called "swatting," and it involves calling 9-1-1 and faking an emergency that draws a response from law enforcement—usually a SWAT team.

Needless to say, these calls are dangerous to first responders and to the victims. The callers often tell tales of hostages about to be executed or bombs about to go off. The community is placed in danger as responders rush to the scene, taking them away from real emergencies. And the officers are placed in danger as unsuspecting residents may try to defend themselves.

Last year, for example, a 19-year-old Washington state man was charged by California authorities after pretending to be calling from the home of a married California couple, saying he had just shot and murdered someone. A local SWAT team arrived on the scene, and the husband, who had been asleep in his home with his wife and two young children, heard something and went outside to investigate—after first stopping in the kitchen to pick up a knife. What he found was a group of SWAT assault rifles aimed directly at him. Fortunately, the situation didn't escalate, and no one was injured.

<u>The schemes can also be fairly sophisticated.</u>

*Five swatters in several states targeted people who were using online telephone party chat lines (or their family or friends).

*The swatters found personal details on the victims by accessing telecommunication company information stored on protected computers.

*Then, by manipulating computer and phone equipment, they called 9-1-1 operators around the country. By using “spoofing technology,” the swatters even made it look like the calls were actually coming from the victims!

*Between 2002 and 2006, the five swatters called 9-1-1 lines in more than 60 cities nationwide, impacting more than 100 victims, causing a disruption of services for telecommunications providers and emergency responders, and resulting in up to $250,000 in losses.

*“Swats” that the group committed included using bomb threats at sporting events, causing the events to be delayed; claiming that hotel visitors were armed and dangerous, causing an evacuation of the entire hotel; and making threats against public parks and officials.

Case work. The swatters were tracked down through the cooperative efforts of local, state, and federal agencies and the assistance of telecommunications providers and first responders. In all, the case involved more than 40 state and local jurisdictions in about a dozen states. All five subjects have pled guilty to various charges and are scheduled to be sentenced in 2008.

Why did they do it? Majority of them said, they did it for the bragging rights and ego, versus any monetary gain.” Basically, they did it because they could.

Law enforcement agencies at all levels are currently working with telecommunications providers around the country to help them address swatting activity.

You can help, too—if you believe you’ve been a victim of a “swat” please contact your local FBI office.

**Warning #55. Sweepstakes Fraud**

A North Carolina couple recently pled guilty to running a sweepstakes fraud scheme that targeted elderly Americans, in some cases causing victims to lose their entire life savings.

Jessica and Jason Brown acknowledged in federal court that they operated call centers in Costa Rica that falsely informed U.S. residents—predominantly senior citizens—that they had won a substantial cash prize in a global sweepstakes, but the prize was only redeemable if the "winners" sent money to cover insurance and other fees. From 2004 until 2013, the Browns and their crew fleeced hundreds of elderly Americans out of nearly $900,000

"They could make themselves extremely believable over the phone," said Special Agent Scott Duffey, who investigated the case from our Baltimore Division. "For people on the other end of the line who were even a little bit gullible or desperate for money, the deception could be too much to resist."

"The victims of these scams are not just people without an education," noted Pat Donley, a senior litigator with the Department of Justice who has prosecuted many sweepstakes fraud cases. "Some victims have been doctors, others Ph.Ds. They are just taken in."

Those who carry out these types of telemarketing frauds, including the Browns, use Internet technology and even forged documents to dupe their victims. They also purchase marketing lists—commonly used by lawful telemarketers—so they may know something about their victims, such as credit cards they might possess

The fraudsters work out of so-called boiler rooms, usually apartments or offices with banks of phones. They might make hundreds of calls before finding one person receptive to their pitch. Typically, the criminals say they are calling on behalf of some reputable insurance company or a U.S. federal agency such as the Federal Trade Commission or the Internal Revenue Service. The imposters say they want to make sure all the taxes are paid on the sweepstakes money so the winner faces no legal or tax issues.

To mask that they were calling from Costa Rica, the Browns used readily available technology that made victims think they were talking to someone from an area code in

Washington, D.C. This added a further air of legitimacy to the scheme, since the callers frequently claimed to be representing a U.S. federal agency.

Though initial prizes were usually billed as second-place winnings, the $350,000 to $400,000 figures were still substantial. The victims were told they would have to pay fees and taxes of about 10 percent—between $3,500 and $4,000—and were often directed to send the money via Western Union.

It didn't stop there. After receiving money, the scammers would contact the victims again and inform them that their prize amount had increased, either because of a clerical error or because another prize winner was disqualified. Of course, the new, larger prize meant more taxes and fees. The attempts to collect more cash would continue until a victim either ran out of money or realized what was going on, Duffey explained. "One Delaware woman was swindled out of more than $300,000—her life savings," he added.

Donley has seen similar schemes ruin elderly victims financially. "One person in Florida gave up more than $800,000," he said, "and a woman from California gave up most of her savings that she was going to use to care for her two handicapped children. These criminals are heartless," he continued. "It's easy for them to rob people, because they never meet the victims and never see the consequences."

Follow These Tips:

Criminals who prey upon the elderly through sweepstakes fraud and other telemarketing schemes can be extremely convincing, but you can avoid becoming a victim by keeping a few simple guidelines in mind.

The Federal Trade Commission (FTC), the nation's consumer protection agency charged with preventing fraud and deceptive practices in the marketplace, offers these common-sense tips:

- Don't wire money, ever. No government official will ask you to send money in this manner. If you have to pay for a prize, it's not a prize.

- Never give callers financial or personal information. Don't give out sensitive information such as your credit card or Social Security number unless you absolutely know who you're dealing with.

- Don't trust a name or number. Fraudsters use official-sounding names, like Lloyds of London of Costa Rica, to make you trust them. No matter how convincing their story—or their stationery—they are most likely lying. To make a phone call seem legitimate, scammers use technology to disguise where they are calling from. Even though it may look like they're dialing from Washington, D.C., they could be anywhere in the world.

- Put your number on the National Do Not Call Registry. This won't stop fraudsters from calling, but it should make you skeptical of random calls. Most legitimate sales people generally honor the Do Not Call list. Scammers ignore it. Register your phone number at donotcall.gov.

- Report the scam. If you get a call from a government imposter or someone attempting a sweepstakes fraud, file a complaint with the FTC at ftc.gov/complaint.

- Here's the bottom line: If someone is pitching something on the phone that doesn't sound right, you always have the option to just hang up. If it sounds too good to be true, it probably is.

## Warning #56. Telemarketing Fraud

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.

<u>Here are some warning signs of telemarketing fraud—what a caller may tell you:</u>

*"You must act 'now' or the offer won't be good."

*"You've won a 'free' gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.

*"You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.

*"You don't need to check out the company with anyone." The callers say you do not need to speak to anyone including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.

*"You don't need any written information about their company or their references."

*"You can't afford to miss this 'high-profit, no-risk' offer."

If you hear these or similar "lines" from a telephone salesperson, just say "no thank you" and hang up the telephone.

<u>More Tips for Avoiding Telemarketing Fraud:</u>

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

*Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.

*Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.

*Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.

*Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

*Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.

*Before you send money, ask yourself a simple question. "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"

*Don't pay in advance for services. Pay services only after they are delivered.

*Be wary of companies that want to send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.

*Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.

*Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.

*Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.

*Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.

*Never respond to an offer you don't understand thoroughly.

*Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.

*Be aware that your personal information is often brokered to telemarketers through third parties.

*If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.

*If you have information about a fraud, report it to state, local, or federal law enforcement agencies.

## Warning #57. The Latest Phone Scam Targets Your Bank Account

Imagine getting hundreds or thousands of calls on your home, business, or cell phone, tying up the lines. And when you answer, you hear anything from dead air to recorded messages, advertisements, or even phone sex menus.

It's annoying, no doubt. But it could be more than that—it could be a sign that you're being victimized by the latest scam making the rounds. This "telephone denial-of-service attack" could be the precursor to a crime targeting your bank accounts.

Denial-of-service attacks, by themselves, are nothing new—computer hackers use them

to take down websites by flooding them with large amounts of traffic.

In a recent twist, criminals have transferred this activity to telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens.

Why are they doing it? Turns out the calls are simply a diversionary tactic: while the lines are tied up, the criminals—masquerading as the victims themselves—are raiding the victims' bank accounts and online trading or other money management accounts.

Here, in a nutshell, is how the whole thing works:

*Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that this person's bank or financial institution would have—like account numbers and passwords. Perhaps the victim responded to a bogus e-mail phishing for information, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals.

*Using technology, the criminal ties up the victim's various phone lines.

*Then, the criminal either contacts the financial institution pretending to be the victim…or pilfers the victim's online bank accounts using fraudulent transactions. Normally, the institution calls to verify the transactions, but of course they can't get through to the victim over the phone.

*If the transactions aren't made, the criminals sometimes re-contact the financial institution as the victim and ask for it to be done. Or they add their own phone number to victims' accounts and just wait for the bank to call.

*By the time the victim or the financial institution realizes what happens, it's too late.

Law enforcement and industry response teams. First learned about this emerging scheme through one of its private industry partners, which told them about a Florida dentist who lost $400,000 from his retirement account after a denial-of-service attack on his phones.

In of April 2010 to 2015, there has definitely been a noticeable surge in telephone denial-of-service attacks, with numerous incidents having been reported in several Eastern states.

To help fight these schemes, the FBI has teamed up with the Communication Fraud Control Association—comprised of security professionals from communication providers—to analyze the patterns and trends of telephone denial-of-service attacks, educate the public, and identify the perpetrators and bring them to justice.

Ultimately, though, it's individual consumers and small- and medium-sized businesses on the front line of this battle. So take precautions: never give out personal information to an unsolicited phone caller or via e-mail; change online banking and automated telephone system passwords frequently; check your account balances often; and protect your computers with the latest virus protection and security software.

And if you think you may have been targeted by a telephone denial-of-service attack, contact your financial institution and your telephone provider, and file a complaint with the FBI's Internet Crime Complaint Center.

**Warning #58. Work at Home Jobs - Don't Fall For It**

Everyone's seen them—seductive work-at-home opportunities hyped in flyers tacked to telephone poles, in newspaper classifieds, in your e-mail, and all over the web, promising you hundreds or thousands of dollars a week for typing, stuffing envelopes, processing medical billing, etc. And it's just a phone call or mouse click away…

Might be tempting during these uncertain economic times, but beware of any offers that promise easy money for minimum effort—many are scams that fill the coffers of

criminals.

Here are a few of the most common work-at-home scams.

*Advance-fee: Starting a home-based business is easy! Just invest a few hundred dollars in inventory, set-up, and training materials, they say. Of course, if and when the materials do come, they are totally worthless…and you're stuck with the bill.

*Counterfeit check-facilitated "mystery shopper:" You're sent a hefty check and asked to deposit it into your bank account, then withdraw funds to shop and check out the service of local stores and wire transfer companies. You keep a small amount of the money for your "work," but then, as instructed, mail or wire the rest to your "employer." Sound good? One problem: the initial check was phony, and by the time your bank notifies you, your money is long gone and you're on the hook for the counterfeit check.

*Pyramid schemes: You're hired as a "distributor" and shell out big bucks for promotional materials and product inventories with little value (like get-rich quick pamphlets). You're promised money for recruiting more distributors, so you talk friends and family into participating. The scheme grows exponentially but then falls apart—the only ones who make a profit are the criminals who started it.

*Unknowing involvement in criminal activity: Criminals—often located overseas—sometimes use unwitting victims to advance their operations, steal and launder money, and maintain anonymity. For example, they may "hire" you as a U.S.-based agent to receive and re-ship checks, merchandise, and solicitations to other potential victims…without you realizing it's all a ruse that leaves no trail back to the crooks.

Add identity theft to the mix. As if these schemes aren't bad enough, many also lead to identity theft. During the application process, you're often asked to provide personal information that can be used to steal from your bank account or establish new credit cards in your name.

On the job. A host of law enforcement and regulatory agencies, including the FBI, investigate these schemes and track down those responsible. But the most effective

weapon against these fraudsters is you not falling for the scams in the first place.

Here's A few tips:

*Contact the Better Business Bureau to determine the legitimacy of the company.

*Be suspicious when money is required up front for instructions or products.

*Don’t provide personal information when first interacting with your prospective employer.

*Do your own research into legitimate work-at-home opportunities, using the “Work-at-Home Sourcebook” and other resources that may be available at your local library.

*Ask lots of questions of potential employers—legitimate companies will have answers for you!

"Remember if you or some one you know has been scammed -- don't forget to contact your local lawenforcement agency or FBI's Internet Crime Complaint Center to file a complaint".