**Internet Fraud**

You may be at risk if you answer “yes” to any of the following questions:

* Do you visit websites by clicking on links within an e-mail?
* Do you reply to e-mails from persons or businesses you are not familiar with?
* Have you received packages to hold or ship to someone you met on the Internet?
* Have you been asked to cash checks and wire funds to someone you met on the Internet?
* Would you cash checks or money orders received through an Internet transaction without first confirming their legitimacy?
* Would you provide your personal banking information in response to an e-mail notification?

If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the IC3 at [**www.ic3.gov**](http://www.ic3.gov/).  Its website also includes tips to assist you avoiding a variety of Internet frauds.  Some of these are presented below.

Delete any suspicious e-mail without replying, especially the following:

* Business opportunities to make money with little effort or cash outlay
* Offers to sell lists of e-mail addresses or software
* Chain letters involving money
* Work-at-home schemes
* Health and diet claims of scientific breakthroughs, miraculous cures, etc.
* Get-rich-quick schemes
* Free goods offered to fee-paying group members
* Investments promising high rates of return with no risk
* Kits to unscramble cable TV signals
* Guaranteed loans or credit on easy terms
* Credit repair schemes
* Vacation prize promotions
* Special offers that require a credit check and a small fee for verification expenses to be paid by a credit card

***Online shopping frauds*.** Do not use a debit card when shopping online, especially on an unfamiliar website.  If something goes wrong your account can be emptied quickly without your knowledge.  This can result in overdrafts, fees, and an inability to pay your bills.  Even if your bank offers a fraud guarantee it is not obligated to restore your funds for at least two weeks while it investigates.  If you use a credit card the federal Fair Credit Billing Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error.  To protect yourself you need to do the following:

* Write to your credit card company within 60 days after the date of the statement with the error and tell it your name and account number, that your bill contains an error and why it is wrong, and the date and amount of the error.
* Pay all other charges.  You do not need to pay the disputed amounts.

Consumers should be aware that if a deal looks too good to be true, it probably is. An example of such a scam occurred in December 2009 when the victim located a car on the Auto Trader website and contacted the seller directly by e-mail. He was told that the car would be shipped to him for inspection and approval if he wired the money to a bank account where it would be held in escrow. He wired the money but the car never arrived. To prevent this kind of scam consumers need to be diligent in verifying all the parties involved in the purchase by phone calls, face-to-face meetings, etc. In a similar case the consumer asked to see the car before wiring any money. The scammer ended all contacts at that point.

Another example involved a Craigslist ad for a vacation apartment rental in New York City. The renter was told he had to act fast and wire the money or he’d lose out on this good deal. All three elements of a typical scam were present in this case: (1) act fast or lose the deal, (2) wire the money, and (3) a price that was too good to be true.

For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse’s website at [**www.privacyrights.org**](http://www.privacyrights.org).

***Phishing*.** In an e-mail scam known as “phishing” identity thieves fish for personal information by sending realistic-looking e-mail that asks recipients to go to a bogus website and provide personal information such as credit card and Personal Identification Numbers (PINs).  Legitimate banks and financial institutions don’t send e-mails asking you to verify your account information.  They already have it. The following are examples of scammers posing as the IRS, FBI. FDIC, U. S. Census Bureau, and the CDC.

Each year during tax preparation time there is a surge in the number of frauds by criminals posing as IRS officials to obtain personal information for identity theft.  The IRS never sends out unsolicited e-mails or asks for detailed personal and financial information.  Any such e-mail is a fraud.  So are telephone calls from someone stating they are from the IRS.  Go to the IRS website at [**www.irs.gov**](http://www.irs.gov/) for information on the latest scams and instructions on how to protect yourself from suspicious e-mails or phishing schemes.  The IRS also recommends forwarding the suspicious e-mail to it at **phishing@irs.gov**.

Fraudulent e-mails have also been sent out by criminals posing as FBI agents and officials.  They give the appearance of legitimacy by using the FBI seal, letterhead, and pictures of the FBI Director.  They may also claim to come from the FBI’s domestic or overseas offices.  Like the IRS, the FBI does not send out e-mails soliciting personal or financial information.  For more information on this kind of fraud go to the FBI website at [**www.fbi.gov**](http://www.fbi.gov/) and click on New E-Scams and Warnings under Be Crime Smart.

Another agency that has become aware of fraudulent e-mails in its name is the Federal Deposit Insurance Corporation (FDIC).  These ask recipients to “visit the official FDIC website” by clicking on a hyperlink that directs them to a fraudulent website that includes hyperlinks that open a “personal FDIC insurance file” to check on their deposit  insurance coverage.  Clicking on these links will download a file that contains malicious software to collect personal and confidential information.

And with the 2010 U.S. Census underway do not click on any link or open any attachment in an e-mails appearing to come from the U.S. Census Bureau.  They will be fraudulent.  The Census Bureau may contact you by telephone, mail, or in person at home.  It will not contact you by e-mail.

On Dec. 2, 2009 the Centers for Disease Control and Prevention (CDC) issued a health alert warning people not to respond to an e-mail referencing a CDC-sponsored state vaccination program for the H1N1 (Swine Flu) contagion that requires registration on “[**www.cdc.gov**](http://www.cdc.gov).”  People that click on this embedded link risk having a malicious code installed on their computer.  Examples of this and other hoaxes and rumors can be seen at **http://www.cdc.gov/**.

The following tips will help you counter phishing:

* Do not open any e-mail from an unknown sender.
* Do not open any unexpected e-mail attachments.
* Do not open any attachments that ask you to reset a password.
* Do not click on website addresses in e-mails you get even if they look real.  Retype them into your browser.
* Do not click on links within e-mail messages purporting to come from your bank.
* Do not double click on an Internet pop-up offering a link or provide personal information in response to an e-mail or Internet pop-up offer.
* Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the “protected mode,” which restricts the installation of files without the user’s consent, and set the “Internet zone security” to high. That disables some of Explorer’s less-secure features. And set your operating system and browser software to automatically download and install security patches.
* Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to identify phishing attacks.  Set your operating system and browser software to automatically download and install security patches.
* Make sure the website page you are entering sensitive information on is secure.  The address should begin with **https://** rather than **http://.**
* Read the website’s privacy policy.  It should explain what personal information it collects, how the information is used, whether it is provided to third parties, and what security measures are used to protect the information.  Consider taking your business elsewhere if you don’t see, understand, or agree with the policy.
* Keep your computer up to date with the latest firewalls, and anti-virus and anti-spyware software.  The latter counters programs that secretly record what you type and send the information to the thieves.  They are often installed when you visit websites from links in e-mail.  Use security software that updates automatically.  Visit [**www.OnGuardOnline.gov**](http://www.onguardonline.gov/) for more information.
* Do not buy “anti-spyware” software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected viruses known as malware, i.e., malicious software.
* Do not respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee.  “Helpful hackers” use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information.  If you already have anti-virus software on your computer you’ll receive a security update or warning directly on your computer.
* Look for valid trust marks to increase your confidence in using a website.  Reputation trust marks like BBBOnline offer a basic level of proof that there is an actual business behind the website and that it follows proper business practices.  Privacy trust marks like TRUSTe indicate that the business is aware of identity theft and personal data abuse and abides by the requirements of the trust mark provider in its privacy policy.   Secure Socket Layer (SSL) trust mark like VeriSign indicate that the site uses up-to-date encryption technology to scramble communications between the website and your computer.  And security-scanning trust marks like McAfee SECURE indicate that the business uses a regularly scheduled security auditing service for its website to ensure that it is free of viruses, malware, spyware, etc.  Before trusting a trust mark you should verify it by clicking on it.  A live link attached to the mark should take you to a verification website of the trust mark provider.  However, because a criminal could create a false mark and verification website, you cannot know that the mark is valid unless you investigate it further. In any case, use caution when visiting un-trusted websites.
* Contact your e-mail provider.  Most keep track of scams.  Send your provider the suspicious message header and complete text.
* Use caution when entering personal information online.

***Whaling*.** In another scam known as “whaling” fake e-mails have been sent to high-ranking executives to trick them into clicking on a link that takes them to a website that downloads software that secretly records keystrokes and sends data to a remote computer over the Internet.  This lets the criminal capture passwords and other personal or corporate information, and gain control of the executive’s computer.  In one case fake subpoenas have been sent to executives commanding them to appear before a grand jury in a civil case.  The link that offers a copy of the entire subpoena downloads the malicious software.

***Social Networking Dangers.*** Virus creators, identity thieves, and spammers are increasingly targeting users of social networking sites in an effort to steal personal data and account passwords.  One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online friends.  For example, some Facebook users have been receiving e-mails from their “friends” that claim to contain a video of them.  When they click on it they download a virus that goes through their hard drives and installs malicious programs.  The virus, known as Koobface, then sends itself to all the friends on the victim's Facebook profile.  A new version of the virus also is affecting users of MySpace and other social networking sites.  Cyber-criminals are tricking social networking users into downloading malicious software by creating fake profiles of friends, celebrities, and others.  Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites.  They warn that users need to be very careful about what information they post because it can be used to steal their identities.  Facebook users should become a fan of its security page at [**www.facebook.com/security**](http://www.facebook.com/security), which has posts related to all sorts of security issues, tips, resources, and other information.

To avoid problems on social networks or anywhere in the Internet, users should:

* Not to click on any links, videos, programs, etc. provided in messages, even if a “friend” encourages you to click on them.
* Get program updates from the company’s website, not through a provided link.
* Customize your personal privacy settings so only your friends have access to the information you post.
* Read your network’s privacy policy regularly to stay informed on how it uses or discloses your information.
* Scan your computer regularly with an updated anti-virus program.

***Fraudulent Websites.*** Cybercriminals are now creating fraudulent websites that will receive high search-engine rankings and thus attract the attention of persons searching for information on a particular subject.  Persons just visiting those sites risk having their computers infected with viruses.  And if they click on any links in those sites they risk becoming a victim of identity theft and various scams, e.g., ones that claim you can make a lot of money for a small initial investment.  To avoid these problems users should:

* Keep your computer’s anti-virus system up to date with the latest firewalls and software.
* Use caution clicking on links that claim to provide videos or information on hot topics in the current news, e.g., the earthquakes in Haiti and Chile.  And be aware that the bad guys are now tricking Google into telling you that the link is a PDF file, which makes it look more authentic.
* Not click on links to other websites.  Look up the address elsewhere and retype it into your browser.
* Use the tips provided above to counter phishing.

***E-card Dangers.*** You receive an e-mail saying “A friend has sent you an e-card.”  The e-mail appears to be from a legitimate card company, but malware or a virus is downloaded into your computer when you click the link to see the card.  You should delete the e-mail if you don’t recognize the sender or if you are instructed to download an executable program to view the e–card.  And make sure your computer has adequate anti-virus protection.

***Security alerts*.** Information on various Internet frauds is available at no cost to the public on USA.GOV: [**http://www.usa.gov/Citizen/Topics/Internet\_Fraud.shtml**](http://www.usa.gov/Citizen/Topics/Internet_Fraud.shtml)

Even if your computer has up-to-date firewalls, and anti-virus and anti-spyware software, one should be very cautious in visiting unfamiliar websites.  Websense Security Labs identified a 233 percent growth in the number of malicious sites in the first half of 2009.  It also found the following:

* 77 percent of websites with malicious codes were legitimate sites that have been compromised.
* Web 2.0 sites allowing user-generated content are a top target for cybercriminals and spammers.  95 percent of all comments to blogs, chat rooms, and message boards were spam or malicious.
* 69 percent of all Web pages with “objectionable” content, i.e., sex, adult content, gambling, and drugs, had at least one malicious link.
* 37 percent of malicious Web attacks included data-stealing code.
* 85 percent of all unwanted emails in circulation contained links to spam or malicious websites.  In June alone, the total number of emails detected as containing viruses increased 600 percent over the previous month.

Another security alert on September 24, 2009 warned of rogue anti-virus sites returned by Google searches on a person in the news.  These sites claim that your computer requires an immediate anti-virus scan and prompts you to download a malicious file.