Preventing and Dealing with Identity Theft

Every person who willfully obtains personal identifying information, e.g., name, address, date of birth, Social Security Number (SSN), mother's maiden name, etc. as defined in Cal. Penal Code Sec. 530.5(b), and uses that information for any unlawful purpose is guilty of a public offense. Identity theft is the fastest growing crime in the United States. Every year about 15 million people become victims. Everyone is vulnerable. Skilled identity thieves use a variety of methods to steal your personal information. These include the following:

- Dumpster diving. They rummage through trash looking for bills and other paper with your personal information on it.
- Skimming. They steal credit or debit card numbers with a special storage device when processing your card.
- Phishing, smishing, and whaling. They send realistic-looking e-mail that asks recipients to go to a bogus website and provide personal information, use text messages instead of e-mails, and send fake e-mails 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.
- Changing your address. They divert your billing statements to another location by completing a change-of-address form.
- Stealing. They steal wallets, purses, mail (credit card and bank statements, pre-approved credit offers, new checks, tax information, etc.), employee personnel records, etc.

Some of the things you can do to minimize your risk of identity theft, and what to do if you become a victim are listed in the following subsections.

Protecting Personal Information:

- Give out credit or debit card, bank account, and other personal information only when you have initiated the contact or know and trust the person you are dealing with. Beware of e-mail or telephone promotions designed to obtain personal information.
- Put strong passwords on your credit card, bank, computer, and online accounts. Avoid using easily remembered numbers or available information like mother's maiden name, date of birth, phone number, or the last four digits of your SSN. Passwords should be more than eight characters in length, and contain both capital letters and at least one numeric character. Use of non-dictionary words is also recommended. Other advice on creating strong passwords can be found at www.microsoft.com/protect/yourself/password/checker.mspx.
- Select password reset questions whose answers cannot be found online or from other research tools. Don't compromise a strong password with an easily answered reset question like: What is your mother's maiden name?
- Use different passwords for banking, e-commerce, e-mail, and other accounts.
- Memorize your passwords. Don't carry them in your purse or wallet.
- Keep personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home.
- Make sure that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier's disk.
- Protect you health insurance cards like you would your credit or debit cards. If asked for your policy numbers or any other personal information in a doctor's office, make sure no one else is near enough to hear or see them.

- Protect your Medicare card number as you would your SSN. Don’t give it to anyone who offers free medical equipment or services and then requests your number. And don’t let anyone borrow or pay to use your Medicare card. That’s foolish and illegal.
- Shred or tear up any documents with personal or financial information before throwing them in the trash. Use a cross-cut shredder.
- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.

Using Credit and Debit Cards:

- Never loan your card to anyone.
- Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
- Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won’t have access to the number.
- Notify your credit card companies and financial institutions in advance of any address or phone number changes.
- Bring home all card receipts and match them against your monthly statements. Look for charges you didn’t make. Dispose of them at home. Never toss your receipts in a public trash container.
- Call the credit card company or bank involved if a new credit card you applied for hasn’t arrived in a timely manner.
- Monitor the expiration dates of your cards and contact the card issuer if new cards are not received before your card expires.
- Report all lost or stolen cards immediately and request cards with new numbers. In this case the federal Truth in Lending Act limits your liability to $50 of any charges made before you report your card lost or stolen. Contact the issuer if replacement cards are not received in a reasonable time.
- Sign and activate new cards promptly on receipt. Or write “See ID” on the signature line on the back of the card. Then a thief won’t have your signature. A merchant will ask you for a picture ID to make sure you are the cardholder.
- Never put a card number on a post card or on the outside of a mailing envelope.
- Make sure only the last four digits of your card number show up on your receipts. A 2001 state law banned the use of full card numbers on electronically printed receipts and gave businesses three years to comply. (Note that the merchant copy can show the full credit card number.) Report non-complying businesses to the Methamphetamine Strike Force hotline at **(877) 662-6384**.
- Cancel accounts you don’t use or need. Carry only the cards and identification you need when you go out.
- Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
- Ask your credit card company to stop sending blank checks.
- Have your name removed from lists supplied by the Consumer Credit Reporting Companies (Equifax, Experian, Innovis, and TransUnion) to be used for pre-approved/pre-screened offers of credit or insurance. Call **(888) 567-8688** or go to www.optoutprescreen.com to do this.
- Don’t let your card out of sight. A person taking it to a Point of Sale (POS) device might have a skimmer to steal the information on the magnetic strip, copy your card number and the 3-digit security number on the back of the card, or switch cards. If you do give your card to a waiter or other sales person, make sure you get your card back. And use a credit card instead of a debit card whenever possible. With the former you don’t have to

pay disputed charges. But with the latter it may take the bank about two weeks to restore the funds to your account.

- Make sure your bank and credit card companies have your latest home and cell phone numbers, and e-mail address so they can contact you quickly if they suspect fraud in your accounts.
- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information is on the chip is not the same as that on the magnetic strip, and it cannot be used to create a functioning counterfeit version of the card. If you have a card with a RFID chip and don't want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.

Protecting your U.S. Passport:

- Since August 2007 all passports issued by the U.S. State Department have a small contactless RFID computer chip embedded in the back cover. They are called "Electronic or e-passports." The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder. The chip can only be read by special secure readers at a close distance. And to reduce opportunities for unauthorized readings of the passport, a metallic element is embedded in it and it must be physically opened before it can be read.
- The U.S. State Department is now issuing U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive that a passport book. It cannot be used for international travel by air. To increase speed, efficiency, and security at U.S. land and sea border crossings the card contains a RFID chip. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the cared when it is not in use. Make sure you carry the card in the sleeve.

Protecting Your Social Security Number:

- Examine your Social Security Personal Earnings and Benefits Estimate Statement for possible fraud. You will receive it about three months before your birthday each year.
- Provide your SSN only when it is required by a government agency, employer, or financial institution. In a recent case a man received a call from a person who claimed to be a jury coordinator and said that a warrant has been issued for his arrest because he failed to report for jury duty. When he protested that he never received a summons he was asked for his SSN and date of birth to verify the records. Caught off guard he provided this information. Instead he should have hung up realizing that court workers would never ask for a SSN or other personal information.
- In a variation of the above scam, the caller says that you've been selected for jury duty and asks you to verify your name and SSN. Remember, notification of jury duty is always done by mail.

- Never use your SSN for identification. Don’t carry it or your Social Security card in your purse or wallet.
- Do not have your SSN or driver’s license number printed on your checks. And never write your SSN on a check.

Managing Your Accounts:

- Keep a record in a secure place of all your credit and debit card, and bank and investment account phone numbers for quick reference if identity theft occurs.
- Review your bank statements carefully. Match your checkbook entries against paid checks. Look for checks you didn’t write.
- Never leave transaction receipts at bank machines or counters, trashcans, gasoline pumps, etc.

Carrying Personal Information in a Purse or Wallet:

- Carry only a driver’s license, cash, and one credit card. Don’t carry blank checks or a checkbook. Don’t carry anything with a PIN written on it.
- Keep a record of its contents. Photocopy both sides of your credit and debit cards and driver’s license and keep them in a safe place at home.
- Don’t carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card is a safe place at home.
- If you carry a wallet in a purse, keep credit or debit cards in separate compartment and not in your wallet.
- Don’t carry personal information of your family members.
- Don’t carry any account or computer passwords.
- Take the measures listed below for victims of identity theft if your wallet is lost or stolen. Don’t wait for someone to find and return it. These include filing a police report, reporting your credit and debit cards missing, closing checking accounts, having a fraud alert placed on your credit reports, notifying your medical insurance companies, reporting a missing driver’s license, etc.

Using the Mail:

- Deposit mail in boxes or slots inside a post office. Use an outside box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Also, do not leave mail for pickups from personal curbside boxes or cluster box units.
- Pick up your mail as soon as possible after it arrives in your personal curbside box or cluster box unit. If this is not possible, have a trusted friend or neighbor collect your mail, especially if you are expecting a box of checks or a new credit or debit card.
- Consider having new checks mailed to your bank for collection to avoid possible theft from your mailbox.
- Use a locked mailbox and make sure the lock works.
- Investigate immediately if bills do not arrive when expected, you receive unexpected credit cards or account statements, you are denied credit for no apparent reason, and you receive call or letters about purchases you did not make.
- Report the non-receipt of expected valuable mail by calling the sender and the Postal Inspection Service as soon as possible.

Using an ATM:

- Use ATMs that are inside a store or a bank. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder’s financial information from an ATM transaction. If you use an outside ATM, it should be well-lighted and under video surveillance.
- Get off your cell phone and be alert when using an ATM.
- Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. If something doesn’t seem right, go to another machine.
- Most ATMs have flashing lights in the card slot. Their obscuration is a sign of tampering.
- Look to see if there is anything in the slot where you insert your ATM card. Thieves place a small, hard-to-detect skimming device in the card slot to steal your PIN and other bank account information. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, contact the SDPD immediately. Don’t throw it away or keep it; that would make it look like you are running the scheme.
- Check for a false keypad that has been installed over the built-in one. False keypads stick out too far or look strange.
- Check the area around the machine for hidden cameras. To be safe shield your hand when entering your PIN so it can’t be seen by anyone near you or by a hidden camera.
- If you use a debit card memorize your PIN and keep it secret. Don’t write it down or keep it in your wallet or purse.
- Keep the customer-service phone numbers of your bank and credit-card company readily available. Call the appropriate number immediately if your card gets stuck in an ATM. Do not leave the ATM.
- Monitor your bank statements frequently and report any unauthorized activity immediately.

Buying Identity Theft Protection:

- You cannot buy absolute protection against identity theft. Beware of any such claims, especially regarding prevention of misuse of existing credit-card accounts, theft of medical records, and theft of personal information from employer’s personnel files.
- Before signing up for protection, be sure to understand what services are provided, what protections they afford, and how the personal information you provide is protected.
- Fraud alerts, which provide some protection against fraud in opening new accounts that require credit reports, do not provide absolute protection and only deal with a small fraction of identity theft incidents.

Checking for Possible Identity Theft:

- Obtain free copies of your credit reports from the three nationwide consumer credit reporting bureaus (Equifax, Experian, and TransUnion) by visiting www.AnnualCreditReport.com or calling **(877) 322-8228**. This is the ONLY source of free reports authorized under Federal law. You can get one free report annually from each bureau. Stagger your requests to obtain one every four months. That way you can monitor your credit during the year. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit. Contact the reporting bureau immediately if you see any inaccuracies. These bureaus may also try to sell you credit monitoring products or services for a fee.

Starting April 1, 2010 the FTC requires that any advertising for such products or services be delayed until after you get your free credit reports.

- Be aware that if you order a free credit report from an unauthorized website such as freecreditreport.com you will be given a free limited-time trial membership in its credit monitoring service that will provide daily monitoring of your credit reports, alert notices of key changes, bi-monthly credit scores, etc. If you don't cancel this membership you will be charged a fee for each month that you remain a member. Before becoming a member you need to understand exactly what protection and services it will and will not provide, and whether you need the additional protection. Some services you will pay for you can do yourself at no cost, e.g., ordering credit reports and placing fraud alerts.
- Starting April 1, 2010 these websites will be required to print a disclosure that states the following at the top of each page that mentions free credit reports: "THIS NOTICE IS REQUIRED BY LAW. Read more at www.FTC.gov. You have the right to a free credit report from www.AnnualCreditReport.com or **(877) 322-8228**, the ONLY authorized source under federal law." They will also have to include a clickable button to "Take me to the authorized source" and clickable links to www.AnnualCreditReport.com and www.FTC.gov.
- Place a security freeze on your credit reports. This will protect you against fraud in new accounts by prohibiting the credit reporting bureaus from releasing your credit reports to a potential creditor without your express permission. Go to their websites for the procedures and fees for placing and lifting freezes. Their addresses are: www.equifax.com, www.experian.com, and www.transunion.com.
- Check your medical bills and health insurance statements to make sure the dates and types of services match your records. Read every letter you get from your insurer, including those that say "this is not a bill." If you see a doctor's name or date of service that isn't familiar, call the doctor and your insurer.
- Once a year request a list of all benefits paid in your name by your health insurer. If the thief has changed your billing address you would not be receiving any bills or statements.

If You Become a Victim:

- File a police report as soon as possible if you become or may become a victim of identity theft. Call the SDPD non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Then do the following:
- Set up a folder where you can keep a log of all your contacts and documents.
- Contact the FTC to report the theft. Its Identity Theft Hotline is **(877) 438-4338**. Or visit its website at www.ftc.gov/idtheft. The FTC is the federal clearinghouse of complaints of victims of identity theft. It helps victims by providing information to resolve financial and other problems that could result from identity theft. Its booklet entitled Take Charge: Fighting Back Against Identity Theft deals with bank accounts and fraudulent withdrawals, bankruptcy fraud, investment fraud, phone fraud, and other specific problems. It also describes the immediate steps victims should take and ways to minimize recurrences.
- Report the theft to the fraud units of Equifax at **(800) 525-6285**, Experian at **(888) 397-3742**, and TransUnion at **(800) 680-7289**. Ask to have a fraud alert placed on your credit reports. It will tell creditors to follow certain procedures before they open new accounts in your name or make changes to you existing accounts. In placing a fraud alert you will be entitled to free copies of your credit reports. Review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Fraud alerts are good for 90 days and can be renewed. They are free.

- Alert your banks of any fraud and request new account numbers with new checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the fraud.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft. If you still want a charge account, request a new number.
- Report the loss of your SSN to the IRS. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. Call its Identity Theft Hotline at **(800) 908-4490** and go to http://www.irs.gov/privacy/article/0,,id=186436,00.html. Follow the directions there regarding identity theft and your tax records, and the need to provide it with proof of your identity. Also contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at www.ssa.gov/org.
- Contact the California DMV Fraud Hotline at **(866) 658-5758** to report the theft and see if another driver's license has been issued in your name.
- Notify the U.S. Postal Inspector if your mail has been stolen or tampered with. Its number is **(626) 405-1200**.
- In the case of medical identity theft request a copy of your current medical files from each health care provider, and request that all false information be removed from your medical and insurance files. Enclose a copy of the police report with your requests. For more information things to do if you are a victim of medical identity theft or concerned about it go the World Privacy Forum's website at www.worldprivacyforum.org/medicalidentitytheft.html.
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any fraud involving Medicare. Additional tips on avoiding and resolving identity theft problems are available on the State of California Office of Information & Privacy Protection website at www.oispp.ca.gov/consumer_privacy/identitytheft.asp. Another useful website is that of the Identity Theft Resource Center (ITRC) at www.idtheftcenter.org. It contains information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft. It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, a "Help, I'm a Victim of Identity Theft" button, and answers to frequently asked questions. Its toll-free victim-assistance number is **(888) 400-5530**.

If You Are Notified of a Security Breach Involving Personal Information:

- Most states now have security breach notification laws under which a person whose personal information is compromised must be notified of the breach. The California Breach Notification Law is in Civil Code Secs. 1798.29, 1798.82, and 1798.84. The first applies to state government agencies; the other two apply to any person or business doing business in the state. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: SSN; driver's license or California Identification Card number; financial account, credit card, or debit card number along with any PIN or other access code required to access the account; medical information; or health insurance information. In a paper dated May 2008 the California Office of Privacy Protection recommended that the letter of notice also specify the type of personal information that was involved and provide information on what individuals can do to protect against identity theft for each type. This information is summarized below.

- SSN. Put a fraud alert on your credit files and order copies of your credit reports. Review them carefully and file a police report if you find anything suspicious. If you don't find anything suspicious at first, renew the fraud alert and check your credit reports periodically. Also report the loss to the IRS and SSA.
- Driver's License or California Identification Card number. Call the DMV Fraud Hotline to report the incident.
- Financial account numbers. Call the institution to request new account numbers and PINs. And provide new passwords.
- Medical or health insurance information. Review your explanation of benefits statements and contact your insurer if you see any services you did not receive. Senate Bill 1166 would have amended the present law to include these recommendations but Governor Schwarzenegger vetoed it on Sept. 30, 2010. For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse's website at www.privacyrights.org.

Using the Internet

- In 2009 the Internet Crime Complaint Center (IC3), which acts in partnership with the National White Collar Crime Center and the FBI, received more than 336,000 complaints on its website and referred over 146,000 to law enforcement agencies for further consideration. The total loss from all of these cases was over $560 million. 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? The following security tips will help you deal with suspicious e-mails, phishing, smishing, whaling, social networking dangers, illegitimate websites, and E-card dangers.

Suspicious E-mails:

- 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 or debit card
- Notices of prize or lottery winnings that require you to pay a fee to cover expenses You should also file a complaint with the IC3 at www.ic3.gov. Its website also includes tips to assist you avoiding a variety of Internet problems.

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 a credit card number or a Personal Identification Number (PIN). 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 Internal Revenue Service (IRS), Federal Bureau of Investigation (FBI), Federal Deposit Insurance Corporation (FDIC), and the Centers for Disease Control and Prevention (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 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 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 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.

On Dec. 2, 2009 the 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." 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/hoaxes_rumors.html.

Use the following tips to 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.
- Make sure the website page you are entering sensitive information on is secure. You can tell it is secure when the address on the top of your screen where the Uniform Resource Locator (URL) is displayed begins with **https://** rather than **http://**. You can also look for a closed padlock or an unbroken key on the bottom of your screen to indicate the page is secure. If the lock is open the site or the key is broken, the page is not secure. Note that on many websites only the order page will be secure.
- 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 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. A Secure Socket Layer (SSL) trust mark like VeriSign indicates 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.

Smishing:

This is phishing with text messages instead of e-mails. Beware of any messages that request personal information or give you a phone number to call. Before calling verify that the number matches the number of the named institution, e.g., your bank. And never give out personal information unless you have initiated the call.

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, 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 privacy 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.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.

Illegitimate Websites:

Cybercriminals are now creating illegitimate 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.
- Do not click on links to other websites. Look up the address elsewhere and retype it into your browser.
- If the link address is correct, before clicking on it check to see where you would actually go. You can do this by scrolling your mouse over the link and reading the address in the box that will pop up over the link. Do not click on the link if this address does not match the one in the link.
- Use the tips provided above to counter phishing. Do the following to make sure a website is legitimate, especially if you are planning to make a purchase of a name brand product:
- Check that the domain name is spelled correctly.
- Check that the domain name ends in **.com**, **.org**, or **.net**. Those ending in .**cn** for China or **.mn** for Mongolia are likely to be fraudulent.
- Call the phone number posted and talk to a live person.

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.

And even if you recognize the sender your computer could be harmed if the incoming e-mail is phony and you click on a link to an e-card or open an attachment. This happened around Christmas time in December 2010 when employees of various government agencies received phony holiday messages that appeared to come from the White House.

Safe Cyber Practices:

There are presently two similar efforts by the U.S. Government to promote safer use of the Internet. The one by the FTC's Bureau of Consumer Protection is called *Stop.Think.Click*. The other, developed by a group representing industry, government, academia, and the nonprofit sector in 2009, and promoted by the Obama administration and the Department of Homeland Security, is called *Stop.Think.Connect.*

Stop.Think.Click defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus and anti-spyware software, as well as a firewall
4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords
6. Backing up your important files
7. Learning who to contact if something goes wrong online. Go to www.ftc.gov/bcp/edu/pubs/consumer/tech/tec15.pdf for information about these practices and tips.

Go to www.ftc.gov/bcp/edu/pubs/consumer/tech/tec15.pdf for information about these practices and tips.

Stop.Think.Connect suggests that users do the following:

- Stop. Before you use the Internet take time to understand the risks and learn how to spot potential problems
- Think. Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.
- Connect. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

You can learn how to become a partner in this effort by going to its website at www.stopthinkconnect.org. This site also contains the tips and advice for doing the following.

Keeping a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from viruses and malware.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protecting your personal information:

- Secure your accounts with protection beyond passwords that can verify your identity before you conduct business.
- Make passwords long and strong with capital and lowercase letters, numbers, and symbols.
- Use different passwords for every account.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connecting with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising. • Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer. • Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Being web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Being a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.

Wi-Fi Hacking and Hotspot Dangers

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be confident that a hotspot is secure only if it asks for the Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is the most secure.

Also, unsecure laptops and smart phones make it easy for a hacker to intercept information to and from the web, including passwords and credit or debit card numbers. They are also vulnerable to virus and spyware infections, and to having their contents stolen or destroyed. A hacked laptop or smart phone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smart phone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.

- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your company offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.
- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack.
- Only log in or send personal information on website pages that are encrypted. They will have https:// or shttp:// in their URLs and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not fraudulent.
- Use a different password for each account.
- When you've finished using an account, log out. Don't stay signed in.
- Pay attention to warnings from your browser if you try to visit a fraudulent website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put strong passwords on your wireless network. They should be more than eight characters in length, and contain both capital letters and at least one numeric character. Other advice on creating strong passwords can be found at www.microsoft.com/protect/yourself/password/checker.mspx.
- In shopping, it's fine to browse website when you're out but wait until you are at home to do any online business.