Social Engineering and Identity Theft

Module 10

Simplifying Security.

Certified Secure Computer User

Module 10: Social Engineering and Identity Theft

Exam 112-12

Module Objective

With millions of individuals becoming victims of **identity theft** each year, billions of dollars lost, and the amount of time victims have to spend to rebuild their credit, identity theft is a menace that is only getting bigger each day. This module will explain what identity theft is and how users can protect themselves from it.

This module will familiarize you with:

- What Is Identity Theft?
- Personal Information that Can be Stolen
- How Do Attackers Steal Identity?
- What Do Attackers Do with Stolen Identity?
- Examples of Identity Theft
- How to Learn if You Are a Victim of Identity Theft
- What to Do if Identity Is Stolen
- Reporting Identity Theft
- Prosecuting Identity Theft
- Guidelines for Identity Theft Protection
- Guidelines for Protection from Computer-Based Identity Theft
- IP Address Hiding Tools

Module Flow

Identity Theft

Social Engineering

How to Find if You Are a Victim of Identity Theft

What to Do if Identity Is Stolen

Reporting Identity Theft

Protecting from Identity Theft

What Is Identity Theft?

Individuals work hard to support themselves or their family. They keep their **credit card scores** clean and yearn for the benefits that accompany good credit. But they would be really frustrated if someone else uses their name to apply for credit cards, runs bills of thousands of dollars using the card, opens bank accounts in their name, or worse yet, commits a crime in their name.

Identity theft or ID fraud refers to crimes in which a person wrongfully obtains key pieces of **personal identifying information** such as date of birth, social security numbers (SSNs), and drivers license numbers and uses them for their own personal gain. Fraudsters **create a persona** similar to the victim and take advantage of his/her **authority** and **privileges**.

The Fair and Accurate Credit Transactions Act of 2003 (**FACTA**) defines identity theft as "a fraud committed using the identifying information of another person."

Identifying information according to the **Federal Trade Commission** is any name or number that may be used, alone or in combination with any other information, to identify a specific individual. Identifying information includes:

- Name, social security number, and date of birth
- Official state- or government-issued drivers license or identification number, alien registration number, government passport number, and employer or taxpayer identification number
- Unique biometric data, such as fingerprint, voice print, retina or iris image, and other unique physical representations
- Unique electronic identification number, address, or routing code
- Telecommunication identifying information or access device

The Australian Bureau of Statistics defines the term identity theft as "**False Identity**," or creating a fictitious identity, modifying one's own identity, and stealing or assuming another's identity and modifying it.

In the United Kingdom, identity theft is called "**identity fraud**." And the French prefer to call it vol d'identité ("identity theft") or usurpation d'identité ("Impersonation").

Personal Information that Can Be Stolen

All an identity thief needs is a piece of personal information, which may include:

- Names
- Addresses
- A date of birth

- A mother's maiden name
- Telephone numbers
- Social security numbers
- Drivers license numbers
- Credit card/bank account numbers
- Birth certificates
- Passport numbers

How Do Attackers Steal Identity?

Identity thieves may use traditional as well as Internet methods to steal identity.

Physical Methods

- **Stealing Computers, Laptops, and Backup Media:** Stealing is a common method. The thieves steal hardware from places such as hotels and recreational places such as clubs or government organizations. Given adequate time, they can recover valuable data from these media.
- **Social Engineering:** This technique is the act of manipulating people's trust to perform certain actions or divulge private information without using technical cracking methods.
- **Theft of Personal Belongings:** Wallets/purses usually contain a person's credit cards and drivers license. Attackers may steal the belongings on streets or in other busy areas.
- **Mail theft and rerouting:** Mailboxes are not often protected and may contain bank documents (credit cards or account statements), administrative forms, and more. Criminals may use this information to get credit cards or for rerouting the mail to a new address.
- **Shoulder surfing:** Criminals may find user information by glancing at documents, personal identification numbers (PINs) typed into an automatic teller machine (ATM), or overhearing conversations.
- **Skimming:** Skimming refers to stealing credit/debit card numbers by using a special storage device when processing the card.
- **Pretexting:** Fraudsters may pose as executives from financial institutions, telephone companies, and other sources to obtain personal information of the user.

Internet Methods

- **Pharming:** Pharming is an advanced form of phishing in which the connection between the IP address and its target server is redirected. The attacker may use **cache poisoning** (modify the Internet address with that of a rogue address) to do this. When the user

types in the Internet address, he/she is **redirected to the rogue website** that is similar to the original website.

- **Keyloggers and Password Stealers:** An attacker may infect the user's computer with Trojans and then collect the keyword strokes to steal passwords, user names, and other sensitive information.
- **Phishing:** The fraudster may pretend to be a financial institution or from a reputed organization and send spam or pop-up messages to trick the users to reveal their personal information. Criminals may also use emails to send fake forms such as Internal Revenue Service (IRS) forms to gather information from the victims.
- **Hacking:** Attackers may compromise user systems and route information using listening devices such as sniffers and scanners. Attackers gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

What Do Attackers Do with Stolen Identity?

Once the identity thieves collect the stolen information, they can use it for the following purposes:

In **credit card fraud**, criminals may:

- Use the information to route the mail to a new residential address. This way, the victims will not be able to receive any credit card bills and the criminal can just keep piling up the credit on their cards and severely affect their credit scores.
- The criminal may also use the information to **apply for a new credit card** in the victim's name and run high bills using the cards.

In **phone or utilities fraud**, the criminal may:

- Apply for a new phone contract or a wireless connection and run up bills in users' name
- Use user information to obtain utility services such as electricity, heating, or cable TV

In **bank/finance fraud**, the criminal may:

- Generate forged checks using the victim's name or account number
- Open a bank account in the victim's name and write bad checks
- Duplicate the user's ATM or debit card and withdraw money, thus depleting the victim's bank resources
- Apply for bank loans

In **government documents fraud**, the criminal may:

- Obtain a drivers license, state ID, and more, with a user's name and the criminal's picture

- Obtain social security benefits and other government benefits that rightfully belong to the user
- File tax returns in a user's name and obtain tax benefits

Other frauds may include:

- Acquiring a job using the user's SSN
- Leasing a house in the user's name

Identity Theft Example

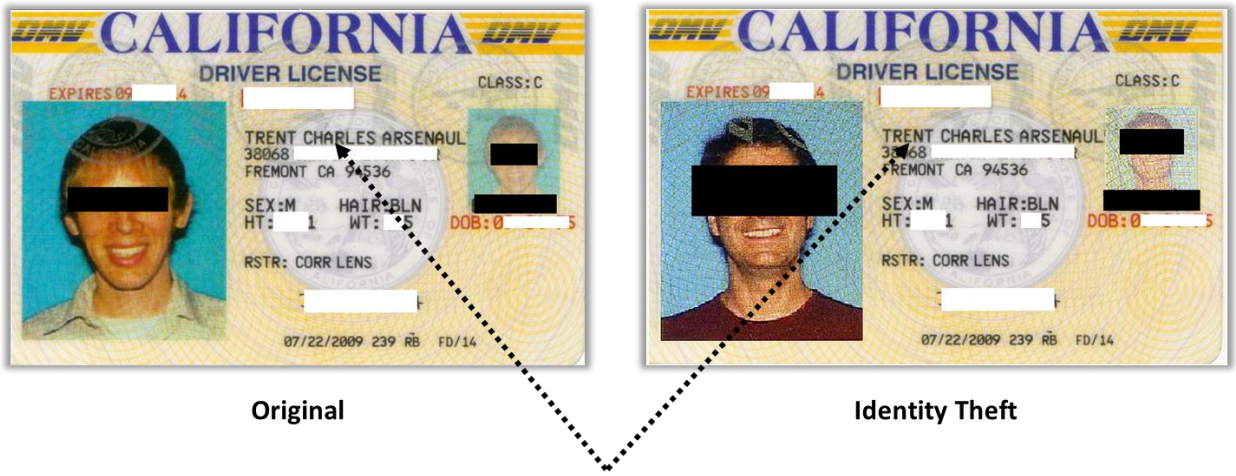


Figure 10-01: Fake Driving License Created Using the Victim's Personal Information

Social Engineering

Social engineering is the art of **convincing** people **to reveal confidential information**. It is a trick used to gain sensitive information by exploiting basic human nature.

Social Engineers Attempt to Gather: Criminals aim to gather sensitive information such as credit card details, social security number, passwords, other personal information, and more.

Types of Social Engineering: There are two types of social engineering:

- Human-based social engineering
- Computer-based social engineering

Social Engineering Examples

Attacker calls a victim posing as a HR manager:

Hi, we are from CONSESCO Software. We are hiring new people for our software development team. We got your contact number from popular job portals. Please provide the details of your job profile, current project information, social security number, and residential address.

Attacker calls a victim posing as a phone banker:

Hi, I am Mike calling from CITI Bank. Due to increasing threat perception, we are updating our systems with new security features. Can you provide me your personal details to verify that you are really Stella?

Thanks, Mike, Here are my details. Do you need anything else?

Attacker calls a victim posing as an authority:

Hi, I am John Brown. I'm with the external auditors, Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a website crash.

Attacker calls a victim posing as a technical support:

A man calls a company's help desk and says he has forgotten his password. He adds that, if he misses the deadline on a big advertising project, his boss might fire him. The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network.

Human-Based Social Engineering

Human-based social engineering is using **direct interactions** with key individuals in an organization to exploit or **manipulate people** into providing the confidential information. These attacks mainly use impersonation. Methods of human-based social engineering include:

- Eavesdropping
- Shoulder surfing
- Dumpster diving

Eavesdropping: Eavesdropping is the **unauthorized listening** of conversations or reading of messages. It is the interception of any form of communication such as audio, video, or written.

Shoulder surfing: Shoulder surfing is a procedure where the attackers **look over** the user's shoulder to gain critical information such as passwords, personal identification number, account numbers, credit card information, etc. An attacker may also watch the user from a distance using binoculars in order to get the information.

Dumpster diving: Dumpster diving includes **searching for sensitive information** at the target company's **trash bins**, printer trash bins, user desk for sticky notes, etc. It involves the collection of phone bills, contact information, financial information, operations-related information, etc.

Computer-Based Social Engineering

Computer-based social engineering is mainly categorized into five main types:

- **Pop-up windows:** Pop-up windows that suddenly pop up while surfing the Internet and ask for users' information to log or sign in.
- **Hoax letters:** Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system.
- **Chain letters:** Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons.
- **Instant chat messenger:** Attackers use instant messaging to gather personal information by chatting with a selected online user to get information like birth dates and maiden names.
- **Spam email:** Spam email is irrelevant, unwanted, and unsolicited email to collect financial information, social security numbers, and network information.

Computer-Based Social Engineering: Phishing

An **illegitimate email** falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information. Phishing emails or pop ups **redirect users** to **fake webpages** of mimicking trustworthy sites that ask them to submit their personal information.

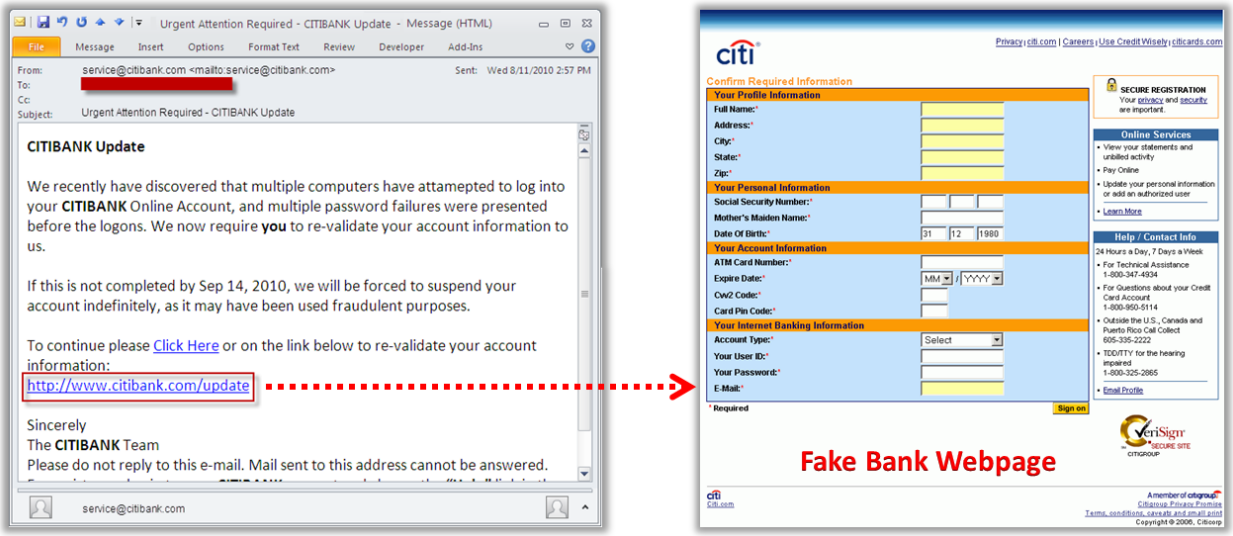


Figure 10-02 Computer-based Social Engineering Through Fake Band Webpage

Phony Security Alerts

Phony Security Alerts are the emails or pop-up windows that seem to be from reputed hardware or software manufacturers like Microsoft, Dell, etc. It **warns/alerts** the user that the system is infected and thus will provide with an attachment or a link to patch the system.

Scammers suggest the user download and install those patches, except these files contain **malicious programs** that may infect the user system.

Figure 10-03 Phony Security Alerts

Computer-based Social Engineering Through Social Networking Websites

Computer-based social engineering can be carried out through **social networking websites** such as Orkut, Facebook, MySpace, LinkedIn, Twitter, etc. Attackers use these social networking websites to exploit users' personal information.

Figure 10-04: Computer-based Social Engineering through Social Networking Sites

How to Learn if You Are a Victim of Identity Theft?

Most **victims do not realize** that their identity has been stolen until it is too late. The best method to find out whether or not an identity has been compromised is by **checking credit score** reports regularly. An early discovery of a possible identity theft can limit the damage. The users have to look for any suspicious activity by regularly monitoring their financial statements, credit reports, credit card statements, etc.

The following is a list of indications that your identity has been stolen:

- Bill collection agencies contact the user for overdue debts they never incurred.
- Users receive bills, invoices, or receipts addressed to them for goods or services they did not ask for.
- A user's request for a mortgage or any other loan is rejected, citing bad credit history despite the user maintaining a healthy credit record.

- You notice that some of your mail seems to be missing.

How to Learn if You Are a Victim of Identity Theft?

- Users receive mail about an apartment they never rented, a house they never bought, or a job they never held.
- Users lose important documents such as a passport or drivers license.
- Victims identify irregularities in credit card and bank statements.
- Victims are denied social benefits.
- Users receive a credit card statement for a new account.

What to Do if Identity Is Stolen?

The identity theft victim needs to take the following steps:

- **Place fraud alerts on credit reports and review credit reports regularly.** There are two types of fraud alerts—**initial** and **extended**. An initial fraud alert stays on the credit report for **at least 90 days**. The users may ask a credit reporting agency to place a fraud alert on their credit report if they believe that they are or will be victims of identity theft, if they have been a victim of a phishing scam, or if they have lost personal belongings that contain personally identifiable information such as credit cards, a drivers license, etc.

  An extended fraud report stay on a credit report for **up to seven years**. Users may ask a credit reporting agency to place a fraud report on the credit report if they have previously been victims of identity theft. Users will have to prove their identity to the credit reporting agency to have a fraud alert placed on their credit report.

  Fraud alerts may help prevent the user's identity from being used further. The victim can ask one of the three following commercial reporting agencies to place a fraud report on his/her credit report:

  - **TransUnion** (*www.transunion.com*)
  - **Equifax** (*www.equifax.com*)
  - **Experian** (*www.experian.com*)

  The users only have to contact one of these reporting companies to have a **fraud alert** placed on his or her credit report. The reporting company chosen by the user will then contact the other two reporting companies and ask them to place a fraud alert on their versions of the credit report. The user may ask the reporting agency for a free copy of his/her credit report (the first copy is not charged). Once the users receive the credit

report, they need go through the report thoroughly and **contact companies/banks** for the accounts they have not opened, credit cards they did not use, or an apartment they have not rented. They also need to check all information on the credit report including name, social security number, address, etc. if they are correct. Users should ensure that they continue to check their credit reports periodically, especially the first year after their identity has been compromised.

The identity theft victim needs to take the following steps:

- **Close the bank accounts that have been compromised with or the accounts that have been opened fraudulently.** The victim should call his or her banks or creditor's security and fraud department. He or she should also notify the banks and the credit card companies in writing. Victims need to ensure that they **document all conversation** and mail information such as when they have received mail and so on for future use.

  Users should not use the same personal identification number (PIN) or password for any new bank accounts or credit cards they apply for. For any of the compromised accounts or new accounts opened fraudulently in a user's name, the user should file a dispute with the company directly. Victims may also choose to lodge a complaint with the local authorities.

Reporting Identity Theft

Federal Trade Commission

Source: http://www.ftc.gov

Victims of identity theft may report the crime to the Federal Trade Commission (FTC), econsumer.gov, or FBI's **Internet Crime Complaint Center** (IC3).

- Victims can file a complaint with the FTC through an online complaint, call the FTC's **Identity Theft hotline**, or lodge a complaint in writing. The information that victims provide to the FTC is crucial in tracking the culprit who stole the identity. The victim may also provide a printed version of the complaint to the police for their records. The FTC identity theft complaint along with **the police report** constitutes the identity theft report that provides the victim with extra protection.

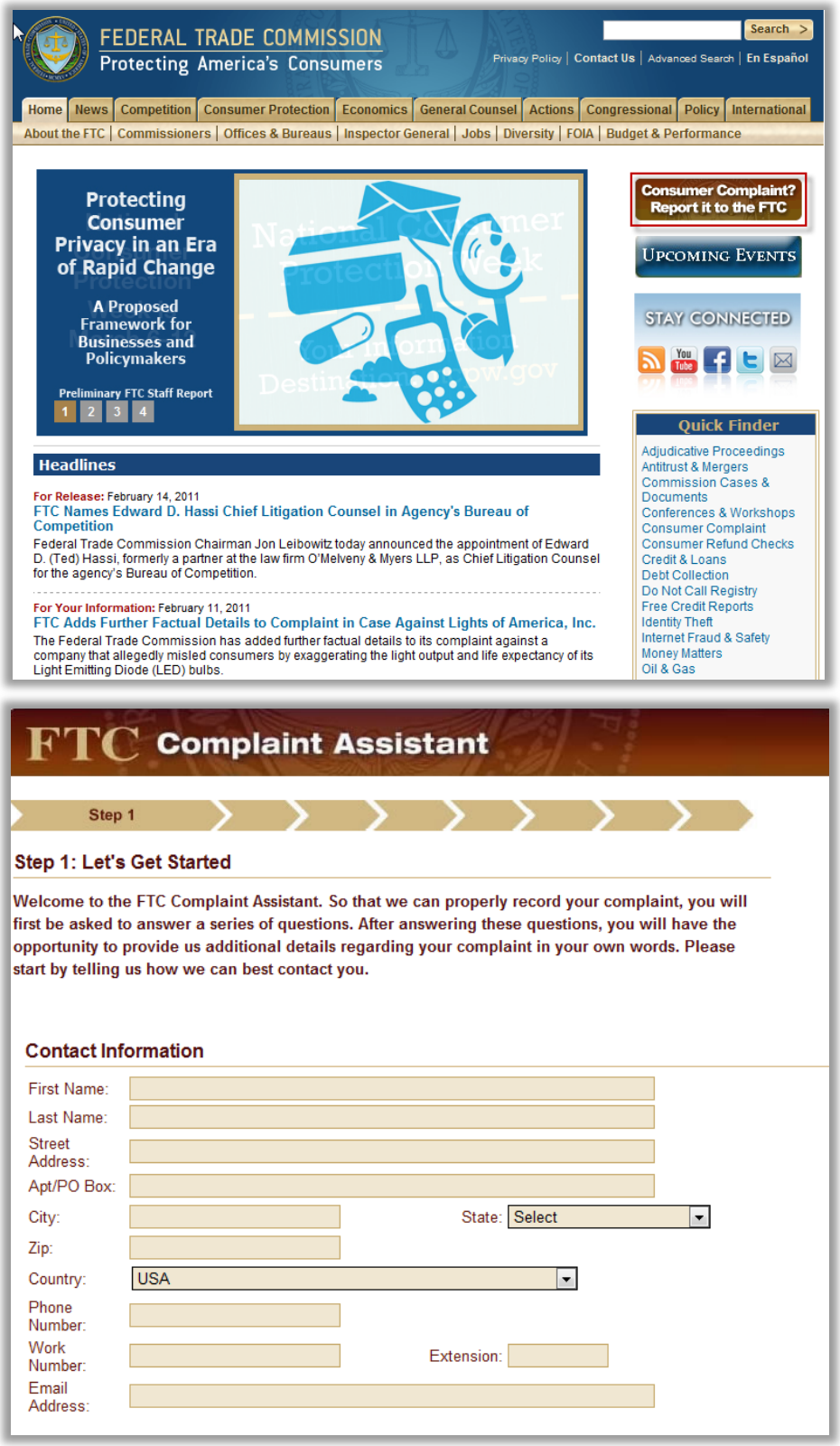
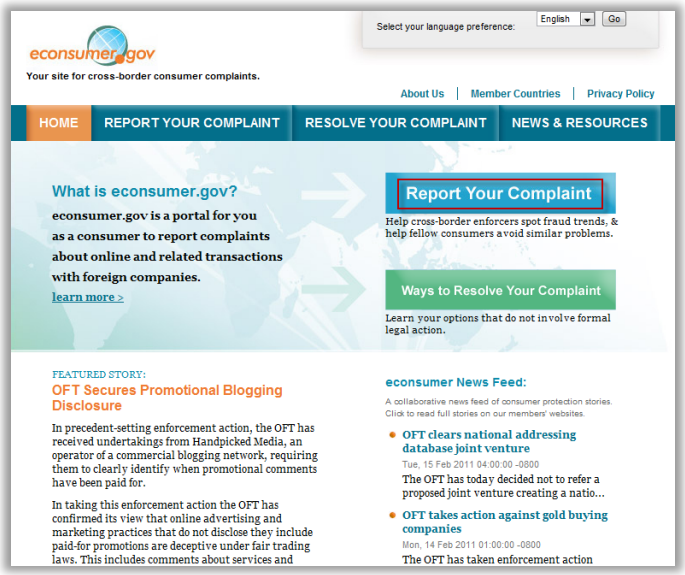


Figure 10-05: Reporting Identity Theft with FTC

econsumer.gov

Source: http://www.econsumer.gov



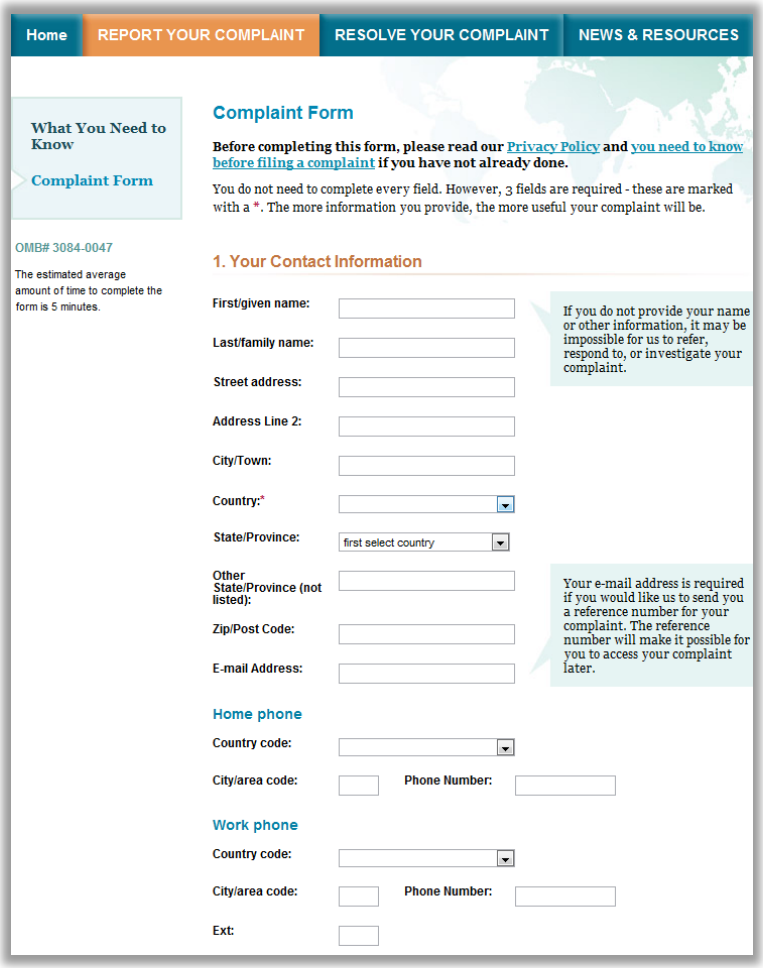


Figure 10-06: Reporting Identity Theft with econsumer.gov.

Internet Crime Complaint Center

Source: http://www.ic3.gov

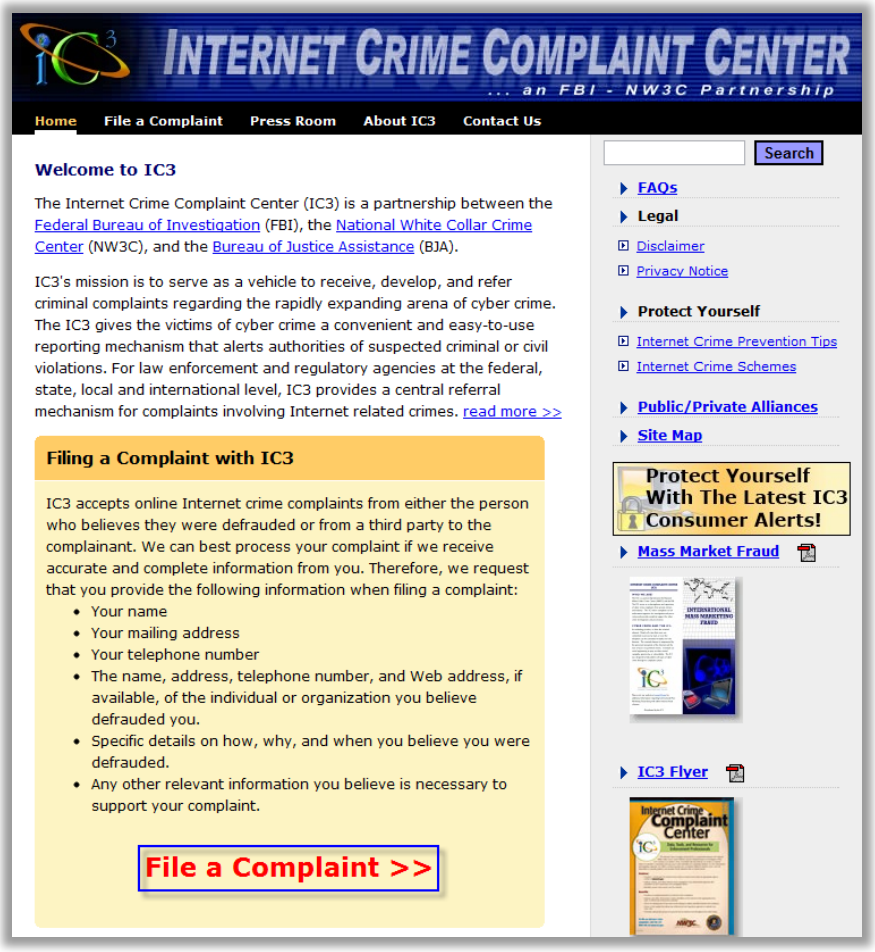


Figure 10-07: Reporting Identity theft with IC3.

Prosecuting Identity Theft

- Begin the process by **contacting** the bureaus, banks, or any other organizations who may be involved.
- File a **formal complaint** with the organization and with the police department.
- File a complaint with the Federal Trade Commission and **complete affidavits** to prove your innocence on the claims of identity theft and fraudulent activity.
- Obtain a copy of **the police complaint** to prove to the organizations that you have filed an identity theft complaint.

- Contact the **District Attorney's office** for additional prosecution of the individuals who may be involved in the identity theft.
- Regularly **update yourself** regarding the investigation process to ensure that the case is being dealt with properly.

Protecting from Identity Theft

Hiding IP Address Using Quick Hide IP Tool

Source: http://www.quick-hide-ip.com

Your IP address can link your internet activities directly to you; it can be used to find your name and location. So protecting your **Online Identity** is a must, thus **Anonymous Web Surfing** and the ability to hide your IP address are mandatory in order to ensure a high level of online protection.

Features:

- Hide your IP address and location from the web sites you visit.
- Fully compatible with Internet Explorer, Google Chrome, Mozilla Firefox.
- Fully compatible with Windows XP, Windows 2003, Windows Vista and Windows 7.
- Easy way to change browser proxy settings on the fly.
- Automatically switch IP address every X minutes for better anonymous surfing.
- Choose your favorite hidden geographic location (country) all around the world.
- Advanced proxy list testing, sorting, and management.

Figure 10-08: Quick Hide IP Tool

IP Address Hiding Tools

Ultra Surf

Source: http://www.ultrareach.com

Ultrasurf is a product of Ultrareach Internet Corporation. Originally created to help internet users in China find security and freedom online, Ultrasurf has now become the world's most popular pro-privacy, anti-censorship software, with millions of people using it to bypass firewalls and protect their identity online.

Hide My IP

Source: http://www.hide-my-ip.com

By using Hide My IP surf anonymously, prevent hackers from acquiring your IP, encrypt your Internet connection, send anonymous email and un-ban yourself on forums. Hide your IP with the click of the button.

IP Hider

Source: http://www.iphider.org

IP-Hider is a Free Anonymous Proxy that will help you open up blocked websites from school, work, library, or any other firewall protected place. Unblock Myspace, Orkut, Bebo, hi5 and other websites.

Anti Tracks

Source: http://www.giantmatrix.com

Anti Tracks provides you with a set of tools that will not only securely erase your tracks and unwanted files so that they are gone forever, without any chance of getting them back but will also protect your identity and important files by hiding your machine IP and securely locking your important files and folders. Moreover, Anti Tracks provides you with a set of tools that will help you maintain healthy PC performance and keep your PC in top-notch condition.

Hide IP NG

Source: http://www.hide-ip-soft.com

Hide IP NG (short for Hide IP Next Generation) is an easy to use software that helps you hide your IP address when you are surfing Internet.

TOR

Source: http://www.torproject.org

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.

Anonymizer Universal

Source: http://www.anonymizer.com

Anonymizer Universal takes Anonymous Surfing to the next level giving you the ultimate in online privacy protection from home or when using Wi-Fi, anytime and anywhere you connect. Ease-of-use, faster surfing, a powerful VPN client, and Anonymizer's proprietary technologies combine to keep your online activities—email, surfing, chat, all the things you do online—private and secure on your computer and iPhone.

Hide The IP

Source: http://www.hide-the-ip.com

Hide IP can hide your IP address and protect you from anybody who wants to monitor your reading interests and spy upon you.

Module Summary

Identity theft is the process of using someone else's personal information for the personal gain of the offender.

Criminals look through trash looking for bills or other paper with personal information on it.

Criminals call a victim while impersonating government official or other legitimate business person and request personal information.

Keep the computer operating system and other applications up to date.

Do not reply to unsolicited email that requests personal information.

Use strong passwords for all financial accounts.

Review bank/credit card statements/credit reports regularly.

Identity Theft Protection Checklist

Guidelines that help protect the user from becoming an identity theft victim include:

- ☐ Never give away the social security information or private contact information on the phone—unless *you* initiated the phone call
- ☐ Shred papers with personal information, credit card offers, and "convenience checks" (that are not useful) instead of throwing them away
- ☐ Ensure your name is not present in the marketers' hit lists
- ☐ Use strong passwords for all financial accounts
- ☐ Check the telephone and cell phone bills for calls you did not make
- ☐ Read before you click
- ☐ Stop pre-approved credit offers
- ☐ Read website privacy policies

Identity Theft Protections Checklist

Guidelines that help protect the user from becoming an identity theft victim include:

- ☐ Do not carry your Social Security card in your wallet
- ☐ Do not reply to unsolicited email requests for personal information
- ☐ Do not give personal information over the phone
- ☐ Review bank/credit card statements regularly
- ☐ Shred credit card offers and "convenience checks" that are not useful
- ☐ Do not store any financial information on the system and use strong passwords for all financial accounts
- ☐ Check the telephone and cell phone bills for calls you did not make
- ☐ Read before you click, stop pre-approved credit offers, and read website privacy policies

Computer Based Identity Theft Protection Checklist

Fraudsters may use a computer that is connected to the Internet to steal personally identifiable information or he/she may just steal laptops, computers, or other media containing personal information. Guidelines to protect yourself from computer/Internet-based identity theft include:

- ☐ Keep the computer operating system and other applications up to date
- ☐ Install anti-virus software and scan the system regularly
- ☐ Enable firewall protection
- ☐ Check for website policies before you enter
- ☐ Be careful while opening email attachments
- ☐ Clear the browser history, logs, and recently opened files every time
- ☐ Check for secured websites while transmitting sensitive information