Identity Theft

Identity theft is the willful act of stealing someone’s identity for monetary benefits. Criminals obtain personal information about a person and misuse it, causing heavy financial loss to the victim. False shopping sites and spam mails that contain irresistible offers are common means used to obtain a victim's credit card numbers. Criminals not only withdraw huge amounts from the victim’s bank accounts but can also make the victim bankrupt.

Chain E-Mails

A chain e-mail is a message that is sent successively to several e-mail users. It directs the recipients to circulate multiple copies of the e-mail, often promising rewards for this compliance, such as a blessing or good luck. A chain e-mail can be in the form of sympathy or threats.

Phishing

Phishing has emerged as an effective method to steal the personal and confidential data of users. It is an Internet scam that tricks users into divulging their personal and confidential information by making false statements and enticing offers. Phishers can attack users through mass mailings to millions of e-mail addresses around the world.

A successful phishing attack deceives and convinces users with fake technical content and social engineering practices. The major task for phishers is to make the victims believe in the phishing sites. Most phishing attacks are initiated through e-mails, where the user gets an e-mail that prompts him or her to follow a link given in the e-mail. This link leads to a phishing Web site, though the e-mail says otherwise. The e-mail may contain a message stating that a particular transaction has taken place on the user’s account, and a link is provided to check his or her balance. Or the e-mail may contain a link to perform a security check on the user’s account.

E-Mail Spoofing

E-mail spoofing is the process of altering e-mail headers so that an e-mail appears to be from someone or somewhere other than the original source. Spammers and phishers use this technique to conceal the origin of their e-mail messages. The following are the e-mail header fields that are most often changed during e-mail spoofing:

- From
- Return-Path
- Reply-To

Investigating E-Mail Crimes and Violations

The steps involved in investigating e-mail crimes and violations are as follows:

1. Examine an e-mail message.
2. Copy the e-mail message.
3. Print the e-mail message.
4. View the e-mail headers.
5. Examine any attachments.
6. Trace the e-mail.

Obtaining a Search Warrant and Seizing the Computer and E-Mail Account

A search warrant application should include the proper language to perform on-site examination of the suspect’s computer and the e-mail server used to send the e-mails under investigation. The investigator should seize all