The victims sent tens of thousands of dollars through online transfer to bank accounts held in Calgary. But they would either fail to receive the purchased vehicle or receive a vehicle that was not the same as the item purchased. The money that was sent by the victims to the holding company bank accounts was then directed elsewhere.

**Introduction to Investigating Internet Crime**

This chapter focuses on investigating Internet crimes. It starts by describing the different types of Internet crimes. It then discusses the different forensic methods and tools investigators use when investigating Internet crimes.

**Internet Crimes**

Internet crimes are crimes committed over the Internet or by using the Internet. The executor or perpetrator commits criminal acts and carries out wrongful activities on the Web in a variety of ways.

The following are some of the different types of Internet crimes:

- **Phishing**: Phishing is an e-mail fraud method in which the perpetrator sends out official-looking e-mail to the possible victims, pretending to be from their ISP, bank, or retail establishment, to collect personal and financial information. It is also known as “brand spoofing,” which is a trick to steal valuable information such as passwords, credit card numbers, Social Security numbers, and bank account numbers that the authorized organization already has. During this process, users are asked by e-mail to visit a Web site to update their personal information.

- **Identity theft**: Identity theft is a crime where a person’s identity is stolen. The perpetrator then uses the victim’s personal data—such as Social Security number, bank accounts, or credit card numbers—to commit fraud. Identity thieves obtain the names, addresses, and birth dates of victims, and may apply for loans in the name of their victims. In other instances, attackers acquire information such as usernames and passwords to login and steal valuable information and e-mails. Multiple methods are used to commit these frauds, such as purse or wallet theft, or posing as fake marketing executives. The Internet is the easiest and most effective way to carry out identity theft. It is simple for criminals to use a person’s credit card information to make purchases because transactions over the Internet occur quickly and without prior personal interaction. It is quite easy for any person to get another’s personal details if a victim is careless. Shoulder surfing is a method by which a thief looks over a person’s shoulder to see the person’s password or PIN. Identity thieves also use phishing to acquire personal information.

- **Credit card fraud**: In credit card fraud, attackers illegally use another's credit card for purchasing goods and other services over the Internet. Attackers can steal personal details using different techniques such as phishing, eavesdropping on a user’s transactions over the Internet, or using social engineering techniques. In social engineering, an attacker extracts personal details from a user through social interactions.

- **Illegal downloading**: Illegal downloading is an offense under the cyber laws. Downloading from an authorized Web site is acceptable; however, an unauthorized organization or individual cannot sell any product that is copyright protected. Illegal downloading affects the sales of that product. This type of crime is rampant because of the availability of tools for cracking software. Different types of services are provided for customer satisfaction but are misused. There are many issues that lead to illegal downloading. These include:
  - Getting products at low cost or for free
  - No personal information required
  - Readily available throughout the world

The following are the types of items downloaded illegally most often:

- **Music**
- **Movies**
- **Software**
- **Confidential or defense information**