Chapter 1 INTRODUCTION:

1.1 Preamble

It is observed that, now-a-days, all most every one of us, use “credit cards, debit cards, ATM cards” and do transactions on the Internet. The users are increasing exponentially. And so are the frauds such as phishing, Pharming, DoS attacks. We read about somebody’s e-mail account getting hacked. We read all that and as long as it doesn’t happen to us, we have a tendency to ignore, overlook and postpone the issue. Unfortunately there is nothing like “Disaster Planning” in the minds of a common man. Is it that the people are waiting for the disaster to happen first and only then they will understand the seriousness and depth?

We, therefore, must realise that there exists a certain amount of RISK and every citizen should be ALERT and AWARE of these threats and not only know the solutions theoretically but also implement the remedial measures.

1.2 About Internet:

The Internet, an inevitable tool: In today's world, the Internet is considered to be one of the most useful tools for people to communicate, find information and to buy goods and services.

With the growth of e-commerce also comes a significant increase in the variety of fraudulent Web activities. Phishing and other online scams involving the misappropriation of consumers’ digital identities is on the rise. Phishers are constantly experimenting, looking for better ways to defraud Internet users and reap more money from their crimes.

The trust factor: Many people deliberately limit the transactions they do online because they don’t fully trust the e-commerce process. These people simply fear for the security of personal and financial information transmitted over the Web.

Innocents are getting affected. “Ignorance” is also a crime in the books of law. Business people and people doing a major transactions on the net are the Cracker’s main victims.

Easy Victims: Younger generation, say from the age of 12 to 20, are more vulnerable to Cyber attacks because of their half knowledge and the trills of doing something to impress their friends.
where the “wrong deeds” are glorified. Their curiosity and attraction pulls them into the cyber crime activities.

Limitation of the Society: Business leaders often struggle with the challenge of staying current on relevant topics when they have limited time to devote to the effort.

- The time constrain
- Geographical distance constraint
- The availability of knowledge
- Apathy in the minds of people
- A more casual attitude & mind-set

Need “to be ALERT & AWARE”: It is a fact that many people already have been victimized by identity theft resulting in their losing money or even facing charges for crimes they did not commit. This is why it is very important for you to secure yourself from these crimes not just in the real world, but also in the cyber world as well.

Prevention is the best policy: You can stop these crimes from happening by simply installing the best kind of Internet security software available. Internet security software is a program that combats modern day threats, such as viruses, spyware, adware, trojans, keyloggers and hackers. It is software that will protect your computer from being invaded by these malicious programs.

A Continuous process: Security should always be high on the IT agenda simply because cyber criminals know that a successful attack is very profitable. This means they will always strive to find new ways to circumvent IT security, and users will consequently need to be continually vigilant. uppermost among its requirements.

1.3 About Cyber-security & Ethical Hacking

Cyber-security professionals protect data and systems in networks that are connected to the Internet. On the other hand Cyber-criminals or hackers strike in various ways by virus attacks, which may erase your entire system or someone can steal confidential information from your systems or even break into your systems and modify your files and that too without your knowledge.
A hacker finds the loopholes in a system, called “trap-doors” and breaks into it. The information security professional, an ethical hacker too has a similar job. He needs to think like a hacker: find the loopholes in the system before a cracker can. And patch it.

All communications must be secured since the information stored is ultimately a valuable resource of the business. The growing number of the computer Network attacks and sophistication in attack technologies has made this task more complicated.

Therefore the need of the hour is to update the knowledge on the network security issues and solutions, not only of the personnel manning networks and systems but also the common man like you and me. Make a better place for you and for me.

“ …… Heal The World, Make It A Better Place (To Surf) For You And For Me And The Entire Human Race…..”

1.4 Importance of Internet Security

In the conventional commerce the assets are land, building plant and machinery.
However, in e-commerce the assets are “data”, “database”, “user-id”, “password”, “pin”, “Biometrics”, “the web-page”, “the I.P. Address”. The currency of today is “Time”, “Information”, “Knowledge”, “Human Talent” and “Royal customers base”.
All these can easily be stolen / tampered if proper care is not taken.
We need to protect them from Crackers: who can not only withdraw all the money that you have in the account but also take advance on your-name and the crackers enjoys the money and YOU keep paying throughout your life.
You can lose all the goodwill in the market if your “website” gets stolen / defaced.

1.5 The statistical facts & International Standards:

Millions of phishing URLs were reported in 2008. The number of phishing attacks continues to grow, with the number of global phishing attacks growing by a whopping 66 percent compared to 2007, equating to 135,426 separate incidents, according to research from RSA Security.3 It’s no surprise that cyber-crime has moved from being a part-time activity to a full-time career for true criminals. Cyber crimes range from tampering computer documents, hacking, cyber
pornography to false electronic evidence, unauthorised access to protected computer documents and breach of confidentiality.

1.6 Consumer Needs:

As a result the clients are less inclined to make online purchases and give away private and confidential and other financial information. 

The needs of the consumers all over the world, today NEEDS the following.

1. Consumer need to feel that the site they visit and transact is secure that their personal and financial information is safe from online theft.

2. Consumer need to feel confident that your site is authentic.

In a Phishing attack, the innocent customer is (mis) guided to a fraudulent site and for some excuse or the other promotes the user to giveaway his personal and confidential information such as user-id, password, pin etc.

Guess which one is genuine and which one a Fraudulent?

Difficult to judge! No wonder 90% were deceived!

This is just the “front-end” of the PHISHING attack!