CHAPTER – VIII

LIMITATIONS, RECOMMENDATIONS, SUGGESTIONS AND FURTHER RESEARCH
CHAPTER – VIII

LIMITATIONS, RECOMMENDATIONS, SUGGESTIONS AND FURTHER RESEARCH

8.1 Limitations

The participants may potentially heighten the awareness of the subject matter. Suspicion and the security knowledge may be related. Some individuals were aware of phishing but due to their negligence in reporting they are victimised. The survey method was used in Data Collection, where the participants were distributed instrument either physically or electronically and asked to respond. The participants may hide off the facts even they were fallen prey for phishing attacks due to shy that others may suspect their expertise in using the web.

8.2 Recommendations and Suggestions

The astounding growth of online users, the difficulty in establishing trusted identity online and the lack of standardization around protection all contribute to the challenge of developing a regulatory scheme. But phishing and e-crime losses may compel interested parties to action.

There is no single solution that can counter attack. A combination of existing techniques and commitments can considerably mitigate the risk and financial effects of phishing. Future technologies hold the assurance of spectacular security betterments.

Organizations spend a lot of time and money trying to protect their networks. They focus on technology like upgradation, high-end encryption techniques but a popular means of gaining access bypasses the technical systems completely, which is based on the long-time con or confidence game and has a new name and new face – social engineering.

As business entities have increased their digital presence, the economic value of conciliatory account credentials has increased considerably. Fraudsters such as phishers can yield to invest in technology commensurately with the illegal benefits gained by their crimes.
Good policies are the vital foundations to a security program. They should be designed keeping in mind about the target audience. They should be written in a simple, clear, concise language, avoiding IT jargon.

Policies must be for a span of period and must be reviewed and kept current. Policies must be reviewed on a rotational basis, on a specific time frame. As and when the issues arise the policies may be changed to suit changing requirements and technologies.

Policies can be modified, and obsolete policies should be cleared out. Upon updating, the policies can be posted on the institution intranet, with current version number and date, so that the current version is always readily available to the stakeholders.

As the business entities are making customers aware of the threat of phishing and their policies and practices for their customers, there should also be consideration for providing them with the ability to verify the authenticity of digital communications.

There are wide varieties of tools that can be utilised in a security awareness program, all interrogatively efficient to a degree. Institutions can eye upon use of videos, newsletters, brochures, booklets, signs, posters, caps, coffee mugs, pens and pencils, printed computer mouse pads, screensaver, logon banners, note books, note pads, desktop artefacts, tee shirts and stickers for propagation.

The government should play a role in security regulation for cyber defence. It should establish a regulatory construct for assessing the state of security and setting minimum standards of security for entities that are part of critical infrastructure. The aim should be to identify deficiencies and assess certain sectors with a security grade. It could be supported with a tax credit for businesses that make the grade. Most importantly, any government involvement should not inhibit innovation or investment.

More government-private sector task force (e.g., CERT-IN) to oversee and coordinate its implementation of implications for phishing-related legislation should be established. They also should aid in forwarding best security practices for ISPs and other network operators, and for digital marketing. The law be enacted to prevent emerging threats to the safety and protection of the Network.
A legal coordinating entity should be formed to cover the issue on current grounds. This is crucial for the phishing issue, since it is carried out through the technique of spamming, by means of which unsolicited, bulk e-mails are sent. Spam routinely allows fraudsters to send deceptive e-mails to many recipients at moderate cost.

The law enforcement agencies should adopt particular criminal laws on identity theft which can be utilized to phishing, in addressing spreading of deceptive emails and the use of phishing email headers or other techniques feature of criminal fraudsters. The agency should aid in preparation of a strategically mean to counter all forms of identity theft more efficaciously, including possible modifications in laws where allowed.

Users, legal enforcement agencies, and the private entities should realise that as public education about phishing enhances, fraudsters will continue to use these chances to develop additional variants and refining their phishing techniques.

8.3 Further research

The results suggest that, the use of anti-phishing counter measures is habitual behaviour; further research can be carried to study the ways by which anti-phishing counter measures becomes habitual. This might aid the practicing researchers and developing practitioners to understand means to create the habit of using anti-phishing counter measures.

Spear Phishing have become a menace to the organizations. By means of Spear Phishing, the organizations reputation will be under jeopardy. As like a standard phishing e-mail, the Spear message looks to be originated from a trusted source, such as co-worker who will e-mail message to other employees or for a selected people in the organization (Example, HR manager or a system admin), in an attempt to gain login information. Since the recipients receive message from a known and trusted source, requisition for sensitive information such as login names or passwords may appear more credible. Spear phishing frauds work to gain entry to an entities computer network.
The Information Security Behaviour can be studied separately for system users at work and home environment. The present work demonstrates, users’ demographic is valuable constituents for social engineering researches and other Information security research.

The user factor allows substantial measures for Information security, and a worthy constituent that controls the HCI with Information security. The study showed that young users are more likely to fall prey and victimised for phishing attacks. The casual relationship between gender and social engineering is determined by the behaviour of internet usage. A machine learning model for anticipating users’ susceptibility to phishing, and assessing current deployable means to counter social engineering threat at the technology front can be studied. By means of this, broader class of solutions can be investigated.

Phishing awareness training can be conducted with before- and after- testing upon experiment and control sections may be carried on to view upon the effectiveness the training program will have on users.

The Security Threats of the Mobile phone users can be studied separately as the usage of smart phones is increasing rapidly.