Sri Lanka CERT Cyber Security Awareness Survey, 2015- Summary of Findings

The following survey was conducted by Sri Lanka CERT, the focal point for Cyber security research in Sri Lanka to investigate the level of cyber security awareness among our citizens. The data was gathered over a three day period. The following analysis involves a dataset of 347 responses.

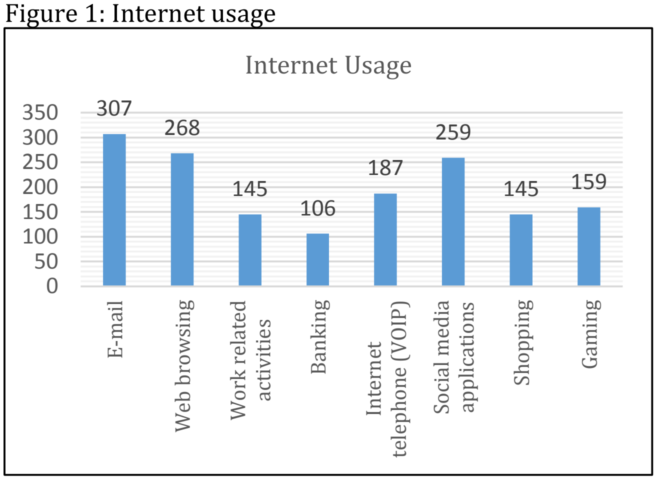
Demographic Profile of Respondents

Of the total sample, 84% was male and 16% was female. Majority of the respondents were in the age category 15-25 (66%). The distribution of the sample by the level of education show that 34% of the respondents have studied up to A/L while another 33% have undergraduate degrees. Majority of the respondents (35%) have 6-10 years of Internet experience while another 34% have 1-5 years of experience. 52% of the respondents were students while another 21% responded as working in the private sector.

Internet usage

According to the data (see *Figure 1*), majority of the respondents use the Internet for E-mailing, Web browsing and for interacting on social media sites. The frequency of usage is lower for Internet shopping (42%) and banking (31%). Note that this question required the users to select more than one option (if applicable) in terms of their Internet usage behavior. Participants also mentioned that other than the activities listed in *Table 1*, they also use the Internet for blogging, educational and entertainment purposes.

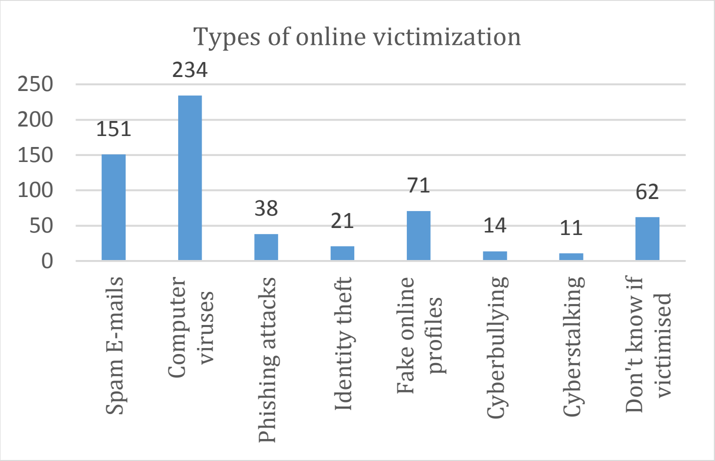
Figure 1: Internet usage



Online victimization

Online victimization statistics indicate that 67% of respondents has been affected by computer viruses at one time or another (see *Figure 2*). Reports of Cyberbullying and cyberstalking incidents were less than 5%. Few mentioned that they have been affected by adware and spyware while using the Internet.

Figure 2: Types of online victimization



Cybersecurity awareness

The survey respondents' seems to be more aware about certain types of cybersecurity threats than others (See *Table 1*). For instance, 85% knew how to install and update anti-virus programs and 75% knew how to activate the computer's firewall. Similarly, 75% were aware how to change social media privacy settings in order to increase the level of online privacy. Only 50% of the respondents knew how to identify an email scam while only less than half the sample said they will not open email attachments without verifying the authenticity of the sender. Only a small percentage of individuals (15%) said that they would share their passwords with someone else. Interestingly, 54% of the sample were parents and only 22% of them knew how to activate parental control on their computers as a safety measure to protect their children online.

Table 1: Online threat awareness

Type of threat awareness	Frequency	%
Installing & updating anti-virus programs	294	85
Enabling computer's firewall	259	75
Changing social media privacy settings	259	75
Ability to identify email scams	173	50
Opening email attachments only from trusted sources	166	48
Belief that one's personal information is of no value to hackers	123	35
Ability to activate parental control	77	22
Adding unknown individuals to social media accounts	70	20
Giving password to someone else	53	15

Overall, the survey participants seem well aware of the most common type of security enhancement tools/techniques such as using anti-virus programs and enabling firewalls etc.,. However, their awareness about email scams, ability to verify whether an email attachment is safe to open, and the ability to activating parental control on home computing devices is not adequate and should be improved through awareness education. It is somewhat surprising that 35% of the respondents believed that their information is of no use to hackers. This shows that the users are unaware of the value of personal information, especially in the hands of third parties or cybercriminals who could misuse such information in various ways.