Security-Aware Passwords and Services Usage in Developing Countries: A Case Study of Bangladesh

Rasib Khan[1(✉)] and Ragib Hasan[2]

[1] Department of Computer Science, Northern Kentucky University, Highland Heights, KY, USA
khanr2@nku.edu

[2] Department of Computer Science, University of Alabama at Birmingham, Birmingham, AL, USA
ragib@uab.edu

Abstract. Users from developing nations, such as Bangladesh, had a rather late entry into the information highway and may not be equally aware of the different secure practices on the Internet. Such behaviors include awareness of security technologies, having similar/dissimilar passwords, frequency of changing passwords, saving passwords on browsers, and verifying authenticity of visited websites. The category of services being accessed as well as the type of devices being used may implicate the level of exposure to identity theft threats. Unfortunately, users never behave in the expected manner in terms of practicing secure technologies. In this paper, we present a study on security-aware usage of passwords and Internet-based services for users from Bangladesh. We conducted an online survey on a total of 1682 Bangladeshi Internet users in English and Bengali language. We analyzed the survey statistics to study the general trend of behavior, practices, and expectations pertaining to secure Internet usage and identity preservation. We posit that such a study can help researchers identify the weakest-link of Internet safety and focus on building secure technologies to protect users from online crimes in developing countries.

Keywords: User study · Developing country · Security awareness
Case study · Bangladesh

1 Introduction

The rate of Internet penetration in developing countries is increasing everyday. Each of these users on the Internet has their personal behavior and practices [16,27]. Unfortunately, a lack of IT-education in such developing countries result in a lower level of awareness and cognizance of secure Internet practices and is a crucial concern in terms of protecting their digital identities [11].

J. E. Ferreira et al. (Eds.): SCC 2018, LNCS 10969, pp. 67–84, 2018.
https://doi.org/10.1007/978-3-319-94376-3_5

Bangladesh is a South Asian country with a population of approximately 156.6 million and a growth rate of 3.6% as of 2013 [29]. The IT infrastructure is progressive with a mobile penetration rate of 56% as of 2011 and increasing every year [28]. The number of mobile subscribers and Internet users were 121.9 million (≈77.8%) and 42.7 million (≈27.3%) as of January 2015 [3]. Advancement of the IT infrastructure has significantly affected the way people use their personal information on the Internet and has been misused in developed countries since the beginning [9,13,30]. We posit that a lack of Internet security awareness in developing countries as Bangladesh may result in increased e-crimes with this exponential increase in the number of Internet users. Various studies have been conducted on users from developed countries [7,12,17]. However, to the best of our knowledge, this is the first time a study on security-oriented practices of Internet users from developing countries has been performed.

The frequency of accessing the Internet and the types of services being used can imply the susceptibility of the users. Secure password policies aim to ensure safety of the users [10,25]. Unfortunately, complicated policies result in degraded usability and reduced memorability [32]. Usable technologies, such as, saving of passwords on mobile devices and/or web browsers, provide users with various tools and services to manage and use their personal information [7,20,24]. Unfortunately, the different types of devices, such as smartphones, which are being used to access the Internet, are exposed to different levels of threat, resulting in compromised private information [2].

Such incidents are quite often the result of unawareness of users towards secure technology usage. Password habits of users do not comply to the secure practices suggested by security experts [27]. Moreover, enforced security does not always guarantee proper behavior [10]. There had been numerous research which illustrate the inability of general users to apply secure technologies in commonplace activities, such as risk evaluation, secure emailing, and web surfing [6,8,26]. Researchers have also attempted to tie information security with the psychology of Internet users in various contexts [1]. Therefore, the security of devices and services on the Internet must be designed to address the security holes created due to the users' behaviors and practices [25]. However, most of such studies have been performed on users from the developed world. In this study, we bring these perspectives on the behavioral aspects of Internet users from Bangladesh. In the context of developing countries as Bangladesh, the lack of awareness on secure practices makes the situation complicated with a greater risk of exploitation of Internet users.

Contributions: In this paper, we present the results of an online survey on security-oriented usage of passwords and services for 1682 Internet users from Bangladesh. The survey data reveals crucial information regarding the weakest-links in Internet security: the practices of the users. We performed a cross-analysis of password and service usages to identify the security-critical aspects in online behavior. We posit that such a study can greatly help researchers to design Internet-enabled services with a guided knowledge of the users' behavior and ensure greater security in developing countries.

The rest of the paper is organized as follows. We present the related work in Sect. 2 and our survey methodology in Sect. 3. The results from the study and a discussion on the presented work are presented in Sect. 4 and Sect. 5 respectively. Finally, we conclude in Sect. 6.

2 Related Work

A lot of people fall victims to Internet scams every day [4,13]. Susceptibility of naive Internet users being victims of malware and viruses is not new [12,18,23]. The number of identity theft cases have increased from 12 million in 2012, which was a 13% increase from 2010, to 13.1 million in 2013 [17,21]. Unfortunately, one-third of such victims do not take any further actions to prevent future exploitation [19]. With a high Internet and mobile penetration rate in Bangladesh [3,28], the aspects of secure Internet practices is a crucial field of study with respect to such developing parts of the world.

Hull et al. [9] analyzed the contextual privacy issues on Facebook and the way social media effects privacy issues. User behavior regarding disclosing the identity on micro-blogs and the relative factors have been studied by Lee et al. [16]. Wagner et al. [30] presents an interesting work on malware infected Twitter users and their actions, and categorizing them based on the users' level of susceptibility. According to most studies, the primary factors influencing the behavior of users on the Internet are age, education, gender, technology experience, content creation and sharing, online activities, income group, amount of leisure time, and the type of job.

Kumaraguru et al. [14,15] presented a qualitative study based on 20 individual interviews, focus group discussions, and a widely circulated survey on privacy-oriented practices in India. Pew Research Center published a report [22] on Internet usage and psychology of users from developing countries while using various services. Chen et al. [5] discussed the security perceptions in Ghana from an interview survey of 193 participants. However, our study focuses on the analysis of security-aware practices and the overall safe/unsafe behaviors of users on the Internet in such developing countries.

Stanton et al. [27] presented an analysis of user behavior based on a two-factor taxonomy for classification. A large-scale study on the use and re-use of web passwords was presented by Florencio et al. [7]. A survey on the usability of passwords enforced by password creation policies was presented by Inglesant et al. [10]. The reasons why people generally maintain Internet anonymity was studied by Kang et al. [11]. Most of such studies focus mainly on developed countries. However, Internet trends in developing countries are different than that in developed counties. Additionally, our study intends to unfold the generalized aspect of security-oriented behavior for Internet usage in developing countries.

3 Survey Methodology

Survey Questionnaire: The survey consisted of two demographic questions, and 18 information-oriented questions. We inquired the age and geographic location

of the respondent and no other private information (e.g. name, IP address) were asked/stored. The survey was conducted using a publicly accessible online form. The survey was available in two languages: Bengali and English. The translation of the questionnaire from English to Bengali was performed by four volunteer Bengali native-speakers. The survey agreement stated that no personally identifiable information would be asked or stored, and the published research will only include aggregated results. The agreement also specified that the storage of all collected data will be within secure physical perimeter within the research institution. The responses for each of the questions were qualified with pre-specified options. All questions were provided with an explanatory sub-text and examples (e.g. *changing passwords of your account is a complex operation, website authenticity can be validated by the secure lock symbol at the corner of your browser*) to ensure clarity of understanding for both language versions.

Population Recruitment: The survey population of 1682 users were all voluntary participants. The survey questionnaire was promoted via social media networks (Facebook, LinkedIn, Twitter, Google+), personally, as well as in different social and professional groups. The survey included a consent form, upon agreeing to which, the user was taken to the survey page. The survey data was collected over a period of three months between September 2014 and December 2014.

Limitations: The primary target of the survey was to collect preferential and behavioral data from Bangladeshi Internet users regarding secure password and service usage. Due to the nature of publicity, the collected data may have a certain bias towards the behavior of users who are active in social networks. The participation in the survey was not controlled and was completely voluntary. The authors' social network connections and community groups were utilized for publicity.

4 Survey Results

In this section, we present the summary of the findings from the security survey on the Internet users from Bangladesh.

4.1 Survey Demographics

The survey included respondents over the age of 19 in five different age groups and excluded minors (18 and below). The box-plot of the respondents in five different age groups is shown in Fig. 1. The median age was between the ages 25 to 29 years with the interquartile range between ages

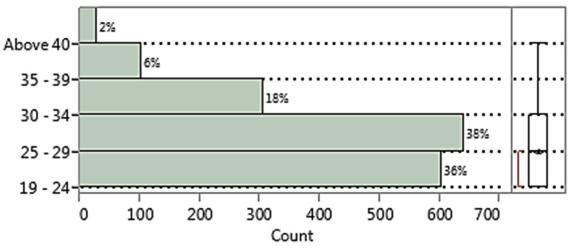

Fig. 1. Age group distribution

19 and 29 years. The age distribution shows that most of the users who participated in the online survey were rather young and active on the Internet and can be considered as the tech-savvy generation of users. The data was collected using survey forms in Bengali and English languages. Table 1 summarizes the response distribution for the two languages.

4.2 Usage Frequency Vs. Security Knowledge

We surveyed the frequency of Internet access of the users, varying from more than once a day to at least once a month. Majority (96%) of the users claimed they were very frequent Internet users, accessing the Internet at least once a day. Hence, we were assured that the study emphasized on the behaviors of the most frequent Internet users.

Table 1. Distribution for Bengali and English responses

Language	Count	Percentage
Bengali	1507	89.59
English	175	10.41
Total	**1682**	**100**

We asked the level of (self-proclaimed) knowledge the respondents had in security. Only 16% of the users felt that they have a high level of (self-proclaimed) security-oriented knowledge on the Internet. On the other hand, 65.1% and 18.7% of users responded to have moderate or low level knowledge of Internet security respectively.

We were also interested to see the variation of (self-proclaimed) Internet security knowledge with respect to the frequency of access to the Internet. Figure 2 shows the distribution of users for different levels of knowledge for varying Internet access frequencies. The frequencies are shown in numbers (1 to 7) with decreasing frequency, based on the different options from 'more than once a day' to as few as 'at least once a month'. We observed an overall trend of moderate level of security awareness among the users regarding Internet safety, varying within 63% and 68% among most frequency groups with at least 1% of total user responses.

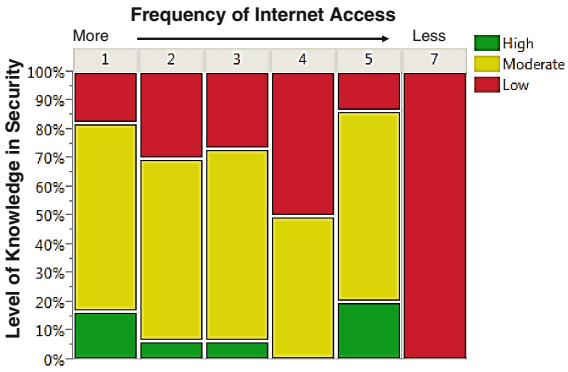

Fig. 2. Frequency of Internet access vs. (self-proclaimed) Knowledge of Internet security

4.3 Security Knowledge Vs. Language

We further investigated the (self-proclaimed) knowledge of security on the basis of the response language (Bengali and English). A higher percentage of English language respondents (24%) compared to the Bengali language respondents (15.34%) claimed to have 'high' level of knowledge of Internet security. The statistical test

displayed heterogeneity of the proportions among the two groups (chi-Square $\chi^2 = 8.119$, Degrees of Freedom (DF) = 2, p-value = 0.0173). We believe that there might be two probable reasons for this particular observation. First, the fact that 55.5% of contents on the Internet till today are in English, which creates a general obstacle for self-awareness among other Internet users [31]. The second probable reason might be that non-native English speakers in developing countries, such as Bangladesh, might be considered more educated than the rest of the population.

4.4 Popularity of Internet Services

We surveyed the users regarding their usage of online services, such as email, social networks, messaging, and media streaming. The summary of the results is presented in Table 2. Online social networks were the most popular service among the users (98.9%). However, social media was one of the major channels of our survey publicity and might have created a certain bias in the result. The second-most popular service is emails (95.4%), which is followed by the rest. Table 2 also lists the top 6 combinations (above 4%) of popular Internet-enabled services. We found that 25.5% of the respondents were users of all the listed services.

Table 2. Popularity of Internet-enabled services

Internet-enabled services	% Users
Social networks	98.9%
Email	95.4%
Messaging	68.1%
Streaming	79.5%
Maps and navigation	66.2%
Finance management	43.0%
Bill payments	42.9%
Top 6 combinations of popular Internet-enabled services	% Users
All services	25.5%
Emails, social networks, messaging, streaming, maps & navigation	15.1%
Emails, social networks, messaging, streaming	7.3%
Email, social networks	5.2%
Email, social networks, streaming	5.0%
Email, social networks, streaming, maps & navigation	4.5%

4.5 Password-Oriented Behavior

The data showed that 72.2% (23.7% + 48.5%) of the users had all or at least some of their passwords similar to each other. 7.7% of them also responded that they never changed their passwords with 74.1% rarely changing their passwords. We performed a cross-variance analysis for the two variables. As seen from the heat map in Fig. 3, the largest class of users are those who had all or some of their passwords similar to each other and rarely changed the credentials (37.4%). Given the current scenario of online account breaches and similar attacks, the behavior of users for password-oriented practices poses as a critical security issue in terms of identity thefts. The behavior of users regarding similar passwords and frequency of changing passwords were homogeneous for the two language groups (*Similar passwords*: $\chi^2 = 0.247$, $DF = 2$, p-value = 0.8839; *Changing passwords*: $\chi^2 = 3.121$, $DF = 2$, p-value = 0.2101).

4.6 Logging-In Practices

The survey included three questions to extract the behavioral practices pertaining to logging-in to online services. We observed that 62.5% (19.6% + 42.9%) of users saved most or at least some of their passwords on web browsers. Additionally, 57.9% of users preferred automated sign-in with 44.6% using Single-Sign-On (SSO) services. We analyzed the cross-variance in terms of the preference for automated sign-in for both saved passwords and SSO services. Among the users who preferred automated sign-in (44.6%), as shown in Fig. 4, 82.5% (32.1% + 50.4%) actually saved most or some of their passwords on the web browsers. Interestingly, many users (34.8%) still saved passwords on their browsers even though they did not prefer automated sign-in.

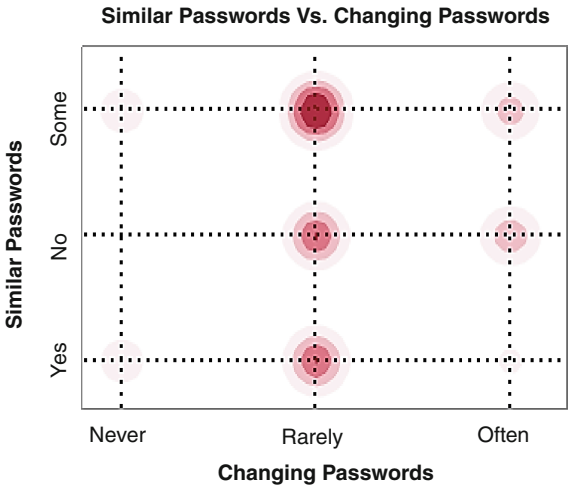

Fig. 3. Usage of similar passwords vs. changing passwords

For users who preferred automated sign-in (44.6%), as illustrated in Fig. 5, 53.3% of users were using SSO for automated sign-in. However, we also observed that many users (32.5%) also used SSO even though they did not prefer automated sign-in. We drilled down further to observe the effects of saved passwords and SSO on the preference of using automated sign-in. We created a nominal logistic model and a generalized linear model to fit the data for the corresponding classes. Both models performed similarly with p-value < 0.001 and maximal standard error 0.095 for the two intercepting variables. The result implied a high correlation between the preferences for automated sign-in with saving passwords and using SSO services.

4.7 Third-Party Applications

Third-party applications, such as Facebook apps, require authenticated access to personal accounts. Surprisingly, only 34.3% of the users responded that they do not allow these applications access to their accounts. This is a positive indication of a good number of online users being aware of their privacy. However, 65.6% (2.1% + 63.5%) of users, always, or at least sometimes, grant such applications the access rights to their personal accounts. For the people who saved most or at least some of their (probably the most frequently used) passwords on web browsers (62.4%), 70.1% of the users (which is 43.8% of the total sample

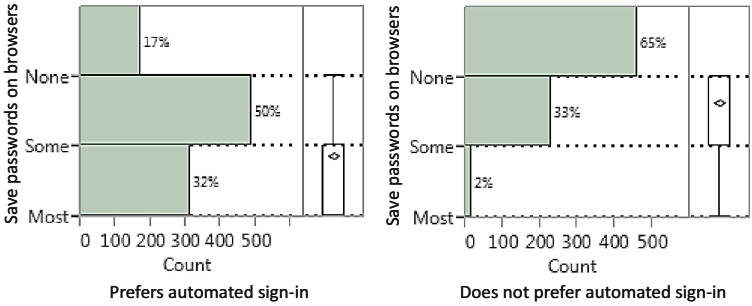

Fig. 4. Saving passwords on browsers vs. preference for automated sign-in

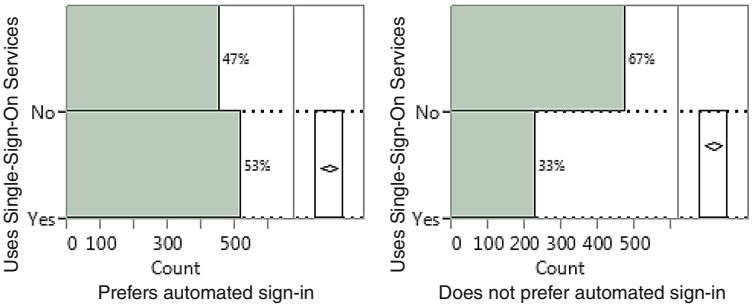

Fig. 5. Using Single-Sign-On services vs. preference for automated sign-in

population) always or at least some times allowed third-party applications to access their personal information. On the other hand, among the users who never saved their passwords on web browsers (37.5%), 41.7% of them never allowed third-party applications to have access to their accounts. Therefore, the distribution of users allowing third-party applications with respect to saving their passwords was heterogeneous ($\chi^2 = 26.402$, $DF = 4$, p-value < 0.001).

4.8 Usage History Vs. Anonymity

Usage history is commonly utilized for augmenting online services, such as, search results, recommendations, advertising, and financial activity detection. Overall, 88.1% (36.2% + 51.9%) of users felt strongly, or at least to some degree, that, usage history is useful in identifying them on the Internet. On the other hand, 52.2% of users responded that anonymous authentication is useful for them while accessing Internet services. 26.7% of the users felt that anonymous access might be something which is useful to them, even though they weren't completely sure about it.

As shown in the heat map in Fig. 6, almost 39% of the users were inclined towards benefiting from usage history but still preferred anonymity while accessing the services. However, we observed a heterogeneous distribution for the preference of usage history with respect to anonymity ($\chi^2 = 24.781$, $DF = 4$, p-value < 0.0001). This was due to the fact that a total of 62.2% of the survey sample were probably confused or unsure regarding their preference for either usage history or anonymity. We found that usage history and anonymity were heterogeneously distributed among the Bengali and English language respondents (*Usage history*: $\chi^2 = 11.475$, $DF = 2$, p-value $= 0.0032$; *Anonymity*: $\chi^2 = 17.391$, $DF = 2$, p-value $= 0.0002$).

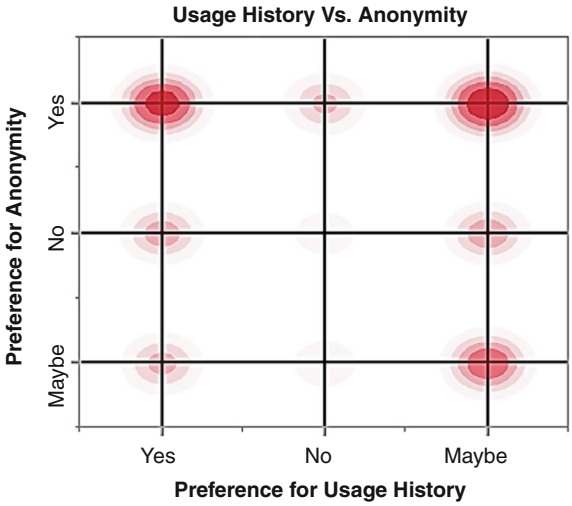

Fig. 6. Expectation of users regarding usage history vs. anonymous access

4.9 Usage of Internet-Enabled Devices

The type of devices that the users utilize to access the Internet can imply a lot on Internet-safe behavior. Our survey inquired the users on the different types of devices that they use. The summary of the different types of Internet devices is presented in Table 3. The most popular devices are personal laptops (77.7%) and smartphones (75.5%). Table 3 also shows the top 7 combinations (above 5%) for the combinations of Internet-enabled devices owned by the survey respondents. We observed that 22.4% of the respondents used both laptops and smartphones. The survey results showed that 82.9% of the users were using at least two devices to access the Internet and online services.

Table 3. Popularity of devices

Internet-enabled devices	% Users
Personal laptop	77.7%
Smartphone	75.5%
Personal desktop PC	54.3%
Tablet	22.6%
Public desktop PC	11.7%
Top 7 Combinations of popular Internet-enabled devices	% Users
Personal laptop and smartphone	22.4%
Personal desktop PC, personal laptop, smartphone	15.4%
Personal desktop PC, smartphone	10.3%
Personal desktop PC, personal laptop, smartphone, tablet	9.3%
Personal laptop	8.8%
Personal laptop, smartphone, tablet	6.0%
Personal desktop PC	5.8%

4.10 Complex Operations from Portable Devices

Given the popularity of portable devices, as shown in Table 3, we inquired if the respondents accessed complex operations, such as changing passwords and making secure transactions, from their smartphones and tablets. Such statistics are important to evaluate the scenario of privileged operations which the users perform on such portable mobile devices, and is summarized in Fig. 7. The results were similar between tablets and smartphones. We observed that 51.8% (17.2% and 34.6%) of smartphone users and 58.6% (18.7% and 39.8%) of tablet users accessed such operations on a regular basis or at least some times. Respondents who owned both smartphones and tablets had a higher percentage (61.1%) of privileged usage with both devices.

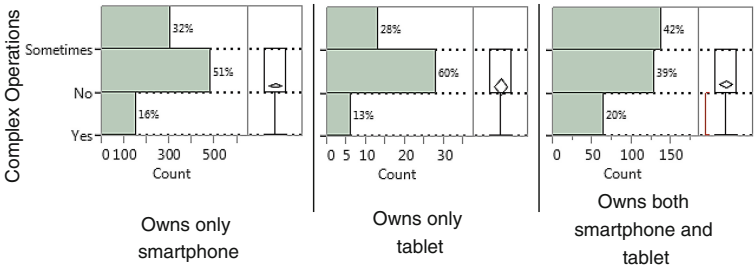

Fig. 7. Accessing complex operations from portable devices

4.11 Effective Re-authentication

A lot of Internet-enabled services require users to re-enter the authentication credentials for enhanced security. We found that 51.6% of the users were actually happy that they are being secure. Interestingly, 28.6% of the users seemed irritated with re-entering information, with 19.9% only doing it because they are asked for it. However, re-entering credentials does not carry any meaning if the users actually never changed their passwords, saved their passwords on the browsers, or were accessing privileged operations from their portable devices. We investigated the data using two approaches for modeling the mentality of users regarding re-authentication credentials.

In the first case, we utilized the responses for password-oriented behaviors, logging-in practices, and accessing privileged operations from smartphones/tablets to create a nominal logistic model. The model gained an Akaike Information Criterion (AIC) of 3146.53 ($\chi^2 = 328.886$, $DF = 20$, p-value < 0.0001). The primary effects were introduced by the preference for saving passwords on web browsers and automated sign-in (p-value < 0.001), followed by frequency of changing passwords (p-value $= 0.0089$) and having similar passwords (p $= 0.0157$). Next, we created a generalized linear model using the same response variables. However, we enforced a binomial distribution on for people

who were happy to be secure versus the others. The model reached an AIC of 2086.65 ($\chi^2 = 264.195$, $DF = 10$, p-value < 0.0001) with the same primary indicators.

Given the outcome of the models, we were interested to investigate the cross-variance of responses for re-entering credentials with the responses for saving passwords on browsers and preference for automated sign-in. We observed that among the users who were irritated to re-enter authentication credentials for secure logins and preferred automated sign-in (23.8% of total survey population), 85.8% saved at least some of their passwords on web browsers. Only 20.9% of users who were happy to be secure by re-entering their credentials but preferred automated sign-in did not save any passwords.

4.12 Privacy Awareness

Careless web browsing, especially, providing private information and not using privacy settings, may be considered a critical issue to address the increasing rate of e-crimes. 76.9% (37.8% + 39.1%) of the users responded that they never or only sometimes check the authenticity of websites prior to providing any private information. However, 64.8% of users mentioned that they use privacy settings, with 9.9% users who never use any privacy settings. A heat map of the two behavioral aspects is illustrated in Fig. 8.

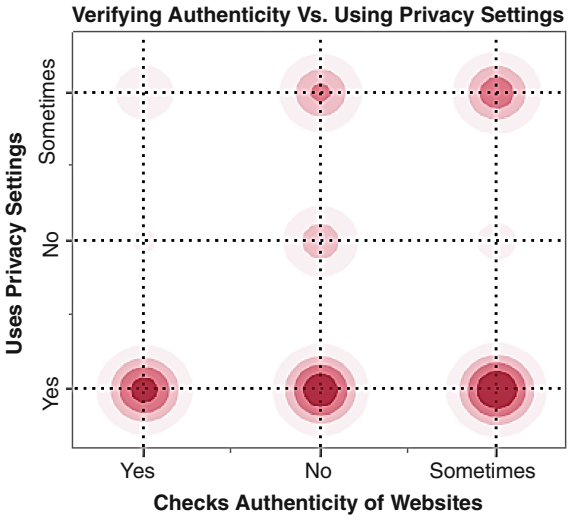

Fig. 8. Verifying authenticity of websites and using privacy settings on Internet

The cross-validation revealed that 71.4% (33.1% + 38.3%) of the users never or only some times checked the authenticity of the visited websites even though they were using privacy settings. We found that only 18.5% of the survey population used privacy settings and verified the authenticity of websites. Unfortunately, 67.7% of the users who did not use privacy settings did not check the authenticity of the websites at all. Additionally, 87.3% (38.2% + 49.1%) of respondents with sparing use of privacy settings mentioned that they were also not always aware of the authenticity of the websites.

4.13 Exploitation Victims

Internet users may be victims of various forms of e-crimes. We inquired if the respondents had the experience of hacked online accounts or misused shared online contents. 13.3% of the users reported that they had the experience of having their account(s) hacked with 16.4% of users who shared online contents which were later misused. A total of 25.7% of the users either had an experience of having their accounts hacked or their shared contents misused. A cross-variance analysis revealed that 24.3% of users who had experiences with content abuse also had their account(s) hacked.

We studied different models to fit the class of users with account breaches. We performed a stepwise iteration model generation approach to minimize the AIC. The model converged with AIC 1278.64 with 5 indicator variables ($\chi^2 = 57.661$, $DF = 7$, p-value < 0.0001). The model also had a lack-of-fit p = 0.5339. Experience of previous shared-content misuse played the major indicating role (p-value < 0.0001). The age of the user was the next key indicator (p-value = 0.0111). We observed that users who preferred anonymity were one of the other major indicators of prior victims of account breaches (p-value = 0.0231). The other indicator variables were users who allowed third-party applications to access their personal accounts (p-value = 0.0328) followed by the frequency of Internet usage (p-value = 0.0442).

Given that information misuse was the primary indicator of account breaches, we performed a stepwise model generation for information misuse victims. The model converged with AIC 1461.5 and had a different set of primary indicators ($\chi^2 = 61.955$, $DF = 10$, p-value < 0.0001) and a lack-of-fit p = 0.4429. The type of services accessed, the devices used to access the Internet, and the preference of usage history had dominant effects (p-value < 0.009). Additionally, the frequency of Internet usage (p-value = 0.0106), allowing access to third-party applications (p-value = 0.0.0141), and performing complex operations from portable devices (p-value = 0.0155) had significant effects on the outcome variable.

5 Discussion

We were able to gain insightful information regarding the security-oriented behaviors, practices, experiences, and usability preferences of Internet users from Bangladesh who are mainly active on social networks. The key findings from our study are summarized in Table 4. The survey population comprised of considerably active Internet users with varying frequencies for different types of services and moderate (self-proclaimed) level of security knowledge. Unfortunately, we still found that the users are not exercising proper behaviors in terms of password usage and security-awareness. Unfortunately, the preference for seamless authentication experience probably drives a lot of users towards 'unhealthy' practices. Users are quite often trusting third-party applications to have access to their personal accounts, which is inherently a risky behavior. Some users prefer anonymity while using the Internet, but which somewhat contradicts with their preference for usage history based services.

Table 4. Summary of key findings from the security-oriented survey

Key Findings
Participation: 74% of participation was between ages 19 and 29 with 91% of the respondents claiming to be frequent Internet users.
Awareness: Moderate Internet security awareness varies within 63% and 68% among all frequency groups, and was heterogeneously distributed within Bengali and English language respondents.
Service Usage: Above 95% of respondents used online social networks (98.9%) and email (95.4). 25.5% of respondents were users of all of the listed services. Low penetration of e-commerce in Bangladesh is a probable reason for only 43.0% and 42.9% respondents using financial services.
Password Usage: 72.2% of users had similar passwords for online services. 81.8% of users never or rarely changed their passwords. 37.4% of users had both similar passwords and rarely changed the credentials.
Logging-in Practices: Among the users who preferred automated sign-in, 82.5% of users saved passwords on web browsers and 53.3% used SSO services. Among users who did not prefer automated sign-in, 34.8% still saved passwords on the web browsers and 30.2% used SSO.
Third-party Application Access: 65.6% of users always or at least some times allowed third-party applications to access their personal accounts. 70% of users who saved their passwords on web browsers allowed third-party applications to access their personal information.
Anonymity and Usage History: 38.3% of users wanted anonymity with usage history. 49.6% of users did not feel the necessity for usage history, but still wanted anonymity. 62.2% of the users were unsure about the implications and applications of usage history and anonymity.
Internet-enabled Devices: Personal laptops (77.7%) and smartphones (75.5%) were the most popular Internet devices. 22.4% of respondents used both devices. 51.8% of smartphone owners, 58.6% of tablet owners, and 61.1% of both device owners accessed privileged operations from their portable devices.
Re-Authentication: Saving passwords on web browsers, preference for automated sign-in, accessing privileged operations from portable devices, changing credentials, and using similar passwords had influence on users in terms of re-entering authentication credentials for secure logins.
Privacy Awareness: 76.9% of users do not check website authenticity. 9.9% of respondents never use any privacy settings. 71.4% of users with privacy settings do not always verify website authenticity. 67.7% of users without privacy settings never verify website authenticity. 87.3% of users with sparing use of privacy settings are also not always aware of the authenticity of the visited websites.
Exploitation Victims: 13.3% and 16.4% of users had their account hacked or shared contents abused. Victims of shared content misuse, age, preference for anonymity, allowing access to third-party applications, and frequency of Internet usage had dominant effects in determining account hack victims. 24.3% of the content abuse victims had their accounts hacked. Type of services and devices, preference for usage history, frequency of Internet access, allowing access to third-party applications, and performing complex operations from portable devices had dominant effects in determining victims of content misuse.

The choices of Internet-enabled devices were considerably high for portable devices. Unfortunately, a high percentage of users performed privileged operations from such devices. As a result, this puts the users into the risk of identity thefts in case of a stolen device. Re-authentication mechanisms enforced

by service providers are supposed to enhance the security. However, a considerable segment of users were irritated with the process. Therefore, such users are inclined towards insecure practices which questions the overall effectiveness of the two-factor procedure. We also observed a general lack of awareness regarding the authenticity of websites and privacy settings when presenting personal information. Users who were victims of account hacks and information misuse had dominant effects on other behavioral aspects. However, some of the factors might be the reason why they were the victims, such as age and type of service/devices used, while some may have evolved as an effect of being prior victims, such as preference for anonymity and usage history.

5.1 Security Implications

Our key findings from the online survey can be leveraged by security researchers and service providers for designing security technologies and to ensure the safety of the Internet users. Moreover, educators can utilize the identified opportunities to deliver awareness messages for addressing the particular insecure practices.

Observation 1 (Language): Even though a developing nation, the high percentage of responses in Bengali from the younger tech-savvy generation shows the predominant interest for contents in their native language. This creates a concern, given that 55% of contents on the Internet are, in fact, available only in English [31]. As a result, security-news, tutorials, and similar contents are being circulated in a limited context. Therefore, contents on security-awareness should be available in native languages to gain the attention from such Internet user groups.

Observation 2 (Education Methods): We found that the knowledge on Internet security was not generally high irrespective of the frequency of Internet usage. Moreover, research works have suggested that self-proclaimed evaluations tend to be higher than collective comparison. In practice, many of the respondents claiming to be moderately well-aware of Internet security may actually be less educated than expected. As a result, a tendency of overconfidence usually leads to people being reluctant towards learning and being careless. The critical mass requires innovative and passive security education methods without the requirement of active involvement. Moreover, the majority of the educational institutions in Bangladesh have a Bengali medium of instruction. This provides us with an opportunity to leverage the role of such educational components to deliver security-awareness on the Internet from the grass-roots of the society.

Observation 3 (Service Channels): Users are regularly accessing different types of services, and therefore, all of them should be the focus of enhanced security. Moreover, the variety of service usage also provides us with opportunities to deliver security-awareness education via multiple channels. The high popularity of social networks and messaging is a direct implication of the younger generation being more active on the Internet. Therefore, the younger user group should be addressed with a higher concern for ensuring the security and privacy awareness on such social Internet-based services.

Observation 4 (Passwords): Majority of the users are vulnerable to insecure password-oriented practices. Users having similar passwords are evident in most Internet user groups. However, the reluctance to changing the passwords creates an incremental threat for such users. As a result, a stolen identity for one account can lead to the revelation of multiple accounts for the given user. Users can be educated on developing useful password setting techniques, which are both easy to remember and not similar across all the online accounts. Service providers are also required to instigate the password changing process for their users to ensure greater protection.

Observation 5 (Usable Security): Internet users have a tendency to prefer usability over security. Users were generally inclined towards experiencing automated and seamless authentication for Internet services. This is implied with the high percentage of users who usually saved their passwords to avoid typing in their passwords every time. As a result, this creates a weak link to ensure the security of such users and may be easily targeted by phishing and cross-site scripting attacks. The results signify the importance of usable security designs for services, and the impact such technologies can have on the security of Internet users.

Observation 6 (Relative Knowledge): Users allowing access to third-party applications may be the target of malicious advertisers and app developers. Client-side scripts and malicious applications can easily exploit the users in terms of privacy of their personal data using the saved credentials on the web browsers. We found that a general lack of security awareness can have relative effects on multiple insecure practices. On the other hand, users being educated on a particular security aspect may also learn to be aware of other secure practices by induction. Security educators can leverage the transitional knowledge application to create better awareness among the Internet users.

Observation 7 (Privacy): There is a limited rising awareness of users in terms of anonymity and privacy protection. However, a significant number of respondents were unsure regarding their preferences, showing the general lack of privacy issues on the Internet. Moreover, the heterogeneity for Bengali and English language respondents may be related to the limited security education, language barrier, and predominant English language contents on the Internet [31], as discussed earlier in observations 1 and 3.

Observation 8 (Device Usage): Users are logging into online websites from various devices and locations. Majority of the users are preferring portable devices (laptops and smartphones). However, mobility comes with the inherent risk of theft and loss. Therefore, users being prone to saving passwords on their devices (observation 6) are putting them under the risk of losing their credentials along with the loss or theft of a personal device. Security educators are therefore required to highlight the risks of using portable devices and the associated security concerns.

Observation 9 (Service Access): Users are performing complex operations from their hand-held devices while accessing Internet services. Public usage of

devices puts the users at risk of shoulder-surfing attacks. Accessing such services also results in an increased risk of user security and privacy. Unfortunately, the users are not being aware of the associated risks. Institutions and device sellers can be a channel to deliver awareness messages to the end users to not use such devices for complex and secure operations.

Observation 10 (Effective Security): The negative impact in the experience of users while re-authenticating was primarily driven by the reduced usability of the system. Users require intuitive and highly usable interfaces for properly utilizing security enforcing technologies. Conventional models simply burden the users with repetitive tasks and result in insecure practices. The general users are saving passwords on their browsers and opting for automated sign-ins, and thus, making the security ineffective for re-authentication. As a result, requirement engineering for Internet security technologies should be highly behavior and usability driven.

Observation 11 (Web Browsing): We observed a lack of awareness in web browsing, which is highly correlated to the privacy-unaware usage of online services. While some users claimed using privacy settings, most users were not aware of the authenticity of the websites. However, security of a system is only as strong as the weakest link. Such contradictory behavior puts the users at risk of phishing and exploitation attacks, irrespective of the active privacy settings. Online service providers generally display privacy concern for users due to the legal aspects of protecting the users' personal information. Unfortunately, a victim of a phishing attack is not the service providers' legal responsibility. Hence, security education for general users must thus focus on the importance of verified websites with corresponding implications.

Observation 12 (Victimology): Victims of identity thefts and misused shared contents had a high dependency on each other. However, we are unsure of the cause-and-effect relationship between the two cases. Our results show that users are inducing the threat upon themselves based on various combinations of behavioral practices. Such information can be highly leveraged to design user-oriented technologies for greater Internet safety and security. Researchers and developers should carefully study such cases of exploitation and design secure solutions based on the behavior of the users.

6 Conclusion

Proliferation of the Internet had also brought along various threats on the users. Secure technologies aim to protect the users, but often reduce the usability and force the users to incline towards insecure practices. The developing world had a slower start but is catching up to the tech-trends on the information highway. In this paper, we summarized the various implications based on the study on security-oriented practices, expectations, behaviors, and usability preferences of 1682 Internet users from Bangladesh. Our findings reflect that users do not behave in the ideal way that security experts believe that they should.

Expectations such as hassle-free and seamless authentication, drive behaviors and practices such as using SSO services. Moreover, degraded user experiences for increased security, such as, while re-authenticating, create inclination towards ineffective practices, such as, saving the passwords to avoid re-typing. We believe that security technologies should evolve from behavioral aspects and security comprehensibility of users, rather than only focusing on attacker models. Unfortunately, in today's world, Internet users circumvent the security and safety of technologies using improper practices, or simply suffer from degraded user experience. We provided a set of observations and the ways we can leverage the aspects of user behavior for providing security-awareness education. We believe, that, such a study can greatly help security researchers in designing effective, yet usable, and non-obtrusive technologies, to ensure the safety of Internet users from developing countries.

Acknowledgment. This research was supported by the National Science Foundation CAREER Award CNS-1351038, ACI-1642078, and DGE-1723768.

References

1. Anderson, R., Moore, T.: Information security: where computer science, economics and psychology meet. Philos. Trans. R. Soc. A Math. Phys. Eng. Sci. **367**(1898), 2717–2727 (2009)
2. Auchard, E.: Smartphones at Risk: Vulnerable to Stolen Passwords, Data Theft, August 2014. http://www.carriermanagement.com/news/2014/08/05/127054.htm
3. Bangladesh Telecommunication Regulatory Commission: Internet Subscribers in Bangladesh, January 2015. http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-january-2015
4. Bureau of Justice Statistics: Identity Theft Supplement (ITS) to the National Crime Victimization Survey (2012). http://www.bjs.gov/content/pub/pdf/vit12.pdf
5. Chen, J., Paik, M., McCabe, K.: Exploring internet security perceptions and practices in Urban Ghana. In: Proceedings of SOUPS. Usenix (2014)
6. Cybenko, G.: Why Johnny can't evaluate security risk. IEEE S&P **4**(1), 5 (2006)
7. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of WWW. ACM (2007)
8. Herzberg, A.: Why Johnny can't surf (safely)? Attacks and defenses for web users. Comput. Secur. **28**(1–2), 63–71 (2009)
9. Hull, G., Lipford, H.R., Latulipe, C.: Contextual gaps: privacy issues on Facebook. Ethics Inf. Technol. **13**(4), 289–302 (2011)
10. Inglesant, P.G., Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In: Proceedings of SIGCHI. ACM (2010)
11. Kang, R., Brown, S., Kiesler, S.: Why do people seek anonymity on the internet? Informing policy and design. In: Proceedings of SIGCHI. ACM (2013)
12. Khan, R., Hasan, R.: The story of naive alice: behavioral analysis of susceptible users on the internet. In: Proceedings of COMPSAC. IEEE (2016)
13. Khan, R., Mizan, M., Hasan, R., Sprague, A.: Hot zone identification: analyzing effects of data sampling on spam clustering. JDFSL **9**(1), 67–82 (2014)

14. Kumaraguru, P., Cranor, L.: Privacy in India: attitudes and awareness. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 243–258. Springer, Heidelberg (2006). https://doi.org/10.1007/11767831_16
15. Kumaraguru, P., Sachdeva, N.: Privacy in India: attitudes and awareness v 2.0. Available at SSRN 2188749 (2012)
16. Lee, S., Kim, Y., Lee, B.G.: Determinants of voluntary self-disclosure in the usage of micro-blog. In: Proceedings of ICONI, December 2010
17. Lipka, M.: Rise in Identity Fraud Tied to Smartphone Use, February 2012. http://www.reuters.com/article/2012/02/22/us-idtheft-javelin-idUSTRE81L16520120222. Reuters
18. Moore, T., Clayton, R., Anderson, R.: The economics of online crime. J. Econ. Perspect. **23**(3), 3–20 (2009)
19. National Consumers League: The consumer data insecurity report: examining the data breach - identity fraud paradigm in four major metropolitan areas. Technical report, Javelin Strategy & Research (2014)
20. Oh, H.K., Jin, S.H.: The security limitations of SSO in OpenID. In: Proceedings of ICACT (2008)
21. Pascual, A.: Identity fraud report: card data breaches and inadequate consumer password habits fuel disturbing fraud trends. Technical report, Javelin Strategy & Research (2014)
22. Poushter, J., Carle, J., Bell, J., Wike, R., Cuddington, D., Devlin, K., Keegan, M., Parker, B., Simmons, K., Stokes, B., Deane, C., Drake, B., Kent, D., Schwarzer, S., Smith, B., Zainulbhai, H.: Internet seen as positive influence on education but negative on morality in emerging and developing nations. Pew Research Center Studies, March 2015
23. Reynolds, J.K.: RFC1135: The Helminthiasis of the Internet, December 1989. http://tools.ietf.org/html/rfc1135
24. Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J.C.: Stronger password authentication using browser extensions. In: Proceedings of Usenix Security (2005)
25. Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F.: Encountering stronger password requirements: user attitudes and behaviors. In: Proceedings of SOUPS. ACM (2010)
26. Sheng, S., Broderick, L., Koranda, C.A., Hyland, J.J.: Why Johnny still can't encrypt: evaluating the usability of email encryption software. In: Proceedings of SOUPS. Usenix (2006)
27. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Comput. Secur. **24**(2), 124–133 (2005)
28. The World Bank: Bangladesh - leveraging ICT for governance, growth, and employment project (2012)
29. United Nations: World population prospects: the 2012 revision, highlights and advance tables. Economics and Social Affairs (2013)
30. Wagner, C., Mitter, S., Körner, C., Strohmaier, M.: When social bots attack: modeling susceptibility of users in online social networks. In: Proceedings of MSM. Citeseer (2012)
31. W^{3}Techs Web Technology Surveys: Usage of Content Languages for Websites, January 2015. http://w3techs.com/technologies/overview/content_language/all
32. Yan, J.J., Blackwell, A.F., Anderson, R.J., Grant, A.: Password memorability and security: empirical results. IEEE S&P **2**(5), 25–31 (2004)