USER BEHAVIOURS ASSOCIATED WITH PASSWORD SECURITY AND MANAGEMENT

Kay Bryant

Department of Management
Griffith University
k.bryant@griffith.edu.au

John Campbell

School of Information Sciences and Engineering
University of Canberra
john.campbell@canberra.edu.au

ABSTRACT

Control mechanisms established on the boundary of an information system are an important preliminary step to minimising losses from security breaches. The primary function of such controls is to restrict the use of information systems and resources to authorized users. Password-based systems remain the predominant method of user authentication despite the many sophisticated and viable security alternatives that have emerged from research and development. However, the literature shows that passwords are often compromised through the poor security and management practices of users. This paper examines user password composition and security practices for email accounts. The results of a survey that examines user practice in creating and using passwords are reported. The results show that many users know about the risks of hackers, viruses and so on and take preliminary steps to combat them such as having passwords longer than eight characters. However, this appears to be as far as many users are willing to accede to the probability that their information and computing resources can be compromised. This paper makes some recommendations for the education of users in creating and maintaining their passwords. The responsibility for these educational programs can be shared between governments, organisations, educational institutions at all levels, and software vendors.

Keywords: Password management, password security, user behaviours, user authentication, password composition

INTRODUCTION

Computers and information systems are pervasive in our modern world. The ready availability of the Internet and its continuing growth on a global scale only extends access to widespread computing and communication networks. Any communication sent over the Internet travels across unsecured channels, raising the spectre of security breaches for all who use the Internet. User identification and authentication along with encryption key distribution is one of the important functions provided by communication network services. In today's Internet-based environment, the reach of organisational networks and its external connections is significant. As such, the use of specialized software and hardware such as firewalls is used to implement basic access control functions (Oppliger, 1997). Controlling access to system resources is usually a three-step process. Firstly, users identify themselves to the mechanism, then they must authenticate themselves and the mechanism authenticates itself. Lastly, users request information technology resources and the actions they will take and the mechanism will either permit or deny the request based on information held on files that denote the resources and actions a user is permitted to undertake. The means by which users make themselves known to the system is typically through a unique identifier such as a name or an account number. Once the access control mechanism establishes that it has a valid user, authentication of that user is undertaken.

Establishing security on the boundary of a system is the first step in minimizing losses. Access controls are the usual type of control implemented on the boundary of a system (Weber, 1999). The function of these controls is to restrict the use of systems and resources to authorized user, as well as limiting the type of actions that a user can perform. There are three main approaches to user authentication: something the user has such as a smart card or other token; some physical characteristic of the user such as a fingerprint, retinal image, voiceprint or facial pattern; or something that the user remembers such as a password or PIN (Furnell et al., 2000). Each approach has its advantages as well as its intrinsic flaws. Regardless of the approach selected by the organisation, there is a trade-off between the value of the resources being protected and the effectiveness and cost of implementing and maintaining it. While significant advances have been made in graphics-based approaches (see for example Man et al. 2004 and Wiedenbeck et al. 2005) and in biometrics and visualization-based approaches (for example, see Jain et al. 2004, de Paula et al 2005), passwords remain the most common means of authenticating a user. Despite their potential weaknesses, password-based systems prevail because they can provide effective protection if they are used correctly used. However, they are conceptually simple for both system designers and especially end users who often compromise password security by forgetting them, writing them down, sharing them with other people and selecting easily guessed words. Research has shown that users are considered to be one of the main risks to the effectiveness of security measures designed to counter information system threats (Rhodes, 2001; Aytes and Connelly, 2004).

Individuals are particularly vulnerable to security threats as many do not have adequate knowledge to recognise the risks in the first instance nor to implement appropriate protection mechanisms in the second instance. This study focuses on password issues by examining behaviours exhibited by user when creating and managing passwords. The aim of this study is to assess the attitudes and awareness of users to password security issues, and to gain insight into password composition, reuse, and management practices. This paper outlines the major problems associated with password-based authentication systems. Computer security issues associated with passwords are discussed in the following section.

SECURITY ISSUES ASSOCIATED WITH PASSWORDS

The password-based approach to user authentication has a number of shortcomings that can undermine the efficacy of computer system security (see for example Jobusch and Oldehoeft 1989, Furnell et al. 1999, Conklin et al. 2004, Carstens 2004, Ives et al. 2004). There are many different methods used to compromise password security, some of which are unsophisticated requiring little or no technical knowledge while others require a high level of technical expertise. Unsophisticated techniques include guessing, observing, viewing written records, being told, tricks and artifice and even sifting through rubbish bins. Other methods that require a high level of expertise include keyboard monitoring, packet interception, keystroke interception, host emulation and so on.

Several studies have examined the ease with which passwords can be determined or ‘cracked’. In one of the earliest empirical studies, Morris and Thompson (1979) found that a personal computer could guess 86 percent of passwords in less than one week. Subsequent replications of the study by Klein (1990) and Spafford (1992) found that password selection had improved over time with only 21 percent being guessed in a week. Unfortunately, the software tools that can deduce passwords have become even more powerful and seditious in recent years. A modern program designed to crack passwords by brute force can discover a randomly generated 5-character alphabetic password in less than two seconds and an 8-character one in a little under ten hours (Keith et al 2006). However, one saving grace is that longer passwords take longer to discover. Notwithstanding this, if the password is commonly used or is a dictionary word, the time taken to discover it by brute force attack is significantly reduced (Keith et al 2006).

Many researchers have suggested various strategies to overcome the threat of software to break passwords. The focus has been placed on various algorithms for encryption (Bishop and Klein 1995; Liao et al 2006), the use of biometrics (Walton 2005, Jain 2004; Ratha 2001) and graphics (Man et al. 2004 and Wiedenbeck et al. 2005). Researchers have also been recommending strategies to overcome inherent limitations in password systems, most focused on the user (Bishop and Klein 1995). The major strategies for overcoming the inherent weaknesses in password usage include the following:

- Password lengths of at least 8 characters: longer passwords increase the time taken by software cracking programs to determine it.
- Passwords with mixed case/symbols: Including both upper/lower case and symbols (!£$% etc.) in passwords requires attacks to use brute force methods and increases the number of character permutations that must be tried.
- Non-Dictionary words: selecting non-dictionary passwords prevents the use of dictionary-based attacks. Such attacks can identify a password in less than 20 minutes even on dictionaries with up to one million words. The only way to identify non-dictionary passwords is using a brute-force approach (testing every combination of characters for every length of password).
- Password ageing: Should an intruder obtain a valid password, most systems will allow them to continue to access the system until the intrusion is noticed. Users need to change their passwords regularly, thus forcing the intruder to identify the new password.

While these strategies may help improve password security, these restrictions make the composition and memorizing of passwords a complex and unintuitive exercise. The rapid proliferation of electronic commerce and other public access systems requires users to manage a large number of passwords on a day-to-day basis. Unfortunately, typical users are capable of managing a relatively small number of passwords – typically less than five unique passwords (Adams and Sasse, 1999). Consequently, users may be tempted to reuse passwords to access multiple systems. The analysis of data collected from a survey of 884 computer users reveals some interesting characteristics surrounding user practices in creating and maintaining passwords.

A SURVEY OF EMAIL PASSWORD SECURITY

Password reuse can compromise the security of all of the password systems that a user might access. Cognitive limitations mean that many users will choose passwords that are easy to remember; typically these passwords are based on some meaningful combination of names and/or numbers (Bishop and Klien, 1995; Brown et al 2004). If the security of one system is breached, then all other password-based systems and other computing assets might become vulnerable to unauthorised access and malicious damage. For example, a list of usernames and passwords gained from one system might then be used in brute-force attacks on other password-protected systems. Many systems protect against brute-force attacks by restricting the number of unsuccessful logon attempts before denying further access. However, this type of control offers no protection from brute-force attacks that use datasets of different username and password combinations.

Electronic mail (email) is universally the most widely adopted password-protected application and affects the daily life of almost every working person in the industrialized world (Rudy 1996, Bälter 2000). It was concluded that email systems would prove a useful application domain to use as a research context because of its importance and widespread social and organisational impact. The aim of this study was to assess the attitudes and awareness of users to password security issues, and to gain insight into password composition and management practice. A copy of the survey instrument is contained in the Appendix. The first section of the questionnaire collected demographic data about the participants and their computer and email usage. It also sought to ascertain the extent to which participants shared passwords across applications and their awareness of password cracking techniques. The second section focused specifically on password composition and management practices.

Study Data

Undergraduate level students from an Australian university business faculty were chosen to be the research participants. This sample can be considered as representing practicing, non-specialist computer users whose typical password security behaviours are indicative of those that potential employees might be expected to bring with them into organisations. The survey was administered across three campuses located in close proximity to one another (that is, no two campuses are more than 50 miles apart). All of the students surveyed were in the Business School and in their first year of study. Participation in the survey was entirely voluntary. In all, 884 students volunteered to participate in this study. Table 1 shows the relevant demographic details for the participants.

There were marginally more males than females in the sample[1]. The majority of the participants were under 26 years of age; 213 participants were under 18 and 584 between 18 and 25. The remaining 87 participants were mature aged (greater than 25 years of age). Most of the participants were enrolled at the University on a full time basis (811) and 59 were enrolled on a part-time basis.

[1] On one of the campuses sampled offered programs that typically attract a higher proportion of female students. Therefore, it was not surprising that there were significantly more female participants than males from this particular campus. Subsequently, tests were conducted across all of the study variables for introduced bias. These tests revealed that this phenomenon had no significant impact on any of the findings reported here.

Thirteen participants did not respond to this question and one participant was auditing the course and therefore was not formally enrolled. Similarly, most of the participants were either not employed (257) or employed on a part-time basis (533). Sixty-five were full-time employees, while 29 participants did not respond to this question. The majority of participants had used computers for more than 5 years; 480 had used computers between 6-10 years and 252 for longer than 10 years. Only 25 participants had used computers for less than 2 years, while 126 had used computers between 3 and 5 years. One participant did not respond to this question.

Variable	**Category**	**Total**	**% ***
Gender	Male	378	42.8%
	Female	505	57.1%
	No response	1	0.1%
Age	< 18 years	213	24.1%
	18 – 25 years	584	66.1%
	26 – 35 years	55	6.2%
	36 years +	32	3.6%
Enrolment Status	Full-time	811	91.7%
	Part-time	59	6.7%
	Not enrolled	1	0.1%
	No response	13	1.5%
Employment Status	Full-time	65	7.4%
	Part-time	533	60.3%
	Not employed	257	29.1%
	No response	29	3.3%
Computing Experience	0 – 2 years	25	2.8%
	3 – 5 years	126	14.3%
	6 – 10 years	480	54.3%
	> 10 years	252	28.5%
	No response	1	0.1%
	Total Participants:	884	100.0%

* Percentage totals may exceed 100% due to rounding.

Table 1: Demographic Details of Participants

Analysis

Participants were asked to indicate for what purposes they used computers; selecting as many options as was relevant. More than 83% of participants indicated their main use was for Internet (92.9%), email (90%) and home use (83.4%). Banking (50.2%) and work use (47.7%) formed a second grouping and other areas of use (e.g. study and research; entertainment including games; and online purchasing and selling) accounted for 15.0%.

Participants were also asked to indicate what their email usage was. Personal email use was most prevalent (95.5%), followed by University use (84.7%) and Work-related use (24.9%). The majority of participants had either two or three email accounts; 49.4% had two and 27.9% had three. The remaining participants had either one account (11.7%), or they had four or more email accounts (11.0%). Almost half of the participants accessed their email at least once a day, with another 27.7% accessing several times a week. Sixty-one participants did not answer question. Given that more than 95% percent of participants reported that they used email for personal communication, serious implications for organisational security are raised, especially if users reuse passwords across email and other computer applications. This is because password reuse and poor security practices increase the likelihood that a password might be deduced thereby increasing the vulnerability of other systems where this password had been used.

Participants were then asked questions concerning the composition and choice of passwords – see Table 2a and b. The average length of a password was 8.3 characters, and ranged between 1 and 25 characters. The majority of participants had passwords of greater than 5 characters in length. Participants typically used 8 characters in their password (29.2%), and 7.4% of participants had passwords exceeding 11 characters. Approximately 39.4% used only alphabetic characters in their passwords, while 42.3% used alphanumeric characters. The remainder either used numerals only (6.4%); added symbols (4.1%); or did not respond to the question (7.5%). Typically, their choice of password contained meaningful data (43.1%) such as a name, street, preferred word, nickname, registration number and so on. A few selected pronounceable words (5.2%). Another 23.8% combined meaningful data items to make up their passwords. Only 10.7% choose a random combination of characters. Very few participants had their passwords chosen for them (1.6%), while another 8% selected their password by some other means. There were 61.9% of participants who never changed their password and a further 19.8% who changed it no more than three times a year. Participants were divided with respect to admitting whether they had forgotten their password – 60.9% said they had not forgotten it compared to 30.4% who had; 8.7% chose not to answer this question.

Variable & Category	**Total**	**% ^**
Password Length		
1-5 characters	31	3.5
6 characters	126	14.3
7 characters	93	10.5
8 characters	258	29.2
9 characters	104	11.8
10 characters	68	7.7
11 characters	34	3.8
> 11 and <26 characters	65	7.4
No response	105	11.9
Password Composition		
1. Alphabetic only	348	39.4
2. Numeric only	57	6.4
3. Alphanumeric	374	42.3
4. Includes symbols	36	4.1
5. Other	3	0.3
No response	66	7.5
Choice of Password		
1. Meaningful data	381	43.1
2. Combo meaningful data	210	23.8
3. Pronounceable word	46	5.2
4. Random characters	95	10.7
5. Not self-chosen	14	1.6
6. Other	71	8.0
No response	67	7.6
Frequency of Changing Password		
1.Never	547	61.9
2. Less than once a year	119	13.5
3. 1-3 times a year	56	6.3
4. 4-6 times a year	79	8.9
5. Once a month	10	1.1
6. Several times a month	6	0.7
Did not respond	67	13.5
Forgotten Password		
1. Yes	538	60.9
2. No	269	30.4
Did not respond	77	8.7

^ Percentage totals may exceed 100% due to rounding.

Table 2a: Participant Practices Relating to Password Composition and Management

Since the survey data is categorical, nonparametric statistics were employed in analysing the data across three variables: gender, age and employment status. Table 2b provides details of the results of the nonparametric analysis conducted on participant practices related to password composition and management. The results from the analysis on the number of characters in a password have not been reported, as there were no significant findings for any of the independent variables. There were significant differences in the type of characters used in the composition of passwords for all independent variables; employment status and age group at the 1% level, while gender was significant at the 5% level. Females are more likely to choose alphabetic or numeric characters only, while males will choose a combination of characters, including symbols. Full-time employees and those who are unemployed tend toward combination of characters while those who are employed on a part-time basis are more likely to choose alphabetic or numeric characters only. With respect to age group, participants aged 25 years and under are more likely to choose alphabetic or numeric characters only, while the older participants will choose alphanumeric combinations that may include symbols. There is a significant difference in the method of choosing passwords for gender only. Females are more likely to choose more meaningful detail or some combination thereof, while males tend towards pronounceable passwords or a random combination of characters. The frequency of changing passwords was only significant for age groups. Older participants are likely to change their passwords more often than those who are younger. There was only a significant difference in whether the participant had forgotten their passwords for age group. It appears that the older the participant, the more likely they are to forget their passwords.

Password composition				
	Groups	*Count*	*Mean Rank*	*P-value*
Gender	Male	346	430.54	0.014
	Female	470	393.10	***NS***
Age Groups	Under 18yrs	202	347.91	0.000
	18-25yrs	541	418.05	
	26-35yrs	48	515.03	
	36 and over	26	524.91	
Employment	Full/Time	63	413.23	0.004
	Part/Time	499	378.03	
	Not Employed	230	432.00	

Choice of password				
	Groups	*Count*	*Mean Rank*	*P-value*
Gender	Male	346	438.36	0.001
	Female	470	386.52	
Age Groups	Under 18yrs	202	393.46	0.290 ***NS***
	18-25yrs	541	412.32	
	26-35yrs	48	389.48	
	36 and over	26	530.12	
Employment	Full/Time	62	388.98	0.761 ***NS***
	Part/Time	497	399.82	
	Not Employed	231	387.96	

Frequency of changing password				
	Groups	*Count*	*Mean Rank*	*P-value*
Gender	Male	347	412.77	0.593
	Female	469	405.34	***NS***
Age Groups	Under 18yrs	201	383.33	0.042 ***NS***
	18-25yrs	541	410.73	
	26-35yrs	49	470.46	
	36 and over	26	402.91	
Employment	Full/Time	62	433.20	0.204 ***NS***
	Part/Time	497	388.80	
	Not Employed	231	399.79	

Forgotten password				
	Groups	*Count*	*Mean Rank*	*P-value*
Gender	Male Female	339 467	391.45 412.25	0.125 ***NS***
Age Groups	Under 18yrs 18-25yrs 26-35yrs 36 and over	200 534 48 25	374.41 404.00 471.25 488.92	0.002
Employment	Full/Time Part/Time Not Employed	61 492 229	383.29 386.07 405.63	0.383 ***NS***

NS = Not Significant p > 0.01

Table 2b: Results of Non-Parametric Analyses of Number of Password

Composition and Management

Table 3a and 3b provide relevant details about password reuse; specifically those passwords associated with email accounts and other computer applications. Over half of participants used the same password (24.9%) or a slight variation of that password (31.2%). More than one-third used passwords that were very different (36.3%). Sixty-seven participants (7.6%) did not answer this question. The participants were also asked whether they used other applications that required the use of passwords. Approximately 60% of participants use passwords for other applications. There were three predominant groups: (1) banking, (2) other University applications and (3) communication applications such as chat rooms, messenger services and forums. When asked whether they reused the same passwords across other applications, 37.5% reported using the same password (17.4%) or a slight variation (20.1%). Approximately 40% of participants did not answer this question.

Variable & Category	**Total**	**%**
Password Reuse Across Email Accounts		
1. Same password	220	24.9
2. Slightly different	276	31.2
3. No similarities	321	36.3
No response	67	7.6
Password Reuse Across Other Applications		
1 Same password	154	17.4
2. Slightly different	178	20.1
3. No similarities	194	21.9
No response	358	40.5

Percentages have been calculated in terms of the total number of participants.

Table 3a: Participant Practices Related to Password Reuse

Password reuse across email accounts				
Gender	*Groups*	*Count*	*Mean Rank*	*P-value*
	Male	349	391.98	0.065
	Female	467	420.85	***NS***
Age Groups	Under 18yrs	198	396.39	
	18-25yrs	541	412.50	0.905
	26-35yrs	51	418.20	***NS***
	36 and over	27	423.40	
Employment	Full/Time	61	465.02	0.005
	Part/Time	490	399.72	
	Not Employed	238	367.34	
Password reuse across other applications				
Gender	*Groups*	*Count*	*Mean Rank*	*P-value*
	Male	227	259.79	0.653
	Female	298	265.44	***NS***
Age Groups	Under 18yrs	116	247.19	
	18-25yrs	344	261.87	0.178
	26-35yrs	43	286.15	***NS***
	36 and over	23	315.39	
Employment	Full/Time	49	303.49	0.039
	Part/Time	325	249.85	***NS***
	Not Employed	152	251.71	

NS = Not Significant p > 0.01

Table 3b: Results of Nonparametric Analyses of Password Reuse

Password reuse was tested using nonparametric analyses with gender, age group and employment status as independent variables. Table 3b shows that there is no significant difference in reusing passwords across email accounts that is associated with age. However, there is a significant difference with respect to employment status (at 1% level). Full-time employees have the least similarity, while unemployed participants have the most. There is only a significant difference due to gender at the 10% level, where females are more likely to have less similar passwords than males. With respect to sharing passwords across other computer applications, there is no difference due to gender and age group. There is a significant difference due to employment (5% level). Full-time employees are more likely to have less similar passwords for other computer applications than part-time employees or the unemployed.

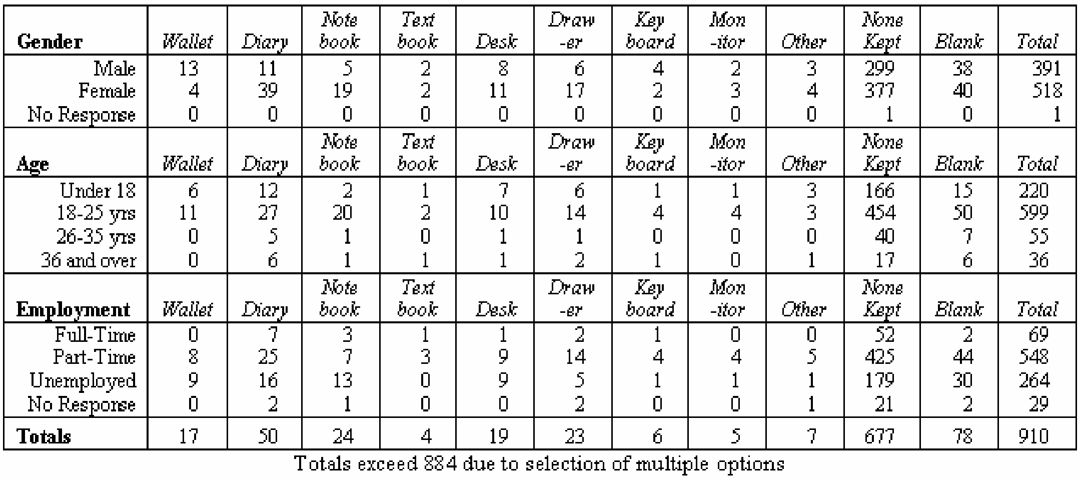
Gender	*No One*	*Sib-ling*	*Parent*	*Partner/ Spouse*	*Other Relative*	*Close Friend*	*Collea-gue*	*Other*	*Blank*	*Total*
Male	242	26	12	41	6	36	4	4	34	405
Female	271	47	24	93	6	75	7	6	37	566
No Response	0	1	0	0	0	0	0	0	0	1
Age										
Under 18	122	12	9	21	2	45	4	5	12	232
18-25 yrs	338	58	26	94	8	65	6	4	47	646
26-35 yrs	34	3	1	12	1	1	1	1	6	60
36 and over	19	1	0	7	1	0	0	0	6	34
Employment										
Full-Time	39	6	3	15	1	4	1	1	3	73
Part-Time	295	48	25	82	5	82	6	6	39	588
Unemployed	164	17	7	33	6	21	3	2	27	280
No Response	15	3	1	4	0	4	1	1	2	31
Totals	513	74	36	134	12	111	11	10	71	972

Totals exceed 884 due to selection of multiple options

Table 4a: Participant Practices Related to Password Sharing

Participants were also asked to indicate their personal practices related to sharing passwords and whether or not they kept written or electronic copies of their passwords. Participants were asked to select as many options as were relevant to them. Tables 4a, 4b and 4c show the results across the variables of interest, namely, gender, age and employment status. These outcomes are very promising. Table 4a shows that over half of the participants (52.78%) reported that they did not share their passwords with others, and another 7.3% of participants did not respond to this question. The tendency to not share their password was very similar for males (24.90%) and females (27.88%). Within the Age and Employment groups, 18-25 year olds (34.77%) and part-time employees (30.35%) respectively, were the ones least likely to share their passwords. For those who did report sharing their password, spouses or partners (13.79%) was the preferred choice followed by close friends (11.24%) and siblings (7.61%).

Table 4b reports on whether participants kept a handwritten record of their password. Nearly three-quarters (74.4%) of participants did not, while 8.57% did not respond to this question. Females (41.43%) were less likely to keep handwritten records than males (32.86%). The 18-25 year old group (49.89%) and part-time employees (46.70%) were also less likely to keep handwritten records. For those who did report keeping a handwritten copy of their password, diaries (5.49%) was the preferred choice. Other choices included notebooks (2.64%), drawers (2.53%) and desks (2.09%).

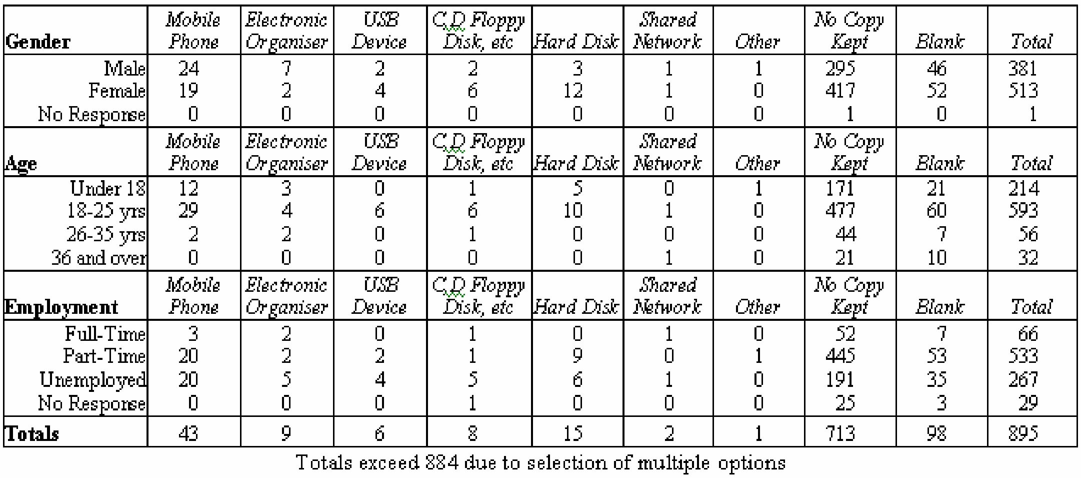


Gender	Wallet	Diary	Note book	Text book	Desk	Draw-er	Key board	Mon-itor	Other	None Kept	Blank	Total
Male	13	11	5	2	8	6	4	2	3	299	38	391
Female	4	39	19	2	11	17	2	3	4	377	40	518
No Response	0	0	0	0	0	0	0	0	0	1	0	1
Age	Wallet	Diary	Note book	Text book	Desk	Draw-er	Key board	Mon-itor	Other	None Kept	Blank	Total
Under 18	6	12	2	1	7	6	1	1	3	166	15	220
18-25 yrs	11	27	20	2	10	14	4	4	3	454	50	599
26-35 yrs	0	5	1	0	1	1	0	0	0	40	7	55
36 and over	0	6	1	1	1	2	1	0	1	17	6	36
Employment	Wallet	Diary	Note book	Text book	Desk	Draw-er	Key board	Mon-itor	Other	None Kept	Blank	Total
Full-Time	0	7	3	1	1	2	1	0	0	52	2	69
Part-Time	8	25	7	3	9	14	4	4	5	425	44	548
Unemployed	9	16	13	0	9	5	1	1	1	179	30	264
No Response	0	2	1	0	0	2	0	0	1	21	2	29
Totals	17	50	24	4	19	23	6	5	7	677	78	910

Totals exceed 884 due to selection of multiple options

Table 4b: Participant Practices Related to Handwritten Records of Passwords

Similar results were apparent for participants reporting on whether they kept an electronic copy of their password (Table 4c). Nearly 80% of participants did not keep an electronic record, but 10.95% did not respond to this question. As with handwritten copies, females (46.59%) were less likely to keep and electronic record than males (32.96%). Similar results are also apparent with Age and Employment groups; 18-25 year olds (53.30%) and part-time employees (49.72%) reported not keeping electronic records. The mobile phone (4.80%) was the option of choice for those who did keep an electronic copy. Overall, 640 participants (72.40%) did not keep any kind of record of their passwords, while 8.14% did not answer either question. A few of the participants did not keep an electronic copy but kept a handwritten copy in their wallet (4.07%), a drawer (1.81%) or in their desk (1.13%). Others had no handwritten record but kept a copy on their mobile phone (2.38%), while another 24 participants (2.71%) did not indicate whether they kept an electronic record.



Gender	Mobile Phone	Electronic Organiser	USB Device	C,D Floppy Disk, etc	Hard Disk	Shared Network	Other	No Copy Kept	Blank	Total
Male	24	7	2	2	3	1	1	295	46	381
Female	19	2	4	6	12	1	0	417	52	513
No Response	0	0	0	0	0	0	0	1	0	1
Age	Mobile Phone	Electronic Organiser	USB Device	C,D Floppy Disk, etc	Hard Disk	Shared Network	Other	No Copy Kept	Blank	Total
Under 18	12	3	0	1	5	0	1	171	21	214
18-25 yrs	29	4	6	6	10	1	0	477	60	593
26-35 yrs	2	2	0	1	0	0	0	44	7	56
36 and over	0	0	0	0	0	1	0	21	10	32
Employment	Mobile Phone	Electronic Organiser	USB Device	C,D Floppy Disk, etc	Hard Disk	Shared Network	Other	No Copy Kept	Blank	Total
Full-Time	3	2	0	1	0	1	0	52	7	66
Part-Time	20	2	2	1	9	0	1	445	53	533
Unemployed	20	5	4	5	6	1	0	191	35	267
No Response	0	0	0	1	0	0	0	25	3	29
Totals	43	9	6	8	15	2	1	713	98	895

Totals exceed 884 due to selection of multiple options

Table 4c: Participant Practices Related to Electronic Records of Passwords

Participants were also asked whether they were familiar with password cracking techniques. Again, participants were asked to select as many options as were relevant to them. Details organised by gender, age and employment status are shown in Table 5. Table 5: Participant Practices Related to Electronic Records of Passwords

Gender	*Not Aware*	*Worm*	*Virus*	*Program File*	*Other*	*Blank*	*Total*
Male	4	192	235	147	36	96	710
Female	6	161	292	103	2	155	719
No Response	0	1	1	1	1	0	4
Age	*Not Aware*	*Worm*	*Virus*	*Program File*	*Other*	*Blank*	*Total*
Under 18	3	85	131	65	10	65	359
18-25 yrs	5	236	350	163	26	157	937
26-35 yrs	0	20	29	15	2	19	85
36 and over	2	13	18	8	1	10	52
Employment	*Not Aware*	*Worm*	*Virus*	*Program File*	*Other*	*Blank*	*Total*
Full-Time	1	33	38	21	3	18	114
Part-Time	3	208	329	152	25	153	870
Unemployed	4	102	145	69	2	73	395
No Response	2	11	16	9	9	7	54
Totals	10	354	528	251	39	251	1433

Totals exceed 884 due to selection of multiple options

Table 4c: Participant Practices Related to Electronic Records of Passwords

The data show that the majority of participants (81.79%) are familiar with at least one technique for cracking passwords. Only 10 participants (0.70%) reported not being aware of any such techniques, while 17.52% did not respond to the question. The technique selected most often by participants was viruses (36.85%), followed by worms (24.70%), program files (17.52%) and other techniques (2.72%). There was very little difference between awareness of females (50.17%) compared to males (49.55%). As was the case with sharing passwords and keeping records of passwords, the 18-25 year old group (65.39%) were more aware than other Age group categories, while those employed part-time (60.71%) were most aware for the Employment Status group. Lastly, participants were asked whether they had changed their password because they believed someone else had had discovered it. The majority of participants responded in the negative (585 or 66.18%), 228 (25.34%) said they had and 75 (8.48%) did not respond to this question.

DISCUSSION

Email accounts are heavily used with approximately 30% of participants checking their email several times a week and a further 50% who check one or more times a day (Table 2). What is concerning, is the reuse of the exact or similar passwords for different email accounts and other applications (Table 3). Many of the participants responding to these two questions used the exact same password or had passwords with a slight variation. One promising factor was that half of the passwords contained a combination of alphabetic, numerical and symbol characters and was on average 8 characters in length. Another positive fact was that password length ranged between six and 25 characters (Table 2) with 60% of participants having passwords of eight or more characters in length. Password of this length increase the time taken for password detection software to determine them. However, while these results are positive, the fact that almost three-quarters of the passwords contained meaningful detail, a combination of meaningful details or pronounceable words reduces its impact. This implies the passwords are easier to guess, especially by those who have even a modicum of personal knowledge about the user. A serious lack of concern with password security is indicated when this outcome is coupled with the fact that over three-quarters of the participants, never changed their password or changed it no more than three times a year. This finding is similar to that of the Aytes and Connelly (2004) study who found that participants rarely, if ever, changed their passwords voluntarily.

It appears that while most participants have some rudimentary knowledge of good password practices, for example, password lengths of 8 or more characters, this is as far as the participants were prepared to go to secure their passwords. The extent of password reuse is an issue that organisations appear to be addressing, given that full-time employees are less likely to reuse passwords than unemployed or part-time employees. In an attempt to increase security, organisations may be taking the necessary security measures. Nonetheless, it would appear that without the influence of full-time work environment, participants are either not sufficiently informed of the risks they are facing through poor password practices or they do not believe that they are at risk even though most are aware of one or more of the techniques used to break passwords.

It also appears that age is a contributing factor to poor password practices. Younger participants are more likely to have simplistic passwords; that is, those derived using alphabetic and numeric characters. Further, they don't change their password as frequently as older participants, but they are also are less likely to forget their password. This finding may simply be due to the fact that younger participants change their password less frequently so familiarity has an impact. In addition, they do not have to remember complex passwords. It would appear that the younger generation is more in need of education programs. Gender differences seem to balance the various behaviours. Both males and females have poor practices, although in different areas. Females are more likely to have simplistic passwords that are meaningful, but they also are less likely to reuse them. Males, on the other hand, have pronounceable words using combinations or symbols and characters but are more likely to reuse them. Neither situation is ideal, so it can be concluded that both females and males have equally poor practices when it comes to password management.

Overall, participants appear to be unconcerned about the risks associated with poor password composition and management practices. This outcome is of concern, given that over 82% of the participants can be considered as experienced computer users since they had been using computers for six or more years. It would appear there is a need for a better education process on password composition and management for users. The education process should also focus on the risks of not having appropriate password practices and what the consequences are for failure to adhere to such practices.

This issue of who should provide this education is one yet to be investigated. Governments are a likely provider especially since the youngest and the older participants have been shown to have weakest password practices. Education can take the form of information provided online, but many older members of the community do not have access to the Internet. Newsletters are another alternative, but this approach relies on the user reading and understanding the information it contains. Information sessions can be held, but again not all users would be able to or even willing to attend. This option would be the most expensive one and thus least likely to be adopted by governments. A tutorial available on CD, DVD or online is another strategy that could be used to educate users. This technique has been used with some degree of success (Gips, 2001). Gips reported that the product delivered awareness messages to users via animation and graphics on screensavers. Further, Gips reported that while user awareness increased, it was necessary to change the screensaver regularly so they did not become bored with the message it was portraying. While animated tutorials may be expensive to develop initially, provided they are set up using the latest information and rules for designing strong passwords – ones difficult to crack – means the product can be used for some time and so reduce the overall cost involved. Such a product could be provided free online or sent on CD or DVD to households.

Education could also be provided as part of study programs. Tertiary institutions can provide information on good password practices during a student's first year of study. However, given the results of this study, tertiary education is perhaps too late. Since children are using computers and accessing the Internet from an early age, primary schools may be the best option for providing education on password composition and related behaviours. Good practices can be developed from the outset of the child's use of computers rather than trying to correct bad habits some years later. Video clips, animated tutorials or games would most likely hold the child's attention better than printed sheets of information or formal classes. Teachers can introduce the learning material and allow the children's skills to develop over time. These types of activities could be extended into their secondary education. Follow-up 'lessons' can be part of the curriculum for all students undertaking secondary education. Equivalent classes can be established for the adult learner at TAFE colleges, adult education classes and even provided through local libraries.

Software vendors are another likely provider of this educational material. Vendors who supply relevant software such as operating systems, firewalls and other security software, email systems and such like, could also build in tutorials or rule sets for constructing and maintaining passwords. These components should be an integral part of the software suite and not considered as an add-on. Further they should, by default, be active in the application ready for when the user needs to change their password. As a user creates their password, rule sets can be provided so they can better understand what they are required to do and why. The strength of the created password can be assessed and, if it does not reach a predetermined level, the password can be rejected. Feedback is provided to the user so they fully understand why their selected password was a security risk. Rewards can be provided to those users who create strong passwords on their first attempt. The rewards need not have a high monetary value; they can be a straightforward as officially recognising appropriate behaviours. Rewarding positive and desired behaviours is more likely to achieve results than negative or fear-based strategies.

These are a few strategies for providing users with appropriate information to develop good password practices and security awareness. All of these strategies have merit, so some combination of them would provide the broadest possible coverage to the general public. Organisations and businesses can also take a role in reinforcing this knowledge, rather than assuming their employees are aware of the risks of poor password behaviours. Simply educating their employees on the reasons why security and password practices have been implemented rather than keeping them ignorant due to misguided sense of "the need to know" can move users towards adopting good password and security practices. One organisation reported punishing its employees for poor security behaviours by requiring them to attend extremely mind-numbing courses on good password practices (Tuesday, 2001). The punishment for continued poor practices was attendance at even longer mind-numbing courses.

CONCLUSION

The aim of this study was to assess the attitudes and awareness of users to password security issues, and to gain some insight into password composition, reuse, and management practice. This study explored aspects of user password management practice within the context of email usage by profiling email account usage and password reuse and management practice. The results from this study provide important insight into ongoing issues relating to the creation and management of user-based password management systems. The poor practices evidenced in the survey results support our initial focus on email account management as an important end-user application context. Participants typically operate two or more email accounts as well as a host of other computer-based applications that require the use of passwords. As anticipated, this created password management difficulties for users and encouraged password reuse across different email accounts, and/or other computer-based applications. Further, users do not appear to fully realise the risks of their poor password practices, nor are they aware of many of the consequences associated with breaches in security.

The poor password composition practices adopted by many of the participants clearly highlight this problem. Our results show that the vast majority of users are choosing passwords that are based on meaningful personal details that can be more readily guessed by others. It does appear that being a full-time employee is a mitigating factor, but this is more likely due organisational security requirements rather than better personal practices by these employees. However, further research is needed to fully explore this finding. Younger participants appear to have the worst practices in terms of password management and so are the most at risk. Any educational programmes should be targeted towards this group in the first instance. These programmes should highlight the risks of such poor practices in terms younger people can relate to. Several options for providers of this education have been suggested including governments, educational institutions and software vendors. Some combination of all options would provide the broadest possible coverage.

While there have been significant technological developments in online authentication methods, user behaviours associated with password practices is an area that remains under researched. The results of this expanded study show that on the whole, the majority of users do not adopt secure management practices. This in turn exposes them, the organisations for which they work and their service providers, to higher levels of risk and potential breaches in security. Future research needs to build upon this understanding and aim to gain further insight into how user practices can be improved. The research can build on this study's findings to determine the underlying reasons why younger people tend to have the poorest password practices. It would be useful to discover at what point these practices were established and determine if early intervention during secondary or even primary school would have payoffs. Further research could also be targeted towards full-time and part-time employees in order to examine whether it is organisational requirements that is driving their password practices. Any research within organisations should also discover whether security requirements actually interfere with the functions employees are required to undertake as part of their jobs. Such interference may be a factor in explaining why poor security behaviours are still being practiced. Any knowledge gained from such research can then be used as a basis for sound educational programs that focus on improving personal password practices as well as helping the organisation understand why users seek to circumvent security measures.

REFERENCES

Adams, A. & Sasse, M.A. (1999) "Users Are Not the Enemy", Communications of the ACM, Vol 42 No 12, pp 41-46.

Aytes, K. & Connolly, T. (2004) "Computer Security and Risky Computer Practices: A Rational Choice Perspective”, Journal of Organisational and End-User Computing, Vol 16 No 3, pp 22-41.

Bälter, O. (2000) "How to Replace an Old Email System with a New", Interacting with Computers, Vol 12 No 6, pp 601-614.

Bishop, M. & Klein, D.V. (1995) "Improving System Security via Proactive Password Checking" Computers & Security, Vol 14 No 3, pp 233-249.

Brown, A.S., Bracken, E., Zoccoli, S. & Douglas, K. (2004) "Generating and Remembering Passwords", Applied Cognitive Psychology, Vol 18, pp 641-651.

Carstens, D.S., McCauley-Bell, P., Malone, L.C. & DeMara, R.F. (2004) "Evaluation of the Human Impact of Password Authentication Practices on Information Security", Informing Science Journal, Vol 7 No 1, pp 67 – 85.

Conklin, A., Dietrich, G. & Walz, D. (2004) "Password-Based Authentication: A System Perspective", Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii.

De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D.F., Ren, J., Rode, J.A. & Filho, R.S. (2005) "In The Eye of The Beholder: A Visualization-Based Approach to Information System Security", International Journal of Human Computer Studies, Vol 63 No 1-2, pp 5-24.

Furnell, S.M., Dowland, P.S., Illingworth, H.M. & Reynolds, P.L. (2000) "Authentication and Supervision: A Survey of User Attitudes", Computers & Security, Vol 19 No 6, pp 529-539.

Gips, M.A. (2001) "Plugging Into Awareness", Security Management, Vol 45 No 11, pp 21-22.

Ives, B., Walsh, K.R. & Schneider, H. (2004) "The Domino Effect of Password Reuse", Communications of the ACM Vol 47 No 4, pp 75-78.

Jobusch, D.L. & Oldehoeft, A.E. (1989) "A Survey of Password Mechanisms: Part 1", Computers & Security, Vol 8 No 7, pp 587-604.

Jain, A.K., Ross, A. & Prabhakar, S. (2004) "An introduction to biometric Recognition", IEEE Transactions Circuits Systems Video Technology, Vol 14 No 1, pp 4–20.

Keith, M., Shao, B. & Steinhardt, P.J. (2006) "The Usability of Passphrases for Authentication: An Empirical Study", International Journal of Human-Computer Studies, forthcoming.

Klein, D. (1990) "A Survey of, and Improvements to, Password Security", Proceedings of the USENIX Second Security Workshop, Portland, Oregon, August 1990: pp 5-14.

Liao, I.E., Lee, C.C. & Hwang, M.S. (2006) "A Password Authentication Scheme over Insecure Networks", Journal of Computer and System Sciences, Vol 72 No 4, pp 727-740.

Man, S., Hong, D., Hayes, B. & Matthews, M. (2004) "A Password Scheme Strongly Resistant to Spyware", Proceedings International Conference on Security and Management, Las Vegas, pp 94-100.

Morris, R. & Thompson, K. (1979) "Password Security: A Case History", Communications of the ACM, Vol 22 No 11, pp 594-577.

Oppliger, R. (1997) "Internet Security: Firewalls and Beyond", Communications of the ACM, Vol 40 No 5, pp 92-105.

Ratha, N.K, Connell, J.H. & Bolle, R.M. (2001) "Enhancing Security and Privacy in Biometrics-Based Authentication Systems", IBM Systems Journal, Vol 40 No 3, pp 614-634.

Rhodes, K. (2004) "Operations Security Awareness: The Mind Has No Firewall", Computer Security Journal, Vol 16 No 2: pp 27-36.

Rudy, I.A. (1996) "A Critical Review on Research on Electronic Mail", European Journal of Information Systems, Vol 4, pp 198-213.

Sherman, R. (1992) "Biometrics Futures", Computers & Security, Vol 11 No 2, pp 128-133.

Spafford, E.H. (1992) "Opus: Preventing Weak Password Choices", Computers & Security, Vol 11 No 3, pp 273-278.

Tuesday, V. (2001) "Human Factor Derails Best-Laid Security Plans", Computerworld, Vol 35 No 18, p 52.

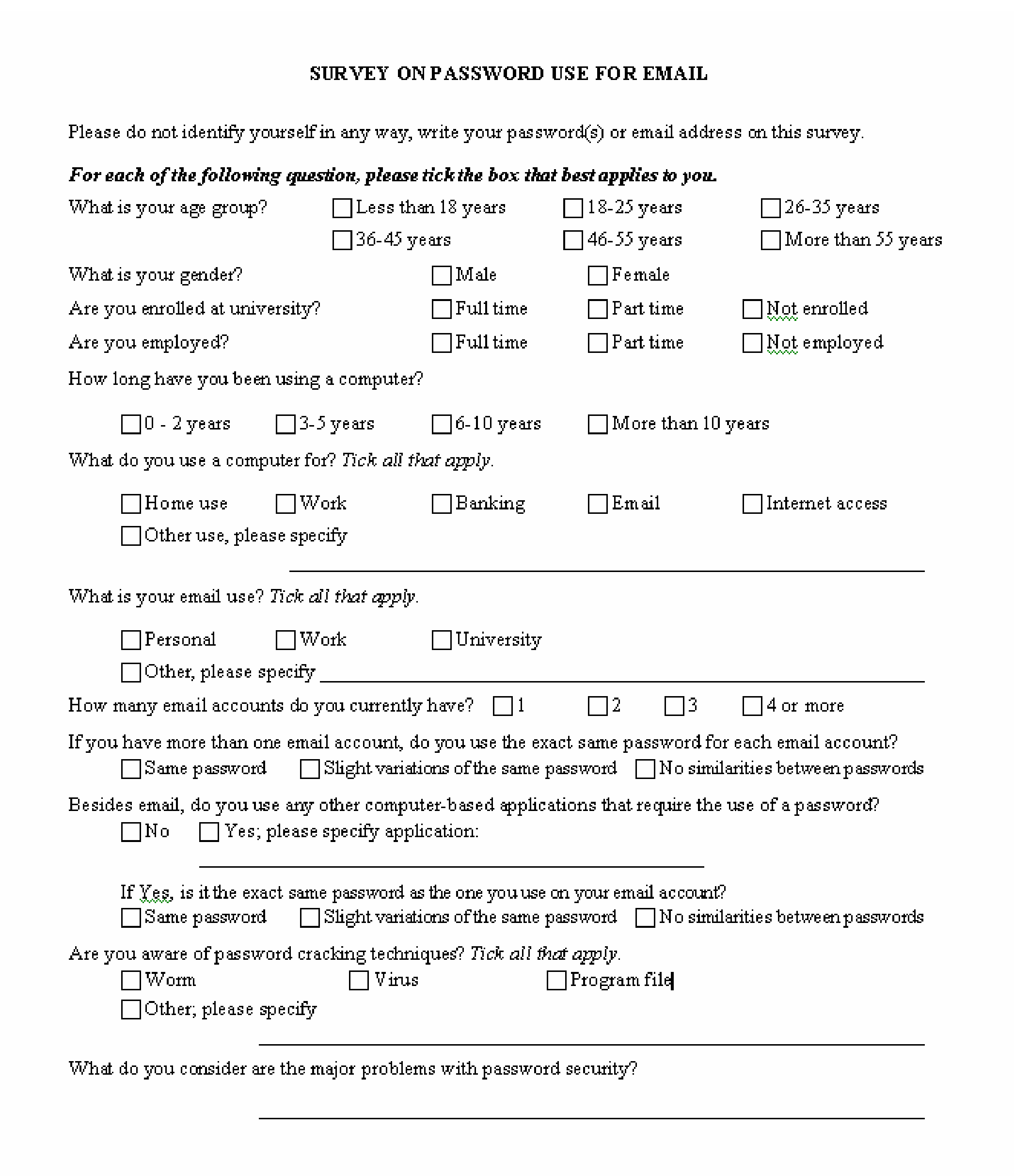
Walton, R.W. (2005) "Combining Biometric Measurements for Security Applications", Computer Fraud & Security, Vol 4, pp 7-13.

Weber, R. (1999) *Information Systems Control and Audit*, Prentice-Hall, Upper Saddle River, NJ.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. & Memon, N. (2005) "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, Vol 63 No 1-2, pp 102-127.

Zviran, M. & Haga, W.J. (1999) "Password Security: An Empirical Study", Journal of Management Information Systems, Vol 15 No 4, pp 161-185.

APPENDIX



SURVEY ON PASSWORD USE FOR EMAIL

Please do not identify yourself in any way, write your password(s) or email address on this survey.

For each of the following question, please tick the box that best applies to you.

What is your age group? □ Less than 18 years □ 18-25 years □ 26-35 years
□ 36-45 years □ 46-55 years □ More than 55 years

What is your gender? □ Male □ Female

Are you enrolled at university? □ Full time □ Part time □ Not enrolled

Are you employed? □ Full time □ Part time □ Not employed

How long have you been using a computer?

□ 0 - 2 years □ 3-5 years □ 6-10 years □ More than 10 years

What do you use a computer for? *Tick all that apply.*

□ Home use □ Work □ Banking □ Email □ Internet access
□ Other use, please specify

____

What is your email use? *Tick all that apply.*

□ Personal □ Work □ University
□ Other, please specify ______________________________________

How many email accounts do you currently have? □ 1 □ 2 □ 3 □ 4 or more

If you have more than one email account, do you use the exact same password for each email account?
□ Same password □ Slight variations of the same password □ No similarities between passwords

Besides email, do you use any other computer-based applications that require the use of a password?
□ No □ Yes; please specify application:

____

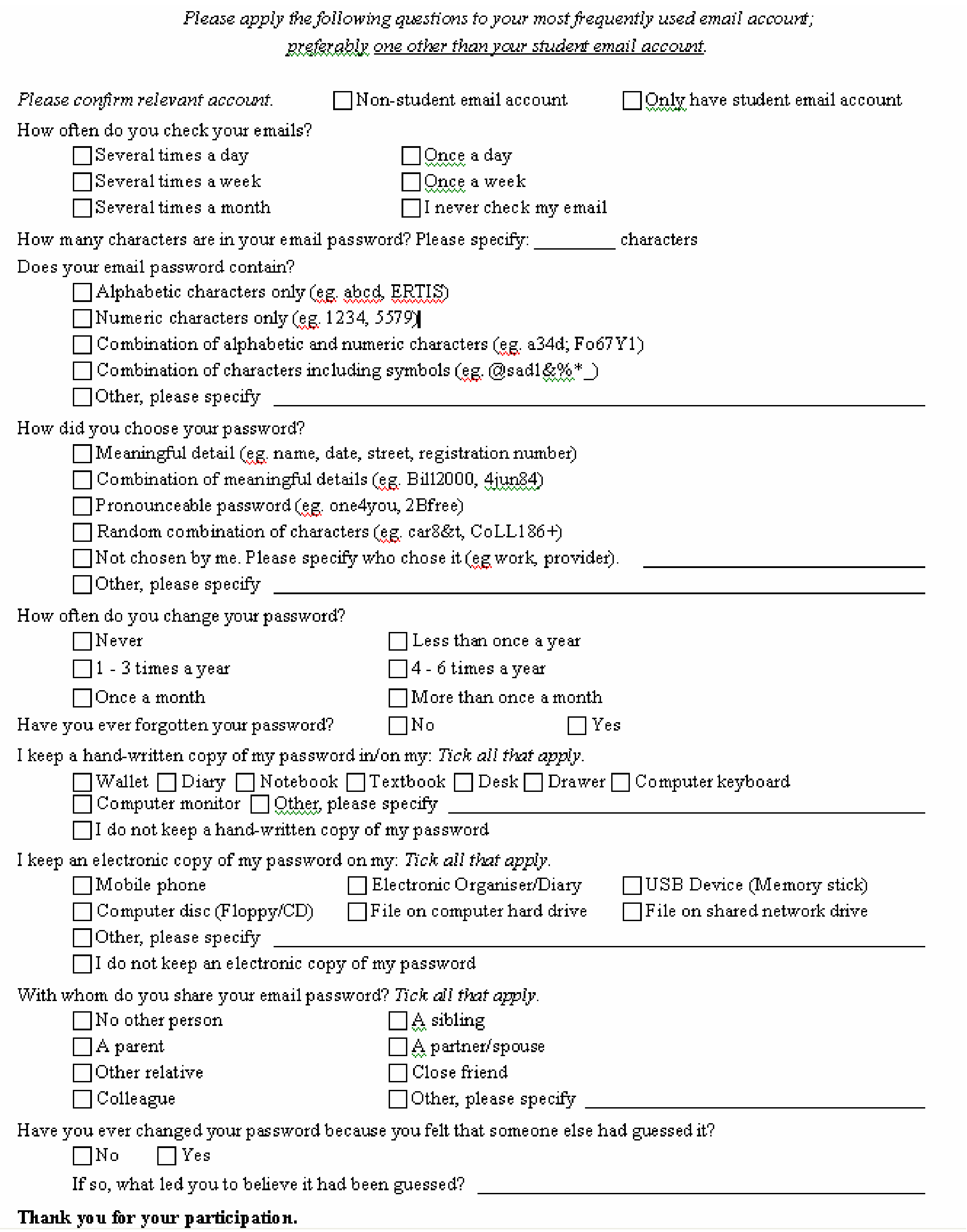
If Yes, is it the exact same password as the one you use on your email account?
□ Same password □ Slight variations of the same password □ No similarities between passwords

Are you aware of password cracking techniques? *Tick all that apply.*
□ Worm □ Virus □ Program file
□ Other; please specify

____

What do you consider are the major problems with password security?

____



Please apply the following questions to your most frequently used email account;
preferably one other than your student email account.

Please confirm relevant account. □ Non-student email account □ Only have student email account

How often do you check your emails?

□ Several times a day
□ Several times a week
□ Several times a month
□ Once a day
□ Once a week
□ I never check my email

How many characters are in your email password? Please specify: ________ characters

Does your email password contain?

□ Alphabetic characters only (eg. abcd, ERTIS)
□ Numeric characters only (eg. 1234, 5579)
□ Combination of alphabetic and numeric characters (eg. a34d; Fo67Y1)
□ Combination of characters including symbols (eg. @sad1&%*_)
□ Other, please specify ____________________

How did you choose your password?

□ Meaningful detail (eg. name, date, street, registration number)
□ Combination of meaningful details (eg. Bill2000, 4jun84)
□ Pronounceable password (eg. one4you, 2Bfree)
□ Random combination of characters (eg. car8&t, CoLL186+)
□ Not chosen by me. Please specify who chose it (eg work, provider). ____________________
□ Other, please specify ____________________

How often do you change your password?

□ Never
□ 1 - 3 times a year
□ Once a month
□ Less than once a year
□ 4 - 6 times a year
□ More than once a month

Have you ever forgotten your password? □ No □ Yes

I keep a hand-written copy of my password in/on my: *Tick all that apply.*

□ Wallet □ Diary □ Notebook □ Textbook □ Desk □ Drawer □ Computer keyboard
□ Computer monitor □ Other, please specify ____________________
□ I do not keep a hand-written copy of my password

I keep an electronic copy of my password on my: *Tick all that apply.*

□ Mobile phone
□ Computer disc (Floppy/CD)
□ Electronic Organiser/Diary
□ File on computer hard drive
□ USB Device (Memory stick)
□ File on shared network drive
□ Other, please specify ____________________
□ I do not keep an electronic copy of my password

With whom do you share your email password? *Tick all that apply.*

□ No other person
□ A parent
□ Other relative
□ Colleague
□ A sibling
□ A partner/spouse
□ Close friend
□ Other, please specify ____________________

Have you ever changed your password because you felt that someone else had guessed it?

□ No □ Yes

If so, what led you to believe it had been guessed? ____________________

Thank you for your participation.