Linking Student Information Security Awareness and Behavioural Intent

B. Ngoqo[1] and S.V. Flowerday[2]

[1]Applied Informatics Department, Walter Sisulu University, East London, South Africa
[2]Department of Information Systems, University of Fort Hare, East London, South Africa
e-mail: bukelwa.ngoqo@gmail.com

Abstract

This study analysed existing theories from the social sciences in order to gain a better understanding of factors which contribute to student mobile phone users' poor information security behaviour. Two key aspects associated with information security behaviour were considered, namely: awareness and behavioural intent. Researchers have identified the most common cause of poor security practices on the part of mobile phone users, and which cause them to fall victim to social engineering techniques such as phishing, is their lack of awareness of existing security threats, vulnerabilities and risks. However, an increasing number of researchers consider human behaviour to be another cause of security breaches. Zhang *et al. (*2009) concur with this view and state that understanding human behaviour is important when dealing with the problems caused by human errors. Harnesk *et al.* (2011) expressed a concern that existing research does not address the interlinked relationship between anticipated security behaviour and the enactment of security procedures. Existing researchers in the field of information security still grapple with the 'knowing-and-doing' gap, where user information security knowledge/awareness sometimes does not result in safer behavioural practises. This paper proposes that the knowing-and-doing gap can possibly be reduced by addressing both awareness and behavioural intent. This paper explores the relationship between student mobile phone user information security awareness and behavioural intent in a developmental university in South Africa.

Keywords

Mobile phone information security, information security awareness, information security behavioural intent

1. Introduction

The field of information security management for organisations is pervaded with policies, standards and frameworks. However, for application to the student mobile phone user context, this paper adopts the definition of information security management suggested by Parakkattu *et al.* (2010:318) which simply states that information security management is concerned with "ensuring the security of information through the proactive management of information security risks, threats and vulnerabilities". Although the information security environment of private mobile phone users is not regulated by standards, mobile phone users as owners of a technological asset (phone) which contains or is used to transmit information (asset) should be concerned with ensuring the security of this information. Humans have been repeatedly identified as the most important factor to be considered in the securing of information assets. People use technology in one of two environments, namely: the workplace and home (Talib, Clarke and Furnell, 2010). The mobile phone user considered in this study falls into the latter group of technology users. A unique attribute of these students is that they are registered in a newly restructured South African educational entity referred to in this study as a 'developmental university'.

In 2002 the Higher Education Restructuring Proposal (Ministry of Education, 2003) for the consolidation of higher education institutions through mergers and incorporations was approved by the government and resulted in the higher education system comprising eleven universities, six comprehensive universities and six universities of technology. The participants in this study are students from a comprehensive university structure which was formed in 2005 by merging three 'historically black' institutions. The Draft National Plan for Higher Education in South Africa (Department of Education, 2001) justly makes references to the demographic profile of the student body with the teaching of under-prepared students being an inherent characteristic associated with the 'historically black' institutions. These students are second language English speakers in an environment where instruction and teaching materials are presented in English and access to technological resources (e.g. computer labs, Internet) is limited. Arguably, in this developmental environment students are more vulnerable to information security threats than their counterparts in more well established universities.

Van Niekerk and Von Solms (2010) mention two primary human related factors in information security, namely: knowledge and behaviour. They caution that adequate security measures may be rendered inadequate if there are low levels of user cooperation or knowledge. For example, mobile phones have a password lock feature which requires the user to enter a password prior to accessing any information on the phone; however, if the mobile phone user does not activate the password, it cannot serve its purpose of protecting the information asset. For the purposes of this paper, the primary human related factors are considered to be awareness and behaviour. To determine participant information security threat knowledge/awareness ('know'), this paper firstly discusses how the level of awareness was calculated using Kruger and Kearney's (2006) method. Following this, a discussion of participant information security behaviour ('doing') and an explanation on how participant behavioural intent levels were calculated using similar methods follows. Finally, a discussion of the findings and concluding remarks is presented.

2. Measuring mobile phone information security awareness

In view of the poor levels of knowledge about the information security threats to which they are exposed in their environment, mobile phone users pose the biggest threat to information security (Chen, Medlin and Shaw, 2008; Talib *et al.*, 2010) with some security breaches (virus infections, identity theft, dumpster diving) being a direct result of what Chen *et al.* (2008) consider to be user carelessness or a lack of action. There is little evidence which proves that mobile phone users are knowledgeable about or are, in fact, practising information security (Talib *et al.*, 2010). This study adopted Chen *et al.'s* (2008) definition of information security awareness who consider the ultimate goal of information security awareness to be an awareness of security threats, an understanding of the way in which these threats work, and the ability to predict/anticipate potential outcomes if the threats are ignored.

Awareness campaigns are aimed at improving user knowledge, attitude and behaviour towards information security and were used as the interventions in this action research study. Kruger and Kearney (2006) identified a set of factors which contribute to information security awareness as knowledge (related to what users know), attitude (what they think) and behaviour (what they do). "Each dimension was then divided into focus areas" (Kruger and Kearney, 2006:291).

This study adopts the awareness measurement tool proposed by Kruger and Kearney (2006) for the purpose of measuring the level of student mobile phone user information security awareness. However, the following considerations must be noted:

- The dimension weights were kept at the percentages calculated by Kruger and Kearney (knowledge (30), attitude (20) and behaviour (50)).
- Due to the longitudinal nature of the study, different measurements were taken over a period of time. The initial calculated values were only important for checking the degree of observed changes between each subsequent measurement taken.
- The original measurement tool (Kruger and Kearney, 2006) refers to user actual behaviour. Users gave an indication of how they behaved by answering a set behaviour related questions. However, Kruger and Kearney (2006) acknowledge that users are not always truthful when answering such questions and as a result the measurement for actual behaviour may not be accurate. In lieu of this, this study substitutes the 'Behaviour' dimension with questions addressing 'Perceived Behavioural Intent'.
- Perceived Behavioural Intent helps to mitigate the impact of this possible inaccuracy by acknowledging the calculated value is based on what the mobile phone user professes.

Factoring the comments above, the tool was adapted for application in the student mobile phone user environment of a developmental university. The level of awareness map is then modified as follows:

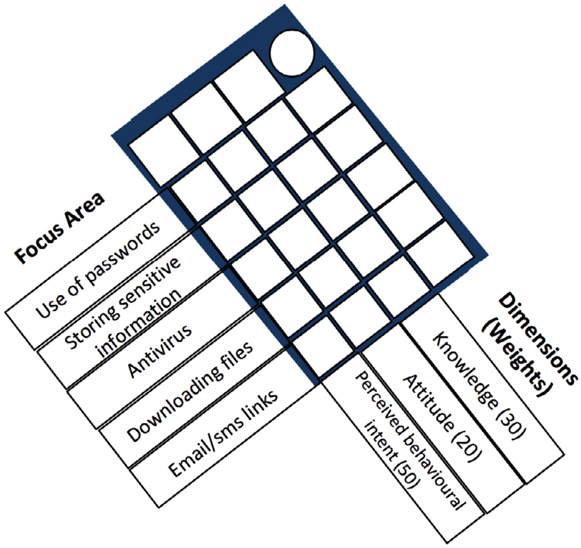

Figure 1: Level of Awareness map (adapted from Kruger and Kearney, 2006)

Recognising the limitation of undertaking an awareness campaign and its potentially poor impact on user behaviour, this study attempted to use information security awareness to stimulate security compliant student mobile phone user behaviour. While Furnell (2010) recognises that raising awareness is an important step, he does not consider it to be sufficient to overcome all the information security hurdles/challenges and concedes that it does not always result in improved security behaviour. Behavioural intent and how it can be applied to the student mobile phone user context is discussed in the next section.

3. Measuring mobile phone information security behavioural intent

The poor information security awareness of mobile phone users has a direct impact on their information security behaviour. To gain a better understanding of mobile phone user information security behaviour, this study relied on the Theory of Planned Behaviour (TPB) formulated by Ajzen (1991). The TPB outlines the interaction between a person's attitude, subjective norms, perceived behavioural control and their behavioural intentions. The TPB suggests that an individual's behaviour is determined by the person's intention to perform that behaviour and that intention is a function of their attitude, subjective norms and the perceived behavioural control which are important to the individual. Attitude looks at the individual's negative or positive feelings about performing the behaviour. Ajzen (1991) suggests that people are inclined to have a positive attitude towards behaviours believed to yield desirable consequences, while a negative attitude will be present where the consequences are believed to be negative. Ajzen (1991) describes subjective norms as the individual's perception about whether people important to the individual think the behaviour should be performed, and considers perceived behavioural control to be the extent to which the individual feels they are able to enact the behaviour. This can be influenced by non-motivational factors such as the availability of resources or opportunities (Ajzen, 1991). As a result of these non-motivational factors, students in the developmental context are faced with added challenges compared to students in developed countries. Oyedemi (2011) mentions that students in developing countries are at a disadvantage because they are faced with challenges relating factors like access to the Internet or limited access to computers. Ajzen (1991) makes a further argument that the person's perceived, and not necessarily the actual behavioural control, is a strong enough motivator for influencing behavioural intention. Whether or not the student mobile phone user has actual (or as much as they think they have) control over the given behaviour, if they perceive themselves as having control over the behaviour, their intention to act will increase.

Regarding the correlations between the components of the TPB model, Ajzen (1991) notes that the more favourable the attitude and subjective norms and the greater the perceived behavioural control, the stronger the behavioural intention and the more likely the person is of enacting the given behaviour.

The TPB has found wide application in the information security context, having been applied to computer abuse problems (Lee and Lee, 2010), security policy compliance (Pahnila *et al.*, 2007), and insider security contravention (Workman and Gathegi, 2007). This study relies on the TPB for determining factors which influence mobile phone users' information security behavioural intent. Based on the same focus areas used in measuring level of awareness, the dimensions considered in calculating behavioural intent are (*attitude*, *subjective norms* and *perceived behavioural control*) adopted from the TPB. However, unlike the *'perceived behavioural intention'* referred to used when calculating level of awareness, a critical difference exists in how the terms *'perceived behavioural intent'* (*cf* section 2 above) vs *'behavioural intent'* are defined and applied in this study. Behavioural intent is a calculated value based on the mobile phone users' scores in response to questions relating to their attitude, subjective norms and perceived behavioural control over information security related behaviour. On the other hand, the level of perceived behavioural control is a value solely based on the mobile phone users' scoring on answers to questions relating to their information security behaviour.

For the purposes of determining baseline figures, equal weights were allocated to each dimension. The findings will be used to determine how these weights can be adjusted for future application. For the purposes of this paper, the degree of the change between iterations of the study cycles is deemed to be a sufficient indicator for purposes of reviewing the relationship between awareness and behavioural intent.

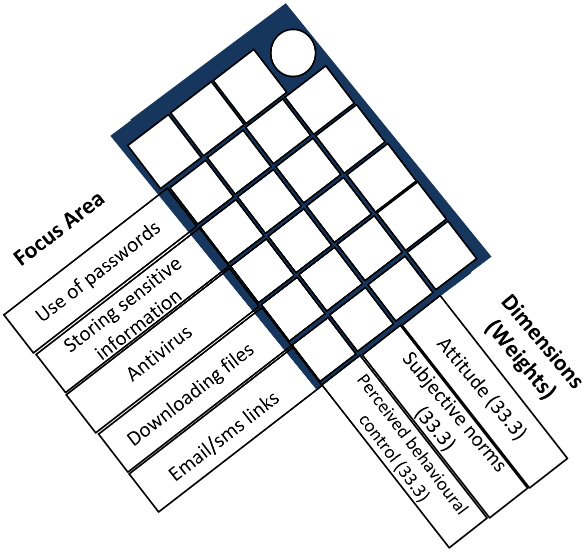

Figure 2: Level of Behavioural intent map (adapted from Kruger and Kearney, 2006)

The level of behavioural intent was determined by using the scorecard approach (see Figure 2) based on mobile phone users' responses to information security behaviour related questions. While the focus areas remained the same (see Figure 1), the dimensions considered (attitude, subjective norms and perceived behavioural control) are the main difference between the Level of Awareness map (Figure 1) and the suggested Level of Behavioural intent map in Figure above. The relationship between awareness and behavioural intent is discussed in the next section.

4. Relationship between awareness and behavioural intent

This paper suggests that there is a relationship between the student mobile phone user information security awareness levels and their levels of information security behavioural intent. While studies have been undertaken to assess levels of awareness in an organisation, the field of information security behavioural intent is rarely researched with most of the focus being on actual behaviour. While interventions like awareness campaigns result in an observable change in levels of what people 'know', sometimes a difference exists between what people 'know' and what they 'do'. Using the TPB, this paper acknowledges that behavioural intention is a predecessor to actual behaviour which is used as a proxy measure of actual behaviour for the purposes of this study. The following similarities and overlaps exist between the factors used to calculate level of awareness and those used to calculate behavioural intent:

- *Attitude* is a common factor.
- The factor *Behaviour* is referred to in Kruger and Kearney's level of awareness model (*see section 2 above*). Behaviour is determined by scoring participants responses to behaviour related questions.
- Using the TPB approach to calculate Behavioural Intention (BI), BI is a derived value based on the calculated and weighted scores of the factors: *attitude, subjective norms* and *perceived behavioural control*. Whereas in calculating Level of Awareness (LA) behaviour is a contributing factor.
- To highlight the distinction in how Behaviour/ Behavioural Intent is used differently in the calculating the values for the main components (LA and BI), the term *'Perceived Behavioural Intent'* (PBI) is introduced in this study. PBI refers to the behavioural intent value obtained by asking participants to respond to behaviour related questions. The answers provided are how the participants think ('perceive') they would respond to information security related incidents. This PBI is different to the calculated BI used the TPB approach. Using the TPB approach, BI is a calculated value based on the participant's score on questions relating to attitude, subjective norm and perceived behavioural control.

With the evident overlapping of factors from the underlying theories used in defining level of awareness and behavioural intent in this study, serious consideration was given to the existence of a relationship or inter-dependence between the two components.

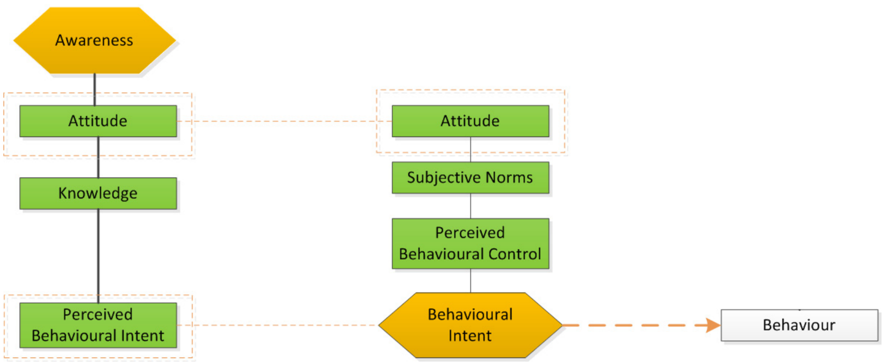

Figure 3: Mobile phone information security constructs

Figure 3 provides a graphic representation of identified associations between information security awareness, behavioural intent and actual behaviour. Behavioural intention influences actual information security behaviour. A survey was conducted using action research principles amongst 90 students from a developmental university in South Africa. Information security awareness interventions were implemented during the three cycle data collection process and a baseline survey (before any intervention was implemented) and subsequent surveys were taken after the completion of each intervention. The findings from the administered surveys are summarised below.

5. Findings

The main focus during analysis of the study findings remained on observing any changes to constructs awareness and behavioural intent. Correlation analysis tests were conducted to determine whether relationships existed between the different factors. The correlation coefficients give an indication of whether the relationship is a positive relationship (changes to constructs increase or decrease in the same direction) or a negative relationship (constructs respond in opposite directions). This section concludes by analysing the relationship between overall awareness and behavioural intent. Level of awareness is presented below.

Level of Awareness (LA)

Awareness factors (Knowledge (K), attitude (A), behaviour (PBI)). Relationships between factors are presented below:

		K	PBI	A
K	Pearson Correlation	1	.022	-.176
	Sig. (2-tailed)		.844	.117
	N	81	81	81
PBI	Pearson Correlation	.022	1	.219
	Sig. (2-tailed)	.844		.050
	N	81	81	81
A	Pearson Correlation	-.176	.219	1
	Sig. (2-tailed)	.117	.050	
	N	81	81	81

Table 1: Correlation (K, A, PBI)

Knowledge and attitude

As shown in Table 1, Pearson's correlation coefficient was used to investigate the relationship between knowledge and attitude of student mobile phone users. It was found that there was a low degree of negative correlation between knowledge and attitude at [$r = -0.176$, $n = 81$, $p = 0.117$].

Knowledge and perceived behavioural intent

Table illustrates how Pearson's correlation coefficient was used to investigate the relationship between knowledge and perceived behavioural intent of student mobile phone users. It emerged that there was a low degree of positive correlation between knowledge and perceived behavioural intent at [$r = 0.022$, $n = 81$, $p = 0.844$].

Attitude and perceived behavioural intent

As presented in Table above, Pearson's correlation coefficient was used to investigate the relationship between attitude and perceived behavioural intent. It was found that there was a low degree of positive correlation between attitude and perceived behavioural intent at [r = 0.219, n = 81, p = 0.050].

Correlation between the factors *knowledge/attitude* and *knowledge/perceived behavioural intent* was determined to be non-existent or negligible. Therefore based on the findings, no relationship can be assumed between these factors. However, a weak positive relationship is shown between *attitude/perceived behavioural intent*. It can therefore be inferred that a more positive student mobile phone user information security attitude is associated with an increased information security behavioural intention. The relationship was found to be weak; its significance is also negligible with p=0.050.

Behavioural Intent (BI)

Behavioural intent factors (Attitude (A), subjective norms (SN), perceived behavioural control (PBC)). Relationships between factors are presented below:

		A	SN	PBC
	Pearson Correlation	1	.399	.185
A	Sig. (2-tailed)		.000	.098
	N	81	81	81
	Pearson Correlation	.399	1	.337
SN	Sig. (2-tailed)	.000		.002
	N	81	81	81
	Pearson Correlation	.185	.337	1
PBC	Sig. (2-tailed)	.098	.002	
	N	81	81	81

Table 2: Correlations (A, SN, PBC)

Attitude and subjective norms

As illustrated in Table 2 above, Pearson's correlation coefficient was used to investigate the relationship between attitude and subjective norms of student mobile phone users. A moderate degree of positive correlation exists between attitude and subjective norms at [r = 0.399, n = 81, p = 0.000]. With $p < 0.05$ this correlation is statistically significant with high scores for attitude associated with high scores for subjective norms.

Attitude and perceived behavioural control

As shown in Table 2 above, Pearson's correlation coefficient was used to investigate the relationship between attitude and perceived behavioural control for student mobile phone users. It was found that there was a low degree of positive correlation between attitude and perceived behavioural control at [r = 0.185, n = 81, p = 0.098].

Subjective norms and perceived behavioural control

As shown in Table 2, Pearson's correlation coefficient was used to investigate the relationship between subjective norms and perceived behavioural control for student mobile phone users. It was found that there was a moderate degree of positive correlation between subjective norms and perceived behavioural control at [r = 0.337, n = 81, p = 0.002]. With $p < 0.05$ this correlation is statistically significant with high scores for subjective norms associated with high scores for perceived behavioural control.

With the exception of *attitude/perceived behavioural control* which showed a non-existent or negligible relationship, moderate positive relationships which were determined to be statistically significant were found between *attitude/subjective norms* and *subjective norms/perceived behavioural control.* The findings show that it can be anticipated that a more positive student mobile phone user information security attitude is associated with positive information security behaviour subjective norm propositions. The tests for significance show the result is not due to chance.

Awareness and Behavioural intent

Correlation analysis tests performed also confirmed the existence of relationships between two of the constructs used in the model. A key assumption made in developing the proposed model in this study was that a relationship exists between level of awareness and the level of behavioural intent.

Overall effects of Awareness **(LA)** on Behavioural Intent **(BI)** – is there a negative or positive relationship?

		LA	BI
LA	Pearson Correlation	1	.374
	Sig. (2-tailed)		.001
	N	81	81
BI	Pearson Correlation	.374	1
	Sig. (2-tailed)	.001	
	N	81	81

Table 3: Correlations (LA, BI)

As shown in Table 3 above, the value of Pearson's product between the two factors (LA and BI) was r=.374 ($p<0.05$). The results show a moderate positive correlation between level of awareness and level of behavioural intent with statistically significant result ($p < 0.05$).

The statistical tests confirmed the existence of a positive relationship between the constructs (LA and BI). The main inference which can be made based on this determination is that the more aware the student mobile phone users are about information security threats, their intention to follow safe information security practices will also increase.

6. Discussion and concluding remarks

Due to their usage of mobile phones and more specifically mobile phone applications, students in a South African developmental university are faced with the same threats as students in a better developed university. However compared to their global counterparts from more developed countries, they are more vulnerable to threats because of the developmental university environment where students have limited access to sources of information (e.g. Internet) that could help improve their awareness. Thus the findings of this study are important by providing better insight on the awareness and behavioural intent related factors which must be considered to influence a change in South African students' mobile phone information security behaviour.

Statistical tests conducted to determine the extent to the factors that contribute to mobile phone user information security awareness confirmed the levels of influence between the factors knowledge and attitude; knowledge and behaviour and between attitude and behaviour are not significant. Based on the study findings, no claims can be made on the relationships between the individual Level of Awareness (LA) factors.

In reviewing the results obtained from exploring the relationships between the factors which contribute to mobile phone user information security behavioural intent, significant influences were recorded between the following factors: attitude and subjective norms and subjective norms and perceived behavioural control. However, the influence between attitude and perceived behavioural control was found not to be significant. In a similar pattern uncovered in the relationships between the awareness factors, mobile phone users' information security attitude will influence or be influenced by their subjective norms and perceived behavioural control. The extent to which mobile phone users feel they have control over information security behaviours/actions is also influenced and influences the mobile phone users' perceptions about what they think their family or peers deem to be acceptable information security behaviour.

The significant positive correlation found between Level of Awareness (LA) and Behavioural Intention (BI) was a key finding which confirmed this study's premise, which suggests that a relationship exists between information security awareness and behavioural intent. The most common efforts aimed at addressing the 'knowing-and-doing' gap have concentrated on improving awareness, and this paper suggests that this gap can be reduced by addressing awareness in conjunction with behavioural intent.

7. References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behaviour and Human Decision Processes,* 50, 179-211.

Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security,* 16(4), 360-376.

Department of Education, "National Plan for Higher Education in South Africa", *Ministry of Education*, South Africa, February 2001.

Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security*, 1074.

Harnesk, D. and Lindstrom, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security,* 19(4), 262-276.

Kruger, H.A., Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security,* 25, 289-296.

Lee, H. and Lee, S. (2010). Internet vs mobile services: comparisons of gender and ethnicity. *Journal of Research in Interactive Marketing,* 4(4), 346-375.

Ministry of Education. (2003). *Higher Education restructuring. Guidelines for mergers and incorporations.* Retrieved November 11, 2013, from http://www.education.gov.za/LinkClick.aspx?fileticket=Fk0AzO7hgqA%3D&tabid=95&mid=507

Oyedemi, T.D. (2012). Digital inequalities and implications for social inequalities: A study of Internet penetration amongst university students in South Africa. *Telematics and Informatics*, 29(2012), 302-313.

Pahnilla, S., Siponen, M. & Mahmood, A. (2007, 14-16 May). Employees adherence to information security policies an empirical study. *IFIP TC-11 22nd International Information Security Conference*. Johannesburg, South Africa.

Parakkattu, S. and Kunnathur, A.S. (2010, March). A framework for research in information security management. *Northeast Decision Sciences Institute Proceedings*, pp. 318-323.

Talib, S., Clarke, N.L. and Furnell, S.M . (2010, 15-18 February). An analysis of information security awareness within home and work environments. *Conference on Availability, Reliability and Security, ARES'10 International conference*, (pp. 196-203). Krakov.

Van Niekerk & Von Solms. (2010). Information security culture: A management perspective. *Computers & Security,* 29, 476-486.

Workman, M. & Gathegi, J. (2007). Punishment and ethics deterrents: a study of insider security contravention. *Journal of the American Society for Information Science and Technology,* 58(2), 212-222.

Zhang, J., Reithel, B.J. and Li, H. (2009). Impact of perceived technical protection on security behaviours. *Information Management & Computer Security,* 17(4), 330-340.