

Information Security Competence Test with regards to Password Management



Paul Tarwireyi
Stephen Flowerday
Anass Bayaga



University of Fort Hare
Together in Excellence



Recipient of the
**Supreme Order
of Baobab**
(Gold)

Outline

- Background
- Motivation
- Related work
- Our Approach
- Results
- Conclusion



Background

- The human factor is widely acknowledged as the weakest link in Information Security.
- Security awareness programmes
- They employ mechanisms that reinforce good security practices and change employee security behaviour



Background

- A security competence assessment approach that uses competence based behavioural questions
- Application and findings of a study that examined password management practices of university students.



Motivation

- Even though work has been done in implementing security awareness programmes
- Work on assessing their effectiveness is still in its infancy
- It is important to assess to see if there was an improvement or not.



Related work

- Other researchers have used different techniques such as
 - knowledge, attitude and
 - vocabulary tests
- to assess security awareness and culture in organisations



Our Approach

- Since an organisation's success or failure depends on things that its employees do or fail to do
- Information security strategy should pay close attention to employee behaviour.
- Depicting normal behaviour implies having appropriate knowledge



Our Approach

- One can evaluate the security competence of an individual by assessing the way they behave in certain security scenarios
- The objective in the application of our assessment method was to investigate if there was a relationship between level of study and security competence



Our Approach

- In our study we endeavoured to ascertain the security competence of university students with regards to password management.
- A questionnaire with competence based behavioural questions was administered to
 - First year students and
 - Third year students



Competence based questions

- Competence based questions have long been used in HR to select employees with the necessary skills to perform effectively in a job.
- Competence is the ability to apply knowledge, skills, abilities and traits to perform tasks
- is a description of something that a person who works in a given occupational area should be able to do.



Competence based questions

- Competence based tests focus on behaviours and traits for success in a particular field
- They do not look for opinion but rather seek past behaviour
 - Reduce misunderstandings about past experience
 - Provide actual examples of knowledge, skills and attributes
 - A quick way of covering behavioural facets of an individual



Password management areas

- Sharing passwords
- Storage of passwords
- How often passwords are changed
- Using same password for multiple accounts
- Password remembering options
- Default passwords



Example question: Storage of passwords

- In terms of a new password. How do you store your password if you do not want to forget it?
 - Simply write it down somewhere
 - Write down a reminder/ hint
 - Store the password / hint in a secure, locked place
 - Memorise it



Data Analysis and Interpretation

- There were 140 usable responses
- 73 first year students
- 67 third year students

- Data was analysed in SPSS
- The password management competence levels at the different years of study were compared



Data Analysis and Interpretation

Option	Frequency	Percent
Simply write it down somewhere	21	15.0
Write down a reminder/ hint	19	13.6
Store the password / hint in a secure, locked place	15	10.7
Memorise it	85	60.7
Total	140	100.0



Summary of Research findings

Password Question	Relationship with year of study	
	YES	NO
Sharing Passwords	✓	
Storage of passwords		✓
Changing passwords		✓
Using the same password for accounts		✓
Choosing the remember password option		✓
Password strength	✓	
Default passwords	✓	



Research findings

- 38.4% of first year students will share their passwords whilst 59.7% third year students will do the same
- A weak negative relationship
- 19.2% and 22.4% of first year and third year students respectively shared their passwords even though they knew there was a risk



Research findings

- First year students created weaker passwords than third year students
- Almost two thirds (63%) of first year students
- Compared to 41.8% third year students



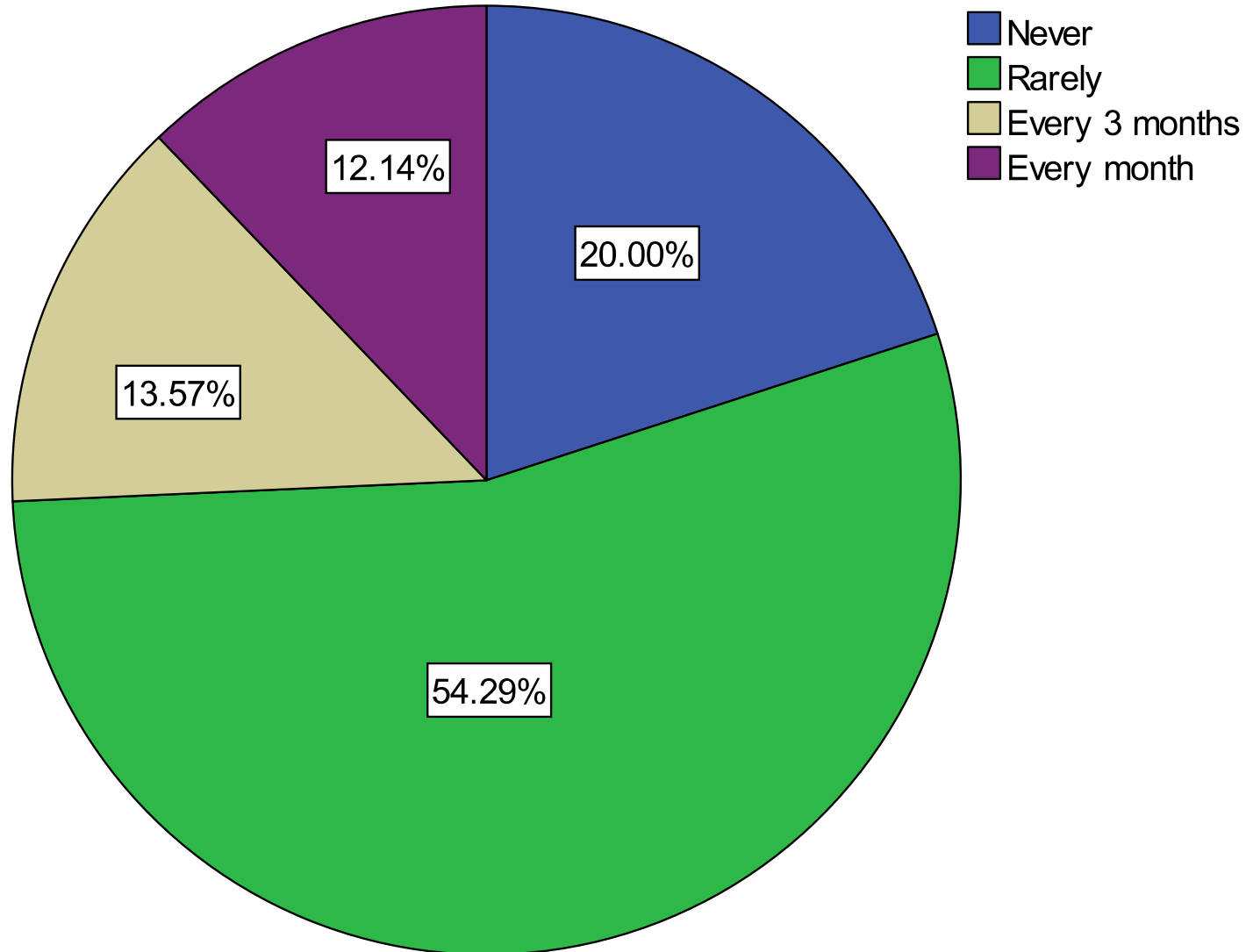
Research findings

- 69.9% first year students do not change their default passwords whilst
- 40.3% third year students also do not change default passwords



Problematic area

How often you change passwords



University of Fort Ha
Together in Excellence



Comparison of competence levels

Password Competence	Competent percentage	
	1 st years	3 rd years
Sharing Passwords	61.7	40.3 ↓
Storage of passwords	68.5	74.7 ↑
Changing passwords	30.1	20.9 ↓
Using the same password for different accounts	42.4	53.8 ↑
Choosing the remember password option	61.7	76.1 ↑
Password strength	37	52.2 ↑
Default passwords	30.1	59.7 ↑



Way forward

- From these results it was possible to draw conclusions between the levels of security competence at the different years of study
- This can be used as a valuable tool for assessing security competence before and after the implementation of security awareness programs.



Way forward

- Nonetheless, research is still needed to enhance this assessment approach
- It should be tested in other environments
- Since password management is only one area of information security, it should be applied to other areas such as phishing



Conclusion

- It is important to have a way of assessing the effectiveness of security awareness programs
- This allows you to see if the intended goals were met.



Thank You!



University of Fort Hare
Together in Excellence

