IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Ethical Behaviours Towards Enhanced Data Security Among Youth In Zimbabwean Tertiary Education Institutions In Marondera District.

Abbermore Stokozile Chipashu, Dr Onesmus Nyaude(Phd)
Noida International University, School Of Business Management – Research Scholar

Abstract

Innovative Mobile Health Interventions Have Been Made Possible By The Growing Global Usage Of Digital Technology Such As Smartphones, Especially When It Comes To Connecting And Interacting With Young People. Thus, Utilizing These Tools Could Alienate People Who Don't Have Access To Them. The Study Interrogates Ethical Behaviours Among Youths Towards Enhanced Data Security Targeting The Youth In Selected Zimbabwean Tertiary Educational Institutions. The Study Is Premised On The View That The Youths Are Going To Be The Future Leaders Of Zimbabwe And Need To Have Informed Information On Data Security. The Research Was Informed By The Phenomenological Paradigm. The Research Adopted The Qualitative Approach Using Personal In-Depth Interviews Involving 24 Participants Of Mixed Gender. The Data Was Analysed Using The Thematic Approach In Which Themes Were Developed Related To Youth Ethical Behaviours Meant To Enhance Data Security. The Results Of The Survey Showed That Knowledge Of Cyber-Security Was Still Significantly Lower Than Anticipated. The Study Findings Revealed That Citizen Awareness Efforts On Cybercrime And Security Is An Imperative. In Addition, Young People Need To Cope With Irrational Anxieties And Experiences That Restrict Their Capacity To Freely And Thoughtfully Accomplish The Things They Reasonably Value. It Was Recommended That Law Enforcement Agencies Need To Collaborate With Academic Institutions And Other Relevant Stakeholders To Integrate Digital Literacy Initiatives Into The Curricula. The Urgent Need For Organizations And Individuals To Improve Their Cyber Hygiene Was Highly Emphasized To Bridge The Existing Digital Literacy Gap.

Key Words : Ethical Behaviours, Youth, Data Security

1. Introduction And Background Of The Study

The Study Interrogated Ethical Behaviours Among The Youth Towards Enhanced Data Security In Zimbabwe Selected Tertiary Educational Institutions In Marondera District. The Two Tertiary Institutions Were, Kushinga Phikelela Polytechnic And Kushinga Phikelela Agricultural College. These Colleges Were Conveniently Chosen. The Process Of Protecting Digital Information From Corruption, Theft, And Illegal Access Over The Course Of Its Whole Life Cycle Is Known As Data Security. Innovative Mobile Health Interventions Have Been Made Possible By The Growing Global Usage Of Digital Technology Like Smartphones And The Internet, Especially When It Comes To Connecting And Interacting With Young People (Adeniyi, And Ocholia, 2019). Innovative Mobile Interventions Have Been Made Possible By The Growing Global Usage Of Digital Technology Like Smartphones And The Internet, Especially When It Comes To Connecting And Interacting With Young People In Tertiary Institutions. But There's A Chance That Utilising These Tools Could Alienate People Who Don't Have Access To Them.

Many Industries, Including Education, Now Depend More Heavily On Digital Networks, Systems, And Data Storage As A Result Of The Quick Development Of Technology. Like Everywhere Else, Zimbabwe's Tertiary Institutions Have Embraced Digital Technologies To Improve Research, Teaching, And Learning.

However, New Risks And Difficulties Have Also Been Brought About By This Expanded Digital Presence, Especially In Relation To Data Security. Mobile Technology Is Increasingly Being Deployed To Support Education And Improve Access To Research And Publication By The Youths.

Youth In Marondera Urban Use Information And Cyber Technology To Complete A Variety Of Academic Assignments On A Daily Basis. The Use Of Such Technology Is Governed By Ethical Standards, Which Help To Prevent Ethical Transgressions To Some Degree. But According To Study, Students Typically Don't Comprehend Or Know How To Utilize Cyber Technology Ethically, Which Causes Them To Make Decisions Without Considering Their Ethical Obligations And Repercussions (Moor, 2003, In Adeniyi, And Ocholia, 2019). Unethical Behaviours Practiced By Some Of The Youth Include Cyberbullying, Plagiarism, Copyright And Digital Piracy Hence It Is Necessary To Carry Out This Research.

The Study Will Cover 5 Thematic Areas As Follows:

a) Security
b) Honesty
c) Accountability
d) Integrity
e) Transparency

These Five Themes Will Suffice The Objectives The Study In Relation To Ethical Behaviours Of Youths Towards Enhanced Data Security.

2 Problem Statement

Notably Many Young People In Zimbabwe Lack Sufficient Knowledge About The Ethical Ramifications Of Their Online Behaviour And The Significance Of Data Security, They May Engage In Reckless Behavior, Such As Sharing Sensitive Information Or Creating Weak Passwords, Which Could Jeopardize Personal Information And National Security. It's Possible That Zimbabwe's Educational System Isn't Offering Enough Instruction And Training On Internet Responsibilities, Ethics, And Data Security. Young Individuals May Lack The Abilities And Knowledge Necessary To Securely And Responsibly Navigate The Online Environment As A Result Of This.

3 Research Questions

3.1 What Are The Ethical Behaviours Exhibited By The Youth In Zimbabwe Towards Enhanced Data Security?

3.2 Which Ethical Behaviours Are For And Against Enhanced Data Security Among Youth In Zimbabwe?

3.3 What Are The Reality Impacts Of Violations Of Data Security Among Youth In Zimbabwe?

3.4 What Interventions Are At The Society's Disposal To Deal With Or Address Effects Of Violations Of Data Security Among Youth In Zimbabwe?

4 Significance Of The Study

The Importance Of The Study Was That It Was Conducted In View Of The Youths Who Are Going To Be The Future Leaders Of Zimbabwe And Need To Have Informed Information On Ethical Behavior Regarding Data Security, As Well As Finding Out What Are The Ethical Behaviours Exhibited By The Youths In Terms Of Data Security In Zimbabwe And Also Looking At Their Ethical Behavior For And Against Enhanced Data Security. This Study Led To The Development Of A New Framework Towards Data Security. This Study Helped To Identify Area Of Improvement And Came Up With Proposed Interventions. The Information From This Research Paper May Contribute To The Existing Body Of Knowledge And Inform Future Studies.

5 Delimitations

Data Was Collected From Two Marondera District Tertiary Education Institutions Students That Is Kushinga Phikelela Polytechnic And Kushinga Phikelela Agricultural College.

6 Limitations

I) One Of The Limitation Is That Some Youth May Not Have Receive Adequate Training On Data Security And Ethical Behavior, Hence Some Were Not Familiar With Ethical Conduct.

Ii) Few Participants Were Reluctant To Answer Questions Appropriately Hence There Was A Probability Of Getting Inadequate Responses. Hence The Researcher Overcame This Limitation By Comparing The Responses With Those Of The Majority.

Iii) Some Youths Were Not Familiar With The Ethical Behaviours Pertaining To Data. The Researcher Had To Explain So That They Could Comprehend The Meanings.

7 Literature Review

There Are Relatively Few Research Publications On Cyber Ethics In Africa, And The Current Interest In Unethical Behaviour In Research Is Relatively New In This Part Of The World (Adeniyi, And Ocholia, 2019). This Also Motivated The Researcher To Undertake This Research.

Ethical Behaviour In Data Security

The Legal Right Of The Data Subject To Access, Use, And Acquisition Of Data Is Known As Data Privacy, Information Privacy, Or Data Protection (Wanbiland Wolfgang, 2016. This Includes The Following: Freedom From Illegal Access To Private Information; Inappropriate Use Of Information; Accuracy And Completeness When Technology Collects Information On An Individual Or Individuals, Including Companies; Availability Of Data Content; And The Legal Right Of The Data Subject To Access, Ownership, And The Authority To Review, Amend, Or Rectify These Data. These Commandments Need To Be Abided To In Order Not To Breach Ethical Data Security, Otherwise Stern Measures May Be Taken Against Perpetrators.

Data Ethics Encompasses The Moral Obligations Of Gathering, Protecting, And Using Personally Identifiable Information And How It Affects Individuals (Havard School Of Business Onlne). The Five Principles Of Data Ethics Are, Ownership, Transparency, Privacy, Intention And Outcomes According To Havard Business School Online. If Data Has Such Qualities Then It Is Said To Be Enhanced Data.

Unethical Behaviour Exhibited By Youths In Tertiary Institutions

The Increasingly Limitless Access To The Internet In University Campuses Has Made Cyber Piracy Among Students, Prevalent, (Adeniyi, And Ocholia, 2019). This Behavior Is Also Prevalent At Kushinga Phikelela Polytechnic And Kushinga Phikelela Agricultural College. One Of The Risks Of Cyberbullying, Is That There Are Many Examples Of Young People Committing Serious Online Assaults That Result In Suicides Or Leave Others With Physical Or Psychological Scars (Kusuma, 2020).

Overuse Of Social Media Is Linked To A Number Of Mental Health Conditions, Such As Eating Disorders, Anxiety Connected To One's Own Appearance, And Other Concerns. Adolescents Have Experienced A Sharp Increase In The Prevalence Of Some Mental Health Disorders, Including Depression And Suicide, In Recent Years. Between 2007 And 2017, The Suicide Rate Among Youth Aged 10 To 24 Increased By 56% (Mapuvire, And Mapuvire, 2022). The Use Of Social Media Is Also Affecting The Youths In Marondera Urban, Hence Proper Awareness Campaigns On The Proper Use Of These Digital Platforms Are Required.

Level Of Awareness Among Youths Towards Enhanced Data Security

Since Computers Have Become A Necessary Component Of People's Lives, There Is A Greater Chance That Information Will Be Compromised. The Purpose Of Awareness, As Defined By Nist Special Publication (Sp) 800–16, Information Technology Security Training Requirements: A Role And Performance-Based Model, “Is Simply To Focus Attention On Security”(Mapuvire And Mapuvire). The Goal Of Awareness Is "To Enable People To Identify It Security Issues And React Appropriately." This Is Crucial Since An Organization's Cybersecurity Posture Relies Heavily On Its Users.

The Amount Of Work Done To Provide Users With Adequate Cybersecurity Awareness And Education In Zimbabwe Is Insufficient. Users Cannot Learn From Any Digital Hubs Or Websites Devoted To Cyber

Security Tactics, And Zimbabwe Has Neither Created Nor Executed Any Awareness Campaigns (Martin, Et. Al 2024).

The Primary Motivation For Hacking Is The Financial Gain Obtained By Stealing Sensitive Information And Holding It For Ransom. Hackers Can Also Earn Money By Selling Secret Data To Competitors On The Dark Web, Which Makes Cyberspace Unsafe And Poses Considerable Risks To Organizations And Their Customers (Mutunhu, Et Al 2022). This Is An Unfortunate Situation Whereby Our Youths Are Lured In Doing Such Unscrupulous Activities.

Given The Rapid Growth In Cyber Threats And Cybercrime, Cybersecurity Awareness In The Kingdom Has Neither Received Sufficient Attention Nor Has The Importance Of Security Been Investigated Among College Students (Alharbi, And Tassaddiq, 2021). Due To The Higher Recurrence Of Hacking Assaults On The Data Frameworks In Schools And Colleges, It Is Vital That Students Be Aware Of The Consequences And Challenges Of Cybersecurity And Cybercrime (Alharbi, And Tassaddiq, 2021). This Also Applies To Our Youths In Zimbabwe Whereby, Vigorous Cybercrime Awareness Campaigns Are Required In Order To Reduce The Occurrence.

8 Methodology

The Research Adopted The Qualitative Approach, In Particular, The Phenomenological Paradigm Which Focused On Exploring Students' Knowledge On Ethical Behavior Towards Data Security. Personal Interviews Involving 24 Participants Of Mixed Gender Selected From Two Educational Tertiary Institutions In Marondera District Were Conducted, Namely Kushinga Phikelela Polytechnic And Kushinga Phikelela Agricultural College. The Age Ranged From 18 Years To 40 Years. 24 Participants Were Personally Interviewed From Both The Tertiary Institutions That Included 12 Ladies And 12 Males. 11 Participants Were From Kushinga Phikelela Agricultural College And 13 Participants From Kushinga Phikelela Polytechnic.

8.1 Sampling And Selection Of Participants

The Research Made Use Of Non-Probability Sampling Method, Using The Purposive Sampling Technique. 24 Participants Of Mixed Gender Were Purposively Selected From Kushinga Phikelela Polytechnic And Kushinga Phikelela Agricultural College. The Sample Comprised Of 12 Female Students And 12 Male Students. The Saturation Point Was Reached At 24 Participants. The Participants Involved In This Study Included Students Doing Various Courses, Agriculture, Health Services Management, Accountancy, Information Technology, Fabrication And Transport And Logistics Management. The Interviewees Were Coded 1 Up To 24. The Research Sample Was Tabulated As Follows:

Table 1: Research Sample

Interviewee No	Gender	Age	Level Of Education	Field
1	Male	18	Nc	Fabrication
2	Female	19	Nd	Health Services Management
3	Female	21	Nd	Accountancy
4	Male	21	Nd	It
5	Male	22	Nd	It
6	Female	22	Nd	Agriculture
7	Female	22	Nd	Agriculture
8	Male	22	Nd	It
9	Male	23	Nc	Fabrication
10	Female	23	Nd	Transport And Logistics
11	Female	23	Nd	Agriculture
12	Female	24	Nd	Agriculture
13	Male	24	Bsc	Computer Engineering
14	Male	24	Nd	Health Services Management

15	Male	25	Nd	Agriculture
16	Female	25	Nd	It
17	Female	26	Nd	Agriculture
18	Female	26	Nd	Agriculture
19	Male	26	Nd	It
20	Female	27	Hnd	Agriculture
21	Male	28	Nd	Agriculture
22	Female	29	Nd	Agriculture
23	Male	35	Nd	Agriculture
24	Male	40	Nd	It

Key: Nc – National Certificate
Nd – National Diploma
It - Information Technology

8.2 Data Collection

In-Depth Face-To-Face Interviews Were Undertaken Using Open Ended Questions. The Data Used In This Article Is Primarily Qualitative. The Face-To-Face Interviews Were Organised With Students From Kushinga Phikelela Polytechnic And Kushinga Phikelela Agricultural College. Personal Interview Were Conducted Until The Researcher Reached A Saturation Point Of 24 Participants Whereby Participants Were Now Giving Similar Points. The Saturation Point Is Refers To The Point Refers To The Point At Which No New Information Or Themes Emerge From The Data Collection Process

9 Data Analysis

The Data Was Analysed Using A Qualitative Method, Which Is The Thematic Approach In Which Themes Were Developed Related To Youth Ethical Behaviours Meant To Enhance Data Security. Codes, Category Patterns And Themes Were Identified Within The Data. Descriptive Codes Were Allocated To Each Category.Questionnaires Were Numbered From Number 1 To 24. The Themes Were Numbered From Number 1 To 5. The Data Will Be Analysed Using The Two Objective Outlined In This Study, Which Are As Follows:-

9.1 What Are The Ethical Behaviours Exhibited By The Youth In Zimbabwe Towards Enhanced Data Security.

The Above Research Question Was Used To Analyse Five Themes As Follows:-

9.1.1 Security

i) Thirteen Participants Out Of 24 Outlined That The Data Was Secured Through Using Passwords, Patterns, Fingerprints And Data Encryption. This Translated To 54% Of The Sample Size. They Indicated That It Was Not Easy For Unauthorized People To Access The Information.

ii) Four Participants (17%) Indicated That, Because Of Advancement In Technology, They Were Not Whether Their Data Was Secure Through The Use Of Eg, Passwords Or Data Encryption. The Youth Indicated That They Were Afraid That Their Security Measures May Have Been By-Passed Through The Use Of Advanced Technology Like Phishing And Hacking.

iii) Participant Number 4 (4%) Disclosed That At Times There Is Disclosure Of Information By Others Without Consent

iv) Two Participants (8%) Highlighted That The Information May Leak Because Of Using Passwords That Are Not Strong Because Of Ignorance.

v) Four Participants (17%) Indicated That Security Was Not Guaranteed Because Of Hacking, Phishing And Sharing Of Laptops.

9.1.2 Honesty

i) Eight Participants (33%) Were Of The Opinion That Youths Produce Their Information Honestly And Diligently Although At Time They Use Websites To Get Some Of The Data.

ii) Sixteen Participants (67%) Outlined That There Is Misuse Of Different Media. Data Was Being Shared On Internet And At Times Someone's Data Is Modified. This May Be As A Result Of Ignorance At Times. Some Give False Data Because They Thought There Was Nowhere That Was Going To Be Proven That They Are The Ones That Gave False Data. Plagiarism Is Also Taking Centre Stage Because Of Using Artificial Intelligence And Google. Originators Of The Data Were Not Quoted. Participant Number 24 Buttressed The Issue By Highlighting That Youths Were Not Honest With Data. "They Tended To Abuse

Data By Leaking Information, Eg, Pictures Purposively Insocial Media Through Trending In Order To Get Popularity". This Was A Reflection That Youths Were Abusing Data.

9.1.3 Accountability

i) Fifteen Participants (63%) Out Of 24 Outlined That Youths Were Accountable Their Data.

ii) Seven Participants (29%) Highlighted That Youths Were Not Accountable To Their Data Because Of Some Underlying Reasons Like They Were Afraid Of Victimization After Publishing False Information Or Have Plagiarised The Data Or Were Involved In Cyber Bullying Or The Data May Have Been Hacked. It Was Also Highlighted That They Could Not Produce Useful Information By Themselves Of May Have Tempered With Sensitive Issues Like Political Issues, So They Do Not Want To Be Accountable.

iii) One Participant (4%) Outlined That, It Depends Whether The Data Is Good Or Bad. If The Data Is Good Youths Will Be Accountable. If The Data Is Bad No One Wanted To Be Associated With Such Data. Youth Ended Up Using Pseudo Names So That They Were Not Easily Identified And Not Become Accountable. They Were Also Afraid Of Victimization And Facing The Law.

9.1.4 Integrity

i) Fourteen Participants (58%), Were Agreeable That They Produce Reliable And Accurate Data.

ii) One Participant (4%) Indicated That Some Of The Data Was Accurate And Reliable.

iii) Nine Participants (38%) Were With The Opinion That Most Data By Youth Was Not Consistent, Reliable Or Accurate Because They Falsify The Data Or May Have Inadequate Facts, Data May Have Been Plagiarized, Publishing False Information, Cannot Produce Useful Information By Themselves. It Was Highlighted That Sometimes It Was Not Easy To Find Bad This In Data Because Of Security.

9.1.5 Transparency

i) Thirteen Participants (54 %) Were With The Opinion That The Data Produced By The Youth Were Transparent.

ii) Nine Participants (38%), Highlighted That The Data Produced By Youth Was Not Quite Transparent. Some Feared Their Parents If They Could Come Across The Data There Would Be Some Misunderstandings. In Addition Data Encryption Or Passwords Were Used To Disguise The Information To Other People Because At Times The Data Might Have Been Copied Of Stolen. It Might Be Fraudulent Data As Well.

iii) Two Participants (8%) Were Caught In Between. It Was Indicated That At Times It Is Transparent And At Times It Is Not.

9.2 What Ethical Behaviours Are For And Against Enhanced Data Security Among Youth In Zimbabwe?

The Above Research Question Was Used To Analyse The Following Four Themes

9.2.1 Honesty

I) Sixteen Participants (67%) Of The Sample Honesty Were In Agreement That When Producing Data And Documents To Curb Fights And Misunderstandings That Might Lead To Someone Being Apprehended By Police Misunderstanding And Fights. They Outlined That Intellectual Property Needed To Be Honoured. The Participants Indicated That, Data Honesty Improved Data Quality, Produce Accurate Information And The Data Will Be Easily Traceable When Lost As Well As Able To Identify Source Of Data. The Other Reasons For Honest Data That Were Mentioned Were That, The Information Would Be Reliable And It Enhances Data Security And Expose The Threats That May Have Affected The Data.

Ii) Four Participants (8%) Indicated That Some Youths Are Not Honest, They Would Steal Someone's Work For Mischievous Reasons And They Do Not Respect The Honest Part Of Data.

iv) Two Participants (4%) Outlined That Some Youths Desist From Disclosing Honest Information Because They Fear Some People Will Judge Them According To That Information And Portray Wrong Narratives About Them Hence Dwelling On Their Weaknesses.

v) Two Participants (4%) Highlighted That It Ideal To Whistle-Blow If Anyone Gave Dishonest Information So That The Law Would Take Its Course.

9.2.2 Accountability

I) Eighteen Participants (75%) Outlined That A Person Was Supposed To Own Or Accept The Data If The Data Was Compiled In Good Faith. They Suggested That Sensitive Information Needed To Be Shared Personally. They Indicated That If People Were Accountable To Their Data They Would Work Responsibly Because They Would Fear To Be Humiliated In The Event That The Data Is Inaccurate And Also Not Consistent. The Participants Outlined That If Someone Is Accountable For Her Data It Was Easier To Identify The Originator Of The Data Without Prejudice Or Malice And People Would Come Up With Trustworthy Documents. They Mentioned That It Was Necessary To Filter The Data. Accountability Was Said To Reduce Cyber Bullying.

Ii) Two Participants (8%) Indicated That There Was No Action Taken Upon Who Broke The Law In Tempering With Data, Eg Plagiarism, Phishing, And People Did Not Honor Their Mistakes.

iv) Three Participants (13%) Outlined That Youth Tend To Produce Biased Data.

v) One Participant (4%) Indicated That Accountability Of Data Was Not Necessary.

9.2.3 Integrity

I) Twenty Participants (83%) Were Of The Opinion That Integrity Of Data Was Very Vital If Observed Accordingly, In Order To Protect Cultural Heritage, Not Sharing Data Where It Is Not Needed. Integrity Of Data Makes It Possible To See If There Are Any Breaches Of Data. It Improved Data Quality As Well As Increasing Authenticity. The Participants Highlighted That The Data Became Reliable And Understandable As Well As Accurate And Consistent. Plagiarism And Piracy Would Be Easily Be Identified. They Mentioned That If Data Is Up To The Required Standard, It Was Easy To Identify Its Loopholes Especially In Groups. If Something Fishy Enters The Group, It Is Easily Identified. Integrity Needed To Be Maintained In Order To Get Respect From The Community.

Ii) Three Participants (13%) Outlined That The Data By Youths Was Not Genuine Because Of Hackers And Mischief, So As A Result The Data Is Not So Useful.

iv) One Participant (4%) Outlined That There Were Limited Resources In Order To Produce Data With Integrity.

9.2.3 Transparency

I) Seventeen Participants (71%) Outlined That If The Da Was Transparent It Was Going To Be Easy To Analyse, No Challenges Of Breaches Would Be Experienced, Recovery Of Data Would Be Made Easy, It Would Help The Data To Be Easily Traceable In The Event That It Is Lost. They Also Mentioned That It Was Easy To Identify The Originator Of The Data Or Document And Breaches Were Easily Identified, Then Security Would Be Increased If Need Arises. The Participants Indicated That If There Is Transparency, Data Became Reliable And No Cyber Bullying Would Be Experience. Again They Mentioned That If The Data Was Transparent, No Back-Biting Would Be Experienced, Inn Times When Others Would Peep To Check The Data Without His/Her Consent.

Ii) Seven Participants (29%) Highlighted That It Was Difficult To Maintain Transparency Of Data Since People Came From Different Backgrounds. The Also Mentioned That Data Could Be Used For Unintended Purpose And Also Can Be Hacked.

9.3 Recommendations From Participants

The Current Study Evidence Generally Shows That Enhanced Data Security Is Affected By Several Data Breaches, Hence The Researcher Came Up With The Following Suggestions.

I) Use Of Disguised Names In Order To Conceal Identity Of The Information. Some Of The Information Is Hidden In Vaults. Some Files Are Hidden As Well. This Would Make It Difficult To Tress The Perpetrator Of Breach Of Data Ethics.

Ii) Participants Outlined That They Were Not Aware Of The Policies Pertaining To Data Protection And They Suggested That Comprehensive Policies On Data Security And Protection Be Crafted By The Government Through The Ministry Of Ict.

iii) Programs On Teaching The Youth On The Effects Of Plagiarism And Cyberbullying Needed To Be Rolled Out By The Government Through The Tertiary Institutions.

iv) Government Needed To Protect The General Public In Protecting Devices From Hackers.

v) The Government Needed To Come Up With More Secure Technology.

vi) Anti-Virus And Anti-Malware Are Very Expensive In Zimbabwe.

10 Major Findings

The Researchersare Going To Outline Some Of The Major Findings.

I) As A Country There Is Need To Produce Our Own Antivirus And Anti-Malware Software In Order To Reduce Prices. Imported Software Is Expensive. Foreign Countries Can Easily Spoof Information Through The Anti-Virus Programs. They Can Filter Data And Use The Data For Whatever They Want. Even Using It For Mischievous Activities.

Ii) The Government Needed To Support Developers Or Innovators Of Anti-Virus Or Anti-Malware Software So That They Are Produced Locally, By Funding The Research Department In Order To Get Cheaper Software.

Iii) Youths Needed To Follow Ethical Behavior Pertaining To Security Of Data Laid Down By The Government In Order To Get Enhanced Data If Ever That Policy Exist.

Iv) 70% Of The Participants Disclosed That Security, Honesty And Transparency Were The Drivers Of Getting Enhanced Data Security And Cybersecurity Needed To Be Enhanced Through The Government Arms Concerned.

V) It Was Emphasised That Law Needed To Be Enforced To Punish The Perpetrators Of Breaching The Security Of Data Eg, Phishing, Cyberbullying And Hacking.

Vi) It Was Suggested That It Was A Requirement That Youth Be Trustworthy In Relation To Issues Concerning Data Security Especially To Issues Concerning Intellectual Security As Discovered By The Study That, The Youth Were Not Respecting Intellectual Property. Plagiarism Was Being Extensively Practiced.

Vii) Participants Outlined That The Zimbabwe Government Need To Roll Out Awareness Campaigns Pertaining To Ethical Behavior That Is In Line With Security Of Data In Zimbabwe. The Awareness Campaigns Could Be Done On Television, Radio, Road Shows Of Bill Boards.

11 Discussion

After Analyzing The Findings It Is Concluded That Cyberbullying And Plagiarism Are The Most Data Breaches Being Practiced By The Youth. Some Are Doing Knowingly And Some Out Of Ignorance And Other Are Doing Under Peer Pressure. It Was Discovered That 80% Of The Participants Are Not Aware Of The Policies Regarding Data Security In Zimbabwe. The Responsible Authority Was Not Cascading The Information Pertaining To Data Security In Zimbabwe To The General Public Including The Youth.

Based On This Research There Could Be A Need For The Country To Craft A Data Security Policy Written In All Official Languages In Zimbabwe So That No One Is Left Behind. It Is Also Important For The Government To Come Up With Affordable Anti-Virus Software In Order To Benefit Even The Underprivileged And Also To Protect Our Data From Foreigners.

It Was Also Noted That Transparency, Security And Honesty Were The Key Drivers Of Coming Up With Enhanced Data.

12 Conclusion

Based On The Above Findings It Is Concluded That Most Of The Youths Are Not Familiar With The Ethical Behavior Pertaining To Enhanced Data Security. They Are Not Even Aware Whether There Are Policies In Relation To Data Security In Zimbabwe. Data Security Awareness Campaigns Are A Priority. The Information Need To Be Cascaded To The General Public And Youth. Lawis Supposed To Be Enforced To Those Who Breach The Laws Of Data Security. Government Need To Consider Developing Their Own Anti-Virus Packages In Order To Have Enhanced Data Security.

13 Recommendations

13.1 Government Has To Come Up With Data Protection Act That Has To Be Cascaded To The General Public. It Has To Be Written In All Official Languages In Zimbabwe.

13.2 The Government Needed To Support Developers Or Innovators Of Anti-Virus Or Anti-Malware Software So That They Are Produced Locally, By Funding The Research Department In Order To Get Cheaper Software.

13.3 Enforcement Of Laws To Those Who Share Sensitive Information Without Consent Is A Priority.

13.4 Awareness Campaigns On Ethical Behavior Towards Data Security Need To Be Rolled Out As A Matter Of Urgency By The Government Though The Ministry Of Ict. This Can Be Done Through Radios, Television, The Internet, Road Shows, Newspapers, Or Bill Boards.

14 References

- Adeniyi, A, And Ocholia, D, N, 2019, Ethical Behaviour Among Undergraduate Students In Selected African Universities: An Overview , Https://Www.Researchgate.Net/Publication/335961179.

- Havard Business School Online, Five Principles Of Data Ethics

- Mapuvire D, H, And Mapuvire V, 2022, Social Media And Behaviour : A Case Of The Ruwa Youths In Harare, Online Sabinet, African Journals.

- Martin K, Wei R, Peh C, Tembo M, Mavodza C, V, Doyle A, M, Dziva C, Dauya E, Bandason T, Azizi S, Simms V, Ferrand R, A, 2024,Factors Associated With The Use Of Digital Technology Among Youth In Zimbabwe: Findings From Cross-Sectional Population Based Survey, Journal Of Medical Internet Research, Vol. 26, Science Direct.
- Mutunhu B, Dube S, Ncube N, Sibanda S, 2022, Cyber Security Awareness And Educationframework For Zimbabwe Universities: A Case Of National University Of Science And Technology, 2022, International Conference Of Industrial Engineering And Operations Management, Nsukka, Nigeria.

- Alharbi T, And Tassaddiq A, 2021, Assessment Of Cybersecurity Awareness Among Students Of Majmaah University, Mdpi

Wanbil W, Lee And Wolfgang Z, 2016, An Ethical Approach To Data Privacy Protection