Plan Overview

A Data Management Plan created using DMP Tool

Title: Financial Literacy Challenges

Creator: Mohamed Khashbah

Affiliation: Claremont Graduate University (cgu.edu)

Funder: Digital Curation Centre (dcc.ac.uk)

Template: Digital Curation Centre

Last modified: 07-08-2024

Financial Literacy Challenges

Data Collection

What data will you collect or create?

Appendix . Questionnaire:

How will the data be collected or created?

Questionnaires/Surveys: The primary method of data collection here is a structured questionnaire, as indicated by the multiple-choice format and Likert-scale questions. Respondents will select their answers from the provided options or rate their agreement with the statements.
Digital Platforms: If the questionnaire is administered online (e.g., via a platform like SurveyMonkey, Google Forms, or Qualtrics), then data will be automatically recorded and stored on the platform. This can help in collecting data from a larger and more diverse audience quickly.
Physical Paper Surveys: If the questionnaires are administered in a traditional paper format, the responses would need to be manually entered into a digital system for analysis.
Interviews: Some of the open-ended questions, or those that may require elaboration, could benefit from face-to-face or telephonic interviews, allowing for more in-depth responses.

Documentation and Metadata

What documentation and metadata will accompany the data?

Appendix A: Questionnaire

First: Demographic Data

Gender
- [ ] Male
- [ ] Female

1. Age
- [ ] Less than 30 years old
- [ ] From 30 to 50 years old
- [ ] Over 50 years old

2. Educational Level
- [ ] Bachelors Degree
- [ ] Middle Certification
- [ ] Basic Education

3. The Service Used
- [ ] ATM Service
- [ ] Mobile Banking

4. Bank Name
Please select your bank from the list below (write the corresponding number):

1. Egypt Bank
2. National Bank
3. The Egyptian Arab Land Bank
4. Main Bank for Development and Agricultural Credit
5. Emirates NBD Bank
6. Cairo Bank
7. United Bank
8. Alex Bank
9. Qatar National Al Ahli Bank
10. Arab Investment Bank
11. Piraeus Bank
12. Audi Bank
13. The Bank of Nova Scotia
14. Ahli United Bank
15. Faisal Islamic Bank
16. Housing & Development Bank
17. Al Baraka Bank
18. National Bank of Kuwait
19. Abu Dhabi Islamic Bank
20. Union National Bank
21. Egyptian Gulf Bank
22. HSBC Bank
23. Arab Banking Corporation Bank
24. Egyptian Bank for Export Development
25. Arab International Bank
26. National Bank of Oman
27. Misr Iran Development Bank
28. Commercial International Bank
29. Barclays
30. Arab International Banking Company Bank
31. Blom Bank
32. Credit Agricole Bank
33. Suez Canal Bank
34. Arab African International Bank
35. Abu Medical National Bank
36. Arab Bank
37. Mashreq Bank
38. National Bank of Greece

Second. Independent variables: (Baabdullah et al., 2019, Çera et al., 2020, Gunawan et al., 2021, Banthia and Dey, 2022, Masoud and Basahel, 2023)

EAES (Easy Access to Electronic Services)

Please rate the following statements based on your level of agreement:

Legend:
1 = Strongly Disagree
2 = Disagree

3 = Neutral
4 = Agree
5 = Strongly Agree

1. I use electronic payment methods to pay my bills.
Rating: _____

2. I am good at handling day-to-day financial matters, such as checking accounts and credit and debit cards.
Rating: _____

3. Banking services make it easier for customers to access necessary electronic services.
Rating: _____

4. Easy access to electronic services enhances technology utilization in financial forecasting and planning.
Rating: _____

5. I have the ability to analyze my personal account data and manage my personal accounts.
Rating: _____

6. There is an ease in finding help or technical support when using electronic banking applications.
Rating: _____

7. You can easily find the information or service you want through electronic banking services.
Rating: _____

8. The digital content of electronic banking services is understandable and easy to use.
Rating: _____

9. You think banks should invest more in educating customers about electronic banking.
Rating: _____

10. Have confidence in using ATMs for functions other than withdrawing cash, such as money transfers and bill payments.
Rating: _____

QEFS (Quality Of Electronic Financial Services)

For each of the following statements, please indicate your level of agreement or answer the question accordingly:

11. My interactions with the bank occur through both traditional and digital channels.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

12. The bank designs its digital content to be user-friendly.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

13. I believe my bank stays updated with the latest electronic banking technologies.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

14. The bank provides me with timely updates about the information in my account.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

15. Electronic banking operations help maximize the benefits of electronic service quality for clients.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

16. The bank provides all information related to banking services that have an impact on the level of financial culture among customers.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

17. The bank's protection of customers' information has an impact on the quality of the electronic financial service.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

18. Do you encounter any technical problems while using the electronic services?

Yes
No

If yes, please specify: _____

19. You feel that the bank acts promptly on complaints you make.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

20. How would you rate your bank's electronic features compared to those offered by other banks?

Much Worse
Somewhat Worse
About the Same
Somewhat Better
Much Better

EF (Electronic Flexibility)

Please indicate your level of agreement with the following statements or answer the questions accordingly:

21. I find flexibility in managing my electronic financial accounts.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

22. The diversity of electronic banking services has a positive impact.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

23. Digital channels for banking services increase customer loyalty.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

24. Financial transformation is realized when information is available on the behavior and needs of the bank's customers, which improves banking service.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

25. Customers adapt to the digital transformation processes designed by the bank.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

26. The digital transformation of electronic banking services achieves efficiency and flexibility in using these services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

27. Digital technologies provide the ability to perform integrated electronic banking operations.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

28. Digital channels provide the benefits of communication and rapid response in electronic banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

29. Would you recommend your bank's online banking services to a friend or family member?

Definitely Not
Probably Not
Neutral/Unsure
Probably Yes
Definitely Yes

30. In the event of discrepancies in your account, you are faced with the ease of reporting and correction through electronic services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

FK (Financial Knowledge)

Please indicate your level of agreement with the following statements or answer the questions accordingly:

31. I'm knowledgeable in using various electronic financial services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

32. I possess the financial knowledge to manage my personal accounts effectively.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

33. Banks should produce awareness programs to enhance customers' financial knowledge.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

34. The bank provides customers with guidebooks related to the types of electronic banking services to raise their level of financial knowledge.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

35. I have the knowledge to make bank transfers through the electronic banking services available to me.

Strongly Disagree
Disagree
Neutral
Agree

Strongly Agree

36. I have the ability and knowledge to review my financial activities through my online account.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

37. I have the knowledge and ability to make financial investments through electronic banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

38. You can attend or search for financial literacy seminars or workshops offered by the bank.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

39. You think that your level of financial literacy affects your confidence in electronic banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

40. You believe that electronic payment methods are more efficient than traditional methods.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

Third: dependent variables- 1-(Risk of Technique(RT) (Abdou et al., 2014, Abdou et al., 2015, Sonono and Ortstad, 2017, Dehnert and Schumann, 2022, Icardi, 2022)

1. I'm concerned that the banking system might be vulnerable to cyber threats.

Strongly Disagree
Disagree
Neutral

Agree
Strongly Agree

2. Concerns about technological risks deter me from switching from traditional to digital banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

3. I'm hesitant to use electronic banking due to potential data loss risks.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

4. The Bank ensures the integrity of electronic banking transaction data and customer records.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

5. The Bank takes measures to ensure the confidentiality of customers' electronic banking information.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

6. The bank has the capacity for business continuity and contingency planning to ensure the availability of effective electronic banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

7. The Bank shall take appropriate measures to confirm the identity of customers who conduct their banking business electronically.

Strongly Disagree
Disagree
Neutral
Agree

Strongly Agree

8. The bank provides easy access to electronic banking systems, databases, and applications.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

9. People ask me how to use electronic banking services due to the difficulty of using them.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

10. To what extent do you not want to move from traditional banking services to digital ones that are hindered by the risks of technology?

Not at all
Slightly
Moderately
Very Much
Extremely

11. Does the bank's customer service department cooperate with customers who face difficulties using electronic technologies?

Yes
No
Not Sure

12. The Bank has established clear audit trails for electronic banking transactions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

13. You think there is a need for more financial education sessions on the risks of electronic banking.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

14. You update your data when prompted by various electronic banking services programs.

Always
Often
Sometimes
Rarely
Never

2-Risk of Cheating and Fraudulence(RCF)

15. Concerns about data privacy deter me from switching from traditional to digital banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

16. Using electronic banking reduces the need to carry cash and the associated risks.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

17. There are significant legal and security issues with electronic banking.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

18. Electronic banking services seem to lack robust information security.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

19. I am cautious about using electronic banking services to avoid the chance of fraud that I may face.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

20. The Bank has planning to respond to incidents of fraud and cheat.

Yes
No

Not Sure

21. I feel safe in dealing with electronic banking services.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

22. The Bank has appropriate disclosures for electronic banking services.

Yes
No
Not Sure

23. You regularly update or change your passwords for your online banking services.

Always
Often
Sometimes
Rarely
Never

24. Your online banking application notifies you of any unusual account activity.

Always
Often
Sometimes
Rarely
Never

3-Making Finance Decision(MFD)

25. I feel anxious and uncomfortable when making electronic financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

26. Would you prefer making digital financial decisions if they offered more personalized and improved decision-making?

Yes
No
Maybe

27. Electronic banking services enhance the quality of my financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

28. The use of electronic banking services saves time when making financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

29. Services provide updated information to facilitate the process of making financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

30. The bank gives customers financial advice when making financial decisions about their investments.

Always
Often
Sometimes
Rarely
Never

31. I often show my friends or family the electronic banking products and services that I use.

Always
Often
Sometimes
Rarely
Never

32. The provided electronic banking services fulfill their tasks when making any financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

33. Sometimes I feel helpless when I'm in the middle of making a financial decision using electronic banking services.

Strongly Disagree
Disagree

Neutral
Agree
Strongly Agree

34. Customers are having difficulties reaching out for information when making financial decisions because it is insufficient on the website.

Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

35. The Bank uses appropriate measures to ensure the separation of financial decisions.

Yes
No
Not Sure

36. The level of my financial knowledge affects my confidence in making financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

37. You feel that electronic banking services provide sufficient data for you to make informed financial decisions.

Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

38. Customers feel dissatisfied when a problem occurs during their financial decision-making process.

Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree

39. Rely on various electronic banking applications when making investment decisions.

Always
Often
Sometimes
Rarely
Never

40. Makes financial decisions based on information from electronic banking applications.

Always
Often
Sometimes
Rarely
Never

Ethics and Legal Compliance

How will you manage any ethical issues?

Informed Consent:

Ensure participants know the purpose of the data collection, how their data will be used, and any potential risks involved.
Obtain explicit consent, preferably written, before collecting any data.
Anonymize Data:

Strip away personally identifiable information (PII) to protect participants' privacy.
Use pseudonyms, codes, or other anonymization techniques.
Transparency:

Be transparent about the methods of data collection, sources of data, and the purpose of the study.
Share findings openly, but without compromising data privacy.
Data Security:

Use encryption, secure databases, and other methods to ensure data is stored securely.
Regularly update security protocols and software to protect against breaches.

How will you manage copyright and Intellectual Property Rights (IP/IPR) issues?

Question not answered.

Storage and Backup

How will the data be stored and backed up during the research?

Primary Storage:

Cloud Storage: Platforms like Google Drive, Dropbox, Microsoft OneDrive, or specialized research data platforms can be used. They offer real-time syncing, version history, and accessibility from different devices and locations.
Local Storage: Use dedicated servers or high-quality external hard drives or SSDs for storing data.
Data Encryption:

Encrypt data at rest and in transit. Tools like VeraCrypt or BitLocker can be used for encrypting data on local drives. Many cloud platforms offer encryption as a built-in feature.
Regular Backups:

Automated Backups: Set up automated backups to run at regular intervals, ensuring that recent data changes are always saved.
Offsite Backups: Store backup copies in a different physical location from the primary data. This can be achieved using cloud platforms or by manually taking external drive backups to a different location.
Version Control:

Use version control systems like Git (combined with platforms like GitHub or GitLab) for datasets and code. This allows for tracking changes, rolling back to previous versions, and collaboration.
Redundancy:

Maintain multiple copies of data on different storage mediums and/or locations. For example, if using a local server and a cloud storage provider, you have two copies in different places.
Physical Security:

If storing data on local servers or external drives, ensure they're kept in a secure location, such as a locked room or cabinet, to prevent theft or damage.
Consider using fireproof and waterproof safes for critical backups.
Access Control:

Limit access to the data to only those who need it. Use strong, unique passwords and consider two-factor authentication if the platform supports it.
Assign different user roles and permissions as needed. For instance, some team members might only have read access, while others can edit.
Regular Audit and Testing:

Periodically test backup processes to ensure they're working as expected. Restore data from a backup to a separate location to verify its integrity.
Audit who has access to the data and adjust permissions as necessary.
Metadata and Documentation:

Store metadata and documentation alongside the data. This includes information about the data format, collection methods, data dictionaries, and any transformations applied to the data.
Data Lifecycle Management:
Consider how long the data needs to be kept. Set up policies for archiving or deleting old data, ensuring compliance with any legal or institutional data retention policies.

How will you manage access and security?

User Authentication:

Strong Password Policies: Require complex passwords and change them periodically. Implement policies such as minimum password length, mandatory use of numbers, symbols, and both uppercase and lowercase letters.
Two-Factor Authentication (2FA): Implement 2FA for added security. This often involves receiving a code on a mobile device or email, in addition to entering a password.
Access Control:

Role-Based Access Control (RBAC): Assign roles to users based on their responsibilities in the research. Roles determine the level and type of access a user has. For instance, some might only have read access, while others can edit or delete data.
Principle of Least Privilege (PoLP): Provide only the minimal essential access rights or permissions necessary to perform a function.
Data Encryption:

At Rest: Encrypt data when it's stored on servers or external drives using tools like BitLocker or VeraCrypt.
In Transit: Ensure data is encrypted during transmission using protocols like TLS/SSL.
Regular Audits:

Periodically review and audit access logs and permissions. Check who accessed what data and when. Investigate any anomalies or unexpected access patterns.
Physical Security:

Ensure servers and storage devices are in secure locations, like locked rooms or cabinets. This prevents unauthorized physical access.
Use security cameras and alarm systems in places where sensitive data is stored.
Firewalls and Network Security:

Use firewalls to monitor and control incoming and outgoing network traffic.
Segment the network to ensure sensitive data is separated from general traffic.
Anti-Malware Software:

Install and regularly update anti-malware software to protect against viruses, ransomware, and other malicious threats.
Data Backups:

Regularly backup data and ensure backups are also secure. Consider encrypting backups and storing them in a separate secure location.
Secure Data Sharing:

If data needs to be shared, use secure methods such as encrypted file transfers or secure file-sharing platforms.
Avoid sharing sensitive data via email unless it's encrypted.

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

Question not answered.

What is the long-term preservation plan for the dataset?

Question not answered.

Data Sharing

How will you share the data?

Question not answered.

Are any restrictions on data sharing required?

Yes, several restrictions on data sharing might be required based on the nature and sensitivity of the data, the source of the data, ethical considerations, legal obligations, and stakeholder agreements. Here are some common restrictions on data sharing:

Personal and Sensitive Information:

Data that contains personally identifiable information (PII) or other sensitive details must be treated with caution. Sharing such data without proper anonymization or pseudonymization could breach privacy laws, such as the General Data Protection Regulation (GDPR).
Intellectual Property:

Data resulting from research might be subject to intellectual property rights, such as patents or copyrights. Sharing this data might infringe on these rights or hinder the ability to obtain future rights.
Consent Limitations:

If data was collected under specific consent agreements (e.g., surveys, interviews), it might stipulate that the data is only to be used for certain purposes and not be shared beyond the research team.
National Security:

Data that has implications for national security or contains state secrets might be subject to stringent restrictions or classified and hence cannot be shared.
Trade Secrets and Commercial Interests:

Data that reveals trade secrets, business strategies, or any other proprietary information can't be shared as it might jeopardize business interests or give unfair advantages to competitors.
Third-Party Agreements:

Sometimes data is obtained under licenses or agreements with third parties, which may impose sharing restrictions.
Data that Reveals Locations of Vulnerable Entities:

For example, data showing the locations of endangered species should not be openly shared as it might make them targets for poachers.
Ethical Considerations:

Some data, even if not personally identifiable, might be ethically sensitive. For instance, data regarding vulnerable populations or controversial topics might need restrictions to prevent misuse.
Legal Restrictions:

There are often legal obligations or restrictions on sharing data, especially across borders. For instance, health data in many countries is subject to strict regulations.

Responsibilities and Resources

Who will be responsible for data management?

Question not answered.

What resources will you require to deliver your plan?
