

Task 1 Project Proposal

27 November 2025 15:51

Stefania Mioara Ionescu

2336875

Module : Changemakers: Creativity and Value Creation

ACCA5033

Innovation & Business Practice

Project Proposal (Mind map)

Task 1: Mind Map – Ideation & Innovation

Central Node: Innovation & Creativity in Society

Innovation and creativity are key drivers in shaping societal progress, technological evolution, and personal development. According to Christensen (2013), innovation reshapes industries by introducing new value propositions that alter how people live and work. Creativity acts as the foundation of innovation, enabling individuals and organisations to conceptualise novel ideas that can be transformed into impactful solutions (Runco & Acar, 2012).

Node 1: Role of Innovation in Society

Economic Growth: Technological advancements drive productivity, new markets, and employment. The World Economic Forum (2020) highlights innovation as a lynchpin for national competitiveness.

Technological Advancement: Breakthroughs such as AI, mobile technology, and automation transform communication, healthcare, and mobility.

Social Progress: Innovations like renewable energy and digital learning platforms help address global challenges.

Node 2: Creativity & The Individual

Self-development: Creativity encourages problem-solving, exploration, and critical thinking. According to Amabile (1996), intrinsic motivation and open thinking enable individuals to generate original ideas.

Entrepreneurial Mindset: Creative individuals are more likely to identify unmet needs and propose new solutions.

Skills for the Future: Modern careers demand adaptability, ideation skills, and digital literacy.

Node 3: Sources of Innovation

Technological Drivers: AI, cloud computing, data analytics, cybersecurity trends.

Market Needs: Customer pain points push industries to innovate more rapidly.

Cultural Change: Increasing digital adoption encourages modern, user-centric solutions.

Sustainability Pressures: Climate issues promote eco-innovation and green technologies (OECD, 2018).

Node 4: Programme-Related Themes (Computing / Technology)

Since this project connects to your technology-focused programme of study, relevant concept nodes include:

Software Solutions: Mobile apps, automation tools, dashboards.

Cybersecurity: Threat mitigation, secure authentication, intrusion detection.

Data & AI: Personalisation systems, predictive analytics, machine learning.

Digital Innovation: Smart systems, cloud computing, IoT integration.

Human-Computer Interaction (HCI): UX/UI design, assistive technology.

Node 5: Personal-Interest Project Ideas

These ideas reflect innovation themes alongside typical computing-related interests:

AI-Powered Study Assistant

Uses NLP to summarise notes, create flashcards, and support revision.

Helps students overcome information overload.

Cybersecurity Awareness App

A gamified mobile tool teaching secure behaviour (password hygiene, phishing detection).

Aligns with real-world cybersecurity gaps.

Health-Tracking Dashboard for Mental Wellbeing

Integrates wearable data to provide wellbeing insights.

Uses AI to flag unhealthy behavioural patterns.

Smart Home Efficiency Monitor

Suggests energy-saving recommendations using IoT data.

Supports sustainability innovation.

Scrabble-Training Software (linked to your course project)

Word recommendation engine.

Timed challenges for vocabulary building.

Node 6: Selected Project Idea

Chosen Project: Cybersecurity Awareness Application

This project has been selected because cybersecurity is an essential global challenge, and many breaches still occur due to human error. The National Cyber Security Centre (2023) reports that phishing attacks and weak passwords remain the most common

vulnerabilities. A gamified awareness app can:

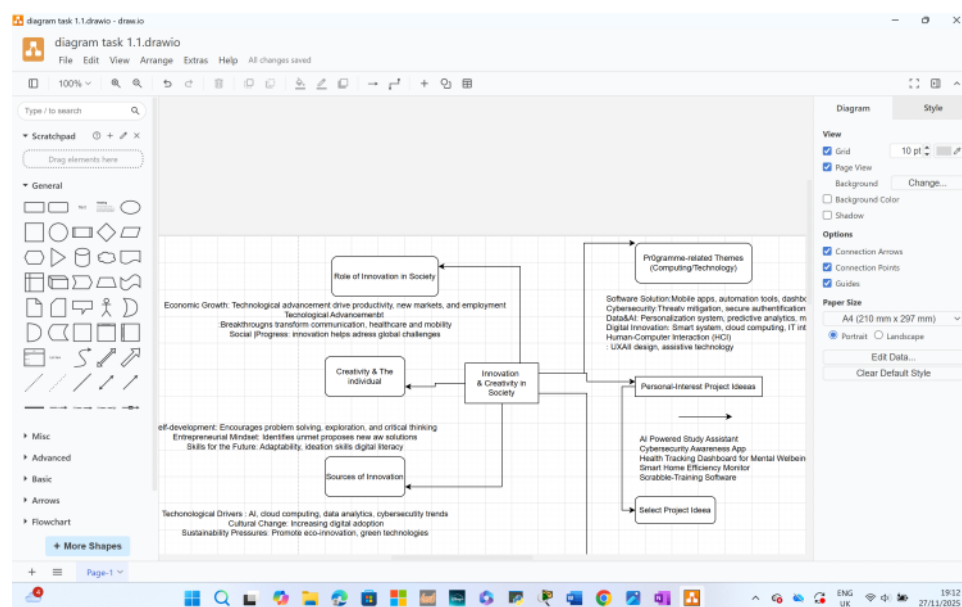
Provide real-time simulated phishing challenges.

Teach behavioural security through micro-learning.

Offer scenario-based quizzes and rewards.

Increase user engagement compared to traditional training modules.

The project strongly aligns with innovation themes—blending technology, creativity, and societal need by aiming to reduce cyber-threat exposure through education.



Task 2: Aim, Objectives & Research Area

Q1. Aim and Objectives

Project Aim

The aim of this project is to design and develop an interactive Cybersecurity Awareness Application that educates users on common cyber threats—such as phishing, weak passwords, and social engineering—through gamified learning experiences and scenario-based challenges. The application seeks to improve user cybersecurity behaviour by increasing awareness, strengthening digital literacy, and encouraging safe online practices.

Project Objectives

To identify and analyse the most common user-related cybersecurity vulnerabilities, including phishing susceptibility, poor password hygiene, and unsafe browsing behaviours.

To design a user-friendly mobile or web-based interface using usability principles that promote engagement and motivation.

To incorporate gamification elements (e.g., quizzes, points, levels, badges) shown to improve learning retention and behavioural change.

To develop a prototype cybersecurity awareness system that delivers micro-learning modules and real-world threat simulations.

To evaluate user engagement and knowledge improvement through testing sessions, feedback surveys, and performance metrics.

To propose recommendations for future improvements, scalability, and integration with organisational security training programmes.

Q2. Research Philosophy

Choosing an appropriate research philosophy is essential to ensure that the project's methods align with its goals. For this project, Pragmatism is the most suitable research philosophy.

Pragmatism focuses on practical solutions and outcomes, prioritising methods that effectively address real-world problems (Creswell & Creswell, 2018). Since cybersecurity behaviour is a human-centred challenge, pragmatic research allows for combining both quantitative and qualitative data to generate actionable insights. The goal of the Cybersecurity Awareness Application is not merely to theorise about threats but to create a functional technological intervention that improves user behaviour, which aligns closely with the pragmatic emphasis on usefulness and problem-solving (Morgan, 2014).

Furthermore, cybersecurity awareness research frequently uses mixed methods—such as surveys to measure awareness levels, usability testing to evaluate design choices, and behavioural assessments to track improvement (Parsons et al., 2017).

Pragmatism supports this flexible methodological approach, enabling

the project to draw upon varied evidence to understand user interactions, motivation, and learning outcomes.

In contrast, positivism alone would be too restrictive, as it focuses exclusively on measurable outcomes and overlooks user experience and perceptions. Interpretivism alone may overemphasise subjective experiences and lack the empirical robustness needed in cybersecurity research. Pragmatism, therefore, provides a balanced and practical foundation for designing, implementing, and evaluating the proposed solution.

Q3. Research Tools, Databases, and Search Strategies

Effective research requires the use of suitable academic databases and search tools to gather reliable information on cybersecurity, user behaviour, and digital learning technologies.

Research Tools and Databases

The following databases are well-suited for locating scholarly and industry-based cybersecurity research:

IEEE Xplore – Provides peer-reviewed papers on cybersecurity systems, authentication, threat detection, and software solutions.

ACM Digital Library – Contains research on human-computer interaction (HCI), gamification, and cyber awareness training.

ScienceDirect – A large database of journals covering behavioural cybersecurity, digital education, and software engineering.

Google Scholar – A broad research tool useful for finding grey literature, conference papers, and citations across disciplines.

NCSC & ENISA Publications – Industry reports offering up-to-date insights into threat trends and human-factor vulnerabilities.

These databases are appropriate because they offer high-quality peer-reviewed research, technical studies, and behavioural insights—all essential for a hybrid technological and educational project.

Search Strategies

To locate relevant research, the following search strategies were applied:

Boolean operators

("cybersecurity awareness" AND gamification)

("phishing training" OR "security behaviour")

("user behaviour" AND "cyber threats")

Advanced filtering

Publication dates (last 5–10 years for current threat relevance)

Peer-reviewed journal articles

Keywords related to HCI and UX design

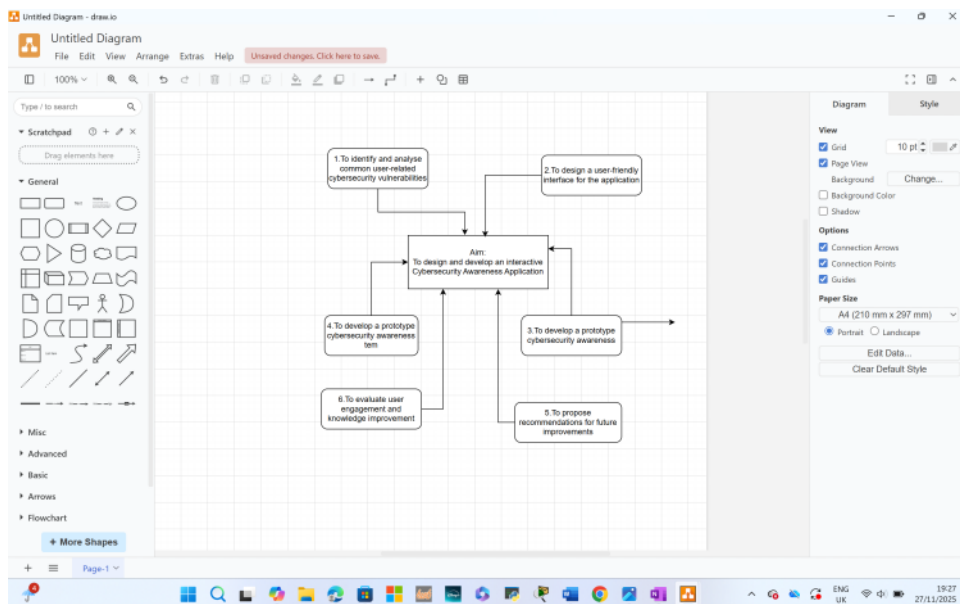
Citation chaining

Reviewing reference lists of key papers to identify influential studies.

Keyword variations

“digital literacy”, “security education”, “risk perception”,
“behavioural cybersecurity”.

These strategies ensure a thorough and systematic search process, producing reliable and relevant research that supports design decisions, understanding of the target audience, and evaluation methods.



Task 3: Research Strategies

Q1. Strategies to Enhance Validity, Reliability, Generalisability & Ethical Considerations

Ensuring high-quality research requires carefully planned strategies that enhance validity, reliability, generalisability, and ethical integrity. For the Cybersecurity Awareness Application project, these components are critical, as the research involves human participants and the collection of behavioural insights.

Validity

Validity refers to how accurately a method measures what it intends to measure (Creswell & Creswell, 2018). To strengthen validity in this project:

Triangulation will be used by combining multiple data sources, such as user surveys, usability testing, and system analytics.

Clear operational definitions will be applied when measuring cybersecurity awareness (e.g., phishing detection accuracy, password strength rating).

Pilot testing (described in section Q2) will help refine questions and remove ambiguities.

Using validated instruments, such as adapted components from the

Human Aspects of Information Security Questionnaire (HAIS-Q), will improve construct validity (Parsons et al., 2017).

Reliability

Reliability refers to the consistency of results (Saunders et al., 2019). To enhance reliability:

Standardised procedures will be used during usability testing so all participants follow identical instructions.

Survey questions will be designed using consistent scales (e.g., 5-point Likert scale).

Internal consistency will be checked using Cronbach's Alpha if multiple survey items measure similar concepts.

Generalisability

Generalisability concerns how well findings can apply to a broader population. Although the project focuses on a student-based sample, generalisability will be improved by:

Using a diverse sample across age, study discipline and digital skill level.

Conducting testing with individuals who represent typical cybersecurity awareness needs.

Documenting contextual limitations and identifying pathways for broader testing in future versions.

Ethical Considerations

Cybersecurity-related research presents important ethical challenges. Key ethical strategies include:

Informed consent clearly outlining the voluntary nature of participation.

Avoiding exposure to real cyber threats; simulated threats will be safe and controlled.

Anonymisation of participant data to avoid identification.

Secure data storage, following GDPR principles for confidentiality and retention.

Providing participants with debriefing, including educational information about safe cybersecurity practices.

Q2. Research Strategies & Pilot Data Collection Method

Selected Research Strategies

This project uses a mixed-methods approach, consistent with the pragmatic research philosophy selected in Task 2. The main data collection methods include:

Online Surveys

To measure awareness levels, user confidence, and perception of cybersecurity risk.

Usability Testing of the Prototype

Participants complete tasks (e.g., identify phishing attempts) while observations and performance metrics are recorded.

Semi-structured Interviews or Feedback Forms

Collect qualitative insights on user experience, motivation, and interface design.

System Analytics

Track user behaviour—such as quiz completion rates or time spent on modules.

These strategies together provide both measurable outcomes and rich explanatory data.

Pilot Data Collection Method (For Appendix)

A pilot questionnaire was designed to test clarity, structure, and content relevance. The pilot included 6 students from mixed academic backgrounds. Sample pilot questions:

How confident are you in spotting phishing emails? (1–5 scale)

Which cybersecurity topics do you want to learn more about?
(Multiple selection)

Have you received formal cybersecurity training before? (Yes/No)

Would you prefer learning through videos, quizzes, or scenarios?

Feedback from Pilot

Participants indicated:

Likert scale questions were clear and easy to complete.

More examples of online threats should be included.

The questionnaire should clarify whether the app is mobile or web-based.

Add one open question for suggestions.

These refinements will be implemented in the final questionnaire used in the main study.

Q3. Types of Quantitative & Qualitative Analysis

Quantitative Analysis

Quantitative analysis involves numerical data and statistical testing. For this project:

Descriptive statistics (mean, frequency, percentages) will summarise awareness scores.

Inferential tests (paired t-tests) can measure improvements before and after interacting with the application.

Correlation analysis may be applied to examine relationships such as digital literacy vs. awareness improvement.

Qualitative Analysis

Qualitative analysis focuses on meaning, patterns, and themes.

Thematic analysis (Braun & Clarke, 2006) will be used to identify recurring themes from feedback and interviews.

Content analysis may be applied to categorise user comments related to usability.

Narrative analysis could help explore individual experiences with simulated cyber threats.

Using mixed analysis enables both behavioural measurement and understanding user motivations.

Reference List

- ✓ Amabile, T. (1996). Creativity in Context. Westview Press.
- ✓ Christensen, C. (2013). The Innovator's Dilemma. Harvard Business Review Press.
- ✓ OECD. (2018). Innovation and the Environment. OECD Publishing.
- ✓ Runco, M. & Acar, S. (2012). "Divergent Thinking as an Indicator of Creative Potential." Creativity Research Journal.
- ✓ World Economic Forum. (2020). Global Competitiveness Report.
- ✓ National Cyber Security Centre (2023). Cyber Threat Report.
- ✓ Creswell, J. & Creswell, D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage.
- ✓ Morgan, D. (2014). Pragmatism as a Paradigm for Social Research. Qualitative Inquiry.
- ✓ Parsons, K. et al. (2017). "The Human Aspects of Information Security Questionnaire (HAIS-Q)." Computers & Security.
- ✓ National Cyber Security Centre (NCSC). (2023). Cyber Threat Report.
- ✓ Braun, V. & Clarke, V. (2006). "Using Thematic Analysis in Psychology." Qualitative Research in Psychology.
- ✓ Creswell, J. & Creswell, D. (2018). Research Design. Sage.

- ✓ Parsons, K. et al. (2017). Human Aspects of Information Security Questionnaire.
- ✓ Saunders, M., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students. Pearson.