

Title

Thursday, 9 July 2026 2:54 pm

Project Proposal

Changemakers: Creativity & Value Creation

Name: Yevhen Lytko

Student Number: 2424747

Course: BSc Cyber Security

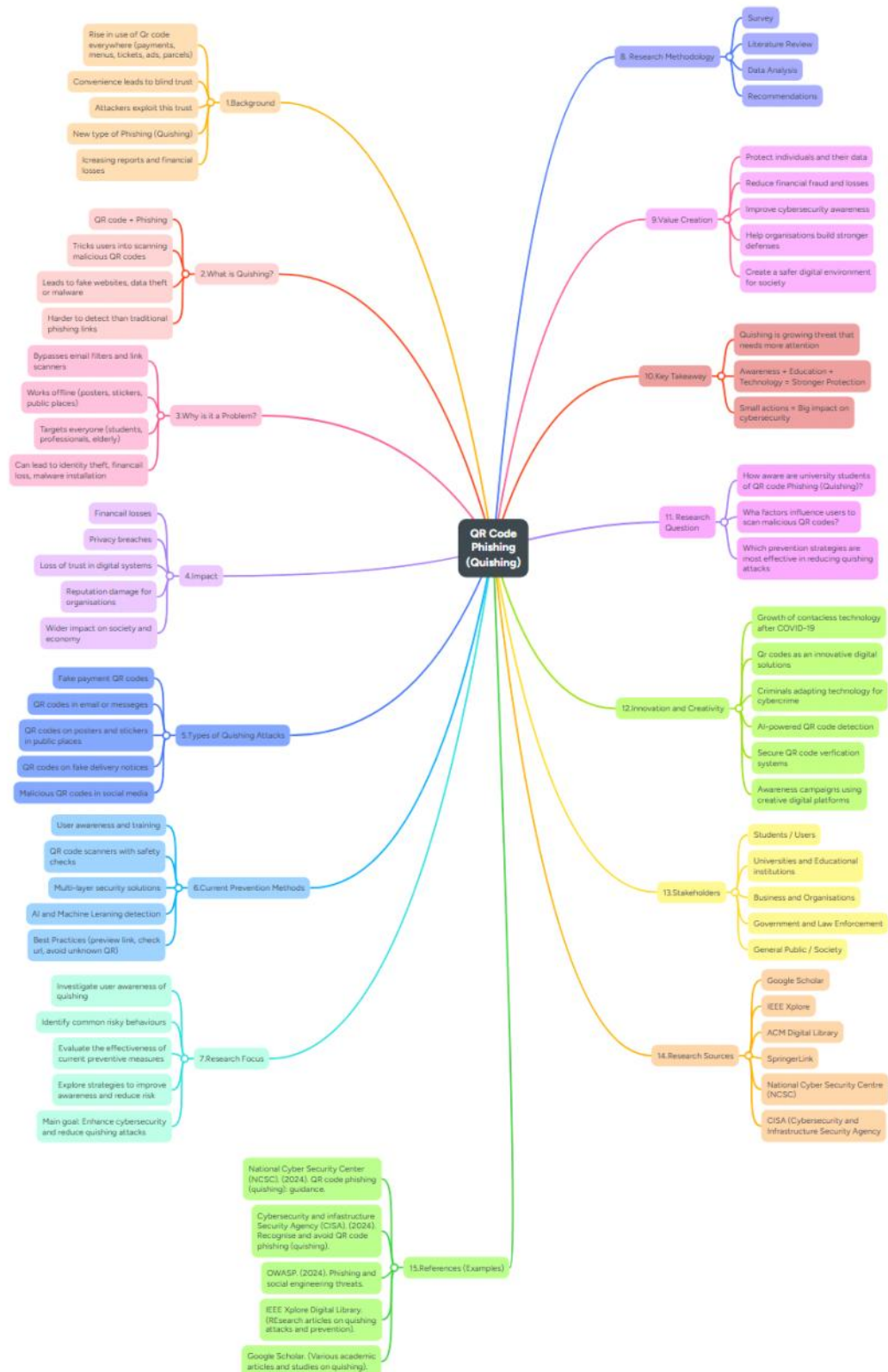
E-portfolio URL: <https://sites.google.com/view/yevhen-lytko-portfolio/%D0%B3%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F-%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0>

Research area / project idea: QR code phishing ("quishing")

Task 1

Thursday, 30 July 2026 4:33 pm

Task 1: Ideation & Mind Map



Central theme: QR Code Phishing ("Quishing")

The rise of QR codes since the COVID-19 pandemic — used everywhere from payments to menus to parcel deliveries — has created widespread convenience, but also blind trust in scanning without checking where a code leads (Background branch). Attackers have exploited this trust, giving rise to a distinct form of phishing known as "quishing": a malicious QR code that redirects users to fake websites, data-harvesting pages, or malware downloads (National Cyber Security Centre (NCSC),

2024). Unlike traditional phishing links in emails, quishing is harder to detect because the destination URL is hidden until the code is scanned, bypassing the visual cues people are trained to spot. This is a growing problem for several reasons. Quishing bypasses email filters and link scanners entirely, since the payload is not a clickable link but an image (Cybersecurity and Infrastructure Security Agency (CISA), 2024). It also works offline — malicious codes appear on posters, stickers, and parking meters in public places — and targets everyone from students to professionals to the elderly, with consequences ranging from identity theft to financial loss and malware installation (Why is it a Problem branch).

The impact extends beyond the individual victim. Financial losses and privacy breaches erode trust in digital systems generally, damage the reputation of organisations whose branding is spoofed, and create a wider societal and economic cost as digital trust declines (Impact branch). Attackers have also diversified their methods: fake payment QR codes, malicious codes embedded in emails or messages, codes placed over legitimate ones in public spaces, fraudulent delivery notices, and QR codes spread through social media (Types of Quishing Attacks branch).

In response, current prevention methods include user awareness training, QR scanners with built-in safety checks, multi-layered security solutions, and AI/machine-learning-based detection tools, alongside simple best practices such as previewing a link before opening it and avoiding unfamiliar codes altogether (Current Prevention Methods branch; OWASP, 2024). This is where innovation and creativity intersect with the problem: just as attackers adapt existing technology for cybercrime, defenders are innovating in response — through AI-powered QR verification systems and creative awareness campaigns delivered via digital platforms (Innovation and Creativity branch).

Selected project idea (Q2)

From the Research Focus and Research Question branches of the map, the project idea taken forward is: investigating how aware university students are of QR code phishing, what factors influence them to scan unfamiliar QR codes, and — most importantly — designing and piloting a practical countermeasure that improves safer scanning behaviour. Rather than only documenting the problem, the project's value lies in its solution: a short, testable intervention such as a scanning safety checklist or guidance card, built directly from the Current Prevention Methods branch (user awareness training, preview-before-scan habits) and refined using pilot feedback from real participants. This idea was chosen because it moves beyond theory into something with genuine value for a real stakeholder group — students, universities, and the wider public identified in the Stakeholders branch — directly supporting the Value Creation branch of the map: reducing financial fraud, improving cybersecurity awareness, and helping build a safer digital environment.

This project idea, and its proposed solution, carries forward into Task 2, where it is developed into a formal Aim, Objectives, and research strategy.

References

Cybersecurity and Infrastructure Security Agency (CISA) (2024) Recognise and avoid QR code phishing (quishing).

National Cyber Security Centre (NCSC) (2024) QR code phishing (quishing): guidance.

OWASP (2024) Phishing and social engineering threats.

IEEE Xplore Digital Library (2024) Research articles on quishing attacks and prevention.

Google Scholar (2024) Various academic articles and studies on quishing.

Task 2

Thursday, 30 July 2026

4:33 pm

Task 2: Aim & Objectives and Research Area

Aim and objectives

Aim: To find out why students are likely to scan unsafe QR codes without checking them, and to create and test a simple, low-cost way to help students scan more safely.

Objectives:

To review existing research on how quishing attacks work, how they are usually carried out, and what has already been suggested to prevent them.

To find out what makes students scan a QR code without stopping to check where it leads, including habits, confidence levels, and lack of awareness.

To compare how aware students are of quishing against how aware they are of normal email phishing, to see if there is a gap.

To design a short, practical intervention, such as a checklist or short guidance card, and test it on a small group of students to see if it changes their scanning habits.

To use the feedback from that small test to improve the intervention and turn the findings into simple, usable recommendations.

Research philosophy

This project fits best with a pragmatist research philosophy, which is one of the philosophies described in Saunders, Lewis and Thornhill's "research onion" model, commonly used for business and computing-related research projects (Saunders, Lewis and Thornhill, 2019). Pragmatism was chosen because the project is not trying to test a single theory in a lab setting; it is trying to solve a real, practical problem — students scanning unsafe QR codes — and understand it well enough to build something that actually helps. The project also plans to collect two different types of data: a short quantitative survey to measure how aware students currently are, and qualitative feedback once a small group has tried the intervention. A purely positivist approach would focus too heavily on numbers and would miss the reasons behind people's behaviour, while a purely interpretivist approach would make it difficult to measure whether awareness or behaviour has actually improved. Because the project needs both an understanding of behaviour and a measurable outcome, a pragmatic, mixed approach is the most realistic fit.

Search tools and research strategy

To find relevant research, computing and cybersecurity-focused databases were used, mainly IEEE Xplore, the ACM Digital Library, ScienceDirect and SpringerLink, along with Google Scholar to track how often certain papers were cited by others. Search terms included "quishing", "QR code phishing" and "malicious QR code", combined using AND/OR to widen or narrow the results depending on how many papers came back. Results were mostly limited to sources from 2021 onwards, since attacker techniques in this area change quickly and older sources may already be out of date. One useful shortcut was finding an existing literature review that had already summarised a lot of the research on quishing; from there, it was possible to look backwards through its reference list to find older, relevant studies, and forwards through Google Scholar to find newer papers that had cited it. This approach was combined with checking current threat reports from cybersecurity vendors and organisations such as the National Cyber Security Centre and CISA, since industry sources tend to report on new attack trends faster than academic papers are published.

References

Saunders, M., Lewis, P. and Thornhill, A. (2019) Research Methods for Business Students. 8th edn. Harlow: Pearson Education.

National Cyber Security Centre (NCSC) (2024) QR code phishing (quishing): guidance.

Cybersecurity and Infrastructure Security Agency (CISA) (2024) Recognise and avoid QR code phishing (quishing).

IEEE Xplore Digital Library (2024) Research articles on quishing attacks and prevention.

Google Scholar (2024) Various academic articles and studies on quishing.

Task 3

Thursday, 30 July 2026 4:33 pm

Task 3: Research Strategies

Validity, reliability, generalisability and ethics

To support validity, the survey questions and the draft intervention will be piloted with a small group before being used properly, to check that the questions are actually measuring awareness and behaviour rather than something unrelated or confusing. To support reliability, the same wording, scale and method of delivery will be used with every participant, and where possible the questions will be based on measures already used in earlier phishing-awareness studies rather than newly invented ones, since reused, tested questions are less likely to be misunderstood. Generalisability is limited from the start: because the sample will be a small group of students or peers rather than a large random sample, the findings cannot be claimed to represent all students, or the wider public. Instead, the results will be treated as an early, indicative picture and a starting point for a larger study, not as a generalisable conclusion. On ethics, the project will only use safe, clearly labelled test QR codes rather than real malicious ones, participants will give informed consent before taking part, and all responses will be kept anonymous. This mirrors how similar quishing research has been carried out safely in the past, using controlled, non-harmful QR codes instead of real attacker infrastructure.

Research strategy and data collection, including pilot

The project will use a mixed-methods approach: a short quantitative survey to measure current awareness levels and self-reported scanning habits, followed by a short qualitative feedback stage once a small group has tried the draft intervention. For the pilot stage, a short questionnaire of around 8 to 10 questions will be created, covering how often people scan QR codes, whether they had heard of quishing before, and how confident they feel judging whether a QR code is safe. This questionnaire will be shared with a small group of peers first, and their feedback on the wording, length and clarity of the questions will be used to fix any confusing or unnecessary questions before the main survey is sent out more widely. The pilot questions themselves, along with a summary of the feedback received, will be included in the appendix and referred to here as the basis for improving the final version of the survey.

Types of quantitative and qualitative analysis

For the quantitative side, answers to closed survey questions will be analysed using basic descriptive statistics, such as percentages and frequencies, to show overall awareness levels and common scanning habits. Simple cross-tabulation will also be used to check whether awareness seems to differ depending on other factors, such as how often someone scans QR codes in general. For the qualitative side, open-ended comments from the pilot feedback, and any other written responses, will be analysed using thematic analysis. This means reading through the comments and grouping similar ideas into themes, for example comments along the lines of "I didn't know QR codes could be dangerous" or "I would check a link on my laptop but not on my phone." These themes will help explain the numbers from the quantitative survey and will be used to improve the final intervention.

References

Saunders, M., Lewis, P. and Thornhill, A. (2019) Research Methods for Business Students. 8th edn. Harlow: Pearson Education.

National Cyber Security Centre (NCSC) (2024) QR code phishing (quishing): guidance.

Cybersecurity and Infrastructure Security Agency (CISA) (2024) Recognise and avoid QR code phishing (quishing).

Appendix

Thursday, 30 July 2026

4:33 pm

Appendix: Pilot Data Collection Instrument

Draft pilot questionnaire (to be distributed to a small peer group before the main survey):

1. How often do you scan QR codes in a typical week?
2. Before today, had you heard the term "quishing" or "QR code phishing"?
3. How confident are you in judging whether a QR code is safe to scan? (scale 1–5)
4. Do you check where a QR code leads before entering any personal details? (yes / sometimes / no)
5. Have you ever scanned a QR code in a public place (poster, sticker, menu) without checking who placed it?
6. What would make you more cautious about scanning an unfamiliar QR code?
7. After reading the draft guidance card, was anything unclear or missing?
8. Any other comments on the length, wording or usefulness of this questionnaire?

Pilot feedback summary: The questionnaire was piloted with three participants. Responses showed relatively low prior awareness of quishing, with none of the three having heard the term before taking part, despite two of the three reporting they check where a QR code leads before entering personal details, and two reporting they scan QR codes only from sources they consider official or trusted (e.g. hotels, institutions). A consistent issue emerged with Question 3: all three participants found the wording ambiguous, unsure whether it was asking about their general confidence in judging QR code safety, or their confidence in that specific moment. Two participants also raised a related point not directly asked about — that trusting an "official" source does not guarantee their data is handled safely afterwards, suggesting the current question may oversimplify how users actually judge risk. As a result, Question 3 was reworded for clarity, from "How confident are you in judging whether a QR code is safe to scan?" to "In general, how confident are you that you could tell a safe QR code from a risky one?" No questions were removed, and feedback on length and overall clarity was positive across all three participants. This feedback was used to refine the wording of the main survey instrument before wider distribution. This appendix is referred to in Task 3 (Research Strategy and Data Collection) as the basis for refining the final survey instrument.

Person 1

- 1) Twice a week
- 2) no
- 3) 2
- 4) Yes
- 5) No
- 6) I never scan unknow QR codes , I decide to scan them only if I know where it goes to
- 7) No, everything was covered.
- 8) I found Question 3 a bit confusing — I wasn't sure if 'confident in judging whether a QR code is safe' meant confident in general, or confident right now in this specific test.

Person 2

- 1) almost never
- 2) no
- 3) 2-3
- 4) yes
- 5) yes
- 6) I only scan QR's from official institutions or their representatives, however, I am not sure about where my personal data goes then anyway
- 7) No, everything is clear
- 8) I was not sure what was exactly meant in question 3, as I never scan suspicious QR's, but I can't be sure that even official organisations don't sell or use my data in way I would not appreciate that,

so it is quite difficult to identify my judging skills.

Person 3

1)twice a week

2)no

3)3-4

4)yes

5)yes

6)I only scan QR code from Hotel , and from official institutions

7)No

8)I wasn't sure what question 3 meant, as I never scan suspicious QR codes. However, I can't be sure that even official organizations don't share or use my data in ways I wouldn't find offensive, so it's quite difficult to assess my detection skills.