

## Assignment 1.

21 November 2025 15:02

8/21/2025

# Changemakers: Creativity and Value Creation

Module: ACCA5033

Lecturer: Dr. Fahad Ahmad

Higor Scaffi Dutra do Nascimento (2413595)  
UNIVERSITY OF WALES TRINITY SAINT DAVID - EAST  
LONDON

## Contents

|                                                                     |    |
|---------------------------------------------------------------------|----|
| Task 1: Ideation & Mind Map.....                                    | 4  |
| Context and value proposition.....                                  | 4  |
| Design-thinking lens: inventive and usable.....                     | 4  |
| Stakeholders and touchpoints.....                                   | 4  |
| Constraints and practical limits.....                               | 5  |
| Risks and mitigations.....                                          | 5  |
| Ethics and societal benefit.....                                    | 5  |
| Success indicators.....                                             | 5  |
| Task 2: Aim & Objectives; Research Philosophy; Search Strategy..... | 7  |
| Aim.....                                                            | 7  |
| Objectives.....                                                     | 7  |
| Research philosophy.....                                            | 7  |
| Scope and alignment with computing/security.....                    | 7  |
| Search tools and specific databases.....                            | 8  |
| Search strategy and evidence management.....                        | 8  |
| Task 3 - Research Strategies; Pilot; Analysis.....                  | 9  |
| Data collection and pilot.....                                      | 9  |
| Analysis plan.....                                                  | 10 |
| Technical and policy alignment.....                                 | 10 |
| Expected result and value.....                                      | 11 |
| Appendices.....                                                     | 12 |
| Pilot instrument.....                                               | 12 |
| Interview prompts.....                                              | 12 |
| References.....                                                     | 13 |

# Task 1: Ideation & Mind Map

06 November 2025 15:03

## Context and value proposition

Across industries, social engineering via email continues to be one of the most reliable paths attackers use to obtain credentials or trigger harmful actions. The *Data Breach Investigations Report* (DBIR) indicates that phishing and credential theft remain high-impact patterns year after year, while European threat briefings similarly emphasise social tactics and business email compromise. For site supervisors—who juggle shift coordination, ad-hoc approvals, delivery confirmations and contractor communications email is a constant channel that competes with operational demands. This real-world context amplifies the risk: quick decisions are made on small screens, often under time pressure. A workflow intervention that fits the way supervisors already work can meaningfully cut risky clicks and speed up reporting, creating measurable organisational value in the form of fewer compromises, faster response, and reduced dwell time [1], [2].

## Design-thinking lens: inventive and usable

This concept was shaped with design thinking: empathise with the constraints of supervisors, define the moments of risk, ideate lightweight nudges, prototype fast, and test in the field. Three design ideas reinforce one another:

Just-in-time (JIT) decision support. Rather than generic banners on every message, the workflow prioritises moments of highest risk, when a user is about to follow a link to a site that asks for credentials or a payment step. At that point, the interface presents a compact interstitial that: sets expectations about the *relying party* (RP) domain.

surfaces a readable destination (highlight `pay.example.co.uk` vs. `pay-secureexample.co` in a clear font, with RP emphasis). offers a one-tap “Report suspicious” action if something looks off.

This timely cue aligns with human-factors evidence that warnings work best when they are brief, actionable, and delivered exactly when a decision is made [7], [8].

Streamlined reporting and triage. A single, prominent control lets the user report the message in one step. The add-in packages headers, URLs, and user verdict (no message body) and sends to a monitored mailbox or a SOAR playbook. Security teams can automatically quarantine similar emails (same sender domain + look-alike patterns) to reduce further exposure and provide rapid feedback that reinforces positive user behaviour.

Phishing resistant follow ups with passkeys. For portals supervisors’ access after email timesheets, delivery portals, incident logs—the workflow promotes WebAuthn passkeys (FIDO-based public-key credentials bound to origin). Because passkeys authenticate the user and the RP origin, adversary-in-the-middle (AiTM) kits cannot replay captured tokens across look-alike domains. This directly addresses modern phishing and session theft techniques while removing password risks and push fatigue [3],[5], [10].

## Stakeholders and touchpoints

Primary users: site supervisors and shift leads (mobile + desktop, variable network conditions).

Secondary stakeholders: IT/SecOps (instrumentation, tuning, SOAR), HR/compliance (awareness and policy), and external vendors (whose emails should pass authentication checks and appear trustworthy).

## Constraints and practical limits

Time pressure and mobile ergonomics mean the design must be readable at a glance: short text, high contrast, large tap targets.

Integration should work with M365 and Google Workspace without exporting message bodies to third parties.

The system should leverage email authentication signals such as SPF/DKIM/DMARC to contextualise banners (“Sender domain authenticated” vs. “No DMARC alignment”), reducing false reassurance from look-alike domains [6].

## Concept features (mind-map nodes you can draw)

Triage layer: compact banners on new/external emails; show sender domain, DMARC status, and (optionally) domain age to discourage gutfeel clicks.

JIT checker: only appears on credential prompts or payment pages; compares destination domain with expected RP; offers “Report” vs. “Proceed.”

One-tap reporting: headers/URLs/verdict captured; optional auto-quarantine of similar emails; feedback loop to user (“Thanks—Security is reviewing”).

Passkeys for follow-ups: replace passwords/push codes on high-value portals used by supervisors; onboarding wizard to register passkeys on first use [3], [5].

Micro-training: 10–15 second snippets after user actions (report or safe dismiss) explaining *why* a decision was good; this reinforces learning without interrupting tasks.

Admin dashboard (lightweight): basic metrics (report count, time-to-report, false positive rate) and safe-list controls.

## Risks and mitigations

Alert fatigue: throttle banners, ensure the interstitial appears only at true high-risk points, and keep copy to two lines plus a clear primary action.

False positives on legitimate newsletters or partner emails: provide a “mark legitimate” path but require a short justification to discourage overuse; schedule weekly safelist review.

Edge cases on mobile and QR phishing: ensure previews work with mobile deep links and that QR-initiated URLs still trigger the JIT check; include a QR specific tip in microtraining.

Legacy MFA bypass by AiTM: prioritise migration of critical supervisor portals to passkeys; communicate *why* passkeys are different (origin-bound, non-replayable) [4], [5], [10].

## Ethics and societal benefit

The design minimises data by collecting only headers, URLs, verdicts and timing no message body content supports informed consent for research, and anonymises any telemetry used for evaluation. By mapping to usable security research on warning effectiveness, the workflow aims to reduce cognitive load rather than increase it, creating value for both individuals and the organisation [7], [8].

## Success indicators

Lower click-through on simulated phish (primary outcome).

Higher report rates and shorter time to report (secondary outcomes).

Adoption of passkeys on designated portals and reduced reliance on passwords/push approvals.

These measures correspond to contemporary threat patterns and accepted best practice [1], [2], [5].

From <<https://d.docs.live.net/43052e89ef0dd258/Desktop/Changemaker%20Assessment%201.docx>>

# Task 2: Aim & Objectives; Research Philosophy; Search Strategy

12 November 2025 17:10

## Aim

To design and empirically evaluate a low-friction, phishing-resistant email workflow for site supervisors that combines *just-in-time decision support*, *single-tap reporting*, and *passkeybased authentication*, thereby reducing successful phishing outcomes and credential theft within realistic operational constraints.

## Objectives

- O1. Map supervisor decision points with short contextual interviews and observations (where approvals happen, how link previews are used, typical devices).
- O2. Prototype a triage banner, a JIT interstitial, and a one-tap reporting control integrated with M365/Workspace; ensure privacy by design (headers/URLs only).
- O3. Enable WebAuthn passkeys for at least two high-value follow-up services (timesheets, contractor management), including clear onboarding flows.
- O4. Run controlled email simulations to measure click-through, report rate, and time-to-report, with counterbalanced conditions (baseline vs. workflow).
- O5. Assess usability (SUS or UMUX-Lite) and perceived trust; gather qualitative insights into banner clarity and mental models.
- O6. Produce deployable guidance aligned with NIST SP 800-63B (authenticator assurance), W3C WebAuthn L3 (technical capabilities), CISA (policy emphasis on phishing-resistant MFA), and NCSC (organisational phishing defence) [3], [5], [9].

## Research philosophy

A pragmatist philosophical stance guides the study. Instead of privileging one method, pragmatism prioritises problem-centred inquiry and practical outcomes. In phishing defence, user behaviour depends on context, workload, device type, and organisational culture; therefore, mixed methods are essential.

Quantitative measures (click-through, report rate, time-to-report, passkey usage) quantify effect sizes and enable comparisons.

Qualitative interviews explain observed behaviour (why users ignored a banner or trusted a suspicious domain).

This empirical, context-sensitive approach aligns with both threat intelligence that spotlights social engineering and with standards bodies prioritising phishing-resistant authentication over legacy MFA [1], [5], [9].

## Scope and alignment with computing/security

The project sits at the intersection of usable security (warning design, behavioural nudges) and identity security (WebAuthn passkeys). It also touches email authentication posture (DMARC) to improve the reliability of decision cues. The goal is not to create yet another training course, but to shape decisions at the point of risk, then remove passwords from critical flows to neutralise replay and token theft [4], [6], [9].

## **Search tools and specific databases**

### **Academic databases:**

IEEE Xplore and ACM Digital Library for primary research on phishing warnings, decision support, and HCI security (CHI, SOUPS, USENIX Security, IEEE S&P). Scopus for broad discovery and citation chaining across related disciplines

(information systems, human factors, security engineering).

Example queries:

"phishing" AND (warning OR banner OR interstitial) AND (usability OR 'user study')

"Adversary-in-the-middle" AND (passkeys OR WebAuthn OR FIDO)"

"DMARC" AND (usability OR deployment OR effectiveness)"

### **Standards and authoritative guidance:**

NIST SP 800-63B for authenticator requirements and phishing-resistance terminology.

W3C WebAuthn Level 3 (2025 Recommendation) for the current capabilities of passkeys, cross-device credentials, and RP binding.

CISA fact sheet on implementing phishing-resistant MFA (migration patterns and policy stance).

NCSC organisational guidance for UK operational context.

ENISA Threat Landscape for EU threat trends that help justify metric selection [2], [6], [9].

### **Industry intelligence:**

Microsoft Defender Experts case studies on AiTM/BEC to understand the mechanics of token theft and multi-stage phishing, informing both copy and evaluation scenarios [10].

## **Search strategy and evidence management**

Use 2015 - present as a filter for most topics (earlier for foundational warning papers) and focus on peer-reviewed venues and formal standards. For each query, record in a search log: database, keywords, filters, number of hits, inclusion/exclusion decisions, and "cited by" trails from seminal papers (Akhawe & Felt; Egelman et al.). Prioritise primary sources for standards (NIST, W3C, RFCs) and credible government/agency guidance (CISA, NCSC, ENISA). Store PDFs and notes in a reference manager with IEEE output style and DOIs/persistent URLs wherever available.

Expected contribution and impact

This project aims to deliver evidence-backed, deployable guidance for organisations with SME-like constraints:

a lightweight combination of contextual warnings and origin-bound authentication.  
measurable reductions in risky actions and faster reporting. a path to reduce password reliance without sacrificing user productivity.

Aligning with NIST, W3C, CISA, and NCSC positions the outcome as standards-consistent and future-proof, while the pragmatist evaluation ensures it remains usable in day-to-day operations [1], [5], [9].

From <<https://d.docs.live.net/43052e89ef0dd258/Desktop/Changemaker%20Assessment%201.docx>>

# Task 3 - Research Strategies; Pilot; Analysis

18 November 2025 20:33

Validity, reliability, generalisability, and ethics

Construct validity. The core metrics directly capture phishing risk and the intended effect of the intervention: Click-through rate on simulated phish (primary outcome).

Report rate and time-to-report, reflecting detection and escalation behaviours.

Passkey adoption on designated portals, serving as a proxy for reduced password exposure and resilience to AiTM.

These measures align closely with today's attacker playbooks (credential phishing, token replay) and with recommendations prioritising phishing-resistant MFA [1], [2], [5], [10].

**Internal validity.** Use matched message sets across conditions and participants. Randomise message order and counterbalance baseline (no JIT + legacy login) versus treatment (JIT + passkeys) within subjects to reduce learning effects. Keep device, client, and network conditions as consistent as feasible.

## **Reliability.**

Standardise banner copy (two variants maximum) and JIT interstitial wording; run a repeat trial approximately one week later to assess test–retest stability for key metrics and the SUS. For the qualitative strand, double-code a subset of transcripts and compute agreement (e.g., Cohen's  $\kappa$  or percent agreement) before coding the remainder.

## **Generalisability.**

Recruit across multiple sites/shifts and include both desktop and mobile clients; note the hardware diversity typical of supervisors (ruggedised devices, pooled workstations). Acknowledge limits, including small samples and cultural factors that may shape attention to warnings.

## **Ethics.**

Obtain informed consent, avoid distressing content, and debrief immediately after simulations. Collect only headers, URLs, decision events, and timestamps—no message bodies—and store data in line with institutional policy. Pseudonymise all records; store consent forms separately. Make clear that participation does not affect pay or performance evaluation.

## **Data collection and pilot**

### **Instrumentation (quantitative).**

The email add-in logs banner displays, hover previews, click/report actions, and time deltas (arrival → first interaction → resolution).

The portals log authentication mode (passkey vs. legacy), first-time registration events, and failed vs. successful logins.

The pipeline aggregates per-participant metrics for statistical analysis and per-condition comparisons.

### **Surveys.**

After completing the workflow tasks, participants complete SUS or UMUX-Lite, capturing perceived usability and satisfaction. Include one custom item on trust in the banner/JIT advice (Likert 1–5) to track confidence shifts.

### **Interviews (qualitative).**

15–20-minute semi-structured interviews focus on banner clarity, link-preview usefulness, when and why users proceed, and how passkeys compare to existing sign-ins (effort, speed, perceived security). Prompts encourage concrete examples (e.g., “Tell me about the last time you had to approve something quickly from your phone”).

### **Pilot.**

Conduct a pilot with 3–5 supervisors to validate copy, timing, thresholding for the JIT interstitial, and report button placement. Specifically assess: whether the domain emphasis in the JIT screen is noticeable on mobile. whether the preview is readable and unambiguous. whether report is quick enough during a busy shift. whether passkey onboarding is self-explanatory.

Use pilot findings to refine wording (e.g., keeping the JIT text under 18–22 words), adjust the frequency of prompts, and tune the safelist process.

### **Analysis plan**

#### **Quantitative analysis.**

Compute descriptive statistics (mean, median, 95% CIs) for click-through, report rate, time-to-report, and SUS/UMUX-Lite.

Use within-subjects tests to compare baseline vs. treatment: paired *t*-tests for normally distributed differences; Wilcoxon signed-rank otherwise. Present effect sizes (Cohen’s *d* or rank-biserial correlation) to show practical importance beyond *p*-values.

Conduct a process analysis for passkey adoption: weekly percentages of logins via WebAuthn and the proportion of first-time registrations completed without support. If data permit, model a simple interrupted time series around the introduction of passkeys to assess trend changes.

Where relevant, stratify by device type (mobile vs. desktop) or shift type (day vs. night) to understand context effects.

Interpret outcomes against policy/standards priorities (e.g., demonstrate that passkeys materially reduce risk relative to push-based MFA) [3], [5], [9].

#### **Qualitative analysis.**

Apply thematic analysis with a priori codes (e.g., *alert clarity*, *false reassurance*, *workflow friction*, *trust*, *mobile constraints*), adding inductive codes as patterns emerge.

Ensure at least two coders review 20–30% of transcripts to discuss codebook adjustments.

Produce 3–5 salient themes with short, anonymised quotes (e.g., “The domain looked right at a glance, but the JIT screen made me realise the hyphen was wrong”), and design implications (simplify domain rendering; avoid jargon like “RP” in end-user text).

Triangulate with telemetry (e.g., long hover durations but eventual clicks might correspond to interview themes around ambiguity or time pressure).

### **Technical and policy alignment**

WebAuthn Level 3 passkeys: recommend defaulting to passkeys for supervisor portals, emphasising origin binding (public-key credentials scoped to the RP) to neutralise AiTM replay across look-alike domains [4], [10].

DMARC signals: integrate SPF/DKIM/DMARC verdicts into the banner so that *legitimate*, *authenticated senders* gain trust affordances while unauthenticated or misaligned mail is flagged, reducing false reassurance [6].

Guidance mapping: align outcomes with CISA's call to prioritise phishing-resistant MFA and NCSC's layered organisational approach to phishing defence. Use NIST SP 800-63B to justify authenticator choices and assurance levels [3], [5], [9].

### **Expected result and value**

The anticipated outcome is a statistically and practically significant reduction in risky clicks, faster reporting, and sustained passkey adoption on high-value workflows. Together, these translate into a smaller attack surface for credential theft and AiTM, shorter incident response times, and a culture that treats email risk as a shared, lightweight routine rather than a separate training task. The approach is scalable (add-in + policy changes), privacy-conscious (no body capture), and standards-consistent, which supports sustainability beyond the study period. [1],[5], [9], [10].

From <<https://d.docs.live.net/43052e89ef0dd258/Desktop/Changemaker%20Assessment%201.docx>>

# Appendices

21 November 2025 14:33

## **Pilot instrument**

Enable the add-in in Outlook/Workspace (desktop and mobile if available).

Triage 10 mixed emails (internal/external, varied cues); read the banner and, where present, the DMARC note.

Hover 3 links; confirm the preview shows the expected domain (or not); choose Report or Proceed.

Use Report suspicious for 2 messages; confirm the confirmation toast and that headers/URLs were captured.

Sign into the “Contractor Portal” using a passkey (demo account); enrol if first-time; capture any friction points.

Complete SUS (10 items; 1–5) or UMUX-Lite (4 items).

## **Interview prompts**

Which banner words were most/least helpful?

Did the link preview change your decision? Why?

Under what conditions would you still proceed?

Was reporting sufficiently fast during a busy shift?

How do passkeys compare with your usual login (time, confidence)?

What one change would most increase your trust?

## **Metrics and instrumentation.**

Behavioural: click-through (%), report rate (%), time-to-report (min), hover rate (%), passkey usage (%).

Context: record SPF/DKIM/DMARC verdicts; do not store email bodies.

Quality controls: pre-register measures; randomise message order; counterbalance conditions; repeat after a week; double-code ~20–30% of transcripts.

## **Risk and mitigation examples.**

Prompt fatigue → throttle interstitials; restrict to credential prompts.

False positives → safelist with weekly review and a required justification for “mark legitimate.”

Mobile ergonomics → large tap targets; minimal copy; ensure QR-originated links trigger the same JIT checks.

Legacy MFA bypass via AiTM → prioritise passkeys and explain, in simple language, why they’re different from codes/push [4], [5], [9], [10].

Search log template.

Date | Database | Query | Filters | Hits | Kept (why) | Discarded (why) | Next steps.

From <<https://d.docs.live.net/43052e89ef0dd258/Desktop/Changemaker%20Assessment%201.docx>>

# References

21 November 2025 15:47

- [1] Verizon, “2025 Data Breach Investigations Report,” May 2025.
- [2] ENISA, “ENISA Threat Landscape 2024,” Sept. 2024.
- [3] P. A. Grassi, J. L. Fenton, et al., “Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B),” NIST, 2017 (incl. errata). doi: 10.6028/NIST.SP.800-63b. Accessed: Oct. 23, 2025.
- [4] W3C, “Web Authentication: An API for accessing Public Key Credentials — Level 3,” W3C Recommendation, Jan. 27, 2025.
- [5] CISA, “Implementing Phishing-Resistant MFA (Fact Sheet),” 2023.
- [6] D. Crocker, T. Hansen, and M. Kucherawy, “Domain-based Message Authentication, Reporting, and Conformance (DMARC),” RFC 7489, Mar. 2015.
- [7] D. Akhawe and A. P. Felt, “A Large-Scale Field Study of Browser Security Warning Effectiveness,” in *Proc. USENIX Security*, 2013
- [8] S. Egelman, L. F. Cranor, and J. Hong, “You’ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings,” in *Proc. CHI*, 2008
- [9] NCSC (UK), “Phishing attacks: defending your organisation,” Guidance, updated 2024.
- [10] Microsoft Defender Experts, “Detecting and mitigating a multi-stage AiTM phishing and BEC campaign,” Microsoft Security Blog, Jun. 8, 2023.

From <<https://d.docs.live.net/43052e89ef0dd258/Desktop/Changemaker%20Assessment%201.docx>>