KBTG KAMPUS HACKATHON 2026 · ONE-PAGE PITCH

TRACK 3 · CYBER SECURITY

K PLUS JobShield

ปกป้อง “เงินสำรองก่อนเงินเดือนแรก” ก่อนถูกบริษัทปลอมขอให้จ่ายเงินเพื่อแลกกับงาน

Career Mode ที่เชื่อมบริบทการหางาน แหล่งเงิน และความเสี่ยงธุรกรรม เพื่อแทรกแซงก่อนเงินออก

Problem Statement — ปัญหาที่ต้องแก้

มิจฉาชีพอาจปลอมเป็นบริษัทหรือ recruiter แล้วเรียกค่าสมัคร ค่าอบรม ค่าอุปกรณ์ หรือเงินมัดจำก่อนเริ่มงาน ผู้สมัครเป็นผู้ยืนยันการโอนเอง จึงผ่าน authentication ได้แม้กำลังถูก social engineering ขณะที่คำเตือนทั่วไปไม่รู้ว่าเงินก้อนนี้จำเป็นต่อการใช้ชีวิตก่อนเงินเดือนแรก

Target Users

First Jobbers 22–30

ผู้ที่กำลังสมัครงาน รอเริ่มงาน หรือรอเงินเดือนแรก และเลือกเปิด Career Mode ด้วยตนเอง โดยไม่เหมารวมว่ากลุ่มนี้ประมาทหรือถูกหลอกมากกว่าคนอื่น

Proposed Solution — 3 ขั้นตอนก่อนเงินออก

1 Prepare

เปิด Career Mode แบบ opt-in กำหนดช่วงเวลา แล้วแบ่ง K-ePocket เป็น Job Search Budget สำหรับค่าใช้จ่ายหางาน และ เงินสำรองก่อนเงินเดือนแรก สำหรับค่าเช่า อาหาร เดินทาง และเหตุจำเป็น

2 Detect

ก่อนโอน รวมแหล่งเงิน ผู้รับใหม่ ยอดและการโอนสะสม บริบทการจ่ายเพื่อเริ่มงาน และ destination risk จากระบบธนาคาร คำตอบของผู้ใช้เป็นเพียงหนึ่งสัญญาณ ไม่อ่านข้อความหรืออีเมลอัตโนมัติ

3 Intervene

ปรับ friction ตามความเสี่ยงพร้อมเหตุผลที่สังเกตได้ หาก High Risk จะพักเป็น Pending Instruction ใน Cooling-off ก่อนส่งเข้าสู่ PromptPay แล้วให้ผู้ใช้

LOW · NORMAL | MED · EXPLAIN | HIGH · PAUSE

ตัวอย่างคำเตือน: พักรายการนี้และตรวจสอบก่อน

ผู้รับใหม่ · ใช้เงินสำรองก่อนเงินเดือนแรก · จ่ายเพื่อเริ่มงาน
คำสั่งยังไม่ถูกส่งเข้าสู่ระบบโอน และผู้ใช้ยังยกเลิกได้

Pause & Verify

Cancel / Report

1 · K-ePocket
บริบทและวัตถุประสงค์ของเงิน

2 · Transaction + Fraud Risk
ผู้รับ · ยอด · รูปแบบ · destination risk

3 · Security & Fraud Response
Warning · Verification · Cooling-off · Report

Value Proposition

FOR FIRST JOBBERS

ปกป้องเงินสำคัญ ณ จุดตัดสินใจก่อนโอน อธิบายว่าเตือนเพราะอะไร และยังมีทางผ่านสำหรับธุรกรรมถูกต้องหรือเหตุฉุกเฉิน เช่น บัญชีตนเองหรือ verified biller

FOR K PLUS

ต่อยอด K-ePocket และ fraud controls ที่มีอยู่ เป็น security journey เฉพาะช่วงหางาน ขยับจาก awareness สู่ pre-loss intervention และเสริม Digital Trust โดยไม่อ่านข้อความส่วนตัว

Track Perspective — Cyber Security & Digital Trust

รับมือ authorized push payment ที่ผู้ใช้ถูก fake recruiter ชักจูงให้โอนเอง ด้วย defense in depth ก่อนเงินออก:

EXPLAINABLE POLICY
Multi-signal rules และเหตุผลที่ผู้ใช้เข้าใจได้

RISK-BASED CONTROL
Low ปกติ · Medium ยืนยัน High ใช้ Cooling-off

EVASION-AWARE
ตรวจยอดสะสมและประเมินซ้ำ รับมือแบ่งยอด/ตอบ purpose ผิด

PRIVACY & AUTONOMY
เก็บ audit data เท่าที่จำเป็น และไม่ล็อกเงินถาวร

PROTOTYPE BOUNDARY

ใช้ synthetic data และ deterministic rules; destination risk เป็น simulated bank-side signal ระยะ Cooling-off จริงต้องผ่าน policy, legal และ usability validation ระบบช่วยลดความเสี่ยง แต่ไม่รับประกันว่าจะหยุด Scam ได้ทุกกรณี

OFFICIAL REFERENCES · ACCESSED 4 SEP 2026

[1] KBank Job Scam [2] K PLUS [3] K-ePocket [4] KBank Anti-fraud Controls

Concept based on reviewed public information; ไม่อ้าง KBank internal access และ Email/Link scanning หรือ Fraud Specialist ไม่อยู่ใน Core