Mission: Fraud Impossible – Innovate to Dominate

A Hackathon to Outwit Scammers and Redefine Security in Banking

Overview

In a world where scammers lurk in the shadows, it's your mission to outsmart them. Gear up, innovate, and disrupt the dark side of financial fraud. This hackathon invites top college grads to combine creativity, technical prowess, and industry insights to craft ingenious solutions that keep the scammers on the run. Let's make fraud prevention a blockbuster story!

Theme & Objectives

- **Theme**: "Fraud Impossible" – harness cutting-edge technologies to make financial fraud a thing of the past.
- **Objectives**:
    1. Develop new methods or improve existing techniques to detect, prevent, and mitigate fraud.
    2. Encourage collaboration between multidisciplinary teams—combining data science, UX, software engineering, compliance, and more.
    3. Inspire participants to think from a real-world, industry perspective while pushing the limits of creativity.
    4. Produce tangible prototypes, demos, and documentation that can evolve into scalable banking security solutions.

Core Challenges

1. **Real-Time Fraud Detection System**
    - **Tagline**: *"The Scam Stops Here – Be the Sherlock of Transactions"*
    - **Goal**: Spot the wolves before they prey. Build a system so precise, it's like sniffing out the fraudsters' next move in milliseconds.
    - **Key Tasks**:
        - Ingest live transaction data and run anomaly detection.
        - Implement machine learning (e.g., random forest, gradient boosting, deep learning) for continuous fraud scoring.
        - Showcase a user-friendly dashboard for real-time alerts.
    - **Expectations**:
        - Accuracy metrics (Precision, Recall, F1-Score).
        - Visualization of live fraud detection.
        - Documentation on model interpretability (e.g., SHAP, LIME).
    - **References**:
        - Kaggle Credit Card Fraud Detection Dataset
        - PCI DSS Guidelines
        - Stripe API Docs for Payment Data (example reference)

2. **Behavioural Biometrics Authentication**
    - **Tagline**: *"License to Authenticate – No Scammer Can Pass"*
    - **Goal**: Think of this as your MI6-level biometric shield. Flag suspicious anomalies in user behaviour faster than Q's gadgets can reboot.
    - **Key Tasks**:
        - Collect user behavioural patterns (typing speed, mouse usage, touchscreen interactions).
        - Compare real-time sessions to baseline user profiles.
        - Integrate multi-factor authentication (MFA) triggers for flagged sessions.
    - **Expectations**:
        - Prototype capturing behaviour with minimal user friction.
        - Clear explanation of data privacy and anonymization.
        - Suggested plan for scaling and real-world deployment.
    - **References**:
        - NIST Digital Identity Guidelines (SP 800-63)
        - W3C Web Authentication: WebAuthn
        - OWASP Best Practices for Security

3. **AI-Driven Scam Call Detection**
    - **Tagline**: *"Why So Serious About Scams? Let's End Them"*
    - **Goal**: Build an AI-driven tool to silence scam calls for good—because no bank customer should feel like the punchline.
    - **Key Tasks**:
        - Integrate voice/speech recognition or text classification for call transcripts.
        - Leverage NLP to detect high-risk keywords or patterns.
        - Create real-time call risk scoring and flag suspicious numbers.
    - **Expectations**:
        - Working prototype that can screen or label incoming calls.
        - Documentation on potential false positive/negative trade-offs.
        - Implementation of user alerts via mobile app, SMS, or email.
    - **References**:
        - Twilio Voice API & Docs
        - PyTorch or TensorFlow for NLP
        - FTC: Consumer Information on Phone Scams

4. **Financial Literacy Gamification**
    - **Tagline**: *"The Great Scam Escape – Level Up Against Fraud"*
    - **Goal**: Teach users to play smart and stay sharp. Gamify financial literacy, and help customers spot scams before they strike.
    - **Key Tasks**:
        - Design an interactive quiz or mobile game that tests real-world scam scenarios.
        - Integrate storytelling or level-based achievements to keep users engaged.
        - Provide immediate feedback on risk and best practices for digital hygiene.
    - **Expectations**:
        - Fun, polished user interface with accessible design.
        - Create awareness for real scam types phishing, vishing, identity theft.
        - Metrics to measure user improvement (score, progression, completion rates).
    - **References**:
        - National Cyber Security Centre (NCSC) Guidance
        - Kahoot! for inspiration on interactive quizzes
        - FTC Scam Prevention Resource

5. **Cross-Channel Fraud Intelligence**
    - **Tagline**: *"No Stone Unturned – Converge Data, Thwart Threats"*
    - **Goal**: Consolidate fraud signals from multiple channels (online banking, mobile apps, ATM networks, call centers) into one unified intelligence hub.
    - **Key Tasks**:
        - Set up APIs for cross-channel data ingestion (transaction logs, user logs, call logs).
        - Build correlation algorithms to detect suspicious patterns spanning different platforms.
        - Create alerts or dashboards showing cross-channel trends.
    - **Expectations**:
        - Proof-of-concept data lake or data warehouse design.
        - Real-time or near-real-time data syncing.
        - Visual reports or graphs demonstrating cross-channel anomalies.
    - **References**:
        - Apache Kafka for Real-Time Data Streaming
        - ELK Stack for Log Management (Elasticsearch, Logstash, Kibana)
        - ISO/IEC 27001 Information Security Management

Final Word

The future of banking security starts here. As you take on these missions—investigating fraud, outsmarting scammers, and empowering customers—you become the scriptwriters of a new chapter in financial safety. Are you ready to craft the blockbuster story that stops scams forever?