Secure Banking

Stay safe, even under threat

Presented by: Andile Gracious Dhlamini

Problem

- Criminals often force people to transfer money under duress.
- Victims can't refuse without risking their lives.
- No current way to:
  - Alert security silently
  - Limit financial loss in real time
  - Mask access to savings and credit

Solution: Danger Password System

1. A dual-password system:
- Normal Password – Full access
- Danger Password – Triggers Emergency Mode

2. Features of Emergency Mode:
- Limited balance display
- Small transaction caps
- Hides savings & credit accounts
- Silent alerts to guardians/security
- Flags attacker's account for review

🛡️ **Product**

Secure Banking – Danger Password & Limited Access System

A mobile banking safety feature that protects users under threat by using a special "Danger Password."

🔐 What it Does:

- Dual Passwords:
    - Normal Password – Full access.
    - Danger Password – Activates Emergency Mode.

🚨 Emergency Mode Features:

- Shows a limited, decoy balance.
- Hides savings, credit, and investments.
- Only allows small transactions (e.g., $100 max).
- Sends silent alerts to trusted contacts or security.
- Auto-logout after fake transaction to stall attacker.

Looks normal to attackers, but secretly protects the user and alerts help.

Target Market

95% of mobile banking users

According to global fintech reports, 95% of banking customers now rely on mobile apps for managing their finances. This makes mobile-first security features not just optional — they're essential.

The Danger Password system meets users exactly where they are: on their smartphones.
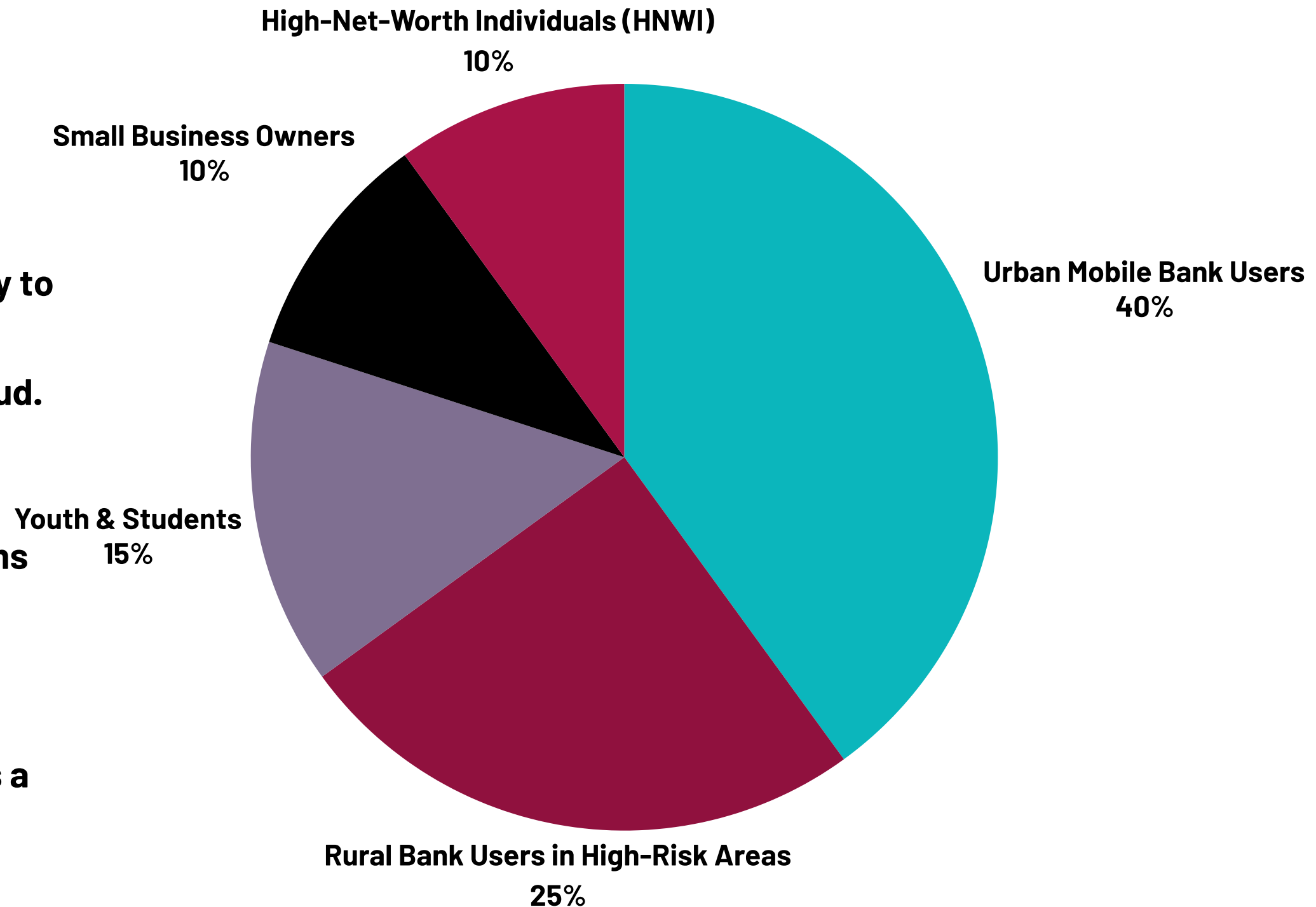
123 million people

There are over 123 million adults across high-risk regions (Africa, Latin America, parts of Asia) who are financially active but vulnerable to coercion, robbery, or fraud during banking transactions.

Our app targets this growing population, offering peace of mind and protection.

Market Size

- **2 billion people use mobile banking around the world, and that number is growing.**
- **Target Users:**
- **40% of mobile banking users live in cities and use banking apps often.**
- **25% live in rural or dangerous areas where people are more likely to be forced to transfer money.**
- **15% are young people who are tech-savvy but also at risk for fraud.**
- **10% are small business owners who make many mobile transactions.**
- **10% are wealthy individuals who are often targeted for large sums of money.**
- **Fraud Problem: Mobile banking fraud costs $5 trillion globally, showing the need for better security.**
- **Growth: The market for banking security is growing fast, and it's a great time to introduce the Danger Password System.**

High-Net-Worth Individuals (HNWI)
10%

Small Business Owners
10%

Urban Mobile Bank Users
40%

Youth & Students
15%

Rural Bank Users in High-Risk Areas
25%

Competitors

1. Apple Pay & Google Pay – Secure payments but don't have emergency features for forced transactions.
2. Two-Factor Authentication (2FA) – Provides extra security but doesn't work in duress situations.
3. Fraud Protection Apps (e.g., LifeLock) – Protect from fraud but don't offer real-time emergency alerts.

Why We're Different:

- Our Danger Password allows users to make transactions under duress, showing only a small balance and sending silent alerts for help.
- It's the only solution designed specifically for forced transactions, keeping users safe while complying with attackers.
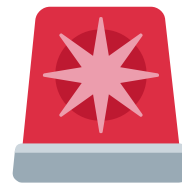
Competitive Advantage

Our solution is unique because it focuses on a real-life problem that most banking apps ignore — forced transactions under threat. Here's what makes us stand out:

🛡️ Danger Password System

- Allows users to enter a special password when under threat.
- Shows a fake low balance and hides real savings/accounts.
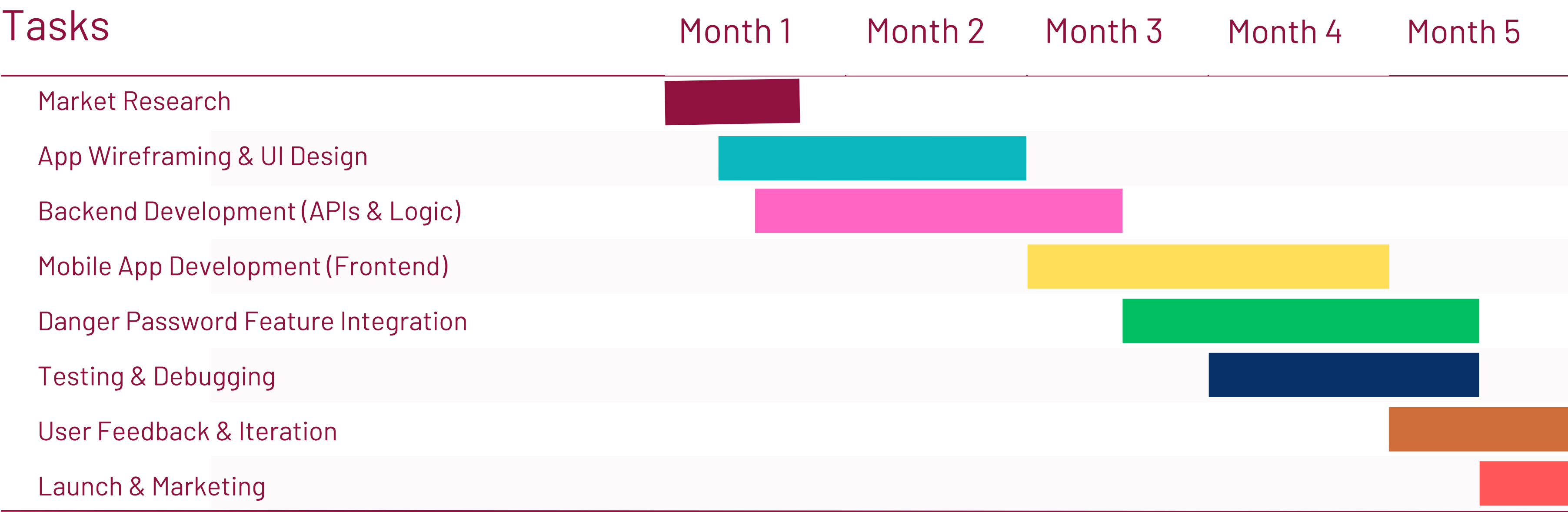- Sends silent emergency alerts without the attacker knowing.

🚨 Real-Time Emergency Response

- Alerts are sent via WhatsApp, SMS, or push notifications.

Project Traction

Tasks	Month 1	Month 2	Month 3	Month 4	Month 5
Market Research					
App Wireframing & UI Design					
Backend Development (APIs & Logic)					
Mobile App Development (Frontend)					
Danger Password Feature Integration					
Testing & Debugging					
User Feedback & Iteration					
Launch & Marketing					

Business Model

Revenue Model – How We Make Money

💰 *1. Subscription Model*

- Partner banks pay a monthly fee to integrate the Danger Password system into their mobile apps.
- Example: $5,000/month per bank, depending on number of users.

📲 *2. Premium App Version*

- Individuals can subscribe to a premium version of the app for added features like:
  - Custom emergency contacts
  - Location tracking history
  - Advanced alert options
- Example: $2.99/month per user

🔒 *3. Security Company Partnerships*

- We earn revenue by licensing the alert system to security firms that want to provide extra protection services.

Profit Margins

📊 Estimated Profit Margin: 60–70%

- Low operational costs once the app is built (maintenance, updates, cloud hosting).
- Most costs are upfront (development & marketing), making this highly scalable.
- The system is automated, reducing human labor needs.

🚀 Go-To-Market Strategy

🏛️ 1. Bank & Fintech Partnerships
- Offer the Danger Password system as a security add-on for banks.
- White-label option for seamless integration into existing apps.

📱 2. Mobile App Launch
- Launch standalone app on Android & iOS.
- Target users in high-risk regions.

🛡️ 3. Security Company Collaboration
- Partner with private security firms to handle alerts.
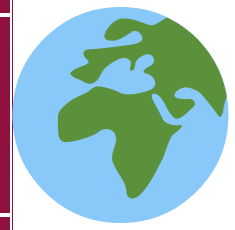- Enable real-time guardian response.

📣 4. Digital Marketing Campaigns
- Use social media, short videos, and infographics to educate users.
- Run targeted ads on Google, Facebook, and Instagram.

📰 5. Media & Influencer Outreach
- Pitch to tech journalists and safety bloggers.
- Share compelling real-world scenarios of how the app saves lives.

🌍 Social Impact – SDGs Addressed

✅ SDG 16: Peace, Justice and Strong Institutions
- Promotes safer access to financial systems.
- Helps combat financial crimes and protect human rights.

✅ SDG 9: Industry, Innovation and Infrastructure
- Leverages innovative technology to enhance security in financial services.

✅ SDG 11: Sustainable Cities and Communities
- Supports safer urban environments by reducing the impact of organized crime.

✅ SDG 5: Gender Equality
- Helps protect vulnerable individuals, especially women, who are often targeted in financial abuse situations.

✅ SDG 8: Decent Work and Economic Growth
- Encourages secure participation in digital finance, which is key for economic development.

Our Ask

We are seeking $100,000 in funding to bring the Danger Password Banking System to life and protect users under threat.

💰 Use of Funds

🔧 40% – Product Development

- Build and test the mobile app
- Integrate biometric and banking APIs

📢 25% – Marketing & Awareness

- Targeted digital campaigns
- Educational content and outreach

🤝 15% – Partnerships & Licensing

- Collaborate with banks and security companies
- Legal and compliance support

🔒 10% – Security Audits & Testing

- Ensure high-level protection and system reliability

👩‍💻 10% – Team & Operations

- Hire key team members (devs, legal, support)

Team

Andile Gracious Dhlamini – Software Engineering Student, Aspiring AI & Security Developer

Thank you!

✉️ Email: vlkz.andy@gmail.com
📱 Phone: +27 76 380 2019
📍 Location: Johannesburg, South Africa