Firma Money Protection pracowała nad aplikacją „Uwaga Oszust", z racji rozbudowy funkcji została zmieniona nazwa systemu na HumanLock360 (doszły nowe funkcje oraz Moduł SOS), zmiana była konieczna.

HumanLock360 - Wielowarstwowy Ekosystem Prewencyjnej Ochrony Głosowej oraz Infrastruktury Krytycznej

GOTOWOŚĆ WDROŻENIOWA PODSTAWOWYCH FUNCJI (kwiecień - maj 2026)

1. ANALIZA ZAGROŻEŃ I MISJA (PROBLEM & MISSION)

Według rygorystycznych szacunków ekspertów sektora bankowego, straty Polaków wynikające wyłącznie z manipulacji telefonicznych (vishing) oraz phishingu SMS, osiągnęły astronomiczną kwotę blisko **800 mln złotych**. Skala ta obrazuje profesjonalizm międzynarodowych grup przestępczych, które wykorzystują zaawansowaną socjotechnikę i AI. HumanLock360 powstał, aby przerwać proces manipulacji tam, gdzie zawodzi czynnik ludzki. Naszą misją jest ochrona pieniędzy, zdrowia i życia obywateli w przedziale wiekowym **13 – 90 lat** poprzez bezkompromisowe bezpieczeństwo komunikacji.

2. UNIKALNA PRZEWAGA TECHNOLOGICZNA: DETERMINISTYCZNA OCHRONA (NO-AI)

W przeciwieństwie do powszechnych trendów rynkowych, HumanLock360 całkowicie rezygnuje z zawodnych algorytmów AI i biometrii głosu na rzecz rozwiązań deterministycznych

Odporność na ataki typu semantycznego (Prompt Injection)

W dobie profesjonalizacji cyberprzestępczości, systemy oparte wyłącznie na modelach AI stają się podatne na nowe klasy zagrożeń, takie jak *Prompt Injection* (manipulacja logiką modelu poprzez tekst). HumanLock360 eliminuje to ryzyko u źródła.

Zamiast polegać na statystycznym prawdopodobieństwie algorytmów AI, które można „oszukać" odpowiednio sformułowaną frazą, stosujemy **podejście deterministyczne**. Nasz system bazuje na twardej analizie intencji i wzorców manipulacji, co czyni go odpornym na kreatywne próby obejścia zabezpieczeń, o których coraz częściej alarmują czołowi eksperci cybersecurity w Polsce.

- **Analiza Intencji, nie Biometrii:** System nie szuka głosu oszusta, lecz skupia się na semantyce ataku – analizie wypowiadanych **SŁÓW, ZWROTÓW i POLECEŃ** (np. „podaj kod BLIK", „przelej środki na bezpieczne konto").
- **Odporność na Deepfake Voice:** Dzięki autorskiej bazie ponad **30 000 wzorców manipulacji**, system jest w 100% odporny na technologię klonowania głosu. Dla ochrony nie ma znaczenia, czyim głosem mówi napastnik, lecz jakie polecenia wydaje ofierze.
- **Automatyczna Reakcja i Blokowanie:** W momencie wykrycia krytycznych fraz, system działa natychmiastowo:
  - **Rozłącza połączenie**, uniemożliwiając dokończenie ataku.
  - **Wrzuca numer do globalnej bazy** potencjalnych oszustów HumanLock360.
  - **Automatycznie wysyła zgłoszenie** o incydencie do odpowiednich służb państwowych, dostarczając twardy dowód próby popełnienia przestępstwa.

3. STRATEGIA „HARDWARE BRIDGE" – OCHRONA 360° (KOMUNIKATORY I WIDEO)

W odpowiedzi na restrykcyjną politykę Apple/Google oraz szyfrowanie WhatsApp/Zoom, rozwijamy technologię **Hardware Bridge**:

- **Niezależna Stacja Bazowa:** Fizyczne urządzenie (skrzynka domowa lub wtyczka desktopowa) analizujące fizyczną falę dźwiękową docierającą do użytkownika.
- **Ominięcie Barier:** Pozwala na skuteczną ochronę w rozmowach wideo i na komunikatorach, gdzie tradycyjne aplikacje mobilne są blokowane przez producentów telefonów.
- **Ochrona Wielopokoleniowa:** System dedykowany dla seniorów w domach, młodzieży (13+) oraz pracowników na stanowiskach wrażliwych w firmach prywatnych.

4. BEZPIECZEŃSTWO I PRYWATNOŚĆ (PRIVACY BY DESIGN)

- **Tryb Full Offline:** Ochrona działa bez dostępu do Internetu, co wyklucza ryzyko wycieku danych do chmury i zapewnia stabilność w każdych warunkach.

- **Brak Inwigilacji:** Aplikacja nie nagrywa, nie archiwizuje i nie przesyła treści rozmów poza lokalne urządzenie użytkownika.
- **Mechanizm Punktów Karnych:** System w milisekundach ocenia ryzyko. Powtórzenie fraz manipulacyjnych skutkuje natychmiastową blokadą i izolacją zagrożenia.

Voice Antivirus Model: Skanujemy audio wyłącznie w poszukiwaniu „wirusów słownych" (frazy i polecenia). Brak nagrywania i przesyłania treści rozmów (Tryb Full Offline).

Interwencja Behawioralna: Mechanizm dyskretnego „pikania" skłania użytkownika do włączenia głośnika, co aktywuje pełną moc analityczną tarczy.

5. OCHRONA INFRASTRUKTURY KRYTYCZNEJ I GOVTECH (STRATEGICZNY FILAR)

Nasze rozwiązanie dla central VoIP zabezpiecza komunikację w kluczowych węzłach państwa:

- **Administracja i Samorząd:** Ministerstwa, Sądy, Urzędy Miast i Gmin, ZUS, Administracja Skarbowa.
- **Infrastruktura Krytyczna:** Wodociągi, Zakłady Energetyczne, Szpitale oraz Służby Ratownicze (Policja, PSP, OSP).

W tych punktach, poprzez procedurę **Hasła Bezpieczeństwa**, system aktywnie uniemożliwia wyłudzenie danych wrażliwych oraz manipulację personelem strategicznym.

Prosty przykład:

1 JAK WYGLĄDA ATAK (dziś – bez systemu)

 Telefon do sekretariatu / dyspozytora:

„Dzień dobry, dział IT z centrali / operator systemu / firma serwisowa.
Mamy alert bezpieczeństwa. Proszę potwierdzić, kto ma dostęp do systemu i jaki macie VPN."

Pracownik:

- jest zaskoczony
- boi się awarii
- chce „pomóc"
- zaczyna odpowiadać

➡ **Dane wyciekają !!!**

2 TEN SAM ATAK Z SYSTEMEM

 Telefon przychodzi do Wodociągów
 System HumanLock360 – Instytucje" działa **w tle**

 Krok 1 – wykrycie kontekstu zagrożenia (nie jedne słowo tylko 2-3 tzw. „ZŁE" frazy

System słyszy frazy:

- „dział IT"
- „alert"
- „system"
- „dostęp"
- „proszę potwierdzić"
- „hasło"
- „VPN"

➡ **Automatyczne podniesienie poziomu zagrożenia**

---

3 Krok 2 – WYMUSZENIE HASŁA JEDNOSTKI (KLUCZ)

System **nie pyta pracownika**.
System **sam przejmuje rozmowę**:

 Komunikat systemowy (Na ekranie telefonu, lub system mowy):

„Połączenie objęte ochroną bezpieczeństwa. Proszę podać aktualne Hasło Autoryzacyjne jednostki”

 Hasło:

- znane tylko:
  - dyrektorowi
  - dyspozytorom
  - certyfikowanym podmiotom (np. prawdziwe IT)
- zmieniane np. **co 7 / 14 / 30 dni**
- NIE JEST wpisywane w rozmowie codziennej

6. MODEL BIZNESOWY I STRATEGIA DYSTRYBUCJI

Stosujemy innowacyjny model **B2G2C / B2B2C** oparty na unikalnych kodach QR:

- **Partnerstwa Samorządowe:** Jednostki publiczne finansują licencje dla mieszkańców (szczególnie seniorów) z funduszy celowych. (Kongresy dla wójtów i burmistrzów w każdym województwie) co skróci rozmowy z gminami. Zbierając ich wszystkich w jednym miejscu, omawiamy problem oszustw i jednocześnie dajemy „wędkę” odnośnie aplikacji/systemu. Wówczas mamy całość Edukacja + Narzędzie. Ma to na celu skrócenie czasu dystrybucji i skalowania (grupa – SENIORZY)
- **Sektor Korporacyjny:** Dystrybucja poprzez Banki, Firmy Ubezpieczeniowe i Operatorów GSM.
- **Analityka Big Data:** Generujemy statystyki trendów przestępczych (metody, słowa-klucze) dla instytucji finansowych i organów ścigania.

7. SKALOWALNOŚĆ I POTENCJAŁ RYNKOWY (EUROPA I USA)

Z potencjałem dotarcia do **30 mln osób w Polsce, 600 mln w Europie i 300 mln w USA**, HumanLock360 jest gotowy do globalnego skalowania.

Analiza rynku europejskiego (UE + Wielka Brytania):

- **Skala prób:** Prawie **50% populacji UE** stało się celem oszustw telefonicznych. W samej Polsce liczba incydentów wzrosła o **152% r/r**.
- **Koszty ekonomiczne:** Wielka Brytania straciła rekordowe **33,2 mld USD** w 2024 r. Niemcy szacują ogólne straty z cyberprzestępczości na **267 mld EUR**.
- **Skuteczność:** Około **10% mieszkańców UE** straciło pieniądze w wyniku vishingu. Europol wskazuje na tysiące połączeń dziennie z "fabryk oszustw".

Analiza rynku USA:

- **Kryzys narodowy:** Straty z oszustw osiągnęły poziom **12,5 – 16,6 mld USD** rocznie (wzrost o **25% r/r**).
- **Intensywność:** Aż **68% dorosłych Amerykanów** otrzymuje scamerskie połączenia przynajmniej raz w tygodniu.
- **Sektor Senioralny:** Realne, niezgłoszone szkody w grupie 60+ szacuje się na astronomiczne **81,5 mld USD**. Średnia strata na jedną ofiarę wzrosła do **3 690 USD**.

8. PARTNERSTWO INWESTYCYJNE I MISJA (INVESTMENT & IMPACT)

Poszukujemy **Odpowiedniego Partnera Inwestycyjnego**, który poza wsparciem kapitałowym, podzieli naszą **misję społeczną**. Szukamy partnera, który chce realnie pomagać – chronić najsłabszych, w tym seniorów i osoby wykluczone cyfrowo, przed bezwzględną cyberprzestępczością.

Zależy nam na inwestorze, który pomoże nam strategicznie otworzyć drzwi do kluczowych rynków międzynarodowych i struktur rządowych, traktując projekt jako inwestycję o wysokim wpływie społecznym (**Impact Investing**).

Wspólnie przekształcimy nasze działające MVP w ogólnoświatowy standard bezpieczeństwa komunikacji, ratując finanse, zdrowie, i życie obywateli. Tak samo zależy nam aby nasze Państwo Polskie było Bezpieczne szczególnie w tych obecnych trudnych czasach.