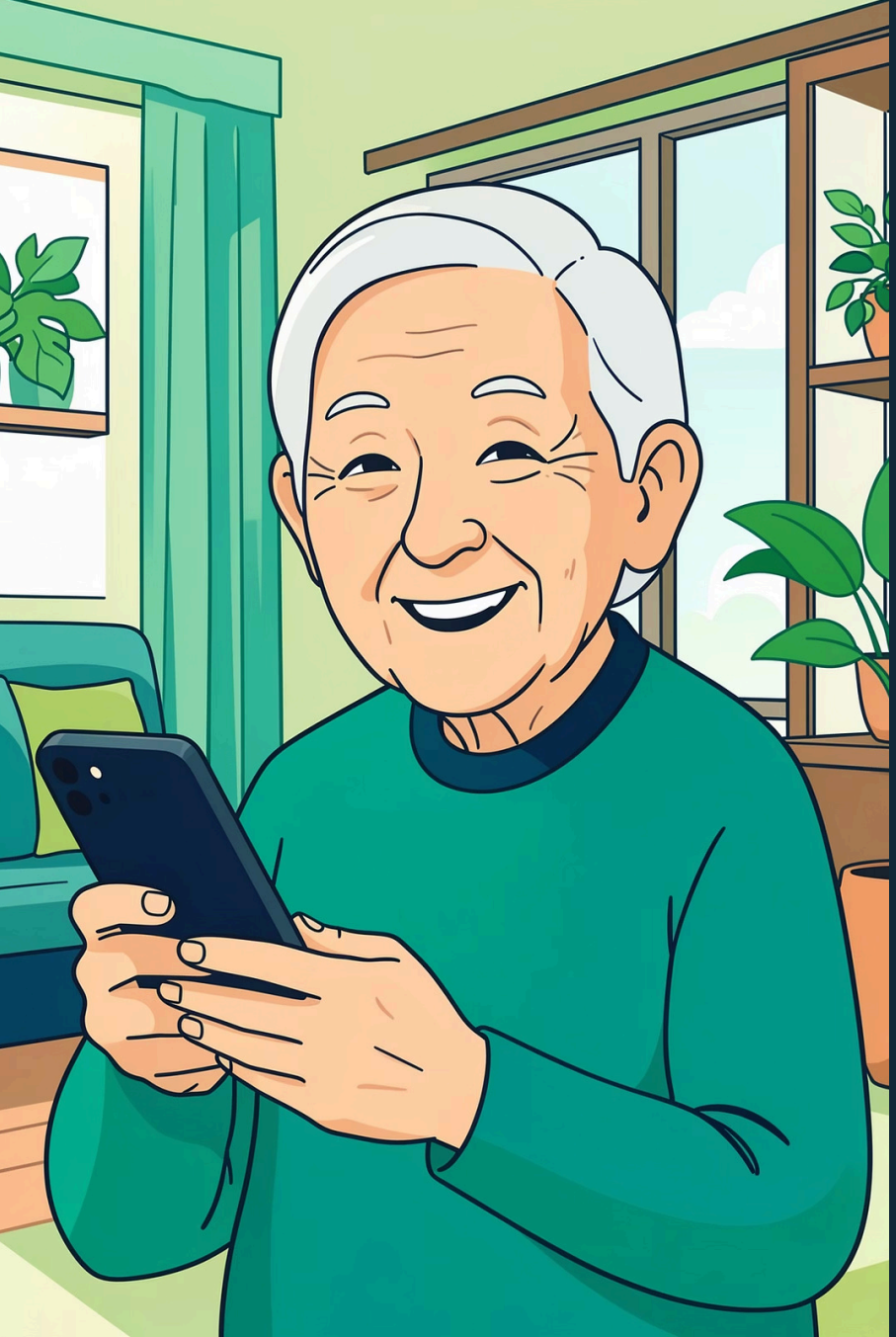


Bezpieczeństwo cyfrowe dla seniorów

Praktyczny przewodnik po bezpiecznym korzystaniu ze smartfona i internetu

WPROWADZENIE

Dlaczego bezpieczeństwo cyfrowe jest ważne?

Smartfon to dziś nieocenione narzędzie – łączy nas z rodziną, umożliwia kontakt z bankiem, lekarzem i urzędami. Dzięki niemu możemy załatwić wiele spraw z domu.

Niestety, przestępcy coraz częściej wykorzystują telefony i internet do oszustw. Atakują osoby starsze, licząc na ich zaufanie i mniejszą znajomość technologii.

Dobra wiadomość? Wystarczy poznać kilka prostych zasad, by uniknąć większości zagrożeń i cieszyć się bezpiecznym korzystaniem z technologii.

⚠ ZAGROŻENIA

Najczęstsze zagrożenia dla seniorów

Oszuści stosują różne metody, by wyłudzić pieniądze lub dane osobowe. Poznanie najpopularniejszych sposobów to pierwszy krok do ochrony.

📞 Fałszywe telefony

Oszuści podają się za wnuczka w tarapatach, policjanta prowadzącego sprawę lub pracownika banku. Wywierają presję czasową i proszą o pieniądze lub dane.

✉️ Podejrzane wiadomości

SMS-y i e-maile z linkami rzekomo od banku, poczty lub urzędu. Kliknięcie w link może prowadzić do fałszywej strony lub zainstalować złośliwe oprogramowanie.

🌐 Fałszywe strony internetowe

Witryny udające bank, pocztę lub sklep. Wyglądają niemal identycznie jak oryginały, ale służą do kradzieży haseł i danych karty.

📲 Złośliwe aplikacje

Aplikacje pobrane spoza oficjalnych sklepów mogą kraść dane, podsłuchiwać rozmowy lub blokować telefon z żądaniem okupu.

💳 Wyłudzanie danych i pieniędzy

Oszuści stosują różne preteksty – dopłata do przesyłki, zwrot podatku, blokada konta – by wymusić podanie PIN-u, hasła lub kodu SMS.

ZASADA NR 1

Nie ufaj nieznajomym

Pamiętaj: bank, policja i urzędy nigdy nie proszą o poufne dane

Żadna instytucja nie zadzwoni z prośbą o podanie:

- PIN-u do karty lub konta
- Haseł do bankowości internetowej
- Pełnego numeru karty płatniczej
- Kodów SMS otrzymanych z banku
- Danych do logowania

W razie wątpliwości: Rozłącz się i zadzwoń samodzielnie na oficjalny numer banku lub instytucji. Nigdy nie oddzwaniaj na numer podany przez rozmówcę.

Co robić, gdy ktoś dzwoni?

Zachowaj spokój. Nie daj się ponaglać. Powiedz, że oddzwonisz. Sprawdź numer w oficjalnych źródłach. Skonsultuj się z rodziną.

OCHRONA PODSTAWOWA

Bezpieczne hasła i blokada telefonu

Zabezpiecz dostęp

Zawsze ustaw PIN, wzór lub odcisk palca na telefonie. To pierwsza linia obrony przed nieuprawnionym dostępem.

Automatyczna blokada

Ustaw blokadę ekranu po kilku minutach bezczynności. Dzięki temu telefon zablokuje się sam, gdy o tym zapomnisz.

Nie zapisuj haseł

Nie trzymaj kartek z hasłami przy telefonie lub w portfelu. Jeśli muszą być zapisane, przechowuj je w bezpiecznym miejscu w domu.

Unikalne hasła

Każda usługa (bank, e-mail, social media) powinna mieć własne, inne hasło. Tak trudniej ukraść wszystkie konta naraz.

SMS I LINKI

Bezpieczne SMS-y i linki

Ostrożność z wiadomościami

Nie klikaj w linki z nieznanych SMS-ów lub e-maili. Przestępcy często podszywają się pod znane firmy i instytucje.

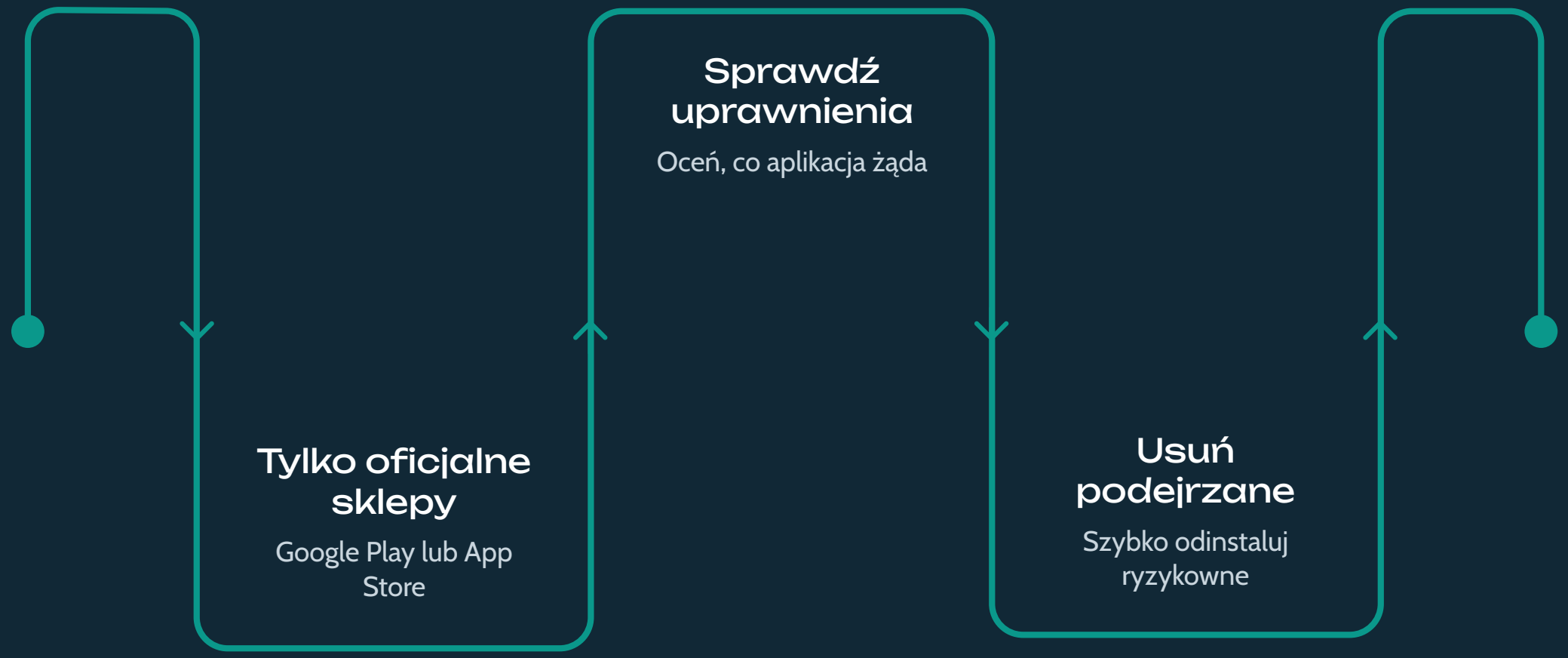
SMS o paczce lub dopłacie?

Jeśli dostajesz wiadomość o przesyłce wymagającej dopłaty lub zwrocie podatku – nie klikaj! Sprawdź bezpośrednio u źródła: zadzwoń do firmy kurierskiej lub wejdź na stronę urzędu samodzielnie.

Sygnały ostrzegawcze:

- Błędy językowe i literówki
- Presja czasowa („zapłać natychmiast")
- Dziwny adres nadawcy
- Prośba o dane osobowe lub płatność

Aplikacje – tylko z zaufanego źródła



Aplikacje są bardzo użyteczne, ale mogą też stanowić zagrożenie, jeśli pochodzą z niewiarygodnych źródeł.

Pobieraj tylko z oficjalnych sklepów

Google Play (Android) i App Store (iPhone) sprawdzają aplikacje przed publikacją. Nigdy nie instaluj aplikacji z linku w SMS-ie czy e-mailu.

Sprawdzaj uprawnienia

Jeśli aplikacja latarka chce dostępu do kontaktów lub mikrofonu – to podejrzane. Każda aplikacja powinna prosić tylko o niezbędne funkcje.

Usuń podejrzane aplikacje

Gdy coś wydaje się dziwne (telefon działa wolniej, pojawiają się reklamy), natychmiast odinstaluj podejrzaną aplikację.

FINANSE

Bezpieczne korzystanie z banku

Ochrona finansów to priorytet

Oficjalna aplikacja banku

Korzystaj wyłącznie z aplikacji pobranej z Google Play lub App Store. Sprawdź nazwę wydawcy – musi być to Twój bank.

Nigdy nie podawaj kodów SMS

Kody z SMS-ów od banku służą do potwierdzania operacji. Nikt – nawet pracownik banku – nie powinien ich od Ciebie wymagać.

Włącz powiadomienia

Powiadomienia o każdej transakcji pozwolą szybko zauważyć podejrzane operacje i zareagować.

PODSUMOWANIE

Złote zasady bezpieczeństwa cyfrowego

Zapamiętaj te pięć prostych zasad, które ochronią Cię przed większością zagrożeń w sieci:

1

Nie ufaj – sprawdzaj

Weryfikuj tożsamość dzwoniących i nadawców wiadomości. W razie wątpliwości dzwoń samodzielnie na oficjalny numer.

2

Nie klikaj – jeśli nie wiesz

Linki w SMS-ach i e-mailach mogą prowadzić do fałszywych stron. Lepiej wejść na stronę samodzielnie.

3

Nie podawaj poufnych danych

PIN, hasła, kody SMS – to informacje tylko dla Ciebie. Żadna instytucja ich nie potrzebuje.

4

Zabezpiecz telefon

Blokada ekranu, silne hasła i aplikacje z oficjalnych źródeł to podstawa bezpieczeństwa.

5

Pytaj bliskich

Gdy coś budzi wątpliwości, porozmawiaj z rodziną lub zaufaną osobą. Lepiej zapytać niż stracić pieniądze.

Pamiętaj: Aktualizuj regularnie system telefonu i aplikacje – to kluczowe dla bezpieczeństwa. Włącz automatyczne aktualizacje, by być zawsze chroniony najnowszymi zabezpieczeniami.