JAK CHRONIĆ SWOJE PIENIĄDZE **PRZED HAKERAMI**

Bezpieczne bankowanie

MAŁGORZATA EWA KACHEL

O czym jest ten poradnik?

JAK BEZPIECZNIE BANKOWAĆ ZA POŚREDNICTWEM INTERNETU

Co musisz zweryfikować? Co trzeba sprawdzić?
O czym dobrze wiedzieć,
zanim zaczniesz *Bezpiecznie Bankować* w sieci.

„WSZYSCY KŁAMIĄ”

dr HOUSE

Benjamin Graham

„UFAJ, ALE SPRAWDZAJ”

A jeżeli Ci powiem, że istnieje magiczna różdżka?

I za jej dotknięciem Twoje tytaniczne zmagania zamienią się w **lekkie i przyjemne działania** i rozwiną TWOJĄ MARKĘ z prędkością światła...

Znam wyzwania z jakimi borykasz się w sieci

Ponad 17 lat prowadzę innowacyjny biznes online.
W 2006 roku otworzyłam pierwszą w Polsce Galerię Sztuki Cyfrowej, udowodniłam, że sztukę i technologię można ze sobą połączyć.

Od początku mojej obecności w Internecie miałam ogrom wyzwań związanych z technicznymi aspektami prowadzenia biznesu w sieci.

Zapraszam Cię do dołączenia do mojej społeczności kobiet, które z powodzeniem wykorzystują sztuczną inteligencję w swoich biznesach online.

POZNAJ AI SZTUCZNĄ INTELIGENCJĘ, KTÓRA PRACUJE ZA CIEBIE

Pomagam kobietom w łatwiejszym korzystaniu z najnowszych rozwiązań technicznych i wykorzystaniu
Sztucznej Inteligencji w skutecznym prowadzeniu biznesu online.

Rozumiem, że technologia może być dla Ciebie trudna, ale wiem, że każda kobieta może z niej korzystać i odnieść sukces.
Nie bój się technologii, po prostu naucz się jej używać!
Jestem tutaj, aby pomóc Ci to osiągnąć!

Moją misją jest pomóc kobietom w rozwoju ich biznesów poprzez wykorzystanie Sztucznej Inteligencji i wsparcie w używaniu technologii do rozwoju swoich działań on-line

Jeden z czołowych ekspertów w dziedzinie sztucznej inteligencji, Andrew Ng mówi:
„Sztuczna inteligencja to nowa elektryczność.”
Moja droga, to jest rewolucja, której moc już lata temu poznały nasze babki, **zamieniając ocynkowaną balię na automatyczną pralkę.**

Masz więcej czasu dla siebie, dla swoich dzieci a Twój biznes rośnie dzięki:

A.I. Marka.

Małgorzata Ewa Kachel

Dzień Dobry

Moją detektywistyczną wiedzę, oraz siedemnastoletnie doświadczenie w prowadzeniu biznesu 0n-line (od 2006r sprzedaję swoje produkty w Internecie), przekładam na realną wartość działań.

Szkolę kobiety, jak bezpiecznie prowadzić biznes w sieci.

Ze mną zweryfikujesz kontrahentów i uchronisz swoją firmę przed atakiem hakerów, scamerów
i różnego rodzaju oszustów.

A po pracy?

Po pracy będziesz wiedziała jak bezpiecznie randkować w Internecie.
Jeżeli już masz rodzinę, nauczę Cię jak zadbać o bezpieczeństwo dzieci i męża.

Małgorzata E. Kachel

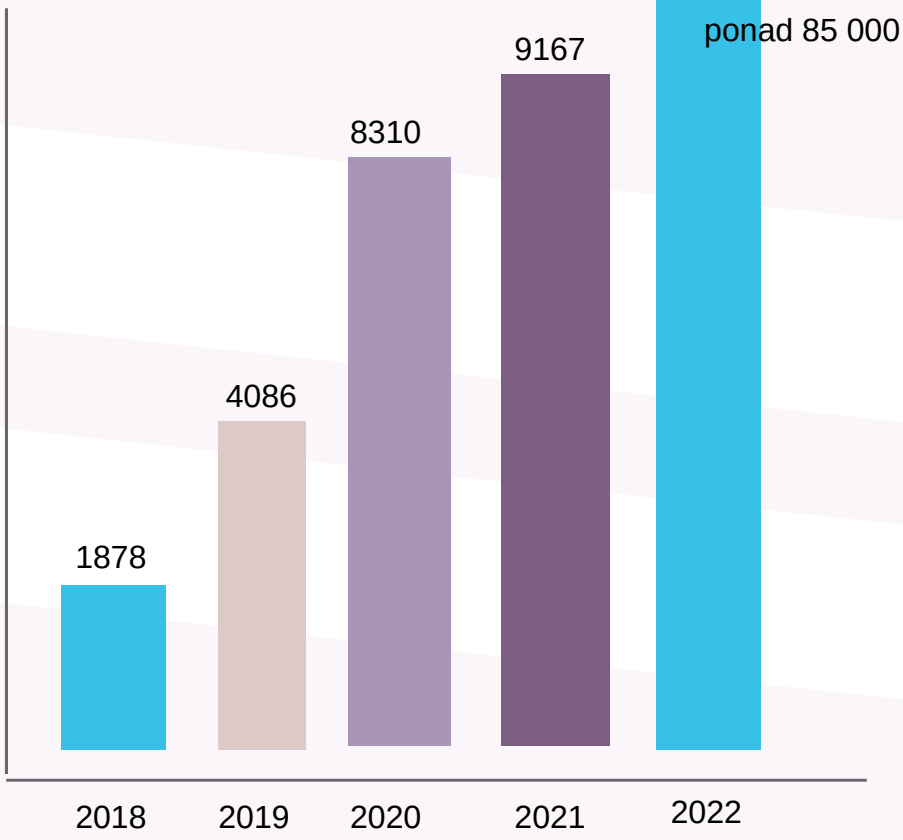
CO ZNAJDZIESZ
W PORADNIKU

SPIS TREŚCI

OSZUSTWA KOMPUTEROWE

LATA **2018-2022** DANE: CERT POLSKA

Skala oszustw komputerowych podwaja się z roku na rok. Dane są alarmujące a nie wszystkie ofiary zgłaszają się na policję. Wystarczy przestrzegać tylko kilku zasad, żeby nie stracić oszczędności życia



01 rok 2018 - dwa tysiąc zgłoszonych przejęć i oszustw

02 rok 2019 - liczba oszustw się podwoiła

03 rok 2020 - kolejny rok z podwojoną liczbą oszustw

04 rok 2021 - niewielki skok

05 rok 2022 - zabrakło skali jeżeli chodzi o ilość zgłoszeń

Oszuści nigdy do tej pory nie działali na taką masową skalę w sieci jak w roku 2022. Rok 2023 zapowiada sie podobnie.

SŁOWNIK

PODSTAWOWE SCHEMATY WŁAMAŃ W SIECI, KTÓRYCH DEFINICJE MUSISZ ZNAĆ JEŚLI CHCESZ SIĘ OCHRONIĆ PRZED OSZUSTWAMI W INTERNECIE

PHISHING

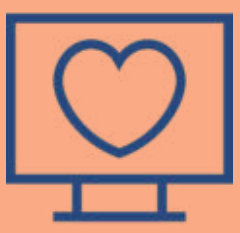
Podszywanie się pod zaufaną witrynę (bank, firmę kurierską) w celu wyłudzenia poufnych danych. Najczęściej są to podrobione witryny bankowe imitujące prawdziwe i zbierające dane do logowania.

SPOOFING

Podszywanie się pod numer telefonu lub e-mail. Oszuści najczęściej udają pracowników banków, firm kurierskich, dostawców mediów. Numer telefonu lub mail z którego się kontaktują jest taki sam jak prawdziwy.

MALWARE

To złośliwe oprogramowanie, które bez naszej wiedzy instaluje się na naszym urządzeniu. Celem jest przejęcie danych do logowania, lub zaszyfrowanie danych i żądanie okupu.



ZDALNY PULPIT

Oprogramowanie, które umożliwia osobie z zewnątrz zarządzać naszym telefonem lub komputerem. Po instalacji, do której namawia Cię oszust, tracisz kontrolę nad swoim sprzętem.

NIEZBĘDNE NARZĘDZIA

JEŚLI Z NICH JESZCZE NIE KORZYSTASZ, TERAZ JEST CZAS NA PRZYGOTOWANIA

OBOWIĄZKOWE

Programy antywirusowe

Zainstaluj oprogramowanie antywirusowe na komputerze, tablecie i telefonie. Uchroni Cię przed malware.

Aktualizacja oprogramowania

Aktualizuj na bieżąco system operacyjny telefonu, tabletu i komputera oraz programy, jeżeli tego wymagają.

Menadżer haseł

Zacznij używać menadżera haseł. Wystarczy darmowy **KeepassXC.** Zawsze ustawiaj unikalne hasła.

OPCJONALNE

Dodatkowy smartfon

Jeżeli chcesz być jeszcze bardziej bezpieczna kup dodatkowy numer telefonu i smartfon.
Będziesz go używać tylko do bankowości internetowej.
Jest to dobre rozwiązanie choć hakerzy już potrafią je obejść.

ELEMENTARNE ZASADY BEZPIECZNEGO BANKOWANIA

W 3 PROSTYCH KROKACH

01

Zawsze loguj się do banku korzystając z bezpiecznego połączenia z Wifi.
Nie łącz się z otwartych sieci w barach, restauracjach, hotelach.

02

Jeżeli zgubisz dokument tożsamości zastrzeż go w banku tak szybko jak to możliwe.
Powiadom policję, jeżeli dokument został skradziony.

03

Zawsze płac kartą w Internecie.
Dlaczego?
Wszystkiego dowiesz się z bonusu gdzie piszę o chargebacku.

Rozdział 01

DZWONI DO CIEBIE BANK

- Konsultant może ostrzegać Cię o włamaniu na konto.
- Konsultant może prosić o instalację ważnej aplikacji na telefonie.
- Konsultant może prosić o login i hasło do konta.
- Konsultant może prosić o generowanie i podanie kodów SMS.

CZY TO PRAWDZIWY PRACOWNIK BANKU?

DZWONI DO CIEBIE BANK
Jak nie zostać ofiarą **spoofingu**

SPOOFING

Podszywanie się pod numer telefonu lub e-mail. Oszuści najczęściej udają pracowników banków, firm kurierskich, dostawców mediów. Numer telefonu lub mail, z którego się kontaktują jest taki sam jak prawdziwy.

3 zasady 100% ochrony

Zawsze je stosuj. Skutecznie zabezpieczysz się przed wyłudzeniami telefonicznymi.

1

Zawsze oddzwaniaj na infolinię

Nawet jeśli jesteś przekonana, że konsultant jest prawdziwy i dzwoni z Twojego banku. Te kilka minut może uratować nie tylko pieniądze na koncie. **Oszuści logując się do banku zaciągają pożyczki.** Banki nie uznają takich reklamacji.

2

Nie instaluj żadnego oprogramowania

Konsultant będzie chciał Cię namówić do instalacji BANKOWEGO oprogramowania. **Nigdy nie instaluj aplikacji,** których nie znasz. Nie zmieniaj domyślnych ustawień bezpieczeństwa w swoim smartfonie. Jest zablokowany przed takimi przejęciami.

3

Nie podawaj loginu, hasła, kodu SMS

Oszuści proszą o podanie **loginów, haseł, kodów jednorazowych. Prawdziwy bank nigdy nie prosi o takie dane**. Jeżeli ktoś chce od Ciebie takie informacje, rozłącz się od razu i zgłoś incydent do swojego banku.

Porada specjalistki:

Jeżeli bardzo boisz się włamania:
Kup smartfon z osobnym numerem.
Zainstaluj tam aplikacje banku i używaj numeru tylko do transakcji bankowych

Chodzi o to, żeby w tym, co złożone, szukać prostoty, zamiast niepotrzebnie komplikować i tak już skomplikowane.

Madeleine Thien

PODSUMOWANIE

Oszuści potrafią podrobić wyświetlany numer telefonu. Nie masz żadnej pewności. że to dzwoni Twój bank. Prawdziwy konsultant nie prosi o dane do logowania, kody SMS ani nie każe Ci instalować oprogramowania na tablecie lub smartfonie. Oszuści wykorzystują elementy inżynierii społecznej.
Starają się wywołać panikę, informując np. o włamaniu na Twoje konto.

Checklista

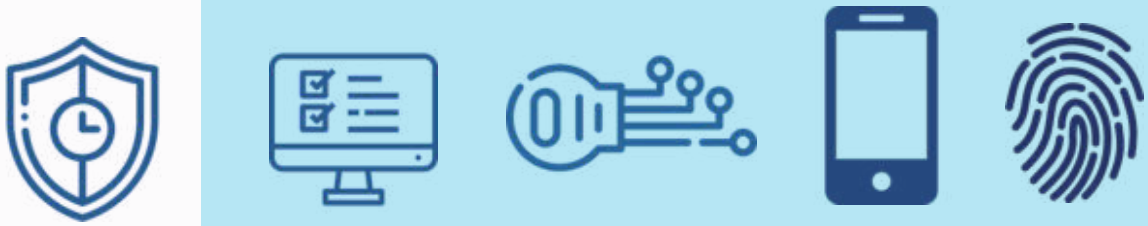
- [ ] **Zawsze oddzwaniaj do banku.**
- [ ] **Nie instaluj na telefonie ani na komputerze żadnych programów zalecanych przez konsultanta.**
- [ ] **Nikomu nie podawaj swojego loginu i hasła do banku.**

Rozdział 02

JAK PRZYGOTOWAĆ SMARTFON, TABLET, LAPTOP?

Pilnuj aby Twoje akcesoria elektroniczne:
telefon, tablet, laptop, komputer stacjonarny były zawsze dobrze przygotowane do przeprowadzania bezpiecznych transakcji.
Unikaj sytuacji, gdy do Twojego sprzętu elektronicznego mają dostęp obce osoby.
Zawsze zabezpiecz ekran - wygaszaczem hasłami, pinem.

JAK SIĘ PRZYGOTOWAĆ?
zabezpiecz urządzenie do bankowania



4 zasady 100% ochrony

Bankuj bezpiecznie używając telefonu, tabletu, laptopa i komputera stacjonarnego.

1

Aktualizuj oprogramowanie

2

Zainstaluj program antywirusowy

3

Ustaw mocne unikalne hasło

4

Zabezpiecz ekran swojego urządzenia

Porada specjalistki:

Nie instaluj oprogramowania z nieznanych zródeł. Jeżeli korzystasz ze smarfona, unikaj aplikacji o małej ilości pobrań. Tutaj też są podrabiane programy, które mogą przejąć telefon

Prostota jest szczytem wysublimowania.

Leonardo da Vinci

PODSUMOWANIE

I CHECK LISTA

Przygotowanie komputera i telefonu do bezpiecznego bankowania nie jest trudne. Nie jest potrzebny do tego, wyspecjalizowany informatyk. Zawsze możesz poprosić kogoś bardziej technicznego w rodzinie o pomoc, w zainstalowaniu menadżera haseł. Sprawdź czy już masz wszystko.

- [ ] Aktualizuj system i oprogramowanie, także to antywirusowe
- [ ] Używaj biometrii do weryfikacji w swoich urządzeniach
- [ ] Ustaw unikalne hasło TYLKO do banku
- [ ] Nie pozwalaj nikomu na dostęp do swoich urządzeń, których używasz do bankowania

Rozdział 03

APLIKACJA CZY KODY SMS

Zapoznaj się z wadami i zaletami obu sposobów potwierdzania transakcji w serwisie bankowym.
Oceń jakie zagrożenia niesie ze sobą każda z tych form dla Twojego sposobu używania smartfona.
Zdecyduj, która forma potwierdzania transakcji jest bezpieczna.

Co wybrać? SMS czy PUSH?

Zobacz porównanie tych dwóch metod potwierdzania transakcji i zdecyduj sama, której używać.

NIE WIESZ CO WYBRAĆ?

PORÓWNANIE DWÓCH METOD POTWIERDZANIA TRANSAKCJI BANKOWYCH

Kody SMS

Wystarczy zwykły telefon obsługujący SMSy

- Łatwo przekierować kod na inny numer telefonu. W przypadku włamania do telefonu oszust będzie przesyłał kody dalej.

W smartfonach zainstalowane aplikacje bardzo często mają dostęp do czytania SMSów.

- Pomimo coraz lepszych zabezpieczeń w firmach telekomunikacyjnych, jest możliwość wykonania duplikatu karty bez wiedzy właściciela numeru.

SMS z kodem potrafi mieć ucięty kawałek i nie widać komunikatu co potwierdzasz.

Aplikacja

Niezbędne jest posiadanie smartfonu i systemu Android lub IOS.

Każdy push jest szyfrowany i aplikacje ze smartfona nie mają do nich dostępu.

Nie ma możliwości przekazania pusha do autoryzacji transakcji z innego urządzenia.

Możliwość szybkiego kontaktu z konsultantami poprzez aplikacje banku w telefonie.

Na ekranie smartfonu wyświetla się szczegółow0 potwierdzanie transakcji, kwota przelewu oraz dane odbiorcy przelewu.

Porada specjalistki:

Wykorzystaj wszystkie możliwe zabezpieczenia jakie daje Twój Bank. To będzie uciążliwe i niewygodne ale sama sobie podziękujesz kiedy hakerzy wezmą na celownik Twoje Konto

Trawimy życie na drobiazgach. Prostota, prostota i jeszcze raz prostota! Tak, niechaj ludzkie sprawy ograniczą się do dwóch czy trzech.

Henry David Thoreau

Rozdział 04

CZY JESTEM W PRAWDZIWYM BANKU?

PHISHING

Podszywanie się pod zaufaną witrynę (bank, firmę kurierską, popularną platformę aukcyjną) w celu wyłudzenia poufnych danych. Najczęściej są to podrobione witryny bankowe imitujące prawdziwe strony banku, zbierające na tak podrobionych witrynach, dane do logowania.

5 kroków do weryfikacji

Poznaj niezawodne sposoby na odróżnienie prawdziwej strony banku od podstawionej przez hakerów.

JAK ZWERYFIKOWAĆ BANK?

W 5 PROSTYCH KROKACH

01

Dokładnie sprawdź adres strony w pasku wyszukiwarki

Magiczna kłódka - certyfikat SSL, sprawdź certyfikat banku w pasku przeglądarki

02

03

Loguj sie tylko przez menadżera haseł i po zakładkach zapamiętanych w Twojej przeglądarce

Sprawdzaj wiarygodność maili z banku. Nie otwieraj załączników jak mail wygląda podejrzanie - mogą zawierać malware.

04

05

W razie jakichkolwiek wątpliwości dzwoń do banku i sprawdz czy dana operacja jest /mail /transakcja jest faktycznie z banku. Dzwoń przez aplikację jak Twój Bank daje taką możliwość.

Porada specjalistki:

W razie wątpliwości zawsze dzwoń na infolinię banku.
Nie daj sie nabrać podstawionym konsultantom, że masz coś zrobić:

NIEZWŁOCZNIE, OD RAZU, SZYBKO.

Połączenie elegancji z prostotą stanowi o szlachectwie każdej rzeczy.

Charles-Maurice de Talleyrand

KLUCZOWE ASPEKTY

BEZPIECZNEGO BANKOWANIA

- Nie śpiesz się, pośpiech nigdy nie jest dobrym doradcą
- Sprawdź dokładnie adres banku w pasku wyszukiwarki
- Zapisz stronę banku w ulubionych zakładkach i tak z niej korzystaj
- Naucz się korzystać z menadżera haseł wbudowanego w przeglądarkę
- Zawsze czytaj dokładnie, co jest w powiadomieniu potwierdzenia transakcji

Rozdział 05

JESTEM W SWOIM BANKU I CO TERAZ?

Jak skonfigurować ustawienia w swoim banku,
żeby bankowanie było zawsze bezpieczne.

CO MOGĘ SAMA ZROBIĆ W BANKU?

O tym pamiętaj i ustaw od razu

Zostań Bankową Zosią Samosią

Poznaj aplikację i stronę internetową banku.
Zabezpiecz sie sama.

BEZPIECZNE BANKOWANIE

PROSTA INSTRUKCJA KROK PO KROKU

Co warto ustawić w aplikacji bankowej lub panelu obsługi bankowości internetowej, aby zwiększyć bezpieczeństwo korzystania z niej:

1

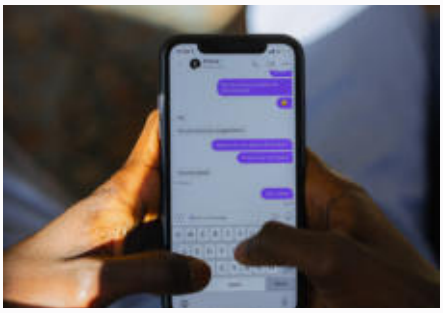
Włącz powiadomienia SMS: skonfiguruj powiadomienia SMS na swoim koncie bankowym, aby otrzymywać natychmiastowe powiadomienia o każdej transakcji dokonanej na Twoim koncie. W ten sposób możesz szybko zareagować, jeśli zauważysz jakieś podejrzane transakcje.

Ustaw mocne hasło i zmieniaj je regularnie. Nie używaj haseł, które są łatwe do odgadnięcia. Nie używaj tego samego hasła do innych kont w mediach społecznościowych lub do poczty elektronicznej.

2

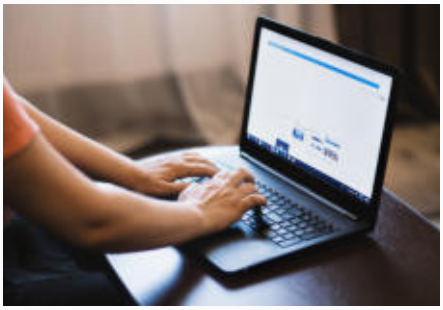
3

Używaj funkcji autoryzacji: wiele aplikacji bankowych oferuje funkcję autoryzacji, która pozwala potwierdzić transakcję za pomocą kodu jednorazowego lub Touch ID/Face ID. Używaj tych funkcji, aby zwiększyć bezpieczeństwo swojego konta.



4

Unikaj używania publicznych Wi-Fi: unikaj korzystania z bankowości internetowej na publicznych Wi-Fi, ponieważ mogą być one niezabezpieczone, co zwiększa ryzyko kradzieży Twoich danych.



Wyloguj się po użyciu: zawsze pamiętaj, aby wylogować się z aplikacji bankowej lub panelu bankowości internetowej, gdy już z niej nie korzystasz. Nie zostawiaj swojego konta otwartego, gdy nie jesteś przy komputerze lub smartfonie.

5

6

Monitoruj swoje transakcje: regularnie sprawdzaj swoje transakcje bankowe i bieżący stan konta, aby upewnić się, że nie ma nieautoryzowanych transakcji lub nieznanych opłat.

7

Używaj aktualizowanej aplikacji bankowej: upewnij się, że korzystasz z najnowszej wersji aplikacji bankowej lub panelu bankowości internetowej, ponieważ aktualizacje zazwyczaj zawierają poprawki błędów i łatki zabezpieczeń.

Ustaw limit dzienny na kwoty przelewów: większość aplikacji bankowych umożliwia ustawienie limitu dziennego na kwoty przelewów. Ustaw limit, który jest odpowiedni dla Twoich potrzeb, aby zminimalizować ryzyko nieautoryzowanych transakcji.

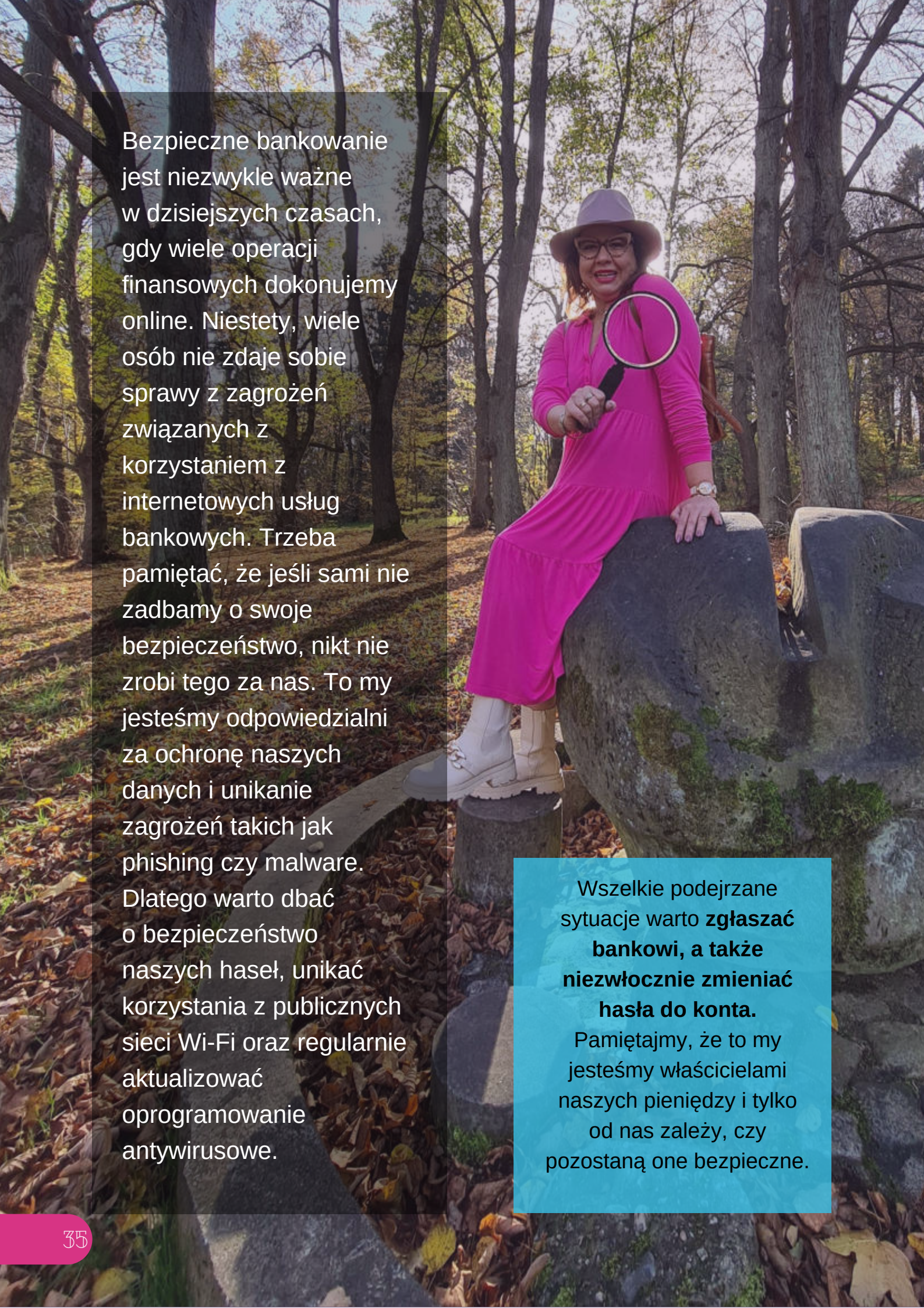
8

Porada specjalistki:

Ogranicz liczbę odbiorców, do których przesyłasz pieniądze i upewnij się, że dokładnie wiesz, kto jest odbiorcą i dlaczego wysyłasz mu pieniądze.

Życie jest naprawdę proste, lecz upieramy się by je komplikować.

Konfucjusz

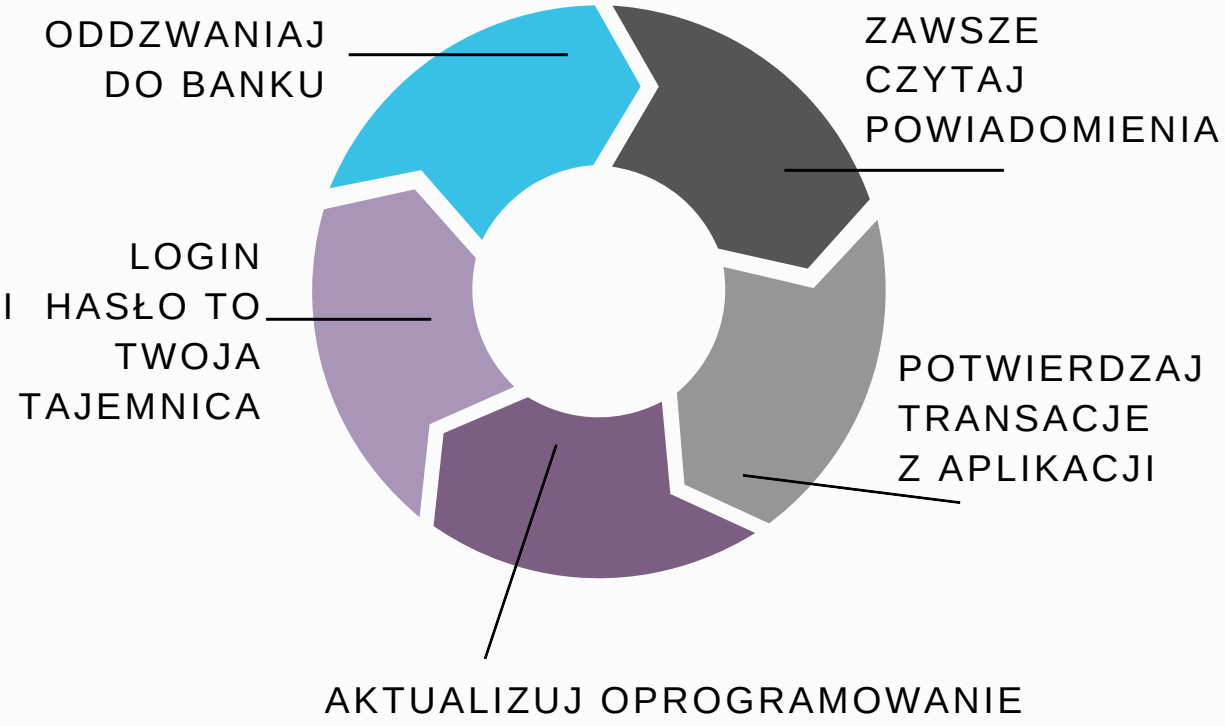


Bezpieczne bankowanie jest niezwykle ważne w dzisiejszych czasach, gdy wiele operacji finansowych dokonujemy online. Niestety, wiele osób nie zdaje sobie sprawy z zagrożeń związanych z korzystaniem z internetowych usług bankowych. Trzeba pamiętać, że jeśli sami nie zadbamy o swoje bezpieczeństwo, nikt nie zrobi tego za nas. To my jesteśmy odpowiedzialni za ochronę naszych danych i unikanie zagrożeń takich jak phishing czy malware. Dlatego warto dbać o bezpieczeństwo naszych haseł, unikać korzystania z publicznych sieci Wi-Fi oraz regularnie aktualizować oprogramowanie antywirusowe.

Wszelkie podejrzane sytuacje warto **zgłaszać bankowi, a także niezwłocznie zmieniać hasła do konta.** Pamiętajmy, że to my jesteśmy właścicielami naszych pieniędzy i tylko od nas zależy, czy pozostaną one bezpieczne.

ŚCIĄGAWKA Z BEZPIECZEŃSTWA

JAK BEZPIECZNIE BANKOWAĆ?



01 ZAWSZE ODDZWANIAJ NA INFOLINIĘ BANKU

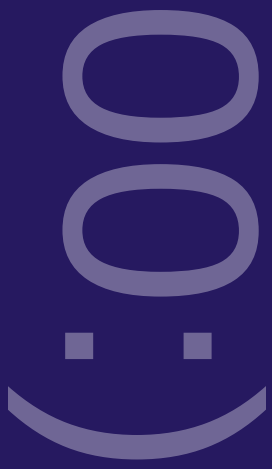
02 NIGDY NIKOMU NIE PODAWAJ LOGINU I HASŁA

03 AKTUALIZUJ SYSTEM OPERACYJNY I ANTYWIRUSA

04 POTWIERDZAJ TRANSAKCJE Z APLIKACJI BANKU

05 ZAWSZE CZYTAJ POWIADOMIENIA O TRANSAKCJI

Bonusy



MENADŻER HASEŁ
PHISHING
CHARGEBACK

Dowiedz się więcej...

ZARZĄDZAJ HASŁAMI
na wszystkich swoich urządzeniach

Menadżer haseł

Zacznij używać menadżera haseł.
Wystarczy darmowy KeepassXC.
Ostatecznie korzystaj z menadżera
wbudowanego w przeglądarkę.

MENADŻER HASEŁ TO NARZĘDZIE, KTÓRE POZWALA NA PRZECHOWYWANIE I ZARZĄDZANIE NASZYMI HASŁAMI W SPOSÓB BEZPIECZNY I WYGODNY. OTO KILKA PODSTAWOWYCH ZALET KORZYSTANIA Z MENADŻERA HASEŁ:

01

Bezpieczeństwo - menadżer haseł pozwala na przechowywanie haseł w bezpieczny sposób, zaszyfrowanych za pomocą silnego algorytmu. Dzięki temu nie musimy pamiętać wielu różnych haseł, co znacznie zwiększa nasze bezpieczeństwo w Internecie.

Wygoda - menadżer haseł pozwala na automatyczne wypełnianie pól logowania na stronach internetowych, dzięki czemu nie musimy wpisywać hasła ręcznie. W ten sposób oszczędzamy czas i unikamy popełniania błędów przy wpisywaniu haseł.

02

03

Organizacja - menedżer haseł umożliwia przechowywanie wielu różnych danych logowania i innych poufnych informacji w jednym miejscu. Dzięki temu mamy uporządkowany i łatwy do zarządzania katalog naszych danych dostępu.

Mobilność - menadżer haseł pozwala na synchronizację naszych danych logowania między różnymi urządzeniami, co daje nam możliwość korzystania z nich z każdego miejsca i o każdej porze.

04

05

Dostępność - menadżer haseł jest dostępny w wielu formach, od wtyczek do przeglądarek internetowych, po odrębne aplikacje. To sprawia, że możemy korzystać z menadżera haseł na każdym urządzeniu.

PODROBIONE STRONY
to obecnie plaga internetowa i występują wszedzie: od bankowości po firmy kurierskie

Phishing

Jak się zabezpieczyć przed podstawionymi stronami w sieci

PHISHING TO TECHNIKA ATAKU, W KTÓREJ CYBERPRZESTĘPCY PODSZYWAJĄ SIĘ POD LEGALNE INSTYTUCJE LUB OSOBY, ABY UZYSKAĆ OD UŻYTKOWNIKÓW INFORMACJE POUFNE, TAKIE JAK HASŁA, NUMERY KART KREDYTOWYCH LUB DANE OSOBOWE.

01

Bądź czujna - Zwróć uwagę na podejrzane e-maile, wiadomości SMS lub linki, które dostajesz. Szczególnie uważaj na e-maile, które informują, że Twoje konto zostało zhakowane lub wymagają pilnej akcji z Twojej strony.

Sprawdź adres e-mail - Przed kliknięciem w link lub otwarciem załącznika, upewnij się, że adres e-mail, z którego dostałeś wiadomość, jest autentyczny. Szczególnie zwróć uwagę na domenę - np. jeśli dostajesz e-maila od banku, upewnij się, że domena w adresie e-mail jest taka sama jak strona banku.

02

03

Nie podawaj poufnych informacji - Nikomu nie podawaj swojego hasła, numeru karty kredytowej lub innych poufnych informacji. Prawdziwe instytucje nigdy nie proszą o takie informacje w e-mailu.

Używaj oprogramowania antywirusowego i zaktualizowanego oprogramowania - Oprogramowanie może pomóc w wykrywaniu i blokowaniu phishingowych stron internetowych. Upewnij się również, że korzystasz z aktualnego oprogramowania i przeglądarki internetowej.

04

05

Używaj autoryzowanych kanałów komunikacji - Jeśli chcesz skontaktować się z instytucją, np. bankiem, skorzystaj z oficjalnej strony internetowej lub numeru telefonu w aplikacji. **Unikaj korzystania z linków lub numerów, które zostały przesłane do Ciebie w e-mailu lub wiadomości SMS.**

ODZYSKAJ SWOJE PIENIĄDZE

nawet jak myślisz że już jest za późno
i zostałaś oszukana jest rozwiązanie

Chargeback

Banki tego nie lubią

CHARGEBACK TO PROCES ZWROTU PŁATNOŚCI, W KTÓRYM KONSUMENT MOŻE OTRZYMAĆ PŁATNOŚĆ DOKONANĄ ZA PRODUKT LUB USŁUGĘ NA SWOJE KONTO BANKOWE, OD BANKU LUB INSTYTUCJI FINANSOWEJ, KTORA **WYDAŁA KARTĘ VISA LUB MASTERCARD.**

01

Odzyskanie pieniędzy - Chargeback umożliwia konsumentom odzyskanie pieniędzy za produkty lub usługi, które zostały niewłaściwie wykonane lub niedostarczone przez sprzedawcę. W ten sposób klienci mogą uniknąć strat finansowych

Ochrona przed oszustwami - Chargeback jest szczególnie przydatny w przypadku oszustw lub nieautoryzowanych transakcji. Klienci mają możliwość złożenia wniosku o chargeback, aby odzyskać swoje pieniądze, jeśli zostaną oszukani. lub jeśli ktoś dokonał nieautoryzowanej transakcji na ich koncie.

02

03

Łatwość użycia - Proces chargeback jest zwykle łatwy do użycia i wymaga od klientów tylko wypełnienia formularza online lub kontaktu z ich bankiem lub instytucją finansową.

Szybkie rozwiązanie - W porównaniu z innymi metodami odzyskiwania pieniędzy, proces chargeback jest zwykle szybki i skuteczny. Bank lub instytucja finansowa przeprowadza dochodzenie i podejmuje decyzję w ciągu kilku tygodni.

04

05

Bezpieczeństwo transakcji - Chargeback zapewnia klientom bezpieczeństwo transakcji i chroni ich przed stratami finansowymi w przypadku, gdy sprzedawca nie wywiązał się ze swoich zobowiązań lub w przypadku, gdy produkt lub usługa była wadliwa lub niezgodna z umową.

KIEDY MOŻESZ SKORZYSTAĆ Z CHARGEBACK

Możesz skorzystać z chargebacku w sytuacjach, gdy dokonałeś transakcji kartą płatniczą (np. kartą kredytową, debetową, prepaid) i masz poważne zastrzeżenia co do jakości lub dostarczenia produktów lub usług. Oto kilka sytuacji, w których możesz rozważyć skorzystanie z chargebacku:

- Produkt lub usługa, za którą zapłaciłeś, nie została dostarczona lub została dostarczona wadliwa.
- Sprzedawca naliczył Ci więcej pieniędzy niż powinien lub naliczył Ci opłaty, o których nie zostałeś wcześniej poinformowany.
- Transakcja została wykonana bez Twojej zgody lub wiedzy.
- Sprzedawca niewłaściwie obsłużył Twoje zamówienie, na przykład nie dostarczył produktu w terminie lub dostarczył inny produkt niż ten, który został zamówiony.

Jeśli korzystasz z karty płatniczej wydanej przez bank lub instytucję finansową, zwykle będziesz miał możliwość skorzystania z tej usługi. Przed skorzystaniem z chargebacku przeczytaj dokładnie warunki korzystania z tej usługi aby upewnić się, że spełniasz wymagania i aby dowiedzieć się, jakie dokumenty lub informacje będą potrzebne do złożenia wniosku o chargeback.

DZIĘKUJĘ

ŻE JESTEŚ W MOJEJ SPOŁECZNOŚĆI

Wiem, że temat nie jest łatwy, ale wierzę,
że mój poradnik pomógł Ci zrozumieć niektóre
zasadnicze kwestie związane z bezpiecznym
bankowaniem w sieci.

Do zobaczenia w Internecie lub na zywo na
szkoleniach.

60 minut na miesiąc. Stwórz i zaplanuj posty na cały miesiąc w godzinę.

Automatyzacja postów na Facebooku dla kobiet biznesu.

KUP KURS

Naucz sie od podstaw korzystać z bezpłatnych narzędzi do A.I. i zaplanuj posty na FB na cały miesiąc w godzinę

Jak tworzyć grafiki do SM za pomocą AI – twórz cyfrowo bez pędzla i aparatu.

Podstawy grafiki dla nietechnicznych

KUP KURS

Odkryj tajemnice szybkiego i efektywnego tworzenia grafik, które zaskakują swoją oryginalnością i przyciągają uwagę odbiorców.

Dziękuję,

ŻE DOŁĄCZYŁAŚ DO MOJEJ SPOŁECZNOŚCI

Wspólnie stworzymy coś unikatowego, wykorzystując
najnowsze technologie
i innowacyjne rozwiązania.
Niech **A.I. Marka** będzie Twoim sprzymierzeńcem
w osiąganiu sukcesu
i w rozwoju Twojej Marki.
Razem możemy przekroczyć granice
i osiągnąć niezwykłe rzeczy używając
w naszej wspólnej pracy Sztucznej Inteligencji!

FACEBOOK: HTTPS://WWW.FACEBOOK.COM/AIMARKAWSIECI
GRUPA NA FB: HTTPS://WWW.FACEBOOK.COM/GROUPS/AIMARKA
MAIL: KONTAKT@AIMARKA.PL
TEL.: 519 129 900