FAMOC

Jak obronić

swojego smartfona?

#5 sposobów na bezpieczeństwo

FAMOC.COM

FAMOC®

Tylko 14%

Polaków zabezpiecza swoje smartfony
przed utratą danych*

FAMOC.COM

*badanie Proxi.cloud oraz Mobiem Polska, 2019

Ile Twój smartfon wie o Tobie?

Dużo. Można powiedzieć, że wie tyle, na ile mu pozwolisz. Ale tak naprawdę jest w stanie dowiedzieć się o wiele więcej… Dlatego ważne jest, by w jak największym stopniu móc tę wiedzę kontrolować i ograniczyć jej udostępnianie.

Droga od odblokowania telefonu do wycieku danych to nie wyprawa na księżyc. I choć ”wycieki danych” mogą się nam kojarzyć jedynie z danymi wrażliwymi dużych firm i poważnych organizacji, sprawa dotyczy każdego z nas.

Wybraliśmy pięć obszarów, w których warto zachować czujność. Jako że całkowita prywatność w sieci jest dziś praktycznie niemożliwa, postarajmy się o nią zadbać możliwie najlepiej, stosując się do kilku dobrych praktyk.

Zatem do dzieła. Dowiedz się, jak obronić swojego smartfona!

FAMOC


#1
DOSTĘP

#1 DOSTĘP

PINY I HASŁA

Najbezpieczniejszą blokadą telefonu jest odpowiednio **długi kod PIN (min. 6 znaków!)** albo **odpowiednio długie i skomplikowane hasło.** Możemy zdradzić, że w naszej firmowej polityce bezpieczeństwa odnoszącej się do urządzeń służbowych mamy wyłączoną opcję blokowania telefonu poprzez znany wszystkim *pattern lock* (wzorek "malowany" palcem po ekranie). Dlaczego? A choćby dlatego, że pod odpowiednim kątem promieni słonecznych możemy go zobaczyć "namalowanego" na naszym urządzeniu. Poza tym, tylko w teorii kombinacji takich wzorków jest k i l k a s e t tysięcy. W rzeczywistości jednak w użyciu jest ich zdecydowanie mniej. Jeśli miałeś kiedyś ustawiony taki rodzaj blokady, to czy Twój wzorek rozpoczynał się w lewym górnym rogu….? Tak właśnie robi co drugi użytkownik korzystający z tego sposobu blokady.

BIOMETRIA

Słyszeliśmy już o uciętym palcu, którym rzekomy złodziej miał odblokować skradzionego smartfona, albo o zdjęciu blokady wskutek zeskanowania zdjęcia twarzy właściciela (zamiast prawdziwej twarzy). Ciągle jednak trend *passwordless* rośnie, a **umiejętne korzystanie z biometrii to metoda skuteczna i nie tak prosta do złamania - korzystajmy z niej, jeśli tylko możemy!**
Tu newralgicznym punktem jest niestety odpowiednie przechowywanie gromadzonych danych biometrycznych i właściwe ich zabezpieczenie (tak, zabezpieczenie danych służących do zabezpieczenia). W końcu biometria to nie tylko odblokowanie służbowego telefonu za pomocą odcisku palca, ale także chociażby skanowanie naszej twarzy przy kontroli lotniskowej. Każdy podmiot gromadzący dane tak wrażliwe na ogromną skalę, powinien je możliwie najlepiej zabezpieczyć. W sytuacji wycieku danych, standardowe hasło zmienimy w kilka sekund, z odciskiem palca nie będzie już tak łatwo...

FAMOC

#1 DOSTĘP

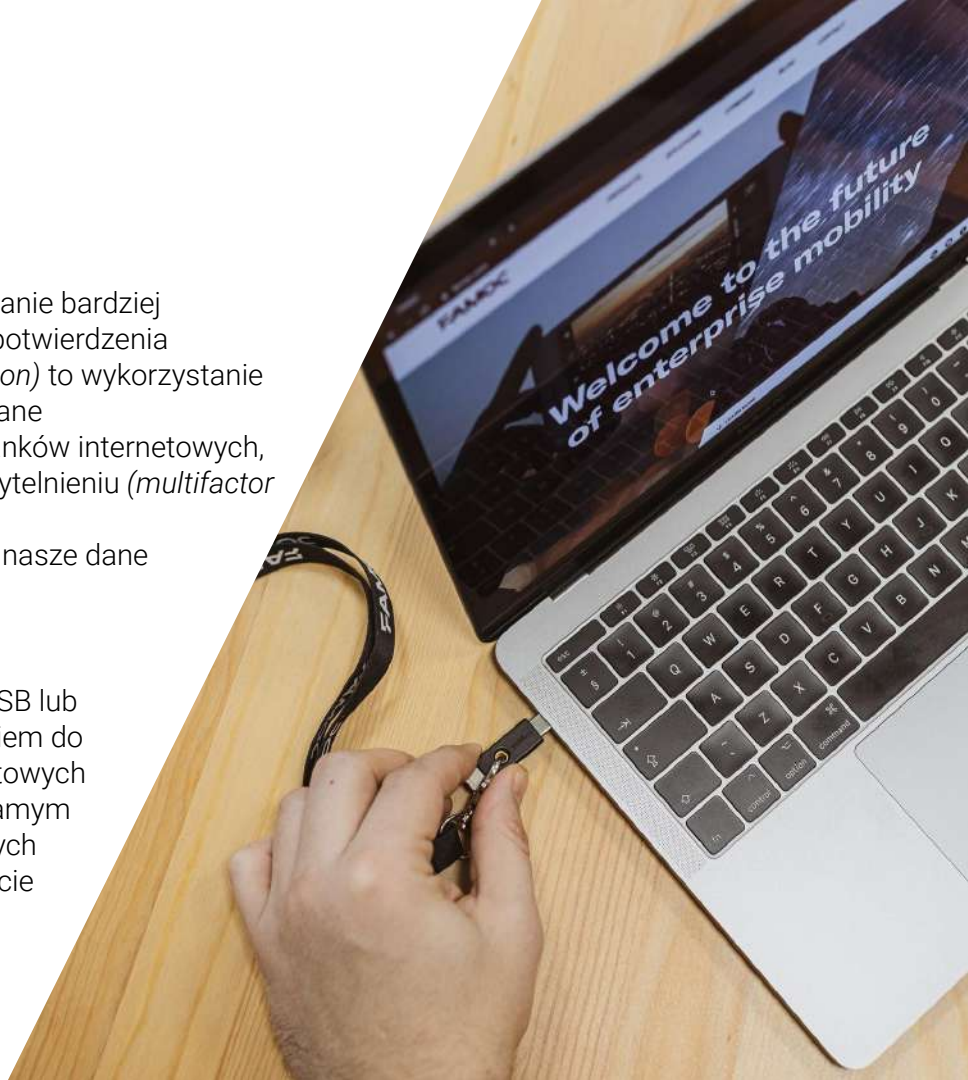
UWIERZYTELNIANIE

Każde hasło odpowiednio długie i skomplikowane będzie zdecydowanie bardziej bezpieczne, kiedy dodamy do niego element uwierzytelnienia, czyli potwierdzenia tożsamości. Dwuskładnikowe uwierzytelnienie *(2-factor authentication)* to wykorzystanie tego, co masz (np. telefon) oraz tego, co wiesz (np. hasło SMS wysłane w celu potwierdzenia tożsamości). Tę metodę stosuje większość banków internetowych, Gmail, Facebook itd. Mówi się również o wieloskładnikowym uwierzytelnieniu *(multifactor authentication)*, gdzie do elementów, które "masz i wiesz", dochodzi to, kim jesteś - takim uwierzytelnieniem są nasze dane biometryczne. Nasza rada: **używaj 2FA, gdzie tylko możesz!**

KLUCZE / TOKENY SPRZĘTOWE

YubiKey to klucz bezpieczeństwa U2F. Podłącza się go do portów USB lub łączy przez NFC z urządzeniami mobilnymi. Jest świetnym narzędziem do wielopoziomowego uwierzytelniania na portalach, skrzynkach pocztowych oraz do danych firmowych. To rozwiązanie jest uniwersalne - tym samym kluczem YubiKey możemy zabezpieczyć dostęp do firmowych danych oraz zabezpieczyć swoje prywatne konto na Gmail! Istnieją oczywiście inne tego typu klucze, np. Titan Security Key od Google.

FAMOC




#2
GEOLOKALIZACJA

#2 GEOLOKALIZACJA

UDOSTĘPNIANIE LOKALIZACJI

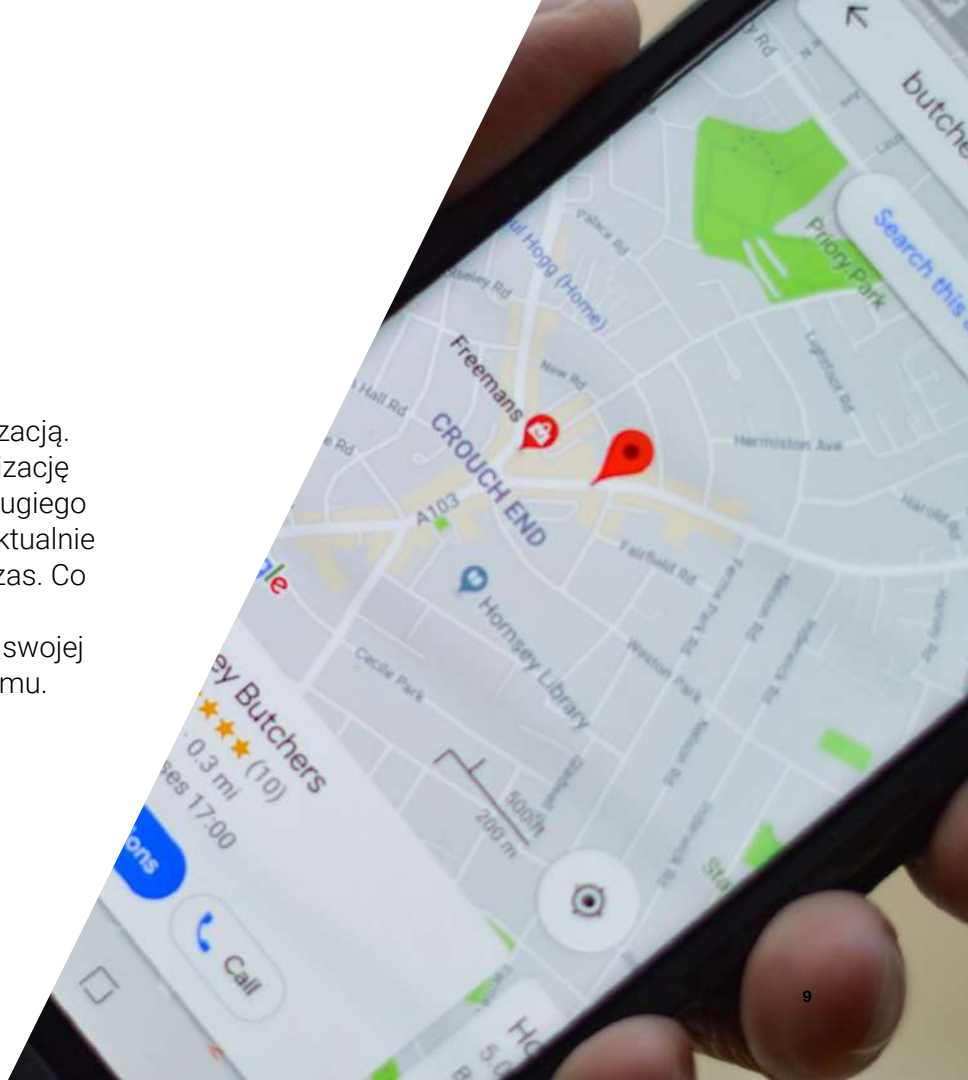
Ta funkcjonalność ma z pewnością mnóstwo zalet, przede wszystkim usprawnia działanie wielu aplikacji: Google Maps, Endomondo, iTaxi, UberEats i wiele innych. Mówi się, że część usług Google zbiera informacje o naszej lokalizacji nawet, jeśli teoretycznie wyłączymy tę opcję na swoim urządzeniu. To oczywiście pozwala gromadzić dane dotyczące naszego poruszania się i aktualnego położenia. Dane te w idealny sposób wykorzystują chociażby reklamodawcy, kierując swoje reklamy np. na konkretną lokalizację. Może to również wpływać na nasze wyniki wyszukiwania.

HISTORIA LOKALIZACJI GOOGLE

Historia lokalizacji to ustawienie na poziomie konta Google, które zapisuje informacje o miejscach odwiedzanych przez nas razem z urządzeniem mobilnym, na którym jesteśmy zalogowani na konto Google oraz mamy włączoną opcję Historia lokalizacji. Dzięki temu mogą nam się wyświetlać m.in. spersonalizowane mapy, rekomendacje na podstawie odwiedzonych miejsc, możemy też odnaleźć swój telefon w przypadku zagubienia, otrzymywać bieżące informacje o ruchu na trasie do pracy oraz reklamy dostosowane do naszych potrzeb. Oczywiście istnieje ryzyko, że dane te wyciekną i trafią w niepowołane ręce, w sytuacji kiedy ktoś włamie się na nasze konto Google czy Apple. Dlatego tak ważne jest, aby odpowiednio te dane zabezpieczać i wszelkie ryzyko ograniczyć do minimum.

#2 GEOLOKALIZACJA

PINEZKI, CHECK-INY...
Wielu z nas bardzo często publicznie dzieli się swoją aktualną lokalizacją. Musimy pamiętać, że publikując w czasie rzeczywistym swoją lokalizację w social media (czy to trasę na Endomondo czy selfie z wakacji z drugiego końca świata), publicznie informujemy świat o tym, że nie ma nas aktualnie w domu i prawdopodobnie nie będzie nas tam jeszcze przez jakiś czas. Co robić, żeby tego uniknąć? Ogranicz widoczność swoich postów do węższego grona znajomych. Możesz też wstrzymać się z relacją ze swojej podróży lub treningu do momentu, kiedy z powrotem będziesz w domu.




#3
KOMUNIKACJA

#3 KOMUNIKACJA

SZYFROWANIE I POUFNOŚĆ

O co chodzi z “bezpiecznymi” komunikatorami? Dlaczego nie wszystkie w odpowiedni sposób chronią naszą prywatność? Najprościej mówiąc, chodzi o s z y f r o w a n i e. **Szyfrowanie *end-to-end (E2E)*** oznacza, że nikt poza komunikującymi się nie będzie miał możliwości przechwycenia wiadomości. Wiadomość, którą wysyłasz, jest szyfrowana na Twoim urządzeniu i rozszyfrowywana dopiero na urządzeniu Twojego rozmówcy.

Sprawdź, czy Twój komunikator szyfruje E2E **domyślnie!** (bez pamiętania o włączeniu lub przejściu w tryb prywatny). Ponadto zastanów się, na ile udasz producentowi i jakie są jego praktyki dotyczące prywatności.

FAMOC

#3 KOMUNIKACJA

BEZPIECZNY KOMUNIKATOR - CZYLI JAKI?

Na co jeszcze, poza odpowiednim szyfrowaniem, powinniśmy zwrócić uwagę przy wyborze i korzystaniu z komunikatora?

AUTODESTRUKCJA WIADOMOŚCI

Dobrze, jeśli użytkownik może zezwolić na znikanie wiadomości, ustawiając przedział czasu dla automatycznego usuwania. Gwarantuje to prywatność, nawet jeśli ktoś inny ma dostęp do Twojego telefonu.

UPRAWNIENIA APLIKACJI

Sprawdź, czy Twój komunikator ma dostęp np. do głośnika lub aparatu. To odpowiedź na częste pytanie: czy mój telefon mnie podsłuchuje?

ZAHASŁOWANE CZATY

Niektóre komunikatory mają dodatkową opcję zabezpieczenia czatów hasłem. To cenna funkcjonalność w przypadku rozmów poufnych czy przy wymianie wrażliwych danych.

OPROGRAMOWANIE OPEN SOURCE

Pozwala to użytkownikom na pewną ”integrację” z aplikacją, wpływa na jej elastyczność oraz zwiększa bezpieczeństwo.

FAMOC


#4
APLIKACJE

#4 APLIKACJE

UPRAWNIENIA

Czy Latarce potrzebny będzie dostęp do Twoich kontaktów? A Kalkulator będzie lepiej liczył, jeśli otrzyma dostęp do Twoich wiadomości? Nie sądzę. Zwracaj uwagę na uprawnienia, o jakie proszą poszczególne aplikacje podczas instalacji lub pierwszego użycia. Szkodliwe aplikacje to jedno z głównych źródeł wycieku danych.

W 2018 r. do sklepu Google Play trafiło aż 109 tys. szkodliwych aplikacji. Na szczęście Google w minionym roku wdrożył skuteczne mechanizmy wykrywania złośliwych programów i **zredukował ich liczbę o 76%.**

ŹRÓDŁO APLIKACJI

Zawsze korzystaj z pewnych źródeł. Staraj się pobierać aplikacje z oficjalnych sklepów. Aplikacje ściągane z niezaufanego forum, załącznika maila lub innego niepewnego źródła będą bardziej narażone na obecność szkodliwego kodu. Czytaj opinie, choć niekoniecznie sugeruj się o c e n ą - bardzo często *rating* aplikacji zostaje podbijany sztucznie. Być może jest Ci znany obrazek osoby, której zadaniem jest wyklikanie wysokich ocen aplikacji na ścianie smartfonów, którą ma przed sobą…

Stosując się do zaleceń, prawdopodobieństwo pobrania PHA (Potentially Harmful Application) ze sklepu Google Play jest **mniejsze, niż uderzenie asteroidy w ziemię!***

FAMOC

*Android Security 2017 Year in Review

#4 APLIKACJE

Sporym problemem w Chinach są tzw. “farmy lajków” *(click farm)*, które zarabiają m.in. na fałszywym podbijaniu ocen aplikacji. W takim miejscu może być nawet **10 000 urządzeń** służących do tego celu.

*fot: .Reddit.com

FAMOC

#4 APLIKACJE

AKTUALIZUJ
Bardzo często aktualizacje zawierają poprawki lub uzupełnienia zabezpieczeń, które ochronią Twoje urządzenia przed nowo odkrytymi zagrożeniami. Dlatego to bardzo ważne, aby mieć zawsze zainstalowaną najnowszą wersję oprogramowania.

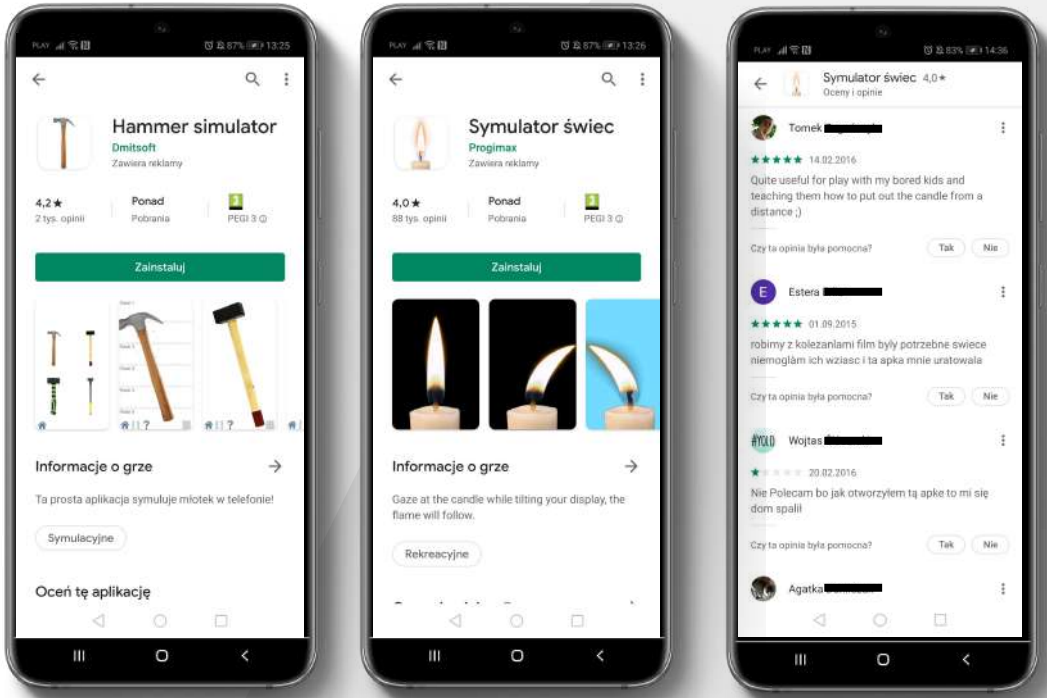
Średnio dziennie używamy **do 10 różnych** aplikacji na smartfonie. Kiedy ostatnio korzystałeś **z pozostałych 90** zainstalowanych na Twoim telefonie?

FAMOC

#4 APLIKACJE

HIGIENA SMARTFONA

Jest wiele aplikacji, które nie pełnią żadnej konkretnej funkcji: aplikacja Nic, Młotek czy Świeca raczej nie usprawnią naszej codziennej pracy, nie zapewnią nam także szczególnej rozrywki. Takie aplikacje są praktycznie bezużyteczne, a jednak… bardzo często mają wysokie noty w rankingach i całą masę opinii. Nie musi oznaczać, że takie oprogramowanie na pewno zaszkodzi naszemu urządzeniu, ale skoro nie ma z niego żadnego pożytku może warto zatrzymać się na zabawnych recenzjach?



FAMOC


#5
MOBILNA
BANKOWOŚĆ

#5 MOBILNA BANKOWOŚĆ

POPULARNOŚĆ ROŚNIE

Według danych PRNews.pl, **aż 11 mln Polaków korzysta z mobilnej bankowości**, z czego 60% ogranicza się tylko i wyłącznie do korzystania z aplikacji (co oznacza, że w żadnej inny sposób nie logują się do swojego banku). Każdego roku liczby tych użytkowników idą w górę. Ta rosnąca popularność mobilnej bankowości wymusza dodatkowe zabezpieczenia, takie jak dwustopniowe poziomy zabezpieczeń czy wykorzystanie biometrii w procesie logowania do banku oraz potwierdzenia transakcji.

Z reguły mobilne aplikacje bankowe są dobrze chronione, jednak należy zachować czujność i przestrzegać kilku zasad, m.in. pobierać aplikację z pewnego źródła, ustalić limity na transakcje mobilne oraz, co bardzo ważne, nigdy nie klikać w podejrzane linki przekierowujące do płatności, które przyszły do nas w postaci wiadomości SMS.

Okazuje się, że **jedynie 19% Polaków**,
w kontekście bezpieczeństwa mobilnego,
boi się kradzieży ze swojego konta bankowego.*

FAMOC

**dużo bardziej boimy się wycieku naszych zdjęć, filmów czy treści wiadomości; badanie Proxi.cloud oraz Mobiem Polska, 2019*

#5 MOBILNA BANKOWOŚĆ

AUTORYZACJA W APLIKACJI MOBILNEJ > AUTORYZACJA SMS

Autoryzacja transakcji w aplikacji mobilnej jest **dużo bezpieczniejsza** niż tradycyjne potwierdzenia SMS. Wówczas możemy mieć pewność, że żaden *malware* na naszym urządzeniu nie przechwyci kodu autoryzacji. Poza tym w ramach powiadomień aplikacji jesteśmy informowani o każdym kroku transakcji. Możemy też poznać więcej szczegółów, aby upewnić się, że rzeczywiście potwierdzamy n a s z przelew.

BLIK

Płatności BLIKIEM uznawane są nie tylko za **wygodne i sprawne, ale również dość bezpieczne**. Sześciocyfrowy kod BLIK jest trudny do przechwycenia (choć oczywiście nie niemożliwy), a w dodatku ma ograniczoną ważność (120 sekund). Dodatkowo, aby go wygenerować trzeba zalogować się do banku, a na koniec wykonać akceptację transakcji w aplikacji mobilnej - to wszystko, aby metoda ta była możliwie najbardziej bezpieczna. Możemy również dzięki temu wypłacać gotówkę z bankomatu bez użycia karty, co jest bardzo przydatne i nie niesie ze sobą ryzyka zgubienia karty płatniczej ;)

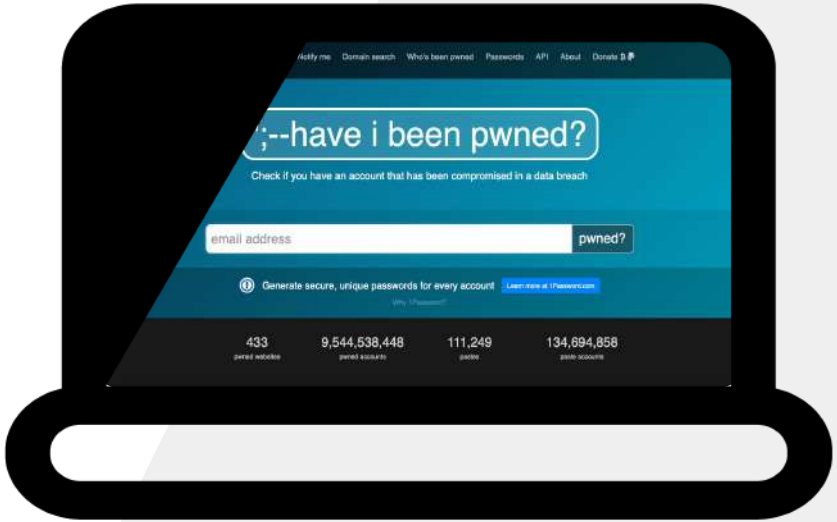
FAMOC


Co jeszcze
mogę zrobić?

Sprawdź, czy Twoje dane nie wyciekły

HaveIBeenPwned

W tym serwisie sprawdzisz, czy używany przez Ciebie adres e-mail nie znajduje się w serwisie, który padł ofiarą hakerów.



FAMOC

Obejrzyj vloga!

#ObsessedWithSecurity

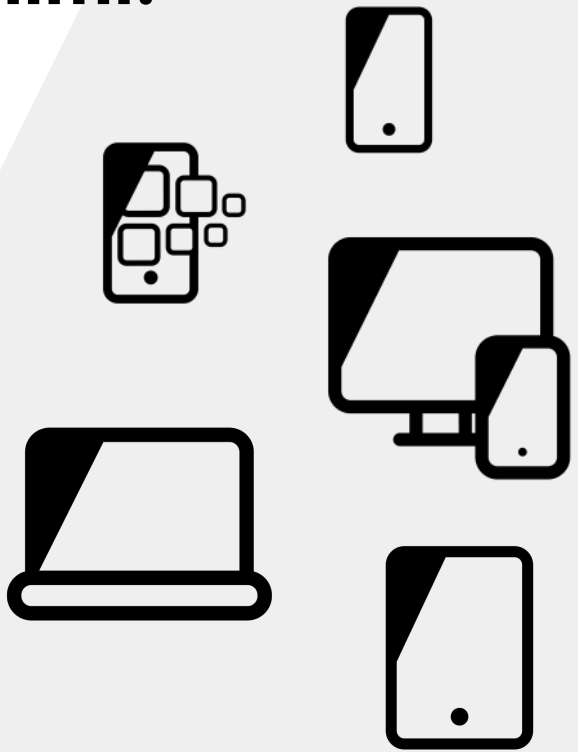
stworzonego we współpracy z redakcją itbiznes.pl

FAMOC

Jesteś w firmie, w której jest więcej urządzeń mobilnych? Zarządzaj nimi!

Mobile Device Management

Narzędzia MDM (Mobile Device Management), służące do zarządzania urządzeniami w firmach i organizacjach, pomagają chronić sprzęty mobilne wykorzystywane do pracy i na bieżąco je monitorować. Dzięki takim narzędziom możemy odpowiednio zabezpieczyć dostęp do danych firmowych oraz wymusić restrykcje bezpieczeństwa na urządzeniu (długość kodu PIN, biała / czarna lista aplikacji, ograniczenia w korzystaniu z publicznych sieci Wi-Fi i wiele innych).



FAMOC

Zapisz się na darmowy trial FAMOC!

Wypróbuj FAMOC manage przez 30 dni.

- bezpieczeństwo danych
- monitoring urządzeń
- zdalny dostęp
- lokalizowanie urządzeń
- integracje
- zaawansowane konfiguracje
- bezpieczna komunikacja
- separacja danych
- zgodność z regulacjami
- wymuszanie aktualizacji

info@famoc.com

FAMOC.COM