14.02.2025 r.

#374

TRANSKRYPT ODCINKA

Co się zdarzyło w iPhonie, zostaje w iPhonie

Partnerem tego podcastu jest iDream.pl.

[MUZYKA]

Tu Krzysztof Kołacz, a ty słuchasz właśnie podcastu, „Bo czemu nie?”. Usłyszysz w nim o technologiach, które nas otaczają i nas w tych technologiach zanurzonych. Sprawdzam, pytam i podpowiadam jak korzystać z nich tak, aby to one służyły nam, a nie my im.

W dzisiejszym odcinku o funkcjach prywatności w ekosystemie Apple, o których będziesz mógł lub będziesz mogła jasno i klarownie odpowiedzieć komuś, kto znowu zapyta: Dlaczego ten iPhone jest taki bezpieczny? No to posłuchaj.

Proszę, zostaw opinię na Apple Podcasts lub na Spotify. Twój głos ma znaczenie!

Zaczynamy.

[MUZYKA CICHNIE]

[KRZYSZTOF] Czołem moi drodzy, witam w 374. odcinku „Bo czemu nie?”. Z tej strony się standardowo kłania Krzych Kołacz. Dzisiaj odcinek, który tak naprawdę przyda się nie tylko tym z Was, którzy od dawna już siedzą w ekosystemie urządzeń i systemów Apple, ale także przyda się tym wokół Was, którzy o ten ekosystem pewnie nieraz pytali: *Dlaczego ten iPhone jest taki dobry?* Albo *dlaczego ten iPhone mówisz, że jest bezpieczniejszy niż mój Android?* Albo *czemu tak naprawdę warto w ogóle rozważyć iPhone’a?* To jest taki odcinek, który mam nadzieję, że będzie taką treścią aktualną prawie zawsze.

Tak przynajmniej chcę go grać razem z moim gościem w dniu dzisiejszym, ale zanim to, to pozwólcie, że przypomnę, iż wszelkiego rodzaju rzeczy, namiary na te rzeczy, czy właśnie namiary na dzisiejszego gościa, którego zaraz Wam przedstawię,

znajdziecie w opisie tego odcinka lub pod adresem boczemunia.pl/374/. Tam także znajdziecie namiary na mój autorski newsletter około-technologiczny, który wysyłam w sobotę o poranku. Sprawdź, może to coś dla Ciebie.

W związku z przypadającym niedawno, bo 28 stycznia, Dniem Ochrony Danych Osobowych, taką globalną inicjatywą mającą na celu przede wszystkim podkreślenie znaczenia tejże ochrony w sieci, czy właśnie na naszych urządzeniach, postanowiłem poświęcić ten odcinek zebraniu takich podstawowych informacji na temat tego, jak Apple chroni naszą prywatność. Nie jest to lista dla zaawansowanych użytkowników, to na pewno, powiedzmy sobie to na dzień dobry, ale raczej taka ściągawka dla każdego i każdej z Was, na wypadek gdyby znowu ktoś z rodziny zadał Wam te pytania, o których mówiłem przed chwilą. Choć dziś nagrywam z gościem, to mam nadzieję, że także jego perspektywa i moja, bo choć mówimy o tym samym, to każdy ma inaczej, wniesie tutaj coś dodatkowego.

No i cóż, nie pozostaje mi nic innego, jak przywitać po raz kolejny w tym podcaście Mateusza Baryłę z iDream.pl. Cześć Mateusz!

[MATEUSZ] Cześć, witam ponownie wszystkich i Ciebie.

[KRZYSZTOF] Fajnie, że wpadłeś znowu i na początek chciałbym podpytać, co tam w ogóle w nowym roku ciekawego w iDream, przede wszystkim u Ciebie w salonie w Krakowie. Coś takiego, co się wybija z tła, jakieś nowe promocje, być może jakaś fajna anegdotka zza kulis. Coś tam tutaj powiesz?

[MATEUSZ] Powiem Ci, że nadzieja na nowości w najbliższym czasie w nas drzemie aktualnie.

[KRZYSZTOF] To tak trochę zawiązuję do poprzedniego odcinka 373., gdzie omawiałem wyniki finansowe Apple i właśnie tak się zastanawiałem, no ponieważ te ostatnie obejmowały okres bożonarodzeniowy. Tak się właśnie zastanawiałem w weekend, czy to jest taka prawidłowość, że teraz już po Nowym Roku jest tak właśnie totalna posucha, czy jednak ktoś się jeszcze tam zbłąkany po coś pojawia.

[MATEUSZ] Może nie totalna, ale ludzie dają nam odpocząć po grudniowym wycisku.

[KRZYSZTOF] Tak jest, no plotki są następujące moi drodzy, a mianowicie być może kiedy to nagrywamy, a jest poniedziałek, to nie wiemy jeszcze do końca, ale jest szansa, że w tym samym tygodniu pojawi się coś nowego, więc jeżeli tak Ci się wydarzyło i Wy zastanawiacie się, dlaczego w tym odcinku nie ma na przykład nic nowym iPhonie SE, czy jakkolwiek go Apple sobie nazwie, to właśnie dlatego, że nagrywamy w poniedziałek i spokojnie w kolejnym będzie na pewno coś o tym urządzeniu, jak to u mnie na spokojnie. To może warto było na początku powiedzieć, więc mówię to teraz.

Dobrze, to zaczniemy ten odcinek od takiej perspektywy właśnie na typową osobę chciałoby się powiedzieć i taką zwykłą codzienność typowego użytkownika Apple, czyli chyba takiego, który też przychodzi do Waszych salonów w większości przypadków. No i tu mam do Ciebie pytanie: Kiedy słyszysz prywatność, bezpieczeństwo albo zderzasz ten temat z klientami, to o co ludzie pytają, albo czego ludzie nie wiedzą najczęściej?

[MATEUSZ] Typowy klient przychodzi zdecydowanie za późno.

[KRZYSZTOF] OK.

[MATEUSZ] Ponieważ przychodzi po incydencie, czyli po braniu środków z konta, czy włamie na konto Apple, jakby już po fakcie. To spotykam się najczęściej chyba w pracy, czyli *„ojejku, stało się to i to”*. Jak to odkręcić i jak temu zapobiec na przyszłość.

[KRZYSZTOF] A to jest bardzo ciekawe, czyli jakby zdarza się nawet w takim, wiesz, żeby Krakowie, nie? To nie jest jakby, wiesz, jakaś ogromna metropolia, no nie?
A zdarzają się, jak mówisz, klienci, którzy przychodzą i już zostali oszukani?
To niesamowite, ja nie spodziewałem się tej odpowiedzi, szczerze powiedziawszy.

[MATEUSZ] Tak, tak, tak. I to znakomita większość właśnie osób, która przychodzi w temacie, który dzisiaj omawiamy, przychodzi właśnie po fakcie. I tutaj wtedy wkraczamy my po pierwsze, żeby ułożyć swojego doświadczenia, żeby to odkręcić w jakikolwiek sposób, bo niektóre rzeczy da się odkręcić, albo żeby właśnie zabezpieczyć to konto na później.

Przychodzą ludzie, którzy myślą, że mają na przykład podsłuch w telefonie i inne tego typu rzeczy, ale no dzięki temu właśnie przydają się te rozwiązania Apple'a jak

informowanie użytkownika o tym, że na przykład mikrofon czy kamera jest używana. Mamy teraz tą magiczną pomarańczową kropkę, która to sygnalizuje, pomarańczową i zieloną chyba.

[KRZYSZTOF] Tak, to sobie to powiemy jeszcze dzisiaj, o tym jasne. A tak się jeszcze dopytam, no dobra, a najczęściej jakby przyczyną tego, że ktoś miał takie nieprzyjemne zdarzenie, no nie wiem, tak jak powiedziałeś, komuś coś się stało w Apple ID, kogoś być może okradziono – czy ten ludzki czynnik (coś nie było włączone, co mogłoby przed tym ją czy jego uchronić) odgrywa istotną rolę?

[MATEUSZ] Wiesz co, często to jest dlatego, bo na przykład klienci nie mają włączonej dwustopowej weryfikacji, co jest mega dziwne i po prostu wyciek danych z jakiegoś serwer. Chodzi o hasło i na przykład skradzenie konta Apple ID, coś takiego. Mam też fajną anegdotkę co prawda nie z rynku krakowskiego, ale od mojego kumpla z Łodzi, przyszedł, zgłosił się do niego w ogóle klient, że ktoś zaproponował mu na Whatsappie z tego co pamiętam, że prosi go bardzo o pomoc, żeby zalogował się na chwilę na swoim iPhonie jego Apple ID i za to dostanie 100 euro. No i ten klient przyszedł do właśnie iDream w porę, co prawda, właśnie opowiedział o tym z Łodzi, mówią *nie, nie, proszę się na to nie zgadzać, proszę się nie wylogowywać*.

Wyszedł, wraca za 10 minut, mówi: *Słuchajcie chłopaki, bo mnie skusiło to 100 euro, wylogowałem się, zalogowałem się swoim Apple ID no i teraz gość mi mówi, że poda mi hasło jak mu wyślę 200 euro, a tej stówy mi nie wysłał*. No to chłopaki, no, a nie mówiliśmy, żeby tego nie robić?

No nie da się z tym nic zrobić.

Oczywiście pan tam został poinstruowany, żeby może zapytał u producenta, u Apple na Infolinii Wsparcia i tak dalej. Wyszedł, wraca za 10 minut, już z informacją, że pan prosi, żeby wysłać ten telefon i jak on im wyśle ten telefon, to on się wyloguje i wtedy odeśle wylogowany. Także to był typ, to było typowe pod po prostu okup i z takimi rzeczami też w iDream się spotykamy. Najczęściej nie chodzi o telefony, a o komputery firmowe.

[KRZYSZTOF] Niesamowite.

[MATEUSZ] Przychodzą ludzie, że nie wiem jakim cudem w ogóle to się dzieje, że ktoś się loguje na kogoś konto, kogoś Apple iD. Możliwe, że też na zasadzie takiej marchewki pomachanej przed nosem typu 100 euro, ale miałem ostatnio klienta właśnie, któremu ktoś się zalogował na komputer i chciał chyba 400 euro okupu za wylogowanie się.

[KRZYSZTOF] To jest w ogóle jakaś, jakaś totalna abstrakcja, że my mówimy w 2025 roku o tym, że ktoś na tak jakby, no to jest, wiesz.

[MATEUSZ] Dokładnie.

[KRZYSZTOF] Najprostsze możliwe jest zrobienie kogoś w balona, jakie chyba istnieje na ten okup, a ludzie się na to nabierają, nie?

W sensie to też pokazuje, że my żyjemy w bańce, nie? W sensie my już tacy rdzenni użytkownicy, że tak powiem, Apple, którzy od lat...

[MATEUSZ] Wiemy na co zwracać uwagę i gdzie się jakiś Red Flag zapala, prawda?

[KRZYSZTOF] Tak, tak, tak. A to nie jest takie oczywiste i my sobie zawsze tak w tych dyskusjach gdzieś tam ze znajomymi, nie wiem czy też tak masz, ale chyba tak, wiesz, mówimy, że nasi rodzice to by się pewnie dali złapać albo nasi dziadkowie. Kurczę, a to są też ludzie często w naszym wieku, nie?

[MATEUSZ] W naszym wieku i ludzie wydawałoby się bardzo ogarnięci życiowo, prowadzący działalności i obracający się w tym sprzęcie nie jednym, a całym ekosystemie, prawda?

[KRZYSZTOF] Tak, ja tutaj polecę od siebie na pewno jakbyście chcieli się w ogóle więcej dowiedzieć na temat tego jak dziś działają cyberprzestępcy, to polecę Wam jeden z ostatnich odcinków podcastu Techstorie, gdzie Sylwia Czubkowska bardzo fajnie opowiada o tym na przykładzie konkretnej ich słuchaczki, która co prawda została oczywiście potraktowana jako osoba anonimowa, ale jednakowoż wypowiada się tam swoim głosem o tym jak została okradziona przez Facebooka, to też bardzo często ostatnio. Podlinkuję Wam oczywiście w opisie i drugie to polecę Wam cały serial audio-podcastowy „Jazgot”, który wspólnie Voice House Polski z mBankiem realizują i tam już na przykładzie fabuły i to całkiem sensownej fabuły, którą napisali ludzie czołowi ludzie w tym kraju od pisania w ogóle True

Crime. Niestety no pisali to na bazie historii, która faktycznie miała miejsce w Polsce, no i to jest coś niesamowitego jak łatwo się jest złapać nawet mając tak jak powiedział Mateusz, doktorat skończony, pracując nawet w IT, a i tak wysłać komuś pieniążki.

[MATEUSZ] Ja jeszcze od siebie bym polecił nowy artykuł Apple na ich stronie wsparcia odnośnie oszustw na karty podarunkowe. One się kiedyś nazywały iTunes Gift, nie?

[KRZYSZTOF] Tak, tak.

[MATEUSZ] A teraz po prostu. Tak, a teraz po prostu karty podarunkowe i uwaga też mam klientów, którzy dają się robić na te karty i dopiero teraz po chyba dwóch latach takiego procederu Apple zdecydowało się zrobić cały artykuł jak się nie dać właśnie na to nabrać.

[KRZYSZTOF] To podlinkujemy oczywiście.

Dobra, no to zaczęliśmy trochę mało optymistycznie, no to przejdźmy do tego, co można zrobić, żeby zanim się przyjdzie jakby do iDream i się zapyta, jak teraz odzyskać hasło, kiedy się komuś wysłało telefon na przykład na Wyspy Owcze.

Apple od lat generalnie, moi drodzy, co jest jakby rzeczą dosyć znaną w szerokich mediach jest traktowana jako firma, która słynie z tej swojej prywatności. Dużo o niej mówi i tak naprawdę no częściej słyszymy, że Apple na przykład nie zrobiło tak zwanego backdora, tak, czyli takiego tylnego wejścia do systemu dla jakichś służb typu, wiecie, FBI, czy tam CSI, etc., niż, że komuś nie wiem, wykradziono w prosty sposób hasło do iPhone'a. No chyba, że są to tego typu scenki, o których mówił Mateusz. Im chcemy przeciwdziałać, między innymi mówiąc Wam dzisiaj o tych dziesięciu podstawowych powiedzmy funkcjach ekosystemu Apple chroniących Waszą prywatność.

No i tak płynnie przechodzimy sobie do kwestii absolutnie podstawowej, która już tutaj dzisiaj padła, a mianowicie do punktu pierwszego, czyli biometria.

Moi drodzy, Face ID, Touch ID, być może Optic ID, jak ktoś sobie korzysta z Vision Pro. W każdym razie, te metody autentykacji z wykorzystaniem Waszego ciała, tak, czyli twarzy, odcisku palcu lub skanu oka to jest coś, co jest absolutnie do

włączenia na dzień dobry i mało tego iPhone i każde inne urządzenie prosi Was o to, żebyście to skonfigurowali i naprawdę nie warto wtedy w tym chociażby jednym kroku klikać przycisku skonfiguruję później, bo myślę, że Mateusz się zgodzi z doświadczenia można o tym zapomnieć i potem jest problem.

[MATEUSZ] Można i nie można, ponieważ nawet jak damy sobie skonfiguruj później to ustawienia będą nam o tym przypominać przez jakiś czas jeszcze cały czas wyświetlając jedynkę na ikonie plus zaraz pod naszą nazwą użytkownika będzie widniał napis, żeby skonfigurować Face ID czy Touch ID więc teoretycznie nie da się o tym zapomnieć, ale zdarzają się ludzie, którzy z tego w ogóle nie korzystają.

[KRZYSZTOF] No tak i tutaj jeżeli chodzi o to, to na tym się historia nie kończy, no bo fakt, że dostęp do telefonu jest chroniony poprzez biometrię jedną z tych trzech, czyli Face ID, Touch ID i Optic ID to jeszcze warto wspomnieć, że te dane są anonimowe także dla Apple w sensie one siedzą w tak zwanym Secure Enclave, czyli Bezpiecznej Enklawie, i to jest jakby nie kolejny punkt, ale jakby gwiazdka przy tym pierwszym. To taki fragment odseparowany zupełnie od tej głównej części krzemu, czyli procesora Apple jest no w nim co prawda, ale jednakowoż oddzielnie, to tak najprościej mówiąc zaszyty i dzięki temu nie da się na przykład na urządzeniu Apple przeprowadzić ataku, który do tych danych biometrycznych dostanie się od razu tak bezpośrednio; wchodząc na przykład na procesor czy w ogóle na maszynę.

To już robią też inne firmy jeżeli chodzi o kopiowanie Apple to też jest akurat pozytywny aspekt tego kopiowania i jakby w ogóle rynku konkurencji dobrze, że to się dzieje m.in. HP takie rozwiązania już u siebie też robi to możesz się posłuchać w odcinku 372. Co do zasady ta Bezpieczna Enklawa jest dobrym rozwiązaniem i tam te najważniejsze dane do których nawet Apple tak jak mówię, bo one są szyfrowane nie ma kluczy deszyfrujących są trzymane i są całkowicie nawet dla samej firmy anonimowe. Dlatego tak ważne jest żeby to o co po prostu w pierwszej linii Was, Wasze urządzenia poproszą w kontekście bezpieczeństwa włączać bo jak już proszą to mają ku temu powód prawda Mateusz?

[MATEUSZ] Dokładnie to nie jest po to żeby było Można przywołać słynne hasło Apple z Las Vegas: Co się stało w iPhonie zostaje w iPhonie.

[KRZYSZTOF] I tutaj przy okazji Face ID i w ogóle każdej innej biometrii jeszcze warto wspomnieć o tym, że też sam system jeżeli aplikacja jest napisana zgodnie ze wzorcami Apple gdy zainstalujemy nową aplikację firmy trzeciej na przykład

aplikację do banku system powinien przy pierwszym uruchomieniu tej aplikacji wyświetlić nam monit wspominający i pytający nas właściwie czy my chcemy używać Face ID do jej odblokowywania lub dowolnej innej metody. Też ludzie często pomijają no, bo to jest komunikat systemowy, a nie komunikat tej aplikacji nie?

[MATEUSZ] To też jest błąd i myślę, że zgodzisz się ze mną że... że jest to po prostu bezpieczne, a to jest jeszcze wygodne?

[KRZYSZTOF] Tak jest, jak najbardziej i tak mi się wydaje, że dziwne jest to że właśnie z uwagi na tą wygodę ludzie to pomijają, nie? Bo jak tak rozmawiam czy to z rodziną czy ze znajomymi którzy są spoza banki technologicznej to nie uwierzysz jak wiele osób nie ma na przykład włączonego Face ID w kontekście aplikacji bankowej co dla mnie no jest już trochę abstrakcją, nie?

[MATEUSZ] OK, to odwdzięczę się też nie uwierzysz ile osób twierdzi, że Touch ID jest lepsze od Face ID A to ciekawe, dlaczego? Ludzie ludzie nienawidzą Face ID nie... oczywiście generalizuje, nie jest tak, że wszyscy ale znakomita większość osób woli Touch ID. Nie wiem dlaczego znaczy tłumaczą oczywiście, że niby jest wygodniejsze, że jest szybsze, co w ogóle nie zgadzam się z żadnym z nich.

Boją na przykład, że a jak założą okulary albo jak się pomalują, albo zmienią fryzurę, no to nie zadziała. Ja uspokajam, że Face ID działa z okularami korekcyjnymi i przeciwsłonecznymi, z makijażem i bez makijażu, z brodą i bez brody

[KRZYSZTOF] Z maseczką bez maseczki tak?

[MATEUSZ] Tak, teraz od jakiegoś czasu jeszcze z maseczką może działać, aczkolwiek lepiej żeby już nie działało…

[KRZYSZTOF] A to prawda, to dla nas wszystkich lepiej.

Zaskoczyłeś mnie, wiesz dlaczego? Bo o ile ta tranzycja faktycznie z ostatnich telefonów takich flagowych z Touch ID na pierwsze Face ID, no to dawno już było przecież kurcze, a no to już była wiele lat temu! To no tak naprawdę nie ma alternatywy, a być może w momencie kiedy nagrywamy ten odcinek, w ogóle jej już nie ma, jeżeli pojawił się nowy iPhone SE 4. gen. to on prawdopodobnie Touch ID

nie ma. Więc ciekawe ciekawe z tą szybkością mnie najbardziej to dziwi nie? Bo Face ID jest radykalnie szybsze niż Touch ID.

[MATEUSZ] Plus Touch ID jest jeszcze bardzo zawodne i uzależniony od czystego palca bo mam do tej pory służbowy telefon z Touch ID no to białego rączki dostaję, jak mam delikatnie zapłacony palec albo brudny albo nie wiem…

[KRZYSZTOF] Tak, a powiem wam że tego problemu na przykład nie ma w Macach i teraz dlaczego a nie w iPadach dlatego, że tam powierzchnia czy to na klawiaturze zewnętrznej Apple czy na klawiaturze MacBooku czy na iPadach właśnie powierzchnia tego Touch ID jest (nie wiem czy zauważyłeś) powierzchnią matową. Natomiast w ostatnim iPhonie, który miał i w ogóle w iPhone'ach który miały Touch ID to było Touch ID na wysoki połysk i tam faktycznie potwierdzam że jakiekolwiek rzeczy o których wspomniałeś no powodowały, że ono nie działało.

[MATEUSZ] Tak, w Macu powiem że nigdy nie miałem z tym problemu i teraz tak patrzę rzeczywiście jest matowe dlatego, że jest matowe tak, ale w iPadzie jest błyszczący tam w przycisku tak? A widzisz to myślałem, że matowe ok, to zwracam miałem do niedawna iPada mini.

[KRZYSZTOF] Zwracam honor. Kolejny, drugi punkt, moi drodzy, czyli blokowanie i ukrywanie aplikacji.

To jest coś, co doszło niedawno i przy okazji biometrii warto o tym wspomnieć, no bo taka możliwość właśnie ukrycia sobie aplikacji daje wam pewność, że nikt przypadkowo nie zobaczy że w ogóle tej aplikacji z tej aplikacji korzystacie lub ją macie zainstalowaną. No i teraz pytanie: kurcze no, ale naprawdę to już prędzej ta retoryka pasowałaby mi do rzeczy związanych z *mindfulness* typu: *no to sobie ukryj Instagrama, żeby zapomnieć że go masz,* nie? Chodzi mi moi drodzy o to, że bardzo wiele firm być może w takich też pracujecie ma swoją politykę prywatności która mówi o tym, że na przykład nie możecie wśród obok znajomych tych słynnych barach, taksówkach etc. pokazać, że pracujecie nad jakimś na przykład prototypowym projektem, który macie zainstalowany w ramach testów. Lub, że korzystacie z tego lub innego systemu jeszcze wewnętrznego bezpieczeństwa firmy który też ma dedykowane aplikacje, po co ta funkcja jest i zdziwilibyście się jak wiele dużych korporacji wywala ludzi, po prostu za złamanie tego typu rzeczy, bo wychodzi to prędzej czy później zawsze. Tutaj iOS bierze i wychodzi naprzeciw tego typu oczekiwaniom no, bo można faktycznie zablokować lub ukryć aplikacje po

prostu usuwając ją z widoczności w telefonie. Wtedy my wiemy jak się do niej dostać po prostu włączając sobie opcję „Pokaż ukryte”.

[MATEUSZ] Dodatkowo dla właścicieli firmy i przedsiębiorstw jest takie narzędzie jak Apple Business Manager właśnie do zarządzania urządzeniami pracowników, gdzie wy jako właściciel, możecie zdefiniować prawie wszystko na telefonie swojego pracownika; łącznie z wymuszeniem specyficznego kodu blokady, właśnie które aplikacje może pobierać, a których nie może pobierać. Które mogą być schowane, a które mają być schowane i tak dalej i tak dalej, więc fajne narzędzie mało w Polsce popularne. Coraz więcej firm jednak, które mają oddziały w Polsce, przychodzą do nas żeby właśnie te sprzęty, które zakupią dodać im do tego Apple Business Manager, bo to my jako sprzedawca musimy po numerze seryjnym w sumie je tam zainstalować.

[KRZYSZTOF] No właśnie i to jest ciekawe też w kontekście całych drożeń w ogóle MDM w Polsce, których też robi się coraz więcej, ale dalej to jest no mała skala. Kiedy się tak jak rozmawiam z właścicielami firm, którzy się zdecydowali w ogóle na przykład a znam takie osoby też przenieść flotę z ekosystemu Android/Windows w całości do ekosystemu Apple, no to tam nie jest tak, że jest 100% zmiana na lepsze, bo niektóre rzeczy idą pod górkę, ale co do zasady jeżeli chodzi o łatwość tego wszystkiego (m.in. wspomnianego przez Ciebie zarządzania flotą), no to tak, to tutaj jest ten głęboki oddech, że w końcu jest to poukładane.

[MATEUSZ] No i lokalizacja wszystkich sprzętów. Tu już nie mówię o śledzeniu pracowników, ale ostatnio klient opowiadał mi taką anegdotkę, że właśnie jego pracownik dostał firmowego MacBooka i jest studentem zabrał go na uczelnię, no i wrócił bez komputer. Oczywiście afera w firmie, po pierwsze dlaczego firmowy komputer był na uczelni, no a po drugie dlaczego go zgubiłeś? Ale na szczęście tam gdzieś po kilku dniach się znalazł i od tego momentu właśnie mój klient zdecydował się na Apple Business Manager, który zresztą wdraża razem z iDream, ponieważ mamy specjalny dział zajmujący się tym/

[KRZYSZTOF] To też warto powiedzieć, oczywiście namiary do tego do kontaktu z Tobą czy w ogóle w takich sprawach zostawimy też w opisie.

[MATEUSZ] Mamy dział biznesowy także kontakt jest.

[KRZYSZTOF] Super, to pora na punkt trzeci: udostępnianie aplikacjom tylko wybranych kontaktów.

To jest coś z czym prawdopodobnie mieliście minimum raz do czynienia a mianowicie, jak instalujecie jakąś aplikację, która na logikę, będzie potrzebowała komunikować się z książką adresową w telefonie, no to iOS Wam wyświetli monit z pytaniem, czy zezwalacie na dostęp do kontaktów. Lub na dostęp do wybranych kontaktów i bardzo często my klikamy – zezwól na dostęp do całości książki – błędnie. Jeżeli używacie na przykład komunikatora, a są takie osoby i są takie rodziny, ja też jestem tego przykładem, że mam WhatsApp'a tylko na wyjazdy zagraniczne, bo są miejsca na świecie gdzie, że tak powiem, nie załatwisz nawet pomocy medycznej bez WhatsApp'a, a już nie mówiąc o wezwaniu jakiejś taksówki czy załatwieniu czegoś z właścicielem noclegu – no to też w rodzinie dwie osoby korzystają z WhatsApp'a. To są osoby poza ekosystemem Apple i ja wiem że tylko z nimi się na tym WhatsApp'ie komunikuje. Więc mam zezwolenie na dostęp do książki tylko dla ich kontaktów i nie widzę powodu żeby WhatsApp miał do całości.

[MATEUSZ] Potwierdzam ja w WhatsApp'ie mam dokładnie to samo żeby miał mieć dostęp do całości no, bo po co na przykład mój Messenger ma mieć, skoro ja w ogóle nie korzystam z Facebookowego Messenger'a. Tam w ogóle jest wszystko wyłączone nawet dostęp do Biblioteki Zdjęć.

[KRZYSZTOF] To jest kolejna sprawa – dostęp do Biblioteki Zdjęć – dobrze, że to powiedziałeś, ponieważ szalenie ważna. Tak samo, jak kontakty, no bo w kontaktach możemy mieć po prostu dane poufne chociażby naszych współpracowników czy naszych klientów, no ale w zdjęciach to my możemy mieć zdecydowanie więcej do opowiedzenia o naszym życiu, czego byśmy opowiedzieć publicznie nie chcieli. Ja mam taką zasadę, że jeżeli mam to pytanie, czy zezwalam aplikację na dostęp do Biblioteki Zdjęć, to moją domyślną odpowiedzią jest – nie. Nawet takie już, wiesz jak jak pamięć mięśniowa – nie. Taki nawyk wyuczony, że zawsze klikam NIE i teraz kiedy zaczynam używać tej aplikacji i znowu mam problem z tym, że już dostanę inne powiadomienie, że nie mogę zrealizować tego i tej operacji w aplikacji lub skorzystać z tej funkcji, bo nie mam dostępu do zdjęć – no to ja się wtedy dowiaduję, dlaczego warto lub nie warto ten dostęp było nadać. Ale co do zasady, nigdy nie nadaje go tak z automatu.

[MATEUSZ] Tto tam jest taka fajna opcja, że możemy sobie na przykład, jeżeli potrzebujemy Instagrama to musi mieć dostęp do zdjęć, żebyśmy dodali zdjęcie

czy, jak zrobimy zdjęcie żeby się zapisało w bibliotece. To my nie musimy dawać dostępu do absolutnie całej biblioteki tylko możemy wybrać jedno czy kilka zdjęć, które będą się wyświetlały, jakby w podglądzie Instagrama, czy innej aplikacji. Też jest w miarę bezpiecznie, bo wybieramy albo to, co chcemy no, a jak chcemy wszystko no to YOLO…

[KRZYSZTOF] Tak i pamiętajcie o tym, bo czasami choćby nie wiem jak Apple zaprojektowało te swoje systemy bezpieczeństwa w kolejnych wersjach iOS, poprawiło zrobiło bardziej niewidoczne, intuicyjne nieważne to i tak jak przyjmiecie sobie taką zasadę, że zawsze jestem na NIE i ona będzie jeszcze wyższym poziomem bezpieczeństwa. Takim Waszym, automatycznym i lepszym niż cokolwiek, co jeszcze wymyśli Apple, żeby lepiej informować użytkowników o potencjalnych zagrożeniach.

[MATEUSZ] Nazwijmy to elektroniczna asertywność.

[KRZYSZTOF] Powiem ci, że dzisiaj Mateusz rzucasz takimi tytułami, że ja tylko mogę je zapisywać na kolejne na przyszłe odcinki. Zanotowane.

Czwarta rzecz moi drodzy, domyślne blokowanie okien przeglądania prywatnego w Safari.

Już tłumaczę, o co chodzi. Mianowicie podczas korzystania z przeglądarki czy z przeglądania w trybie prywatnym w Safari, ono nie zapamiętuje odwiedzanych stron historii wyszukiwania ani danych autouzupełniania. Ja wiem, że zaraz znajdzie się grupka nerdów, którzy powiedzą, ale to się da obejść! Ten odcinek jest do przeciętnego użytkownika, przypominamy, więc kontynuując – Apple wprowadziło możliwość domyślnego blokowania okien przeglądania prywatnego dzięki czemu, użytkownicy mogą zachować otwarte karty i łatwo do nich później wrócić, odblokowując je za pomocą wspomnianej w punkcie pierwszym biometrii czyli Face ID, Touch ID czy Optic ID. Mówiąc na chłopski rozum, macie otwarte coś w trybie prywatnym, minimalizujecie okno w Safari, ono wraca i żeby znowu wyświetlić tę zawartość, musi najpierw być odblokowane jakąś formą biometrii.

[MATEUSZ] Dokładnie i z prywatnego przeglądania polecam na przykład szukać biletów lotniczych bo wtedy przeglądarka nie zapisuje że cały czas śledzicie jakiś lot no i nie podbija wam sztucznie ceny.

[KRZYSZTOF] To tak plus bardzo często robić to, co Mateusz powiedział, czyli w ramach przeglądania prywatnego, bo wtedy nie macie faktycznie tej pamięci jakby o waszych usilnych próbach znalezienia kilkaset złotych taniej tego biletu na konkretny lot, w konkretnym dniu – to jest jeszcze jeden protip ode mnie. Mianowicie korzystać z Safari, na górze tam macie w przeglądarce jak sobie wejdziecie na pasku stanu – wchodzicie na daną stronę Safari w trybie prywatnym i potem sobie dajecie „Wyświetl narzędzia deweloperskie" i dajecie „Wyświetl tę stronę używając agenta XYZ" i tam na przykład dajecie „używając agenta Google Chrome na system Windows". Wtedy Safari jakby wyświetla Wam tę stronę trochę udając przeglądarkę Chrome na Windowsie i dzięki temu, nie jest to jakaś wiedza tajemna, bo można to prosto w Google znaleźć, dzięki temu systemy rezerwacji linii lotniczych czy tam hoteli trochę traktują Was lepiej z punktu widzenia oszczędności. Faktycznie ja już to kilka razy sprawdzałem i jest tak, że użytkownicy Apple'a mają w niektórych systemach droższe ceny na noclegi czy loty niż użytkownicy Windowsa.

[MATEUSZ] To o tym nie wiedziałem, właśnie mi szczęka opadła.

[KRZYSZTOF] Piąta rzecz: Ochrona przed śledzeniem linków.

Pozostajemy w temacie przeglądania internetu czyli niektóre linki zawierają jakby dodatkowe informacje umożliwiające śledzenie Was. To są tak zwane informacje po pytajniku. Jak jest jakiś adres internetowy i tam w pewnym momencie pojawia się pytajnik i potem dziwne literki typu UTM=kampania jakaś tam i dziwny ciąg znaków, no to informuje, że jakby na przykład kiedy otwieracie jakiś newsletter i ktoś ma zapiętą afiliację, która pozwala mu zarobić, jak wy klikniecie w link z jego newslettera. Ta osoba wie, że wy kliknęliście i co zrobiliście dalej no nie? Apple jako ta firma, która ma obsesję na punkcie prywatności, bardzo utrudniła życie marketerom na całym świecie, ponieważ zaczęła to tępić. Zaczęła to po prostu blokować i jak ta funkcja jest w Safari włączona ochrona przed śledzeniem linków w ramach Apple Private Relay, o którym jeszcze powiemy za chwilę, to co do zasady Apple blokuje tego typu rzeczy w linkach na które wchodzicie. Po prostu je wycinając no i też nie daje informacji w drugą stronę, co Wy robicie z tym linkiem i jakie są Wasze kolejne kroki. To się przydaje dlatego. że takie zbędne znaczniki z adresów stron które Wam ktoś daje w wiadomościach mailach czy podczas w ogóle przeglądania w trybie prywatnym. Też po prostu zbierają o Was informacje a mogą nie zbierać i to nie trzeba do tego antywirusów instalować czy jakiegoś

dodatkowego oprogramowania, tylko włączyć ochronę przed śledzeniem linków w ustawieniach Safari w systemie.

[MATEUSZ] Czyli co? Jak na przykład kopiuję sobie od Ciebie link afiliacyjny to Safari utnie mi końcówkę z tą afiliacją nie ona zablokuje?

[KRZYSZTOF] Safari nie wyśle informacji, że na nią wszedłeś tak, jakby ten link był bez tej końcówki. Ono go fizycznie nie utnie, ale pominie.

[MATEUSZ] To może mieć swoje plusy i minusy.

[KRZYSZTOF] Oczywiście, jak wszystko.

[MATEUSZ] Tak, czyli trzeba też sobie świadomie to włączać i wyłączać tak mi się wydaje.

[KRZYSZTOF] Tak aczkolwiek nie dając się zwariować, bo dla takiego zwykłego przeciętnego użytkownika to moim zdaniem lepiej, żeby miał to zapięte i włączone niż niewłączone. Mogą się zdarzyć sytuacje, że na przykład jest jakiś system rezerwacji hoteli, jak już jesteśmy przy tych podróżach, i on na którymś etapie wymaga otwarcia jakiejś zgody w osobnym okienku. Lub zaznaczenia jakiegoś *checkboxa* właśnie w tym okienku wyskakującym lub ma jakieś javascripty po prostu w kodzie, które coś tam muszą przetworzyć tu i teraz. Safari tego w ogóle nie wyświetli i będzie sytuacja taka, że klikasz przycisk – idź dalej – tylko się nic nie dzieje. To jest wtedy powód narzekania wielu osób, że Safari jest gównianą przeglądarką i ja się temu nie dziwię, bo to co do zasady, *usability* jest wtedy skopane. Ale coś za coś, nie? Dlatego zawsze też mam drugą przeglądarkę alternatywną zainstalowaną u siebie na Macu i u mnie jest to akurat Opera, bo ona jakby żeby mieć taką zwykłą przeglądarkę, która obsługuje strony jak cały świat Windows.

[MATEUSZ] To najczęściej strony nasze rządowe nie działają w Safari.

Trzeba to wspomnieć, może ktoś posłucha, ale jeszcze tak a propos Safari to też mamy wyskakujące okienka, które są z automatu zablokowane, a które jakby sygnalizują to, że chcą być otwarte w bardzo nieintuicyjny sposób. Takim małym monitorkiem przy przy pasku adresu, a one nieraz dużo dla nas znaczą, bo powiedzmy jak podpisujemy jakieś raty i musimy pobrać umowę, to ona najczęściej

wyskakuje nam właśnie w takim wyskakującym małym okienku. No i gdy nie możemy po prostu przejść dalej, nie wiemy co jest grane, to wtedy warto spojrzeć z prawej strony w końcówkę adresu i jeżeli tam są na siebie nałożone dwa takie malutkie okienka, to kliknąć w to. To znaczy, że okienko jakieś chce wyskoczyć, a mamy to zablokowane.

[KRZYSZTOF] Dobrze, że o tym powiedziałeś, ponieważ faktycznie jest to w bardzo takim ukrytym miejscu.

Punkt szósty: bezpieczeństwo osobiste, czyli taka funkcja kontrola bezpieczeństwa.

Jeżeli Wasze bezpieczeństwo, osobiste przede wszystkim, jest zagrożone to może on, ten system jakikolwiek z którego korzystacie z Cupertino. użyć funkcji Kontrola bezpieczeństwa, aby szybko zaprzestać udostępniania informacji na Wasz temat, zaktualizować te informacje, które już udostępniacie osobom i aplikacjom trzecim. Ta funkcja może pomóc sprawdzić, kto w ogóle udostępnia te informacje, ograniczyć wiadomości, połączenia na FaceTime, zmienić nawet kod dostępu i wiele więcej. Ona jest zaszyta w ramach właśnie Apple Private Relay i tak, polecamy ją włączyć. Kontrola bezpieczeństwa nigdy nie wiadomo kiedy się przyda, a najlepiej żeby się nie przydała nigdy. To trochę tak, jak AirTag którego kupujesz, żeby go mieć, ale modlisz się, żeby go nigdy nie użyć.

[MATEUSZ] Dokładnie. To ja jeszcze opowiem jedną anegdotę o AirTagu. Miałem klienta, który zgubił AirTaga – zostały mu w rękach klucze, a AirTag wypadł i się zgubił.

[KRZYSZTOF] OK, jak widzicie – żadna ochrona nie jest kuloodporna, żeby ładnie to powiedzieć.

Siódma rzecz: raport prywatności w aplikacjach.

Teraz tak, dzięki w ogóle tej funkcji raport prywatności aplikacje mogą dać znać użytkownikom, jak często one same uzyskują dostęp do danych na które wcześniej wyrazili oni zgody. Pamiętacie, jak mówiliśmy w tym odcinku o wyrażeniu zgody na dostęp do kontaktów, dostęp do zdjęć? No to, to wszystko, te nasze zgody wyrażone lub nie znajdują się w takim miejscu, jak raport prywatności. Chociażby w przeglądarce Safari, czy w systemie. Po włączeniu tej funkcji my możemy zobaczyć szczegóły dotyczące częstotliwości uzyskania dostępu aplikacji do

danych, właśnie takich, jak lokalizacja, aparat, mikrofon, zdjęcia, kontakty no i warto pamiętać, aby sprawdzać sobie te sekcje na karcie danej aplikacji w App Store.
Zanim ją w ogóle pobierzecie lub zdecydujecie się używać, bo co do zasady, to Apple było pierwszą firmą która postawiła na taką bardzo mocną weryfikację tego co trafia do ich sklepu od samego początku jego istnienia. Także weryfikacje z wykorzystaniem rąk ludzkich, nie tylko algorytmów, co robi do dziś. Ten temat jest bardzo kontrowersyjny, a część osób twierdzi, że to jest zamykanie się w ekosystemie, że to jest jakaś tam forma reżimu. Ja twierdzę, że jeżeli Apple może mnie uchronić przed tym, że ktoś mnie okradnie, bo po prostu pobiorę aplikację latarka, która okazała się po prostu aplikacją krypto i wyczyściła moje konta czy jakiś dziwny inny scenariusz – to ja już wolę, żeby te zasieki były mocno wysoko postawione.
Jakby bardzo mało tych rzeczy przechodziło przez ten mur i aby od paru lat wymusiło coś takiego, że każdy developer jeżeli wysyła aplikację do App Store Connect, zanim dostanie zgodę na to, że ona się pojawi w sklepie; będzie można ją pobierać lub kupować, albo kupować w ramach App In Purchase subskrypcję – to musi mieć bardzo wylewnie opisaną tą sekcję o prywatności. Tam są między innymi podane informacje o tym, jakich danych potrzebuje aplikacja, czyli do jakich danych musi mieć dostęp, czy jest związana z płatnościami, czy korzysta z biometrii i tak dalej i tak dalej. To wszystko jest bardzo ważne i warto sobie poczytać po prostu tą sekcję w App Store, zanim pobierzecie jakąś aplikację.

[MATEUSZ] Tak i tu od razu mogę wjechać też z przykładem aplikacji mBanku, o której jakiś czas temu było głośno na Androidzie. Pojawiła się w sklepie aplikacja mBanku, która była aplikacją podrobioną i pobierając taką aplikację, po prostu właściwie nie czytając tego opisu, nowi użytkownicy mBanku pobrali ją, zalogowali się na swoje konto no i okazywało się, że te loginy i jednorazowe hasła dwustopniowej weryfikacji trafiały od razu do oszustów.

[KRZYSZTOF] Tak, słyszałem też w tamtym tygodniu o podrobionej aplikacji mObywatel.

[MATEUSZ] Także to, co mówisz jest bardzo ważne, żeby właśnie tam sobie to przeczytać. Aczkolwiek, no teoretycznie możemy zaufać App Store, że zrobił to za nas prawda?

[KRZYSZTOF] Tak, teoretycznie tak, ale nawet dla pogłębiania swojej wiedzy o tym jak działa rynek aplikacji i co mogą w ogóle o nas wiedzieć, warto, nie?

Ósmy punkt: ukrywanie adresu e-mail w ramach subskrypcji iCloud+.

To jest bardzo ważne, że te subskrypcje należy mieć wykupioną. I w ramach iCloud+ możecie tworzyć unikalne losowe adresy e-mail do wykorzystania w aplikacjach witrynach internetowych lub innych miejscach, gdzie wymagane jest chociażby założenie konta, nie? I tutaj warto też powiedzieć o tym iCloud+, że naprawdę moi drodzy, warto dopłacić te parędziesiąt złotych do tego, żeby mieć ten większy dysk w chmurze i mieć usługę iCloud+, no bo dzięki temu macie dużo więcej tych funkcji bezpieczeństwa dostępnych po prostu. Naprawdę jest to niewspółmierne z tą opłatą miesięczną, także ja polecam ze swojego ze swojej strony. A już idealnie wziąć sobie iCloud+ w ramach pakietu Apple One. No, bo dostajecie w cenie i Apple Arcade i Apple TV+ no i oczywiście Apple Music.

Dobra to wracając i już jeżeli korzystacie z Safari, to Safari samo wam podpowie na tym formularzu tworzenia konta nowego w systemie. że *hej czy chcesz skorzystać z funkcji ukryj mój e-mail?* Jak sobie to klikniecie to Apple wygeneruje dla Was losowy adres e-mail, który tak naprawdę będzie maską dla Waszego prawdziwego adresu e-mail, który zna Apple. Macie go wpisanego w ustawieniach Apple ID czy w ustawieniach swojej karty w kontaktach, no i teraz co się dalej wydarzy? System, w którym zakładacie to konto będzie miał dostęp do tego jednorazowo stworzonego adresu e-mail, tak? Czyli unikatowego, zamaskowanego adresu e-mail, ale jak ktoś wyśle wiadomość na ten adres, to ona dostanie się na ten Wasz prawdziwy adres e-mail, bo po prostu Apple jest tutaj mostem, który w czasie rzeczywistym przekazywanie tej korespondencji robi i działa to sekundowo.

[MATEUSZ] To się *alias* chyba nazywa do maila.

[KRZYSZTOF] Tak i warto sobie to włączać, jeżeli tylko możecie, bo później w Pęku Kluczy czy w aplikacji Hasła teraz w systemach Apple będzie to wszystko zapisane. Wy nie musicie się obawiać o to, że zapomnijcie tego randomowego adresu e-mail, który dla Was stworzono, bo Wy go w ogóle nie musicie znać. Bo, jak macie zapisane dane logowania w Hasłach, to po prostu się logujecie biometrią nie? To jest wszystko za Was uzupełniane, a Wy nawet nie widzicie tych danych.

[MATEUSZ] Na przykład to zamawiamy paczkę i możemy sobie wygenerować taki ukryty losowy adres e-mail, żeby na liście przewozowym się nam nie wyświetlił ten prawdziwy. Będzie tam ten unikalny adres e-mail, dzięki czemu powiedzmy, jeżeli paczka by się gdzieś zgubiła, kurier by ją rzucił pod drzwi, ktoś by sobie zobaczył,

ale nie będzie znał Waszego adresu e-mail, bo na paczce będzie wydrukowany ten *alias* właśnie.

[KRZYSZTOF] Raczej mało osób wpadnie na to żeby ten *alias* wykorzystać i zacząć coś na niego wysyłać, no bo jak zobaczy ciąg cyferek i dziwnych znaczków.

[MATEUSZ] Aczkolwiek zauważyłem, bo ja z tego często korzystam zauważyłem, że Apple dość fajnie generuje te adresy e-mail, bo na przykład mam jakiś e-mail DorotkaCośTamCośTam@icloud.com. Także regionalnie też to robią, a nie na zasadzie alfanumerycznych jakichś znaków.

[KRZYSZTOF] To nie wiedziałem tego.

[MATEUSZ] Powiedzmy logujemy się do jakiejś aplikacji. na chwilę jak była ta aplikacja Face Swap tak? Żeby zamienić się twarzą na zdjęciu, to możemy sobie wygenerować taki adres e-mail i w ustawienia iCloud podpisać nawet do czego on jest używany i może być używany tylko do jednej konkretnej aplikacji właśnie Face Swap i powiedzmy pobawimy się tą aplikacją, usuwamy konto, usuwamy tego maila i żaden spam nam już nie przyjdzie. Jeżeli nawet ten adres e-mail by gdzieś właśnie poszedł na listę mailingową.

[KRZYSZTOF] Dodatkowo jeszcze przy tej okazji warto wspomnieć, że podobnie działa Apple Pay, co do zasady Apple Pay jest globalnie najbezpieczniejszą formą płatności zbliżeniowych. I teraz dlaczego?

I dlaczego nie jest to po prostu kolejne zdanie wyświechtane z materiałów marketingowych Apple'a? No dlatego, moi drodzy, że od samego początku istnienia Apple Pay działa tak, że jest w momencie każdorazowej, jednostkowej płatności generowany dla Was unikatowy token, czyli mówiąc zupełnie wprost, taka wirtualna karta płatnicza tylko dla tej jednej transakcji.

[MATEUSZ] Z jednorazowym numerem karty po prostu.

[KRZYSZTOF] Tak, z losowym numerem karty. I Wy płacicie swoją kartą, ale jakby osoba, której płacicie ma dane tej jednorazowo wygenerowanej na potrzeby – znowu *aliansu*, czyli przekaźnika tej płatności, żeby Was dodatkowo chronić. Dlatego Apple Pay jest najbezpieczniejszą formą płatności zbliżeniowych globalnych.

[MATEUSZ] Tak, możecie mieć z tym problemy jak będziecie robić zwroty w ubraniowych sieciówkach, ponieważ tam miłe panie zawsze proszą, żeby przyłożyć tą samą kartę i weryfikują to z potwierdzeniem płatności, no ale zawsze ten numer będzie inny, więc trzeba im wtedy powiedzieć, że to było płatne Apple Pay'em i tam jest losowy numer. No i wtedy chętnie zrobią zwrot. Ale na początku...

[KRZYSZTOF] Tak, na tą kartę waszą prawdziwą.

Find My i przybliżona lokalizacja.

Kontrola lokalizacji firmy Apple daje wybór, czy aplikacje mogą widzieć ich przybliżoną lokalizację — na obszarze około 26 km kwadratowych — zamiast dokładnej lokalizacji. Dzięki temu możecie korzystać z aplikacji, które wykonują takie czynności, jak wyszukiwanie pobliskich restauracji lub sprawdzanie lokalnej pogody, nie podając więcej informacji, niż potrzebują. W połączeniu z Airbagami i całym Find My, daje to niesamowitą przewagę całemu ekosystemowi Apple.

Tutaj ciekawostka – w Ustawieniach macOS, sekcja Lock Screen (Zablokowany ekran po PL pewnie) i dalej w tej sekcji opcja *„Show message whee locked”* można sobie zdefiniować wiadomość, która wyświetla się na ekranie logowania. Po co?
A no po to, że jak zostawicie lub nie daj Boże zgubicie gdzieś Maca, to podając tam jakiś kontakt do siebie możecie ułatwić osobie, która go znajdzie kontakt z Wami.

[MATEUSZ] Jeżeli zgubicie takie coś, to właśnie logując się na stronę iCloud można oznaczyć takie urządzenie jako utracone i wtedy dodać właśnie notkę, która się wyświetli na ekranie, jak to urządzenie połączyć z internetem. Właśnie też, że został zgubiony należy do mnie zwrócić. Dlatego też moim zdaniem, jak zgubicie telefon czy iPada, a macie w nim kartę SIM, to nie warto jej od razu blokować, żeby ten telefon, to urządzenie, czy tam iPad miało dostęp do internetu.

[KRZYSZTOF] Ono i tak jest, jeżeli ma włączoną biometrię, no nie Mateusz, to ono i tak jest zablokowane, więc i tak nikt tam się nie dostanie. A możecie sobie utrudnić jego znalezienie, jak zablokujecie numer, nie?

[MATEUSZ] Jedyna opcja, kurczę, znowu mam anegdotkę. Jedyna opcja właśnie, żeby coś zrobić z takim telefonem zgubionym, a zablokowanym, to używanie Siri.
W sobotę byłem w pracy i taka dziewczynka zostawiła telefon u nas w sklepie

i kojarzyliśmy ją, bo kupowała z rodzicami Apple Pencila wcześniej. Wiedzieliśmy, która to jest. No i klient nam przyniósł ten telefon, bo leżał gdzieś tam na salonie.

Schowaliśmy go i tak właśnie mój kolega Kamil bierze, kurczę, może zadzwonię do mamy, ale patrzy, kurde, cały telefon po ukraińsku. Szybko sprawdziliśmy, jak w Siri powiedzieć mama po ukraińsku. Okazało się, że bardzo podobnie.

No i powiedział do Siri, call mama i udało się dzięki temu połączyć z jej rodziną i szybko przyszli po telefon. Także obyło się bez stresu.

[KRZYSZTOF] Wow, a to ciekawy protip! No tak, bo Siri co do zasady nie rozpoznaje (z wyjątkiem HomePodów) głosów, a to też bywa różnie, bo czasami tak rozpozna, że nie chce się denerwować… W każdym razie, tak, faktycznie nie wpadłem na to, że można powiedzieć do czyjejś Siri.

[MATEUSZ] Powiem Ci, że też na to nie wpadłem, tylko tak stoimy, a może Siri zadzwonię do jej mamy. No dawaj, no i się udało.

[KRZYSZTOF] To w ogóle nie powinno mieć miejsca, moim zdaniem.

[MATEUSZ] Także pewnie by i tak do nas wrócili, ale oszczędziliśmy im może kilkuminutowego większego stresu.

[KRZYSZTOF] Co do zasady to nie powinno mieć miejsca. Z punktu widzenia dbałości Apple'a o prywatność, moim zdaniem to nie powinno mieć miejsca, żeby tak się dało zrobić, ale się da.

[MATEUSZ] Pewnie można wyłączyć Siri na zablokowanym ekranie, bo na zablokowanym ekranie można prawie wszystko wyłączyć, łączyć z rozsunięciem paska zadań tego od góry.

[KRZYSZTOF] Centrum sterowania, nie? Tak, to prawda.

Ty to masz tych anegdotek. Dobrze, że akurat ciebie zaprosiłem do tego tematu. Tak myślałem, że tu będzie po prostu się sypało z rękawa.

[MATEUSZ] Kto w handlu pracuje, w cyrku się nie śmieje.

[KRZYSZTOF] Ty to masz dzisiaj wenę.

[MATEUSZ] Ja proponuję, Krzysiu, ja Ci dam niebieską koszulkę, zaproszę Cię na weekend i tematy na odcinki będą się pisać sami.

[KRZYSZTOF] Być może powinienem kiedyś zrobić taki test i z Wami jeden dzień weekendu przepracować. Może to by mi pokazało, że moje wyobrażenie o życiu poza bańką i tak jest życiem w bańce.

[MATEUSZ] Tak, tak. Na pewno byłoby to dla Ciebie niesamowicie wielką inspiracją na odcinki.

[KRZYSZTOF]
Dziesiąty punkt tymczasem, moi drodzy.

Wskaźniki nagrywania i w ogóle użycia mikrofonu i kamery, o których wspomniałem na samym początku, Mateusz. To jest sprawa prosta.

Zielone oznacza użycie kamery, pomarańczowe użycie mikrofonu na każdym urządzeniu, łącznie z Apple TV. Tylko, że Apple TV oczywiście tę ikonkę wyświetli Wam na ekranie telewizora, żebyście tam nie szukali pod szafką na Apple TV jako na dostawce. I to jest super!

I zauważ, że chyba dwóch producentów ze świata Androida to wdrożyło z tego, co kojarzę. W każdym razie tego akurat nie skopiowano. Kurczę szkoda. Takie przydatne.

[MATEUSZ] Tak, więc tak podsumowując, jeżeli widzisz pomarańczową lub zieloną ikonkę, a nie używasz kamery albo nie rozmawiasz z nikim, to wiedz, że coś się dzieje.

[KRZYSZTOF] Tak, i że trzeba się tym zainteresować.

[MATEUSZ] Że coś pod spodem nas tam podsłuchuje może.

[KRZYSZTOF] Tak, i dopiero wtedy faktycznie warto pobiec do salonu iDream
i zrobić rozróbę, że mam podsłuch.

[MATEUSZ] Tak, ale jak rozsuniesz sobie właśnie centrum sterowania, Centrum sterowania, to tam od razu na górze powinna być informacja, co używa w tej chwili mikrofonu na przykład, czy kamery.

[KRZYSZTOF] I właśnie czekałem, aż to powiesz. Dokładnie, więc sam system też Wam o tym powie.

[MATEUSZ] Teraz jak rozmawiamy i mam pomarańczową ikonkę, jak sobie rozwijam na Macu właśnie Centrum sterowania, to mam, że QuickTime Player i Zoom używają mikrofonu.

[KRZYSZTOF] Dokładnie tak. A co będzie jak wyciszę, na przykład, bo ktoś może się tak zastanowić teraz, a co będzie jak wyciszę mikrofon w Zoomie? Nic nie będzie.

Dalej ta ikonka się będzie palić, że co do zasady Zoom w trakcie połączenia cały czas używa tego mikrofonu, więc spokojnie, nie da się tego w ten sposób zhakować.

[MATEUSZ] Tak, bo Zoom pewnie używa, ale Ty mnie nie słyszysz wtedy. Dokładnie tak. Po prostu mnie przekazuje dalej.

[KRZYSZTOF] Dokładnie tak.

Dobrze i na sam koniec, moi drodzy, ten iCloud Private Relay, czyli przekazywanie prywatne.

On się tu wiele razy już pojawił, bo co do zasady, to jest taki znowu parasol, który ma pod spodem fragmenty kilku rzeczy, o których mówiliśmy w poszczególnych punktach, a jest to dostępna w ramach znowu iCloud+, taka usługa przekazywania prywatnego, która zwiększa Waszą prywatność podczas przeglądania internetu w Safari konkretnie. Czyli zapewnia, że nikt, nawet Apple, nie widzi, kim jest użytkownik, jakie strony odwiedza, jakie strony odwiedzał wcześniej.
Nie ma tych wszystkich właśnie UTM-ów przekazywanych, tak czy dziwnych, jakby zbierających o użytkowniku mechanizmów na danych stronach internetowych, dlatego chociażby ja od wielu lat używam Safari, jako głównej przeglądarki? Od ponad dekady, choć tak naprawdę to Private Relay relatywnie niedawno weszło dopiero, właśnie ze względu na bezpieczeństwo, ona ma swoje wady, ale ma też

niewspółmiernie dużo zalet i m.in. sam ten raport o prywatności, który już na karcie startowej w Safari się wyświetla. Jak ja tam sobie widzę, nieraz przy końcu tygodnia, że w tym tygodniu zablokowaliśmy 129 mechanizmów śledzących na stronach, które odwiedzałeś, tylu i tylu dziesiątkom stron nie pozwoliliśmy zrobić tego czy tego, to są fajne dane. Też uświadamiające w jak popierdzielonych czasach żyjemy, jeżeli chodzi o śledzenie naszej aktywności.

[MATEUSZ] W luz Safari jeszcze co jakiś czas wyrzuca Ci raport o wycieku haseł. Jeżeli Twoje hasła są na liście danych, które wyciekły, to od razu Safari Cię o tym informuje, żebyś zmienił hasła do konkretnych witryn.

[KRZYSZTOF] Tak i jeszcze warto dodać, jeżeli korzystacie z aplikacji Hasła wprowadzonej od zeszłej jesieni na wszystkich platformach, czyli z dawnego pęku kluczy, to w tej aplikacji hasła, podobnie jak u konkurencji np. w 1Password, także Apple informuje o tym, że w tym tygodniu doszło do wycieków danych w tym i tym serwisie, rekomendujemy zmianę hasła.

[MATEUSZ] Także też warto tego nie olewać. Tak, bo jak działają później takie skradzione dane? Osoby, które zajmują się właśnie takimi oszustwami mają programy, które podstawiają później, powiedzmy wycieka Wasz login i hasło, czyli mail i hasło do Facebooka i jeżeli macie dokładnie tymi samymi danymi logowanie do innej witryny, to hakerzy mają takie strony, które podstawiają to hasło do miliarda stron internetowych, która im wejdzie, no to później się włamują.

[KRZYSZTOF] Dokładnie tak.

Moi drodzy, więcej o tych wszystkich funkcjach prywatności od Apple znajdziecie na specjalnej podstronie w domenie oczywiście polskiej, do której link znajdziecie w opisie tego odcinka. Warto sobie tam wszystko to przeklikać, poczytać po polsku, bo opcji jest naprawdę, naprawdę wiele.

Ja Tobie bardzo serdecznie Mateusz dziękuję, nie tylko za pomysły na tytuły kolejnych odcinków, a być może i książek, ale za oczywiście cały sznurek anegdotek z salonów z pierwszej ręki, bo to właśnie takie historie pokazują nam, mówiąc zupełnie wprost prawdę, a nie nasze wyobrażenia z X czy innych platform, gdzie siedzą technologiczni nerdzi i sobie myślą, że ten świat kończy się na nich.

Bardzo dziękuję.

[MATEUSZ] Dziękuję bardzo i do usłyszenia ponownie.

[MUZYKA]

Raz jeszcze, na koniec, żeby nie umknęło. Przypominam, zostaw na Apple Podcasts lub na Spotify taką liczbę ⭐ gwiazdek, jaką uznasz za stosowną.

Do usłyszenia w kolejnym odcinku, a za dziś bardzo dziękuję.

[MUZYKA CICHNIE – KONIEC ODCINKA]