J@nek radzi: Jak zastrzec swój numer PESEL

Zastrzeżenie numeru PESEL służy temu, by nikt nie mógł wykorzystać go bez naszej wiedzy.

Jeśli chcecie mieć pewność, że nikt nie wykorzysta Waszego numeru PESEL, możecie go zastrzec. Zdarzają się jednak sytuacje, w których niezbędne jest cofnięcie zastrzeżenia. Jak to zrobić z pomocą aplikacji mObywatel – powie o tym J@nek Radzi. Posłuchajcie i zobaczcie.

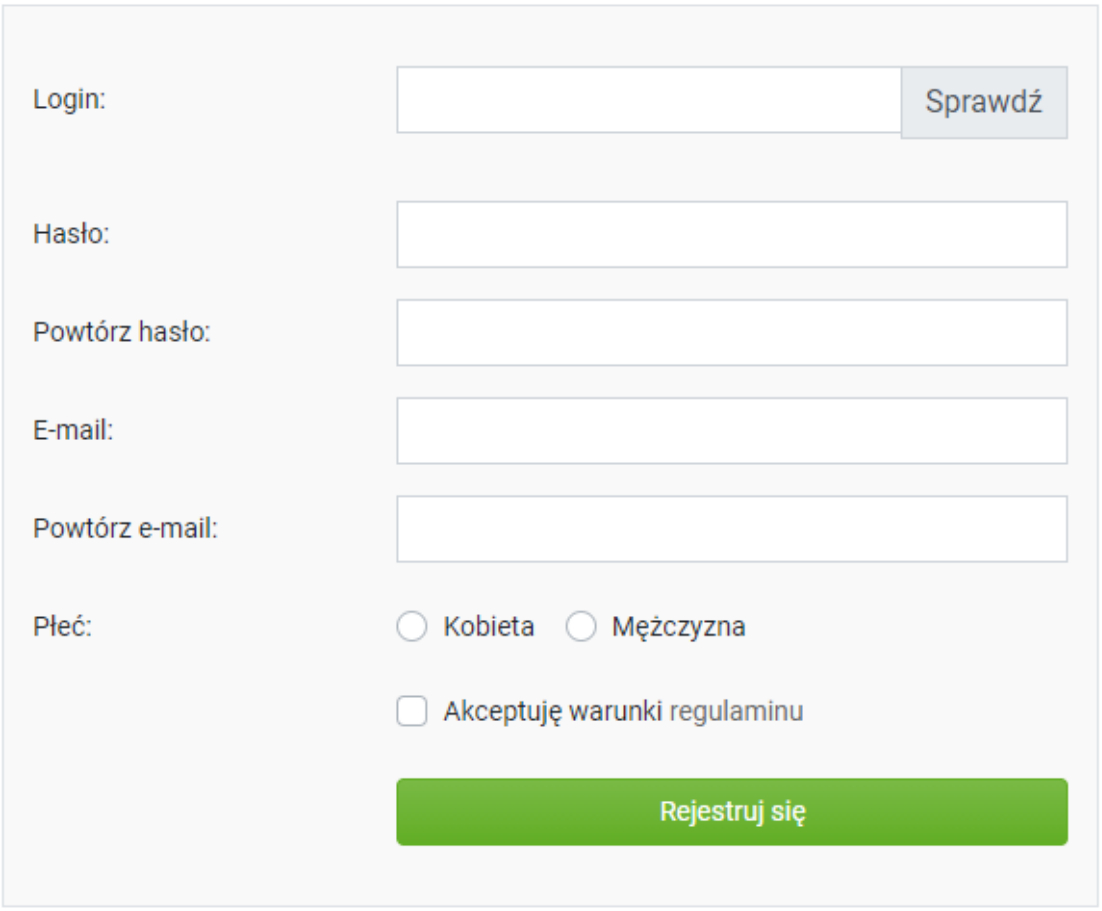
Nick to nie znaczy Nikt – o pseudonimach w internecie

Internet to środowisko, gdzie łatwiej i częściej możesz być osobą anonimową. Możesz ujawniać te informacje o sobie, które chcesz. Wszystkie lub żadnej. Możesz nawet ukryć własne imię!

Internet to także miejsce spotkań. Przy logowaniu na forach czy grupach pojawia się prośba o zarejestrowanie a z nią formularz do wypełnienia. Jedna z rubryk to często nieco zagranicznie brzmiące: NICK.

Nick, login czy chwilowe imię?

NICK [czytaj: niik] to inaczej pseudonim czy przezwisko (bez negatywnego nastawienia), które chcesz używać w danym serwisie internetowym czy grupie. Zdarza się, że podobną rolę odgrywa LOGIN czyli nazwa stosowana do zalogowania się np. do portalu.



Podczas komunikowania się w grupie, na portalu lub forum nick pojawia się obok Twojej wypowiedzi i tym sposobem staje się Twoim identyfikatorem.

Inni użytkownicy mogą za jego pomocą zwracać się do Ciebie. Wyobraź sobie, że Twój nick to: Zielona – „Jak się dziś masz, Zielona?” lub Zamaskowany – „Jak mija Ci dzień, Zamaskowany?”.

Warto podejść rozważnie do wyboru swojego nicka. Nie jest to

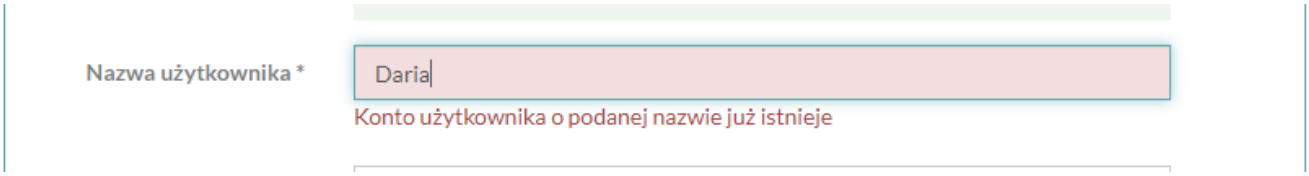
proste zadanie.

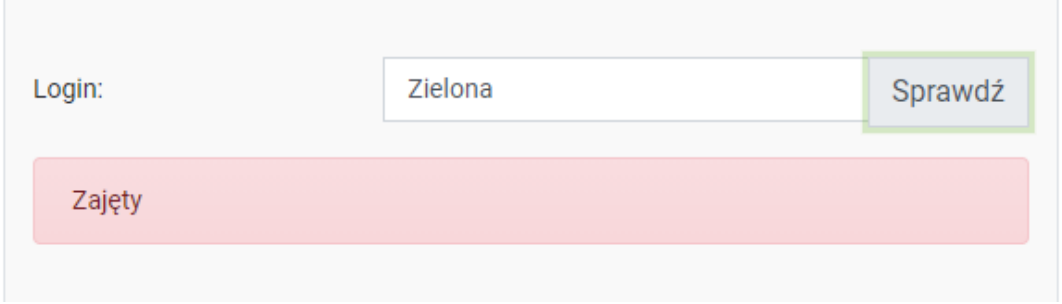
Co powie Twój nick?

Pseudonim nie tyle Cię ukrywa, co kształtuje Twój wizerunek. Pomyśl chwilę, nad osobami używającymi takich nicków: Ruda, Biceps, Różyczka czy Łobuz. Już ich przeczytanie budzi pewne skojarzenia. W pseudonimie możemy zawrzeć swoje poglądy, zainteresowania czy oczekiwania. Niekiedy prowokacje. Możemy też budzić pewne skojarzenia, budując pierwsze wrażenie np. Biedroneczka_w_kropeczki, Wesoły_Romek, Deszczowy Leon.

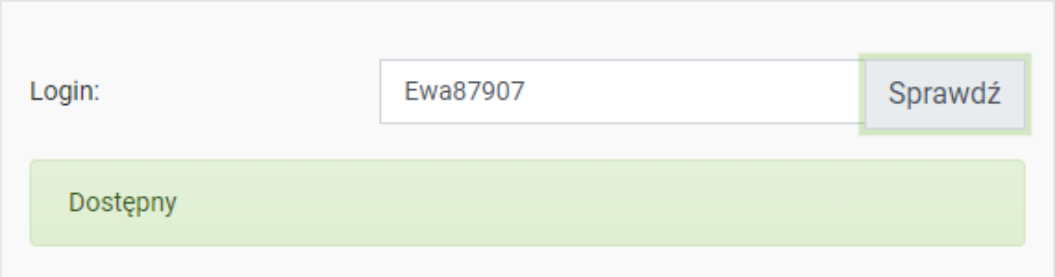
Po prostu – imię?

A jeśli po prostu chcesz użyć swojego imienia? To wydaje się być najprostszym rozwiązaniem. Niestety, zbyt wiele osób chciałoby tak zrobić. Wpisujesz imię i okazuje się, że ten nick już zajęty….

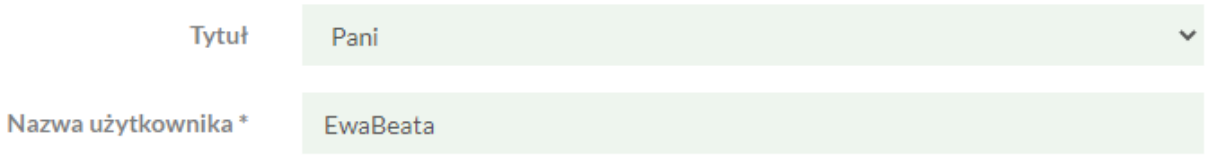




Pierwszym odruchem bywa wpisanie liczby – aktualnego roku, daty urodzenia lub dowolnego ciągu cyfr z klawiatury. Dlatego właśnie jest tak dużo nicków o strukturze: Basia1968.



Inne rozwiązanie, gdy Twoje zestawienie zostało już wykorzystane, to dodać drugie imię. Może to być imię własne lub ulubione. Wzrasta szansa, że zestaw jest niepowtarzalny i, co ważniejsze, że nikt go jeszcze nie użył na tej platformie.



Możesz też połączyć dwa słowa, jak w przykładach przywoływanych powyżej:

Wesoły_Romek lub w innym zapisie: WesolyRomek

Zielona-Ewa lub ZielonaEwa

Zuza.Warszawa

Pomocne może być podwojenie którejś z liter albo zastąpienie jej innym, podobnym znakiem:

Zuzaanka

P@wel

Samych dobrych wyborów NICKÓW!

Sklep, który nigdy nie istniał. Jak rozpoznać fałszywe sklepy?

Czarny piątek, cyfrowy poniedziałek, czy święta Bożego Narodzenia często powodują u nas zakupowy zawrót głowy. Budzi się w nas łowca, który przeszukuje strony internetowe, aby znaleźć jak najlepsze promocje. Niestety, niektóre sklepy istnieją tylko na kartach naszych przeglądarek.

W czasach pandemii kupujemy coraz więcej przez Internet. Dlatego liczba oszustw internetowych także wzrosła. Jak ustrzec się przed oszustwem? Co powinno wzbudzić nasze

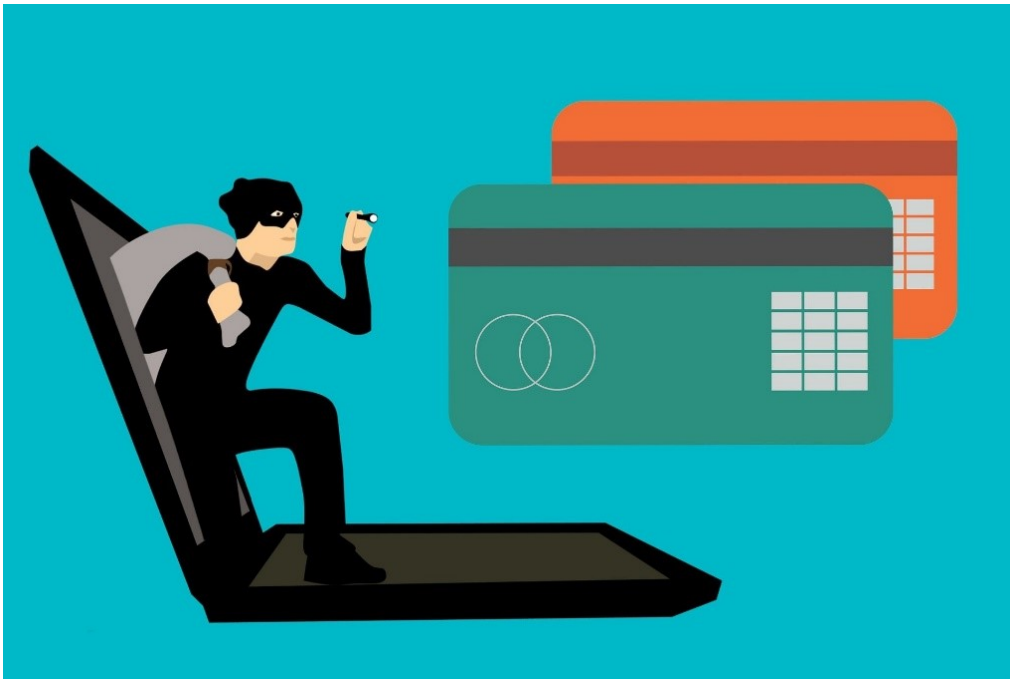
podejrzenia?

Zakupy przez Internet w bardzo szybkim tempie stały się dla wielu z nas czymś codziennym. Kupujemy już nie tylko wyszukane przedmioty, które trudno znaleźć w sklepie stacjonarnym. Przez Internet zamawiamy także ubrania, kosmetyki czy jedzenie. Nie trzeba wychodzić z domu i tracić czasu na dojazdy, szukać miejsca do parkowania i dźwigać zakupów.

Jak w tym gąszczu kolorowych stron, pełnych reklam i promocji rozpoznać fałszywe sklepy Internetowe?

Oto kilka niepokojących kwestii, które powinny zwrócić naszą uwagę:

- brak regulaminu sklepu
- brak adresu sklepu
- brak numeru telefonu – często do kontaktu służy tylko jeden adres mailowy
- bardzo długi czas oczekiwania na dostawę
- bardzo droga przesyłka
- brak możliwości wystawienia opinii i oceny produktu na stronie sklepu
- błędy językowe na stronie. Oznacza to, że treści na język polski tłumaczył program komputerowy, a człowiek
- promocja na cały asortyment przedstawiony na stronie, trwająca pomimo informacji, że kończy się za dzień lub kilka godzin
- nazwa strony sklepu nie jest adekwatna do asortymentu sklepu



Fałszywe sklepy na pierwszy rzut oka wyglądają normalnie. Zdjęcia produktów mogą być starannie dopracowane w programach graficznych, ale takie zabiegi często wykonuje się także w prawdziwych sklepach. Niestety, czas pandemii uśpił nieco naszą czujność i coraz więcej osób pada ofiarą internetowych oszustw.

A jeśli zauważymy kilka z wymienionych powyżej cech sklepu internetowego?

Aby jeszcze się upewnić, czy sklep na pewno istnieje, możemy:

- wpisać w wyszukiwarce nazwę sklepu i dopisać hasło *opinie* – na pewno znajdziesz opinię na temat danego sklepu
- jeśli jesteśmy użytkownikiem jakiegoś forum, możemy zapytać znajomych, czy słyszeli o takim sklepie i czy z niego korzystali
- wejść na stronę –

https://www.legalniewsieci.pl/aktualnosci/podejrzane-sklepy-internetowe

Na stronie znajdziemy aktualizowany spis fałszywych sklepów. Zachęcamy do zajrzenia, aby przekonać się jak taki fałszywy sklep wygląda!

Gdy sklep, w którym chcemy zarobić zakupy ma bardzo negatywne opinie lub widnieje na liście fałszywych sklepów, nic tam nie kupujmy! Nie wiadomo, czy otrzymamy nasz zakup, czy przyjdzie do nas w dobrym stanie. A na pewno trudno będzie otrzymać zwrot pieniędzy czy zareklamować i oddać produkt!

Bądźmy czujni i kupujmy tylko w znanych wam sklepach!

Więcej na temat rozpoznawania fałszywych sklepów możecie przeczytać tutaj:

https://business.trustedshops.pl/blog/jak-rozpoznac-falszywy-sklep-internetowy/

lub

https://www.legalniewsieci.pl/aktualnosci/falszywe-sklepy-internetowe-plaga-naszych-czasow

Mój bezpieczny smartfon cz. 1

Smartfon, który mamy codziennie przy sobie, to nie tylko telefon i internetowe okno na świat, z którego łatwo korzystamy w każdym miejscu i o każdym czasie. Choć dla nas to jest poręczne narzędzie, dla innych to źródło wiedzy o nas. Smartfon może zawierać poufne informacje, dlatego bardzo ważne jest, aby dobrze go zabezpieczyć. Podstawą bezpieczeństwa naszego smartfona jest blokada ekranu głównego. Dlaczego?

Wyobraź sobie sytuację, gdy przypadkiem odłożysz Twój smartfon i znajdzie się w niepowołanych rękach. Do jakich danych zyskałby dostęp? Ktoś może mieć dostęp do zdjęć, mediów społecznościowych, danych logowania do banku, a może jeszcze inne informacje? Jeśli zabezpieczysz smartfon i zostanie skradziony, prawdopodobnie nie odzyskasz już swojego urządzenia, jednak zwiększysz szansę, że złodziej nie dostanie się do Twoich danych.

Jest kilka metod odblokowywania smartfona. Którą z nich wybrać i jak zabezpieczyć smartfon przed obcymi? Metody ochrony mają swoje mocne, ale i słabe strony. Zróbmy przegląd.

Zablokuj dostęp do swojego smartfona

PIN i wzór na ekranie

Większość smartfonów umożliwia blokowanie ekranu przy pomocy PIN-u, czyli kilkucyfrowego hasła, oraz wzoru rysowanego palcem na ekranie. Do dzisiaj te metody blokowania są najbardziej cenione. Jednak – nie należy wybierać najprostszego PIN-u, ani najprostszego wzoru. W praktyce włamanie się do smartfona zajmuje wtedy nie więcej niż 90 sekund.

Rozpoznawanie twarzy

Jest to kolejna metoda odblokowywania telefonu, która jednak może zawodzić np. w słabym oświetleniu. Wybierając rozpoznawanie twarzy, należy mieć jeszcze ustawiony drugi sposób odblokowania. Czy ta metoda jest bezpieczna? Okazuje się, że nie do końca. Sprawdzono w testach, że czy tego typu blokadę można złamać przy pomocy zdjęcia właściciela telefonu. Wystarczy w miarę dobre zdjęcie, aby bez kłopotu dostać się do informacji w smartfonie.

Tęczówka i linie papilarne

Popularne stało się odblokowywanie smartfona przy pomocy czytnika linii papilarnych lub skanera tęczówki. Zarówno odcisk palca jak i tęczówka są niepowtarzalne. Wydaje się, że taki sposób blokowania smartfona daje 100% skuteczności, niestety, rzeczywistość wygląda inaczej. Podobnie jak przy rozpoznawaniu twarzy, zaawansowany złodziej poradzi sobie przy wykorzystaniu zdjęć właściciela sprzętu.

Mój bezpieczny smartfon cz.2

W tekście Mój bezpieczny smartfon cz. 1 dokonaliśmy przeglądu blokad smartfonu, aby nikt niepowołany nie miał dostępu do naszego urządzenia. Jednak bezpieczeństwo naszego smartfona polega też na zabezpieczeniu danych, które na nim przechowujemy. Podobnie, jak w przypadku komputera osobistego, smartfon należy uzbroić w odpowiednie oprogramowanie.

Bezpieczne źródła

Pamiętajmy, aby wszystkie aplikacje instalować z odpowiedniego źródła – czyli internetowego, sprawdzonego sklepu: Google Play lub App Store.

Antywirus

Za pośrednictwem smartfonów mamy dostęp do Internetu, przez co możemy niechcący podłączyć się do innego zainfekowanego urządzenia. Złośliwym, szpiegującym programom oraz szkodliwym wirusom możemy przeciwdziałać, instalując na naszym smartfonie jeden z programów antywirusowych. Warto postawić na prosty, ale bezpieczny program, który zabezpieczy telefon. Zaufane antywirusy znajdziemy w sklepie Google Play lub App Store. Regularne skanowanie telefonu pomoże wykryć złośliwe linki w Internecie, niebezpieczne aplikacje, czy podejrzane sieci Wi-Fi.

Na swoim smartfonie możesz zainstalować program antywirusowy.

Wylogowywanie

Bezpieczeństwo smartfona w dużej mierze zależy od każdorazowego wylogowywania się z wszelkich aplikacji. Wielu użytkowników często o tym zapomina, a jest to skuteczne zabezpieczenie telefonu przed kradzieżą osobistych danych. Nawyk wylogowywania może być szczególnie przydatny w zatłoczonych miejscach, kiedy nasz telefon może być narażony na kradzież.

Kopie zapasowe

Aby zabezpieczyć się przed utratą danych warto wykonywać tzw. backupy danych i dotyczy to zarówno plików multimedialnych, jak i maili, kontaktów, ustawień telefonu, czy zakładek wyszukiwarki. Ustawienia kopii zapasowych znajdują się w ustawieniach smartfona. Jeśli co jakiś czas zrobimy kopię, będziemy zabezpieczeni np. podczas awarii telefonu. Kopię zapasową można odesłać na swojego maila lub umieścić w chmurze, co pozwoli na skuteczny powrót do zapisanych informacji.

Przechowywanie danych w chmurze i na dyskach zewnętrznych

W smartfonie możemy przechowywać dane, na których nam zależy – dokumenty, zdjęcia z wakacji. Powinniśmy przechowywać je albo na zewnętrznym dysku lub na dysku wirtualnym. Zewnętrzne nośniki przydają się także na wypadek awarii telefonu.

Zabezpieczam swój komputer: Firewall

Firewall lub Zapora to program, który pozwala zabezpieczyć nasze komputery i serwery przed atakami. W zasadzie zapory

zatrzymują intruzów lub hakerów przed włamywaniem do naszego komputera z zewnątrz. Drugą funkcją jest powstrzymywanie szkodliwego oprogramowania przed wysyłaniem ważnych informacji na zewnątrz. Firewall pozwala określić, które z elementów sieci internetowej są godne zaufania i odpowiednio filtrować dostęp do sieci lokalnej. Dlaczego firewall jest koniecznością i jak odpowiednio z niego korzystać?

Jeżeli Twój komputer jest podłączony do Internetu, zawsze będzie próbował komunikować się z innymi komputerami. Odbywa się to za pośrednictwem “otworów” w sieci, zwanych portami. Istotą działania firewalla jest zamykanie portów, z których użytkownik nie korzysta oraz sprawdzanie transmisji danych przez pozostałe. Bez zapory, ułatwiasz hakerom włamanie do Twojego komputera i utracenie osobistych danych.

Firewall to obrona przed internetowym włamaniem do naszego komputera

Istnieją dwa typy zapór: sprzętowa i programowa. Firewall sprzętowy znajdują się zazwyczaj na bramce internetowej, która jest eleganckim określeniem dla urządzeń sieciowych takich jak np. modem lub router. W domu częściej korzystamy z programów pełniących funkcję firewalla. Zapory te znajdują się na komputerze w warstwie sieciowej i sprawdzają komunikację pomiędzy maszyną a światem zewnętrznym, blokując każdą nieautoryzowaną transmisję. Stały się one bardzo popularne wśród użytkowników domowych ze względu na łatwość instalacji oraz zarządzania.

Dlaczego warto posiadać ochronę zapory? Firewall zapobiega włamaniom i kradzieży danych, co jest dosyć istotne w czasach, gdy każdy z nas korzysta ze sklepów internetowych oraz bankowości online. Przecież nikt z nas nie chce, aby jakiś haker przechwycił nasze informacje finansowe!

Pamiętaj jednak, że zapora nie chroni przed wirusami! Zapewnia bezpieczeństwo przed innym, równie groźnym typem ataku – bezpośrednim włamaniem do komputera. Tym bardziej warto o niej pomyśleć, a z pomocą programu antywirusowego tworzymy

kompleksową ochronę naszego komputera podczas używania Internetu.

Zabezpieczam swój komputer: Antywirus

Jednym z zagrożeń związanych z przeglądaniem Internetu są wirusy komputerowe. Mogą one wyrządzić duże szkody nieświadomym internautom. Z tego powodu każdy świadomy użytkownik komputera powinien wiedzieć, czym jest program antywirusowy i w jaki sposób działa.

Najpierw odpowiedzmy na pytanie: **czym są wirusy?**

Zwykle nazywa się w ten sposób wszystkie rodzaje szkodliwych programów, które mogą zostać zainstalowane na komputerze. Szkody mogą polegać np. na tym, że tracimy kontrolę nad urządzeniem, usunięte zostają dane na twardym dysku lub ktoś kradnie informacje o nas.

Ochronę przed takimi programami zapewniają antywirusy.

Jak działają?

Ich sposób funkcjonowania przypomina ochronę organizmu przed zarazkami. Programy mają zapisane identyfikatory szkodliwego oprogramowania i niszczą je po rozpoznaniu wśród innych programów zainstalowanych na komputerze. Antywirus pobiera potrzebne informacje i na bieżąco, nawet codziennie, aktualizuje swoją bazę danych, aby móc rozpoznawać najnowsze zagrożenia. Posiadając aktualną bazę danych, skanuje znajdujące się na dysku pliki w poszukiwaniu tych szkodliwych. Po ich znalezieniu wyświetla komunikat na ekranie komputera o wykryciu zagrożenia. Następnie albo sam podejmuje decyzję o usunięciu zainfekowanych plików lub zostawia tę decyzję użytkownikowi.

Pamiętaj, aby Twój antywirus regularnie aktualizował swoje dane.

Zainstaluj oprogramowanie antywirusowe dla bezpieczeństwa Twojego komputera, pamiętając o kilku zasadach:

1. Instaluj oprogramowanie antywirusowe tylko z zaufanych

źródeł. Przestępcy często starają się zainfekować Twój komputer poprzez dystrybuowanie darmowych kopii fałszywych programów antywirusowych.

2. Pilnuj, aby Twoja wersja antywirusa była najnowsza oraz aby baza wirusów i sam program antywirusowy aktualizowały się automatycznie.

3. Upewnij się, że Twój antywirus automatycznie skanuje każdy pendrive i dysk przenośny podłączany do komputera oraz, że masz włączoną ochronę komputera w czasie rzeczywistym.

4. Zwracaj uwagę na powiadomienia, jakie antywirus wyświetla Ci na ekranie. 5. Nie wyłączaj ani nie usuwaj oprogramowania antywirusowego. Może czasem spowalniać Twój komputer, blokować instalację jakiejś aplikacji lub dostęp do strony internetowej. Ale wyłączenie antywirusa może narazić Cię na niepotrzebne ryzyko i dotkliwe straty.

Wśród znajomych i przyjaciół,

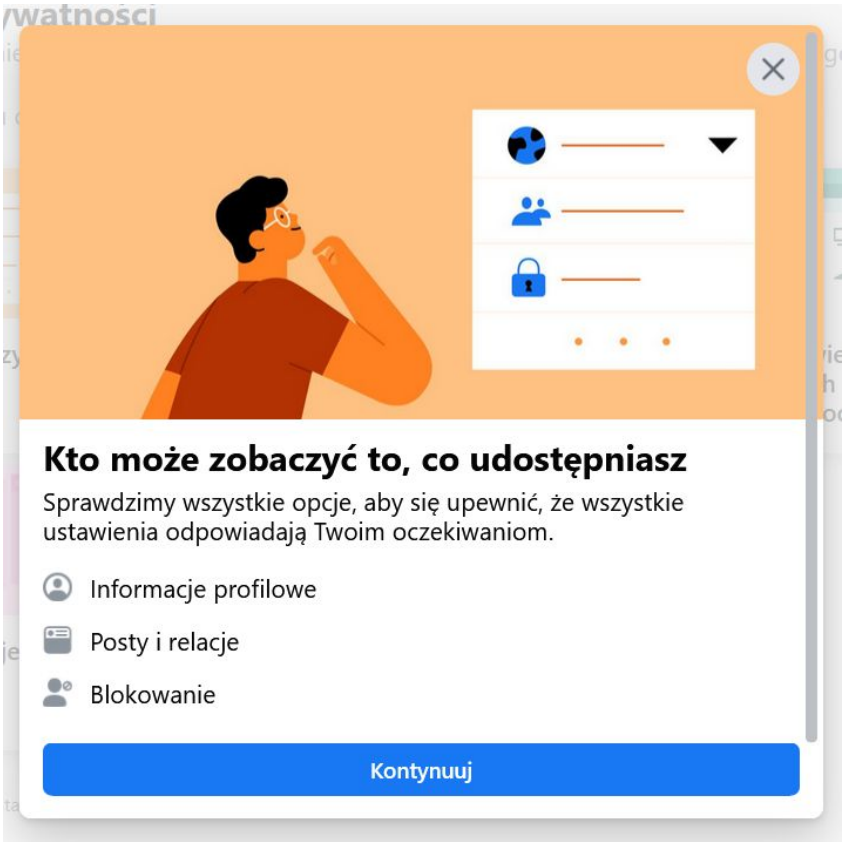
dbając o prywatność

Codziennie Facebooka odwiedza ponad 7 milionów Polaków. Serwis jest najpopularniejszym miejscem spotkań ze znajomymi oraz lubianym źródłem informacji. Nie umiemy sobie wyobrazić ilości danych, które Facebook przechowuje, jest ich zbyt dużo. Mamy jednak kontrolę nad wiadomościami, które publikujemy i przekazujemy dalej. Przedstawimy najważniejsze zasady, o których warto pamiętać.

Najważniejsza osoba na Facebooku

Najważniejszą osobą na Facebooku jesteś **Ty**. To Ty: piszesz posty i komentarze, wklejasz zdjęcia, lubisz strony i

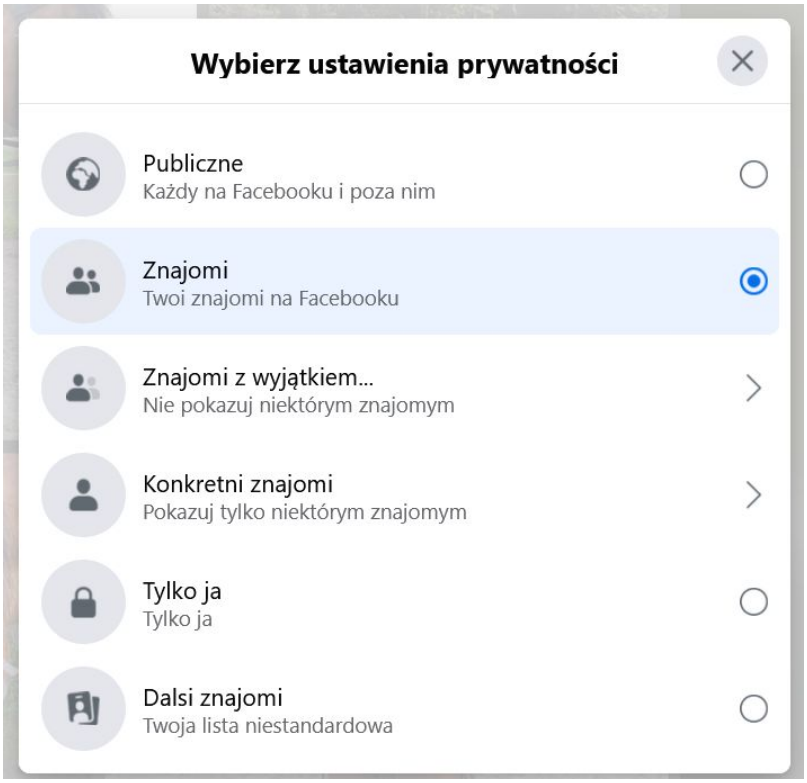
wydarzenia. To oznacza, że Ty decydujesz, jakie treści udostępniasz. Domyślnie twoje wpisy są widoczne dla znajomych, których wybierasz. Czy ktoś jeszcze może je zobaczyć? Tak, możesz określić do nich dostęp: zobaczą je konkretne osoby, znajomi twoich znajomych, wszyscy lub w opcji „publiczne” – nawet osoby, które się nie logują. Opcje „Ustawienia i prywatność” znajdziesz w prawym górnym rogu strony swojego Facebooka. Przewodnik po opcjach wszystko Ci pokaże, zalecamy, aby twoje posty i relacje oglądali twoi znajomi.



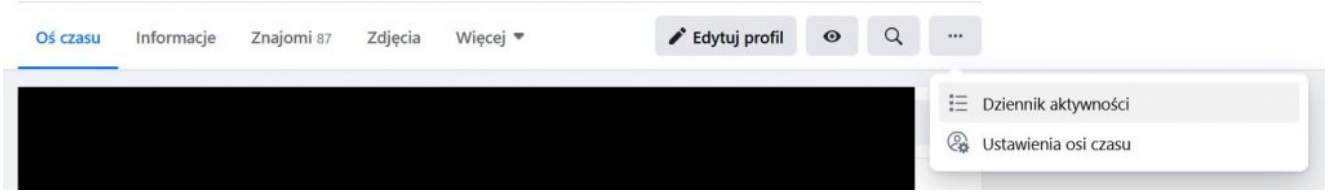
Kto widzi wpisy?

Jeśli chcesz, możesz zmienić ustawienie postu lub zdjęcia

później. Po publikacji możesz decydować, dla kogo te informacje będą dostępne. Możesz też ograniczyć widoczność swoich starszych postów lub nawet je usunąć. Przykład opcji pokazywania postów przedstawia menu poniżej:



Facebook przechowuje każdą Twoją aktywność. Twoje komentarze, kliknięcie „Lubię to”, obejrzenie filmu, zagranie w grę czy zapytanie w wyszukiwarce – wszystkie te rzeczy znajdziesz w dzienniku aktywności, który znajdziesz po prawej stronie głównego panelu serwisu.



Możesz sprawdzić w dzienniku historię twoich postów, zdjęć, odsłuchanych utworów lub obejrzanych filmów. Takich kategorii

jest kilkanaście. Zalecamy – usuwaj od czasu do czasu pojedyncze elementy swojej historii lub listy w całości, aby utrzymać porządek.

Na koniec ważna wskazówka na temat bezpieczeństwa:

Pamiętaj, wyloguj się, gdy już nie przeglądasz Facebooka!

Więcej informacji

Jeśli chcesz dowiedzieć się więcej o Facebooku, zajrzyj na strony:

Szczegółowy poradnik dotyczący ustawień prywatności na Facebooku:

https://trybawaryjny.pl/facebook-prywatnosc-poradnik/

Jakimi danymi i w jaki sposób zarządza Facebook – artykuł na stronie Fundacji Panoptykon, zajmującej kwestiami naszej prywatności:

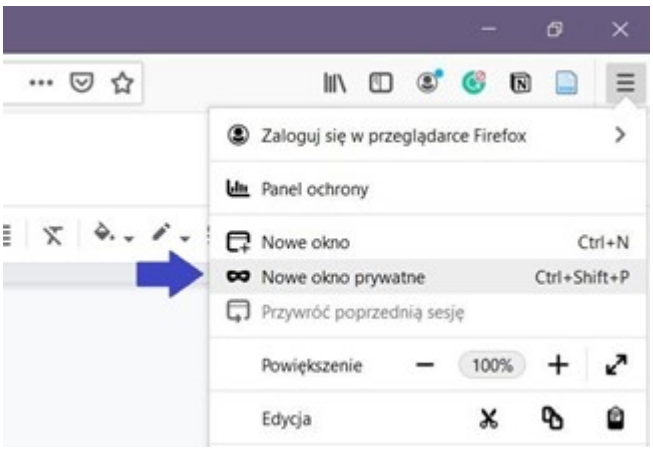
https://panoptykon.org/wiadomosc/odzyskaj-kontrole-w-sieci-odcinek-iii-ustawienia-prywatnosci-na-facebooku

---

Czy naprawdę potrzebuję trybu incognito?

Wszystkie popularne przeglądarki oferują nam wyświetlanie stron internetowych w trybie prywatnym. Czasem ten tryb nazywa się *incognito*.

Przykładowo, w programie Firefox okno prywatne można włączyć, korzystając z menu po prawej stronie przeglądarki:



Słownik języka polskiego pod hasłem *Incognito* wyjaśnia: robimy coś incognito, kiedy ukrywamy swoją tożsamość. Czy to oznacza, że możemy przeglądać Internet anonimowo? I nikt nie może śledzić naszych działań? Niestety, nie. Tryb prywatny polega na tym, że nasza przeglądarka nie przechowuje historii

wyszukiwania i przeglądania stron. Gdy zamykamy program, wyczyszczona zostaje pamięć podręczna oraz “ciasteczka”. “Ciasteczka” (ang. cookies) to są niewielkie informacje zapisywane przez serwisy na komputerach użytkowników, dzięki którym sprawniej działa komunikacja internetowa. Więcej informacji o “ciasteczkach” znajdziesz w naszym kolejnym materiale. Pobrane pliki oraz zapisane zakładki jednak zostają.

Skoro w trybie prywatnym nie zacieramy za sobą śladów, czy warto z niego korzystać? Jak najbardziej! Ma to kilka zalet:

1. Jeśli dzielimy się komputerem z innymi, nasze działania nie będą widoczne dla innych użytkowników tego samego komputera.
2. Jeśli korzystamy z komputera w miejscu publicznym, nie zostawiamy żadnych informacji w obcym miejscu.
3. Nasze wyszukiwanie np. w Google będzie przygotowane na nowo, “na czysto”. Nie będzie się opierać na wcześniejszych wynikach.

Na zakończenie – to prawda, że w trybie prywatnym nie jesteśmy anonimowi. Jednak dane o naszych działaniach w Internecie nie są przechowywane, przesyłane lub wykorzystywane po zakończeniu sesji. Dzięki trybowi prywatnemu W ten sposób reklamy i nasza historia przeglądanych stron nie są podstawą do pokazywania nam wyników wyszukiwania np. innego dnia.

Przydatny link:

Tryb incognito w sieci. Jak korzystać i co można zrobić?

Dzielę się świadomie pomysłami – publicznie czy prywatnie?

Lubisz oglądać piękne fotografie? Zapierające dech w piersiach pejzaże? A może robisz zdjęcia i umieszczasz je w Internecie, aby podzielić się nimi z Twoimi przyjaciółmi?

W takim razie musisz poznać Instagram – najpopularniejsze w roku 2020 medium społecznościowe na świecie!

Instagram to jest aplikacja oraz portal internetowy, które służą do umieszczania i udostępniania zdjęć. Jest on bezpłatnie dostępny we wszystkich rodzajach smartfonów.

Fotografie są kwadratowe – to jest charakterystyczna cecha serwisu.

Jak w innych mediach społecznościowych można i tutaj komentować wpisy, polubić posty lub podać je dalej. Ale funkcji jest niewiele do wyboru.

Czy warto w takim razie myśleć o bezpieczeństwie i ustawieniach prywatności?

Gdy rozważamy umieszczanie fotografii w Internecie, powinniśmy pomyśleć o:

- prawach autorskich do zdjęć;
- prawach do wykorzystania zdjęć zrobionych przez innych;
- prawach do wizerunku;
- kontroli nad dostępem do materiałów własnych;
- granicach poczucia prywatności.

W tym poradniku zajmujemy się tylko naszym **poczuciem prywatności.**

Możliwe w aplikacji opcje pozwalają nam też wybrać poziom dostępu innych do naszych postów.

Konto na Instagramie ma tylko 2 możliwe ustawienia:

- publiczne – domyślnie tak jest ustawione nowe konto; czyli każdy może oglądać Twoje zdjęcia
- prywatne – Twoje zdjęcia i relacje mogą zobaczyć tylko wybrane przez Ciebie osoby

Gdy prowadzisz **konto publiczne**, pamiętaj, aby nie umieszczać na Instagramie informacji prywatnych. Nie powinny się tam znaleźć zdjęcia Twojego domu z adresem, samochodu, ani dokumentów. Dbaj o to, aby osoby na Twoich zdjęciach, szczególnie dzieci, były przedstawione z szacunkiem. Dbaj też o prywatność innych. Jeśli ktoś z obserwujących Cię zachowuje się nieodpowiednio, możesz taką osobę zablokować.

Gdy prowadzisz **konto prywatne**, jest ono dostępne tylko dla tych, którym pozwolisz na obserwację. Zatwierdzasz każdą osobę pojedynczo. Zatwierdzanie próśb o obserwację jest jedną z lepszych metod zabezpieczenia Twojej prywatności.

Zatwierdzaj tylko prośby pochodzące od zaufanych i znajomych osób! Możesz też zablokować kontakty, których utrzymywanie

sprawia Ci przykrość.

Więcej informacji znajdziesz na: https://tinyurl.com/y2cq5n5v

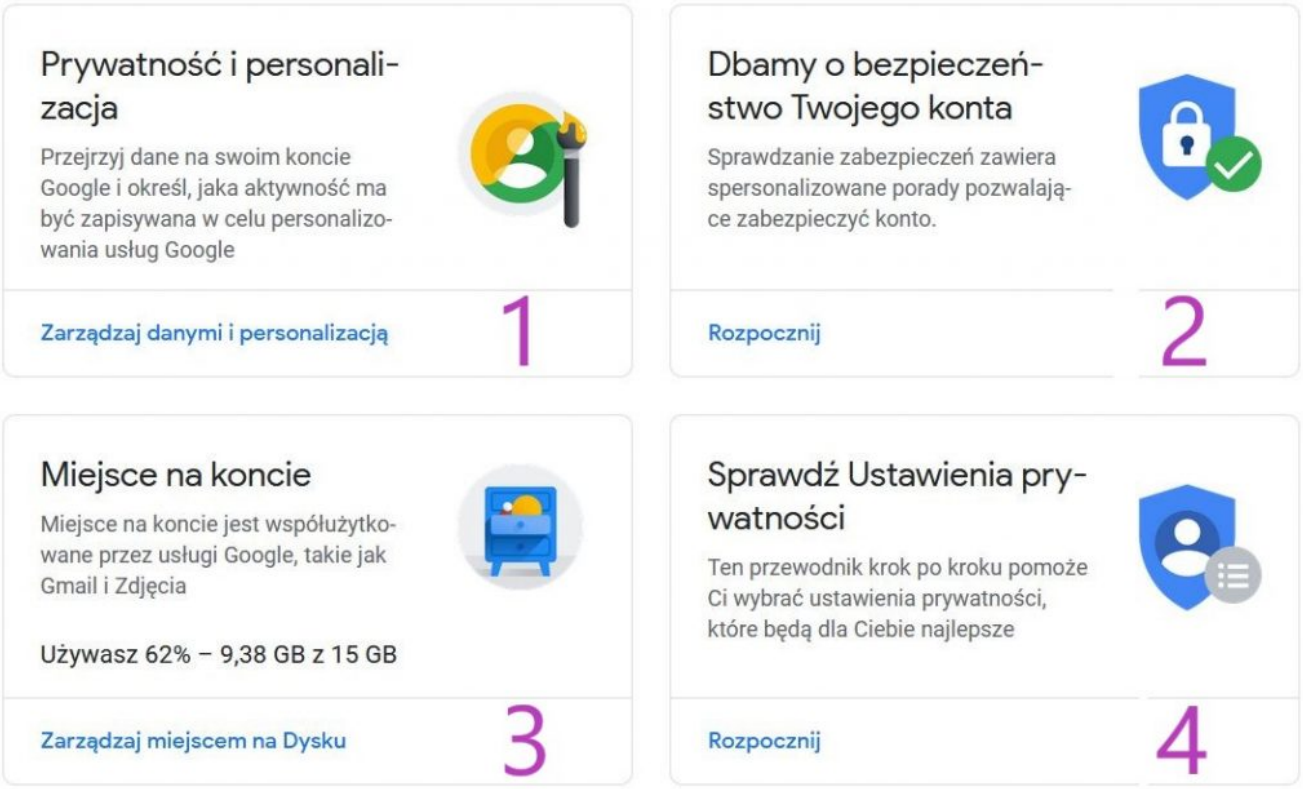
---

Moja bezpieczna poczta, dysk i zdjęcia

Najlepiej poznawać opcje programu, samodzielnie wybierając kolejne ustawienia wybranej przez nas usługi. Popularną pocztą elektroniczną w Polsce jest Gmail w usłudze Google. Zachęcamy do ustawienia swojego konta Google pod względem prywatności i bezpieczeństwa.

Co to znaczy? Będziemy decydować, które informacje o nas mogą być zbierane, udostępniane innym lub wykorzystywane w serwisie Google.

Kiedy wejdziesz do poczty, kliknij swoją ikonkę w prawym górnym rogu i naciśnij klawisz „Zarządzaj swoim kontem Google”. Będziesz wybierać ustawienia, korzystając z 4 przedstawionych poniżej paneli:



Panel 1 – „Prywatność i personalizacja”. To jest panel przedstawiający wszystkie funkcje związane z bezpieczeństwem Twojego konta. Możesz tutaj wybrać przewodnik „krok po kroku”, który będzie Ci wyświetlał kolejne ustawienia do decyzji. Poniżej znajdziesz skróty do funkcji i ustawień z pozostałych Paneli. Dalej są ustawienia ułatwiające korzystanie w konta, np. czytnik ekranu, który czyta dla Ciebie dokumenty Google.

Panel 2 – „Dbamy o bezpieczeństwo Twojego konta” oraz Panel 3 – „Miejsce na koncie” nie wymagają od nas decyzji związanych z bezpieczeństwem konta. Nie będziemy się tutaj nimi zajmować.

Panel 4 – „Sprawdź ustawienia prywatności”. Najpierw jest przewodnik, który przedstawia dostęp narzędzi Google do naszych danych. Przewodnik pokaże sugestie ustawień, wystarczy zaznaczyć zgodę lub brak zgody na nie. Oprócz tego panel składa się z 5 najważniejszych ustawień prywatności, do których radzimy wybór opcji:

- Ustawienia zarządzania aktywnością – Zastanów się, czy chcesz zbierać **historię aktywności w Internecie** oraz czy chcesz ją udostępniać wszystkim usługom Google, np. Google Maps? Zalecamy: wstrzymanie funkcji. Pomyśl następnie, czy przyda Ci się mapa miejsc odwiedzanych przez Ciebie? Jeśli nie potrzebujesz **historii lokalizacji** – zalecamy: wstrzymaj funkcję. Ostatnie pytanie o aktywność dotyczy Twojej **historii zapytań** i **obejrzanych filmów na YouTube**. Jeśli nie korzystasz stale z tego serwisu – zalecamy: wstrzymaj funkcję.
- Zarządzaj informacjami udostępnianymi w YouTube – Tu wybierasz, kto będzie widzieć Twoje filmy, playlisty i subskrypcje w YouTube. Zalecamy: zaznacz swoje playlisty oraz subskrypcje jako prywatne.
- Zarządzaj ustawieniami Zdjęć Google – Gdy udostępniasz zdjęcie, podając link, możesz usunąć informacje o lokalizacji. Raczej nie podawaj Twojego miejsca pobytu do publicznej wiadomości. Zalecamy: włącz funkcję usuwania danych.
- Decyduj, które informacje o Tobie mogą widzieć inni – W tym miejscu decydujesz, czy inni mogą zobaczyć Twój profil „O mnie”, np. nazwisko, zdjęcie, adres e-mail. To, co wpisujesz, jest widoczne dla innych. Jeśli nie podasz pewnych danych, nie będzie ich widać. Zalecamy: podaj tylko niezbędne informacje.
- Dostosuj reklamy do swoich zainteresowań – Chodzi tu o zbieranie przez Google informacji o tym, co lubisz i co kupujesz. Te dane mogą być przesyłane do innych firm i serwisów. Zalecamy: wyłącz tę funkcję.

Jeśli chcesz dowiedzieć się więcej o ustawieniach konta Google odwiedź strony:

https://antyweb.pl/google-nowe-ustawienia-prywatnosci-domyslne/

https://zaufanatrzeciastrona.pl/post/podstawy-bezpieczenstwa-jak-zadbac-o-swoja-prywatnosc-w-uslugach-google/

https://panoptykon.org/wiadomosc/odzyskaj-kontrole-w-sieci-odcinek-iv-google

---

Czy znasz swoją historię przeglądania Internetu?

Przeglądarka internetowa jest programem, którego zadaniem jest ułatwiać nam znalezienie informacji w Internecie. Najbardziej popularne obecnie przeglądarki to Chrome i Firefox w systemie Windows oraz Safari w systemie macOS. Zadaniem przeglądarek jest nie tylko wyświetlać strony, które podaje użytkownik. Programy te zazwyczaj zbierają też informacje o tym, co najczęściej ktoś ogląda lub czego szuka. Dlaczego? Ponieważ przeglądarki mają działać szybko – a najsprawniej podają informacje, które znalazły i podały już wcześniej.

Historia przeglądania to baza wiedzy o odwiedzanych przez nas w Internecie stronach.

Nasza historia przeglądania może nam się przydać. To jest biblioteka wszystkich adresów, które odwiedziliśmy. Można ją przeglądać, przeszukiwać oraz otwierać zapamiętane strony. Jeśli tego potrzebujesz, możesz również pogrupować wszystkie odwiedzone strony.

Wybierz, klikając, kolumnę z nazwami, etykietami, adresem URL lub datę ostatniej wizyty. Dostaniesz całą listę ułożoną według wybranej kolumny.

Możliwe jest również usunięcie wybranych stron internetowych z historii przeglądania lub wyczyszczenie całej historii przeglądania. W ustawieniach możesz też wybrać, czy chcesz mieć tę funkcję włączoną czy nie. Jeśli ją wyłączysz, przeglądarka nie będzie zbierać adresów odwiedzanych stron.

Poniżej znajdziesz opisy historii przeglądania przygotowane dla znanych przeglądarek:

- Firefox https://support.mozilla.org/pl/kb/historia-przegladania-w-firefoksie
- Chrome https://support.google.com/chrome/answer/95589?hl=pl&ref_topic=7438325
- Safari https://support.apple.com/pl-pl/guide/safari/ibrw1114/mac
- Internet Explorer https://support.microsoft.com/pl-pl/help/17438/windows-internet-explorer-view-delete-browsing-history

---

Jeśli chcesz wiedzieć więcej:

tu znajdziesz opisy mniej znanych funkcji przeglądarek, szczególnie pod kątem prywatności –

https://www.komputerswiat.pl/poradniki/programy/najlepsze-przegladarki-internetowe-na-2020-rok/we52sp8

ranking przeglądarek w Polsce i na świecie –

https://www.artefakt.pl/blog/seo/ranking-przegladarek-internetowych-polsce-swiecie-2020

Jak skonstruować hasło?

Hasła są jednym z podstawowych sposobów, w jaki możemy zabezpieczyć nasze dane w internecie. Potrzebujemy ustalić hasło do naszej poczty, do Facebooka lub Instagrama. Dobre hasło przyda się do portali, na których robimy zakupy.

Pamiętaj, każde miejsce, które odwiedzasz w internecie, wymaga innego, indywidualnego hasła!

Używanie silnych haseł jest niezbędne, abyśmy chronili nasze dane takie, jak imię i nazwisko, numer konta bankowego lub adres zamieszkania.

Przedstawiamy kilka porad dotyczących tworzenia silnego hasła:

- **długość hasła** – jeśli serwis nie wymaga hasła o określonej długości, wybierz hasło, które ma co najmniej 8 znaków
- **litery i znaki w haśle** – hasło powinno zawierać co

najmniej: jedną małą literę, jedną wielką literę, jedną cyfrę oraz jeden znak specjalny (np. &)
- **powiedzenie, zdanie** – możesz wybrać zdanie lub cytat, który przekształcisz na hasło; użyj nie tylko liter – ale i cyfr oraz znaków specjalnych, np. “Ala ma kota” można przerobić na 4lam@k07A

Skorzystaj z propozycji reguł zamiany, aby tworzyć bezpieczne hasła. Zawsze możesz też zastosować własne zasady:

- zamień a na @ lub 4 lub A
- zamień s na $
- zamień e na E lub 3
- zamień małe o na 0 [zero]
- zamień b na B lub 8
- zamień i na !

Np. Ela lubi tulipany można zamienić na 3lALu8!tul!P4n7.

Podczas tworzenia hasła zastosuj poniższe reguły:

1. Hasło nie może być takie samo jak nazwa użytkownika lub część tej nazwy.
2. Hasło nie powinno być imieniem nikogo z naszych bliskich lub zwierząt, np. cioci lub psa.
3. Hasło nie może zawierać danych osobowych Twoich ani Twojej rodziny. Przykładowo takimi danymi są: data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy itp.
4. Nie używaj sekwencji kolejnych liter, liczb lub innych znaków, np. abcd, XYZ.

5. Nie używaj pojedynczego wyrazu dowolnego języka pisanego normalnie lub wspak, ani tego wyrazu poprzedzonego lub/i zakończonego znakiem specjalnym lub cyfrą, np. szprotka7.
6. Nie używaj więcej niż 3 kolejnych znaków na klawiaturze, np. QWERTY, 1234.
7. Nie używaj oczywistych wyrażeń, takich jak *wpuscmnie*, *tojesthaslo*, *password*.

Jeszcze jedna porada na koniec:

Najważniejsze hasła zmieniaj co rok. Niech Twoje dane będą bezpieczne!

Jak sprawdzić wiarygodność informacji w internecie?

W internecie znajdziesz wiele informacji na każdy temat. Wiadomości, porady, dane, grafiki powstają w bardzo szybkim tempie i często nie wiesz, które z nich są prawdziwe i wiarygodne, a które wprowadzają w błąd. Ponadto w internecie, szczególnie w social mediach (to znaczy mediach społecznościowych np. Facebook, Twitter, Youtube) bardzo wiele osób dzieli się swoimi opiniami, osobistymi komentarzami, a nie faktami. Dlatego warto nauczyć się odróżniać jedne od drugich i wiedzieć, jak sprawdzić wiarygodność informacji w Internecie.

Z pojęciem wiarygodności informacji jest powiązane również pojęcie “fake news”, czyli “nieprawdziwa/fałszywa informacja”, które czasami jest umieszczana w Internecie specjalnie, aby wzbudzić sensację lub zamieszanie.

10 praktycznych porad, jak odróżnić informację wiarygodną od niewiarygodnej

1. Pamiętaj: opinie to nie fakty!

Czym różni się opinia od faktu?

Faktem jest coś, co miało miejsce lub jesteśmy pewni, że istniało, czyli możemy to potwierdzić za pomocą dowodów. Dowody te mogą być mierzone, obserwowane i sprawdzane. I niezależnie, kto będzie ich autorem wynik będzie taki sam.
Opinia to osobisty pogląd na dany temat, zależny od danej osoby, który może, ale nie musi być poparty faktami lub wiedzą. Opinii może być wiele na temat jednego faktu. Opinie bywają emocjonalne.

W komentarzach np. w mediach społecznościowych (Facebook, Instagram, Youtube, Twitter, Nasza Klasa) i blogach znajdziesz przede wszystkim opinie, osobiste historie, a nie fakty. Opinia jest bardzo indywidualna i może różnić się w zależności od poglądów i emocji autora/autorki danego wpisu. Na temat jednego wydarzenia można znaleźć bardzo wiele opinii. Dlatego zawsze sprawdzaj fakty, czyli: daty, miejsca, liczby, nazwiska, opisy sytuacji tak jak w eksperymencie fizycznym.

2. Zawsze szukaj autora informacji

Jeżeli wpis, notatka, zdjęcie w internecie nie ma podanego autora (autorem może być człowiek, ale autorem może być też grupa osób lub organizacja np. Fundacja Zaczyn) to nie jest to wiarygodna informacja. Wiarygodne informacje mają podanego autora lub możesz o niego zapytać. Nawet w przypadku artykułów, które oznaczone są jako „naukowe" należy sprawdzić, kto jest autorem danej treści. A także sprawdzić, czy taka osoba istnieje, czym się zajmuje, czy zna się na temacie, o którym pisze. Szukaj publikacji, których autorami są osoby doświadczone lub eksperci w danej dziedzinie, osoby, których tożsamość można potwierdzić.

3. Pytaj o źródła danych

Jeżeli na stronie internetowej podana jest informacja, że "20% osób w Polsce lubi zielony kolor", to wiarygodna i rzetelna strona internetowa poda informację skąd pochodzi taka wartość, np. przy wynikach badania pojawi się adnotacja "Główny Urząd Statystyczny, 2020 badanie: Jakie kolory lubią Polacy". Po wejściu na stronę urzędu znajdziesz to badanie i potwierdzisz jego wiarygodność. Miejscami godnymi zaufania są strony urzędów, instytucji, dużych i znanych firm, dużych organizacji pozarządowych, autorytetów w danej dziedzinie, naukowców.

4. Nie opieraj się na jednym źródle danych

Jeżeli jakaś informacja budzi Twoją wątpliwość poszukaj w internecie jeszcze kilku miejsc, które piszą na ten sam temat. Sprawdź, czy dane się zgadzają? Czy wypowiedzi są takie same? Poszukaj również internetowej encyklopedii. Jeżeli nadal nie

jesteś pewny rzetelności informacji – napisz do publicznej instytucji, która zajmuje się danym tematem i zapytaj, czy to, co znalazłeś zgadza się z ich wiedzą.

5. Sprawdź czy informacja jest oficjalna

Ważne dane sprawdź w danej instytucji – skontaktuj się na przykład przez oficjalną infolinię, np. w sprawie szczepień zadzwoń na infolinię NFZ, w sprawie emerytury zadzwoń na infolinię ZUS.

6. Bądź uważny na to, jak wygląda strona internetowa

Sprawdź jak wygląda strona internetowa, na której jest umieszczona informacja. Co to znaczy? Sprawdź czy strona jest aktualizowana (na przykład kiedy został umieszczony ostatni wpis – rok temu, a może dwa, a może nie ma podanej daty), czy jest zrobiona profesjonalnie. Czy linki (odsyłacze do innych stron) działają, czy grafika jest czytelna, czy grafiki i zdjęcia nie są obraźliwie, czy tekst się nie rozsypuje, czy na stronie nie ma zbyt wiele reklam, czy treści napisane są w sposób logiczny.

7. Data powstania danego materiału

Sprawdź, kiedy powstała dana informacja i kiedy została opublikowana. Czasami dane w internecie są nieaktualne, bo zostały umieszczone dość dawno, albo po prostu materiały na które się powołują nie są już aktualne. To dość ważne, bo świat się zmienia i stan wiedzy się zmienia.

8. Nie wierz zbyt emocjonalnym wpisom

Jeżeli dany artykuł jest pełen emocji i ocen, najprawdopodobniej nie będzie opierał się na faktach. Większość zawartych w nim informacji nie będzie rzetelna. Jeżeli czujesz, że artykuł Cię do czegoś namawia, a autor pisze, co masz robić – najprawdopodobniej to poglądy a nie wiarygodna informacja.

9. Uważaj na reklamy, szczególnie te zbyt okazyjne

Reklamy są częścią życia społecznego. Na niektóre z nich należy szczególnie uważać. Jeżeli reklama oferuje nierealne efekty, to najprawdopodobniej jest oszustwem. Przykłady: dieta cud, czyli schudniesz 10 kg w miesiąc bez zmiany nawyków żywieniowych, możliwość szybkiego zarobku 10 000 zł w tydzień bez wychodzenia z domu, wygrałeś samochód, wystarczy, że wyślesz smsa, pozbędziesz się zmarszczek przy pomocy kremu za 500 zł. Takie informacje powinny wzbudzić naszą podejrzliwość!

Nie klikaj w takie oferty i nic nie wypełniaj, nie podawaj swoich danych. Niestety, takie reklamy opierają się na ludzkich marzeniach, dlatego są wyjątkowo okrutne.

10. Skorzystaj ze stron, które sprawdzają informacje

W związku z zalewem nieprawdziwych informacji w sieci powstało wiele stron i organizacji, które zajmują się sprawdzaniem ich wiarygodności. Takie działanie czasami nazywa się “fact-checking”, czyli “sprawdzanie faktów”. W Polsce mamy kilka

organizacji, które zajmują się tym tematem – jeżeli nie jesteś czegoś pewny. napisz do nich i zapytaj. Możesz też obserwować ich strony na bieżąco.

Stowarzyszenie Demagog – działa na rzecz poprawy jakości debaty publicznej w Polsce, tak aby bezstronna i wiarygodna informacja była podstawowym źródłem wiedzy obywateli.

https://demagog.org.pl/

Konkret24 – sprawdza informacje dziennikarskie

https://konkret24.tvn24.pl/

Na świecie strony sprawdzające wiarygodność informacji to: Crosscheck, Fake News Detector czy FactCheck. Niestety są po angielsku.

*

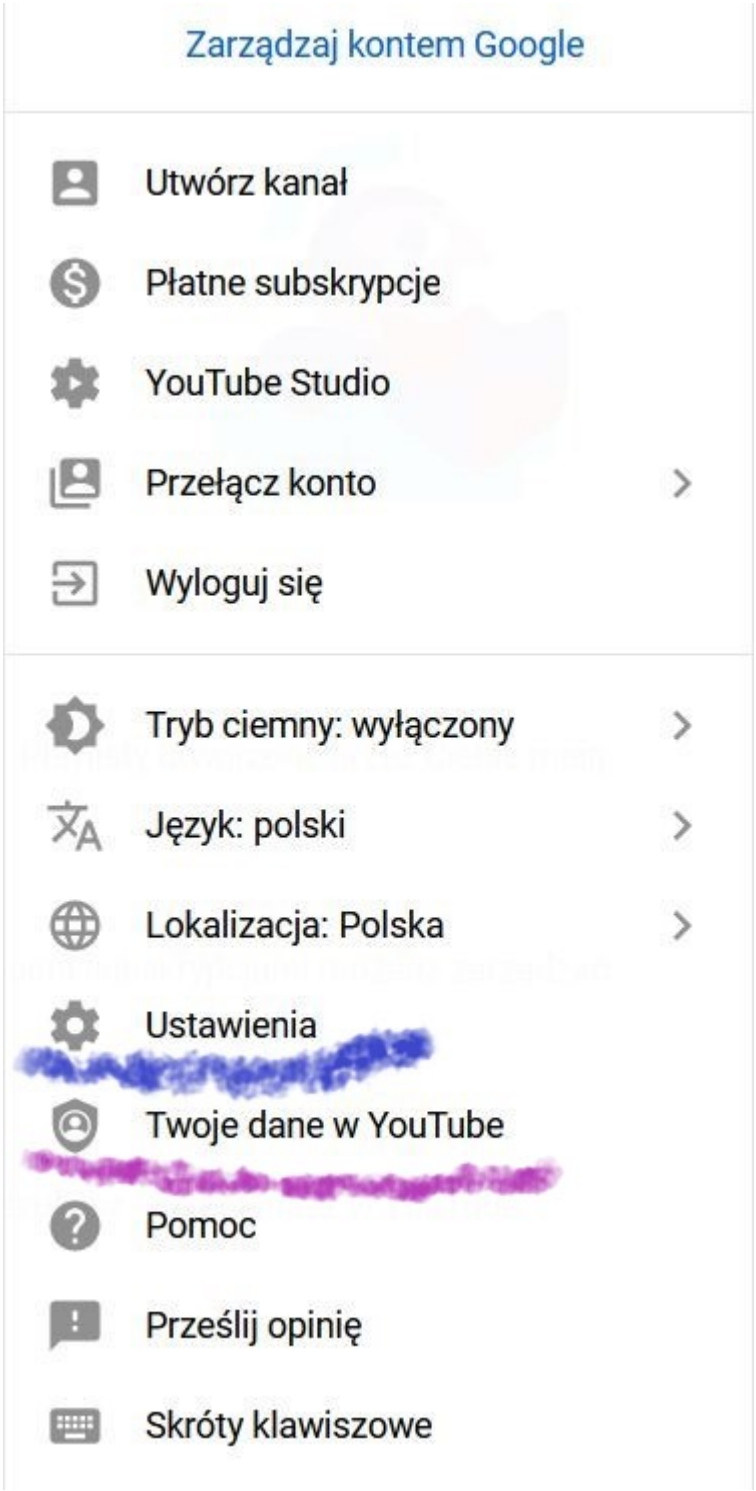
Korzystaj z Internetu. Nie bój się tego. Stosuj po prostu zasadę „ograniczonego zaufania" – tak jak w życiu. Nie wierz we wszystko, co przeczytasz! Nie bój się, że wszystko co czytasz jest nieprawdą. W internecie jest mnóstwo wspaniałych treści.

Bezpiecznie z YouTube’em czyli kilka słów o ustawieniach prywatności

YouTube jest wszechstronnym narzędziem. Dostarcza nie tylko rozrywki, ale też służy nam bogatym wyborem poradników, warsztatów i instrukcji w najlżejszej dla nas formie – poprzez film. Serwis YouTube jest częścią usług Google, na naszym koncie masz ustawione już podstawowe opcje prywatności i bezpieczeństwa.

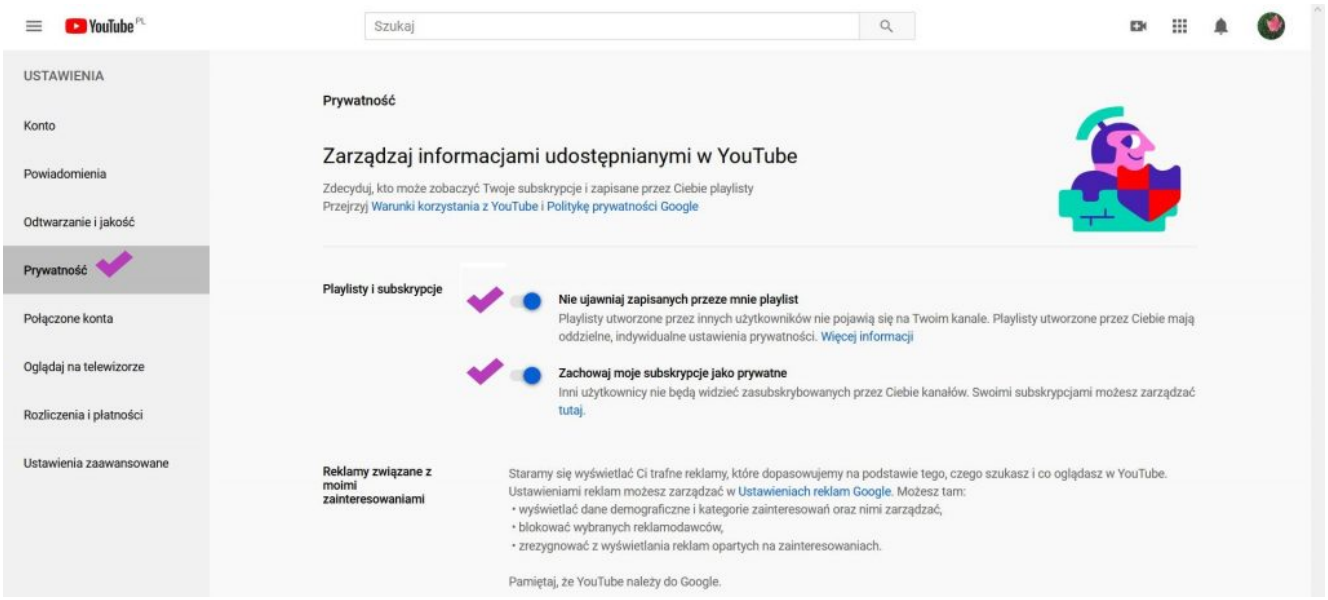
Opcje prywatności serwisu YouTube

Pozostaje sprawdzić dwa miejsca i zastanowić się nad opcjami związanymi wyłącznie z tym serwisem.



Menu programu jest dostępne w prawym górnym rogu, wystarczy nacisnąć swoją ikonkę i rozwija się lista funkcji. Najpierw wybierz Ustawienia i sprawdź, czy w zakładce Prywatność masz włączone opcje „Nie ujawniaj zapisanych przeze mnie playlist” oraz „Zachowaj moje subskrypcje jako prywatne”. Obie opcje chronią twoje wybory: to, co oglądasz, to Twoja prywatna sprawa. Nikt nie powinien zaglądać do Twojej listy utworów i

zapisanych wykonawców bez Twojej zgody.



Twoje dane w serwisie YouTube

Drugie miejsce, które warto odwiedzić, to Twoje dane w YouTube. Tę funkcję również wybierasz z głównego menu. Serwis przedstawia Ci 3 rodzaje danych o Tobie, które zbiera, podczas gdy korzystasz z usługi:

1. Jeśli śledzisz jakiś kanał (czyli masz subskrypcję) albo przesyłasz twoje filmy na YouTube, tutaj jest dostępna pełna lista treści, z których korzystasz. Możesz pobrać te dane na komputer.
2. W tym panelu decydujesz, czy YouTube ma przechowywać historię Twojej aktywności, to znaczy listę filmów,

które oglądasz i listę poszukiwań, gdy wpisujesz zapytania w serwisie. Warto wyczyścić te listy od czasu do czasu.

3. Możesz też sprawdzić, jakie są twoje ustawienia zarządzania danymi w koncie Google. Jeśli opcje wymagają zmian, można przejść do głównych ustawień Google i je poprawić.

Poniżej wymienionych opcji jest przygotowany przewodnik po ustawieniach prywatności. Jeśli temat Cię interesuje, dowiesz się z niego, co YouTube robi z Twoimi danymi i które z nich wykorzystuje w serwisie.

Więcej o korzystaniu z serwisu YouTube znajdziesz na stronie:

https://support.google.com/youtube/