F//TRUST
iWealth

DIT DIRECT IT

CYBERHIGIENA

Jak zadbać o bezpieczeństwo w sieci?

W dobie cyfryzacji większość naszej codziennej aktywności przeniosła się do internetu. Korzystamy z poczty e-mail, bankowości online, mediów społecznościowych i różnego rodzaju aplikacji - wszystkie te miejsca mogą stać się celem cyberataków. **Dlatego odpowiednie zabezpieczenia oraz świadome korzystanie z sieci stają się niezbędne zarówno dla użytkowników prywatnych, jak i firm.**

Cyberbezpieczeństwo to nie tylko techniczne rozwiązania, ale również nawyki i procedury, które pomagają chronić dane, konta oraz prywatność. Silne hasła, weryfikacja dwuskładnikowa, regularne aktualizacje urządzeń i ostrożność przy klikaniu w linki czy otwieraniu załączników to podstawy tzw. cyberhigieny. Ich stosowanie znacząco zmniejsza ryzyko wycieku danych lub przejęcia kont.

Poznaj praktyczne wskazówki, które pozwolą skutecznie zabezpieczyć konta - zarówno pocztę e-mail w serwisach takich jak WP.pl, Onet, Gmail czy Interia, jak i dostęp do mediów społecznościowych oraz innych usług online. Dzięki tym prostym, ale skutecznym działaniom zwiększysz bezpieczeństwo swoich danych i zachowasz spokój w codziennym korzystaniu z internetu.

DIT DIRECT IT

ul. Jana Henryka Dąbrowskiego 273A,
60-406 Poznań

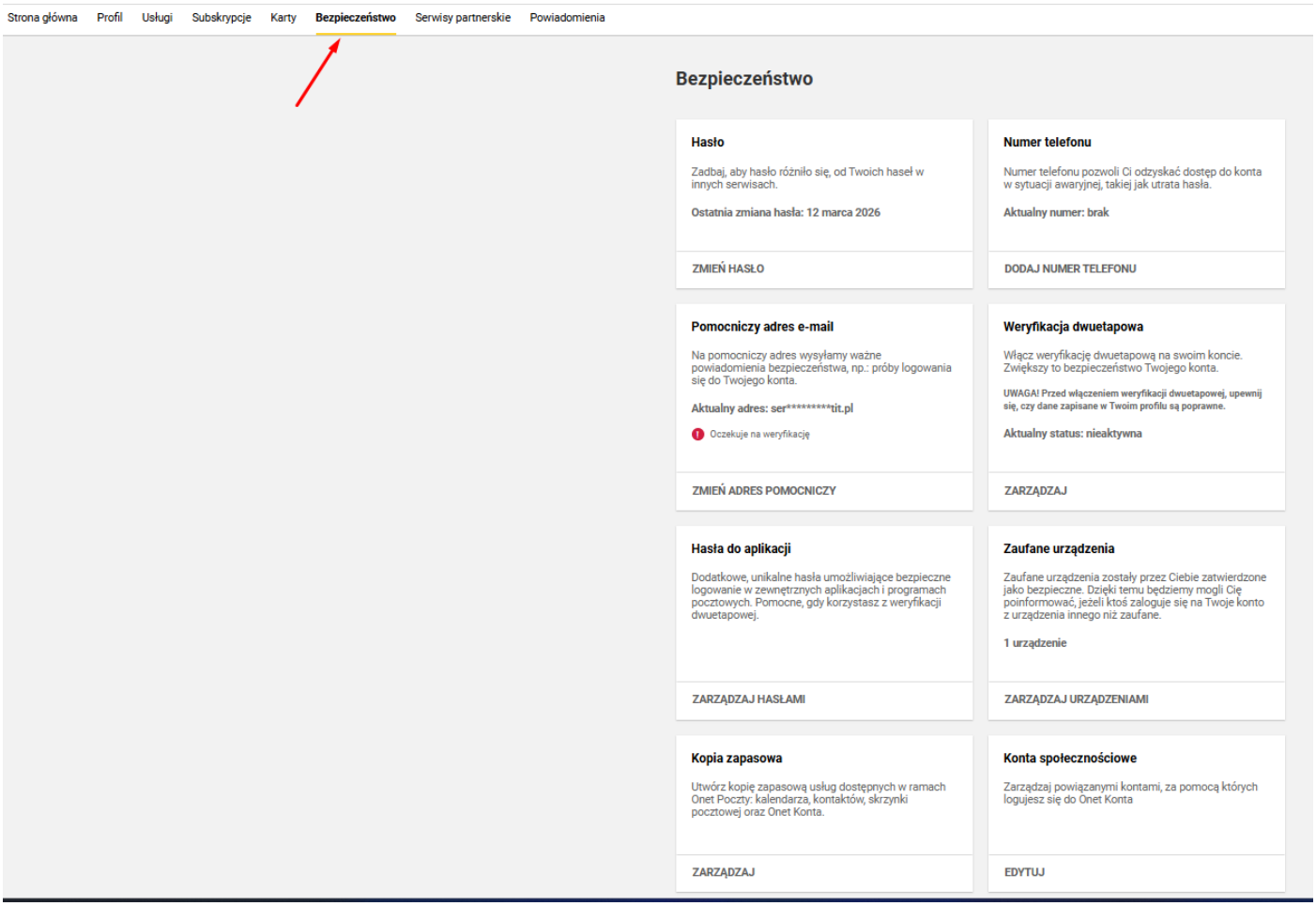
biuro@directit.pl

+48 61 646 08 70

www.directit.pl

POCZTA EMAIL W ONET.PL

W celu weryfikacji zabezpieczeń swojego konta wchodzimy z profilu użytkownika w zakładkę Bezpieczeństwo lub bezpośrednio przez adres:
https://konto.onet.pl/security



1. Ustaw silne i unikalne hasło

Hasło do poczty powinno być trudne do odgadnięcia i nie powinno być używane w innych serwisach. Dobrze, aby było odpowiednio długie i składało się z różnych znaków.

Najlepiej unikać prostych haseł opartych na imieniu, nazwie firmy, dacie urodzenia albo łatwych schematach.

Dobrą praktyką jest korzystanie z menedżera haseł, który pomaga przechowywać silne hasła w bezpieczny sposób.

2. Dodaj numer telefonu

Numer telefonu jest bardzo ważny z punktu widzenia bezpieczeństwa konta. Może pomóc w odzyskaniu dostępu do skrzynki w sytuacji, gdy użytkownik zapomni hasła albo wystąpi problem z logowaniem.

Numer telefonu powinien:
- być aktualny,
- należeć do właściciela konta,
- być dostępny na co dzień.

Jeżeli numer nie jest ustawiony, warto go dodać jak najszybciej. Brak numeru telefonu może utrudnić odzyskanie dostępu do konta.

3. Ustaw pomocniczy adres e-mail

Pomocniczy adres e-mail służy do odbierania ważnych powiadomień bezpieczeństwa, na przykład informacji o próbach logowania albo wiadomości potrzebnych do odzyskania konta.

Taki adres powinien:
- być aktywny,
- należeć do właściciela konta,
- być dobrze zabezpieczony.

Jeżeli adres pomocniczy oczekuje na weryfikację, należy dokończyć ten proces. Niezweryfikowany adres może nie spełniać swojej roli w sytuacji awaryjnej.

4. Włącz weryfikację dwuetapową

Weryfikacja dwuetapowa to jedno z najważniejszych zabezpieczeń konta. Po jej włączeniu samo hasło nie wystarczy do zalogowania się do poczty. Potrzebne będzie jeszcze dodatkowe potwierdzenie, na przykład kod.

To oznacza, że nawet jeśli ktoś pozna hasło, nadal nie powinien uzyskać dostępu do skrzynki bez drugiego etapu logowania.

Warto pamiętać, że:
- weryfikacja dwuetapowa znacząco zwiększa bezpieczeństwo,
- najlepiej włączyć ją jak najszybciej,
- przed włączeniem tej funkcji należy upewnić się, że numer telefonu i dane odzyskiwania są poprawne.

Na Onet.pl dostępne formy Weryfikacji dwuetapowej to:
- Logowanie kluczem dostępu
- Aplikacja uwierzytelniająca
- Klucz zabezpieczeń

5. Korzystaj z haseł do aplikacji, jeśli używasz programu pocztowego

Jeżeli konto pocztowe jest używane w zewnętrznym programie, takim jak Outlook, Thunderbird albo aplikacja pocztowa w telefonie, można korzystać z tzw. haseł do aplikacji.

Są to dodatkowe, osobne hasła przeznaczone do logowania w konkretnych programach. Dzięki temu nie trzeba używać głównego hasła konta w każdej aplikacji.

To rozwiązanie warto stosować szczególnie wtedy, gdy:
- włączona jest weryfikacja dwuetapowa,
- poczta działa w kilku urządzeniach,
- użytkownik chce ograniczyć ryzyko związane z korzystaniem z zewnętrznych aplikacji.

6. Sprawdzaj zaufane urządzenia

W ustawieniach konta można znaleźć listę zaufanych urządzeń. Są to urządzenia, które zostały wcześniej zatwierdzone przez właściciela konta.
Warto regularnie sprawdzać tę listę i upewniać się, że znajdują się na niej tylko znane komputery, telefony i inne używane urządzenia.

Jeżeli pojawi się urządzenie, którego użytkownik nie rozpoznaje, należy:
- usunąć je z listy,
- zmienić hasło,
- upewnić się, że weryfikacja dwuetapowa jest aktywna.

7. Rozważ wykonanie kopii zapasowej

Jeżeli skrzynka zawiera ważne wiadomości, kontakty albo inne istotne dane, warto rozważyć wykonanie kopii zapasowej.

Kopia zapasowa może pomóc w sytuacji, gdy:
- wiadomości zostaną przypadkowo usunięte,
- konto będzie chwilowo niedostępne,
- pojawi się problem techniczny lub bezpieczeństwa.

Jest to szczególnie ważne w przypadku poczty używanej do spraw prywatnych, urzędowych albo zawodowych.

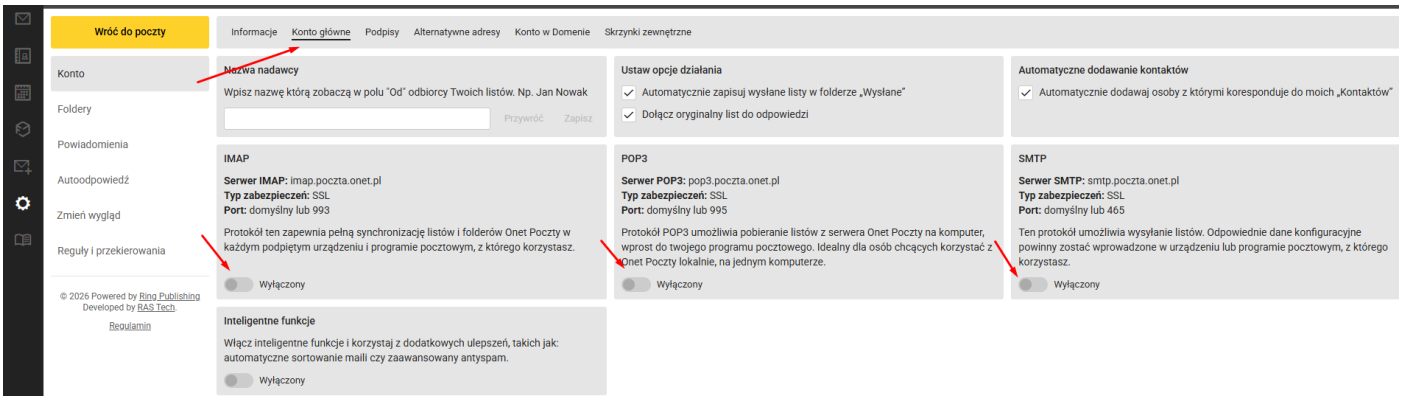
8. Sprawdź powiązane konta społecznościowe

Jeżeli konto Onet jest połączone z innymi usługami lub kontami społecznościowymi, warto sprawdzić, czy wszystkie te powiązania są nadal potrzebne i bezpieczne.

Należy zwrócić uwagę, czy:
- wszystkie połączone konta należą do właściciela,
- nie ma tam starych lub nieużywanych połączeń,
- dostęp nie został nadany przypadkowo.

Im mniej niepotrzebnych połączeń z innymi usługami, tym łatwiej utrzymać konto w bezpiecznej konfiguracji.

Dalej przechodzimy pod adres **https://ustawienia.poczta.onet.pl/Konto/KontoGlowne**



9. Wyłącz protokoły IMAP, POP3 i SMTP, jeśli nie korzystasz z programów pocztowych

W ustawieniach poczty można spotkać opcje związane z protokołami **IMAP, POP3 i SMTP.** Są to funkcje, które pozwalają korzystać ze skrzynki e-mail w zewnętrznych programach pocztowych, takich jak na przykład **Outlook, Thunderbird** albo aplikacja pocztowa w telefonie.

Dlaczego to ważne? Logowanie dwustopniowe na tej poczcie działa tylko przy logowaniu przez przeglądarkę, bez wyłączenia tych protokołów nie mamy w pełni zabezpieczonego dostępu.

Jeżeli użytkownik korzysta z poczty **wyłącznie przez stronę internetową w przeglądarce,** warto rozważyć pozostawienie tych protokołów **wyłączonych**. Dzięki temu ogranicza się dodatkowe sposoby dostępu do skrzynki, co może poprawić bezpieczeństwo konta.

Co oznaczają te protokoły:

- IMAP służy do synchronizacji wiadomości i folderów między serwerem poczty a programem pocztowym.
- POP3 służy do pobierania wiadomości z serwera do programu pocztowego.
- SMTP służy do wysyłania wiadomości z programu pocztowego.

Dlaczego warto je wyłączyć, jeśli nie są potrzebne

Jeżeli użytkownik nie korzysta z żadnego programu pocztowego ani aplikacji do obsługi poczty, włączenie tych funkcji nie daje mu korzyści, a jedynie pozostawia dodatkową możliwość połączenia ze skrzynką.

Wyłączenie IMAP, POP3 i SMTP może pomóc:
- ograniczyć dostęp do poczty tylko do przeglądarki internetowej,
- zmniejszyć ryzyko nieautoryzowanego użycia konta w zewnętrznym programie,
- uprościć konfigurację i codzienne korzystanie ze skrzynki.

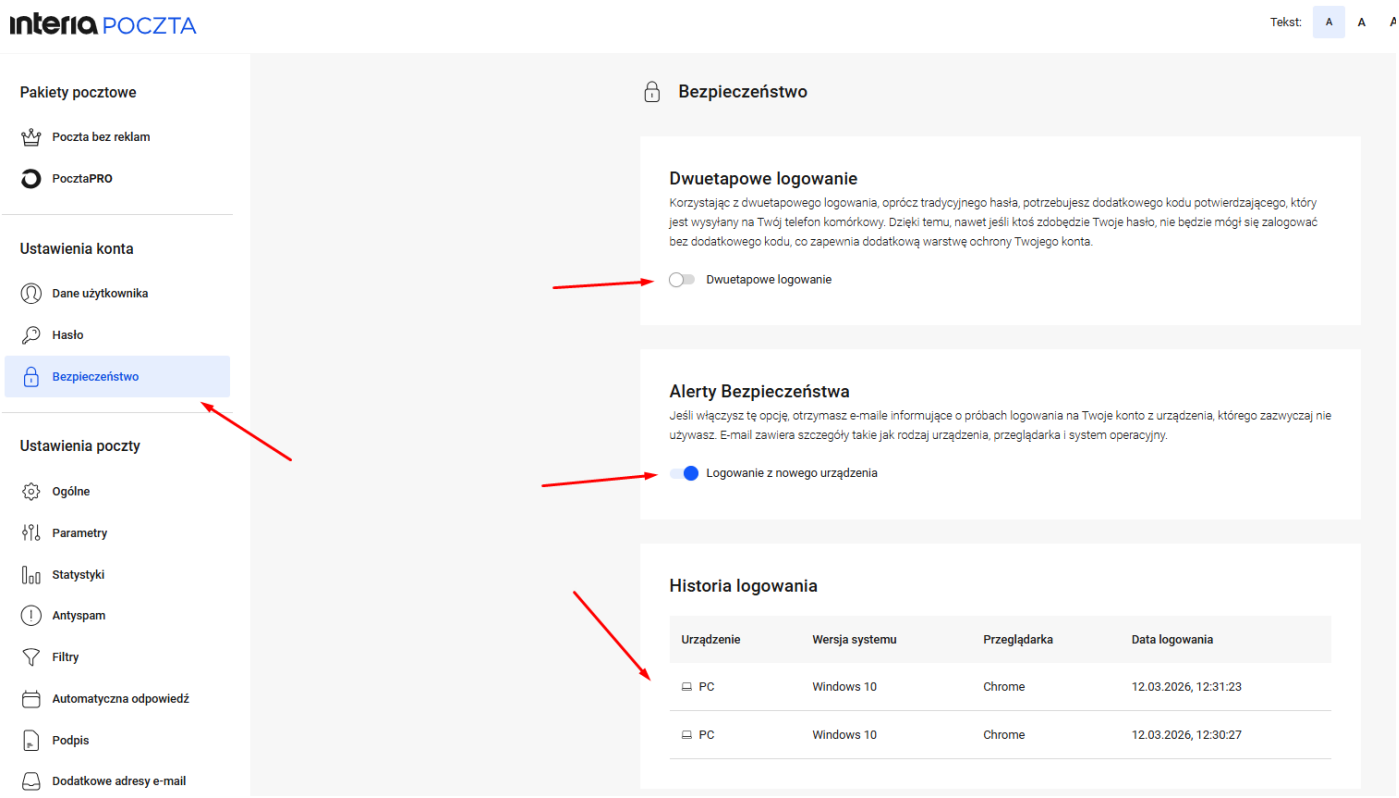
WAŻNA UWAGA

Przed wyłączeniem tych opcji trzeba upewnić się, czy konto nie jest już używane w zewnętrznych programach lub aplikacjach.

10. Rozważ korzystanie z płatnej wersji poczty

Warto rozważyć zakup płatnej wersji poczty Onet.pl, jeśli taka opcja jest dostępna i odpowiada potrzebom użytkownika. Jedną z jej zalet może być ograniczenie liczby reklam i treści promocyjnych widocznych podczas korzystania ze skrzynki. Ma to znaczenie nie tylko dla wygody, ale także dla bezpieczeństwa - im mniej tego typu komunikatów, tym mniejsze ryzyko przypadkowego kliknięcia w treść, która może wprowadzać w błąd, prowadzić do fałszywej strony lub przypominać próbę oszustwa. Mniejsza liczba rozpraszających komunikatów ułatwia też zauważenie prawdziwych wiadomości i podejrzanych e-maili.

W celu weryfikacji zabezpieczeń swojego konta wchodzimy z profilu użytkownika w zakładkę Bezpieczeństwo lub pod adresem:
https://ustawienia-pocztowe.interia.pl/#/bezpieczenstwo



1. Włącz logowanie dwustopniowe

To jedno z najważniejszych zabezpieczeń konta.
Po włączeniu logowania dwustopniowego samo hasło nie wystarczy, aby zalogować się do poczty. Potrzebne będzie jeszcze dodatkowe potwierdzenie, na przykład kod z telefonu. Dzięki temu nawet jeśli ktoś pozna hasło, nie powinien uzyskać dostępu do skrzynki.

2. Włącz alerty bezpieczeństwa

W ustawieniach Interii dostępna jest funkcja alertów bezpieczeństwa. Służy ona do informowania właściciela konta o logowaniu z nowego lub nietypowego urządzenia.

Po włączeniu tej opcji użytkownik otrzyma wiadomość e-mail z informacją o podejrzanej lub nowej aktywności. Taki komunikat może zawierać dane dotyczące urządzenia, przeglądarki lub systemu operacyjnego, z którego wykonano logowanie.

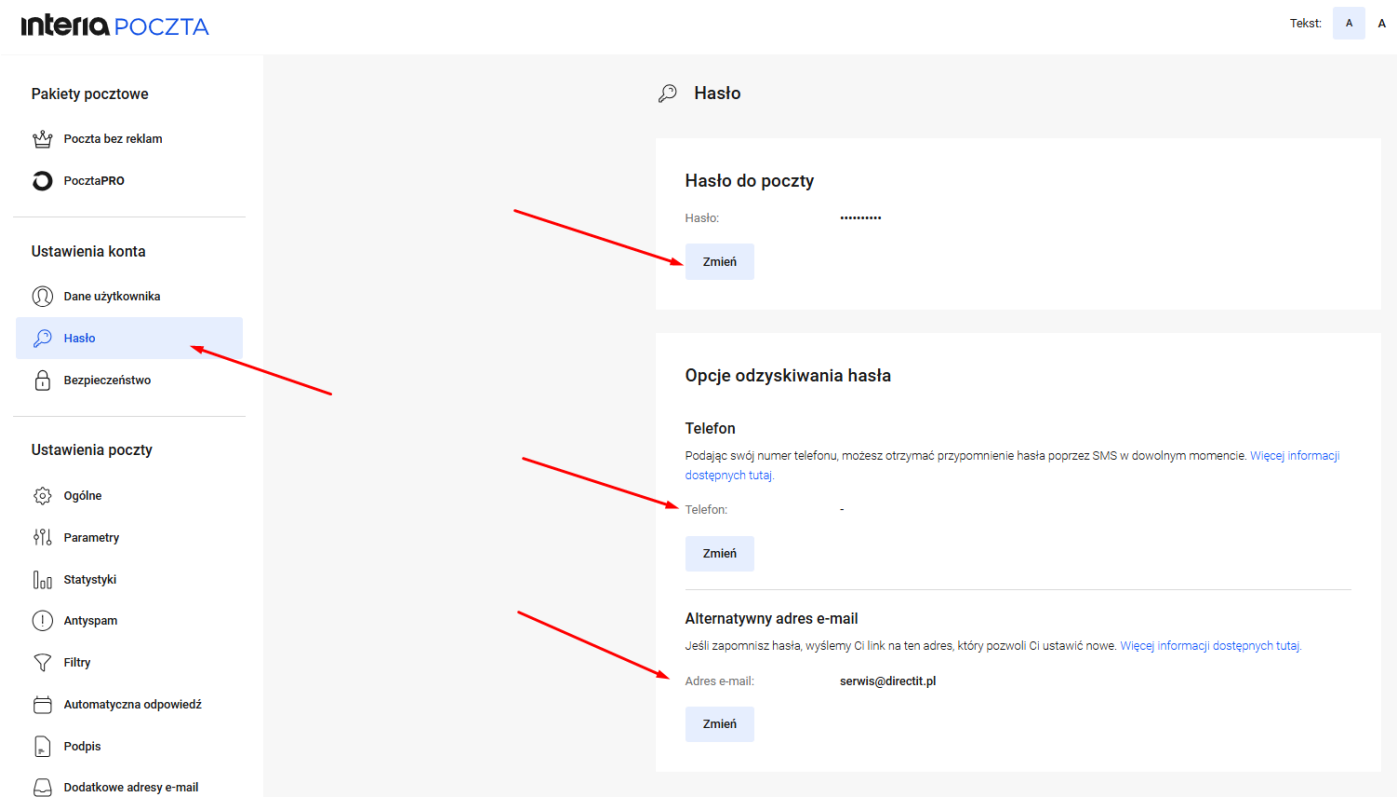
To bardzo przydatna funkcja, ponieważ pozwala szybko zauważyć, że ktoś próbował uzyskać dostęp do skrzynki albo zalogował się na nią z nieznanego urządzenia.

3. Regularnie sprawdzaj historię logowań

W ustawieniach konta warto co jakiś czas sprawdzać, z jakich urządzeń i z jakich miejsc odbywały się logowania.

Jeżeli pojawi się logowanie, którego właściciel nie rozpoznaje, należy potraktować to jako sygnał ostrzegawczy. W takiej sytuacji najlepiej od razu zmienić hasło i wylogować wszystkie pozostałe sesje.

Następnie wchodzimy w zakładkę Hasło



4. Ustaw silne i unikalne hasło

Hasło do poczty powinno być trudne do odgadnięcia i nie powinno być używane w innych serwisach.

Najlepiej, aby było długie i składało się z różnych znaków. Nie warto używać prostych haseł opartych na imieniu, nazwie firmy, dacie urodzenia czy łatwych ciągach znaków. Dobrą praktyką jest korzystanie z menedżera haseł, który pomaga przechowywać silne hasła w bezpieczny sposób.

5. Uzupełnij opcje odzyskiwania hasła

Opcje odzyskiwania hasła pomagają odzyskać dostęp do skrzynki e-mail, jeśli właściciel konta zapomni hasła albo utraci możliwość zalogowania się do poczty. W Interia.pl można w tym celu ustawić dodatkowe dane kontaktowe, które ułatwiają bezpieczne przywrócenie dostępu do konta.

Telefon do odzyskiwania hasła

Jedną z dostępnych opcji jest podanie numeru telefonu. Dzięki temu w razie problemów

z logowaniem można otrzymać wiadomość SMS pomocną przy odzyskaniu dostępu do skrzynki.

Warto pamiętać, że:
- numer telefonu powinien być aktualny,
- powinien należeć do właściciela konta,
- nie należy podawać numeru, do którego użytkownik nie ma stałego dostępu.

Dodanie numeru telefonu zwiększa wygodę i bezpieczeństwo, ponieważ pozwala szybciej odzyskać konto w sytuacji awaryjnej.

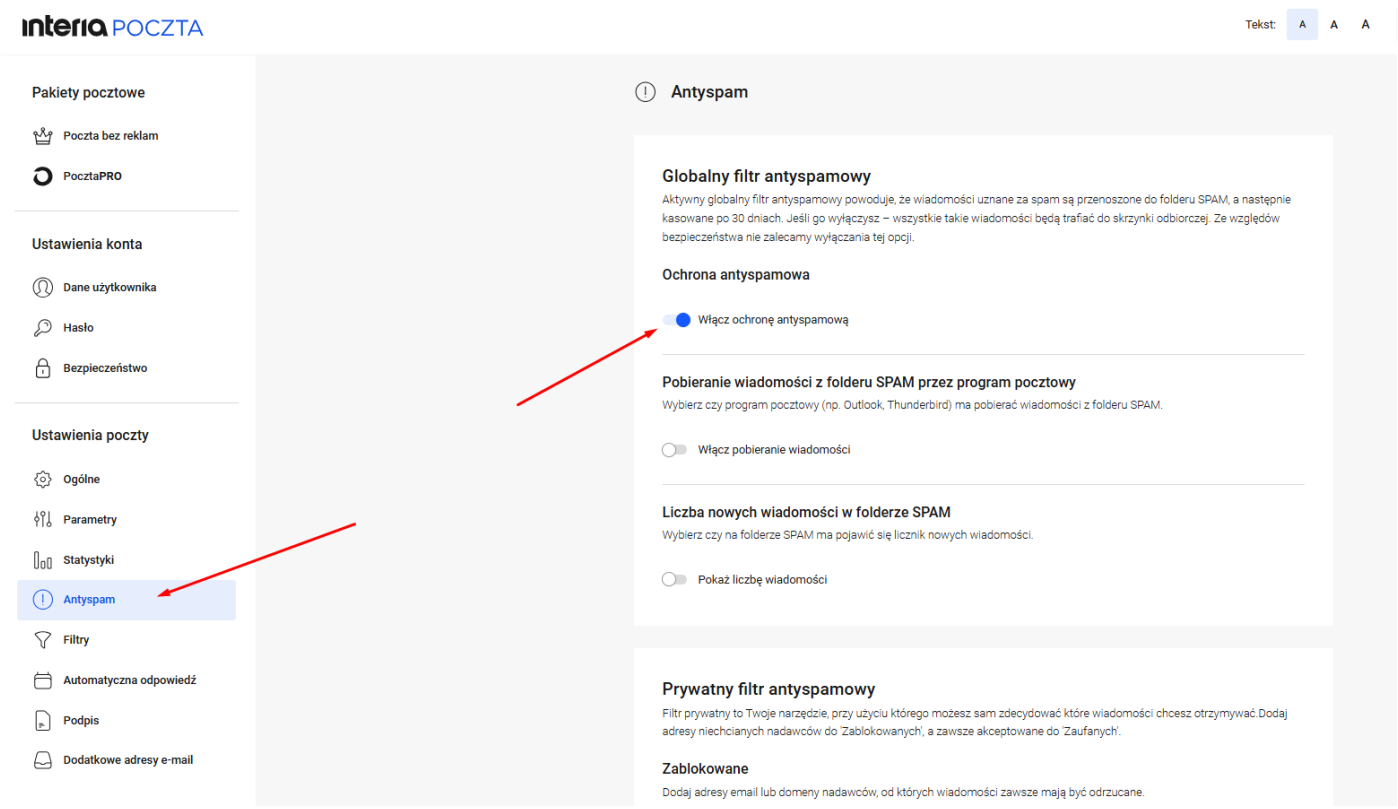
Alternatywny adres e-mail

Drugą ważną opcją jest ustawienie alternatywnego adresu e-mail. Jeżeli użytkownik zapomni hasła, Interia może wysłać na ten adres wiadomość z linkiem lub instrukcją potrzebną do ustawienia nowego hasła.

Taki dodatkowy adres e-mail powinien:
- być aktywny i regularnie używany,
- mieć własne, silne zabezpieczenia,
- nie być adresem przypadkowym ani tymczasowym.

Najlepiej, aby był to adres, do którego właściciel konta ma stały dostęp i który również jest dobrze chroniony.

Następnie wchodzimy w zakładkę Antyspam



6. Włącz ochronę antyspamową

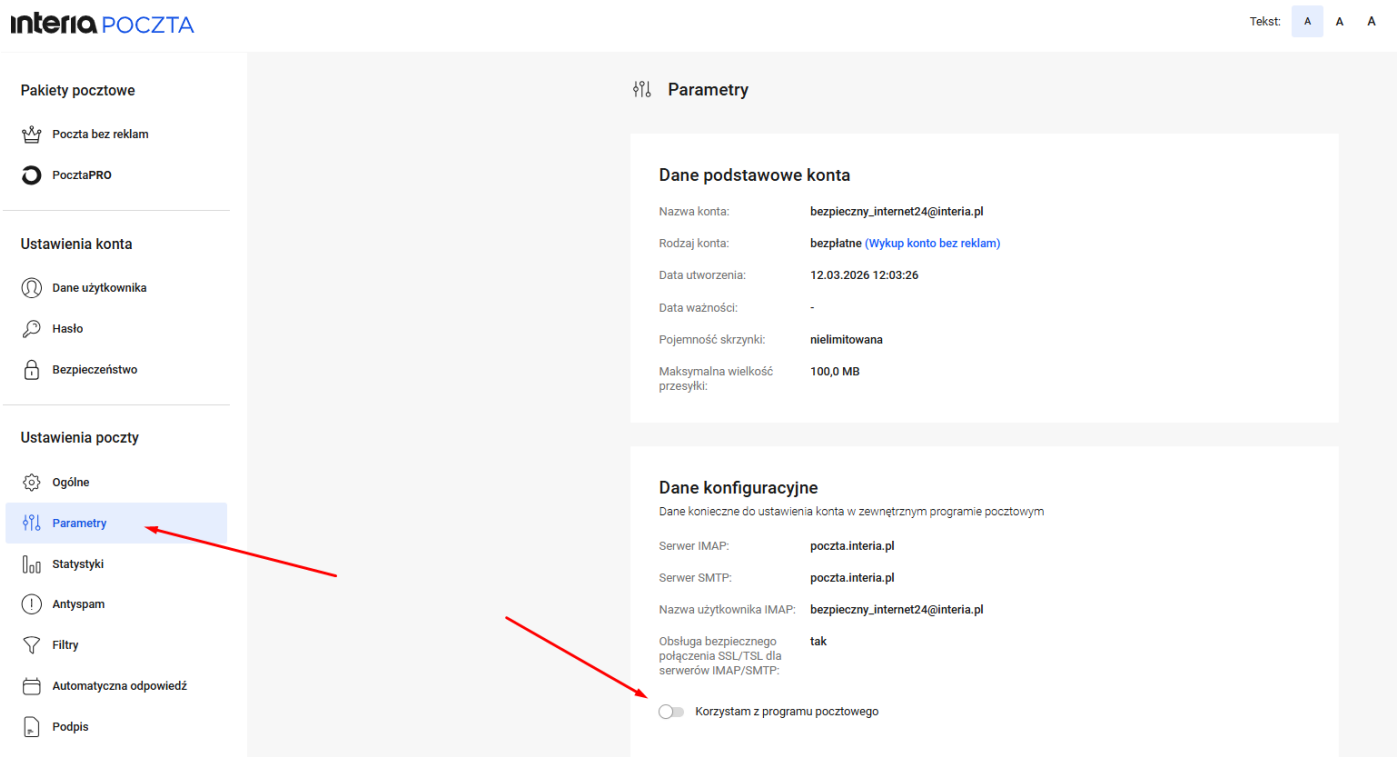
Ochrona antyspamowa pomaga ograniczyć liczbę niechcianych wiadomości trafiających do skrzynki odbiorczej. Po jej włączeniu wiadomości, które system rozpozna jako spam,

są przenoszone do folderu SPAM zamiast do głównej skrzynki.

To ważne zabezpieczenie, ponieważ wiele niebezpiecznych wiadomości przychodzi właśnie pod postacią spamu.

Mogą to być na przykład:
- fałszywe wiadomości z linkami do logowania,
- próby wyłudzenia danych,
- podejrzane załączniki.

Następnie wchodzimy w zakładkę Parametry



7. Pozostaw wyłączoną opcję „Korzystam z programu pocztowego”, jeśli nie używasz dodatkowych aplikacji

W ustawieniach poczty Interia znajduje się opcja **„Korzystam z programu pocztowego”.** Dotyczy ona korzystania ze skrzynki w zewnętrznych programach do obsługi e-maili, takich jak na przykład **Outlook, Thunderbird** albo aplikacja pocztowa w telefonie.

Dlaczego to ważne? Logowanie dwustopniowe na tej poczcie działa tylko przy logowaniu przez przeglądarkę, bez wyłączenia tych protokołów nie mamy w pełni zabezpieczonego dostępu.

Jeżeli użytkownik korzysta z poczty **wyłącznie przez stronę internetową Interia Poczta w przeglądarce**, zaleca się pozostawienie tej opcji **wyłączonej.** Dzięki temu ogranicza się możliwość dostępu do skrzynki z poziomu dodatkowych programów, co może poprawić bezpieczeństwo konta.

Dlaczego warto pozostawić tę opcję wyłączoną

Wyłączenie tej funkcji jest dobrą praktyką wtedy, gdy nie ma potrzeby odbierania poczty w innych aplikacjach. Im mniej sposobów dostępu do skrzynki, tym mniejsze ryzyko nieautoryzowanego użycia konta.

To rozwiązanie może pomóc:

- ograniczyć dostęp do poczty tylko do strony internetowej Interii,
- zmniejszyć ryzyko błędnej konfiguracji w zewnętrznych programach,
- uprościć korzystanie ze skrzynki i jej zabezpieczenie.

WAŻNA UWAGA

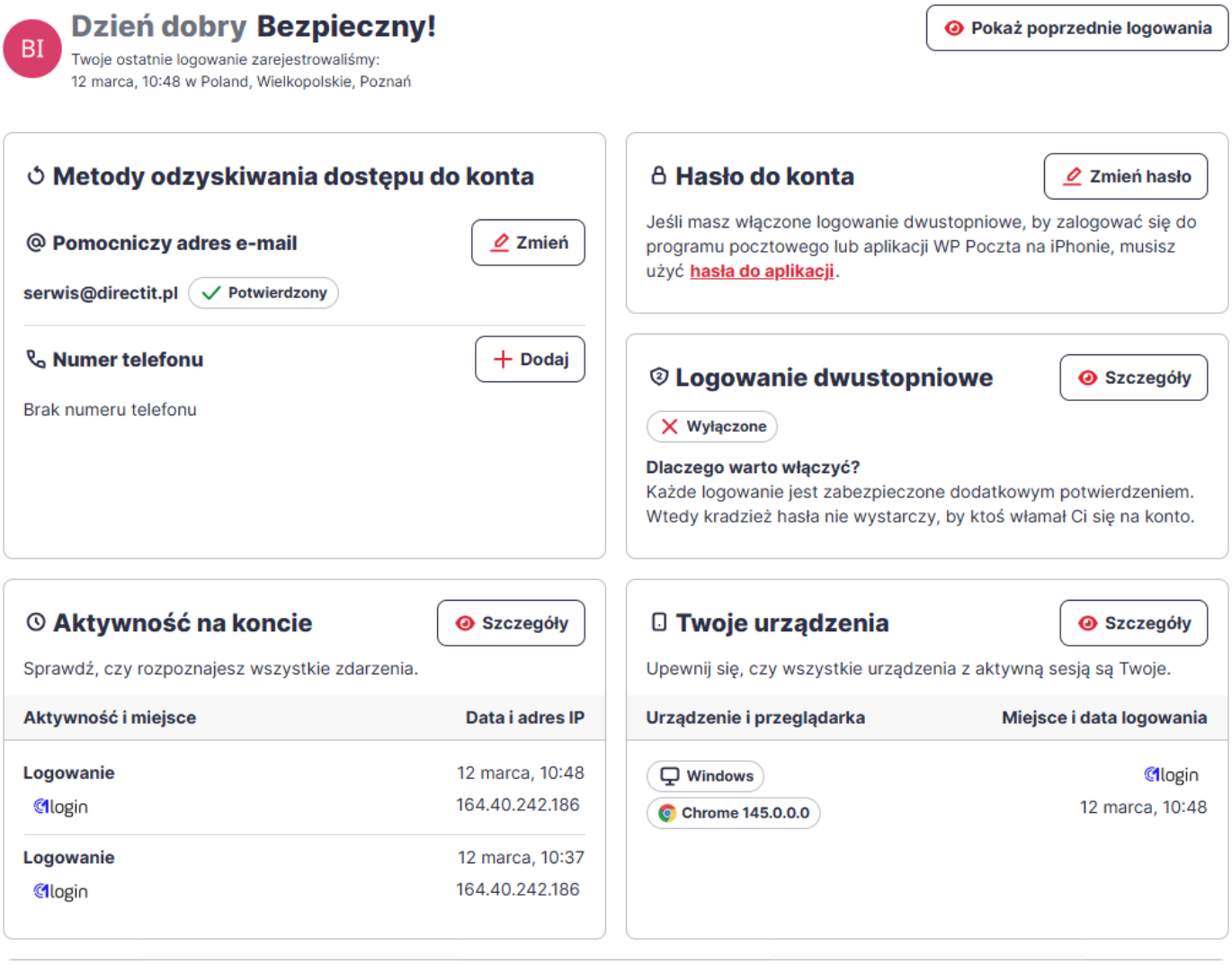
Jeżeli konto jest używane w programach takich jak Outlook, Thunderbird lub w aplikacji pocztowej na telefonie, pozostawienie tej opcji wyłączonej może spowodować, że taka poczta nie będzie działać poza przeglądarką.

8. Rozważ korzystanie z płatnej wersji poczty

Warto rozważyć zakup płatnej wersji poczty Interia.pl, jeśli taka opcja jest dostępna i odpowiada potrzebom użytkownika. Jedną z jej zalet może być ograniczenie liczby reklam i treści promocyjnych widocznych podczas korzystania ze skrzynki. Ma to znaczenie nie tylko dla wygody, ale także dla bezpieczeństwa - im mniej tego typu komunikatów, tym mniejsze ryzyko przypadkowego kliknięcia w treść, która może wprowadzać w błąd, prowadzić do fałszywej strony lub przypominać próbę oszustwa. Mniejsza liczba rozpraszających komunikatów ułatwia też zauważenie prawdziwych wiadomości i podejrzanych e-maili.

POCZTA EMAIL W WP.PL ORAZ O2.PL

W celu weryfikacji zabezpieczeń swojego konta wchodzimy w “Ustawienia konta” lub na adres: https://1login.wp.pl/profil



1. Włącz logowanie dwustopniowe

To jedno z najważniejszych zabezpieczeń konta.

Po włączeniu logowania dwustopniowego samo hasło nie wystarczy, aby zalogować się do poczty. Potrzebne będzie jeszcze dodatkowe potwierdzenie, na przykład kod z telefonu. Dzięki temu nawet jeśli ktoś pozna hasło, nie powinien uzyskać dostępu do skrzynki.

2. Dodaj numer telefonu do odzyskiwania konta

Numer telefonu pomaga odzyskać dostęp do poczty w sytuacji, gdy właściciel zapomni hasła albo konto zostanie zablokowane.

Warto upewnić się, że podany numer jest aktualny i należy do właściciela konta. Dobrze jest także mieć ustawiony pomocniczy adres e-mail, który również może pomóc w odzyskaniu dostępu.

3. Ustaw silne i unikalne hasło

Hasło do poczty powinno być trudne do odgadnięcia i nie powinno być używane w innych serwisach.

Najlepiej, aby było długie i składało się z różnych znaków. Nie warto używać prostych haseł opartych na imieniu, nazwie firmy, dacie urodzenia czy łatwych ciągach znaków.

Dobrą praktyką jest korzystanie z menedżera haseł, który pomaga przechowywać silne hasła w bezpieczny sposób.

4. Regularnie sprawdzaj historię logowań

W ustawieniach konta warto co jakiś czas sprawdzać, z jakich urządzeń i z jakich miejsc odbywały się logowania.

Jeżeli pojawi się logowanie, którego właściciel nie rozpoznaje, należy potraktować to jako sygnał ostrzegawczy. W takiej sytuacji najlepiej od razu zmienić hasło i wylogować wszystkie pozostałe sesje.

5. Kontroluj urządzenia mające dostęp do poczty

Dobrze jest upewnić się, że do skrzynki są podłączone tylko znane i używane urządzenia, takie jak własny komputer czy telefon.

Jeżeli na liście pojawi się urządzenie, którego właściciel nie rozpoznaje, należy usunąć mu dostęp i zmienić hasło do konta.

6. Wyłącz dostęp dla protokołów IMAP i POP

W ustawieniach konta WP można wyłączyć protokoły **IMAP i POP3.** Są to funkcje, które pozwalają odbierać pocztę w zewnętrznych programach pocztowych, takich jak na przykład **Outlook, Thunderbird** lub aplikacja pocztowa w telefonie.

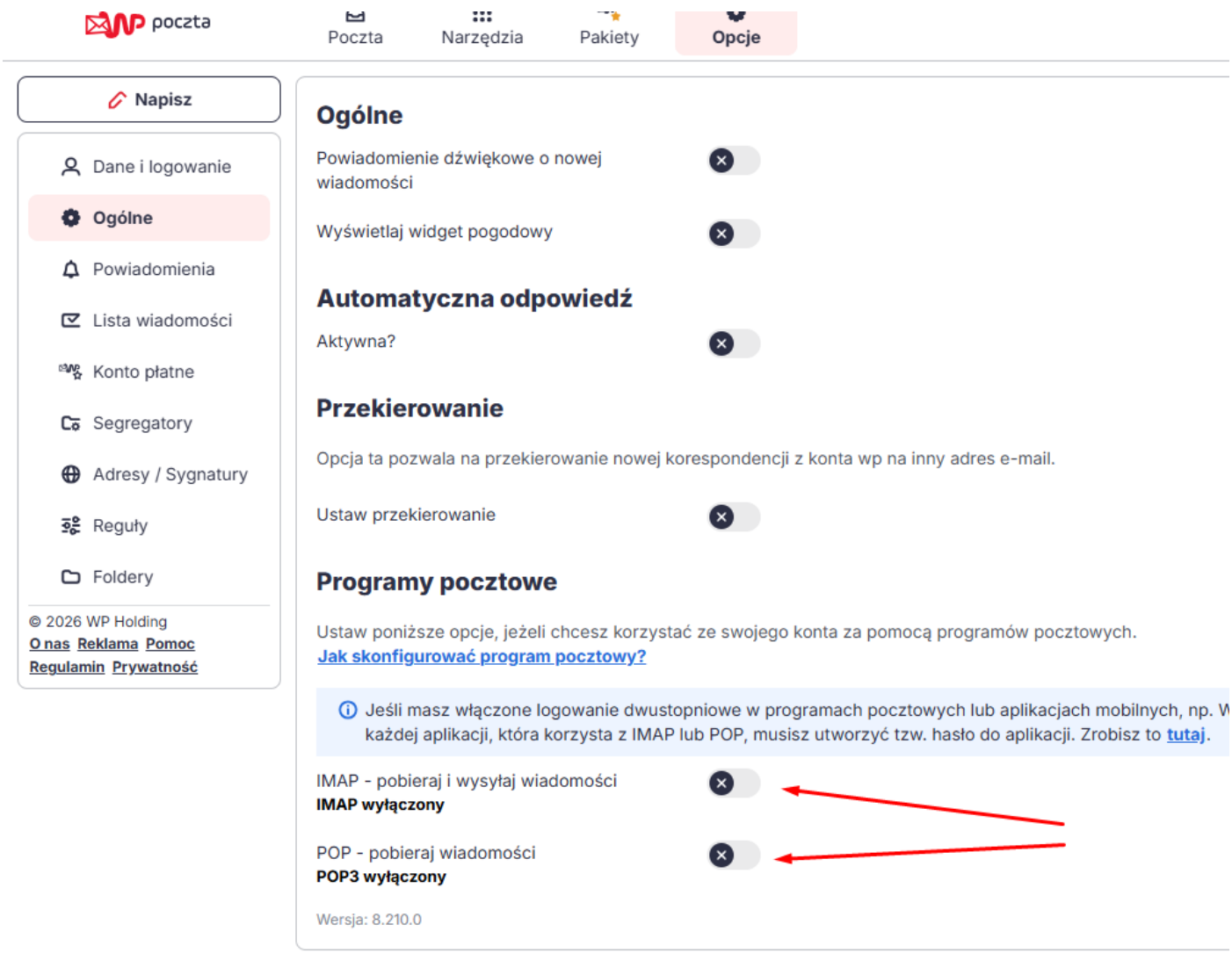
Dlaczego to ważne? Logowanie dwustopniowe na tej poczcie działa tylko przy logowaniu przez przeglądarkę, bez wyłączenia tych protokołów nie mamy w pełni zabezpieczonego dostępu.

Jeśli właściciel skrzynki korzysta z poczty **wyłącznie przez stronę internetową WP Poczta,** wyłączenie tych protokołów zwiększa bezpieczeństwo. Dzięki temu trudniej wykorzystać konto do logowania w zewnętrznych programach.

Trzeba jednak pamiętać, że **wyłączenie IMAP i POP3 spowoduje, że przestaną działać programy pocztowe i aplikacje korzystające z tych ustawień.**

Oznacza to, że wiadomości nie będą już odbierane w takich programach jak:

- Microsoft Outlook,
- Mozilla Thunderbird,
- aplikacja Poczta w telefonie lub komputerze,
- inne zewnętrzne klienty pocztowe.

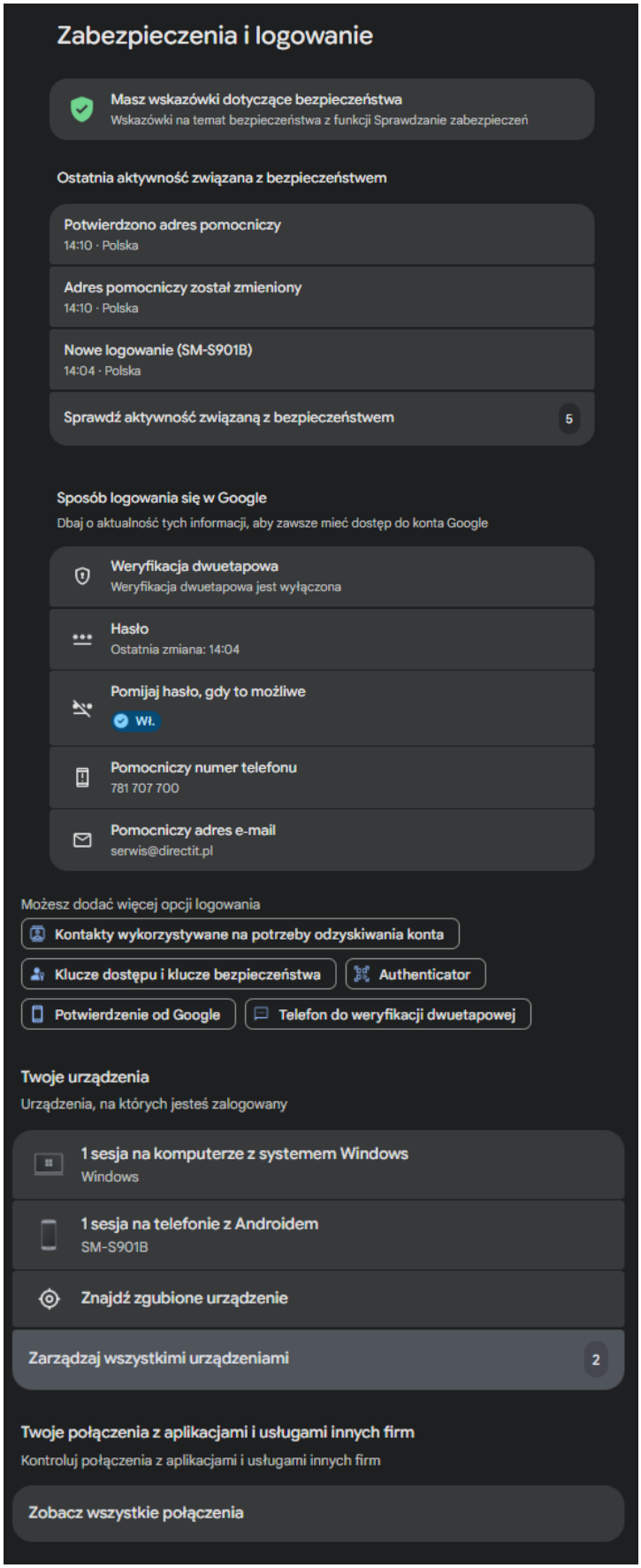


7. Rozważ korzystanie z płatnej wersji poczty

Warto rozważyć zakup płatnej wersji poczty WP, jeśli taka opcja jest dostępna i odpowiada potrzebom użytkownika. Jedną z jej zalet może być ograniczenie liczby reklam i treści promocyjnych widocznych podczas korzystania ze skrzynki. Ma to znaczenie nie tylko dla wygody, ale także dla bezpieczeństwa — im mniej tego typu komunikatów, tym mniejsze ryzyko przypadkowego kliknięcia w treść, która może wprowadzać w błąd, prowadzić do fałszywej strony lub przypominać próbę oszustwa. Mniejsza liczba rozpraszających komunikatów ułatwia też zauważenie prawdziwych wiadomości i podejrzanych e-maili.

POCZTA EMAIL W GMAIL.COM

W celu weryfikacji zabezpieczeń swojego konta wchodzimy na adres **https://myaccount.google.com/security**



1. Włącz weryfikację dwuetapową

Weryfikacja dwuetapowa to jedno z najważniejszych zabezpieczeń konta Gmail. Po jej włączeniu samo hasło nie wystarczy do zalogowania się. Potrzebne będzie jeszcze dodatkowe potwierdzenie, na przykład kod, potwierdzenie na telefonie lub inna metoda wskazana przez Google.

To bardzo ważne, ponieważ nawet jeśli ktoś pozna hasło do konta, bez drugiego etapu logowania nie powinien uzyskać dostępu do skrzynki.

2. Ustaw i sprawdź pomocniczy numer telefonu

Pomocniczy numer telefonu pomaga odzyskać dostęp do konta w sytuacji, gdy użytkownik zapomni hasła albo Google wykryje problem z logowaniem. Jest to jedno z podstawowych zabezpieczeń odzyskiwania konta.

Warto upewnić się, że:
- numer telefonu jest aktualny,
- należy do właściciela konta,
- użytkownik ma do niego stały dostęp.

Jeżeli numer się zmieni, należy jak najszybciej zaktualizować go w ustawieniach bezpieczeństwa.

3. Ustaw i utrzymuj aktualny pomocniczy adres e-mail

Pomocniczy adres e-mail to dodatkowy sposób odzyskania dostępu do konta. Może być używany do otrzymywania ważnych powiadomień bezpieczeństwa lub informacji potrzebnych do odzyskania hasła.

Taki adres powinien:
- być aktywny,
- należeć do właściciela konta,
- być dobrze zabezpieczony,
- być regularnie sprawdzany.

Jeżeli adres pomocniczy nie jest już używany, warto go zmienić na aktualny.

4. Sprawdzaj aktywność związaną z bezpieczeństwem

W ustawieniach Google można sprawdzić ostatnią aktywność związaną z bezpieczeństwem, na przykład:
- nowe logowania,
- zmiany adresu pomocniczego,
- potwierdzenia danych odzyskiwania,

To bardzo przydatna sekcja, ponieważ pozwala szybko zauważyć, czy na koncie nie zaszło coś, czego właściciel nie rozpoznaje. Jeżeli pojawi się informacja o nowym logowaniu, zmianie danych lub innej aktywności, której użytkownik nie wykonywał, należy potraktować to jako sygnał ostrzegawczy.

W takiej sytuacji najlepiej:
- od razu zmienić hasło,
- sprawdzić urządzenia zalogowane do konta,
- włączyć weryfikację dwuetapową, jeśli jeszcze nie jest aktywna,
- przejrzeć ustawienia odzyskiwania konta.

5. Regularnie kontroluj urządzenia zalogowane do konta

Google pokazuje urządzenia, na których konto jest aktualnie zalogowane. Warto regularnie sprawdzać tę listę i upewniać się, że znajdują się tam tylko znane komputery, telefony i tablety.

Należy zwrócić uwagę na:
- nieznane urządzenia,
- stare urządzenia, z których użytkownik już nie korzysta,
- logowania, których nie da się wyjaśnić.

Jeżeli na liście pojawi się podejrzane urządzenie, należy usunąć mu dostęp i zmienić hasło do konta.

6. Sprawdź połączenia z aplikacjami i usługami innych firm

Do konta Google mogą być podłączone różne aplikacje i usługi zewnętrzne. Czasami są to przydatne integracje, ale zdarza się też, że użytkownik zapomina o starych połączeniach, które nie są już potrzebne.

Warto regularnie sprawdzać:
- jakie aplikacje mają dostęp do konta,
- czy wszystkie połączenia są nadal potrzebne,
- czy nie ma tam nieznanych lub nieużywanych usług.

Im mniej zbędnych połączeń, tym łatwiej utrzymać konto w bezpiecznej konfiguracji.

7. Rozważ dodatkowe metody logowania i odzyskiwania

Google pozwala dodać więcej niż jeden sposób potwierdzania tożsamości. Można korzystać na przykład z aplikacji uwierzytelniającej, potwierdzeń od Google, kluczy bezpieczeństwa albo telefonu do weryfikacji dwuetapowej.

To dobre rozwiązanie, ponieważ daje dodatkowe możliwości logowania i odzyskania konta, gdy jedna metoda nie działa. Warto jednak zadbać o to, aby każda dodatkowa metoda była dobrze znana właścicielowi konta i prawidłowo skonfigurowana.

8. Używaj silnego i unikalnego hasła

Nawet jeśli konto ma dodatkowe zabezpieczenia, hasło nadal jest bardzo ważne. Powinno być:
- długie,
- trudne do odgadnięcia,
- nieużywane w innych serwisach.

Nie należy używać prostych haseł opartych na imieniu, dacie urodzenia, nazwie firmy albo łatwych ciągach znaków. Dobrym rozwiązaniem jest korzystanie z menedżera haseł.

CYBERHIGIENA - RADY

Używaj silnych i unikalnych haseł

Każde ważne konto powinno mieć inne hasło, zwłaszcza poczta e-mail, bankowość i media społecznościowe. Jeśli jedno hasło wycieknie, przestępca nie uzyska od razu dostępu do wszystkiego. Hasło powinno być długie, trudne do odgadnięcia i nieoparte na imieniu, dacie urodzenia czy prostych schematach. Najlepiej korzystać z menedżera haseł, który pomaga je tworzyć i przechowywać.

Włącz uwierzytelnianie dwuskładnikowe (2FA)

Samo hasło dziś bardzo często nie wystarcza. Drugi składnik, np. kod z aplikacji lub potwierdzenie logowania na telefonie, znacząco utrudnia przejęcie konta. Warto włączyć 2FA przede wszystkim na poczcie, Facebooku, Google, Apple, Allegro i wszędzie tam, gdzie są zapisane dane osobowe lub płatnicze. To jedna z najprostszych i najskuteczniejszych metod ochrony.

Chroń swoją pocztę e-mail w pierwszej kolejności

Skrzynka e-mail to centrum odzyskiwania dostępu do innych usług. Jeśli ktoś przejmie pocztę, może resetować hasła do banku, sklepów internetowych, portali społecznościowych i innych kont. Dlatego e-mail powinien mieć bardzo mocne hasło, włączone 2FA i aktualne dane do odzyskiwania dostępu. Warto też regularnie sprawdzać historię logowań i alerty bezpieczeństwa.

Nie klikaj bez zastanowienia w linki i załączniki

Oszuści często podszywają się pod bank, kuriera, urząd, znajomego albo portal sprzedażowy. Wiadomość może wyglądać bardzo wiarygodnie, ale prowadzić do fałszywej strony logowania lub zawierać złośliwy plik. Zanim klikniesz, sprawdź adres nadawcy, treść wiadomości i dokąd prowadzi link. Gdy coś wzbudza presję, strach albo pośpiech, trzeba zachować szczególną ostrożność.

Regularnie aktualizuj telefon, komputer i aplikacje

Aktualizacje nie służą tylko nowym funkcjom, ale przede wszystkim łataniu luk bezpieczeństwa. Nieaktualny system lub przeglądarka mogą zostać wykorzystane do infekcji bez żadnego działania z Twojej strony. Dotyczy to także routera domowego, telewizora smart, komunikatorów i innych urządzeń podłączonych do internetu. Im szybciej instalujesz poprawki, tym mniejsze ryzyko ataku.

Pobieraj aplikacje i pliki tylko z zaufanych źródeł

Programy z przypadkowych stron, „darmowe” wersje płatnych aplikacji i podejrzane dodatki do przeglądarki są częstym źródłem problemów. Mogą zawierać wirusy, spyware

albo narzędzia do kradzieży haseł. Aplikacje na telefon najlepiej instalować wyłącznie z oficjalnych sklepów, a programy na komputer ze stron producentów. Zasada jest prosta: im mniej eksperymentów z nieznanym oprogramowaniem, tym bezpieczniej.

Rób kopie zapasowe najważniejszych danych

Zdjęcia, dokumenty, skany, hasła awaryjne i inne ważne pliki warto mieć zapisane w więcej niż jednym miejscu. Kopia zapasowa chroni nie tylko przed awarią sprzętu, ale też przed ransomware, kradzieżą telefonu czy przypadkowym usunięciem danych. Dobrze sprawdza się zasada: dane na urządzeniu, kopia w chmurze i dodatkowa kopia offline. Backup, którego nie da się odtworzyć, nie jest prawdziwym zabezpieczeniem, więc warto go od czasu do czasu sprawdzić.

Zabezpiecz telefon i komputer przed dostępem osób postronnych

Urządzenia powinny być blokowane PIN-em, hasłem, odciskiem palca albo rozpoznawaniem twarzy. Automatyczna blokada ekranu po krótkim czasie bezczynności to prosty, ale ważny mechanizm. W przypadku zgubienia lub kradzieży utrudnia on dostęp do wiadomości, zdjęć, poczty i aplikacji bankowych. Dobrze też włączyć funkcję lokalizacji i zdalnego wymazania urządzenia.

Uważaj na to, co publikujesz w internecie

Zbyt duża ilość informacji o sobie ułatwia oszustwa, podszywanie się i ataki socjotechniczne. Daty urodzenia, adresy, plany wyjazdowe, zdjęcia dokumentów czy informacje o dzieciach mogą zostać wykorzystane przeciwko Tobie. Warto ograniczyć widoczność profili społecznościowych i regularnie sprawdzać ustawienia prywatności. To, co raz trafi do internetu, bardzo trudno potem całkowicie usunąć.

Korzystaj ostrożnie z publicznego Wi-Fi i obcych urządzeń

Otwarta sieć w galerii handlowej, hotelu czy na dworcu nie jest dobrym miejscem do logowania się do banku lub poczty. Nigdy nie masz pewności, kto taką sieć stworzył i czy ruch nie jest podsłuchiwany. Lepiej używać własnego internetu komórkowego albo przynajmniej unikać wrażliwych działań w publicznej sieci. Nie warto też logować się na swoje ważne konta z cudzego komputera.

Regularnie sprawdzaj konta pod kątem podejrzanej aktywności

Wiele usług pokazuje historię logowań, aktywne urządzenia i powiadomienia o nietypowych próbach dostępu. Warto zaglądać tam co jakiś czas, zwłaszcza dla poczty, Google, Facebooka i bankowości. Szybkie wykrycie obcego logowania pozwala zareagować zanim dojdzie do większych szkód. Po zauważeniu czegoś podejrzanego należy natychmiast zmienić hasło i wylogować wszystkie sesje.

Korzystaj z prostych, sprawdzonych materiałów edukacyjnych

Nawet podstawowa wiedza o oszustwach internetowych bardzo zwiększa bezpieczeństwo w codziennym życiu. Warto śledzić krótkie poradniki i przypominać sobie najważniejsze zasady, bo metody przestępców stale się zmieniają. Dobrym źródłem jest cert.pl/ouch/ — to cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek, jak można chronić siebie, swoich najbliższych i swoją organizację.

F//TRUST
iWealth

DIT DIRECT IT

Cyberbezpieczeństwo
zaczyna się od jednego pytania:

„Czy ja i moja firma jest bezpieczna?”

W Direct IT wierzymy, że każda strategia cyberbezpieczeństwa zaczyna się od audytu.

Nie od zakupu nowych systemów.
Nie od zatrudnienia specjalisty do firmy.
Od rzetelnej diagnozy, gdzie naprawdę jesteście.

Od 16 lat pomagamy firmom w Polsce i Europie odpowiedzieć na pytanie:
„Jak odporna jest moja organizacja na cyberatak?”

AUDYTY
cyberbezpieczeństwa

OCHRONA
infrastruktury IT

STRATEGIE
bezpieczeństwa
dla przedsiębiorstw

Bezpłatny audyt cyberbezpieczeństwa dla Państwa firm

(30-minutowa konsultacja strategiczna)

Cyberbezpieczeństwo w firmie zaczyna się od jednego pytania - zadajemy je razem.

DIT DIRECT IT

ul. Jana Henryka Dąbrowskiego 273A,
60-406 Poznań
biuro@directit.pl

+48 61 646 08 70
www.directit.pl