**Jak zabezpieczyć swoją pocztę przed włamaniem?**

**W dzisiejszych czasach, gdy komunikacja i przesyłanie informacji odbywa się głównie za pośrednictwem internetu, zabezpieczenie naszych kont e-mailowych staje się jednym z ważniejszych elementów bezpieczeństwa w sieci.**

Założenie poczty elektronicznej to jedna z pierwszych czynności, które wykonuje się po wkroczeniu w świat internetu. Posiadanie konta e-mail otwiera nam drogę do różnych stron, sklepów i portali, których używanie wiąże się z potrzebą posiadania własnego profilu. Niestety, wiele osób bagatelizuje sprawę cyberbezpieczeństwa i nie chroni dostępu do swojej skrzynki w należyty sposób. Przejęcie kontroli nad naszą pocztą elektroniczną przez osoby niepowołane to nie tylko ryzyko związane z czytaniem prywatnej korespondencji. To także możliwość:

l **kradzieży tożsamości** - posiadanie dostępu do cudzego konta e-mail daje włamywaczowi możliwość podszywania się pod swoją ofiarę. Hakerzy mogą wówczas wysyłać zawirusowane wiadomości w jej imieniu do posiadanych kontaktów.

l **naruszenia bezpieczeństwa innych kont** - jeżeli używamy tego samego hasła lub podobnych kombinacji znaków dla różnych profili internetowych, włamywacz po przejęciu poczty elektronicznej prawdopodobnie zaatakuje także inne nasze konta, w tym te w mediach społecznościowych, sklepach internetowych, a także bankowości online. (*Polecamy:* [Jak stworzyć bezpieczne hasło?](https://cyberszkolenia.pl/jak-stworzyc-bezpieczne-haslo/))

l **wysyłania spamu** - skradzione konto e-mailowe może być wykorzystywane do rozsyłania spamu i phishingowych wiadomości - zarówno do naszych kontaktów, jak i losowych adresów znalezionych przez przestępców w internecie.

W związku z powyższymi zagrożeniami, kluczowe jest, aby dbać o bezpieczeństwo swojej skrzynki pocztowej i chronić ją przed atakami cyberprzestępców. Tylko, jak to zrobić?

**Bezpieczna poczta e-mail: silne hasło**

Podstawowym elementem procesu weryfikacji tożsamości użytkownika danej skrzynki pocztowej jest oczywiście hasło. To ono stanowi pierwszą przeszkodę dla hakerów na drodze do prywatnej korespondencji swoich ofiar. **Ważne jest, aby hasło było silne i trudne do odgadnięcia**, nawet dla doświadczonego cyberprzestępcy. Optymalnie powinno się składać z ciągu różnych liter (dużych i małych), cyfr oraz znaków specjalnych (np. @#$%&\*). Kluczowe jest również, aby nie posługiwać się jednym hasłem na wielu platformach - ułatwi to hakerom przejęcie kontroli nad naszymi innymi kontami.



Dla osób, które mają trudności z zarządzaniem i pamiętaniem wielu skomplikowanych kombinacji znaków, **pomocne mogą okazać się menedżery haseł**. W zależności od wybranego narzędzia, mogą być one zintegrowane bezpośrednio z przeglądarką internetową lub działać jako osobna aplikacja. Co więcej, automatycznie uzupełniają one hasła na wybranych stronach internetowych, co nie tylko ułatwia proces logowania, ale także zapewnia większe bezpieczeństwo użytkownikowi.

**Bezpieczna poczta e-mail: 2FA**

2FA, czyli tzw. **uwierzytelnianie dwuskładnikowe**, to bardzo przydatne narzędzie w kontekście bezpieczeństwa poczty elektronicznej. Dodatkowa warstwa zabezpieczeń stanowi skuteczną przeszkodę przed dostępem do naszej skrzynki dla osób nieupoważnionych - nawet dla hakerów, którzy są w posiadaniu danych logowania.

Wprowadzenie dodatkowego etapu weryfikacji, który wymaga podania jednorazowego kodu generowanego automatycznie, znacznie zmniejsza ryzyko włamania na nasz e-mail. Co ciekawe, istnieje wiele sposobów na dostarczanie wspomnianych kodów użytkownikowi. Mogą one obejmować np. wiadomości SMS czy połączenia telefoniczne.

**Bezpieczna poczta e-mail: U2F**

Dla niektórych użytkowników poczty elektronicznej, przepisywanie jednorazowych kodów dostępu podczas weryfikacji dwuetapowej może być w pewien sposób uciążliwe. Okazuje się jednak, że nawet ten problem można obejść - wszystko to za sprawą kluczy bezpieczeństwa U2F.

Klucze bezpieczeństwa U2F to małe urządzenia, które z wyglądu przypominają nieco pendrive’y. Ich głównym atutem jest to, że całkowicie eliminują konieczność wpisywania danych logowania, włącznie z kodami dostępu. **By dostać się na konto, wystarczy włożyć fizyczny klucz do portu USB komputera**. Konfiguracja U2F odbywa się w ustawieniach naszej poczty.

Korzystanie z U2F niemal eliminuje ryzyko włamania się na naszą skrzynkę pocztową. Dzięki temu rozwiązaniu, tożsamość użytkownika weryfikowana jest za pomocą klucza fizycznego, którego posiadanie świadczy o byciu prawowitym użytkownikiem konta.

**Bezpieczna poczta e-mail: podsumowanie**

Przygoda z internetem zawsze rozpoczyna się od poczty elektronicznej. Ponieważ to na e-mailu opierają się wszystkie konta stworzone w sieci, kluczowe jest zapewnienie mu należytej ochrony przed włamaniem. **Silne hasło to** [podstawa cyberbezpieczeństwa](https://cyberszkolenia.pl/), jednak warto pokusić się również o włączenie usługi 2FA, czyli uwierzytelniania składnikowego. Nieco kosztowną, lecz najbezpieczniejszą opcją, jest zakup fizycznego klucza U2F, dzięki któremu włamanie na nasze konto za pośrednictwem standardowych metod hakerskich, staje się praktycznie niemożliwe.