

JAK DBAĆ O BEZPIECZEŃSTWO SKRZYNKI EMAIL?



Jak dbać o bezpieczeństwo skrzynki e-mail?

Dlaczego ktoś miałby chcieć włamać się do mojego e-maila? Jak cyberprzestępcy mogą uzyskać dostęp do naszego konta? Jak sprawdzić, czy moje konto zostało przejęte? Co zrobić, jeśli po sprawdzeniu okaże się, że konto zostało przejęte? Jak zapobiec przejęciu konta e-mail?

Dlaczego ktoś miałby chcieć włamać się do mojego e-maila?

Każdego roku na całym świecie działalność cyberprzestępców generuje ogromne straty finansowe. W końcu pocztę elektroniczną używamy praktycznie do wszystkiego, od wysyłania zdjęć i utrzymywania kontaktów ze znajomymi po załatwianie spraw urzędowych, kontakt z bankiem, opieką zdrowotną czy punktami usługowymi. Wyciągi bankowe lub umowa najmu znajdująca się w skrzynce może zawierać szereg informacji.

Przechwycone dane mogą posłużyć atakującym do przeprowadzenia kolejnych ataków, mających na celu uzyskanie jeszcze większej ilości informacji na nasz temat. Pozyskanie przez cyberprzestępców danych logowania do innych kont może skutkować poważnymi konsekwencjami. Dodatkowo przejęte konto poczty mailowej stanowi dla oszustów doskonałe narzędzie, dzięki któremu mogą rozsyłać spam i złośliwe wiadomości, także do wszystkich osób znajdujących się wśród kontaktów ofiary. Takie działanie umożliwia im dotarcie do dużej liczby użytkowników, a fakt, że wiadomości wysyłane są z zaufanego źródła, podnosi skuteczność ataków.

Jak cyberprzestępcy mogą uzyskać dostęp do naszego konta?

Jedną z powszechniejszych metod jest przesyłanie wiadomości phishingowych. Nierzadko nadawcy fałszywych wiadomości podszywają się pod zaufane podmioty, jak na przykład banki, urzędy a nawet serwisy poczty elektronicznej i proszą o załogowanie się na specjalnie spreparowanej stronie, która wykrada dane logowania nieświadomego użytkownika. Inną metodą jest odgadywanie haseł na podstawie wcześniej pozyskanych informacji pochodzących na przykład z mediów

społecznościowych. Aby przejąć konto skrzynki mailowej, atakujący posługują się również danymi, które wyciekły z firm lub podmiotów, do usług których zarejestrowaliśmy się w przeszłości. W innym przypadku atakujący mogą posłużyć się złośliwym oprogramowaniem, które będzie miało za zadanie wykraść dane logowania z urządzenia ofiary. Jak sprawdzić, czy moje konto zostało przejęte? W pierwszej kolejności warto zwrócić uwagę na maile znajdujące się w katalogach wiadomości wysłanych i odebranych – szczególnie istotne będą wiadomości, których nie jesteśmy w stanie rozpoznać. Wszelkie problemy z zalogowaniem się do konta poczty, jak i powiadomienia dostawcy poczty o wielokrotnym logowaniu z nieznanym adresów IP i lokalizacji również nie powinny być zignorowane. Jeśli nasze konto służy cyberprzestępcom do rozsyłania spamu, to istnieje duża szansa, że nasi znajomi po otrzymaniu niechcianych wiadomości powiadomią nas o tym.

Aby sprawdzić, czy nasze dane zostały w przeszłości naruszone, można odwiedzić stronę [HaveIBeenPwned.com](https://haveibeenpwned.com), która prowadzi obszerną bazę adresów e-mail i numerów telefonów komórkowych, które wyciekły do Internetu. Ponadto Google umożliwia podgląd ostatniej aktywności na koncie oraz przeprowadzanie „Sprawdzenia zabezpieczeń”, które obejmuje weryfikację zalogowanych urządzeń. Wielu innych operatorów poczty e-mail oferuje podobne opcje, jak na przykład szczegółowe wskazówki dotyczące odzyskiwania przejętego konta. Mogą z nich skorzystać na przykład użytkownicy poczty Gmail, Yahoo Mail oraz Outlook.com.

Co zrobić, jeśli po sprawdzeniu okaże się, że konto zostało przejęte?

W takiej sytuacji należy niezwłocznie zmienić hasło, włączyć wieloskładnikowe uwierzytelnienie oraz – jeśli usługa poczty udostępnia taką funkcjonalność – wylogować wszystkie nierozpoznane urządzenia zalogowane na konto naszej poczty. Wykonanie tych kroków powinno wystarczyć w przypadku, gdy dostęp do konta poczty został uzyskany z urządzenia należącego do cyberprzestępcy, który przechwycił lub odgadł dane logowania. Jeśli natomiast niepowołany dostęp do poczty został uzyskany z należącego do nas urządzenia, które zostało zainfekowane złośliwym oprogramowaniem, to zmiana hasła oraz wieloskładnikowe uwierzytelnienie nie pomogą. W takim przypadku złośliwy program ma dostęp do wszystkich kont, na których jesteśmy zalogowani i konieczne będzie przeskanowanie urządzenia sprawdzonym programem antywirusowym, który pozbędzie się „pluskwy” z systemu.

Jak zapobiec przejęciu konta e-mail?

Przejęcie konta skrzynki mailowej może wiązać się z poważnymi konsekwencjami. Mimo że wachlarz metod oszustw jest bardzo szeroki, to jednocześnie istnieje wiele sposobów przeciwdziałania im. Warto także pamiętać o ogólnych zasadach bezpieczeństwa, aby skutecznie podnieść swoją ochronę w sieci. Co zrobić, aby uniknąć zagrożenia?

- Zmień hasło do poczty e-mail i innych kont, które wykorzystywały te same hasła.
- Włącz uwierzytelnianie wieloskładnikowe, które zmniejszy ryzyko niepowołanego dostępu do konta.
- Przeprowadź pełne skanowanie swojego komputera, aby upewnić się, że nie ma na nim złośliwego oprogramowania.
- Pod żadnym pozorem nie podawaj żadnych danych osobowych ani danych logowania do kont online, jeśli otrzymasz wątpliwe żądanie, na przykład na pośrednictwem poczty email, SMS-a, mediów społecznościowych itp.
- Dla swojego dobra nie loguj się do poczty e-mail w publicznej sieci Wi-Fi lub na współdzielonym komputerze.

Użytkownicy poczty elektronicznej powinni być czujni wobec podejrzanych wiadomości i komunikatów pochodzących z serwisu poczty. Biorąc pod uwagę, że nasze dane lub hasła do kont bankowych mogły wpaść w ręce przestępców, istotne będzie monitorowanie i reagowanie w obliczu podejrzanych aktywności na naszych pozostałych kontach, w tym kontach bankowych. Skrzynka mailowa to kluczowy element naszej cyfrowej tożsamości, dlatego tym bardziej powinniśmy dbać o jej jak najlepsze zabezpieczenie



