pacjent.gov.pl

Jestem pacjentem, chronię swoje dane

Data aktualizacji
2025-07-28

W ostatnim czasie pojawiła się nowa fala oszustw internetowych, w których przestępcy podszywają się pod Narodowy Fundusz Zdrowia (NFZ). Wysyłają e-mailem lub SMS-em wiadomości dotyczące rzekomego zwrotu składek zdrowotnych. Próbują w ten sposób nakłonić do kliknięcia w niebezpieczny link i wyłudzić dane osobowe, loginy, hasła, a nawet pieniądze.

Niedawno też podszywali się pod platformę medyczną Medfile, wysyłając fałszywe powiadomienia o rzekomych wizytach lub wynikach badań.

Takie działania nazywamy phishingiem.

> **Phishing – metoda oszustwa, w której przestępcy podszywają się pod zaufane instytucje (np. NFZ, bank, przychodnię), aby wyłudzić Twoje dane. Często robią to przez:**
>
> - **e-mail,**
> - **SMS (tzw. smishing),**
> - **fałszywe strony internetowe.**

Na co zwracać uwagę

Aby się chronić, pamiętaj o kilku zasadach:

- Sprawdzaj, kto przysłał Ci wiadomość – czy adres e-mail nie wygląda podejrzanie (patrz na cały adres, a nie tylko na nazwę nadawcy, bo tę można wpisać dowolnie).
- Nie klikaj w linki z nieznanych źródeł – mogą prowadzić na fałszywe strony.
- Nie klikaj w linki do informacji, na które nie czekasz – zwłaszcza jeśli oferują Ci szybki zarobek, niespodziewany zwrot pieniędzy czy odebranie e-recepty, o której nic nie wiesz.
- Nie podawaj danych osobowych ani haseł przez e-mail lub SMS – nikt nie powinien znać takich danych, nikt też nie może Cię o prosić.
- Zwracaj uwagę na błędy językowe – oszuści czasami popełniają literówki albo błędy gramatyczne, gdy tłumaczą swój e-mail z innego języka niż polski.
- Zainstaluj program antywirusowy i aktualizuj go regularnie – ochronisz komputer przed nowymi zagrożeniami, które mogą prowadzić do utraty danych lub kradzieży tożsamości.
- Włącz uwierzytelnianie wieloskładnikowe (MFA) tam, gdzie to możliwe. Dzięki temu, nawet gdy Twoje dane do logowania zostaną wykradzione, oszust nie będzie mógł ich użyć, bo nie będzie miał np. dostępu do Twojego telefonu.
- Loguj się tylko przez oficjalne strony, np. pacjent.gov.pl – zminimalizujesz ryzyko wejścia na fałszywą witrynę.

Co zrobić, jeśli podejrzewasz oszustwo

- Nie odpowiadaj na wiadomość.
- Nie klikaj w przesłane linki.
- Zgłoś sprawę do placówki, pod którą podszywa się nadawca (np. NFZ).
- Możesz też zgłosić podejrzenie oszustwa do **CERT Polska**.

Gdzie znajdziesz dane o swoich składkach zdrowotnych

Informację na temat Twoich składek zdrowotnych, a także kosztów Twoich świadczeń, za które zapłacił NFZ, znajdziesz na Internetowym Koncie Pacjenta.

Żeby to sprawdzić:

- zaloguj się na Internetowe Konto Pacjenta. **Sprawdź, jak się zalogować**
- wybierz „Moje konto”
- tuż pod swoimi danymi znajdziesz „Twoje ubezpieczenie zdrowotne” wraz z informacją o tym, czy NFZ potwierdza Twoje prawo do świadczeń. Kliknij na kafelek „Zobacz składki”
- pod „Twoje składki ubezpieczeniowe” zobaczysz dane wszystkich pracodawców, którzy zgłosili Cię do ubezpieczenia zdrowotnego, oraz datę ostatnio zarejestrowanej składki
- pod „Podsumowanie składek na ubezpieczenie i kosztów refundacji” znajdziesz informację „Suma składek na ubezpieczenie zdrowotne”, a także kwotę wpłaconej składki w poszczególnych miesiącach. Możesz wybrać rok.

Ostatnia zarejestrowana składka zwykle dotyczy miesiąca poprzedzającego bieżący.

Przeczytaj też

Twoje bezpieczne IKP

O czym warto pamiętać, korzystając z Internetowego Konta Pacjenta lub aplikacji mojeIKP? Co robić, gdy na swoim koncie znajdujesz błędne dane lub cudze informacje?

Twoje dane medyczne to Twoja własność

Przypominamy: to Ty zarządzasz swoimi danymi dotyczącymi zdrowia i leczenia. Możesz je udostępnić lekarzowi czy placówce, ale nie masz takiego obowiązku

Jak udostępnić dane lekarzowi

Czy Twój lekarz prywatny wie o wszystkich Twoich wizytach u specjalistów? Czy lekarz specjalista na NFZ zna pełną listę leków, które przyjmujesz? Udostępnienie swojej historii leczenia lekarzowi może być kluczowe dla dokładnej diagnozy i skutecznego leczenia