

najczęściej zadawane pytania.

Dotyczące incydentu bezpieczeństwa

W niniejszym dokumencie znajdują Państwo odpowiedzi na najczęściej zadawane pytania dotyczące incydentu bezpieczeństwa oraz możliwego wycieku danych osobowych.

Pytania ogólne

1. Jakie konkretnie dane mogły wycieknąć?

Obecnie nie znamy jeszcze dokładnego zakresu zdarzenia i nadal prowadzimy dochodzenie. Ze względów ostrożnościowych zakładamy jednak maksymalny możliwy zakres, co oznacza, że mogły zostać ujawnione dane identyfikacyjne i kontaktowe, dane dotyczące umowy ubezpieczenia wraz z powiązaną dokumentacją (np. zgłoszenia szkód, ankiety zdrowotne lub dokumentacja medyczna), a także archiwalne rozmowy z infolinią klienta do roku 2021.

2. Kto stoi za atakiem?

Dochodzenie wykazało, że za atakiem stoi międzynarodowa zorganizowana grupa przestępcza. Nadal aktywnie zajmujemy się sytuacją we współpracy z ekspertami ds. cyberbezpieczeństwa, organami nadzorczymi oraz organami ścigania.

3. W jaki sposób doszło do wycieku danych?

Nie był to bezpośredni atak na nasze wewnętrzne systemy. Atak ransomware najpierw dotknął dostawcę odpowiedzialnego za część naszej infrastruktury technicznej. Za jego pośrednictwem napastnicy uzyskali dostęp do części naszej infrastruktury IT, a tym samym do niektórych danych osobowych klientów.

4. Co Simplea robi, aby chronić swoich klientów?

Klientów, których dane osobowe mogły zostać objęte incydemem, na bieżąco informujemy indywidualnie za pośrednictwem poczty elektronicznej, bezpośrednio lub za pośrednictwem Grupy Partners. Ze względu na skalę incydentu dostarczanie powiadomień może potrwać jeszcze kilka kolejnych dni. Nadal aktywnie zajmujemy się sprawą i współpracujemy z ekspertami ds. bezpieczeństwa, organami nadzorczymi oraz organami ścigania.

5. Czy muszę anulować lub zmieniać swoją polisę ubezpieczeniową z powodu incydentu?

Nie. Sam incydent nie stanowi powodu do rozwiązania ani modyfikacji umowy ubezpieczenia i nie ma wpływu na ważność ochrony ubezpieczeniowej ani zakres ubezpieczenia.

6. Na co należy zwrócić uwagę?

Prosimy nie udostępniać nikomu swoich haseł, kodów PIN ani jednorazowych kodów weryfikacyjnych. Prosimy również nie ulegać presji i nie podejmować pochopnych decyzji. Prosimy zachować ostrożność także wtedy, gdy osoba dzwoniąca zna Państwa dane osobowe. Sama znajomość takich informacji nie oznacza, że rzeczywiście kontaktują się Państwo z Simplea Ubezpieczenia, swoim agentem lub bankiem. Prosimy nie klikać w linki ani nie otwierać załączników pochodzących z nieoczekiwanych wiadomości e-mail lub SMS-ów oraz nie podawać w nich żadnych swoich danych. Na podstawie niezweryfikowanej prośby prosimy nie dokonywać żadnych płatności ani nie zmieniać danych do płatności, nawet jeśli taka prośba wydaje się wiarygodna.

7. Jak mogę się upewnić, że naprawdę dzwoni do mnie firma ubezpieczeniowa Simplea?

W razie jakichkolwiek wątpliwości należy zakończyć rozmowę i zweryfikować tożsamość dzwoniącego, kontaktując się ze swoim agentem lub korzystając z naszych oficjalnych danych kontaktowych podanych poniżej oraz na stronie www.simplea.pl/kontakty

najczęściej zadawane pytania.

Dotyczące incydentu bezpieczeństwa

8. Otrzymałem(-am) wiadomość e-mail lub SMS od Simplea Ubezpieczenia. Co powinienem(-am) zrobić?

Jeżeli otrzymana wiadomość zachęca Państwa do zalogowania się, podania danych, dokonania płatności lub podjęcia pilnego działania, prosimy nie klikać w zawarte w niej linki i najpierw zweryfikować jej autentyczność za pośrednictwem naszych danych kontaktowych dostępnych na stronie www.simplea.pl. Do portalu klienta prosimy logować się wyłącznie bezpośrednio przez oficjalną stronę [mojaSimplea](http://mojaSimplea.pl) pod adresem: www.mojasimplea.pl.

9. Czy powinienem/powinnam zmienić hasło lub dokumenty z powodu incydentu?

Tak, zalecamy zmianę hasła do portalu klienta. Jest to środek zapobiegawczy. Dzięki logowaniu potwierdzanemu kodem SMS nawet znajomość hasła nie powinna umożliwić osobie nieuprawnionej dostępu do portalu. Ogólnie zalecamy, aby nie używać tego samego hasła w różnych usługach i nigdy nie zmieniać hasła za pośrednictwem linku przesłanego w nieoczekiwanej wiadomości.

10. Czy ktoś może wykorzystać te dane, aby zaciągnąć pożyczkę na moje dane lub podszyć się pode mnie?

Same dane osobowe lub informacje dotyczące umowy zazwyczaj nie wystarczają do uzyskania kredytu lub dostępu do Państwa rachunku bankowego, ponieważ zwykle wymagane są dodatkowe dane uwierzytelniające. Zalecamy jednak zachowanie zwiększonej ostrożności wobec nietypowych wiadomości i prób potwierdzania Państwa tożsamości.

11. Co powinienem/powinnam zrobić, jeśli otrzymam podejrzany telefon lub wiadomość?

Prosimy niczego nie potwierdzać, nie udostępniać danych dostępowych ani kodów autoryzacyjnych, nie przekazywać pieniędzy oraz niezwłocznie zakończyć taką komunikację. Następnie prosimy zweryfikować otrzymaną prośbę za pośrednictwem naszych oficjalnych danych kontaktowych dostępnych na stronie www.simplea.pl. Jeżeli przekazali już Państwo swoje dane lub dokonali płatności w wyniku podejrzanej komunikacji, prosimy niezwłocznie skontaktować się ze swoim bankiem.

Dane zdrowotne i inne dane wrażliwe

12. Co atakujący mogą zrobić z moją dokumentacją medyczną lub ankietą zdrowotną?

Są to wrażliwe informacje dotyczące Państwa stanu zdrowia. Ryzykiem jest możliwość wykorzystania ich przez oszustów do prowadzenia bardziej wiarygodnej komunikacji. Dlatego zalecamy zwiększoną ostrożność.

13. Czy moje dane zdrowotne mogą zostać opublikowane w internecie?

Niestety nie można całkowicie wykluczyć takiej możliwości. Obecnie jednak nie ma podstaw, aby zakładać, że Państwa konkretne dane zostaną rzeczywiście opublikowane. Nadal badamy sytuację i współpracujemy ze wszystkimi właściwymi organami.

14. Czy ktoś może mnie szantażować, wykorzystując informacje z mojej dokumentacji medycznej?

Teoretycznie może dojść do próby wykorzystania poufnych informacji, choć nie jest to automatyczną konsekwencją wycieku danych. Jeśli ktokolwiek skontaktuje się z Państwem, grożąc lub żądając pieniędzy, prosimy nie reagować na takie żądania i niezwłocznie skontaktować się z Policją.

najczęściej zadawane pytania.

Dotyczące incydentu bezpieczeństwa

15. Czy ktoś może zadzwonić do mojego lekarza i uzyskać dodatkowe informacje?

Może podjąć taką próbę, jednak placówki medyczne mają obowiązek chronić dane zdrowotne pacjentów oraz weryfikować uprawnienia osób ubiegających się o dostęp do informacji. Samo posiadanie kopii dokumentacji medycznej nie uprawnia do uzyskania dodatkowych danych zdrowotnych.

16. Czy ktoś może wykorzystać te informacje przeciwko mnie w innej firmie ubezpieczeniowej?

Samo uzyskanie dostępu do Państwa dokumentacji medycznej nie daje osobie nieuprawnionej prawa do działania w Państwa imieniu ani do wprowadzania zmian w Państwa umowach ubezpieczenia. Zalecamy jednak zachowanie szczególnej ostrożności, jeśli ktoś skontaktuje się z Państwem i będzie znał szczegółowe informacje dotyczące Państwa stanu zdrowia.

17. Jak mogę rozpoznać, że ktoś wykorzystuje moje dane?

Prosimy zwrócić szczególną uwagę na komunikację, w której ktoś wykorzystuje niepubliczne informacje dotyczące Państwa stanu zdrowia w celu zdobycia Państwa zaufania, a następnie prosi o przekazanie pieniędzy, danych dostępowych lub kodu autoryzacyjnego. W takiej sytuacji prosimy natychmiast zakończyć komunikację i skontaktować się z nami, korzystając z danych kontaktowych podanych poniżej.

Przepraszamy za tę nieprzyjemną sytuację oraz za wszelkie obawy, jakie mogła ona spowodować. Bezpieczeństwo Państwa danych traktujemy niezwykle poważnie, dlatego informujemy o incydencie w możliwie najbardziej otwarty sposób.

Kontakty

W przypadku pytań prosimy o kontakt z naszą infolinią pod numerem
+48 22 100 99 44 lub drogą mailową na adres info@simplea.pl.