**Co zrobić po wycieku danych?**

**Według badań firmy Surfshark dotyczących wycieków danych, Polska w 2022r. była na 19. miejscu na świecie w liczbie skompromitowanych kont mając 38. populację na świecie pod względem liczby mieszkańców. Wiedza o cyberbezpieczeństwie wciąż nie jest w naszym kraju najlepsza, a w sieci czyha wiele zagrożeń. Gdy nasze dane zostaną skradzione, w najlepszym wypadku stracimy dostęp do konta, którego i tak nie używaliśmy. W najgorszym – stracimy mnóstwo pieniędzy.**

[Raport Surfshark wskazuje](https://surfshark.com/research/data-breach-monitoring), że osoby z Europy są narażone 3 razy bardziej na wycieki danych z kont niż reszta świata. 29,8% naruszeń to wycieki danych w Europie. Lecz oczywiście nie wszystkie kraje w tym samym stopniu są narażone na zagrożenia cybernetyczne.

**Gdzie sprawdzić, czy padliśmy ofiarą wycieku danych?**

Pierwsza witryna, którą powinniśmy odwiedzić to haveibeenpwned.com. Po wprowadzeniu adresu email lub numeru telefonu można dowiedzieć się czy powiązane z nimi dane wyciekły. Serwis może wskazać również zakres wycieku: czy wyciekły adresy email wraz z hasłami, czy hasła były dodatkowo zaszyfrowane oraz czy są jeszcze w bazie dane takie jak numery telefonów, adresy zamieszkania oraz daty urodzenia. Również niektóre przeglądarki internetowe z wbudowanym menadżerem haseł mają możliwość wskazania, które z haseł pojawiły się w bazie wykradzionych danych.

*Używanie unikalnych haseł w każdej usłudze to często niedoceniany bądź bagatelizowany środek ostrożności. Jednakże dzięki niemu po wycieku nie musimy zmieniać haseł w wielu serwisach. Oszczędzi nam to sporo czasu, stresu, a może nawet pieniędzy - mówi Aleksandr Valentij, Information Security Officer z Surfshark.*

**Co należy zrobić, kiedy jesteśmy ofiarą wycieku danych?**

Pierwszym krokiem jest zmiana hasła w każdej z usług, w których było ono używane. Jest to też dobry moment, aby dla pozostałych serwisów przez nas używanych zastosować silne, unikalne (czyli zupełnie nie podobne do siebie) hasła. Można próbować zapamiętać każde z nich, ale lepszym i wygodniejszym rozwiązaniem będzie skorzystanie z menadżera haseł. Oprócz generowania unikalnych haseł dla każdej z usług, potrafią one bezpiecznie przechowywać dane do logowania. Korzystanie z menadżera haseł wpłynie również pozytywnie na bezpieczeństwo w sieci.

Ważne jest także korzystanie z weryfikacji dwustopniowej. Może mieć ona formę kodu: wysłanego
SMS-em lub generowanego w aplikacji mobilnej. Dwuetapową weryfikację można także przeprowadzić wpinając do komputera czy smartfona niewielki, fizyczny klucz bezpieczeństwa podobny do pendrive’a lub karty płatniczej. Takie zabezpieczenie sprawi, że nikt nie skorzysta z danego serwisu nawet, gdy wycieknie nam hasło.

Dobrym rozwiązaniem dla osób, których numer PESEL został wykradziony są alerty z Biura Informacji Kredytowej. Wyślą one email za każdym razem gdy: ktoś złoży wniosek o kredyt używając naszych danych, zostanie nam przydzielony kredyt oraz gdy bank sprawdza naszą historię kredytową.

**O Surfshark**

*Surfshark to globalna firma zajmująca się rozwiązaniami w zakresie ochrony prywatności założona na Litwie. Surfshark jest jednym z trzech najlepszych na świecie dostawców VPN i jednym z niewielu uznanych przez niezależnych ekspertów ds. cyberbezpieczeństwa. W 2021 w konkursie Cybersecurity Excellence Awards Surfshark zdobył złoty medal i tytuł najbardziej innowacyjnej usługi cyberbezpieczeństwa roku. W 2022 Surfshark po połączeniu się z Nord Security, został drugim oficjalnym jednorożcem na Litwie.*

**Więcej informacji udzielą:**

Paulius Udra

PR Manager Surfshark

paulius@surfsharkpress.com

+370 645 26125

Arkadiusz Sęga

Senior Account Executive, Grayling Poland

arkadiusz.sega@grayling.com

+48 601 960 875