Warto wiedzieć, że...

Wyciek danych a ochrona prywatności w sieci.

Jak zadbać o swoje bezpieczeństwo?

Ogromna ilość informacji łatwo dostępnych w Internecie, to wystarczająca motywacja dla hakerów, aby dokonać ich kradzieży. Hasła są jak klucze do sejfu. Jeśli ktoś zdobędzie nasze hasło do danego portalu, może uzyskać dostęp do naszych prywatnych danych, dokonać przejęcia naszego konta w mediach społecznościowych, kradzieży naszej tożsamości czy transferu pieniędzy. Hasła są więc najbardziej pożądane, bo dzięki nim haker zdobywa dostęp do wielu naszych zasobów, w tym do innych danych osobowych, które może wykorzystać. Wyciek danych w Internecie, to poważne zagrożenie dla naszego bezpieczeństwa. Na co więc powinniśmy zwrócić szczególną uwagę, aby zminimalizować ryzyko? Co zrobić w sytuacji, kiedy dane zostały już zhakowane – podpowiadamy w kolejnej poradzie.

Jak zminimalizować ryzyko wycieku danych?

- **stosujmy silne hasło** – można w tym celu posłużyć się generatorem haseł;
- **stosujmy dwuetapowe logowanie** – jest to podwójne sprawdzenie tożsamości (uwierzytelnianie), które polega na podaniu loginu i hasła, a następnie potwierdzeniu logowania zazwyczaj zewnętrznym tokenem (np. kodem SMS). Zastosowanie takiego dodatkowego zabezpieczenia skutecznie ochroni przed atakami hakerskimi (phishingiem, przechwytywaniem sesji czy wyłudzeniem danych). Ponadto token nie zadziała podczas logowania na fałszywej stronie;
- **logujmy się na własnych urządzeniach**;
- **stosujmy zróżnicowane hasła** do różnych portali i systemów, w czym może pomóc nam manager haseł;
- **korzystajmy z zaufanego połączenia internetowego**, nigdy z publicznych hot spotów;
- **ograniczajmy uprawnienia aplikacji do logowania** za pomocą konta w portalu społecznościowym.

Co zrobić, gdy podejrzewamy, że nasze dane dostały się w niepowołane ręce?

- **zmieńmy hasło** najszybciej jak to możliwe, przy zachowaniu zasad tworzenia silnego hasła;
- zachowajmy szczególną **ostrożność przed atakami phishingowymi,** w tym celu nie otwierajmy załączników i linków od nieznanych osób, instytucji i firm, np. firm kurierskich, gdy nie zamawialiśmy przesyłki. Ataki te mogą się nasilić po wycieku danych kontaktowych;
- **nie udostępniajmy haseł i danych do logowania podczas rozmów telefonicznych z nieznanymi osobami**. Tak jak w przypadku metody na tzw. „wnuczka" czy „policjanta", oszuści mogą za pomocą różnych socjotechnik podszywać się pod inne osoby, dysponując informacjami z portalu. W ten sposób próbują wyłudzić kolejne dane, które umożliwią im dostęp do naszych kont lub urządzeń;
- **weryfikujmy autentyczność certyfikatu SSL** strony, na którą się logujemy. Można to sprawdzić, klikając w ikonę kłódki przy pasku adresu, rozwinąć szczegóły i zobaczyć, czy połączenie jest bezpieczne;
- **nie zapisujmy danych logowania w przeglądarce ani danych kart płatniczej lub kredytowej dla automatycznego wypełniania formularza danymi**. W żadnym wypadku nie podajemy nigdzie kodu dostępu, np. numeru PIN –- o ten element nikt nie ma prawa nas pytać, nawet konsultant instytucji bankowej;
- **nie wchodźmy na strony za pośrednictwem linków przesłanych pocztą elektroniczną czy komunikatorów od nieznanych nadawców czy takie które wydają nam się podejrzane.** To popularna metoda przestępców, aby przekierować użytkowników na fałszywe strony;
- zainstalujmy i utrzymujmy aktualność **zabezpieczenia antywirusowego i zapory w systemie.**

Zwracajmy szczególną uwagę na minimalizowanie liczby danych osobowych i informacji o nas, które udostępniamy w Internecie. Udostępniajmy tylko dane osobowe, w sytuacji kiedy to jest konieczne do realizacji usługi. A w sytuacji wycieku danych z portalu, koniecznie, niezwłocznie zmieniajmy hasło.

URZĄD OCHRONY DANYCH OSOBOWYCH