Warszawa, 15.04.2024 r.

# Kradzież danych z portali społecznościowych oraz jak chronić się przed zagrożeniami w świecie online

## Wstęp

W dzisiejszym świecie internetu, gdzie portale społecznościowe są integralną częścią życia codziennego, ochrona danych osobowych staje się coraz ważniejsza. Facebook, LinkedIn, Instagram - to tylko niektóre z platform, na których dzielimy się swoimi danymi.

Na portalach społecznościowych często udostępniamy szeroki zakres danych osobowych, w różnych formach. Na przykład, podczas rejestracji na Facebooku, Instagramie czy LinkedInie, podajemy nasze imiona i nazwiska, co stanowi podstawowe dane identyfikacyjne. Dodatkowo, często tworzymy pseudonimy (nicki), które również mogą być uznawane za dane osobowe, szczególnie gdy są zestawiane z innymi informacjami na profilu oraz używane w kontekście naszej tożsamości w internecie. Nasze zdjęcia, które publikujemy na platformach społecznościowych, również mogą ujawniać wiele informacji o naszej tożsamości, wyglądzie czy życiu prywatnym. Wraz z postami i komentarzami, które udostępniamy publicznie, mogą one budować kompletny obraz naszej osoby dla potencjalnych przestępców. Szczególne groźne są informacje publikowane na LinkedIn. Informacje o zatrudnieniu, które podajemy na LinkedInie, mogą zawierać szczegóły dotyczące naszych miejsc pracy, stanowisk zajmowanych w przeszłości, a nawet naszych obowiązków i osiągnięć zawodowych, a ich nieuprawnione wykorzystanie może wywoływać konsekwencje dla naszej kariery zawodowej w tym reputacji a nawet rzutować na nasze finanse.

Niestety, w miarę jak korzystanie z tych serwisów staje się popularne, wzrasta również ryzyko kradzieży danych i ich nieuprawnionego wykorzystania. Jak dochodzi do kradzieży danych na portalach społecznościowych, jakie są negatywne konsekwencje tego procederu, a przede wszystkim jak możemy się przed nim zabezpieczyć? O tym poniżej.

## I. Mechanizmy kradzieży danych

Mechanizmy kradzieży danych z portali społecznościowych są różnorodne i często wyrafinowane. Według najnowszych statystyk, aż 64% użytkowników internetu doświadczyło przynajmniej jednego incydentu związanego z bezpieczeństwem online, w tym kradzieży danych z kont na portalach społecznościowych.

Jedną z popularnych technik stosowanych przez przestępców jest phishing. Polega to na podszywaniu się pod zaufane instytucje lub osoby, aby wyłudzić poufne informacje, takie jak hasła czy dane osobowe. Typowe maile phishingowe mogą wyglądać jak oficjalne wiadomości od banków, firm technologicznych czy serwisów społecznościowych. Mogą zawierać linki do fałszywych stron logowania, które wyglądają identycznie jak oryginalne, ale w rzeczywistości przekierowują użytkownika na stronę kontrolowaną przez przestępców, którzy następnie kradną jego dane logowania.

Inną popularną techniką jest wykorzystanie luk w zabezpieczeniach, słabych haseł lub niewłaściwie zabezpieczonych aplikacji. Przestępcy mogą wykorzystać oprogramowanie złośliwe, które wykrada dane logowania z komputerów lub urządzeń mobilnych użytkowników. Mogą również atakować słabe hasła, stosując tzw. brute force, czyli wielokrotne próby odgadnięcia hasła poprzez wypróbowanie wszystkich możliwych kombinacji.

W przypadku podejrzanych aplikacji reklamowanych na portalach społecznościowych, przestępcy mogą udawać twórców narzędzi lub usług, które rzekomo oferują dodatkowe funkcje, takie jak

śledzenie odwiedzających nasz profil czy analizę aktywności. Po zainstalowaniu takiej aplikacji, użytkownik może nie zdawać sobie sprawy z tego, że przekazał dostęp do swoich danych osobowych, które następnie mogą być wykorzystane przez przestępców do różnych celów, włączając w to kradzież tożsamości, szantaż czy oszustwa finansowe.

Powyższe przykłady kradzieży danych z Facebooka, LinkedIna i Instagrama ilustrują skalę problemu, powszechność i jego różnorodność. Należy wskazać, że żadna z tych platform nie jest całkowicie odporna na tego rodzaju ataki. Dlatego tak ważne jest, abyśmy zachowywali ostrożność podczas korzystania z portalów społecznościowych, oraz żebyśmy regularnie aktualizowali nasze zabezpieczenia i świadomie podejmowali działania mające na celu ochronę naszych danych osobowych.

**II. Zagrożenia związane z udostępnianiem danych na portalach społecznościowych oraz negatywne konsekwencje nieuprawnionego wykorzystania, kradzieży tych danych**

Negatywne skutki kradzieży danych z portali społecznościowych mogą być bardzo dotkliwe, zwłaszcza jeśli chodzi o konkretne typy danych. Na przykład, w kontekście Facebooka, kradzież danych dotyczących statusu zatrudnienia, wykształcenia czy miejsca zamieszkania może prowadzić do szantażu lub kradzieży tożsamości. Szacuje się, że ok. 42% użytkowników portali społecznościowych zgłaszało próby kradzieży tożsamości po incydentach związanych z kradzieżą danych na portalach społecznościowych. Kradzież danych z LinkedIna również niesie ze sobą szereg negatywnych konsekwencji. Nasze informacje zawodowe, takie jak umiejętności, doświadczenie i kontakty biznesowe, mogą być wykorzystane do celów szpiegostwa przemysłowego lub czynów nieuczciwej konkurencji. Przestępcy mogą wykorzystać zdobytą wiedzę, aby uzyskać przewagę nad nami w środowisku zawodowym lub nawet doprowadzić do utraty zatrudnienia. Dodatkowo, skradzione dane mogą posłużyć do stworzenia fałszywych profili, co może wpłynąć negatywnie na naszą reputację zawodową i osobistą, a także stać się narzędziem do przeprowadzenia ataków phishingowych lub innych form oszustwa, w tym z udziałem naszych osób najbliższych.

Negatywne konsekwencje kradzieży danych z portali społecznościowych sięgają także aspektów społecznych naszego życia codziennego. Na przykład, skradzione zdjęcia z Instagrama mogą być wykorzystane do stworzenia fałszywych profili lub publikacji reklamowych bez naszej zgody. Może to prowadzić do zakłócenia naszej prywatności oraz obniżenia naszego poczucia bezpieczeństwa w świecie online. Jednym z istotnych aspektów wykorzystania skradzionych zdjęć jest ich nieuprawnione wykorzystanie w kontekście kampanii reklamowych. Przestępcy mogą korzystać z naszych prywatnych fotografii, aby promować produkty lub usługi bez naszej zgody. Mogą również tworzyć fałszywe profile na portalach społecznościowych, na których publikują reklamy wykorzystujące nasze zdjęcia, co może wpłynąć na naszą reputację oraz zaufanie naszych znajomych i osób z naszego kręgu społecznego (sieci społecznościowej). Skradzione zdjęcia mogą być również wykorzystywane przez algorytmy sztucznej inteligencji do różnych celów, włącznie z identyfikacją osób na zdjęciach czy analizą zachowań użytkowników. Jest to szczególnie niebezpieczne, ponieważ może prowadzić do dalszego naruszenia naszej prywatności i wykorzystania naszych danych osobowych w sposób, który jest niezgodny z naszymi intencjami. Algorytmy AI mogą wykorzystywać nasze zdjęcia do tworzenia profili psychologicznych lub do celów manipulacji emocjonalnej, co może mieć długotrwałe negatywne konsekwencje dla naszej psychiki i bezpieczeństwa emocjonalnego w sieci. W kontekście Facebooka oraz Instagrama istnieje także zagrożenie związane z wykorzystaniem naszych danych zawartych w komentarzach, postach i lajkach dla działalności przestępczej. Przestępcy mogą wykorzystać te informacje do manipulacji społecznej lub wyłudzeń. Na przykład, mogą analizować nasze komentarze i lajki, aby zidentyfikować nasze zainteresowania, preferencje zakupowe czy nawet nasze słabości. Następnie mogą wykorzystać te informacje do ukierunkowanych ataków phishingowych lub wyłudzeń, wysyłając fałszywe wiadomości lub reklamy, które są bardziej prawdopodobne do przyciągnięcia naszej uwagi i skłonienia nas do kliknięcia w szkodliwe linki lub udostępnienia poufnych informacji.

Należy również pamiętać, że nasze dane osobowe mogą zostać wykorzystane do popełnienia oszustwa finansowego na naszą szkodę, co może się wiązać z poważnymi konsekwencjami finansowymi, takimi jak utrata środków lub powstanie zobowiązania finansowe tj. kredyty, chwilówki zaciągane w naszym imieniu a także wpływać na obniżenie naszej wiarygodności kredytowej w przyszłości.

W rezultacie, kradzież danych z portali społecznościowych może prowadzić do poważnych konsekwencji zarówno dla jednostek, jak i społeczeństwa jako całości, dlatego tak istotne jest, abyśmy byli świadomi zagrożeń związanych z udostępnianiem danych osobowych w sieci oraz stosowali się do najlepszych praktyk zabezpieczających nasze konta i prywatność online.

**III. Jak zabezpieczyć się przed kradzieżą danych - opcje zabezpieczeń oferowane przez portale społecznościowe**

Aby zminimalizować ryzyko kradzieży danych na portalach społecznościowych, istnieje kilka podstawowych zasad, których warto przestrzegać.

1. **Opcje zabezpieczeń domyślne**: Większość portali społecznościowych, komunikatorów oraz innych platform internetowych, takich jak Facebook, LinkedIn, Instagram czy popularne komunikatory, oferuje domyślne opcje zabezpieczeń, które warto włączyć. Należą do nich m.in., najbardziej popularna, opcja dwuetapowej weryfikacja logowania, która wymaga podania dodatkowego kodu lub potwierdzenia przez aplikację mobilną podczas logowania z nieznanych urządzeń. To proste działanie znacząco zwiększa bezpieczeństwo konta, ponieważ nawet w przypadku przechwycenia hasła, intruz będzie musiał posiadać dodatkowy klucz weryfikacji;
2. **Zarządzanie uprawnieniami aplikacji**: Warto również regularnie sprawdzać i usuwać aplikacje, którym udzieliliśmy dostępu do naszych danych osobowych w komunikatorach. Możemy to zrobić poprzez ustawienia konta, sekcję "Ustawienia i prywatność" lub "Bezpieczeństwo" i "Uprawnienia aplikacji";
3. **Ustawienia prywatności**: Każdy komunikator oferuje opcje zarządzania ustawieniami prywatności, które pozwalają kontrolować widoczność naszych danych osobowych dla innych użytkowników. Warto regularnie przeglądać i dostosowywać te ustawienia w zależności od swoich preferencji i potrzeb. Możemy ograniczyć widoczność naszych danych osobowych tylko dla osób, które znajdują się na naszej liście kontaktów, grupie znajomych, co minimalizuje ryzyko ich nieuprawnionego wykorzystania przez osoby nieznane, nienależące do naszej sieci społecznościowej;
4. **Silne hasła**: Warto stosować również silne hasła do naszych kont w komunikatorach. Silne hasła powinny składać się z różnych znaków (małe i duże litery, cyfry, znaki specjalne) i być unikalne dla każdego konta. Możemy korzystać z menedżerów haseł, które pomagają nam zarządzać i generować bezpieczne hasła dla każdej platformy.
5. **Monitorowanie aktywności na koncie**: Warto regularnie sprawdzać aktywność na naszym koncie w social mediach oraz w komunikatorach, taką jak nieznane logowania czy podejrzane wiadomości. W przypadku otrzymania wiadomości od nieznanej osoby lub podejrzanego konta, należy zachować szczególną ostrożność i nie odpowiadać na nią. W razie podejrzeń o działania niezgodne z regulaminem, należy zgłosić i zablokować takie konto.
6. **Szkolenie w zakresie cyberbezpieczeństwa**: Warto korzystać z dostępnych materiałów edukacyjnych na temat cyberbezpieczeństwa oferowanych przez portale, komunikatory. Możemy nauczyć się, jak rozpoznawać zagrożenia online, jakie są najlepsze praktyki w zakresie ochrony danych osobowych i jak reagować na podejrzane działania w sieci.

Oprócz opcji zabezpieczeń oferowanych przez social media, istotne jest, abyśmy sami zwracali uwagę na nasze zachowanie w sieci. Musimy być świadomi, co klikamy, co komentujemy, co obserwujemy i z kim prowadzimy rozmowy w komunikatorach. Unikanie podejrzanych linków, ostrożność w

udostępnianiu danych osobowych oraz regularne monitorowanie swojego konta to kluczowe działania, które pomogą nam chronić naszą prywatność i bezpieczeństwo online

**IV. Jak reagować w przypadku kradzieży danych**

W przypadku kradzieży danych z profili społecznościowych oraz ich nieuprawnionego wykorzystywania, istotne jest szybkie i skuteczne działanie, zarówno ze strony podmiotu danych, czyli użytkownika konta, jak i organów ścigania. Oto kroki, które należy podjąć:

1. **Zmiana hasła i wylogowanie ze wszystkich urządzeń**: Po wykryciu podejrzanego działania należy niezwłocznie zmienić hasło do konta na platformie społecznościowej. Warto również skorzystać z funkcji "Wyloguj ze wszystkich urządzeń", jeśli taka opcja jest dostępna, aby zabezpieczyć swoje konto przed dalszym nieautoryzowanym dostępem.
2. **Zgłoszenie naruszenia prywatności do administratora platformy**: W przypadku Facebooka, LinkedIna, Instagrama i innych podobnych platform, istnieją mechanizmy zgłaszania naruszeń prywatności. Zazwyczaj można to zrobić poprzez opcję "Zgłoś naruszenie" lub "Skontaktuj się z nami" dostępną w ustawieniach konta. W treści zgłoszenia należy dokładnie opisać, co się stało, w jaki sposób dane zostały skradzione lub wykorzystane oraz jakie działania podjęto w celu zabezpieczenia konta.
3. **Zgłoszenie incydentu organom ścigania**: Jeśli podejrzewasz, że twoje dane osobowe zostały skradzione i są wykorzystywane w celach przestępczych, należy zgłosić ten fakt odpowiednim organom ścigania, takim jak policja, prokuratura czy organy zajmujące się ochroną danych osobowych (Prezes Urzędu Ochrony Danych Osobowych). W przypadku wyłudzeń majątkowych, zwłaszcza tych związanych z instytucjami bankowymi, można również skontaktować się z organem nadzoru finansowego.
4. **Monitorowanie aktywności na koncie**: Po zgłoszeniu incydentu, należy regularnie monitorować aktywność na swoim koncie w social mediach w celu wykrycia dalszych podejrzanych działań lub prób nieautoryzowanego dostępu.
5. **Zwrócenie się o pomoc do specjalistów od bezpieczeństwa IT**: Jeśli jesteś ofiarą kradzieży danych, warto skonsultować się z ekspertami od bezpieczeństwa IT, którzy mogą pomóc w zabezpieczeniu konta oraz śledzeniu działań przestępczych.
6. **Ostrzeżenie znajomych i kontaktów**: Warto poinformować swoich znajomych i kontakty na platformie społecznościowej o incydencie, aby unikali interakcji z nieautoryzowanymi publikacjami lub wiadomościami.

W przypadku poważnych naruszeń prywatności lub wykorzystania danych osobowych w celach przestępczych, organy ścigania mogą podjąć dalsze środki, włączając w to śledztwo oraz współpracę z dostawcami usług internetowych w celu ustalenia tożsamości sprawców. Ważne jest, aby w takich sytuacjach działać szybko i skutecznie, aby ograniczyć skutki kradzieży danych oraz zapobiec dalszym incydentom.

Dodatkowymi działaniami, w przypadku nieuprawnionego wykorzystywania danych, kradzieży w celu oszustwa finansowych, są:

7. **Zamrożenie lub monitorowanie konta bankowego**: Jeśli podejrzewasz, że twoje dane bankowe zostały skradzione lub są wykorzystywane w celach oszustwa finansowego, należy niezwłocznie skontaktować się z bankiem, aby zgłosić incydent. Bank może zarekomendować zamrożenie lub monitorowanie konta w celu zapobieżenia dalszym nieautoryzowanym transakcjom.
8. **Skontaktowanie się z biurem informacji kredytowej**: W przypadku, gdy twoje dane osobowe zostały wykorzystane do zaciągnięcia nieuprawnionych kredytów lub pożyczek, warto skontaktować się z biurem informacji kredytowej, aby zgłosić incydent i poprosić o

zamrożenie swojego raportu kredytowego. Może to pomóc w zapobieżeniu dalszym próbom wykorzystania twoich danych w celach finansowych.

9. **Konsultacja z prawnikiem**: Jeśli doszło do wyłudzeń majątkowych lub innych poważnych naruszeń prywatności, warto skonsultować się z prawnikiem specjalizującym się w sprawach związanych z cyberprzestępczością. Prawnik udzieli porady prawnej dotyczącej dalszych kroków, jakie można podjąć w celu ochrony swoich praw i interesów.

**V. Podsumowanie**

W obliczu rosnącego znaczenia portali społecznościowych w naszym codziennym życiu, ochrona danych osobowych staje się coraz bardziej kluczowa. Facebook, LinkedIn, Instagram - to tylko niektóre z platform, na których dzielimy się naszymi informacjami. Niemniej jednak, w miarę jak korzystanie z tych serwisów staje się powszechne, wzrasta również ryzyko kradzieży danych. Kradzież danych z portali społecznościowych może prowadzić do szeregu negatywnych konsekwencji, włączając w to szantaż, kradzież tożsamości, oszustwa finansowe i naruszenie prywatności. Dlatego tak ważne jest, abyśmy byli świadomi zagrożeń związanych z udostępnianiem danych osobowych online i podjęli odpowiednie środki ostrożności.

Mechanizmy kradzieży danych są różnorodne i często wyrafinowane, obejmując techniki phishingu, wykorzystanie luk w zabezpieczeniach oraz podejrzane aplikacje. Negatywne skutki kradzieży danych mogą być dotkliwe, zarówno dla jednostek, jak i społeczeństwa jako całości. Dlatego tak istotne jest, abyśmy stosowali się do najlepszych praktyk zabezpieczających nasze konta i prywatność online oraz reagowali szybko i skutecznie w przypadku incydentów kradzieży danych.

Opcje zabezpieczeń oferowane przez portale społecznościowe, takie jak dwuetapowa weryfikacja logowania, zarządzanie uprawnieniami aplikacji i ustawienia prywatności, mogą pomóc w zminimalizowaniu ryzyka kradzieży danych. Jednak równie ważne jest, abyśmy sami zachowywali ostrożność online, unikając podejrzanych linków, stosując silne hasła i regularnie monitorując aktywność na swoich kontach.

W przypadku kradzieży danych, należy niezwłocznie podjąć działania, takie jak zmiana hasła, zgłoszenie incydentu administratorowi platformy i organom ścigania, oraz monitorowanie aktywności na koncie. W przypadku wyłudzeń majątkowych, szczególnie z udziałem instytucji bankowych, ważne jest również skontaktowanie się z bankiem i biurem informacji kredytowej, oraz skonsultowanie się z prawnikiem specjalizującym się w cyberprzestępczości.

Ostatecznie, ochrona danych osobowych w świecie online wymaga wspólnego wysiłku użytkowników, platform społecznościowych i organów ścigania. Współpraca i świadomość zagrożeń są kluczowe w zapewnieniu bezpieczeństwa naszych danych osobowych i prywatności w sieci.

**Paweł Wojciechowski** – adwokat, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.