

Kradzież danych osobowych - jakie mogą być konsekwencje kradzieży lub wyłudzenia danych?

Jak mówią niektórzy lekarze - profilaktyka jest ważniejsza niż leczenie. Podobnie jest z danymi osobowymi. Przede wszystkim należy dbać o bezpieczeństwo i chronić je. Ale czy wiesz gdzie i kiedy może dojść do ich pozyskania w celach przestępczych? Sprawdź, jakie mogą być konsekwencje kradzieży danych osobowych w Internecie.



Wyobraź sobie dzień, w którym policja zapuka do twoich drzwi. Na przykład za oszukanie kilkuset osób, wyłudzenie od nich pieniędzy lub niespłacanie zaciągniętych w bankach kredytów. Policja ma dowody mimo że nic złego nie zrobiłeś.

Do kradzieży tożsamości dochodzi niemal na całym świecie. Głośna była sprawa policjanta, który ukradł tożsamość kobiecie, aby kontaktować się z nieznanymi kryminalistami. Za pomocą jej danych i zdjęcia stworzył konto na Facebooku i rozpracowywał szajkę narkotykową. Sprawa wyszła na jaw, gdy prawdziwi znajomi Amerykanki zaczęli pytać o dziwne rzeczy pisane na jej tablicy. Tymczasem ona nigdy nie zakładała konta w tym serwisie. Ten przypadek był niebywałym przekroczeniem uprawnień. Jak się okazuje, kradzież tożsamości może być o wiele groźniejsza. Bo dokonywana w jednoznacznie przestępczym celu.

Zjawisko kradzieży tożsamości istnieje już od wielu lat, ale przestępcy mają coraz szersze możliwości. Wszystko dzięki temu, że coraz więcej spraw załatwiamy za pomocą internetu, a przy tym zapominamy nawet o podstawowych zasadach bezpieczeństwa. Zanim jednak sieciowy kabel trafił do naszych domów, przestępcy kradli nasze dane zaglądając do skrzynek pocztowych i przechwytywali naszą pocztę.

W Polsce zjawisko to z każdym rokiem przybiera na sile. – O kradzieży tożsamości możemy mówić zarówno w sytuacji, gdy ktoś bez naszej wiedzy uzyska dostęp do naszego konta na portalu społecznościowym i opublikuje wpis w naszym imieniu, jak i wtedy, gdy zapłaci naszą kartą kredytową za zakupy w sieci – mówi w rozmowie z naTemat Kamil Sadkowski, analityk zagrożeń z laboratorium ESET.

Przestępcy znają nasze słabości i są dobrze przygotowani do tego, aby osiągać swoje cele. Wykorzystują techniki inżynierii społecznej, które wykorzystują nasze najsłabsze punkty. Nasza niewiedza i naiwność sprawiają, że często dajemy się zmanipulować i na przykład wypełnić stronę ładując podobną do tej, która należy do naszego banku. Powinniśmy także zwracać uwagę na ogłoszenia o pracę, na które odpowiadamy wysyłając swoje CV. Może się okazać, że firma nie istnieje a ogłoszenie jest jedynie wędką, która łapie nasze dane osobowe.

Za najskuteczniejsze metody zabezpieczeń uważa się te, oparte na naszych cechach biometrycznych, takich jak odcisk palca. O ile instytucje finansowe oferują nam coraz lepsze zabezpieczenia, to często sami ułatwiamy wykradanie naszej tożsamości, podając swoje dane w odpowiedzi na sprytnie przygotowanego maila, choćby dotyczącego "nagłej weryfikacji danych" przez

bank. Hasła, zdraпки, tokeny - wszystkie te zabezpieczenia potrafią nie zadziałać, jeśli zawiedzie najważniejsze - nasza czujność i rozsądek.

Możliwości pozyskania danych osobowych niestety jest wiele. Często sami podsuwamy nasze dane złodziejom, np. wyrzucając na śmietnik niezniszczone dokumenty czy nośniki danych, korzystając z Internetu i zostawiając dane w wielu miejscach, kupując, subskrybując, szukając pracy, biorąc udział w konkursach czy wypełniając ankiety. Z pewnością nikt wtedy nie myśli o potencjalnej kradzieży tożsamości.

Jeśli ktoś ukradnie Ci dowód osobisty to sprawa wydaje się oczywista, ale czy zastanawiałeś się ile razy sam dajesz swój dowód osobom, które w ogóle nie mają prawa o niego prosić?

Warto zapoznać się z sytuacjami, w których powinienes okazać dowód i tymi, w których nie masz takiego obowiązku.

Niejednokrotnie bywa, że to co miało ułatwiać nam funkcjonowanie, staje się polem do działalności przestępców. Tak też jest w przypadku sieci Wi Fi, przez którą ktoś może ukraść naszą tożsamość w zaledwie kilku minut. Wystarczy, że w tej samej kawiarni co my będzie siedział haker podłączony do Wi Fi. Dzięki temu, będzie w stanie śledzić nasze ruchy w internecie, pozwać hasła i inne dane wypełnianych przez nas formularzy.

Kto może prosić o okazanie dowodu osobistego?

O Twój dowód może Cię poprosić tylko:

- Policja
- pracownicy inspekcji handlowej w ramach kontroli
- pracownicy kontroli skarbowej w ramach kontroli skarbowej
- pracownicy Zakładu Ubezpieczeń Społecznych podczas kontroli
- funkcjonariusze Straży Granicznej
- funkcjonariusze Biura Ochrony Rządu
- funkcjonariusze Służby Więziennej
- pracownicy ochrony osób i mienia
- sprzedawcy alkoholu
- strażnicy leśni
- osoby działające w imieniu zarządcy drogi
- pracownicy hoteli

Przedstawiciel żadnej innej instytucji nie może odebrać Ci dowodu tożsamości, ani w celu spisania danych, wykonania kserokopii, ani tym bardziej jako „zastaw” w zamian za wypożyczenie sprzętu sportowo turystycznego.

Co dzieje się z naszą tożsamością?

To, co przestępca zrobi z naszą tożsamością, zależy od ilości danych które nam wykradł. Najgorszym zestawem są nasze dane osobowe w połączeniu z dostępem do naszego konta bankowego. Podszywający się pod nas może na przykład założyć konto na serwisie aukcyjnym (może też wykraść nasze) lub nawet założyć sklep internetowy. Pieniądze za sprzedane, lecz nieistniejące przedmioty trafiają na nasze konto, a później są przesyłane dalej, czyli na konta przestępców. O tym, że zrobiono z nas przestępców dowiadujemy już wtedy, gdy do naszych drzwi zapuka policja. Lub windykatrzy.

Właśnie to spotkało wiele osób. Oszuści wzięli na cel osoby szukające pracy. W czasie internetowej "rekrutacji" poprosili o skan dowodu osobistego oraz o przelew minimalnej kwoty na "firmowe" konto. Jak się wkrótce, ale już za późno, okazało, chodziło o założenie konta na odległość w jednym z banków. Kontakt z firmą się oczywiście urwał. Zaczęły za to przychodzić wezwania do zapłaty rat licznych kredytów.

Do czego złodziejom potrzebne są nasze dane?

Pomysłowość osób chcących wykorzystać skradzione dane nie zna granic. Oto przykłady na wykorzystanie cudzej tożsamości:

- podrobienie dowodu w celu realizacji różnych czynności prawnych
- prowadzenie fałszywej działalności biznesowej w imieniu okradzionego i wyłudzenia np. zwrotu podatku
- wyłudzenie kredytu
- założenie konta bankowego
- wynajęcie mieszkania lub pokoju hotelowego w celu kradzieży wyposażenia
- kradzieży wypożyczonego samochodu i innych przedmiotów
- zawarcie umowy z operatorem telekomunikacyjnym
- dokonywanie różnego rodzaju zakupów
- wciągnięcie w proces prania brudnych pieniędzy
- mandat lub rachunek na konto okradzionego
- założenie fałszywego konta internetowego lub fałszywego profilu

- umieszczanie w sieci bądź dystrybucja obraźliwych opinii lub komentarzy

Jedną z najbardziej dotkliwych konsekwencji kradzieży tożsamości jest wyłudzenie kredytu, czy pożyczki. Okradziony o wszystkim dowiaduje się dopiero, gdy otrzyma wezwanie do zapłaty lub telefon z firmy windykacyjnej.

Ze złodziejami tożsamości nie ma żartów. Konsekwencje ich działalności mogą być dla Ciebie bardzo dotkliwe, dlatego warto być czujnym i zawczasu wzmocnić ochronę, zakładając konto w BIK. W razie kradzieży dowodu osobistego będziesz mógł w kilka chwil zastrzec go i „wyprzedzić złodzieja”.