Czym grozi nieprzemyślane ujawnianie danych osobowych?

Pomysłowość złodziei danych osobowych nie zna granic. Mogą podszyć się pod Twój bank, firmę szukającą pracowników albo sklep internetowy. Nieuważny internauta łatwo da się nabrać i udostępni oszustom wszystkie informacje, o które poproszą. Nie wszyscy oszuści są równie wyrafinowani - stosują złośliwe oprogramowanie, przekupują pracowników różnych instytucji lub po prostu… kradną portfele i torebki.

Do czego jednak potrzebne są im Twoje dane osobowe? Możliwości ich wykorzystania jest równie dużo, co metod kradzieży – złodziej może na przykład…

Zaciągnąć kredyt

Spłata cudzego kredytu to najczęstszy problem ofiar cyberprzestępców. Wystarczy, że złodziej uzyska dane z Twojego dowodu, a będzie mógł zaciągnąć nawet sporą pożyczkę przez Internet lub w firmie udzielającej chwilówek. Okradziony o wszystkim dowiaduje się dopiero, gdy otrzyma wezwanie do zapłaty lub telefon z firmy windykacyjnej...

Wynająć mieszkanie

Twój dokument tożsamości to w rękach „uczciwego znalazcy" sposób, by przez jakiś czas pomieszkać w dużym mieszkaniu w dobrej dzielnicy. Kulturalny oszust przynajmniej nie zdemoluje lokalu, ale nigdy nie wiadomo, co podpowie mu fantazja. Kto za to zapłaci? No właśnie…

Podzwonić za darmo

Jeden złodziej wynajmie mieszkanie, drugi zafunduje sobie nowy smartfon z drogim abonamentem. Na Twoje konto obdzwoni wszystkich znajomych, weźmie udział w zabawie audiotele albo odwiedzi kilka stron internetowych – niekoniecznie legalnych. A Ciebie zostawi z wysokim rachunkiem i problemami z policją.

Zrobić duuuuże zakupy

Drogi zegarek, wymarzony rower i ciuchy najmodniejszych marek? A kto bogatemu zabroni? Cudze pieniądze wydaje się najłatwiej, a dane kart kredytowych, niestety, czasem można zdobyć łatwiej niż prognozę pogody na jutro. Lepiej je dobrze chronić – chyba że chcesz sfinansować komuś spełnienie marzeń.

Przespać się w dobrym hotelu

Kiedy ostatnio spałeś w pięciogwiazdkowym hotelu? Złodziej na pewno nie będzie chciał oszczędzać, a jeśli na Twoim koncie znajdzie się odpowiednia kwota, na nocleg wybierze najdroższe miejsce. Wystarczy, że w recepcji poda Twoje dane.

Namieszać w twoim życiu

Przy odrobinie szczęścia uzyska też Twoje dane do logowania w mediach społecznościowych lub poczcie elektronicznej. Po udanych zakupach, usiądzie wygodnie ze szklaneczką dobrego alkoholu (kto stawia?) i trochę się pobawi. Wyśle do Twojego szefa obraźliwego maila, wrzuci na Facebooka kompromitujące zdjęcie i w niewybredny sposób skomplementuje teściową. Na przykład.

Zarobić na Twoich sekretach

Zabawa będzie tym lepsza, jeśli przy okazji pozna Twoje wstydliwe tajemnice. Najpewniej nie upubliczni ich od razu, bo będzie wiedział, że wolałbyś nie chwalić się nimi przed żoną, rodzicami i szefem. I zaproponuje Ci układ. On milczy, Ty płacisz. Cyberprzestępcy nie mają żadnych skrupułów, a szantaż to dla nich kolejna metoda na wyłudzenie dodatkowych pieniędzy.

Sprzedać Twoje dane

Co godzinę odbierasz telefon od telemarketera, a Twoją skrzynkę pocztową bombardują reklamy łatwych sposobów na zarobek i środków na potencję? Przypomnij sobie, czy nierozważnie nie podałeś gdzieś swoich danych kontaktowych. To obecnie cenny towar, a różne firmy są gotowe sporo za nie zapłacić. Irytacja to jednak najmniejszy problem, bo spam może zawierać też niebezpieczne załączniki.

Jak uchronić się przed wyłudzeniem?

Pełna ochrona przed kradzieżą danych jest trudna. Jednak kilka prostych zasad pomoże ustrzec się przed wyłudzeniem pożyczki zaciągniętej na nasze konto. Co warto zatem zrobić? Postępuj zgodnie z zasadą, że łatwiej zapobiegać niż leczyć, dlatego:

Chroń swoje dane osobowe w sieci – dostałeś e-mail z banku prośbą o potwierdzenie danych z dowodu osobistego, bo w innym przypadku Twoje konto zostanie zablokowane? – nie daj się nabrać! Bank ani inna instytucja finansowa w żadnym przypadku nie wyśle takiej informacji. Jeśli otrzymałeś taką wiadomość to masz pewność, że ktoś chce wykraść Twoje dane.

Pilnuj dokumentów – dowód osobisty miej zawsze przy sobie.

Ktoś ukradł Ci dokumenty? Zgłoś to koniecznie na policję! – Każdą kradzież dowodu osobistego lub innych dokumentów potwierdzających tożsamość, które mogą być podstawą udzielenia pożyczki trzeba zgłosić do organów ścigania.

Zgubione lub skradzione dokumenty trzeba koniecznie zastrzec w banku. W zależności od placówki można to zwykle zrobić albo online lub telefonicznie albo bezpośrednio w oddziale banku. Zastrzeżony dokument trafia do Centralnej Bazy Danych Systemu Dokumentów Zastrzeżonych, który należy do Związku Banków Polskich. Dzięki temu można zdecydowanie ograniczyć wykorzystanie dowodu osobistego jako źródła przestępstwa.

Chcesz wziąć pożyczkę? Korzystaj tylko z zaufanych firm pożyczkowych. W sieci można natknąć się na fałszywe strony internetowe, które stworzone są tylko po to, żeby wykraść dane osobowe. Ważne jest sprawdzenie m.in. czy nazwa firmy pożyczkowej nie zawiera literówek oraz czy witryna, z której korzystamy jest bezpieczna (klikając w kłódkę na pasku można sprawdzić czy połączenie jest bezpieczne). Dobrym rozwiązaniem jest korzystanie z renomowanych porównywarek ofert firm pożyczkowych. Na stronie https://sowafinansowa.pl/ można sprawdzić nie tylko opinie o pożyczkodawcy, porównać różne oferty pożyczkowe, ale również bezpośrednio przejść do składania wniosku o pożyczkę. Dodatkowo porównywarka pozwala szybko znaleźć promocyjne oferty: pierwsza pożyczka za darmo według sowafinansowa.pl to informacje, które pozwolą zaoszczędzić spore pieniądze i uzyskać finansowanie bez odsetek czy prowizji.

Co zrobić w przypadku wyłudzenia pożyczki na nasze dane?

Przede wszystkim liczy się czas. W przypadku utraty dokumentów należy:

zgłosić kradzież dokumentów na Policję,

zgłosić utratę dokumentów w urzędzie gminy i złożyć wniosek o wydanie nowego dowodu osobistego – aktualnie wniosek o e-dowód czyli dowód osobisty z warstwą elektroniczną można złożyć przez Internet albo w dowolnym urzędzie gminy bez względu na miejsce zamieszkania,

zastrzec dowód osobisty w banku,

wystąpić do firmy pożyczkowej z informacją, że pożyczka została wyłudzona w oparciu o skradziony albo w inny sposób utracony dowód osobisty.

To po stronie osoby, której dane zostały użyte do zawarcia umowy pożyczki leży konieczność udowodnienia, że pożyczka została udzielona w ramach przestępstwa. Szybkie zgłoszenie kradzieży dokumentów, zastrzeżenie dowodu czy wskazanie, że pieniądze nie zostały wpłacone na konto pokrzywdzonego to dowody, które potwierdzają, że pożyczka trafiła w nieuprawnione ręce.

Przezorny zawsze ubezpieczony – to przysłowie może również znaleźć zastosowanie w przypadku ochrony przed nieuprawnionym wykorzystaniem danych osobowych, choćby w celu wyłudzenia pożyczki czy kredytu. Tym bardziej, że działania prewencyjne dość łatwo wdrożyć.

Korzystasz z różnych usług internetowych. Większość z nich wydaje się darmowa. Jednak to, że nie musisz wydawać pieniędzy, nie oznacza, iż nie ponosisz żadnych kosztów. Za wszystko płacisz swoimi danymi. Twoja aktywność w sieci jest zapamiętywana i analizowana. Strony, z których korzystasz, używają ciasteczek (ang. cookies), czyli specjalnych plików zapisywanych na Twoim komputerze. Część z nich jest niezbędna do tego, by prawidłowo wyświetlać stronę bądź umożliwić Ci logowanie; wiele służy jednak do obserwowania tego, co robisz w Internecie. Do śledzenia Twojej aktywności w sieci są wykorzystywane nie tylko ciasteczka.

Wiedza na temat Twoich działań w sieci służy różnym podmiotom do różnych celów. E-marketerzy interesują się tym, z jakich korzystasz usług i produktów, by dopasowywać określone reklamy. Pracownicy banku, ubezpieczyciele czy potencjalny pracodawca przeglądają zawartość Twojego konta w profilu społecznościowym, by sprawdzić Twoją wiarygodność. Państwo interesuje się tym, czy możesz stanowić zagrożenie dla bezpieczeństwa publicznego.

Tak jak inne osoby korzystające z Internetu podlegasz profilowaniu. To mechanizm, który polega na kategoryzowaniu ludzi według cech i zachowań. Z profilowaniem spotkasz się np. na Facebooku, który zapamiętuje historię Twoich „lajków", by zaprezentować reklamę targetowaną, oraz w rozmaitych serwisach książkowych, filmowych czy muzycznych. Ich działanie opiera się na analizie decyzji użytkowniczek i użytkowników: zostaną Ci zaproponowane te tytuły, które wcześniej wybrały osoby sprofilowane jako podobne do Ciebie. Owszem, to bywa przydatne, ale zawsze ogranicza. Jeżeli na przykład korzystasz z serwisu randkowego i zbytnio zaufasz systemowi, zapewne stracisz szansę na poznanie kogoś interesującego, ale całkowicie różniącego się od Ciebie.

W zależności od tego, czy szukasz czegoś za pomocą szkolnego komputera, czy też swojego laptopa, otrzymujesz inne rezultaty. Znajdujesz się w tzw. bańce filtrującej (ang. filter bubble) — większość wyszukiwarek (np. Google, Bing) dopasowuje określone wyniki, bazując na historii zapytań. Ma to służyć to Twojej wygodzie — i sprawdza się dobrze, gdy musisz zlokalizować pobliską pizzerię, ale w wielu sytuacjach może zawęzić zestaw odpowiedzi. Jeśli często szukasz w sieci informacji o wycieczkach zagranicznych, to po wpisaniu w wyszukiwarkę hasła „Turcja" możesz nie otrzymać ważnych informacji o odbywających się tam protestach. Będzie Ci również trudniej znaleźć opinie na dany temat, które — według systemów profilujących — różnią się od Twoich. To może zawęzić Twoje horyzonty.

Można niwelować negatywne skutki profilowania w sieci. Warto na przykład używać wyszukiwarek niewykorzystujących mechanizmu profilowania, a z Internetu korzystać po wylogowaniu z konta Google czy portali społecznościowych (więcej informacji w materiale pomocniczym „Jak się wydostać z bańki filtrującej" (ODT, DOC)).

Z profilowaniem spotkasz się nie tylko w sieci. Ludzie mogą być profilowani także przez państwo — i choć ma to miejsce w imię zwiększenia bezpieczeństwa, paradoksalnie bywa bardzo niebezpieczne. W USA na czarną listę pasażerów trafiają małe dzieci, które nazywają się tak samo lub podobnie jak osoby podejrzane o popełnienie przestępstwa. Nie mamy żadnego wpływu na interpretację informacji na nasz temat — w Wielkiej Brytanii organy ścigania oznaczały pasażerów linii lotniczych zamawiających wegetariański posiłek (!) jako osoby, które w przyszłości mogą zagrozić bezpieczeństwu państwa. Zastanów się: skoro przy profilowaniu pomylić się może policja bądź inne służby — to tym bardziej wyszukiwarka internetowa.

Handel danymi osobowymi. Ile kosztuje twoje nazwisko?

Firmy marketingowe handlują naszymi nazwiskami i numerami telefonów. Każdy kontakt do potencjalnego klienta jest towarem, który można sprzedać po cenie od kilkudziesięciu groszy do ponad 100 zł. To że nasze dane osobowe znajdują się w obrocie handlowym, to zazwyczaj nasza wina - bo sami wyraziliśmy na to zgodę.

Aby zdobyć informacje o klientach, firmy imają się przeróżnych sposobów. Ostatnio modne są konkursy internetowe, w których kuszą atrakcyjnymi nagrodami, np. tabletami lub samochodami. Aby wziąć udział w losowaniu, wystarczy wypełnić ankietę i wyrazić zgodę na przetwarzanie i udostępnianie danych osobowych.

Nagrody wygrywa niewielu, za to prawie każdy z uczestników może być pewien, że zacznie dostawać telefony, SMS-y i e-maile od mniej lub bardziej namolnych marketerów.

Twoja głowa kosztuje kilkadziesiąt groszy

Samo nazwisko połączone z numerem telefonu, adresem czy wiekiem danej osoby nie stanowi dziś na rynku dużej wartości. Jak czytamy w tygodniku, ceny wahają się między 50 a 80 gr za rekord, a w przypadku dużych zamówień spadają nawet do 10 gr.

O wiele cenniejsze są zatem bazy danych zawierające wyselekcjonowane kontakty, zwłaszcza tzw. leady. Są to kontakty do osób, które już wykazały zainteresowanie danym produktem czy usługą. I tak banki szukają zainteresowanych zaciągnięciem kredytu, a dilerzy samochodowi osób planujących wymianę samochodu

Jednym ze sposobów zdobywania danych o zachowaniach konsumentów z przypisaniem do konkretnych nazwisk są programy lojalnościowe. Zbierając w nich punkty jednocześnie pozostawiamy informacje na temat naszych zakupów, upodobań i stylu życia. Ostatnio nawet brytyjskie media określiły karty lojalnościowe jako "szpiegów w portfelu klienta". W internecie wiele informacji o klientach zbiera się poprzez serwisy społecznościowe i pliki cookies.

Okazuje się jednak, że firmy nie potrzebują nawet naszej współpracy, by zdobyć o nas imponująca wiedzę. Firma Schober chwali się, że posiada dane dotyczące wieku, płci i poziomu zamożności dotyczące 11,5 mln gospodarstw domowych, czyli ok. 37 mln Polaków.

Jak mówi szefowa firmy Magdalena Brzeska bazę opracowano m.in. na podstawie "badań rynku, danych GPS i innych anonimowych danych statystycznych".

Trzeba jednak pamiętać, że choć firmy marketingowe wiedzą o nas coraz więcej, to jednak nie zawsze ich działania są zgodne z prawem. Liczba skarg wpływających do GIODO na niezgodne z prawem przetwarzanie danych osobowych wzrosła w 2012 r. o dwadzieścia kilka proc. w porównaniu do poprzedniego roku.

Za nielegalny handel danymi osobowymi grozi do dwóch lat więzienia.

Mateusz Szpunar kl. II LO