



Kradzież tożsamości

Podstawowe wskazówki

Poznaj fakty

W dzisiejszych czasach nie istnieje coś takiego, jak zbyt ostrożność, jeśli chodzi o ochronę tożsamości.

Złodzieje tożsamości kradną dane osobowe, takie jak numery Social Security, numery kont bankowych i kredytowych, które mogą wykorzystać do uzyskania kredytu, robienia zakupów, a nawet uzyskania polis ubezpieczeniowych na twoje nazwisko. Wyniki mogą być katastrofalne: tysiące dolarów rachunków za cudze zakupy, zrujnowana historia kredytowa; naprawienie takiej sytuacji może potrwać miesiące lub lata.

Współcześni złodzieje tożsamości wysyłają oszukańcze emaily podając się za prawdziwe firmy, agencje rządowe - czasem nawet znajomych i krewnych - starając się skłonić konsumentów do ujawnienia danych, pozwalających na ustalenie tożsamości.

Chroń dane osobowe przed kradzieżą

Możesz zabezpieczyć się przed kradzieżą tożsamości na wiele sposobów:

- W żadnym wypadku nie przekazuj informacji umożliwiających ustalenie tożsamości przypadkowo dzwoniącej osobie, czy też w odpowiedzi na email z banku, od znajomego lub krewnego bez uprzedniego skontaktowania się ze źródłem informacji i potwierdzenia, że email jest prawdziwy i ustalenia, do czego taka osoba lub bank potrzebuje tych informacji. Nie ufaj natychmiast numerom telefonu zamieszczonym w przypadkowych emailach czy wyświetlających się na identyfikatorze rozmowy; potwierdź niezależnie autentyczność numerów.
- Monitoruj swoją historię kredytową: Prawo federalne wymaga, aby trzy główne biura informacji kredytowej - Equifax, Experian i TransUnion - udostępniały ci darmową kopię raportu kredytowego raz w roku. Zamawiając regularnie egzemplarz z tych agencji upewnisz się, że nikt nie otwiera kont kart kredytowych i nie zaciąga pożyczek na twoje nazwisko.
- W żadnym wypadku nie zamieszczaj danych pozwalających na ustalenie tożsamości na Internecie, chyba że istnieje ku temu uzasadniony powód i masz pewność, że witryna internetowa jest bezpieczna. Zanim kupisz coś na Internecie płacąc kartą kredytową, potwierdź tożsamość, fizyczny adres i numer telefonu sprzedawcy na wypadek ewentualnych problemów w przyszłości. Szukaj symboli oznaczających, że strona internetowa jest bezpieczna. Sprawdź, czy nie ma skarg na danego sprzedawcę. FTC zaleca: „Jeżeli otrzymasz email lub wiadomość wyskakującą z prośbą o przekazanie informacji finansowych w trakcie przeglądania Internetu, nie odpowiadaj na nią i nie klikaj na link. Uczciwe firmy nie proszą w ten sposób o informacje”.
- Aby uniknąć złośliwego oprogramowania, pamiętaj:
 - Nigdy nie klikaj wiadomości wyskakujących;
 - Nigdy nie klikaj linków w podczepionych plikach, chyba że wiesz, że źródło ich jest rzetelne;
 - Stosuj zabezpieczenia firewall, programy antywirusowe i antyszpiegowskie i uaktualniaj regularnie to oprogramowanie a ponadto
 - Rozmawiaj o bezpiecznych zasadach korzystania z Internetu ze swoimi dziećmi.
- Dokumenty zawierające dane osobowe należy zniszczyć w niszczarce przed ich wyrzuceniem.
- Nie noś w portfelu karty social security.
- Stosuj silne, unikatowe hasła dla wszystkich kont internetowych i okresowo zmieniaj te hasła. W żadnym wypadku nie udostępniaj nikomu swoich haseł.



Stan Connecticut
Prokurator generalny William Tong

Kradzież tożsamości

Podstawowe wskazówki

Jeżeli padniesz ofiarą kradzieży tożsamości

- Skontaktuj się z bankami i firmami wydającymi karty kredytowe.
- Umieść ostrzeżenie o oszustwie (fraud alert) i/lub bardziej rygorystyczne „zamrożenie dla celów bezpieczeństwa” („security freeze”) na raporcie kredytowym.
 - Możesz skontaktować się z jedną z głównych agencji informacji kredytowej i umieścić ostrzeżenie o oszustwie w swoim raporcie kredytowym, a wówczas taka agencja skontaktuje się z dwiema pozostałymi. Umieszczenie takiego ostrzeżenia powoduje, że każda firma ma obowiązek potwierdzenia twojej tożsamości przed udzieleniem kredytu na twoje nazwisko. Ostrzeżenia o oszustwach są bezpłatne i pozostają w mocy przez 90 dni, chyba że odnowisz takie ostrzeżenie.
 - Jeżeli wolisz wprowadzić bardziej rygorystyczne zamrożenie do celów bezpieczeństwa na raporcie kredytowym, musisz skontaktować się w tej sprawie indywidualnie z wszystkimi trzema agencjami informacji kredytowej. Agencje informacji kredytowej mogą wymagać opłaty za wprowadzenie i wycofanie zamrożenia dla celów bezpieczeństwa, ale po wprowadzeniu takiego zamrożenia agencje informacji kredytowej nie mogą ujawnić żadnych informacji na twój temat potencjalnym kredytodawcom bez twojej wyraźnej zgody.
- Zgłoś sprawę na policję. Przepisy stanu Connecticut umożliwiają ofiarom kradzieży tożsamości zgłaszanie porządku tożsamości organom porządku publicznego w miejscu zamieszkania i uzyskanie kopii takiego raportu.
- Jeżeli twoje dane osobowe zostały naruszone w Internecie, skontaktuj się z Centrum Skarg na Przestępstwa Internetowej (Internet Crime Complaint Center) i złóż skargę pod adresem: www.ic3.gov.

Źródła

- Możesz uzyskać bezpłatne kopie raportu kredytowego z wszystkich trzech głównych biur informacji kredytowej pisząc do: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Koniecznie musisz zaznaczyć, z którego biura chcesz uzyskać taki raport, albo skorzystać z formularza dostępnego pod adresem <http://www.consumer.ftc.gov/articles/0155-free-credit-reports>. Możesz również odwiedzić witrynę www.annualcreditreport.com lub zadzwonić pod numer 1-877-322-8228.
- Te trzy biura zapewniają bezpłatne doroczne raporty kredytowe **wyłącznie** poprzez witrynę annualcreditreport.com, telefonicznie pod numerem 1-877-322-8228 lub wysłanie listu do: Annual Credit Report Request Service.
- W sprawach innych niż uzyskanie bezpłatnego raportu można kontaktować się z biurami bezpośrednio korzystając z następujących informacji:

Equifax
1-888-766-0008
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-888-4213
www.transunion.com



Stan Connecticut
Prokurator generalny William Tong

Kradzież tożsamości

Podstawowe wskazówki

- Można również zgłosić skargę do Jednostki Pomocy Konsumentom przy Urzędzie Prokuratora Generalnego (Office of the Attorney General Consumer Assistance Unit), wypełniając formularz na stronie www.ct.gov/ag.

Ostatnia aktualizacja: 13 grudnia 2021 r.