Drogi mieszkańcu Nowego Jorku!

Pana/i tożsamość jest zagrożona. Oszuści łatwiej niż kiedykolwiek mogą wykraść Pana/i dane osobowe przez Internet, telefon, a nawet osobiście i wykorzystać je do popełnienia oszustwa.

Każdego roku ofiarą kradzieży tożsamości padają miliony osób. Oszuści ubiegają się o karty kredytowe w Pana/i imieniu, otrzymują świadczenia medyczne, a nawet wykorzystują Pana/i numer Social Security (ubezpieczenia społecznego) do oszustw podatkowych, co szkodzi Pana/i wiarygodności kredytowej, a naprawa tego stanu rzeczy jest czasochłonna i kosztowna.

Przy odrobinie wysiłku może Pan/i zabezpieczyć swoje dane osobowe i zapobiec większości form kradzieży tożsamości, a my pomożemy Panu/i dowiedzieć się, jak to zrobić.

Po więcej informacji na temat zabezpieczenia swojej tożsamości lub co zrobić, jeśli uważa Pan/i, że Pana/i tożsamość została skradziona, należy odwiedzić naszą stronę internetową pod adresem ag.ny.gov.

Z poważaniem,

Letitia James

Prokurator Generalny
Stanu Nowy Jork
Letitia James

Źródła pomocy

Biuro Prokuratora Generalnego stanu Nowy Jork, Urząd ds. Oszustw Konsumenckich

Zgłaszanie oszustw lub składanie skarg.

(800) 771-7755 / ag.ny.gov

Federalna Komisja Handlu

Zgłaszanie oszustw lub kradzieży tożsamości.

877- 382-4357 / ftc.gov

Zgłaszanie oszustw lub kradzieży tożsamości

Aby sprawdzić lub zamrozić swoje raporty kredytowe.

877-322-8228 / annualcreditreport.com

Główne agencje informacji kredytowej

Experian:
(888) 397-3742 / experian.com

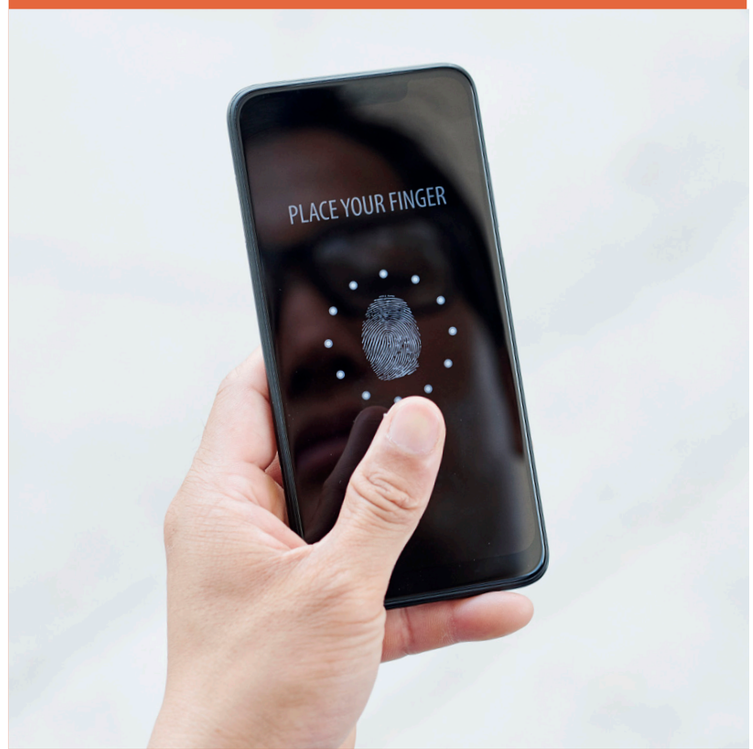
TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

Zabezpiecz swoją tożsamość

Wskazówki jak zachować bezpieczeństwo swojej tożsamości



Biuro Prokuratora Generalnego
stanu Nowy Jork
Letitia James

Zabezpieczenie danych osobowych

Podawanie imienia i nazwiska lub numeru telefonu jest na ogół bezpieczne, ale podawanie innej osobie daty urodzenia, numeru ubezpieczenia społecznego lub dowolnego numeru konta może narażać użytkownika na kradzież tożsamości. Należy również unikać ujawniania stronom internetowym żadnych informacji stosowanych jako odpowiedzi „zapasowe", gdy zapomniał/a Pan/i hasła.

Nigdy nie należy przekazywać swoich danych osobowych osobie, która przypadkowo się z Panem/ią kontaktuje: istnieje szansa, że osoba ta chce coś od Pana/i „wyłudzić", chyba że to Pan/i zainicjował/a ten kontakt.

Wyłudzanie informacji (phishing) to próba nakłonienia ofiary do podania danych osobowych, takich jak nazwa użytkownika, hasło lub numer karty kredytowej. Oszuści mogą się z Panem/ią kontaktować przez telefon lub e-mail i często podszywają się pod agencję rządową, bank lub znaną firmę. Będą żądać od Pana/i danych osobowych, aby rozwiązać jakiś problem lub pilną sprawę, lub powiedzą, że wystarczy „potwierdzić swoje informacje", zanim będą mogli Panu/i coś przekazać.

Żadna z tych organizacji w rzeczywistości nie skontaktowałaby się z Panem/ią w ten sposób, aby uzyskać ważne informacje. Jeśli nie ma Pan/i pewności, należy zadzwonić do tej instytucji korzystając z opublikowanych numerów telefonu, aby sprawdzić, czy to rzeczywiście oni. Niektóre próby wyłudzenia informacji każą przejść na stronę internetową lub otworzyć załącznik. Nie należy pobierać załączników ani klikać na łącza od osób, których Pan/i nie zna. Mogą one zawierać wirusy, które zainfekują Pana/i komputer i wykradną Pana/i dane osobowe.

Podejrzane wiadomości

Nawet jeśli wiadomość wydaje się pochodzić z zaufanego źródła, takiego jak krewny lub znana firma, może to być próba wyłudzenia informacji: oszuści mogli przejąć konto lub utworzyć nowe o podobnej nazwie. Jeśli otrzyma Pan/i wiadomość, która nie brzmi jakby została wysłana przez nadawcę, zawiera tylko link lub załącznik bez żadnego wyjaśnienia lub w inny sposób wydaje się podejrzana, należy sprawdzić dwukrotnie pole „od", aby upewnić się, że zwiera poprawny adres, lub zadzwonić do nadawcy, aby sprawdzić, czy wiadomość rzeczywiście od niego pochodzi. Może się to zdarzyć zarówno w mediach społecznościowych, jak i za pośrednictwem poczty elektronicznej czy SMS-ów, dlatego nie należy ufać podejrzanym wiadomościom tylko dlatego, że pochodzą od „znajomego".

Numer ubezpieczenia społecznego

Istnieje bardzo niewielkie prawdopodobieństwo, aby jakaś firma prosiła o Pana/i numer ubezpieczenia społecznego. Jeśli ma to miejsce, należy zapytać, do czego jest im on potrzebny, zwłaszcza jeśli nie jest to instytucja państwowa, pracodawca, bank lub instytucja finansowa. I ponownie, nigdy nie należy go podawać osobom, które się z Panem/ią kontaktują nieproszone.

Należy stosować zaporę sieciową i aktualizować system operacyjny

Przeglądanie stron internetowych może narazić Pana/i komputer na ataki wirusów. Aby zachować bezpieczeństwo, należy na bieżąco aktualizować system operacyjny i program antywirusowy oraz uruchamiać zaporę sieciową.

Należy tworzyć silne hasła

Jeśli korzysta Pan/i z Internetu, należy korzystać z silnych haseł i należy mieć ich kilka. Silne hasło to takie, które:

- jest długie; Hasło powinno składać się z co najmniej ośmiu znaków, ale im więcej, tym lepiej;
- nie powinno być łatwe do odgadnięcia dla osoby szukającej na Pana/i temat informacji, więc nie należy stosować dat urodzenia lub imion i nazwisk krewnych;
- jest czymś, co może Pan/i zapamiętać. Przydatne może być w tym przypadku łączenie długich, rzadkich słów („zszywaczbaterii");
- zostanie zastosowane tylko raz. Jeśli powtórzy Pan/i hasło, a ktoś raz je pozna, może uzyskać dostęp do wszystkich Pana/i kont.

Menedżerowie haseł

„Menedżerowie haseł", które można zainstalować w nowoczesnych przeglądarkach zapamiętują hasła za użytkownika: wystarczy pobrać menedżera, a cała reszta odbywa się automatycznie. Hasło do Pana/i menedżera musi być możliwie najbezpieczniejsze: jeśli oszust uzyska do niego dostęp, może uzyskać dostęp do wszystkich Pana/i kont.

Urządzenia zabezpieczone hasłem

Należy traktować telefony komórkowe i konta komputerowe tak jak konta na stronie internetowej: stosować w nich unikalne, silne hasła.

Hasła domyślne

Niektóre urządzenia, takie jak router lub modem, są dostarczane z hasłem domyślnym. Domyślne hasła są rzadko bezpieczne, dlatego należy je natychmiast zmienić.

Należy regularnie zmieniać hasła

Nawet jeśli skorzysta Pan/i z tej rady, im dłużej używa Pan/i hasła, tym bardziej prawdopodobne jest, że wpadnie w ręce kogoś niepowołanego: bezpieczeństwo stron internetowych może ulec zagrożeniu. Zawsze należy zmieniać hasło, jeśli dana witryna uległa naruszeniu, i okresowo zmieniać hasła, aby zachować bezpieczeństwo.

Bezpieczne połączenia

Niezabezpieczona strona internetowa lub sieć Wi-Fi mogą ujawniać Pana/i dane osobowe. Nigdy nie należy prowadzić spraw osobistych ani finansowych w sieci publicznej, a przed podaniem jakichkolwiek poufnych informacji należy sprawdzić, czy dana witryna jest „bezpieczna". Bezpieczne strony internetowe rozpoczynają się od „https://" zamiast „http://"

Usuwanie niepotrzebnych danych

Należy zniszczyć wszelkie dane osobowe, gdy już ich Pan/i nie potrzebuje. Należy zniszczyć dokumenty drukowane, takie jak rachunki, deklaracje podatkowe i dokumenty finansowe lub medyczne; należy usunąć lub dezaktywować konta cyfrowe oraz usunąć pliki cyfrowe. Proszę pamiętać, że nawet usunięte pliki mogą nadal znajdować się na dysku twardym, dlatego pozbywając się starego komputera, potrzebuje Pan/i specjalnego oprogramowania zabezpieczającego, aby usunąć wszystkie dane osobowe.

Monitorowanie wyciągów

Należy sprawdzać wyciągi z karty kredytowej oraz wyciągi z banku pod kątem wszelkich działań, które nie zostały przez Pan/ią zatwierdzone. Należy dokładnie sprawdzać rachunki za leczenie i ubezpieczenie zdrowotne, aby upewnić się, że rzeczywiście otrzymał/a Pan/i opisane leczenie.

Raporty kredytowe

Każdy ma prawo do jednej bezpłatnej kopii raportu kredytowego rocznie od każdej z głównych agencji informacji kredytowej. Jeśli zauważy Pan/i konta lub zapytania, które nie zostały przez Pana/ią wystosowane lub których Pan/i nie rozpoznaje, może to oznaczać, że ktoś inny posługuje się Pana/i tożsamością. Raporty z różnych agencji można zaplanować na różne pory roku, aby uzyskać regularne informacje na stronie internetowej pod adresem annualcreditreport.com lub pod numerem (877) 322-8228.

Kradzież tożsamości dziecka

Tożsamość dzieci najczęściej ulega kradzieży, czasami przez członków rodziny ze słabą zdolnością kredytową. Należy chronić dane osobowe swoich dzieci tak, jak swoich własnych. Należy zadawać pytania i podejmować działania, jeśli otrzymają wezwania do zapłaty rachunków lub oferty kredytowe na swoje nazwisko, jeśli odmówiono im świadczeń, ponieważ ktoś inny posługuje się ich numerem, lub jeśli otrzymają zawiadomienia z IRS o należnych podatkach.