Naruszenia danych: co robić i jak chronić się przed oszustwami

Otrzymanie powiadomienia o naruszeniu danych z informacją, że Twoje dane osobowe zostały ujawnione lub utracone, może być niezwykle stresujące. Istnieje wiele wiarygodnych organizacji, które oferują wsparcie w zakresie ograniczenia ryzyka oszustw i kradzieży tożsamości.

Poniższy artykuł zawiera przykład wycieku danych osobowych klientów sieci telekomunikacyjnej Optus, który wydarzył się we wrześniu 2022 roku w Australii.

Co to jest naruszenie danych?

Naruszenie danych ma miejsce, gdy dostęp do danych osobowych zostaje ujawniony bez upoważnienia lub zostaje utracony. Może to nastąpić przez przypadek lub z powodu naruszenia bezpieczeństwa.

Twoje dane osobowe są cenne

Pomyśl o swoich danych osobowych jak o układance. Każdy element (informacja) może wydawać się mały, ale gdy je połączysz, osoba postronna może poznać Twoją tożsamość. Posiadając Twoje dane osobowe złodziej będzie mógł uzyskać dostęp do Twojego konta bankowego, zaciągnąć pożyczkę lub zamówić na Twoje nazwisko nowe karty kredytowe, co będzie miało wpływ na Twoją zdolność kredytową. Inaczej mówiąc, jeśli Twoje imię i nazwisko oraz data urodzenia, a nawet kopia prawa jazdy dostaną się w niepowołane ręce, możesz mieć poważne problemy.

- Na stronie organizacji IDCARE https://www.idcare.org/historic-incidents/optus-db-response znajdziesz informacje, co oszust może zrobić z ujawnionymi danymi uwierzytelniającymi.
- Więcej informacji na temat kradzieży tożsamości, rozpoznawaniu znaków ostrzegawczych i formach dostępnej pomocy znajdziesz na stronie https://www.scamwatch.gov.au/types-of-scams/impersonation-scams.

Jestem/byłem klientem sieci Optus. Skąd mam wiedzieć, czy ujawniono moje dane?

Optus skontaktował się z obecnymi i byłymi klientami, których dane osobowe zostały ujawnione w wyniku naruszenia ochrony danych, które miało miejsce we wrześniu 2022 r. Dotyczy to nazwisk, dat urodzenia, numerów telefonów i adresów e-mailowych. W przypadku części klientów ujawnione zostały także numery ich dokumentów tożsamości, takich jak prawo jazdy, paszport czy numer karty Medicare.

Optus kontaktował się z klientami, których dane osobowe zostały ujawnione, za pośrednictwem poczty elektronicznej lub SMS-ów. W swoich wiadomościach dotyczących naruszenia danych nie zamieścił żadnych linków, więc jeśli otrzymałeś lub otrzymasz wiadomość zawierającą link, nie będzie to prawidłowa wiadomość od Optusa. Nie klikaj w ten link.

Gdzie mogę uzyskać więcej informacji i poprosić o pomoc?

Istnieje wiele niezawodnych instytucji/organizacji, do których możesz zwrócić się o pomoc.

Strona operatora sieci telekomunikacyjnej Optus (jeśli jesteś lub byłeś klientem Optusa)

Jeśli otrzymałeś od Optusa powiadomienie o naruszeniu danych osobowych, powinieneś najpierw skontaktować się z firmą Optus i odwiedzić jej stronę internetową. Znajdziesz na niej najbardziej aktualne informacje na temat mającego miejsce wycieku danych oraz odpowiedzi na najczęściej zadawane odpowiedzi, w tym czy musisz wymienić prawo jazdy i jak sprawdzić, czy numer Twojej karty Medicare został ujawniony.

IDCARE

IDCARE to bezpłatna usługa wsparcia dla osób, które stały się ofiarami kradzieży tożsamości, włamań, oszustw oraz zgubienia lub kradzieży danych uwierzytelniających. W przypadku byłych i obecnych klientów Optusa, których dotyczy naruszenie danych Optus, IDCARE zapewnia również porady dotyczące działań zapobiegawczych, które można podjąć, aby uniknąć podobnych sytuacji w przyszłości:

- jeśli to możliwe, skonfiguruj uwierzytelnianie wieloskładnikowe na swoich kontach i używaj silnych haseł;
- skontaktuj się ze swoimi bankami, funduszem emerytalnym i innymi finansowymi organizacjami, w których posiadasz konto i poproś o zastosowanie dodatkowych zabezpieczeń;
- zarejestruj się, aby otrzymywać bezpłatne raporty od agencji sporządzających raporty kredytowe.

Scamwatch

Scamwatch to wiarygodna organizacja zbierająca i udostępniająca informacje o najnowszych oszustwach i sposobach ochrony przed nimi. Zapewnia porady dotyczące radzenia sobie z przypadkami oszustw, w tym naruszeniem danych osobowych, oraz porady dotyczące tego, co jeszcze możesz zrobić, aby przeciwdziałać kradzieży Twoich danych osobowych i uwierzytelniających. Np. rozważ zmianę adresu e-mailowego, którego używasz do ważnych kont, jeśli jest to ten sam e-mail, który podałeś Optusowi.

Biuro Australijskiego Komisarza ds. Informacji (Office of Australian Information Commissioner, OAIC)

OAIC jest niezależnym krajowym organem regulacyjnym ds. prywatności i wolności informacji. Znajdują się w nich ważne informacje na temat Twoich praw do prywatności, tego, jak zareagować na powiadomienie o naruszeniu danych, co zrobić, jeśli Twoja tożsamość została skradziona, a także jak uzyskać dostęp do raportu kredytowego.

Bądź czujny na oszustwa

Oprócz podjęcia zalecanych działań przez instytucje takie jak IDCARE i OAIC, warto zachować szczególną czujność wobec potencjalnych oszustw typu *phishing*. Są to oszustwa, które często wyglądają, jakby pochodziły od znanych firm/instytucji (np. My Aged Care, ATO, bank) i miały na celu nakłonienie Ciebie do podania danych osobowych i/lub uiszczenia jakieś opłaty.

Zwróć szczególną uwagę na e-maile, SMS-y i połączenia, które otrzymujesz z niby znanych sobie instytucji, banków i agencji rządowych. Oto kilka sygnałów ostrzegawczych, na które należy zwrócić uwagę.

Poczucie pilności

Oszuści znajdują sposoby na przyciągnięcie Twojej uwagi i wywołanie poczucia pilności, które może skłonić Ciebie do działania bez zastanowienia. Oto kilka przykładów tego, co mogą powiedzieć oszuści:

- Twój Internet został zhakowany lub działa wolno, a osoba dzwoniąca twierdzi, że może pomóc Ci to naprawić.
- Twoje konto zostanie zablokowane, jeśli nie zaktualizujesz hasła lub nie zweryfikujesz swojej tożsamości.
- Grozi Ci kara grzywny lub aresztowanie, jeśli nie podejmiesz żadnych działań, takich jak dokonanie płatności na rzecz urzędu skarbowego.
- Wygrałeś nagrodę (w konkursie, w którym nie brałeś udziału) i aby ją odebrać, musisz uiścić opłatę.
- Twój bank wykrył nietypową transakcję lub aktywność na Twoim koncie, więc poprosi abyś zadzwonił na dany pod numer, jeśli to nie byłeś Ty.

Podejrzane linki

Nie wszystkie linki w wiadomościach są złe. Kliknięcie linku w biuletynie/newsletterze, który subskrybujesz od zaufanego nadawcy, jest w porządku. Jednakże link w wiadomości tekstowej lub e-mailu, który zawiera prośbę o podanie jakiegoś rodzaju danych osobowych, nie jest bezpieczny.

Jak odróżnić bezpieczny link od oszustwa? Przeczytaj uważnie wiadomość i zastanów się o co Ciebie proszą. Zadaj sobie pytanie, czy wiadomość ta naprawdę pochodzi od firmy, za którą się podaje.

Fałszywa strona internetowa

Link *phishingowy* może przenieść Cię na fałszywą stronę internetową, która wygląda tak samo jak oficjalna strona organizacji, takiej jak na przykład Twój bank lub portal rządowy myGov. Strona może zawierać pola umożliwiające wprowadzenie danych osobowych takich jak hasło, adres e-mail i odpowiedzi na tajne pytania używane do weryfikacji tożsamości.

Jednym ze sposobów sprawdzenia, czy znajdujesz się na fałszywej stronie, jest sprawdzenie adresu internetowego lub adresu URL. Jeśli strona jest fałszywa, adres witryny będzie nieco inny niż prawdziwy. Na przykład oficjalny adres Twojego banku może brzmieć mybigbank.com.au, ale zamiast tego link prowadzi do mybigbank.net.au.

Wskazówki, jak unikać oszustw typu phishing

Bycie czujnym, a nie zaniepokojonym to najlepsze podejście w przypadku oszustw typu *phishing*. Istnieją kroki, które możesz podjąć – i dobre nawyki dotyczące bezpieczeństwa w Internecie, które możesz wyćwiczyć – aby chronić siebie.

1. Bądź uważny

Czytając wiadomość lub rozmawiając z nieznanym rozmówcą, zadaj sobie pytanie: o co Cię on prosi? Jakich informacji wymaga? Czy brzmi to dla Ciebie wiarygodnie? Nie bój się zadawać pytań ani rozłączyć się z rozmówcą, który wywiera na Ciebie presję, mówiąc, że musisz działać szybko.

2. Pomyśl zanim klikniesz w link

Nigdy nie klikaj linków proszących o aktualizację lub weryfikację danych osobowych, niezależnie od tego, jak pilnie lub oficjalnie wydają się one brzmieć. Banki i inne duże organizacje/instytucje nigdy nie wysyłają linku z prośbą o podanie danych osobowych lub hasła.

3. Nie podawaj danych swojego konta bankowego nieznanym rozmówcom

Nie podawaj danych swojego banku ani karty kredytowej nikomu, kto niespodziewanie do Ciebie zadzwoni, nawet jeśli chce „potwierdzić", że dane te są prawidłowe.

4. Sprawdź adres internetowy (lub URL), kiedy odwiedzasz oficjalną stronę internetową

Scamwatch zaleca, aby nigdy nie wprowadzać danych osobowych, bankowych ani danych karty kredytowej na stronie internetowej, chyba że sprawdzisz ich autentyczność. Jeśli znasz prawidłowy adres internetowy, porównaj go z adresem URL witryny, na której się znajdujesz. W przeciwnym razie wyszukaj w Internecie oficjalny adres danej instytucji.

5. Skontaktuj się bezpośrednio z firmą

Jeśli otrzymasz wiadomość, której nie jesteś pewien, skontaktuj się bezpośrednio z firmą z której rzekomo pochodzi ta wiadomość. Możesz to zrobić poprzez wyszukiwanie online danych kontaktowych tej firmu – nigdy nie używaj danych kontaktowych podanych w przesłanej wiadomości.

Przydatne informacje

Skorzystaj z bezpłatnych artykułów i kursów e-learningowych dostępnych na platformie e-learningowej Be Connected:

- jak unikać oszustw w sieci – kurs „Identyfying and avoiding scams" (polską wersję 5-częściowego kursu znajdziesz tutaj: oszustwa na romans, oszustwa na zdalny dostęp, oszustwa związane z wyłudzeniem danych, oszustwa na inwestycje, oszustwa z kryptowalutami);
- dowiedz się więcej o menedżerze haseł, oprogramowaniu antywirusowym i wirtualnych sieciach prywatnych (VPN) – kursy z działu „Advanced online security";
- dowiedz się, jak chronić się w Internecie – strona Australian Signals Directorate, Australian Cyber Security Centre cyber.gov.au;
- odkryj więcej wskazówek, jak uniknąć kradzieży tożsamości – artykuł „Identity theft: what is it and how to avoid it";
- jak zatrzymać niechciane lub uciążliwe połączenia telefoniczne – artykuł „How to stop unwanted calls".

Artykuł w polskiej wersji językowej opracowała Justyna Tarnowska w oparciu o tekst „Data breaches: what to do and how to protect yourself against scams" udostępniony na portalu Be Connected: https://beconnected.esafety.gov.au/topic-library/articles-and-tips/data-breaches-what-to-do-and-how-to-protect-yourself-against-scams