Moje dane trafiły do darknetu - Co teraz?

Zagłosowałaś w instagramowym konkursie na influencera, a może zalogowałeś się do ulubionej gry on-line lub na portal, w którym szukałeś kodów do jej przejścia? Możliwe, że Twoje dane stały się właśnie przedmiotem obrotu handlowego, prowadzonego w najmroczniejszych zakamarkach internetu. Takie zagrożenie jest coraz bardziej realne. Jak pokazują dane z Raportu antyfraudowego BIK, wyłudzeń i oszustw jest coraz więcej, a z tymi „na BLIKa" albo „na znajomego z Facebooka" zetknęło się już 40 proc. Polaków. Jak uchronić się przed wykorzystaniem naszych skradzionych danych? Wskazujemy sposoby skutecznych metod ochrony i narzędzi, łącznie z monitorowaniem darknetu.

NOWOCZESNE ZARZĄDZANIE BIZNESEM
www.nzb.pl
Partner programu edukacyjnego NZB:
BIK BIURO INFORMACJI KREDYTOWEJ

Trwający przez cały październik Europejski Miesiąc Cyberbezpieczeństwa to doskonała okazja, by o zagrożeniach w sieci mówić często i na wszystkie sposoby. Zwłaszcza, że ich skala nieustannie rośnie, a do znanych już oszustw „na wnuczka" czy „na policjanta", dołączają próby wyłudzeń „na celebrytę lub influencera", na „amerykańskiego żołnierza", a nawet tak absurdalne (ale skuteczne), jak wyłudzenie „na pracownika kopalni węgla w Kambodży". Coraz częściej ofiarami takich oszustw padają osoby młode, na które oszuści czają się w mediach społecznościowych, forach, czatach czy w grach on-line.

Młodzi coraz bardziej narażeni na niebezpieczeństwo

O wycieku ponad 200 tys. rekordów zawierających dane do logowania, takie jak e-mail, login oraz hasło donosiły specjalistyczne media we wrześniu 2025 r. Analiza wykazała, że wśród skradzionych danych znajdowało się wiele stron związanych z grami komputerowymi, co sugeruje, że ofiarami byli m.in. młodzi użytkownicy Internetu i gracze. Podobne wnioski nasuwają się na przykładzie oszustw phishingowych, np. prośba od znajomego o oddanie głosu w konkursie na ambasadora marki czy powiadomienia o naruszeniu praw autorskich na Instagramie.

Zjawisko cyberzagrożeń potwierdzają dane z dorocznego Raportu antyfraudowego BIK, który wskazuje nie tylko rozmaite techniki oszustw, ale również sposoby ochrony przed wyłudzeniami za pomocą manipulacji, nierzadko przy użyciu technologii. Najczęściej zgłaszane przez respondentów incydenty dotyczyły phishingu, czyli podszywania się pod wiarygodną instytucję za pomocą fałszywej strony banku, linku czy smsa, w celu kradzieży danych np. do logowania. Z oszustwem tego typu zetknęło się w 2025 roku 41 proc. badanych. Niewiele mniej, bo 40 proc. spotkało się z próbą oszustwa „na BLIKa" lub „na znajomego z Facebooka", co niejednokrotnie kończyło się przechwyceniem konta w mediach społecznościowych.

- Jak zaobserwowaliśmy, wśród wszystkich rodzajów oszustw, najszybciej rośnie liczba wyłudzeń kodów BLIK oraz przejęć konta w social mediach. W porównaniu z ubiegłym rokiem jest ich już o 10 pp. więcej. To jednocześnie jeden z najbardziej skutecznych sposobów oszustwa. Na uwagę zwraca także rosnąca liczba prób wyłudzeń za pośrednictwem urządzeń mobilnych. 40 proc. ankietowanych wskazuje na oszustwa SMS-owe, a 22 proc. - na próby kontaktu przez komunikatory internetowe, takie jak Messenger czy WhatsApp. Niepokój potęguje bierność, bo wciąż co szósty użytkownik nie zabezpiecza dostępu do swojego smartfonu, nie używa ani haseł dostępu, ani zabezpieczeń biometrycznych, np. odcisku palca - tłumaczy Andrzej Karpiński, Dyrektor Departamentu Bezpieczeństwa, BIK S.A.

Mroczny mechanizm wyłudzenia

Oszuści pozyskują nasze dane na coraz to nowsze sposoby. Od wspomnianego phishingu, przez spoofing polegający na użyciu spreparowanego numeru telefonu w celu podszycia się np. pod pracownika Narodowego Banku Polskiego, poczty, firm kurierskich, po komunikaty od fałszywych sklepów internetowych. Jeśli młody człowiek używa tego samego hasła do gry, poczty i konta społecznościowego, cyberprzestępcy mogą przejąć całą jego tożsamość cyfrową, włącznie z Profilem Zaufanym czy ePUAP. Kradzież konta na Instagramie lub TikToku, to dopiero początek kłopotów. Przejęcie cyfrowej tożsamości to dla złodzieja przepustka do wyłudzeń kredytów, pożyczek, zakupów drogich usług lub produktów.

Sposoby ochrony: od antywirusa po monitoring darknetu

Choć sposobów oszustw, zwłaszcza z wykorzystaniem socjotechnik nieustannie przybywa, to nie jesteśmy zupełnie bezbronni. Jest coraz więcej narzędzi, z których należy korzystać i chronić swoje dane. Wiele zależy jednak od nas samych. Tymczasem jak czytamy w Raporcie antyfraudowym BIK z 2025 roku, 13 proc. klientów w przypadku wycieku danych pozostaje bierna ufając, że „już na pewno ktoś się tym zajmuje". Jak zatem najczęściej bronimy się przed cyberoszustwami i jak reagujemy na informacje o wycieku danych osobowych? Tylko niecała połowa z nas (47 proc.) deklaruje, że chroni się korzystając z funkcji automatycznych aktualizacji w smartfonach. W przypadku wycieku danych osobowych najczęściej zastrzegamy dowód osobisty (46 proc.) czy kontaktujemy się z instytucją, pod którą podszywał się oszust (40 proc.), 34 proc. z nas zgłasza sytuację na policję, a 18 proc. występuje do instytucji z wnioskiem o usunięcie danych z bazy i zgłasza się do UODO.

- *Coraz więcej Polaków obserwuje rosnące niebezpieczeństwo związane z możliwym wyciekiem danych. Jednak niewielu z nas ma świadomość, czym może to grozić i jak udaremnić próbę posłużenia się naszą tożsamością. Wsparciem w tym zakresie są nowoczesne rozwiązania antywyłudzeniowe sektora bankowego, ale również nasza aktywność i prewencja. Są jednak miejsca, takie jak darknet, do których nie powinnyśmy sami zaglądać, a do których dostanie się jest możliwe tylko z pomocą specjalnych przeglądarek. Tu z pomocą przychodzi BIK, który dla nas monitoruje szarą strefę internetu. Alerty BIK z monitorowaniem darknetu, od razu po ich włączeniu poinformują nas czy nasze dane już są w darknecie, a jeśli tak otrzymamy porady co robić w tej sytuacji. Następnie BIK na bieżąco monitoruje, czy nasze dane są na sprzedaż w internetowym podziemiu. Takie ostrzeżenie pozwala szybciej zareagować i zabezpieczyć swoje dane* - tłumaczy Joanna Charlińska, Dyrektor ds. Sprzedaży, Departament Rynku Detalicznego BIK S.A.

Co zatem zrobić, gdy otrzymamy powiadomienie o tym, że nasz adres e-mail znalazł się w darknecie? W pierwszej kolejności zmienić wszystkie krytyczne hasła: do poczty elektronicznej, bankowości cyfrowej, ale też te stosowane w mediach społecznościowych, sklepach i grach on-line. Tam, gdzie to możliwe warto uruchomić uwierzytelnianie wieloskładnikowe. Dobrze jest też zweryfikować listę zaufanych urządzeń i usunąć te nieznane oraz przeskanować komputer czy telefon za pomocą aktualnego oprogramowania antywirusowego. Jeśli w wycieku były dane bankowe lub hasła do bankowości należy natychmiast skontaktować się ze swoją placówką i zastrzec kartę, a w przypadku strat finansowych lub przejęcia tożsamości, zgłosić sprawę na policję.

Źródło: Raport antyfraudowy BIK, 2025 dostępny jest na https://rozwiazania-antyfraudowe.bik.pl/pl/raporty

***

Biuro Informacji Kredytowej oraz BIG InfoMonitor są inicjatorami Programu edukacyjnego Nowoczesne Zarządzanie Biznesem i partnerami w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym".

Więcej: www.nzb.pl / www.facebook.com/NowoczesneZarzadzanieBiznesem