OUCH! Luty 2024

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Kradzież tożsamości: Zapobieganie, wykrywanie i reagowanie

Wstęp

W dzisiejszej erze cyfrowej dane osobowe są cenniejsze niż kiedykolwiek wcześniej. Dlatego aktualnie często celem przestępców jest kradzieży tożsamości. Zrozumienie tego zagrożenia, wykrycie go i wiedza o tym, jak się chronić, są niezbędnymi elementami ochrony cyfrowego życia.

Czym jest kradzież tożsamości?

Kradzież tożsamości jest niczym innym jak bezprawnym pozyskaniem danych osobowych w celu popełnienia oszustwa lub innych przestępstw. Przestępców interesują takie dane jak imię i nazwisko, numery identyfikacyjne tj. numer PESEL, numer dowodu osobistego lub paszportu oraz dane karty kredytowej. Powszechną formą kradzieży tożsamości jest jej kradzież w celach dokonania oszustw finansowych. Na przykład, złodzieje kradną twoją tożsamość i zaciągają kredyt, który finalnie musisz spłacać. Istnieją również inne rodzaje kradzieży tożsamości. Jednym z przykładów jest kradzież tożsamości medycznej, w których przestępcy próbują wyłudzić odszkodowanie z ubezpieczenia na hospitalizację, której nie było. Inną jest kradzież tożsamości związana z podatkami, gdy przestępca wykorzystuje numer identyfikacji podatkowej do złożenia zeznania podatkowego w Twoim imieniu i ubiegania się o nieuczciwy zwrot podatku. A gdy Ty próbujesz złożyć zeznanie podatkowe, nie możesz odzyskać swoich pieniędzy, ponieważ zostały one już przekazane komuś innemu.

Działania zapobiegawcze

Jak możesz się ochronić? Niestety, nie jest to tak łatwe jak mogłoby się wydawać. Wiele organizacji posiada już informacje o użytkowniku i to od nich zależy ich ochrona. Istnieje jednak kilka kroków, które można podjąć.

- **Silne hasła**: Jednym z najskuteczniejszych sposobów ochrony jest zabezpieczenie każdego z kont unikalnym, długim hasłem oraz jeśli to możliwe, włączenie uwierzytelniania wieloskładnikowego.
- **Regularnie aktualizuj oprogramowanie**: Upewnij się, że urządzenia z których korzystasz są zaktualizowane o najnowsze poprawki zabezpieczeń. Włącz automatyczną aktualizację na wszystkich urządzeniach w celu niepominięcia, której z kluczowych poprawek bezpieczeństwa.
- **Karty płatnicze**: Używaj kart kredytowych do zakupów online, nigdy kart debetowych. Korzystanie z karty kredytowych zapewnia znacznie większą ochronę przed oszustwami. Dobrym pomysłem jest używanie jednej karty kredytowej tylko do zakupów online, a drugiej do wszystkich innych transakcji. Istnieją również wirtualne lub jednorazowe karty kredytowe. Warto z nich korzystać, ponieważ w stosunku do tradycyjnych kart, zapewniają jeszcze większy poziom bezpieczeństwa.
- **Zastrzeżenie kredytowe:** Przemyśl włączenie opcji zastrzeżenia kredytowego. Włączając tę opcję zabezpieczysz się na ewentualność, kiedy przestępcy będą próbowali zaciągną kredyt na Twoje dane. Zastrzeżenie kredytowe włączysz internetowo za pośrednictwem strony internetowej Biura Informacji Kredytowej (BIK). Usługa ta jest płatna.

Wykrycie kradzieży tożsamości

Wczesne wykrycie kradzieży tożsamości jest czymś co może ochronić Twoje dane. Im szybciej wykryjesz, że Twoja tożsamość została wykorzystywana przez kogoś innego, tym szybciej będziesz mógł działać. Oto niektóre z najczęstszych oznak kradzieży tożsamości:

- **Podejrzane wyciągi bankowe:** Staraj się regularnie monitorować wszystkie wyciągi z konta bankowego I karty kredytowej. Niech Twoją uwagę przykują opłaty lub przelewy, których nie wykonałeś. Dobrym pomysłem jest włączenie automatycznych powiadomień. W ten sposób za każdym razem, gdy karta kredytowa zostanie obciążona lub nastąpi zmiana na koncie, zostaniesz o tym natychmiast powiadomiony.
- **Nieprawidłowe raporty kredytowe**: Co jakiś czas sprawdzaj swoje raporty kredytowe pod kątem podejrzanych działań. Jeśli nie masz aktywowanej usługi zastrzeżenia kredytowego, regularnie sprawdzaj czy na Twoje dane nie została zaciągnięta pożyczka finansowa.
- **Podejrzane rachunki I powiadomienia**: Zachowaj ostrożność, jeśli zaczniesz otrzymywać rachunki za przedmioty, których nie kupiłeś, lub jeśli skontaktuje się z Tobą firma w sprawie niezapłaconych rachunków za przedmioty lub usługi o których nie masz pojęcia.
- **Niespodziewana odmowa**: Jeśli niespodziewanie odmówiono Ci zwrotu podatku, kredytu lub pożyczki, sprawdź dlaczego tak się stało.

Reagowanie na kradzież tożsamości

Jeśli obawiasz się, że Twoja tożsamość została naruszona, działaj natychmiast.

- **Zgłoś natychmiast**: Jeśli podejrzewasz kradzież, zgłoś ją jak najprędzej. Na przykład, jeśli zauważysz podejrzaną aktywność na swoim koncie bankowym lub karcie kredytowej, skontaktuj się z bankiem. Złóż również zgłoszenie popełnienia przestępstwa w dowolnej jednostce policji. Może to mieć kluczowe znaczenie dla udowodnienia przestępstwa I pomóc w odzyskaniu ewentualnych strat finansowych.
- **Alerty o oszustwach I zastrzeżenie kredytów**: Rozważ włączenie usług Alerty BIK oraz zastrzeż możliwość uzyskania kredytu na Twoje dane. Jak już dojdzie do nieprzyjemnego zdarzenia, współpracuj z biurem kredytowym w celu usunięcia fałszywych informacji.
- **Udokumentuj wszystko**: Dzwoniąc do organizacji w celu odzyskania danych, pamiętaj o prowadzeniu szczegółowej dokumentacji komunikacji I podjętych działań, w tym o tym z kim rozmawiałeś, o jakiej godzinie I o czym rozmawiano.
- **Zmień hasła**: Zaktualizuj hasła do wszystkich kluczowych kont. Jeśli masz problem z zapamiętaniem wielu unikalnych haseł, dobrym pomysłem jest korzystanie z narzędzi takich jak menedżer haseł.

Wnioski

Rozumiejąc czym jest kradzież tożsamości I stosując te środki, można znacznie zmniejszyć ryzyko stania się jej ofiarą.

Źródła

Menedżer haseł: https://www.sans.org/newsletters/ouch/power-password-managers/
Bezpieczeństwo kont bankowych: https://www.sans.org/newsletters/ouch/securing-financial-accounts/
Alerty BIK: https://www.bik.pl/
Raport Identity Theft: https://www.identitytheft.gov/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz