Wykorzystanie nowych technologii w zwiększeniu swojego bezpieczeństwa

Data publikacji: 31.01.2025 8:59

Kradzież tożsamości stanowi coraz powszechniejszą taktykę cyberprzestępców. W 2024 roku oszuści podszywający się pod instytucje publiczne usiłowali wyłudzić numer PESEL od niemal 30% naszych rodaków. Socjotechnicznej presji poddawani są też przedsiębiorcy. Co piąty z nich zetknął się z przypadkiem, kiedy oszuści próbowali dokonać wyłudzenia, udając kontrahentów lub współpracowników firmy. Biorąc to pod uwagę, banki chętnie sięgają po rozwiązania, bazujące na analizie behawioralnej, które skutecznie chronią konsumentów.

Kradzież tożsamości stanowi coraz powszechniejszą taktykę cyberprzestępców. mat.pras.ox.pl

- ***Weryfikacja naszych zachowań w trakcie korzystania z urządzenia mobilnego czy bankowości internetowej, to bardzo skuteczna metoda ochrony środków konsumentów. To sposób, by od początku zalogowania, a także w trakcie całej sesji na bieżąco weryfikować, czy osoba logująca się do konta bankowego i przeprowadzająca operacje finansowe jest właścicielem rachunku czy mamy do czynienia z przestępcą, podszywającym się pod klienta*** – mówi Agnieszka Szopa – Maziukiewicz, Prezes Zarządu Digital Fingerprints, spółki należącej do Grupy BIK.

Narzędzie analizy behawioralnej dostępne jest już w sześciu bankach w Polsce. Warto je poznać i korzystać, nic nie kosztuje ani nie wymaga specjalnych działań od klienta banku. Wystarczy tylko sprawdzić, czy dany bank już wprowadził Weryfikację Behawioralną i wyrazić niezbędne zgody.

Analiza behawioralna – perspektywa banku i klienta

Istotą weryfikacji behawioralnej jest analiza unikalnych zachowań użytkownika podczas korzystania z urządzenia mobilnego czy bankowości internetowej podczas logowania się do swojego banku. Są to takie cechy jak sposób pisania użytkownika, tempo naciskania przycisków na klawiaturze, charakterystyka poruszania myszką czy sposób korzystania z ekranu dotykowego. Dzięki temu system tworzy dynamiczny profil behawioralny użytkownika pozwalający wykryć ewentualne anomalie w jego zachowaniu, wskazujące na próbę oszustwa.

Zaawansowane algorytmy wykorzystane w tym rozwiązaniu pozwalają aktualizować modele w czasie rzeczywistym oraz zatrzymać oszukańcze operacje jeszcze zanim pieniądze wypłyną z rachunku klienta. Banki korzystają z tego rozwiązania zarówno indywidualnie, jak i sektorowo. Ta druga opcja rozszerza zakres ochrony klienta z jednego banku na cały sektor bankowy. Stwarza możliwość wymieniania się wiedzą o schematach oszukańczych i postępowaniu sprawców. I choć te mechanizmy nie są widoczne dla użytkowników indywidualnych, to z perspektywy samego klienta, włączenie tego innowacyjnego rozwiązania będzie kolejną warstwą zabezpieczenia przed następstwem ewentualnych ataków socjotechnicznych i ochroną przed wyłudzeniem.

Co konsument powinien wiedzieć o analizie behawioralnej

Niemal ¾ użytkowników bankowości elektronicznej i aplikacji loguje się do konta w banku wielokrotnie w ciągu tygodnia. Najczęściej stosowanym mechanizmem zabezpieczającym są loginy i hasła (82 proc.), jednak są one uznawane za najłatwiejsze do pokonania przez przestępcę.

- ***Do najczęściej wykrywanych metod oszustw należą m.in. fałszywe linki w mailach, na platformach takich jak Facebook, Messenger czy Vinted, wykorzystanie zdalnych pulpitów, podszywanie się pod pracowników banku oraz fałszywe inwestycje. Wszystkie te metody skutkują wykradzeniem danych do logowania, które są wykorzystywane do przejęcia konta i przeprowadzania nielegalnych transakcji. Łączy je jedno: po zalogowaniu się oszusta można zaobserwować zmianę wzorca zachowania. Dlatego banki wprowadzają kolejne nowatorskie metody zabezpieczeń. Jedną z najnowszych jest weryfikacja***

behawioralna. Okazuje się jednak, że choć blisko ¾ Polaków (67 proc.) ma do niej dostęp w swoim banku, 22 proc. nie wie, jak ona działa. To wystarczający powód, by lepiej poznać jej walory – mówi Karol Głogowski, dyrektor IT usług antyfraudowych BIK.

Oto wybrane najważniejsze informacje o weryfikacji behawioralnej BIK:

- Analiza behawioralna jest bezkontekstowa i służy zwiększeniu ochrony przed nieuprawnionym przelewem z konta i złożeniem wniosku kredytowego. To dzięki nowatorskiej technologii weryfikacji behawioralnej BIK, która identyfikuje unikatowe zachowania człowieka podczas logowania się do bankowości online lub mobilnej,
- O unikatowości rozwiązania świadczy uwierzytelnianie osoby w czasie ciągłym. Oznacza to, że analizowany jest sposób korzystania z urządzenia podczas logowania, ale także w trakcie całej sesji, w czasie rzeczywistym. Dzięki temu wszelkie anomalie w zachowaniu człowieka pozwalają wykryć oszukańczą operację i ustrzec prawowitego klienta banku, np. przed nieuprawnionym przelewem z jego konta,
- Samo gromadzenie informacji o użytkowniku dokonuje się bez jego zaangażowania i ingerowania w prywatność.
- Gdy wyrazimy zgodę w swoim banku na taką ochronę, niezauważalnie wejdziemy na wyższy poziom bezpieczeństwa w cyberprzestrzeni,
- Warto podkreślić, że wszelkie modele zachowań klienta banku są bezkontekstowe, czyli analizie podlega sposób korzystania, a nie treść.

Wraz ze wzrostem liczby użytkowników korzystających z elektronicznych usług bankowych, potrzebna jest współodpowiedzialność sektora finansowego i klientów banków za budowanie odporności na zagrożenia ze strony cyberprzestępców. Zwłaszcza że jak notuje najnowszy Raport InfoDOK ze stycznia br., wydawany przez Związek Banków Polskich, kwota prób wyłudzeń w 2024 roku wyniosła 324,2 mln zł i była prawie o jedną dziesiątą wyższa r/r.

Nowe technologie, które wdrażają banki, a klienci mogą z nich korzystać to współpraca, która może zaowocować lepszą ochroną środków finansowych na koncie oraz zabezpieczeniem informacji o sobie w cyfrowym świecie.

***

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