**Informacja prasowa**

**Warszawa, 11.12.2023 r.**

**Bezpieczeństwo w sieci w erze dynamicznego rozwoju cyfrowej bankowości**

**Bankowość nieustannie zmienia swoje oblicze. Coraz więcej osób przekonuje się do korzyści płynących z usług bankowych online. Wszystko dlatego, że znacznie ułatwiają zarządzanie finansami z dowolnego miejsca i o dowolnej porze. Jak wynika z raportu LeanCode i Kearney, 21% Europejczyków zrezygnowało z wizyt w stacjonarnych oddziałach banków, a ponad jedna czwarta bywa w nich nie częściej niż raz do roku. Bankowe kanały cyfrowe zyskują na popularności, jednak w tym cyfrowym środowisku dane osobowe i finansowe stają się podatne na nowe rodzaje zagrożeń.**

W raporcie LeanCode i Kearney „Bankowość mobilna w Polsce 2022 oczami klienta” wskazano, że aplikacje mobilne, początkowo rozwijane jako przedłużenie serwisu online czy sposób na przeniesienie transakcji poza oddziały, teraz stają się najbardziej powszechnym sposobem interakcji z klientem oraz łatwo dostępnym narzędziem, spełniającym wszystkie typowe potrzeby, zintegrowanym z pozostałymi kanałami banków.

Z badania Związku Banków Polskich wynika, że w 2019 roku 5,7 mln klientów banków w Polsce korzystało tylko z aplikacji mobilnych. Natomiast już w trzecim kwartale ubiegłego roku było to 12,5 mln, co oznacza wzrost o 120%. Ponadto, 58% użytkowników bankowych kanałów cyfrowych używa tylko aplikacji mobilnych.

Pracownicy banku są przeszkoleni w zakresie obsługi klientów oraz procedur bezpieczeństwa. Istnieje jednak pewna zasada, której należy przestrzegać – nigdy nie powinno się ujawniać haseł do kont bankowych, kart kredytowych lub innych poufnych informacji osobom trzecim, w tym również pracownikom banku. Właściwym podejściem jest traktowanie haseł i informacji finansowych jako świętej tajemnicy, dostępnej tylko dla nas samych.

*Pracownik banku nie powinien i nie ma prawa prosić nas o podanie hasła do konta bankowego lub innych poufnych danych. To jest absolutny, podstawowy przepis bezpieczeństwa. Banki stosują zaawansowane metody uwierzytelniania, takie jak hasła jednorazowe, tokeny SMS czy aplikacje autoryzacyjne, aby potwierdzić naszą tożsamość. Jeśli zostaniemy poproszeni o podanie hasła, powinniśmy odmówić i natychmiast skontaktować się z naszym bankiem, aby zgłosić zaistniałą sytuację* – mówi **Marta Fila, członkini zarządu i Chief Sales Officer w AIQLabs, właścicielu marek SuperGrosz i „Kupuj Teraz – zapłać później”.**

Maksymalna ostrożność powinna zostać również zachowana w sytuacji, gdy pracownik banku wymaga instalacji dowolnego oprogramowania na naszym urządzeniu. Współczesne technologie umożliwiają cyberprzestępcom podszywać się pod pracowników instytucji finansowych i nakłaniać do pobrania złośliwego oprogramowania, które może zagrażać bezpieczeństwu danych wrażliwych. Przed instalacją, należy upewnić się, że prośba pochodzi od oficjalnego źródła i jest potwierdzona przez bank.

Warto także przestrzegać kilku kluczowych zasad, aby chronić własne finanse oraz dane. Zawsze należy potwierdzić tożsamość osoby kontaktującej się w imieniu instytucji finansowej. Można to zrobić, dzwoniąc na oficjalny numer telefonu znanego z oficjalnej strony internetowej lub z karty plastikowej. Hasła oraz poufne informacje nigdy nie powinny być ujawniane. Na własnym urządzeniu warto zainstalować oprogramowanie antywirusowe, a następnie regularnie je aktualizować. Należy też korzystać wyłącznie z bezpiecznych połączeń internetowych i unikać korzystania z publicznych sieci Wi-Fi.

Pracownik banku nie powinien prosić klienta o jakiekolwiek hasło, a tym bardziej nakazywać instalację oprogramowania. Ochrona danych finansowych to nasza osobista odpowiedzialność. Dbając o bezpieczeństwo tych danych, można cieszyć się komfortem korzystania z usług bankowych online.

**\*\*\***

**AIQLABS Sp. z o.o. – zaawansowany FinTech od 2015 r. działający w branży consumer finance**. Misją firmy jest dostarczanie produktów finansowych dopasowanych do zdolności kredytowej i potrzeb klientów, dzięki zaawansowanej analityce, technologii i nowoczesnym procesom obsługi. Spółka oferuje kompletny ekosystem usług związanych z finansowaniem gotówkowym potrzeb zakupowych klientów, w tym kredyty konsumenckie, finansowanie usług medycznych oraz odroczone płatności za zakupy.

**Więcej informacji:**

[**http://aiqlabs.pl/**](http://aiqlabs.pl/)

[**https://kupujteraz.pl/**](https://kupujteraz.pl/)

[**https://supergrosz.pl/**](https://supergrosz.pl/)

**Kontakt dla mediów:**

**Bartosz Sosnówka**

communications manager

E: [Bartosz.sosnowka@dwapiar.pl](mailto:Bartosz.sosnowka@dwapiar.pl)

M: 517 476 361