**Informacja prasowa**

**Warszawa, 02.07.2024 r.**

**Gdzie nie logować się na konto bankowe?**

***Świadomość potencjalnych zagrożeń i środki ostrożności***

**W czasach, gdy coraz więcej codziennych transakcji przenosi się do świata online, bezpieczeństwo kont bankowych jest absolutnym priorytetem. Zachowanie ostrożności podczas logowania jest kluczowe dla zabezpieczenia danych.**

Niezabezpieczone sieci Wi-Fi stanowią poważne zagrożenie dla bezpieczeństwa kont bankowych. Korzystając z takich sieci, naraża się na ryzyko przechwycenia danych przez niepowołane osoby. Niezależnie od tego, czy jesteśmy w domu, w pracy czy w miejscu publicznym, zawsze powinniśmy upewnić się, że połączenie jest bezpieczne. Podczas korzystania z niezabezpieczonych sieci Wi-Fi, dane mogą być łatwo przechwycone przez hakerów. Mogą oni uzyskać dostęp do haseł, numerów kart kredytowych, a nawet kont bankowych. Dlatego też zawsze powinno się korzystać z sieci Wi-Fi, które są zabezpieczone silnym hasłem. Ponadto, warto korzystać z dodatkowych środków bezpieczeństwa, jak VPN (Virtual Private Network), które zapewniają dodatkową warstwę ochrony danych.

*Logowanie się na konto bankowe na komputerze, który jest używany przez wiele osób, niesie ze sobą wiele ryzyk. Współdzielone komputery są często celem ataków hakerów, którzy instalują na nich oprogramowanie szpiegujące w celu kradzieży danych bankowych. Nawet jeśli komputer jest chroniony przez najnowsze oprogramowanie antywirusowe, nie ma gwarancji, że jest on całkowicie bezpieczny. Zawsze należy wylogować się z konta bankowego po zakończeniu sesji. Niezależnie od tego, czy jest to komputer w bibliotece, w kawiarni czy w domu, istnieje ryzyko, że ktoś inny może uzyskać dostęp do konta. Radzę, aby nie zapisywać nigdy swojego hasła, zwłaszcza na współdzielonym komputerze i upewnić się, że strona banku jest bezpieczna* – mówi **Marta Fila, członek zarządu AIQLabs, właściciela marek SuperGrosz i „Kupuj Teraz – zapłać później”**.

Logowanie do konta bankowego za pomocą urządzeń mobilnych niesie ze sobą pewne ryzyko. Podstawowym zagrożeniem jest możliwość infekcji urządzenia szkodliwym oprogramowaniem, które może przechwycić dane logowania. W przypadku korzystania z publicznych sieci Wi-Fi, istnieje ryzyko, że niezabezpieczone połączenie może być wykorzystane do przechwycenia informacji. W celu uniknięcia wspomnianych zagrożeń, należy regularnie aktualizować oprogramowanie na swoim urządzeniu, ponieważ aktualizacje często zawierają poprawki bezpieczeństwa. Ponadto, niezależnie od tego, czy korzystamy z telefonu, tabletu czy laptopa, zawsze należy korzystać z oficjalnej aplikacji banku, która jest regularnie aktualizowana i ma wbudowane mechanizmy zabezpieczające.

*Phishing to technika stosowana przez cyberprzestępców, którzy próbują wyłudzić od nas cenne informacje, takie jak dane logowania do konta bankowego. Zazwyczaj odbywa się to poprzez wysyłanie fałszywych wiadomości e-mail, które wyglądają, jakby pochodziły od zaufanego źródła, na przykład od naszego banku. Wiadomości te często zawierają linki prowadzące do fałszywych stron internetowych, które wyglądają identycznie jak strony naszego banku. Gdy wprowadzimy na nich nasze dane, przestępcy je przechwytują –* dodaje **Marta Fila**.

Chcąc zabezpieczyć konto bankowe przed phishingiem, warto zastosować kilka prostych zasad. Nigdy nie klikać w linki zawarte w wiadomościach e-mail, które wyglądają podejrzanie. Zawsze sprawdzać adres strony internetowej, na którą zostało się przekierowanym. Jeżeli jest inny niż adres banku, nie wprowadzać żadnych danych. Należy pamiętać, że bank nigdy nie prosi o podanie hasła do konta przez e-mail. Regularna aktualizacja oprogramowania na komputerze, w tym przeglądarki internetowej, może pomóc w blokowaniu fałszywych stron internetowych. Wreszcie, jeżeli pojawiają się jakiekolwiek wątpliwości co do wiadomości z podejrzanego źródła, koniecznie należy skontaktować się z bankiem za pomocą oficjalnych kanałów komunikacji.

**\*\*\***

**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