Hakerzy co rusz podszywają się pod polskie banki i tworzą fałszywe strony, na które próbują zwabiać swoje ofiary. Następnie dochodzi do próby wykradzenia danych logowania do bankowości elektronicznej, co może mieć katastrofalne skutki. Dlatego tak ważne jest, aby nie wchodzić w linki otrzymane od nieznanych osób.

Policjanci apelują o ostrożność podczas dokonywania transakcji zakupowych przez aplikacje. Przede wszystkim należy pamiętać, aby nie klikać w żadne linki wysyłane przez nieznane osoby. Robiąc zakupy przez aplikację internetową, dokonujmy również płatności poprzez tą aplikacje a nie przez link wysłany przez sprzedającego.
Jeśli jesteś sprzedającym również oczekuj na płatność poprzez aplikację lub na przelew na Twoje konto i nie wchodź w wysłany przez kupującego link, poprzez który rzekomo zobaczysz potwierdzenie otrzymania zapłaty.

Przykładowa wiadomość jaką mogą wysyłać oszuści: „Otrzymanie zapłaty: https://bcrepsnj.com/eguga", gdzie po kliknięciu w linka i zalogowaniu się do swojego banku przekazujemy oszustowi dane dostępowe.
Aplikacje sprzedażowe nie wysyłają takich linków! Już z treści linku, gdzie jest to ciąg liter widać, że jest to podejrzane i nie należy w niego wchodzić a już na pewno nie podawać żadnych danych. Otrzymanie płatności należy zweryfikować w posiadanej przez nas aplikacji a nie w otrzymanym linku!

Należy zwrócić również uwagę na otrzymywane z banku wiadomości. Banki starają się nas chronić i wysyłają ostrzeżenia.
Przykładowa wiadomość z banku: „Uwaga, aktywujesz aplikację mobilną na nowym urządzeniu. Jeśli to nie ty, zadzwoń … Dodanie do zaufanych urządzenia mobilnego:….Hasło nr 1 …."
Wystarczy przeczytać taką wiadomość, w której wprost wskazane jest, że osoba nieuprawniona dodaje nowe urządzenie do banku. Po otrzymaniu takiego smsa nie przekazujmy hasła, tyko od razu kontaktujmy się z bankiem.