Policja ostrzega: SMS z prośbą o dopłatę do przesyłki lub uzupełnienie danych? To może być oszustwo!

Przestępcy wciąż wymyślają nowe sposoby, którymi próbują pozbawić nas naszych pieniędzy. W ostatnim czasie internetowi oszuści coraz chętniej podszywają się pod firmy kurierskie i wysyłają SMS-y z linkiem do strony, na której należy dokonać rzekomej dopłaty do przesyłki i tym samym umożliwić im wyłudzenie środków z konta bankowego. Do właścicieli telefonów zaczęły również przychodzić smsy z prośbą o uzupełnienie danych i wejście w podejrzany link w celu ich uzupełnienia. To może być próba wyłudzenia pieniędzy lub danych! Zachowaj ostrożność!

Przestępcy wciąż wymyślają nowe sposoby, którymi próbują pozbawić nas naszych pieniędzy. W ostatnim czasie internetowi oszuści coraz chętniej podszywają się pod firmy kurierskie i wysyłają SMS-y z linkiem do strony, na której należy dokonać rzekomej dopłaty do przesyłki i tym samym umożliwić im wyłudzenie środków z konta bankowego. Do właścicieli telefonów zaczęły również przychodzić smsy z prośbą o uzupełnienie danych i wejście w podejrzany link w celu ich uzupełnienia. To może być próba wyłudzenia pieniędzy lub danych! Zachowaj ostrożność!

Oszuści ciągle modyfikują swoje metody działania i korzystają z każdej nadarzającej się okazji, aby wprowadzić w błąd i wykorzystać zaufanie niczego niepodejrzewających osób. Coraz chętniej podszywają się pod firmy kurierskie i wysyłają SMS-y z informacją o konieczności dopłaty do przesyłki. Zazwyczaj kwota, jaką należy wpłacić, jest bardzo niska-w granicach 1 zł. W wiadomości podany jest także link, który przekierowuje potencjalną ofiarę na stronę łudząco podobną do strony banku bądź operatora płatności, gdzie nieświadoma osoba wprowadza wrażliwe dane dotyczące konta takie jak login czy hasło i umożliwia tym samym przechwycenie tych danych przez oszustów. Ktoś, kto często otrzymuje paczki, jest łatwym celem dla przestępców, zwłaszcza jeśli oczekuje akurat na przesyłkę.

W innym wariancie wspomnianej metody, oszuści w wiadomości na przykład z prośbą o uzupełnienie danych do wysyłki przesyłają link do aplikacji, które infekują telefon. W ten sposób niepowołane osoby mogą wyciągać hasła do aplikacji bankowych, czy też przekierowywać SMS-y, dzięki czemu przejmują kontrolę nad konkretnym kontem bankowym. Telefony są bardzo często na celowniku oszustów. Głównie dlatego, że są gorzej zabezpieczane przed tego typu atakami niż komputery osobiste.

Apelujemy o ostrożność i dokładne czytanie wiadomości od rzekomych operatorów czy kurierów. Poświęcenie kilku sekund na zweryfikowanie, jaką transakcję mamy zaakceptować, może uratować nas przed utratą pieniędzy.

Inf. policjaśląska