POLICJA MAŁOPOLSKA

https://malopolska.policja.gov.pl/krk/aktualnosci/20995,Olkuska-policja-ostrzega-przed-falszywymi-SMS-ami-Sprawdz-wiarygodnosc-wiadomosc.html
2023-06-05, 05:10

OLKUSKA POLICJA OSTRZEGA PRZED FAŁSZYWYMI SMS-AMI. SPRAWDŹ WIARYGODNOŚĆ WIADOMOŚCI, ZANIM ZAPŁACISZ

Data publikacji 28.03.2022

Przestępcy próbują różnych sposobów, by przejąć nasze oszczędności. W ostatnim czasie najczęściej praktykowanym przez nich sposobem jest oszustwo na kod „BLIK". Internetowi oszuści podszywając się np. pod firmę kurierską wysyłają fałszywy SMS z prośbą o dopłatę do przesyłki bądź udając zakład energetyczny czy gazowy wysyłają wiadomość z informacją konieczności uiszczenia dopłaty w wysokości kilku złotych. Oszuści czyhają również na osoby sprzedające w sieci podszywając się pod klientów. Próbują uzyskać dane kart kredytowych swoich ofiar, a do porozumiewania się poza siecią wykorzystują komunikatory telefoniczne.Policjanci po raz kolejny apelują, aby nie otwierać nieznanych nam linków i nie ufać wszystkim wysyłanym wiadomościom.

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. Zazwyczaj kwota dopłaty zawarta w wiadomości nie jest wysoka i oscyluje w granicach kilku złotych. Przesłana informacja zawiera również link, który po kliknięciu w niego przekierowuje ofiarę na fałszywą stronę, gdzie podając swoje dane umożliwia się przechwycenie ich przez oszustów.

W sobotę, mieszkanka powiatu olkuskiego otrzymała SMS-a z prośbą o dopłatę do energii elektrycznej w wysokości 4,27 zł. 52- letnia kobieta otrzymała sms o treści „Na dzień 27.03. zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności." Była to wiadomość od oszusta, której treść zawierała link przekierowujący na fałszywą stronę banku. W ten sposób przestępca wszedł w posiadanie loginu i hasła do kobiety internetowego konta bankowego. Swoim przestępczym działaniem zasilił swoje konto o 2000 zł.

Parę dni temu do mieszkanki Olkusza, która wystawiła na OLX przedmiot na sprzedaż, poprzez komunikator WhatsApp odezwał się oszust i zaproponował, że sam zorganizuje dostawę kurierską kupowanego przez siebie towaru. Twierdził, że "ma środki na koncie InPost", złoży i opłaci zamówienie przez stronę tego popularnego dostawcy, a kobieta odbierze opłatę na swoje konto na stronie zamówienia. Miało to działać jak "przedpłata na konto". Po potwierdzeniu zamówienia do kobiety miał zadzwonić kurier, aby ustalić termin odbioru przesyłki. Kiedy olkuszanka zgodziła się, oszust przesłał jej link do fałszywej strony InPostu. Tam 41-letnia ofiara miała wybrać swój bank, wprowadzić potrzebne dane i odebrać opłatę. Oczywiście podane tam informacje trafiły wprost do przestępcy, który wykorzystał je do przejęcia środków na koncie. Kobieta straciła blisko 17000 swoich oszczędności.

Pamiętaj! Weryfikuj kto i co do Ciebie pisze. Nie wpisuj nigdzie numeru swojej karty. Nie klikaj w nieznajome linki do stron.

Apelujemy o zachowanie szczególnej ostrożności. Nie korzystaj nigdy z linków, które przychodzą w wiadomościach. Najbezpieczniej jest wpisać samodzielnie adres internetowy strony danego serwisu ogłoszeniowego lub banku. Sprawdzaj zawsze, czy witryna jest bezpieczna. Jeśli korzystasz z kodów autoryzacyjnych przesłanych SMS-em przez bank lub inne instytucje sprawdzaj, czy zawiera polskie znaki.

Trzeba też pamiętać, by przy podawaniu danych karty bankowej zachować szczególną ostrożność. Należy upewnić się, czy oszuści nie zastawili na nas pułapki.

Przed potwierdzeniem operacji zawsze sprawdź też, czy zgadza się numer konta odbiorcy oraz kwota, jaką chcesz

przelać.