POLICJA MAŁOPOLSKA

https://malopolska.policja.gov.pl/krk/aktualnosci/26551,Oszustwo-na-platformie-VINTED-metoda-na-link-do-otrzymania-zaplaty.html
2023-06-05, 04:38

OSZUSTWO NA PLATFORMIE „VINTED” METODĄ „NA LINK DO OTRZYMANIA ZAPŁATY”

Data publikacji 28.09.2022

Dwie mieszkanki powiatu nowotarskiego zostały oszukane sprzedając ubrania za pośrednictwem serwisu ogłoszeniowego Vinted. Aby otrzymać pieniądze „weszły” w link przesłany w wiadomości sms od „kupca”, wpisały dane do logowania w banku i straciły łącznie ponad 4 000 złotych. Postrzegamy i przypominamy - sprzedając w Internecie również możesz zostać oszukany. Oszuści podszywają się pod kupujących i za pomocą fałszywych linków wyłudzają dane dostępowe do kont bankowych.

Przedwczoraj do nowotarskiej komendy zgłosiły się dwie osoby, które zostały oszukane podczas sprzedaży ubrań na internetowej platformie handlowej Vinted. Mieszkanka powiatu nowotarskiego wystawiła do sprzedaży sukienkę. Bardzo szybko poprzez platformę Vinted skontaktowała się z nią osoba zainteresowana kupnem. Pod pretekstem wykonania przelewu za sukienkę, najpierw poprosiła sprzedającą o numer telefonu. Następnie w wiadomości sms przesłała link i przekonała kobietę, że aby otrzymać przelew musi „wejść” w przesłany w wiadomości link i zalogować się na stronę „swojego” banku. Tu sprzedająca popełniła błąd. Kliknęła w przesłany link prowadzący do strony przypominającej stronę aukcyjną, wybrała z listy swój bank i niczego nie podejrzewając – na fałszywej stronie banku - wpisała dane potrzebne do logowania i kody autoryzacyjne. Tymczasem oszust, mając podgląd na jej hasła na tej fałszywej stronie, zalogował się na jej rzeczywiste konto bankowe i wypłacił z jej konta ponad 2 tysiące złotych.
W ten sam sposób została oszukana nastolatka z powiatu nowotarskiego. Dziewczyna na Vinted wystawił do sprzedaży spodnie. Po wejściu w link przesłany w wiadomości sms od potencjalnego kupca i wpisaniu kodów autoryzacyjnych z banku straciła 2 tysiące złotych.

Pamiętaj! Sprzedając w Internecie również możesz zostać oszukany. Nie klikaj w linki przesłane w wiadomościach kierujące do płatności. Czytaj uważnie SMS-y autoryzacyjne.

Nie wolno reagować na prośby o zalogowanie się do konta bankowego, podania hasła jednorazowego lub jakiegokolwiek identyfikatora, loginu do banku.

Zwróć uwagę na poprawność językową strony, na której przekazujesz dane karty. Fałszywe strony często zawierają błędy, są napisane niegramatycznie.

Najbezpieczniej jest wpisać samodzielnie adres internetowy strony danego serwisu ogłoszeniowego lub banku. Sprawdzajmy zawsze, czy witryna jest bezpieczna.

Jeżeli niefortunnie staniemy się ofiarą przestępstwa, należy niezwłocznie skontaktować się telefonicznie ze swoim bankiem w celu zablokowania dostępu do rachunku lub karty bankomatowej.