

Klikając w linki czy odnośniki niewiadomego pochodzenia możemy zostać przekierowani na stronę do

złudzenia przypominającą oryginalną. Po złożeniu zamówienia, podaniu danych i dokonaniu płatności on-line oczekujemy na zakupiony towar, który w rzeczywistości nigdy nie przyjdzie. Dokonujemy transakcji nieświadomi, że podczas próby logowania do serwisu lub do banku oszuści poprzez złośliwe oprogramowanie wykradają nasze dane hasła i loginy.

Inną metodą stosowaną przez internetowych przestępców są fałszywe esemesy, podszywając się pod serwisy z aukcjami internetowymi. W otrzymanej wiadomości znajdziemy link do podstrony umożliwiającej pobranie mobilnej aplikacji. Na pierwszy rzut oka wszystko wygląda prawdziwie, ale patrząc na URL w adresie zauważymy drobne nieprawidłowości, czyli jednoznacznie potwierdzenie, że strona nie jest oryginalna.

- Nie instalujmy takich aplikacji. Cyberprzestępcy korzystają z fałszywej aplikacji serwisu, która wygląda niemal identycznie jak oryginał. Jej pobranie może skutkować utratą oszczędności znajdujących się na koncie bankowym – to kolejna policyjna przestroga.

Nie daj się okraść

- Zwracajmy uwagę na cenę oferowanego towaru – nikt nam nic nie odda za darmo.
- Weryfikujmy wiarygodność sprzedawcy, zwracając uwagę na liczbę i jakość wystawionych mu komentarzy.
- Róbmy zakupy w znanych i renomowanych sklepach internetowych.
- Dbajmy o bezpieczeństwo komputera, z którego korzystamy.
- Żaden bank nie prosi mailowo o zweryfikowanie lub podanie poufnych danych.

Źródło: <https://eglos.pl/aktualnosci/item/37692-internetowy-szal-zakupow-oraz-oszustw>