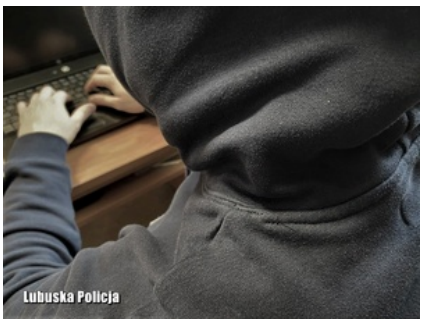
UWAŻAJ NA CYBEROSZUSTÓW! NIE KLIKAJ W PODEJRZANE LINKI CZY SMSY

Data publikacji 08.08.2022

Zielonogórscy policjanci codziennie przyjmują zgłoszenia od osób pokrzywdzonych, które zostały oszukane podczas różnych transakcji zawieranych przez Internet. Przestępcy wyłudzają pieniądze od nieświadomych osób najczęściej poprzez przesłanie fałszywych linków do stron internetowych banków, stron portali aukcyjnych czy firm kurierskich. Pamiętajmy, aby nie klikać w przesłane nam linki i dokładnie czytać treść SMS-ów od nieznanych nadawców. Nigdy podawajmy również żadnych szczegółowych danych, aby nie paść ofiarą cyberoszustów.



Nie ma dnia, żeby zielonogórscy policjanci nie otrzymali zgłoszenia od oszukanych mieszkańców, którzy przez nieostrożność w internecie tracą pieniądze. Czasami oszuści nakłaniają do kliknięcia przesłanych przez siebie linków, które kierują do fałszywych stron wyłudzających dane dostępowe do konta. Innym razem każą instalować różne aplikacje, które również umożliwiają im dostęp do naszych kont i kradzież pieniędzy. A w jeszcze innych przypadkach udają klientów, którzy chcą od nas kupić towar wystawiony na portalu aukcyjnym i wyłudzają od nas dane, żeby następnie nas okraść. Często też zdarzają się przypadki fałszywych ofert na sprzedaż różnego rodzaju towarów, które po opłaceniu nie docierają do klientów.

Czasami jest też tak, że poprzez kliknięcie przesłanego przez oszustów linku, nieświadomie instalujemy program hakerski, poprzez który przestępcy uzyskują dostęp do kontaktów w naszym telefonie i wysyłają bez naszej wiedzy i zgody prośbę do znajomych o pożyczkę, a ci także nieświadomie przekazują pieniądze przestępcom. Pamiętajmy, aby po otrzymaniu takiej wiadomości natychmiast zablokować numer i skasować taką wiadomość bez sprawdzania. Radzimy ją skasować także po to, żeby przez przypadek nie uruchomić hakerskiego oprogramowania, które może doprowadzić do przykrych konsekwencji: kradzieży, blokady telefonu, utraty ważnych czy poufnych danych lub też wyłudzenia

pieniędzy od naszych znajomych.

Pamiętajmy o bezpieczeństwie przy korzystaniu z Internetu. Chrońmy swoje dane — nie podawajmy danych do logowania na konta bankowe czy numerów kart, w żadnym wypadku nie skanujmy i nie wysyłajmy zeskanowanych dokumentów takich jak na przykład dowód osobisty. Nie przekazujmy też żadnych poufnych informacji przez telefon. Nie klikajmy na podane linki i nie instalujmy w ten sposób aplikacji, aby nie narazić się na utratę oszczędności życia.

Jak mogą działać oszuści?

1. Sprzedajesz coś na portalu aukcyjnym.
2. Kupujący zgłasza się do ciebie, ale tylko na komunikatorze.
3. Kupujący twierdzi, że wysłał pieniądze na portal aukcyjny i wysyła link, gdzie rzekomo „odbierzesz” swoje pieniądze.
4. Klikasz w link, który przekieruje cię do fałszywej strony portalu aukcyjnego, banku albo firmy kurierskiej.
5. Ta fałszywa strona wymaga od ciebie podania danych dostępu do twojego konta bankowego albo danych twojej karty.
6. Oszuści w kilka minut robią sobie przelewy albo zaciągają kredyt na twoim koncie, a pieniądze wypłacają kodem blik w bankomacie.
7. Do ciebie przychodzi sms z banku z kodem potwierdzającym – ale ty niestety nie czytasz dokładnie co potwierdzasz.

Jak ustrzec się przed oszustwem?

1. Za rzeczy sprzedawane na portalu aukcyjnym przyjmuj jedynie wpłaty na konto.
2. Nie zgadzaj się na żadne „pośrednie” formy płatności. Żadnych linków i żadnych płatności „za pomocą” innych portali czy stron.
3. Nigdy nie klikaj w żadne linki przysłane przez obce osoby.
4. Nigdy nie podawaj danych do logowania do konta lub do karty na niesprawdzonych stronach internetowych.
5. Zawsze loguj się do swojego banku z twojego komputera.
6. Zawsze czytaj SMS-y z banku i sprawdź jaką transakcję czy czynność potwierdzasz. Nie klikajmy w żadne linki przysłane przez nieznane nam osoby.

(KWP w Gorzowie Wlkp. / kp)