

Kolejny raz ostrzegamy

Data publikacji: 14.03.2022 13:10

Coraz większa liczba zgłoszeń oszustw internetowych od osób, które tracą pieniądze - to efekt działalności cyberprzestępców. Przed oszustami ostrzega policja. - To, czy przestępcy wyłudzą od nas pieniądze, zależy przede wszystkim od nas samych - podkreślają mundurowi



Fot: ilustracyjne /pixabay.com

Oszuści nieustannie doskonalą i modyfikują swoje metody działania i korzystają z każdej nadarzającej się okazji, aby wprowadzić nas w błąd, wykorzystać nasze zaufanie i okraść z pieniędzy. Zakupy przez internet to też doskonała okazja dla oszustów próbujących wykraść nasze hasła, dane i pieniądze.

W tej opcji oszuści podszywają się pod firmy kurierskie i za pomocą SMS-a informują o konieczności dopłaty do przesyłki. Zazwyczaj kwota, jaką należy wpłacić, jest bardzo niska i nie wzbudza naszego podejrzenia. W wiadomości podany jest także link, który przekierowuje potencjalną ofiarę na stronę łudząco podobną do strony banku, gdzie osoba wprowadza wrażliwe dane dotyczące konta, takie jak login czy hasło i umożliwia tym samym przechwycenie tych danych i przejście kontroli przez oszustów nad konkretnym kontem bankowym.

Innym wariantem, z którego chętnie korzystają oszuści, jest SMS z prośbą o dopłatę do rachunku za prąd. Przestępcy podszywają się pod zakład energetyczny i poprzez wiadomość SMS, informują, że trzeba będzie dopłacić niewielką kwotę, by uregulować zaległości, co wstrzyma wydaną dyspozycję odcięcia dopływu energii elektrycznej do twojego domu. W SMS-ie zamieszczają link przekierowujący do bankowości elektronicznej. W momencie, kiedy w niego klikniemy, pozwalamy dysponować swoim kontem.

Wystawiłeś przedmiot na sprzedaż? Uważaj, możesz paść ofiarą oszustwa. Przestępcy wyszukują oferty sprzedaży, a potem kontaktują się ze sprzedawcą przez SMS lub jeden z popularnych komunikatorów i od razu deklarują, że są zainteresowani zakupem. Sprzedawca otrzymuje wiadomość od osoby potencjalnie zainteresowanej kupnem, która proponuje zapłatę poprzez specjalny link wysłany do sprzedawcy. Żeby sfinalizować transakcję, wymaga podania danych z karty płatniczej tj. numeru, daty ważności, kodu CVV/CVC, często też hasła jednorazowego, który przychodzi SMS-em na telefon zaraz po podaniu danych karty. Gdy ofiara wpisze takie dane, zamiast otrzymać zapłatę za towar, z jej konta znikną wszystkie oszczędności.

Policjanci ostrzegają!

Aby uniknąć problemów, należy dokładnie i uważnie czytać otrzymywane wiadomości, a przede wszystkim nie „klikać” w podejrzaną linki, szczególnie jeśli prowadzą do systemów elektronicznych płatności. Poświęcenie kilku sekund na zweryfikowanie, jaką transakcję mamy zaakceptować, może uratować nas przed utratą pieniędzy, danych osobowych, a także zawartego na nasze konto kredytu.

red./mat.pras.