UWAŻAJMY NA NOWĄ METODĘ OSZUSTWA "NA POCZTĘ GŁOSOWĄ"

Coraz częściej słyszy się o oszustach internetowych, którzy podszywają się pod różne instytucje wysyłając fałszywe linki. Ich celem jest otrzymanie dostępu do kont bankowych oraz kont do mediów społecznościowych. Oszuści wciąż modyfikują swoje przestępcze metody, m. in. te dotyczące nadsyłanych SMS-ów, chcąc stworzyć wrażenie legalności takiej wiadomości. Ostatnio policjanci otrzymują zgłoszenia dotyczące oszustwa "na pocztę głosową".

Kolejnym pomysłem oszustów internetowych jest podszywanie się pod operatora telekomunikacyjnego. Oszust wysyła wiadomość z linkiem, która sugeruje o nieodsłuchanej poczcie głosowej, oraz podaje link prowadzący na stronę internetową z fałszywym komunikatem o “nowej poczcie głosowej”.

Po kliknięciu na link ściągniemy na swój telefon złośliwe oprogramowanie, co może doprowadzić do kradzieży pieniędzy z naszego rachunku bankowego. Wiadomości rozsyłane są z różnych numerów ale **najczęściej pojawiają się takie z prefiksami z Niemiec (+49).**

Co zrobić gdy kliknąłeś w link i zainstalowałeś podejrzane oprogramowanie? Wyłącz telefon i przełóż kartę SIM do innego telefonu, skontaktuj się ze swoim bankiem, zmień hasła. Bliźniacze oszustwa mogą dotyczyć również SMS-ów związanych z aplikacją dyskontów spożywczych, serwisów aukcyjnych, instalacji sterowników LTE, RODO.

Nie klikajmy w linki z SMS-ów, nie dokonujmy płatności poprzez linki w SMS-ach, nie ściągajmy aplikacji proponowanych w SMS-ach.

(KWP w Opolu / mw)