

Konsumenci coraz częściej padają ofiarą cyberoszustów. Ich metody są coraz bardziej wyszukane i niemal każdego dnia przybierają nowe formy. Skuteczność przestępczych działań zwiększa wykorzystywanie emocji potencjalnych ofiar, ich trudnych czy też zwykłych, życiowych sytuacji. Aby zwrócić uwagę społeczeństwa na ten problem, Prezes Urzędu Ochrony Konkurencji i Konsumentów Tomasz Chróstny zainicjował kampanię „Stracisz dane, stracisz pieniądze!”. Ostrzega w niej przed groźbą utraty danych i środków finansowych oraz apeluje o wzmożoną ostrożność konsumentów.

- Konieczne są intensywne działania informacyjne i edukacyjne na temat oszustw, których ofiarami padają konsumenci, w tym seniorzy. Elektroniczne transakcje i płatności, aplikacje ułatwiające załatwianie spraw stały się już naszą codziennością. Niestety, przestępcy nie pozostają w tyle. Nie muszą już kraść portfela, żeby pozbawić nas środków do życia. Wystarczy, że ukradną nasze dane. Chwyty socjotechniczne mogą osłabić czujność konsumentów. Poczucie zagrożenia, strachu czy presji często uniemożliwia im chłodną ocenę sytuacji. Uważajmy, każdy z nas może znaleźć się na celowniku przestępców – mówi Tomasz Chróstny, Prezes UOKiK.

Spoty kampanii „Stracisz dane, stracisz pieniądze!”, które można zobaczyć m.in. w TVP i usłyszeć w Polskim Radiu, skupiają się na wybranych sytuacjach, w których może dojść do wyłudzenia danych i kradzieży pieniędzy z rachunku bankowego. Spoty dostępne są [tutaj](#).

Niedopłata

Metoda na niedopłatę polega na wysłaniu SMS-a lub e-maila, w którym oszust informuje o rzekomej zaległości w płatnościach i jednocześnie grozi natychmiastowym odcięciem np. prądu, gazu lub telewizji. W wiadomości jest link do płatności. Kliknięcie przekierowuje na fałszywą stronę przypominającą strony pośredników płatności. W ten sposób oszuści zdobywają dane uwierzytelniające.

Podszywanie się pod pracownika instytucji

Często dochodzi również do sytuacji, w których oszust podaje się np. za pracownika banku i straszy, że zagrożone są pieniądze właściciela rachunku. Następnie prosi o podanie loginu i hasła do konta. Może też namawiać do kliknięcia w link lub zainstalowania aplikacji, która w rzeczywistości będzie umożliwiać śledzenie aktywności i pozyskanie w ten sposób danych do logowania.

To tylko przykładowe pułapki - oszuści niemalże codziennie wymyślają nowe. Wstrzymanie przesyłki lub realizacji zamówienia, planowane odłączenie dostępu do internetu... Czasem czujność konsumentów usypia niewielka kwota, np. 2 zł. W ten sposób też można stracić oszczędności życia.

STOP! Nie daj się zmanipulować oszustom! Pamiętaj!

1. Nigdy nie podawaj ani nie wysyłaj nikomu loginu i hasła do bankowości internetowej czy aplikacji mobilnej. Prawdziwy pracownik banku nie będzie cię o to pytać.
2. Nigdy nie klikaj w linki przesłane SMS-em. Potwierdź ewentualne istnienie zaległości samodzielnie, kontaktując się np. z dostawcą gazu czy firmą kurierską.
3. W przypadku telefonu od osoby przedstawiającej się jako pracownik banku, rozłącz się, samodzielnie znajdź numer infolinii i potwierdź, czy ktoś do ciebie dzwonił.
4. Nigdy nie instaluj oprogramowania z przesłanych linków ani w trakcie rozmowy telefonicznej, dotyczącej twojego rachunku lub środków na nim zgromadzonych.

"Stracisz dane, stracisz pieniądze!" - startuje kampania Prezesa UOKiK

Kategoria: Aktualności

Opublikowano: poniedziałek, 05, grudzień 2022 18:17

Tomasz Smaś

Odśłony: 763

Co zrobić w sytuacji, gdy oszustom udało się zdobyć dostęp np. do rachunku płatniczego lub danych karty płatniczej? Jak najszybciej należy poinformować swojego dostawcę usług płatniczych, zastrzec kartę i zmienić dane do logowania lub zablokować rachunek płatniczy. Dzięki temu uniemożliwimy oszustom kradzież środków lub w przypadku, gdy już do niej doszło - zapobiegniemy wykonywaniu dalszych transakcji. Jak najszybciej należy zgłosić także sprawę policji i poinformować o tym swojego dostawcę usług płatniczych.

Źródło: UOKiK