

NIE DAJ SIĘ ZŁAPAĆ NA PHISHING

Data publikacji 21.12.2020

Internetowi oszuści chwytają się różnych sposobów. Często podszywają się pod firmy kurierskie i wysyłają sms-y z informacją o konieczności dopłaty do przesyłki. Poszkodowany klika w link, który ma podany w odebranej wiadomości. Wprowadza dane do swojego konta i zamiast niewielkiej sumy, którą ma rzekomo dopłacić, często traci kilka tysięcy złotych.

Dlatego robiąc zakupy przez internet zachowajmy ostrożność. W świecie wirtualnym nie brakuje nieuczciwych sprzedawców, którzy w łatwy i szybki sposób chcą osiągnąć zysk.

Jedną z internetowych metod, po które sięgają oszuści, jest tak zwany phishing. Oszuści podszywają się pod firmy kurierskie, sklepy internetowe, dostawców prądu czy gazu. Wysyłają sms-y o konieczności dopłaty. Zazwyczaj, kwota jaką należy wpłacić jest niska. Aby usprawnić nam szybkie załatwienie sprawy, w wiadomości podają link, który przekierowuje na stronę łudząco podobną do banku lub operatora płatności. Kiedy klikniemy w niego, następnym krokiem jest wprowadzenie danych wrażliwych, które oszust przechwytuje i dzięki nim może się zalogować na nasze bankowe konto.

Ofiarą takiego właśnie oszustwa padł 36-letni mieszkaniec Brzegu. Na swój telefon otrzymał wiadomość sms, z której wynikało, że do zamówionej przesyłki musi dopłacić brakującą kwotę 0,50 zł. Po kliknięciu w podany w wiadomości link wprowadził swój login, hasło i autoryzował przelew bankowy. W ten sposób stracił 5 000 złotych.

Jak się chronić przed taką utratą pieniędzy?

Przede wszystkim nie klikajmy w nieznane linki w wiadomościach czy mailach. A jeśli nam się to zdarzy, dokładnie sprawdzajmy, na jakiej stronie się znajdujemy. Czytajmy też dokładnie wiadomości od rzekomych operatorów czy kurierów - bardzo często pełne są literówek czy błędów - a także sms-y z banku. Poświęcenie kilku sekund na sprawdzenie, jaką transakcję mamy zaakceptować, może uratować nas przed stratą pieniędzy.

Pamiętajmy również, że bank nigdy nie prosi nas o wpisanie całego hasła, a jedynie kilku znaków w nim zawartych. Kiedy musimy wpisać całe hasło to sygnał, że nie jesteśmy na platformie banku, tylko łudząco podobnej stronie stworzonej przez oszustów.