POLICJA LUBUSKA

https://lubuska.policja.gov.pl/go/serwis-informacyjny/aktualnosci/39691,Zadbaj-o-swoja-tozsamosc-nie-ulatwiaj-dzialania-oszustom.html
2022-01-27, 01:36

ZADBAJ O SWOJĄ TOŻSAMOŚĆ - NIE UŁATWIAJ DZIAŁANIA OSZUSTOM

Data publikacji 19.11.2021

Wiele mówi się na temat płatności mobilnej i oszustw dokonywanych za jej pośrednictwem. Błąd który najczęściej popełniamy, to brak weryfikacji otrzymanej wiadomości, który może nas dużo kosztować. Ma to jednak swój początek, gdyż zanim oszust zwróci się do nas o BLIKa, musiał wcześniej ukraść tożsamość naszych znajomych. Pamiętaj, że nie dbając o ochronę danych i prywatność w sieci, ułatwiasz działanie oszustom.

Informacji o oszustwach metodą na „BLIKa ” możemy znaleźć wiele. Mimo to w dalszym ciągu oszuści osiągają cel i wykradają pieniądze z konta bankowego swojej ofiary. Najczęściej podszywają się pod znajomych prosząc o szybką pożyczkę, zapłacenie przesyłki lub dopłatę do zakupów. Takie historie dostosowane są do rozmówcy, za którego się podszywają. Zanim jednak dojdzie do wyłudzenia pieniędzy, dochodzi do kradzieży tożsamości osoby, za którą się podają. Dzieje się to wówczas, gdy nienależycie chronimy dane i prywatność w sieci. Nie korzystamy z dobrych programów antywirusowych, stosujemy proste hasła i wykorzystujemy je do logowania w różnych serwisach. Często korzystamy z sieci publicznych Wi-Fi, czy też stron których połączenia nie są szyfrowane. Znakomitym źródłem danych są portale społecznościowe, gdzie na profilach zamiast zadbać o prywatność, udostępniamy wszystkim swoje dane. Przestępcy kradnąc tożsamość osoby mają już pierwszy krok za sobą. Wysyłają następnie do jej znajomych wymyślone zdarzenie z prośbą o przesłanie numeru BLIK. Często osoba, której tożsamość została skradziona, dopiero po telefonach od znajomych dowiaduje się, że doszło do włamania na konto i zanim zareaguje, ktoś zawierzy oszustowi i stanie się jego ofiarą.

Tak było w przypadku mieszkanki powiatu krośnieńskiego, która będąc przeświadczoną, że pomaga koleżance w opłacie przesyłki, ponieważ ta miała problem z zalogowaniem się do banku, udostępniła BLIKa oszustowi. Na jego działanie nie musiała długo czekać. Już po chwili z jej konta bankowego zniknęło 800 złotych. Takie sytuacje jak ta, zdarzają się w

Polsce dość często. Dlatego otrzymując wiadomość z prośbą o przesłanie numeru BLIK, pierwszą czynnością jaką musisz zrobić, to zweryfikować treść smsa. Wykonaj ją za każdym razem, gdy otrzymasz taką prośbę. W ten sposób upewnisz się, czy dana osoba faktycznie potrzebuje pomocy, czy też stałaś/eś się potencjalną ofiarą oszusta.

Ponadto korzystając z płatności mobilnych i stron internetowych:

-stosuj zasadę ograniczonego zaufania i nie działaj w pośpiechu;

-zawsze chroń swoje konta internetowe i nigdy nie udostępniaj haseł do logowania;

-pamiętaj o każdorazowym wylogowaniu się z konta;

-używaj różnych haseł do poszczególnych kont i zadbaj, żeby ich kombinacja liter, cyfr i znaków była trudna do złamania;

-nie udostępniaj nikomu wygenerowanych kodów do transakcji internetowych;

-nie wchodź na dołączone do wiadomości linki i nie loguj się przez nie na swoje konto bankowe (dotyczy to także otrzymanych wiadomości email);

-zawsze zwracaj uwagę na logo, nazwę i adres URL strony internetowej. Sprawdzaj czy po lewej stronie linku znajduje się mała kłódka oraz wyrażenie „https” świadczące o tym, że dane połączenie jest szyfrowane;

-robiąc przelew, upewnij się o prawidłowości numeru konta adresata oraz przesyłanej kwoty;

-zanim potwierdzisz otrzymany z banku kod do przelewu, upewnij się czy widniejąca w treści sms kwota jest właściwa;

-przypominaj o tych zasadach w rozmowie z rodziną i znajomymi, w ten sposób pomożesz im ustrzec się przed działaniem oszustów.

podkomisarz Justyna Kulka

Komenda Powiatowa Policji w Krośnie Odrzańskim