KOMENDA POWIATOWA POLICJI W RADOMSKU

http://radomsko.policja.gov.pl/era/informacje/71808,Dostales-smsa-o-nieuregulowanym-rachunku-za-energie-elektryczna-badz-gaz-Uwazaj-.html
2023-02-05, 07:59

DOSTAŁEŚ SMS'A O NIEUREGULOWANYM RACHUNKU ZA ENERGIĘ ELEKTRYCZNĄ BĄDŹ GAZ? UWAŻAJ, TO MOŻE BYĆ OSZUSTWO

Phishing to rodzaj oszustwa, który polega na podawaniu się za inną osobę, podszywaniu się pod firmę lub instytucję w celu wyłudzenia poufnych informacji, danych logowania, danych karty kredytowej, konta bankowego lub używanych haseł. W naszym regionie złodzieje w ciągu ostatnich kilku dni podszywają się pod „PGE" i żądają od swoich potencjalnych ofiar dopłat do energii. Nie dajcie się nabrać, nie klikajcie w załączone linki. Te wiadomości to pułapka.

Radomszczańscy policjanci ostrzegają przed oszustami podszywającymi się pod „PGE", którzy za pośrednictwem wiadomości SMS, wzywają do uregulowania należności grożąc odłączeniem energii. Jest to jedna z metod działania oszustów. Zazwyczaj w wiadomościach jest informacja o konieczności dokonania dopłaty oraz link, który ma teoretycznie pozwolić szybko rozwiązać problem. W rzeczywistości zostaniemy przekierowani na fałszywą stronę, gdzie ofiara ma do wyboru kilka metod płatności. Jeżeli natychmiast nie przerwiemy tej operacji, w tym miejscu nastąpi próba wyłudzenia danych kart lub loginów oraz haseł do bankowości elektronicznej.

W ostatnich dniach z różnych numerów telefonów rozsyłane są SMS-y o treści "PGE również w powiecie radomszczańskim i bełchatowskim. Treść takiej wiadomości to przykładowo: „Na dzień 27.04 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności: https://xvxvxv.... Treść zawiera link, za którego pośrednictwem można pobrać aplikację. Ostrzegamy - to oszustwo i próba kradzieży pieniędzy z konta bankowego adresata. Przestępcy, podszywając się pod różnego rodzaju portale ogłoszeniowe, czy też firmy kurierskie wysyłają do przypadkowych osób powyższe wiadomości. Zależy im, aby adresat wiadomości szybko kliknął w link i zainstalował na swoim telefonie złośliwe oprogramowanie, które umożliwi przejęcie kontroli nad telefonem i dostanie się do bankowości mobilnej. Link może również przekierować nas na fałszywą stronę banku. Wówczas przestępcy mogą wejść w posiadanie loginu i hasła do naszego internetowego konta bankowego.

Przestrzegamy przez sprawcami oszustw. Ich metody są cały czas udoskonalane, dlatego bardzo ważne jest, żebyśmy nie robili niczego pochopnie i pod presją czasu. Zanim dokonamy płatności musimy zweryfikować czy opisana w wiadomości sytuacja faktycznie ma miejsce. Nigdy też nie wchodźmy w otrzymane linki, które przekierowują nas na fałszywe strony banku. Nie dajmy się zwieźć, gdyż są one łudząco podobne do tych, z których korzystamy na co dzień. Podczas logowania się musimy być bardzo ostrożni i czujni. Ważne jest także, żebyśmy o metodach stosowanych przez oszustów rozmawiali z najbliższymi. To pozwoli im ochronić nie tylko pieniądze, ale i dane osobowe.

nadkom. Aneta Wlazłowska