ODPOWIE ZA OSZUSTWO

Data publikacji 25.11.2011

Za oszustwo odpowie 20-letni mieszkaniec gm. Hańsk, który wspólnie z innymi osobami posługując się tzw. metodą phishingu, wyprowadził z kont bankowych dwojga obywateli Niemiec środki pieniężne w kwocie około 27 tys. zł. Wobec podejrzanego prokurator zastosował dozór policji oraz poręczenie majątkowe. Za oszustwo grozi kara do 8 lat pozbawienia wolności.

W miniony wtorek włodawscy kryminalni przy współpracy z policjantami Wydziału do walki z Przestępczością Gospodarczą KWP w Lublinie zatrzymali 20-letniego mieszkańca gm. Hańsk.Jak wynikało z ustaleń policjantów z Komendy Wojewódzkiej Policji w Lublinie, 20-latek w celu osiągnięcia korzyści majątkowej doprowadził do niekorzystnego rozporządzenia mieniem dwoje obcokrajowców. Posługując się metodą phishingu z kont bankowych obywateli Niemiec wyprowadzone zostały środki pieniężne w łącznej kwocie około 27 tys. zł. Pieniądze te później zostały przelane na konto bankowe 20-latka. Młody mężczyzna ze swojego konta zdołał przetransferować dalej 12 tys. zł.

Jak ustalili policjanci z Wydziału dw. z Przestępczością Gospodarczą KWP w Lublinie, 20-latek na jednym z portali znalazł ofertę pracy. Polegała ona na przyjmowaniu wpłat pieniędzy na swoje konto osobiste, a później przelewaniu gotówki do wskazanego klienta. Za swoją pracę miał otrzymywać miesięczne wynagrodzenie.

Prokurator Rejonowy we Włodawie zastosował wobec podejrzanego dozór policji oraz poręczenie majątkowe. Dalsze postępowanie w sprawie prowadzą policjanci z Komendy Powiatowej Policji we Włodawie. Sprawa ma charakter rozwojowy. Śledczy ustalają inne osoby zamieszane w proceder. Przestępstwo oszustwa zagrożone jest karą do 8 lat pozbawienia wolności.

Policjanci przypominają: phishing polega na tworzeniu oszukańczych wiadomości e-mail i witryn WWW, które wyglądają identycznie jak serwisy internetowe znanych firm, aby skłonić klientów tych firm do podania swoich danych osobowych, numeru karty kredytowej lub informacji o elektronicznym rachunku bankowym – kodów i haseł potrzebnych do zalogowania i autoryzacji transakcji. Typowy atak phishingowy składa się zazwyczaj z dwóch głównych elementów: autentycznie wyglądającej wiadomości e-mail oraz fałszywej strony WWW. Pozyskane w ten sposób dane wykorzystywane są do oszukańczych transakcji internetowych lub kradzieży pieniędzy z rachunków bankowych. Sprawcy phishingu korzystają z pośredników często określanych mianem „ mułów” osób - nieświadomych pochodzenia pieniędzy, które przyjmują na swoje konto.

(KWP w Lublinie / ep)