PKO BP OSTRZEGA PRZED CYBERATAKAMI NA KONTA BANKOWE

Największy polski bank PKO BP S.A. ostrzega przed nowym rodzajem oszustw z wykorzystaniem bankowości elektronicznej. Hakerzy włamują się na konta na Facebooku i wysyłają do znajomych ofiary prośbę o przelew na małą kwotę. Następnie wysyłają fałszywy link, który ułatwia kradzież pieniędzy.

Jak czytamy w komunikacie PKO BP, cyberprzestępca, po przejęciu cudzego konta na Facebooku, loguje się na nie i wysyła do znajomych użytkownika wiadomość z prośbą o pomoc, tj. dokonanie przelewu na drobną kwotę (nadawca wyjaśnia zwykle, że do dokonania płatności zabrakło mu kilku złotych i prosi „znajomego" o jej uzupełnienie).

Następnie nadawca przesyła potencjalnej ofierze link do dokonania płatności internetowej za pośrednictwem jednego z popularnych serwisów oferujących płatności natychmiastowe (np. Przelewy24, Dotpay, BlueCash, itp.), a w rzeczywistości do fałszywej strony pośrednika, umieszczonej na kontrolowanym przez oszusta serwerze.

Gdy odbiorca wybiera na stronie „płatności" swój bank i klika na stosowną ikonę, zostaje przekierowany na fałszywą stronę do logowania do banku. Podanie na tej stronie danych do logowania umożliwia ich przejęcie przez oszusta, który natychmiast loguje się przy ich użyciu w autentycznym serwisie internetowym banku i zleca dyspozycję utworzenia nowego szablonu zaufanego odbiorcy na wskazany przez siebie rachunek. W tym czasie na fałszywej stronie banku pojawia się komunikat z prośbą o wprowadzenie kodu jednorazowego w celu autoryzacji przelewu na małą kwotę, o którego wykonanie prosił „znajomy" z Facebooka.

Czytaj także: Ekspert: Atak na KNF skoordynowany i bardzo dobrze zaplanowany

Podany przez klienta kod w rzeczywistości jest wykorzystywany przez przestępcę do zatwierdzenia dyspozycji utworzenia odbiorcy zdefiniowanego, przy użyciu którego może on potem zlecać z rachunku klienta – bez dodatkowej autoryzacji – przelewy na znacznie większe kwoty.

PKO BP ostrzega swoich klientów, żeby logując się do serwisu internetowego, zawsze wprowadzali adres strony ręcznie – nie korzystając z linków. Ponadto radzi sprawdzać poprawność adresu strony, widniejącego w przeglądarce internetowej. Bank ostrzega też, że podczas logowania do serwisu ani bezpośrednio po zalogowaniu do niego nie jest wymagane podawanie kodu z narzędzia autoryzacyjnego. - Przed potwierdzeniem operacji zlecanej w serwisie iPKO kodem SMS przeczytaj uważnie treść otrzymanego SMS-a, aby upewnić się, że dotyczy on właściwej operacji (zwróć uwagę na rodzaj dyspozycji, poprawność numeru rachunku odbiorcy, kwotę transakcji) – czytamy w komunikacie banku największego polskiego banku.