

Komunikat w sprawie „phishingu” danych

Do Urzędu Komisji Nadzoru Finansowego (dalej: UKNF) od pewnego czasu napływają sygnały wskazujące na znaczne ryzyko związane z zakładaniem rachunków bankowych, bądź uzyskiwaniem kredytów bankowych z wykorzystaniem informacji wyłudzonych od obywateli, głównie przez internet¹. Jednym z mechanizmów zgłaszanych przez poszkodowanych tym procederem jest gromadzenie podstawowych danych osobowych, adresów, numerów dowodów tożsamości w ramach procesu rzekomej rekrutacji do pracy „w domu”. Potencjalnie nieuczciwi/fałszywi pracodawcy wymagają podania tych informacji i dokonania przelewu drobnej kwoty (np. 1 zł) na wskazany przez nich rachunek bankowy. Tym sposobem na podstawie wyłudzonych danych osobowych próbują założyć rachunki bankowe bądź pozyskać kredyty, a w niektórych przypadkach jako mechanizm weryfikacji tożsamości wykorzystywane są przez banki właśnie przelewy pochodzące z innego rachunku bankowego danej osoby. Pokrzywdzony staje się tym samym dłużnikiem banku z tytułu uzyskanego kredytu, a w przypadku założenia rachunku bankowego z wykorzystaniem jego danych osobowych, przez ten rachunek mogą być transferowane środki pochodzące z przestępstw.

W związku z powyższym, niezmiernie istotne jest zwrócenie uwagi na konieczność nieujawniania w sytuacjach wzbudzających jakiegokolwiek wątpliwości swoich danych, w szczególności tych zapisanych w dowodzie osobistym.

Podkreślić należy również, że bardzo niebezpieczne może być przeprowadzanie na zlecenie nieznanych osób operacji przelewu środków z wykorzystaniem własnego rachunku bankowego (często w zamian za gratyfikację pieniężną). Osoba, która dokonuje takiej transakcji, nie wie, czy

¹ Mechanizm pozyskiwania danych jest zwany „phishingiem”. Jest to forma oszustwa, która może polegać m.in. na wysyłaniu do użytkowników bankowości internetowej fałszywych maili z prośbą o podanie danych autoryzacyjnych lub umieszczaniu w mailach linku z przekierowaniem do fałszywej strony internetowej banku.

środki nie pochodzą z przestępstwa, ani tym bardziej w jakim celu są one przekazywane. Za szczególnie niebezpieczny należy uznać schemat działania, w którym jesteście proszeni o dokonanie wypłaty otrzymanej kwoty przelewu i następnie przekazanie jej za pośrednictwem banku lub instytucji płatniczej. W przypadku, gdyby rzeczywiście przekazywane środki pochodziły z przestępstwa, jakakolwiek styczność z nimi, a w szczególności przyjęcie ich na własny rachunek bankowy, może zostać uznane za samoistne przestępstwo bądź współudział w przestępstwie.

Pamiętać należy również, że korzystanie z bankowości internetowej bez zachowania odpowiednich standardów bezpieczeństwa może stwarzać znaczne zagrożenia. Najpoważniejszym jest niebezpieczeństwo dostępu bez naszej wiedzy i zgody do rachunku przez nieuprawnione osoby. Zdarza się, że użytkownicy bankowości internetowej nieświadomie wchodzi na fałszywe strony bankowe lub reagują na prośby o podanie mailem danych osobowych i danych do logowania. Zastosowanie się do takich poleceń może spowodować nawet całkowitą utratę zgromadzonych na rachunku środków.

W razie zaistnienia symptomów opisanych powyżej konieczne jest przekazanie szczegółowych informacji do banku bądź instytucji płatniczej prowadzącej rachunek, które są zobowiązane w zakresie swojej działalności do powiadamiania o przestępstwie odpowiednich organów państwa.

W związku z powyższym UKNF sugeruje zachowanie daleko posuniętej ostrożności w powyższych sytuacjach i bezwzględne chronienie swoich danych osobowych.