

Policja przestrzega przedsiębiorców korzystających z Programu Tarcza Finansowa PFR przed działaniami oszustów

Okres pandemii koronawirusa COVID-19 jest wykorzystywany przez przestępców, którzy dostrzegają swoją szansę w pozyskaniu środków pochodzących z rachunków klientów banków, w tym pozyskanych w ramach Programu Tarczy Finansowej PFR. Przestępcy wykorzystują trudny czas, jakim jest pandemia, wymyślając coraz to nowe scenariusze oszustw, często oparte na strachu przed skutkami koronawirusa.

Wiemy, że oszuści dzwonią, głównie do osób prowadzących działalność gospodarczą, proponując pomoc w złożeniu wniosku i uzyskaniu subwencji finansowych w ramach Tarczy Finansowej PFR. W trakcie rozmowy przestępcy starają się namówić rozmówców do skorzystania z ich usług w zakresie złożenia wniosku o wsparcie finansowe, który można złożyć za pośrednictwem bankowości elektronicznej. Wmawiają przy tym przedsiębiorcy, że jest to proces bardzo skomplikowany i czasochłonny, sugerując, że bez eksperckiego wsparcia sobie nie poradzi – używają przy tym wysublimowanych metod socjotechnicznych.

Podczas połączenia przestępcy proszą o podanie:

- danych osobowych;
- loginów i haseł do bankowości internetowej;
- treści SMS – kodów.

Pozyskanie takich danych pozwala przestępcom na wyprowadzanie środków z rachunków bankowych przedsiębiorcy, zarówno tych zdeponowanych już na nim, jak i tych, które wpłyną w ramach pomocy publicznej.

W związku z powyższym, w przypadku otrzymania oferty pomocy przy złożeniu wniosku w ramach Programu Tarczy Finansowej PFR Komenda Główna Policji oraz FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP zaleca:

- niepodawanie loginu i hasła do bankowości internetowej, które powinien znać tylko jego właściciel;
- niepodawanie innych informacji wrażliwych np. danych osobowych, a w szczególności adresu skrzynki poczty elektronicznej;
- upewnienie się, że osoba dzwoniąca do przedsiębiorcy, jest faktycznie tą, za którą się podaje;
- nieotwieranie wiadomości poczty elektronicznej i załączonych do niej dokumentów lub linków, które pochodzą od osoby dzwoniącej lub innych podmiotów oferujących pomoc w założeniu wniosku w ramach Programu Tarczy Finansowej PFR – to działanie może mieć na celu zainfekowanie sprzętu, którym posługuje się w przedsiębiorca;
- jeżeli osoba dzwoniąca podaje się za funkcjonariusza Policji i twierdzi, że środki w Banku są w niebezpieczeństwie – nie należy wierzyć, zaleca się zerwanie połączenia i wykonanie samodzielnego połączenia na infolinię Banku;
- nieinstalowanie dodatkowego oprogramowania, na urządzeniach z których następuje logowanie do bankowości internetowej.

Należy zachować zdrowy rozsądek oraz dużo ostrożności przy kontakcie telefonicznym. Nie ulegajmy presji, nie dajmy skusić się pozornie atrakcyjnymi ofertom, nie działajmy pod wpływem chwili.

Klienci banków w sytuacjach nietypowych zawsze mają prawo skontaktować się ze swoim bankiem, a w przypadku gdy podejrzewają, że dochodzi do popełnienia przestępstwa, mają prawo zgłosić to na Policji.

Aby uzyskać więcej informacji, warto odwiedzić stronę Związku Banków Polskich – <https://zbp.pl/Aktualnosci/Wydarzenia/Uwaga!-przestepcy-atakuj-a-przedsiębiorców-korzystających-z-Programu-Tarcza-Finansowa-PFR>

źr.: Komenda Główna Policji/ FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP