Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
z dnia XX października 2021 r.
w sprawie podszywania się oszustów pod pracownika banku oferujących samorządom lokaty bankowe np. „Lokatę bliżej samorządów”

Szanowni Państwo,

W ramach prowadzonego monitoringu oraz we współpracy z bankami FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP ustalił, że w ostatnim okresie jednostki administracji samorządowej narażone są na bezpośrednie ataki ze strony przestępców, którzy podszywają się pod pracowników banków i z użyciem socjotechniki podejmują próbę wyłudzenia środków, oferując założenie lokaty terminowej w banku np. „Lokaty bliżej samorządów”.

Najnowszy scenariusz oszustwa można opisać w 5 krokach:

1. Kontakt telefoniczny lub mailowy osoby podszywającej się pod pracownika banku (oszusta) ze skarbnikiem urzędu miasta/gminy,
2. Oszust przedstawia ofertę produktu specjalnego – lokatę terminową – „Lokata bliżej samorządów” oraz proponuje otwarcie rachunku technicznego do obsługi lokaty, przesyła również via mail umowę/parametry lokaty terminowej na ustaloną kwotę,
3. W następnym kroku zainteresowany podmiot ma dokonać przelewu środków na wskazany numer rachunku technicznego,
4. Po dokonaniu przelewu klient za pośrednictwem kuriera ma odesłać umowę rachunku i lokaty terminowej,
5. Środki przekazane na rzekomo konto techniczne lokaty terminowej faktycznie trafiają na rachunek słupa/muła, skąd są dalej transferowane na konta przestępcze.

Wszystkie formalności realizowane są za pośrednictwem poczty elektronicznej, dokumenty lub warunki lokaty są wysyłane z adresu mailowego podszywającego się pod bank.

W takich okolicznościach rekomendujemy zachowanie najwyższej ostrożności!!!
Zastosuj się do kilku ważnych zasad:

- nie podawaj żadnych informacji poufnych związanych z funkcjonowaniem jednostki samorządowej oraz danych dostępowych, w tym loginu i hasła do bankowości internetowej – te informacje są poufne, powinny być tylko w posiadaniu osób upoważnionych i nikt nie ma prawa wymagać ich podania, faktyczny przedstawiciel banku nigdy o to nie zapyta,
- jeżeli rozmowa wzbudza jakiekolwiek wątpliwości lub niepokój, należy rozłączyć się, odczekać minimum 30 sekund, a następnie samodzielnie połączyć się z bankiem, którego rzekomy przedstawiciel dzwonił, koniecznie wybierając oficjalny numer na klawiaturze numerycznej, a nie oddzwaniając na wcześniejsze połączenie,
- należy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z faktycznym przedstawicielem banku,
- należy zwrócić uwagę na adres e-mail i upewnić się, że należy do banku, z którym masz relacje biznesowe (wyświetlany adres e-mail może być podobny do adresu e-mail Twojego banku).

W przypadku podejrzenia próby popełnienia przestępstwa lub gdy przestępstwo to zostało popełnione niezwłocznie poinformuj o tym fakcie swój bank oraz złóż stosowne zawiadomienie na Policję lub do Prokuratury.

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP funkcjonuje w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich i gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń o charakterze przestępczym, godzącym w bezpieczeństwo banków oraz ich klientów.