Gmina Mielec
ul. Głowackiego 5, 39-300 Mielec
Godziny pracy Urzędu: pon.: 7:30 - 17:00, Wt. - Czw.: 7:30 - 15:30, Pt.: 7:30 - 14:00
Telefon: 17 773 05 90 Fax: 17 773 05 91 Email: sekretariat@ug.mielec.pl

Ostrzeżenie CERT Polska o atakach socjotechnicznych na klientów banków

2023-02-15 14:22:01

Pełna treść ostrzeżenia dostępna w komunikacie "Ataki socjotechniczne" na stronie CERT.

- **Szczególnie narażeni użytkownicy: Klienci banków**
- **Wektor ataku: Połączenie telefoniczne**
- **Możliwe skutki: Uzyskanie danych uwierzytelniających do konta przez osoby trzecie**
- **Atakowane platformy: Różne**

Schemat działania

Cyberprzestępcy kontaktują się ze swoimi potencjalnymi ofiarami telefonicznie. Na początku rozmowy przedstawiają nieprawdziwą sytuację, która wydaje się pilna i wymaga szybkiego działania. Oto dwa najczęstsze przykłady:

- **dzwoniący przedstawia się jako pracownik konkretnego banku, Biura Informacji Kredytowej, KNF lub innej instytucji finansowej. Informuje, że w danym momencie ktoś próbuje złożyć wniosek kredytowy na dane ofiary, zmienić dane uwierzytelniające lub wykonać przelew. Zachęca do współpracy w celu powstrzymania tego działania.**
- **sprawcy podszywają się pod pracowników znanych giełd kryptowalut lub Forex (np. Blockchain, XTB) i informują o koncie rzekomo założonym kilka lat temu, na którym pozostawiona przez ofiarę niewielka kwota, poprzez automatyzację inwestowania, urosła do sumy kilku tysięcy złotych. Proponują wypłacenie tych środków, dodatkowo wzmacniając presję koniecznością poinformowania Urzędu Skarbowego w przypadku odmowy współpracy.**

Następnie podczas kolejnych połączeń i rozmów ofiara zachęcana jest do zainstalowania aplikacji Anydesk. Program ten pozwala na zdalny dostęp do pulpitu, a co za tym idzie na wykonywanie czynności za tego użytkownika. Dodatkowo poszkodowani proszeni są o zalogowanie się do swojego konta bankowego, w celu wykonania kolejnych niezbędnych czynności. Sprawcy, mając dostęp do pulpitu i konta wykonują przelewy na swoje rachunki. Dodatkowo są w stanie zaciągnąć szybką pożyczkę w banku na dane swojej ofiary i również te środki ukraść.

Skutki oszustwa

Podjęcie komunikacji oraz udostępnienie zdjęć skutkowałoby najprawdopodobniej kolejnymi szantażami oraz próbą wyłudzenia środków pieniężnych. Należy zauważyć, że jakiekolwiek próby podejmowania rozmowy czy negocjacji z przestępcami eskalują potencjalny konflikt i prowadzą jedynie do coraz to większych żądań.

Jak się zachować, kiedy zadzwoni do nas taka osoba:

Jeśli zauważysz, że rozmowa telefoniczna jest opisaną tutaj próbą wyłudzenia, po prostu się rozłącz. Jeśli mimo świadomości, że jest to kłamstwo, chcesz się upewnić czy Twoje konto bankowe jest bezpieczne, przejdź do witryny internetowej organizacji (np. Banku) i zadzwoń bezpośrednio na numer obsługi klienta. W ten sposób możesz się upewnić, że rozmawiasz z pracownikiem konkretnej organizacji.

Ważne informacje:

Należy zwrócić uwagę, że przestępcy potrafią sfałszować numer telefonu, który wyświetla się potencjalnej ofierze. Jest to tzw. spoofing numeru telefonu. Często sprawcy podszywają się pod oficjalne numery banków lub zwykłych osób fizycznych, mimo że połączenia tak naprawdę wykonywane są z zupełnie innych numerów. Dlatego też odradzamy oddzwaniania na te numery, ponieważ często kontaktujemy się w takim wypadku z osobami, które nie są niczego świadome, a połączenie nie wyszło z ich telefonu.

Co zrobić w przypadku, gdy wyłudzono dane logowania do bankowości internetowej?

W przypadku, gdy oszust uzyska dostęp do danych logowania konta bankowości internetowej, zalecamy podjąć następujące kroki:

- **jak najszybciej skontaktować się ze swoim bankiem,**
- **zmienić hasło do bankowości internetowej,**
- **jeżeli doszło do wyłudzenia środków finansowych, zgłosić ten fakt na najbliższym komisariacie Policji.**
- **podejrzane wiadomości SMS, zawierające adres URL, przekazać nam na numer 799-448-084, a wszelkie inne zagrożenia zgłosić za pomocą formularza na stronie Zgłoś incydent CERT.PL.**

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www