ZWIĄZEK BANKÓW POLSKICH

Rekomendacje sektora bankowego dot. przeciwdziałania transakcjom oszukańczym- założenia

Kongres Prawa Bankowego, 14 czerwca 2023

Wyzwania sektora bankowego związane z cyberprzestępczością

- Skala wykorzystywania różnorodnych instrumentów płatniczych – opartych o nowoczesne technologie – powoduje, że stały się one jednym z najistotniejszych elementów współczesnej bankowości.
- Rozwój technologiczny oraz migracja transakcyjnej aktywności klientów z tradycyjnych placówek bankowych do internetowych i mobilnych kanałów obsługi klientów przyczynił się do wzrostu liczby oszukańczych transakcji płatniczych.
- Z tego względu uwierzytelnienie, autoryzacja i odpowiedzialność za nieautoryzowane transakcje płatnicze nabierają coraz donioślejszego znaczenia dla dostawców, jak i użytkowników usług płatniczych.

Spoofing/Vishing – podszywanie się pod inna osobę/instytucję w celu wprowadzenia w błąd odbiorcy informacji

aleBank.pl

OCEŃ swój bank!

Ranking Banków Miesięcznika Finansowego BANK

Rejestracja
Zaloguj się!
Newsletter

Wiadomości | Miesięcznik BANK | Prenumerata | Konferencje / Szkolenia | Reklama | Archiwum | Kontakt | OK

Uwaga na fałszywe połączenia telefoniczne przestępców podszywających się pod banki!

Bezpieczne Finanse / Bezpieczny Klient

15.11.2021 14:16, Związek Banków Polskich / ZBP

W ostatnich miesiącach częstym sposobem dokonywania przestępstw na szkodę klientó banków jest wykorzystanie telefonicznego połączenia głosowego z osobą, która jest przekonywana, że rozmawia z pracownikiem banku lub inną osobą godną zaufania (np. policjantem).

Jest to rodzaj phishingu, nazywany vishingiem. Nazwa jest połączeniem słów „voice phishing",

POLICJA.PL

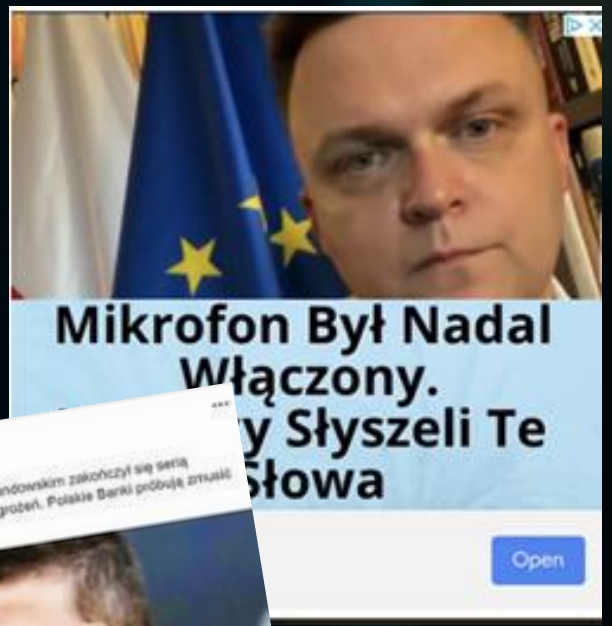
AKTUALNOŚCI

UWAŻAJMY NA FAŁSZYWE POŁĄCZENIA TELEFONICZNE PRZESTĘPCÓW PODSZYWAJĄCYCH SIĘ POD BANKI

Komenda Główna Policji, CERT Polska – Bankowe Centrum Cyberbezpieczeństwa ZBP i Polska Izba Informatyki i Telekomunikacji ostrzegają przed fałszywymi połączeniami telefonicznymi przestępców podszywających się pod banki.

Wykorzystanie tożsamości osoby znanej i rozpoznawanej

- Robert Lewandowski, Szymon Hołownia, Maciej Musiał …
- to tylko niektóre osoby, których tożsamość została wykorzystana w celu zmanipulowania pokrzywdzonego np. zachęcenie do inwestowania w kryptoaktywa lub na rynku FOREX;
- często osoby, których wizerunek został wykorzystany dementują fałszywe doniesienia medialne;



„Robert Lewandowski zdradził podczas rozmowy w programie Wojewódzkiego bardzo łatwy sposób na zarobienie dużych pieniędzy"

Źródło:
archiwum FinCERT.pl - BCC ZBP

https://www.wykop.pl/wpis/62947797/coo-jest-xdd-heheszki-rosja-holownia-polityka/
https://www.wykop.pl/wpis/62947797/coo-jest-xdd-heheszki-rosja-holownia-polityka/

Oszustwa z wykorzystaniem zdalnego pulpitu

Spoofing / Vishing - sprawca podszywa się pod bank i w ramach rzekomego wsparcia technicznego próbuje przejąć kontrolę nad urządzeniem ofiary

Fałszywe Inwestycje - doradca finansowy oferuje zdalną pomoc na rynku FOREX lub na giełdzie kryptowalut

Wnioski płynące z analiz zdarzeń prowadzonych przez FinCERT.pl – BCC ZBP

- Przy wszystkich tego typach przestępstwach kluczową rolę odgrywa socjotechnika i manipulacja jakiej używają przestępcy;
- Pokrzywdzony często udostępnia dane uwierzytelniające oszustom (np. spoofing);
- Zmanipulowany klient często sam autoryzuje transakcję płatniczą (inwestycje w krypto, Forex, przy okazji przestępstw z wykorzystaniem platform e-commerce);
- Zmanipulowany klient sam inicjuje płatność na własną szkodę (oszustwo „na wnuczka”, „na policjanta”, itd.);

Działania edukacyjne klientów – Policja, FinCERT.pl – BCC ZBP i banki ostrzegają

Straciła oszczędności na leczenie. Seniorka oszukana na bitcoina

Kilkadziesiąt tysięcy złotych straciła 75-latka ze Szczecina, która została namówiona do inwestycji w krypotowaluty przez oszustów. Część pieniędzy pochodziło z oszczędności na drogie leczenie córki, a reszta z pożyczki.

Chciała zarobić na kryptowalucie. Rawiczanka oszukana na blisko 200 tysięcy złotych. Oszuści wyczyścili jej konto i wzięli na nią pożyczkę

Jakub Latusek • 24 marca

Fałszywi brokerzy kuszą "atrakcyjnymi" inwestycjami w kryptowaluty

publikacja
2021-03-25 10:00

Nie ma haczyków! Wystarczy się zarejestrować, wpłacić początkową kwotę w wysokości 250 €, a my zajmiemy się resztą.

oszukańcze serwisy internetowe, które oferują kryptowaluty i
a rynku Forex" – ostrzega Komenda Główna Policji i Bankowe
erbezpieczeństwa ZBP (FinCERT.pl). Oszuści zachęcają do
szą wysokim i szybkim zyskiem.

https://rawicz.naszemiasto.pl/chciala-zarobic-na-kryptowalucie-rawiczanka-oszukana-na/ar/c1-8197651
https://www.money.pl/gospodarka/stracila-oszczednosci-na-leczenie-seniorka-oszukana-na-bitcoina-6627645248133920a.html
https://www.bankier.pl/wiadomosc/Falszywi-brokerzy-kusza-atrakcyjnymi-inwestycjami-w-kryptowaluty-8081096.html

Rekomendacje sektora jako próba zaadresowania problemu transakcji oszukańczych

- **Projekt rekomendacji** jest wypracowywany przez ekspertów z sektora bankowego przy udziale przedstawicieli UOKIK i UKNF;
- Celem rekomendacji ma być podniesienie bezpieczeństwa konsumentów korzystających z usług bankowości elektronicznej;
- Celem banków musi być zapewnienie bezpieczeństwa środków powierzonych im przez klientów;
- Oznacza to, że obowiązkiem banku jest troska nie tylko o konkurencyjność oferty i związanych z nią funkcjonalności, ale również skuteczne identyfikowanie, kwantyfikowanie i mitygowanie ryzyk wiążących się z korzystaniem z tych funkcjonalności przez klientów banków;

Struktura dokumentu

1 ZASADY OGÓLNE

2 CZYNNIKI RYZYKA

3 ŚRODKI ZARADCZE

Rekomendacje sektora jako próba zaadresowania problemu transakcji oszukańczych

PROJEKT!

1 Zasady ogólne

- Rekomendacje należy traktować jako zbiór dobrych praktyk;
- Zakres i sposób stosowania Rekomendacji powinien być uzależniony m. in. od wielkości banku, zakresu prowadzonej działalności oraz profilu ryzyka;
- Standardem wspólnej troski o bezpieczeństwo klientów powinna być regularna, wzajemna wymiana informacji o aktualnych zagrożeniach i metodach popełniania przestępstw oraz dobrych praktykach przeciwdziałania tym zagrożeniom pomiędzy bankami;
- Wdrożenie rozwiązań w zakresie bezpieczeństwa transakcji, w tym rozwiązań zaprezentowanych w Rekomendacjach nie ogranicza ani nie wyłącza obowiązku dostawcy usług płatniczych do zwrotu kwoty nieautoryzowanej transakcji płatniczej na zasadach wynikających z przepisów prawa;

Rekomendacje sektora jako próba zaadresowania problemu transakcji oszukańczych

PROJEKT!

2

Czynniki ryzyka [katalog otwarty]

Czynności Klientów mogące wiązać się z podwyższonym ryzykiem, w szczególności:

- Zlecenie zwiększenia limitów transakcyjnych;
- Odblokowanie możliwości dokonywania transakcji niespecyficznych dla danego Klienta;
- Zlecenie zmiany danych użytkownika, w tym zmiana metod komunikacji z bankiem;
- Złożenie dyspozycji przelewu środków pochodzących z kredytu tzw. na klik*, m.in. w przypadku gdy bezpośrednio lub w niewielkim odstępie czasu zainstalowano bankowość mobilną na nowym urządzeniu, lub po zmianie telefonu zaufanego, danych teleadresowych, itd.
- Inne okoliczności, sekwencje zdarzeń, które wg historycznych doświadczeń banku mogą wskazywać na ryzyko transakcji oszukańczej;

*kredyty na klik nie są transakcjami płatniczymi w rozumieniu ustawy o usługach płatniczych

Rekomendacje sektora jako próba zaadresowania problemu transakcji oszukańczych

PROJEKT!

2 Czynniki ryzyka

W przypadku czynności klientów, które mogą wywoływać podwyższone ryzyko oszustw, banki będą stosowały środki zaradcze i dodatkowe mechanizmy bezpieczeństwa.

Każdy bank opracowuje indywidualną strategię ograniczenia wystąpienia transakcji oszukańczych oraz wdraża skuteczne w ocenie banku mechanizmy bezpieczeństwa dążąc do mitygowania tych ryzyk, dobierając mechanizmy bezpieczeństwa adekwatnie do zidentyfikowanego poziomu ryzyka i rozwiązań dostępnych w banku;

Rekomendacje sektora jako próba zaadresowania problemu transakcji oszukańczych

PROJEKT!

3 Środki zaradcze

- **Cooling period** – wyłączenie lub opóźnienie możliwości korzystania z określonych produktów, funkcjonalności w bankowości elektronicznej;
- **Weryfikacja z wykorzystaniem połączenia telefonicznego** w celu przekazania informacji o inicjowaniu transakcji lub potwierdzenia woli jej dokonania przez klienta;
- Domyślne **limity transakcyjne** Klientów powinny być na stosunkowo niskim poziomie.
- **Metody uwierzytelniania i kaskadowe mechanizmy bezpieczeństwa** adekwatne do zidentyfikowanego poziomu ryzyka i rozwiązań dostępnych w banku;
- **Umożliwienie klientom ograniczenia funkcjonalności bankowości internetowej i mobilnej –** np. przelewów transgranicznych;
- **Umożliwienie klientom weryfikacji autentyczności kontaktu inicjowanego przez bank;**
- Bank powinien kierować do klientów **proste i zrozumiałe komunikaty;**
- Umożliwienie klientom **szybkiego zgłoszenia oszukańczej transakcji płatniczej i zastrzeżenia instrumentu płatniczego;**
- **Stosowanie systemów biometrii behawioralnej;**

Środki zaradcze można ze sobą łączyć, aby uzyskać ich wysoką skuteczność.

ZWIĄZEK BANKÓW POLSKICH

Związek Banków Polskich

Ul. Kruczkowskiego 8
00-380 Warszawa

Katarzyna Urbańska
Dyrektor Zespołu Prawno-Legislacyjnego

Katarzyna.urbanska@zbp.pl

www.zbp.pl