

# POLICJA MAZOWIECKA

<https://mazowiecka.policja.gov.pl/ra/dzialania-policji/zespol-funduszy-pomoc/archiwum-projekto/bezpieczni-w-bankowosci/58670,Seminarium-Bezpieczni-w-bankowosci-elektronicznej-doskonalenie-wiedzy-i-dzialan-.html>  
2023-03-31, 20:32

## SEMINARIUM „BEZPIECZNI W BANKOWOŚCI ELEKTRONICZNEJ – DOSKONALENIE WIEDZY I DZIAŁAŃ POLICJI [IV EDYCJA]”

Data publikacji 09.09.2021

**Oszustwa związane z systemami płatności mobilnych, identyfikowane trendy w przestępczości związanej z kryptowalutami czy wyłudzeniami leasingu to tylko niektóre spośród tematów poruszanych podczas trzydniowego seminarium organizowanego dla funkcjonariuszy Policji garnizonu mazowieckiego, na co dzień zajmujących się problematyką dotyczącą bezpieczeństwa w bankowości elektronicznej oraz przeciwdziałaniem i zwalczaniem przestępczości gospodarczej.**

Seminarium otworzył mł. insp. Piotr Janik, zastępca Komendanta Wojewódzkiego Policji z siedzibą w Radomiu, przedstawiając główny cel i założenia czwartej edycji projektu "Bezpieczni w bankowości elektronicznej (...)" oraz dziękując obecnym za przybycie i współuczestnictwo w tym wydarzeniu.

Rolę prelegentów pełnili przedstawiciele kilkunastu instytucji rynku finansowego, wśród których znalazły się przede wszystkim banki, m.in. PKO Leasing, Bank Pocztowy S.A., BNP Paribas Bank Polska S.A., PKO Bank Polski, Citi Handlowy, Bank Pekao S.A. czy Alior Bank S.A. Wystąpienia poprowadzili także reprezentanci innych ogniw rynku finansowego, takich jak BitBay, Euronet Polska Sp. z o.o., Polski Standard Płatności Sp. z o.o., PayPal, jak również biegły sądowy i funkcjonariusze Wydziału dw. z Cyberprzestępczością KWP z siedzibą w Radomiu. Organizację seminarium wsparli przedstawiciele Biura do Walki z Cyberprzestępczością Komendy Głównej Policji, pełniąc jednocześnie rolę prelegentów.



Uczestnicy mieli możliwość pracy warsztatowej w oparciu o konkretne przypadki wyłudzeń i kradzieży zanotowane przez banki. Jedno z takich studiów przypadku przedstawił prelegent z Departamentu Bezpieczeństwa Banku Pekao S.A., zapoznając słuchaczy z systemem działania przestępców w schemacie tzw. voice phishing z użyciem oprogramowania Anydesk. Cennym materiałem użytym w trakcie analizy były autentyczne nagrania rozmów telefonicznych, skany fałszywych wiadomości elektronicznych czy zrzuty ekranu stron internetowych do złudzenia imitujących oryginalne witryny bankowości internetowej.

Wśród wątków poruszanych podczas wykładów znalazły się także zróżnicowane formy wykorzystania giełdy kryptowalut do działań niezgodnych z prawem, takie jak chociażby anonimizacja środków skradzionych w wyniku różnego rodzaju oszustw i wyłudzeń czy lokowanie środków pochodzących z przestępstw w kryptowaluty. Omówione zostały m.in. ataki socjotechniczne na tzw. brokera inwestycyjnego, funkcjonowanie piramid finansowych i schematów Ponziego oraz

przestępstwa skarbowe w realiach giełdy kryptowalut. Część praktyczną poświęcono analizie sieci blockchain oraz zasad współpracy z organami ścigania, w tym procedur umożliwiających szybką reakcję administracji giełdy kryptowalut.



Jedną z prelekcji, które przykuły szczególną uwagę słuchaczy, poprowadził przedstawiciel Euronet Polska Sp. z o.o., omawiając strukturę ataków logicznych na bankomaty i drogi dostępu do systemu, ze szczególnym uwzględnieniem tzw. Man in the Middle. Analizie poddano m.in. specyfikę Black Box, w przypadku którego ataki dokonywane są najczęściej przez zorganizowane grupy przestępcze z dużą wiedzą na temat technologii bankomatowej. Pełen atak składa się z trzech etapów: fazy rozpoznania, przygotowania oraz samego ataku i wypłacenia gotówki. Dostęp do przewodów komunikacyjnych następuje najczęściej poprzez siłowe naruszenie górnej części obudowy bankomatu, a komendy wypłat wysyłane są z innego urządzenia elektronicznego, podłączonego bezpośrednio do dyspensera.



Ostatni dzień seminarium poświęcony był wewnętrznym procedurom Policji w zakresie zwalczania przestępstw o charakterze finansowym. Przedstawiciele Biura do Walki z Cyberprzestępczością Komendy Głównej Policji omówili szczegółowo m.in. kampanię opartą na fałszywych wiadomościach sms, w których oszuści wykorzystali fałszywy wizerunek PGE, informując o fikcyjnej należności za prąd elektryczny. Funkcjonariusze Wydziału dw. z Cyberprzestępczością KWP zs. w Radomiu przeprowadzili warsztaty z zakresu uzyskiwania danych od zagranicznych dostawców usług internetowych, omówili także trendy dotyczące fraudów internetowych w 2021 roku przez pryzmat czynności będących w zakresie uprawnień śledczego.

Seminarium zorganizowano w dniach 6-8 września 2021 roku w ramach czwartej edycji projektu pn. „Bezpieczni w bankowości elektronicznej - doskonalenie wiedzy i działań Policji”, realizowanego przez Komendę Wojewódzką Policji z siedzibą w Radomiu z Narodowym Bankiem Polskim w ramach programu edukacji ekonomicznej. W wydarzeniu uczestniczyło 70 osób.

Głównym celem projektu jest wzrost kompetencji policjantów i pracowników mazowieckiej Policji w zakresie identyfikacji i zwalczania zagrożeń i przestępstw związanych z bankowością elektroniczną (karty płatnicze, rachunki internetowe) oraz w zakresie nowych trendów w szeroko rozumianej przestępczości gospodarczej.

Realizatorem merytorycznym projektu jest Wydział do walki z Cyberprzestępczością KWP z siedzibą w Radomiu.



**NARODOWY  
BANK POLSKI**

Projekt realizowany  
z Narodowym Bankiem Polskim  
w ramach programu edukacji ekonomicznej

*Opracowanie: Eliza Sułkiewicz, Zespół Funduszy Pomocowych KWP zs. w Radomiu*