Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
z dnia 28 lutego 2022 r.
w sprawie rozprzestrzeniania się treści dezinformujących dotyczących sytuacji sektora bankowego w Polsce

Dziś w okresie rosnących niepokojów w związku z sytuacją w Ukrainie należy zachować szczególną rozwagę przy analizie i interpretacji „komunikatów prasowych" a szczególnie newsów z portali społecznościowych, które bez weryfikacji przekazywane są między użytkownikami wywołując niepokój.

Klika dni temu obserwowaliśmy kolejki na stacjach benzynowych czy wzmożona wypłatę środków z bankomatów i w placówkach bankowych. Reakcja społeczeństwa w tych okolicznościach była podobna do obserwowanych reakcji ludności z początków pandemii COVID-19. Związek Banków Polskich ściśle współpracuje z Narodowym Bankiem Polskim, który informuje, że jest przygotowany do zasilania banków w związku z obsługą zwiększonych wypłat gotówki, której nie zabraknie. Podejmowane działania przez banki mają za zadanie sukcesywne uzupełnianie niedoborów. Co jest bardzo istotne, pieniądze w bankach są bezpieczne i klienci banków mogą realizować swoje bieżące zobowiązania finansowe z użyciem zdalnych kanałów dostępu do swoich pieniędzy.

Czas paniki to doskonała okazja dla oszustów. Personalizowane sms- czy wiadomości e-mail mogą być próbą oszustwa. W treści fałszywej wiadomości oszuści mogą Państwa prosić o wsparcie finansowe dla zaatakowanego kraju lub informować o mobilizacji i powołaniu do wojska. Klikniecie w zamieszczone tam linki może wywołać działania, w wyniku których klient może nawet utracić swoje pieniądze.

Szanowni Państwo,

Działajmy jak dotychczas i z rezerwą podchodźmy do otrzymywanych informacji, nawet jeśli ich nadawcami są członkowie naszych rodzin, przyjaciele lub znajomi. To uchroni nas przed realizacją planu nakreślonego przez osoby manipulujące sytuacją.

Możemy się chronić:

1. Nie ulegajmy panice, na spokojnie i ze zrozumieniem czytajmy treść, weryfikujmy ja w kilku niezależnych źródłach;
2. Nie przekazujmy dalej treści wątpliwych, to może wywołać efekt kuli śniegowej, którą ciężko jest zatrzymać i ograniczyć skutki jej działania;
3. Nie starajmy się być ekspertami we wszystkich dziedzinach, mało kto z nas zna strategie wojskowe czy potrafi celnie dokonać analizy rynku;

4. Chrońmy naszą młodzież i dzieci przed informacjami niesprawdzonymi/ niepotwierdzonymi;
5. Czytajmy z uwagą wszystkie personalizowane do nas wiadomości sms i mailowe. Nie klikajmy w zamieszczone tam linki;
6. Nie dajmy się nabrać na telefony od rzekomych służb mundurowych, które będą „wymuszały" na nas przekazanie środków;
7. Mogą być próbą oszustwa, a klikniecie w linki może spowodować utratę wszystkich zgromadzonych na rachunkach pieniędzy. Czas paniki to doskonała okazja dla oszustów. Personalizowane sms'y, czy wiadomości e-mail mogą być próbą oszustwa.

W przypadku podejrzenia próby popełnienia przestępstwa lub gdy przestępstwo to zostało popełnione należy niezwłocznie poinformować o tym fakcie swój bank oraz złożyć stosowne zawiadomienie na Policję lub do Prokuratury. Szybkość złożenia takiego zawiadomienia może zwiększyć szansę uratowania utraconych środków, które fizycznie mogły jeszcze nie zostać wypłacone przez oszustów przede wszystkim jednak należy zachować spokój i wnikliwie analizować docierające do nas treści.

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.