Ostrzegamy przed oszustwami „na koronawirusa".

Prosimy o zachowanie odpowiedniej czujności przy korzystaniu z elektronicznych form dostępu do środków finansowych - oszuści wykorzystując sytuację zagrożenia epidemicznego podejmują działania w celu wyłudzenia loginu i hasła do bankowości za pomocą fałszywych stron płatności, a także próbują wyłudzać pieniądze poprzez portale społecznościowe i metodą na BLIK'a.

Przykłady ataków:

- **Fake newsy:**
  Oszuści podszywają się w fałszywych wiadomościach SMS, e-mail bądź telefonach pod firmy lub strony instytucji rządowych (np. Ministerstwo Zdrowia) przekazując rzekome informacje na temat epidemii lub informują np. o wsparciu żywnościowym, darmowych maseczkach, blokowaniu pieniędzy na rachunkach bankowych w związku ze specustawą, itp. Jednocześnie, wyłudzają od swoich ofiar dane osobowe, poufne dane do bankowości elektronicznej. Wysyłane są także wiadomości e-mail z treściami m.in. poradnikowymi na temat wykrywania i leczenia koronawirusa. Dołączane do tego typu wiadomości pliki i/lub linki zawierają złośliwe oprogramowanie. Do pozyskania poufnych danych wykorzystywane są również fałszywe strony (np. Ministerstwa Zdrowia), gdzie wymagane jest zalogowanie za pośrednictwem serwisu bankowości elektronicznej - próba „logowania" prowadzi do udostępnienia swoich poufnych danych oszustom, co może doprowadzić do kradzieży środków finansowych),
- **Mapy przedstawiające zasięg oddziaływania koronawirusa:**
  Na tego typu stronach oferowane mogą być np. aplikacje informujące użytkownika na bieżąco o rozprzestrzeniającym się wirusie. Pobierając taką aplikację użytkownik ściąga złośliwe oprogramowanie, które może pozyskiwać poufne dane np. login i hasło do bankowości elektronicznej,
- **Oszustwa z wykorzystaniem BLIKA**
  Przestępcy podszywając się pod portale informacyjne lub strony agend rządowych udostępniają np. film, którego obejrzenie wymaga zalogowania się danymi z portalu społecznościowego. Wpisując login i hasło, użytkownik portalu nieświadomie przekazuje dane atakującym, którzy za pośrednictwem jego konta są w stanie przesyłać dalej zainfekowaną stronę oraz mogą przesyłać znajomym użytkownika portalu prośbę pilnego przelewu pieniędzy za pośrednictwem kodu BLIK,
- **Oferowanie leków, testów na koronawirusa**
  Powstają dedykowane sklepy internetowe „specjalizujące się" np. w sprzedaży leków, a nawet szczepionek chroniących przed koronawirusem z fałszywymi stronami pośredników płatności, które mogą pozyskiwać poufne dane tj. login i hasło do bankowości elektronicznej,

Jak chronić się przed działalnością oszustów?

1. Informacje na temat koronawirusa warto czerpać z oficjalnych źródeł. Szczególnie w mediach społecznościowych należy weryfikować autentyczność interesujących nas wpisów związanych z zagadnieniem wirusa zanim podzielimy się nimi dalej w sieci.
2. Celem ochrony przed działalnością oszustów internetowych, należy pamiętać o zachowaniu maksymalnej ostrożności przy dokonywaniu transakcji w sklepach internetowych bądź na portalach aukcyjnych. Dobrą praktyką jest zawsze:
   - sprawdzać wiarygodność sklepu internetowego bądź portalu aukcyjnego,

- zwracać uwagę na adres strony internetowej serwisu bankowości elektronicznej, na której logujesz się lub wykonujesz płatności,
- dokładnie czytać treści SMS-ów/ powiadomień jakie otrzymujesz z Banku,
- weryfikować otrzymywane prośby o wysłanie pieniędzy BLIKIEM poprzez kontakt telefoniczny.

3. Należy bezwzględnie pamiętać, aby nie otwierać podejrzanych i nieoczekiwanych linków lub załączników zawartych w korespondencji e-mail i SMS/MMS oraz nigdy nie podawać poufnych danych do bankowości elektronicznej na stronach wskazanych w linkach będącymi załącznikami do tych wiadomości.

Zachęcamy do zapoznania się z ostrzeżeniami dotyczącymi oszustw internetowych publikowanych na stronach ZBP https://zbp.pl/dla-klientow/bezpieczne-bankowanie/Aktualnosci.