Korona-oszuści – posty do mediów społecznościowych

1) Możesz otrzymać fałszywe smsy lub maile z informacją o rzekomym przekazywaniu środków do rezerw NBP i poleceniem zalogowania się na swoje konto, aby do tego nie dopuścić. Link kieruje do strony podstawionej przez przestępców, która wygląda jak strona Twojego banku. Taka spreparowana strona zapisuje dane do logowania na Twoje konto. Nie klikaj w link i skasuj wiadomość!
Instytucje finansowe nigdy nie rozsyłają do swoich klientów wiadomości wraz z linkami do logowania.

2) Przestępcy podszywają się pod serwisy informacyjne lub strony rządowe i przesyłają informację lub film, których obejrzenie wymaga zalogowania się przez Facebooka. Nie rób tego – logując się tak naprawdę przekazujesz swoje dane i umożliwiasz oszustom wejście na swoje konto. Przez to Twoi znajomi mogą otrzymać, z Twojego profilu, prośbę o przesłanie pieniędzy za pomocą BLIKA oraz linki do wyłudzeń ich danych. Takie prośby od „znajomych" możesz także otrzymywać Ty. Nie daj się oszukać, nie podawaj kodu BLIK w wiadomościach! Najlepiej w takiej sytuacji skontaktować się telefonicznie z osobą proszącą o pomoc.

3) Fake news, czyli fałszywe, często sensacyjne informacje na temat epidemii, potrzebnego wsparcia żywnościowego, czy prośby o przekazanie brakujących środków ochrony itp. Wiadomości te zawierają

złośliwe oprogramowanie oraz linki lub załączniki, które mają na celu wyłudzenie danych osobowych, a najczęściej też danych do logowania na Twoje konto w bankowości internetowej. Nie klikaj w takie linki!

4) Dostałeś propozycję zainstalowania aplikacji związanych z epidemią, np. mapy przedstawiające na bieżąco jej zasięg? Nie rób tego! Pobierając taką aplikację ściągasz złośliwe oprogramowanie, które może pozyskiwać poufne dane, np. dane logowania do bankowości internetowej. Wszystkie wiadomości możesz na bieżąco śledzić w oficjalnych serwisach informacyjnych, nie musisz niczego instalować na telefonie czy komputerze.

5) Uważaj na leki i testy na koronawirusa oferowane w internecie. Te „specjalistyczne” sklepy prowadzą do fałszywych stron pośredników płatności np. PayPal, pozyskujących poufne dane, czyli poświadczenia do bankowości internetowej. Nie daj się korona-oszustom!