Bank Spółdzielczy w Świdnicy informuje i ostrzega:

1. Pracownicy naszego Banku **NIGDY** podczas rozmowy telefonicznej nie poproszą o podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji.

W celu wyłudzenia poufnych danych przez telefon - przestępcy podszywają się pod pracowników banków lub innych instytucji publicznych (np. policjantów, pracowników CBŚP).

Oszuści podający się za pracowników Banku lub innych instytucji w celu rzekomej weryfikacji podejrzanej transakcji czy logowania, proszą o instalację oprogramowania, dzięki któremu mogą przejąć kontrolę nad urządzeniem klienta (np. AnyDesk, TeamViewer). Przestępcy mogą też jako pracownicy instytucji obdarzonych publicznym zaufaniem (np. policjanci) przekazać informację o zagrożeniu środków na koncie i poprosić o przekazanie pieniędzy na wskazane przez nich konto w celu ich zabezpieczenia. **NIE WOLNO TEGO ROBIĆ!!!**

Aby zdobyć dane do logowania, narzędzia autoryzacyjne, lub inne dane, przestępcy mogą korzystać z techniki tzw. spoofingu nr telefonu tak, aby na telefonie klienta wyświetlił się nr infolinii Banku BPS SA lub nr placówki Banku.

Jeśli odbiorą Państwo podejrzany telefon lub wiadomość tekstową od osoby, która podaje się za pracownika Banku lub pracownika instytucji publicznej lub zaistnieją jakiekolwiek wątpliwości, czy zasadne jest podanie danych (np. kodu z narzędzia autoryzacyjnego), a także gdy podczas korzystania z elektronicznych kanałów dostępu, spotkacie się Państwo z sytuacją, która jest nietypowa lub wzbudzi niepokój, **powinniście Państwo rozłączyć się i skontaktować z Bankiem, dzwoniąc na znany nr telefonu wybrany ręcznie, najlepiej z wykorzystaniem innego urządzenia. Nie należy oddzwaniać na podejrzany numer.**

Nigdy nie należy przez telefon zdradzać szczegółów transakcji, podawać zbyt dużo informacji.

2. **Przy korzystaniu z portali sprzedażowych, aukcyjnych itp. należy zachować ostrożność**. Nie należy otwierać linków, które rzekomo mają umożliwić odbiór pieniędzy. Najlepiej rozliczać się bezpośrednio przez dany portal i unikać kontaktu poza portalem czy aplikacją.

Przestępcy wykorzystają każdą okazję, żeby uzyskać od klienta dane dotyczące karty płatniczej, czy dane logowania do bankowości internetowej.

3. **Należy czytać SMS-y od Banku i zwracać uwagę na to, co się autoryzuje.**
   Oszuści wysyłają sms z informacją o przelewie, do wiadomości jest dołączony link, który kieruje na fałszywą stronę, gdzie klient rzekomo ma odebrać środki. Po otwarciu linku pojawi się okienko z wyborem banku. Ta strona i strona banku jest fałszywa i pozwoli oszustowi pozyskać Państwa dane.

4. **Należy zachować ostrożność przy otwieraniu e'maili zwłaszcza z linkami lub załącznikami** (najczęściej dokumentami Microsoft Office: Word, Excel) lub archiwami chronionymi hasłem (*.zip, *.rar). Załączone dokumenty mogą informować o płatności za fakturę, a przestępcy mogą podszywać się pod istniejące instytucje. Otwarcie dokumentu (włączenie zawartości) powoduje zainfekowanie złośliwym oprogramowaniem.

5. **Przy inwestowaniu pieniędzy należy zachować czujność.**
   W celu przeprowadzenia oszustwa inwestycyjnego, przestępca kontaktuje się telefonicznie lub e'mailem (ewentualnie przez media społecznościowe) i oferuje super okazję (obietnicę szybkiego zysku). Oszuści chcą doprowadzić do zainstalowania programów, które rzekomo mają ułatwić inwestowanie, a tak naprawdę umożliwiają oszustowi zdalne korzystanie z Twojego komputera. **Cechy fałszywej inwestycji: doradca kontaktuje się z klientem wielokrotnie, podaje przykłady inwestycji, na których zarobiły znane osoby, zapewnia wsparcie poprzez programy do obsługi zdalnej np. AnyDesk, decyzja musi być podjęta szybko.**