Uważaj na oszustów!

Z uwagi na możliwość wystąpienia przestępstw dotyczących bankowości elektronicznej z udziałem np. aplikacji do połączeń zdalnych z komputerem lub logujących (zapisujących) wpisywane na komputerze hasła **prosimy o zwracanie szczególnej uwagi na zabezpieczenie dostępu do komputerów i telefonów pod względem zezwoleń aplikacji typu remote access (dostęp zdalny do urządzenia, pulpitu).**

Przypominamy najważniejsze kwestie bezpieczeństwa:

- Pracownicy banku **nigdy** nie oferują pomocy zdalnej poprzez aplikacje wykorzystujące usługę pulpitu zdalnego, nie pomagają bezpośrednio w realizacji przelewów,

- Pracownicy banku **nigdy** nie proszą o instalację oprogramowania na komputerze/tablecie/telefonie i nie wysyłają linków do takiego oprogramowania. Lista wymaganego oprogramowania do działania aplikacji bankowych wymieniona jest w wymaganiach systemowych aplikacji,

- Pracownicy **nigdy** nie proszą o loginy, hasła czy kod potwierdzający sms,

- Instrukcje i wymagania systemowe dla aplikacji mobilnej, dostępu do bankowości elektronicznej eBSR i eBSR-BIZNES są zamieszczone na stronach internetowych banku,

- W przypadku jakichkolwiek wątpliwości co do tożsamości konsultanta banku rozłącz się i skontaktuj się z bankiem , informując o zaistniałej sytuacji,

- Dbaj o odpowiednie skomplikowanie hasła do systemów bankowych zgodnie z zaleceniami aplikacji/systemu. Staraj się nie

używać tego samego hasła do innych aplikacji, systemów, stron internetowych.

W celu zobrazowania schematu działania przestępców przedstawiamy przykładowy scenariusz próby takiego wyłudzenia:

1. Otrzymujemy telefon od oszusta podającego się za pracownika banku. Taka osoba zazwyczaj nie mówi o jaki bank chodzi ale tak kieruje rozmową aby rozmówca sam zdradził, z usług którego banku korzysta.

2. Cyberprzestępca podszywający się pod pracownika banku informuje o konieczności autoryzacji transakcji lub o konieczności zablokowania transakcji (np. wykryto włamanie na konto). W przypadku nabrania podejrzliwości przez rozmówce zazwyczaj informuje, że rozłączy się, a za chwile zadzwoni z numeru infolinii banku, który można sprawdzić na stronie banku.

3. Oszust używając różnych metod zmiany prezentacji numeru dzwoni z numeru, który wyświetla się jako numer infolinii banku co zazwyczaj przełamuje opory.

4. Cyberprzestępca podczas rozmowy zdobywa kolejne informacje i w rezultacie może się zautoryzować w aplikacji bankowej. Prosi o pobranie oprogramowania, dzięki któremu może sprawdzić wpisywane przez nas loginy i hasła lub prosi o instalację oprogramowania dzięki któremu sam może sterować naszym komputerem.

5. W ten sposób możemy stracić środki oraz dostęp do konta.

Oczywiście taki scenariusz to tylko przykład, a kreatywność przestępców stoi na bardzo wysokim poziomie.

Takie sytuacje powinny wzbudzić Twoją czujność co do intencji rozmówcy:

- Bazowanie na sytuacjach stresowych (np. informuje o próbie kradzieży lub włamaniu na konto bankowe, podaje się za policjanta, pracownika służby bezpieczeństwa, pracownika instytucji finansowej). Taki wstęp do rozmowy zawsze obniża naszą czujność i ma skłonić do pochopnych działań.

- Nakłanianie do kliknięcia w linki, odnośniki wysłane mailem, smsem lub próba wskazania strony, na którą masz się zalogować.

- Namawianie do instalacji jakiegokolwiek oprogramowania do zdalnego dostępu lub/i podawania ID, loginu, hasła, hasła jednorazowego do już zainstalowanych aplikacji lub bankowości elektronicznej.

Życzymy bezpiecznego korzystania z naszych systemów/aplikacji!