Uwaga!

Ostrzegamy o nowym typie ataku cyberprzestępców skierowanym na Klientów Bankowości Elektronicznej z wykorzystaniem duplikatu karty SIM lub przekierowania połączeń na inny numer telefonu

Wspomniana metoda polega na przejęciu dostępu do numeru telefonu komórkowego poprzez wyłudzenie duplikatu karty SIM od operatora sieci komórkowej.

Jeśli więc zauważyłeś, że nie masz dostępu do sieci komórkowej – skontaktuj się jak najszybciej z operatorem sieci, z której korzystasz i ustal, czy w ostatnim czasie Twoja karta SIM była wymieniana na nową (bez Twojego zlecenia).

Jeśli operator potwierdzi taką sytuację – zadzwoń natychmiast pod nr 44/635-72-55 i poinformuj nas o tym. Pracownik banku zablokuje dostęp do Bankowości Internetowej, aby uniemożliwić dokonanie kradzieży Twoich środków.

Schemat ataku:

1. W pierwszej kolejności przestępcy pozyskują dane osobowe swojej ofiary oraz środki dostępu do Bankowości Elektronicznej (ID i hasło). Dane te pozyskują poprzez :
   a. obserwację samego Klienta, jego otoczenia, wpisów na Facebooku, Twitterze i innych aplikacjach społecznościowych,
   b. wcześniejsze zainfekowanie urządzenia złośliwym oprogramowaniem
   c. fałszywe ogłoszenia o pracę, załączniki do fałszywych maili, phishing, nieuprawniony dostęp do konta pocztowego, podszywanie się pod pracowników banku lub organy ścigania w rozmowie telefonicznej itp.
2. Podszywając się pod Klienta, kontaktują się z operatorem sieci telefonii komórkowej w celu włączenia **przekierowania połączeń przychodzących** z numeru ofiary na swój numer telefonu lub podszywając się pod ofiarę udają się do salonu operatora GSM i **wyrabiają duplikat karty SIM**.

Dzięki temu mają dostęp do numeru telefonu danej osoby, a co za tym idzie - kodów SMS, które służą do potwierdzania przelewów.

Jak się bronić przed takim atakiem:

I.-MONITORUJ:

Jeśli Twój telefon nie może uzyskać połączenie z siecią operatora **natychmiast skontaktuj się z nami i swoim operatorem telefonii**. Analogicznie należy postąpić w przypadku otrzymania wiadomości SMS od operatora o dokonaniu przekierowania, którego nie planowałeś. Należy również zachować szczególną ostrożność, w sytuacji, kiedy osoby próbujące się z nami skontaktować informują nas o tym, iż nie odbieramy od nich połączeń.

II. ZAPOBIEGAJ:

1. Chroń swoje dane osobowe, kradzież dokumentów jak najszybciej zgłoś na policji oraz w Banku.
2. **Ostrożnie** udostępniaj swój numer telefonu komórkowego (oraz inne dane dotyczące swojej osoby), zwłaszcza na portalach społecznościowych oraz serwisach, w których wymagane jest uzupełnienie profilu o numer telefonu.
3. **Nie otwieraj – od razu usuwaj** wiadomości SMS i e-maili pochodzące od nieznanych nadawców a w szczególności nie otwieraj linków (przekierowań), które się w nich znajdują oraz dołączonych załączników.. Na urządzeniu, z którego korzystasz **nie instaluj aplikacji z nieznanych źródeł**.
4. Zwracaj uwagę na komunikaty, które pojawiają się na Twoim urządzeniu, szczególnie gdy instalujesz nową aplikację. Zwracaj uwagę na to, jakich uprawnień wymaga instalowana aplikacja – jeśli żąda uprawnień do wysyłania i odbierania SMSów, zachodzi ryzyko przejęcia przez osoby nieuprawnione SMSów autoryzacyjnych wysyłanych przez Bank. **Zachowaj czujność** również podczas pobierania aplikacji z oficjalnych sklepów.
5. Dbaj, aby nikt poza Tobą nie znał loginów i haseł do Bankowości Internetowej, Mobilnej, Telefonicznej.
6. Nigdy nie loguj się do Bankowości korzystając z nieznanych/obcych urządzeń.
7. Dbaj o aktualizację systemu operacyjnego w Twoim komputerze/telefonie.
8. Korzystaj z programu antywirusowego.

Jeśli podejrzewasz, że Twój telefon został zainfekowany:

1. - usuń złośliwe oprogramowanie poprzez przywrócenie ustawień fabrycznych w telefonie oraz skontaktuj się w tym celu z operatorem sieci komórkowej (lub serwisem Twojego telefonu),
2. - koniecznie szybko zmień hasło do Bankowości Elektronicznej
3. Dostępu do **Bankowości Elektronicznej chroń poprzez używanie unikalnego hasła (nie zapisuj go w swoim telefonie, tablecie oraz komputerze)** – Ustaw trudne do odgadnięcia hasło dostępu do Bankowości Internetowej (inne, jak do poczty elektronicznej, portali społecznościowych itp.) i nigdy nikomu go nie zdradzaj .Pracownicy banku ani organy ścigania nigdy nie zapytają Cię o hasło dostępu