Policja ostrzega - uważaj na przestępców i nie daj się oszukać

04-04-2024

Przestępcy stosują różne metody oszustw - „na wnuczka”, „na policjanta”, „na kryptowaluty” czy „na fałszywy link”. Jak zareagować i co zrobić kiedy podejrzewamy, że ktoś próbuje nas oszukać? Pamiętajmy, że nasze bezpieczeństwo i bezpieczeństwo naszych pieniędzy w największej mierze należy do nas samych.

W ostatnim czasie oszuści najczęściej próbują poniższych metod:

- „na wnuczka” - oszuści zazwyczaj kontaktują się telefonicznie. Przerwij połączenie, nie przekazuj nikomu swoich pieniędzy ani kosztowności, zweryfikuj przekazane podczas rozmowy informacje i skontaktuj się z bliskimi lub Policją;
- telefonicznie - przerwij połączenie, nie przekazuj żadnych pieniędzy ani kosztowności, zweryfikuj przekazane podczas rozmowy informacje, skontaktuj się z bliskimi lub Policją;
- „na policjanta” - policja nie prosi o pieniądze ani o udział w działaniach operacyjnych oraz nie informuje o szczegółach podejmowanych czynności. Przerwij połączenie, nie przekazuj oszczędności, skontaktuj się z bliskimi lub Policją;

- „na kryptowaluty” - mądrze inwestuj pieniądze, nie ufaj obietnicom łatwego i szybkiego zysku, nie zezwalaj na dostęp do swojego urządzenia innym osobom, chroń swoje dane, loginy i hasła, korzystaj ze sprawdzonych instytucji finansowych;
- „na inwestycję” - mądrze inwestuj pieniądze, nie ufaj obietnicom łatwego i szybkiego zysku, nie zezwalaj na dostęp do swojego urządzenia innym osobom, chroń swoje dane, loginy i hasła, korzystaj ze sprawdzonych instytucji finansowych;
- „na fałszywe linki” - nie klikaj w nieznane linki, stosuj w bankowości elektronicznej dwuskładnikową weryfikację dostępu, loguj się do banku tylko przez oficjalną stronę lub aplikację, strzeż swoich danych, loginów i haseł;
- „na Blika” - nie przesyłaj pochopnie kodów Blik, zweryfikuj prośbę o pieniądze za pomocą innego kanału informacyjnego niż ją dostałeś, upewnij się, że przekazujesz pieniądze właściwej osobie, przed potwierdzeniem w aplikacji skontroluj kwotę.

Na czym polega oszustwo na „Portal ogłoszeniowy”

- wystawiasz coś na portalu ogłoszeniowym. Znajduje się kupiec. Twierdzi, że chce zapłacić za wystawiony do sprzedaży towar, a pieniądze możesz odebrać po wejściu w link. W ten sposób -„Oszust zastawia na Ciebie pułapkę”
- teraz oszust wysyła Ci linka. Klikasz i trafiasz na stronę łudząco podobną do strony portalu ogłoszeniowego. Na stronie jest formularz z prośbą o podanie danych Twojej karty i stanu Twojego konta. Wypełniasz formularz. -„Oszust ma już prawie wszystko żeby Cię okraść”
- przychodzi do Ciebie SMS z banku, z kodem do autoryzacji. Ty nie czytasz go uważnie i wpisujesz kod do formularza. W SMS-ie napisaliśmy, że autoryzujesz dodanie Twojej karty do Google Pay lub Apple Pay. -„Oszust Cię okrada. Płaci Twoją kartą za pomocą aplikacji płatniczej lub wypłaca nią gotówkę w bankomacie”
- koniec. Twoje konto jest puste.
- Jak uniknąć oszustwa

Czytaj SMS-y od Banków

- zwróć uwagę na to, co autoryzujesz;
- poznaj zasady bezpieczeństwa swojego banku i stosuj się do nich

Gdy korzystasz z portali aukcyjnych

- miej ograniczone zaufanie do potencjalnych kontrahentów;
- rozliczaj się bezpośrednio przez dany portal. Unikaj bezpośrednich transakcji. Uważaj na próby nawiązania kontaktu poza portalem, np. przez WhatsApp czy Messenger. Zobacz instrukcje płatności portali ogłoszeniowych;
- oszuści mogą podrobić stronę portalu aukcyjnego – tak samo jak i każdą inną stronę, również naszą. Dlatego zwracaj uwagę na adres widoczny w przeglądarce;
- zwróć uwagę na poprawność językową strony, na której przekazujesz dane karty. Fałszywe strony często zawierają błędy, są napisane niegramatycznie.

Na czym polega oszustwo na „Pracownika banku, lub platformy inwestycyjnej”

Oszuści podszywają się pod pracowników banków. Dzwonią do klientów z numerów bardzo podobnych do numeru infolinii, a nawet wyświetlających się jako numer naszego banku i informują, że bank udaremnił nieuprawnioną wypłatę pieniędzy z konta. Aby zapobiec takim sytuacjom w przyszłości proszą o zainstalowanie na smartfonie pewnej aplikacji. W rzeczywistości jest to narzędzie do przejęcia kontroli nad naszym telefonem i hasłami bankowości mobilnej. Niektórzy podejrzliwi klienci po rozmowie z oszustem kontaktują się z prawdziwą infolinią banku. Mogą też prosić o wypłatę pieniędzy z konta i wpłatę na inne wskazane lub zainwestowanie na przykład w kryptowaluty. Wtedy okazuje się, że żadna taka sytuacja nie miała miejsca.

Na co zwracać uwagę?

- pracownicy Banku nigdy nie proszą podczas rozmowy o login lub hasło do bankowości internetowej;
- pracownicy Banku nigdy nie proszą o zainstalowanie dodatkowego oprogramowania lub uzyskanie zdalnego dostępu do komputerów klientów;
- pracownicy Banku nigdy nie proszą o pełen numer karty i kod CVV;
- pracownicy nie proszą o zlikwidowanie lokat, wypłaty pieniędzy, dokonywanie przelewów wskazując inne rachunki do wpłaty;
- jeśli masz wątpliwości czy rozmawiasz z pracownikiem Banku - rozłącz się - sprawdź numer na stronie internetowej i oddzwoń.