Komenda Powiatowa Policji w Sokólce

ul. Białostocka 69b, 16-100 Sokółka

Tel.: 47 7123 215 Fax.: 47 7123 204

TPP.0151.111.2024

Sokółka, 12 września 2024 roku

Panie/Panowie Burmistrzowie
i Wójtowie Miast i Gmin
Powiatu Sokólskiego

Szanowni Państwo,

W związku ze wzrostem ilości zgłoszeń dotyczących oszustw na terenie Powiatu Sokólskiego i zintensyfikowanymi działaniami profilaktycznymi mającymi na celu ostrzeżenie mieszkańców naszego powiatu zwracam się z uprzejmą prośbą o zamieszczenie na stronie internetowej urzędu ostrzeżeń i przykładowych metod działania przestępców próbujących wyłudzić oszczędności od mieszkańców naszego powiatu.

Z poważaniem

KOMENDANT POWIATOWY POLICJI
W SOKÓLCE
mł. insp. Marcin Rymarski

wyk. 1 egz – MA
przesłano e-mailem

Algorytm postępowania przestępców:

OSZUSTWO „NA POLICJANTA/ PROKURATORA"

Oszuści dzwonią zazwyczaj na numer stacjonarny. Przestępcy podają się za policjanta, funkcjonariusza CBŚP lub CBA, prokuratora. Oszuści przekonują swego rozmówcę, że np. rozpracowuje zorganizowaną grupę przestępczą i prosi, aby mu w tym pomóc – poprzez przekazanie gotówki. Głos w słuchawce podkreśla, że dzięki temu będzie można zatrzymać prawdziwych przestępców. W rzeczywistości działanie nie ma nic wspólnego z postępowaniem funkcjonariuszy Policji, a tylko i wyłącznie przejęciem środków pieniężnych. Po przekazaniu pieniędzy lub wpłaceniu ich na wskazane przez oszusta konto - kontakt się urywa.

OSZUSTWO „NA WNUCZKA/WYPADEK"

Oszuści wykonują telefon podając się za członka rodziny. Tłumaczą, że był wypadek i że potrzebna jest kaucja, by uniknąć aresztu. Proszą o przekazanie dużej sumy pieniędzy lub posiadanej biżuterii. Oszuści w trakcie rozmowy umiejętnie manipulują rozmówcą tak, by uzyskać o nim jak najwięcej informacji i wzbudzić w nich strach.

„WYKORZYSTANIE SYSTEMU PŁATNOŚCI INTERNETOWEJ"

Oszuści udają osoby zainteresowanie zakupem przedmiotów wystawionych na serwisach internetowych. Kontaktują się ze sprzedającym za pośrednictwem popularnego komunikatora lub e-maila, a nie samej platformy sprzedażowej. Finalizując transakcję podsyłają link, który ma służyć do przyjęcia płatności przez sprzedającego. Link przenosi nas na stronę łudząco przypomnijaącą stronę do logowania naszego banku. Aby odberać płatność należy podać swoje dane do logowania do bankowości internetowej. Wpisując je dajemy oszustom dostęp do naszego rachunku bankowego.

OSZUSTWO „NA BLIK-A"

Oszuści podają się za znajomych wybranej ofiary. Kontaktują się poprzez portal społecznościowy, wcześniej uzyskując dostęp do konta jej przyjaciół, i proszą o „szybką pożyczkę", tłumacząc się chwilową niedyspozycją. Obiecują zwrócić tego samego dnia pożyczoną gotówkę. Pokrzywdzeni nieświadomi niczego, przesyłają BLIK-iem umówioną kwotę i tym samym tracą swoje pieniądze.

OSZUSTWO „NA KRYPTOWALUTY"

Przestępcy kontaktują się z wybraną ofiarą telefonicznie bądź przez portal społecznościowy i zachęcają do powiększenia swoich oszczędności. Oszust sprytnie i umiejętnie prowadzi rozmowę tak, by wzbudzić w nas zaufanie i przekonać do wpłaty najpierw mniejszej zaliczki,

a potem pokazuje zyski i wybrana ofiara pod wpływem emocji inwestuje kolejne oszczędności, tym razem nieco wyższe. W ten sposób pokrzywdzeni tracą po kilkanaście, a nawet kilkadziesiąt tysięcy złotych. Bardzo często w tych przypadkach sprawcom udaje się osiągnąć dostęp zdalny do pulpitu ofiary i dzięki temu do konta bankowego, namawiając ofiary do zainstalowania specjalnego programu bądź aplikacji (AnyDesk).

OSZUSTWO „NA PRACOWNIKA BANKU"

Oszuści dzwonią i przedstawiają się jako pracownik banku. Informują swoja ofiarę, że pieniądze na jej koncie są zagrożone, dlatego jak najszybciej musi zalogować się na swoje konto, zainstalować aplikację i postępować zgodnie ze wskazówkami. Ofiara będąc pewna, że rozmawia z prawdziwym pracownikiem bankowym, postępuje zazwyczaj zgodnie z poleceniami rozmówcy. Klient banku instaluje przesłaną mu aplikację, przekazuje dane do logowania oraz przychodzące kody autoryzacyjne. Oszuści wypłacają pieniądze znajdujące się na koncie bądź zaciągają kredyty.

OSZUSTWO „NA PRACOWNIKA BANKU/POLICJANTA/PROKURATORA"

Na telefon ofiary dzwoni osoba, która podaje się za pracownika banku. Rozmówca oświadcza, że pieniądze na koncie są zagrożone, gdyż widzi w systemie próbę wypłaty dużej sumy pieniędzy z konta ofiary lub próbę włamania na jej konto. Informuje także, że hakerzy są namierzani przez Policję, której funkcjonariusze będą się kontaktować z ofiarą telefonicznie. Po chwili dzwoni policjant lub nawet prokurator, który potwierdza słowa dzwoniącego wcześniej pracownika banku. Rzekomy policjant lub prokurator poleca przelać wszystkie pieniądze na wskazane „bezpieczne" konto, do którego tylko on ma dostęp, prosi też o dane do logowania lub inne dane osobowe, które służą następnie do zaciągnięcia kredytów.

PAMIĘTAJĄC O KILKU PODSTAWOWYCH ZASADACH, MOŻEMY UNIKNĄĆ KŁOPOTÓW I UTRATY OSZCZĘDNOŚCI NASZEGO ŻYCIA.

- Policja nigdy nie prosi o przekazanie pieniędzy i nigdy nie dzwoni z takim żądaniem!
- Policja nigdy nie informuje telefonicznie o prowadzonych działaniach! Jeżeli odebrałeś taki telefon, bądź pewien, że dzwoni oszust!
- Nigdy w takich sytuacjach nie przekazuj pieniędzy, nie podpisuj dokumentów, nie zakładaj kont w banku i nie przekazuj nikomu swoich danych, numerów PIN i haseł dostępu!
- Po takiej rozmowie natychmiast zadzwoń do kogoś bliskiego na znany Ci numer i opowiedz o tym zdarzeniu. Poinformuj policję, zadzwoń na numer alarmowy 112.
- Zawsze rozłączaj połączenie przed wykonaniem kolejnego. Na tym często bazują oszuści!
- Pod żadnym pozorem nie przekazujmy jakiejkolwiek osobie, co do tożsamości której nie jesteśmy stuprocentowo pewni, loginu i hasła do bankowości internetowej oraz danych karty płatniczej. Są to informacje poufne i powinny być tylko w posiadaniu ich użytkownika. Nikt nie ma prawa wymagać od nas ich podania. Prawdziwy przedstawiciel banku nigdy o to nie zapyta;
- Nawet jeśli zostaliśmy poinformowani o potencjalnym zagrożeniu np. ataku hakerów na nasze konto bankowe, należy spokojnie przemyśleć, czy środki zgromadzone na rachunku naprawdę mogą być w niebezpieczeństwie, czy może rozmowa prowadzona jest z oszustem. Musimy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym przedstawicielem tej instytucji.
- Jeśli o „szybką pożyczkę" zwracają się do nas znajomi poprzez portal społecznościowy- pisząc, że np. stoją przy kasie, zabrakło im środków na koncie, a muszą zapłacić za zakupy – proszą o przesłanie pieniędzy BLIKiem, weryfikujmy takie informacje. Lepiej zadzwonić do takiego znajomego i upewnić się czy na pewno to on do nas pisze.
- Nigdy nie przekazuj dostępu do swoich urządzeń osobom, których nie znasz.
- Nie ufaj oferowanej "pomocy", o którą nie prosiłeś! Żaden bank ani firma nie poproszą Cię przez telefon o pobranie oprogramowania! Jeśli „konsultant" proponuje Ci zainstalowanie oprogramowania typu AnyDesk, możesz być pewien, że to oszustwo.
- Jeśli osoba podająca się za pracownika banku żąda zweryfikowania Twoich danych i danych konta lub zainstalowania jakiegokolwiek oprogramowania rozłącz się i zadzwoń do biura obsługi klienta Twojego banku.
- Pracownicy banku nie wymagają od klientów podawania haseł i loginów do konta!