26.11.2020 Ostrzegamy o kolejnych oszustwach w internecie

- Najpierw pomyśl, potem… nie rób!

Chcesz sprzedać swój towar za pomocą popularnego serwisu internetowego np. OLX? Wystawiasz ogłoszenie o sprzedaży przedmiotu. Kupujący kontaktuje się z Tobą za pomocą komunikatora np. WhatsApp i wykazuje zainteresowanie kupnem przedmiotu. Dostajesz od niego gotową instrukcję:

Uważaj! To oszustwo, link prowadzi do fałszywej strony, na której masz ujawnić dane swojej karty płatniczej.

- Nie klikaj!

Oszuści wykorzystają każdą okazję, żeby nakłonić Cię do przekazania danych Twojej karty płatniczej czy danych do logowania do bankowości internetowej. Mogą poprosić Cię o hasła, kody z wiadomości SMS od banku. Dla nich nie jest istotne, czy sprzedajesz przedmioty, czy je kupujesz. Przestępcom chodzi o przejęcie Twoich danych, by móc Cię okraść. Jeśli nie będziesz postępował według oczekiwań oszustów – 1:0 dla Ciebie!

- Zadbaj o to, na co masz wpływ

Wielkimi krokami zbliżają się Święta, a więc czas wzmożonych zakupów. Bądź uważny i ostrożny w tym, gdzie kupujesz. Jeśli Twoja intuicja podpowiada Ci, że przedstawiona okazja jest podejrzana – wycofaj się z niej. Przed transakcją sprawdź opinie o sklepie i o sprzedającym. Sprawdź także, gdzie ewentualnie będziesz mógł złożyć reklamację oraz w jaki sposób będziesz mógł skontaktować się ze sprzedającym w razie napotkanych problemów.

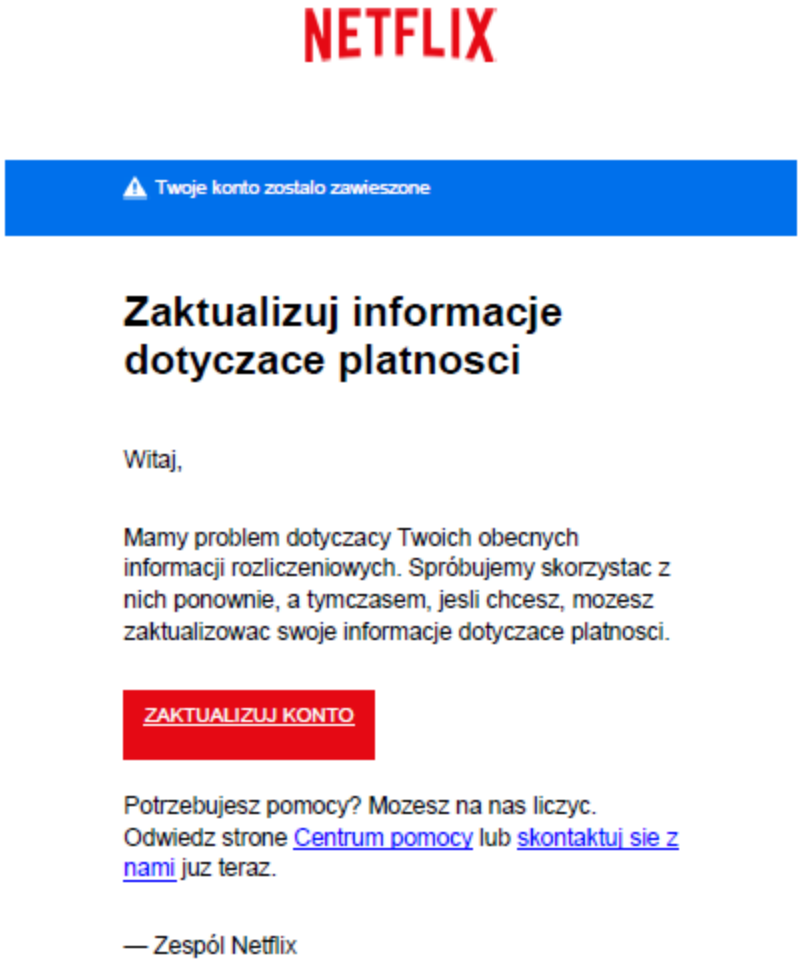
Koniecznie zapoznaj się z ostrzeżeniami Związku Banków Polskich: www.zbp.pl/dla-klientow/bezpieczne-bankowanie/bezpieczne-zakupy-przez-internet

20.10.2020 Ostrzegamy przed oszustwem "na Netflixa"

Ostrzegamy przed kolejną odsłoną manipulacji przestępców stosowanej wobec Klientów Banków.

Pod pretekstem zawieszenia konta u powszechnie znanego dystrybutora filmów Netflix, oszuści nakłaniają potencjalną ofiarę do przekazania danych umożliwiających dokonanie oszukańczych transakcji kartowych.

Oto jeden z przykładów tego typu fałszywej wiadomości:



Co prowadzi do utraty pieniędzy?

3 x „P”

- Postępowanie wg zaleceń oszustów (na to liczą)
- Pośpiech (w końcu czas to pieniądz)
- Przepisywanie zawartości kodów SMS z wiadomości z Banku (przestępcy liczą na to, że nie doczytasz treści wiadomości z Banku, nie zastanowisz się nad tym na co wyrażasz zgodę i, że podasz wszystko o co Cię poproszą na fałszywej stronie).

Pamiętaj, że:

- to Ty masz wpływ na to co zrobisz z fałszywą wiadomością (e-mail czy SMS);
- od Ciebie zależy gdzie i komu ujawnisz informacje o sobie czy o swoich produktach

- to Ty masz „klucze” do swoich pieniędzy w Banku!

W razie jakichkolwiek wątpliwości skontaktuj się z BS w Kórniku: 618170401

12.10.2020 Ostrzegamy przed kolejnymi stronami podszywającymi się pod BS W KÓRNIKU

Informujemy, że w dalszym ciągu pojawiają się strony, za pośrednictwem których przestępcy podszywają się pod stronę Bankowości Internetowej BS W KÓRNIKU.

Przypominamy:

- Wpisuj w pasku adresu przeglądarki pełny adres strony logowania do Bankowości Internetowej BS W KÓRNIKU – nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce. Adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe).
- Zawsze sprawdzaj adres strony www, na której się logujesz. Adres rozpoczyna się od https:// (w adresie strony widnieje wyłącznie domena pl, czyli https://BS w Kórniku.pl/). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla BS w Kórniku.pl przez firmę DigiCert. Możesz to sprawdzić, klikając w kłódkę. Podczas korzystania z Bankowości Internetowej sprawdzaj regularnie, czy na pasku adresu przeglądarki widnieje domena BS w Kórniku.pl (https://BS w Kórniku.pl/ – po drugim i trzecim “ukośniku” od lewej strony musi występować wyłącznie domena BS w Kórniku.pl).
- Nigdy nie loguj się do Bankowości Internetowej za pośrednictwem linku otrzymanego np. w wiadomości e-mail/ sms, czacie lub będącego wynikiem wyszukiwania w przeglądarce.
- Uważnie czytaj treść w kodach SMS/ Mobilnym Tokenie SGB.

W razie jakichkolwiek wątpliwości skontaktuj się z BS w Kórniku:618170401

22.09.2020 Uwaga na fałszywe strony podszywające się pod Bankowość Internetową (Phishing)

Nadal ostrzegamy przed kampanią phishingu, podczas której przestępcy podszywają się pod strony Bankowości Internetowej.

Celem ataku jest wyłudzenie środków dostępu do Bankowości Internetowej za pomocą fałszywych stron, które mogą przypominać m.in. strony Bankowości Internetowej BS W KÓRNIKU oraz innych banków.

Przestępcy mogą wykorzystać wyszukiwarki internetowe oraz wiadomości e-mail czy SMS (jako wynik wyszukiwania/w otrzymanej korespondencji mogą pojawić się fałszywe strony).

Pamiętaj:

- Wpisuj adres strony logowania do Bankowości Internetowej lub korzystaj z oficjalnej strony Banku – nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce.
- Zawsze sprawdzaj adres strony www, na której się logujesz oraz jej certyfikat (symbol zamkniętej kłódki. Adres rozpoczyna się od https:// w adresie strony widnieje wyłącznie domena BS w Kórniku.pl. Po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla BS w Kórniku.pl przez firmę DigiCert).
- Nigdy nie loguj się do Bankowości Elektronicznej za pośrednictwem linku otrzymanego w wiadomości e-mail lub sms.

W razie jakichkolwiek wątpliwości skontaktuj się z BS w Kórniku: 618170401

19.08.2020 Oszustwo na dopłatę do przesyłki kurierskiej

Otrzymałeś wiadomość e-mail? Spójrz, kto jest nadawcą? Pamiętaj, że adres, który widzisz, może nie być prawdziwy – pod wyświetloną nazwą może kryć się adres e-mail oszusta.

Masz kliknąć w link w treści wiadomości by dopłacić za usługę? Czekasz na paczkę i przez to ufasz, że komunikat jest wiarygodny? Zatem najedź kursorem na link i – bez klikania! – zobacz do jakiej strony prowadzi! Dokładnie przeczytaj adres strony, może się różnić od prawdziwej strony operatora płatności tylko jednym znakiem. Nie klikaj gdy nie rozpoznajesz adresu.

Jeśli jednak kliknąłeś i jesteś na stronie, na której masz podać wszystkie dane, rzekomo potrzebne do zrealizowania zamówienia – zatrzymaj się na chwilę i pomyśl, czy na pewno podanie wszystkich informacji o sobie jest konieczne? W realnym świecie rzadko tak robimy…

W wirtualnym świecie również zastanów się, gdy ktoś prosi Cię o dane Twojej karty, hasła dostępowe do bankowości internetowej czy zażąda zawartości wiadomości SMS z Banku!

Jeśli jesteś uważny i roztropny przestępcom będzie trudno Cię zmanipulować i ukraść Twoje pieniądze.

Pamiętaj! Zawsze czytaj wiadomości SMS z Banku, zanim przepiszesz kod zastanów się co akceptujesz.

Jeśli potrzebujesz zasięgnąć wiedzy i zdobyć więcej informacji zachęcamy do przeczytania poniższych komunikatów na stronie SGB-Banku SA. Możesz także zapoznać się z ostrzeżeniami o zagrożeniach na stronach Związku Banków Polskich

Pamiętaj, że to Ty masz „klucze" do swoich pieniędzy w Banku!

Przykład autentycznych wiadomości oszustów – ku przestrodze – kliknij TUTAJ

17.07.2020 Uwaga na fałszywe strony podszywające się pod Bankowość Internetową (Phishing)

Obecnie obserwujemy kampanię phishingu, podczas której przestępcy podszywają się pod strony Bankowości Internetowej.

Celem ataku jest wyłudzenie środków dostępu do Bankowości Internetowej za pomocą fałszywych stron, które mogą przypominać m.in. strony Bankowości Internetowej SGB oraz innych banków.

Przestępcy mogą wykorzystać wiadomości e-mail, SMS oraz wyszukiwarki internetowe (w otrzymanej korespondencji/jako wynik wyszukiwania mogą pojawić się fałszywe strony).

Pamiętaj:

- Wpisuj adres strony logowania do Bankowości Internetowej lub korzystaj z oficjalnej strony Banku – nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce.
- Zawsze sprawdzaj adres strony www, na której się logujesz oraz jej certyfikat (symbol zamkniętej kłódki. Adres rozpoczyna się od https:// w adresie strony widnieje wyłącznie domena BS w Kórniku.pl. Po

kliknięciu w kłódkę pojawi się certyfikat wystawiony dla BS w Kórniku.pl przez firmę DigiCert).
- Nigdy nie loguj się do Bankowości Elektronicznej za pośrednictwem linku otrzymanego w wiadomości e-mail lub wiadomości SMS.

W razie jakichkolwiek wątpliwości skontaktuj się z BS w Kórniku: 618170401

13.07.2020 r. Uwaga na oszukańcze serwisy internetowe oferujące inwestycje w kryptowaluty oraz na rynku Forex

W trosce o bezpieczeństwo środków oraz danych naszych klientów ostrzegamy przed próbami wyłudzeń związanych z inwestowaniem na rynkach kryptowalut i Forex.

Szczegółowe informacje w informacji Prokuratury Krajowej, Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP o zagrożeniu związanym z ofertami inwestycji na rynku Forex i Bitcoin z dnia 10 lipca 2020 r.

W razie jakichkolwiek wątpliwości skontaktuj się z BS w Kórniku: 618170401

8.06.2020 r. Uwaga na wiadomości e-mail z szantażem udostępnienia prywatnych danych

Szanowni Klienci,

obserwujemy obecnie kampanię e-mail związaną z rozsyłaniem przez przestępców fałszywych wiadomości z żądaniem okupu (zapłaty).

Atakujący mogą wykorzystywać w polu nadawcy (ang. FROM) imiona i nazwiska pracowników SGB-Banku oraz Banków Spółdzielczych naszego Zrzeszenia. Przestępcy żądają okupu w zamian za nie ujawnianie kompromitujących treści, które pochodzą z Państwa komputerów. Jest to blef, atakujący nie są w posiadaniu takich danych.

Przestępczy e-mail ma na celu wyłudzenie okupu. Prosimy nie odpowiadać na taką wiadomość oraz nie podejmować prób związanych z opłaceniem okupu. Podejrzaną wiadomość rekomendujemy usunąć ze swojej skrzynki odbiorczej.

Wszelkie zaobserwowane nieprawidłowości prosimy zgłaszać za pośrednictwem naszego Call Center:

25.05.2020 r. Uwaga! Przestępcy atakują przedsiębiorców korzystających z Programu Tarcza Finansowa PFR

Ostrzegamy przed telefonicznymi próbami podszywania się pod pracowników Banku, pracowników instytucji publicznych – Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Policji, Prokuratury oraz za przedstawicieli firm, które proponują pomoc w złożeniu wniosku i uzyskaniu subwencji finansowych w ramach Programu Tarczy Finansowej PFR.

Celem przestępców jest wyłudzenie Państwa danych, dotyczących m.in.: danych identyfikacyjnych, haseł, kodów PIN/SMS, danych osobowych (w tym nr PESEL) czy danych związanych z saldem konta lub ostatnimi operacjami wykonywanymi na rachunku. Próba wyłudzenia danych może być realizowana także za pomocą komunikacji SMS lub e-mail.

W takich przypadkach prosimy o szczególne zachowanie ostrożności i nie podawanie jakichkolwiek danych przez telefon czy e-mail. W przypadku otrzymania podejrzanej wiadomości SMS lub e-mail prosimy na taką korespondencję nie odpowiadać.

W razie jakiejkolwiek wątpliwości prosimy o przerwanie połączenia telefonicznego i natychmiastowy kontakt z Bankiem za pomocą oficjalnego numeru infolinii:618170401

Przypominamy!

- Pracownik Banku podczas rozmowy telefonicznej nigdy nie poprosi o podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji.
- Pracownik Banku nigdy nie prosi o zainstalowanie jakiejkolwiek aplikacji, do której link (lub załącznik) wysłany jest za pomocą SMS lub poczty e-mail.
- Dzwoniąc na infolinię Banku, mogą Państwo poprosić o zweryfikowanie tożsamości pracownika.

16.03.2020 r. Ostrzegamy przed oszustwami „na koronawirusa”

Przestępcy wykorzystują każdą okazję – w obecnej sytuacji do wyłudzenia pieniędzy oraz danych osobowych stosują socjotechniki związane z koronawirusem.

Przykładami takich ataków mogą być m.in.

- Fake newsy

(Oszuści podszywają się w fałszywych wiadomościach SMS, e-mail bądź telefonach pod firmy, lub strony agend rządowych np. Ministerstwo Zdrowia przekazując rzekome informacje na temat epidemii lub informują np. o wsparciu żywnościowym, darmowych maseczkach itp. Jednocześnie, wyłudzają od swoich ofiar dane osobowe, poufne dane do Bankowości Elektronicznej. Wysyłane są także wiadomości e-mail z treściami m.in. poradnikowymi na temat wykrywania i leczenia koronawirusa. Dołączane do tego typu wiadomości pliki i/lub linki zawierają złośliwe oprogramowanie. Do pozyskania poufnych danych wykorzystywane są również fałszywe strony (w oszustwie wykorzystującym Ministerstwo Zdrowia Profil Zaufany), gdzie wymagane jest zalogowanie za pośrednictwem Bankowości Elektronicznej – Próba „logowania" prowadzi do oddania swoich danych, a następnie środków, złodziejom),

- Mapy przedstawiające zasięg oddziaływania koronawirusa

(Na tego typu stronach oferowane mogą być np. aplikacje informujące na bieżąco o rozprzestrzeniającym się wirusie. Pobierając taką aplikację ściągamy tak naprawdę złośliwe oprogramowanie, które może pozyskiwać poufne dane np. poświadczenia do Bankowości Elektronicznej),

- Oszustwa z wykorzystaniem BLIKA

(Przestępcy podszywając się pod portale informacyjne lub strony agend rządowych udostępniają np. film, którego obejrzenie wymaga zalogowania się danymi z Facebooka. Wpisując login i hasło, nieświadomi przekazujemy dane atakującym, którzy za pośrednictwem naszego konta na Facebooku są w stanie przesyłać dalej zainfekowaną stronę. Mogą także przesyłać naszym znajomym prośbę pilnego przelewu pieniędzy za pośrednictwem kodu BLIK),

- Oferowanie leków, testów na koronawirusa

(Powstają dedykowane sklepy internetowe „specjalizujące się” np. w sprzedaży leków, a nawet szczepionek chroniących przed koronawirusem z fałszywymi stronami pośredników płatności np. PayPal, które mogą pozyskiwać poufne dane tj. poświadczenia do Bankowości Elektronicznej),

- Jak chronić się przed działalnością oszustów?

Informacje na temat koronawirusa warto czerpać z oficjalnych źródeł. Szczególnie w mediach społecznościowych weryfikujmy autentyczność interesujących nas wiadomości oraz postów związanych z zagadnieniem wirusa zanim podzielimy się nimi dalej w sieci.

Celem ochrony przed działalnością oszustów internetowych, którzy chcą wyłudzić nasze poufne dane bądź pieniądze, pamiętajmy o maksymalnej ostrożności przy dokonywaniu transakcji w sklepach internetowych bądź na portalach aukcyjnych. Zawsze sprawdzajmy wiarygodność sklepu. Pamiętajmy też, aby nie otwierać podejrzanych linków lub załączników i nigdy nie podawać – wprowadzać poufnych danych do Bankowości Elektronicznej na stronach wskazanych w linkach będącymi załącznikami do wiadomości SMS lub e-mail.

12.02.2020 r. Ostrzegamy przed atakami na Bankowość Elektroniczną wykorzystującymi subskrypcje dla numeru telefonu

Szanowny Kliencie,

Ostrzegamy przed próbą wyłudzenia poufnych danych do Bankowości Elektronicznej.

Atakujący próbują pozyskać poufne informacje wysyłając SMS o treści:

Twoja zamówiona subskrypcja została aktywowana dla numeru: [tu numer] Opłata zostanie naliczona automatycznie na numer telefonu dnia: 13.03.2020. Formularz zgłoszenia telefonu do naprawy, rezygnacja z abonamentu dostępne na: subskrypcjax.xx.xx

Po wejściu na stronę (link wskazany) w treści SMS Klient informowany jest o możliwości rezygnacji z usługi SmartCare. Kolejne kroki wymagają podania numeru telefonu, wybrania Banku, a następnie wprowadzenia poświadczeń do Bankowości Elektronicznej!

Zapamiętaj!

Login i hasło wpisuj wyłącznie na stronie swojego Banku. Adres strony do logowania rozpoczyna się od https:// (w adresie widnieje domena BS w Kórniku https://bskornik.ebp.cui.pl/ oraz symbol zamkniętej kłódki)

Bank nie wysyła drogą SMS oraz e-mailową linków do stron Banku oraz do serwisu transakcyjnego oraz wszelkich stron, gdzie rzekomo ma nastąpić weryfikacja czy aktualizacja danych.