Ogólne zasady bezpieczeństwa w sieci

Poznaj najważniejsze zasady bezpieczeństwa w internecie

Najważniejsze zasady bezpieczeństwa w bankowości elektronicznej

Przypominamy:

- Wpisuj w pasku adresu przeglądarki pełny adres strony logowania do Bankowości Internetowej – **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://ebanknet.bsnowytomysl.pl/). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla ebanknet.bsnowytomysl.pl przez firmę Unizeto Technologies S.A.. Możesz to sprawdzić, klikając w kłódkę. Podczas korzystania z Bankowości Internetowej sprawdzaj regularnie, czy na pasku adresu przeglądarki widnieje domena ebanknet.bsnowytomysl.pl (https://ebanknet.bsnowytomysl.pl/ – pomiędzy drugim i trzecim "ukośnikiem" od lewej strony musi występować wyłącznie domena ebanknet.bsnowytomysl.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 przy potwierdzaniu operacji realizowanych bankowości elektronicznej.**

W razie jakichkolwiek wątpliwości skontaktuj się z bankiem pod numerem telefonu:

- 61 442 17 50

26.07.2022 Uważaj na próby wyłudzenia poufnych danych przez telefon – przestępcy podszywają się pod pracowników banków lub innych zaufanych instytucji (np. policjantów)!

Ponownie ostrzegamy przed przestępcami, którzy podają się za pracowników banku lub innych zaufanych instytucji (np. policjantów). Oszuści podają się za pracowników SGB-Banku pod pretekstem weryfikacji podejrzanego logowania czy transakcji. Proszą o instalację oprogramowania, dzięki któremu mogą przejąć kontrolę nad pulpitem, np. Any Desk, TeamViewer.

Próbują podszywać się również pod pracowników zaufanych instytucji (np. policjantów). Informują o zagrożeniu finansów na koncie. Proszą o przekazanie pieniędzy na „konto techniczne", na którym będą bezpieczne. Nie rób tego!

Przestępcy mogą korzystać z techniki tzw. spoofingu numeru telefonu, w taki sposób, by na Twoim telefonie wyświetlił się numer infolinii banku lub zaufanego pracownika banku. W rzeczywistości chcą m.in. zdobyć dane do logowania, narzędzia autoryzacyjnego lub Twoje inne, równie cenne dane.

Pamiętaj, pracownicy naszego banku nigdy nie zadzwonią do Ciebie z numeru infolinii 800 888 888. Z tego numeru korzystamy tylko, aby odbierać połączenia.
Przypominamy też, że pracownicy banku podczas rozmowy telefonicznej nigdy nie poproszą Cię o:

- podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji
- instalację jakiegokolwiek oprogramowania na Twoim komputerze lub telefonie.

W przypadku, gdy:

- odbierzesz podejrzany telefon lub wiadomość tekstową od osoby podającej się za pracownika banku lub instytucji zaufanej
- masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych
- podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie

rozłącz się i skontaktuj się z bankiem.

Pamiętaj – nigdy nie podawaj przez telefon nadmiarowych informacji. Nie zdradzaj szczegółów swoich transakcji. Nie oddzwaniaj na połączenie, z którego wcześniej rozmawiałeś z podejrzanym rozmówcą!

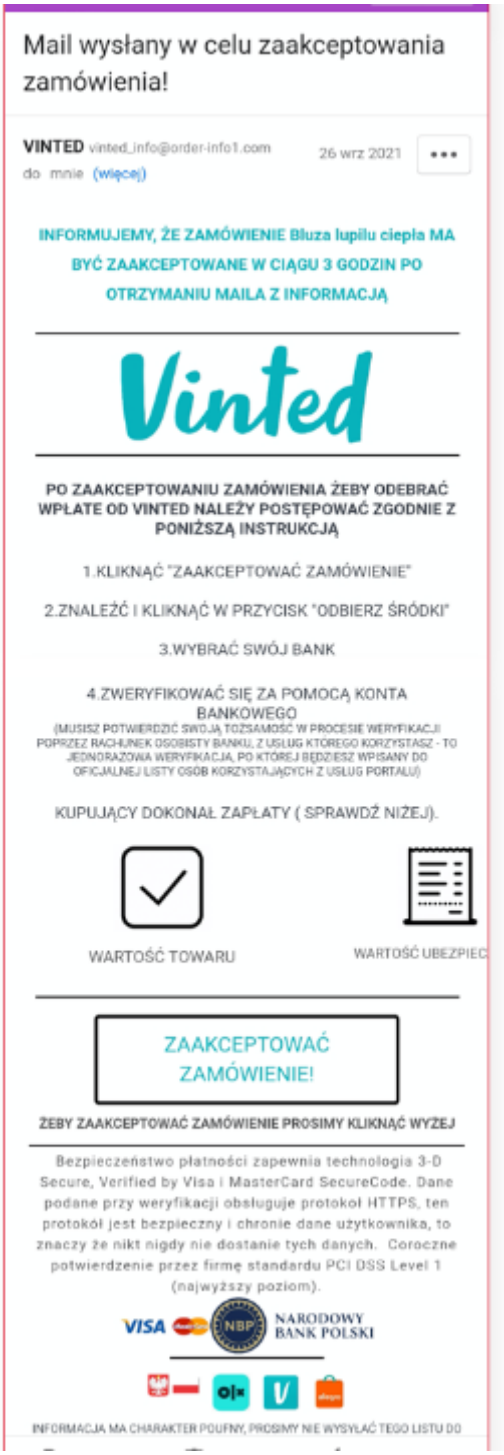
Jeżeli masz wątpliwości – skontaktuj się osobiście z placówką banku lub zadzwoń do nas na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia). Nasze numery kontaktowe znajdziesz na www.sgb.pl/kontakt lub na stronie do logowania https://sgb24.pl/frontend-web/app/auth.html#/content/login. Zawsze też ręcznie wpisuj pełen adres strony banku w pasku adresu przeglądarki (znajduje się u góry okna z otwartą przeglądarką internetową).
Kontakt z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

24.06.2022 Ponownie ostrzegamy przed oszustwami na portalach OLX/Vinted/Allegro

Sprzedajesz coś przez OLX, Vinted czy Allegro? Wystawiasz ogłoszenie o sprzedaży, a kupujący kontaktuje się z Tobą za pomocą komunikatora (np. WhatsApp) i chce kupić przedmiot? Później możesz dostać od niego link na WhatsAppie do rzekomego odbioru pieniędzy:

albo instrukcję wraz z linkiem na Twój adres e-mail:


Mail wysłany w celu zaakceptowania zamówienia!

VINTED vinted_info@order-info1.com
do mnie (więcej)
26 wrz 2021

INFORMUJEMY, ŻE ZAMÓWIENIE Bluza lupilu ciepła MA BYĆ ZAAKCEPTOWANE W CIĄGU 3 GODZIN PO OTRZYMANIU MAILA Z INFORMACJĄ

Vinted

PO ZAAKCEPTOWANIU ZAMÓWIENIA ŻEBY ODEBRAĆ WPŁATE OD VINTED NALEŻY POSTĘPOWAĆ ZGODNIE Z PONIŻSZĄ INSTRUKCJĄ

1.KLIKNĄĆ "ZAAKCEPTOWAĆ ZAMÓWIENIE"

2.ZNALEŹĆ I KLIKNĄĆ W PRZYCISK "ODBIERZ ŚRÓDKI"

3.WYBRAĆ SWÓJ BANK

4.ZWERYFIKOWAĆ SIĘ ZA POMOCĄ KONTA BANKOWEGO
(MUSISZ POTWIERDZIĆ SWOJĄ TOŻSAMOŚĆ W PROCESIE WERYFIKACJI POPRZEZ RACHUNEK OSOBISTY BANKU, Z USŁUG KTÓREGO KORZYSTASZ - TO JEDNORAZOWA WERYFIKACJA, PO KTÓREJ BĘDZIESZ WPISANY DO OFICJALNEJ LISTY OSÓB KORZYSTAJĄCYCH Z USŁUG PORTALU)

KUPUJĄCY DOKONAŁ ZAPŁATY (SPRAWDŹ NIŻEJ).

WARTOŚĆ TOWARU

WARTOŚĆ UBEZPIEC

ZAAKCEPTOWAĆ ZAMÓWIENIE!

ŻEBY ZAAKCEPTOWAĆ ZAMÓWIENIE PROSIMY KLIKNĄĆ WYŻEJ

Bezpieczeństwo płatności zapewnia technologia 3-D Secure, Verified by Visa i MasterCard SecureCode. Dane podane przy weryfikacji obsługuje protokół HTTPS, ten protokół jest bezpieczny i chronie dane użytkownika, to znaczy że nikt nigdy nie dostanie tych danych. Coroczne potwierdzenie przez firmę standardu PCI DSS Level 1 (najwyższy poziom).

VISA NBP NARODOWY BANK POLSKI

INFORMACJA MA CHARAKTER POUFNY, PROSIMY NIE WYSYŁAĆ TEGO LISTU DO

Uważaj! To oszustwo. Link prowadzi do fałszywej strony, na której masz ujawnić swoje dane do logowania. Ta strona łudząco przypomina stronę logowania do Twojego banku. Jeśli ujawnisz na niej swój login, hasło oraz kod SMS – te dane trafią bezpośrednio do oszusta.
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 działać według oczekiwań oszustów – 1:0 dla Ciebie!

Nie podawaj żadnych kodów z wiadomości SMS od banku!
Możesz dostać wiadomość z kodem SMS, który dotyczy aktywacji aplikacji mobilnej na nowym urządzeniu. To oszust próbuje na swoim urządzeniu aktywować aplikację mobilną. Jeśli mu się to uda – będzie mógł zmienić limity dla Twojej karty, limity przelewów oraz aktywować usługę BLIK i w ten sposób wyprowadzić pieniądze z Twojego konta.

Zadbaj o to, na co masz wpływ.
Jeśli Twoja intuicja podpowiada Ci, że przedstawiona okazja jest podejrzana – wycofaj się z niej.

Pamiętaj:

- czytaj SMS-y od Banku. Zwracaj uwagę na to, co autoryzujesz. Jeśli w treści SMS-a informujemy, że aktywujesz aplikację SGB mobile – a tego nie zlecasz, to właściwie pewne, że na Twoim koncie bankowym jest zalogowany oszust.
- nie otwieraj linków, które rzekomo mają pozwolić na odbiór pieniędzy za wystawiony przez Ciebie przedmiot.
- rozliczaj się bezpośrednio przez dany portal. Uważaj na próby nawiązania kontaktu poza portalem czy aplikacją, np. WhatsApp, e-mail.

Jeśli podejrzewasz, że Cię oszukano, przerwij transakcję i skontaktuj się z nami:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

4.03.2022 Uważaj na wiadomości e-mail zawierające załączniki lub linki (Trojan QakBot)

Ostrzegamy przed kampaniami spamowymi, w których rozsyłane są maile z linkami lub załącznikami (najczęściej dokumentami Microsoft Office: Word, Excel) lub archiwami chronionymi hasłem (*. zip, .* rar). Załączone dokumenty informują np. o fakturze. Co więcej, mogą to być wiadomości, w których oszuści podszywają się pod istniejące – zaufane organizacje.

Dokumenty zawierają makra, a ich otwarcie (włączenie zawartości) powoduje infekcję złośliwym oprogramowaniem QakBot.

Prosimy – zachowaj szczególną ostrożności podczas otwierania korespondencji elektronicznej, zwłaszcza załączników i linków.
Nie otwieraj i usuwaj wiadomości, które budzą Twoje podejrzenia.

W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

24.02.2022 Uważaj na fałszywe serwisy internetowe, które oferują kryptowaluty i inwestycje na rynku Forex

Ostrzegamy przed próbami oszustw przy inwestowaniu w kryptowaluty oraz na rynkach Forex.
Oszustwo inwestycyjne najczęściej ma miejsce, kiedy ktoś kontaktuje się z Tobą telefonicznie, e-mailem lub przez media społecznościowe i oferuje szansę zainwestowania w „jedyną w swoim rodzaju okazję". Oszuści często brzmią wiarygodnie i mają wiedzę, która może uśpić Twoją czujność, np. operują liczbami czy prognozami zysków. Fałszywy doradca dąży do tego, aby na Twoim komputerze zostały przez Ciebie zainstalowane odpowiednie programy. Rzekomo mają one ułatwić Ci inwestowanie. W rzeczywistości najczęściej są to programy, które umożliwiają oszustowi zdalne korzystanie z Twojego komputera.
Możesz również natknąć się na ogłoszenie w internecie lub w mediach społecznościowych z obietnicą szybkiego zysku. Przykład fałszywej oferty inwestycyjnej:

Jak rozpoznasz fałszywą inwestycję?

Oferta inwestycyjna może być oszustwem, jeśli rzekomy doradca:

- dzwoni do Ciebie wielokrotnie lub często kontaktuje się z Tobą za pomocą portali społecznościowych
- powołuje się na przykłady inwestycji, na których zyskały znane osoby
- nakłania do podjęcia szybkiej decyzji, aby nie stracić okazji
- oferuje wsparcie poprzez program do obsługi zdalnej, np. AnyDesk lub TeamViewer.

Zachowaj czujność:

- jeżeli nie rozumiesz oferty, poproś o jej ponowne i dokładne wyjaśnienie
- jeżeli nie masz pewności i nie ufasz firmie, niczego nie podpisuj i na nic się nie zgadzaj
- nie ulegaj presji. Uważaj na pozornie atrakcyjne oferty. Nie działaj pochopnie, pod wpływem chwili i emocji.

Pamiętaj! Przy inwestowaniu pieniędzy zawsze stosuj metodę ograniczonego zaufania!
W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

08.02.2022 Uważaj na próby wyłudzenia poufnych danych przez telefon – przestępcy podszywają się pod pracowników banków lub innych zaufanych instytucji (np. policjantów)!

Ponownie ostrzegamy przed przestępcami, którzy podają się za pracowników banku lub innych zaufanych instytucji (np. policjantów). Oszuści podają się za pracowników SGB-Banku pod pretekstem weryfikacji podejrzanego logowania czy transakcji. Proszą o instalację oprogramowania, dzięki któremu mogą przejąć kontrolę nad pulpitem, np. Any Desk, TeamViewer.

Próbują podszywać się również pod pracowników zaufanych instytucji (np. policjantów). Informują o zagrożeniu finansów na koncie. Proszą o przekazanie pieniędzy na „konto techniczne", na którym będą bezpieczne. Nie rób tego!

Przestępcy mogą korzystać z techniki tzw. spoofingu numeru telefonu, w taki sposób, by na Twoim telefonie wyświetlił się numer infolinii banku lub zaufanego pracownika banku. W rzeczywistości chcą m.in. zdobyć dane do logowania, narzędzia autoryzacyjnego lub Twoje inne, równie cenne dane.

Pamiętaj, pracownicy naszego banku nigdy nie zadzwonią do Ciebie z numeru infolinii 800 888 888. Z tego numeru korzystamy tylko, aby odbierać połączenia.
Przypominamy też, że pracownicy banku podczas rozmowy telefonicznej nigdy nie poproszą Cię o:

- podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji
- instalację jakiegokolwiek oprogramowania na Twoim komputerze lub telefonie.

W przypadku, gdy:

- odbierzesz podejrzany telefon lub wiadomość tekstową od osoby podającej się za pracownika banku lub instytucji zaufanej
- masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych

- podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie

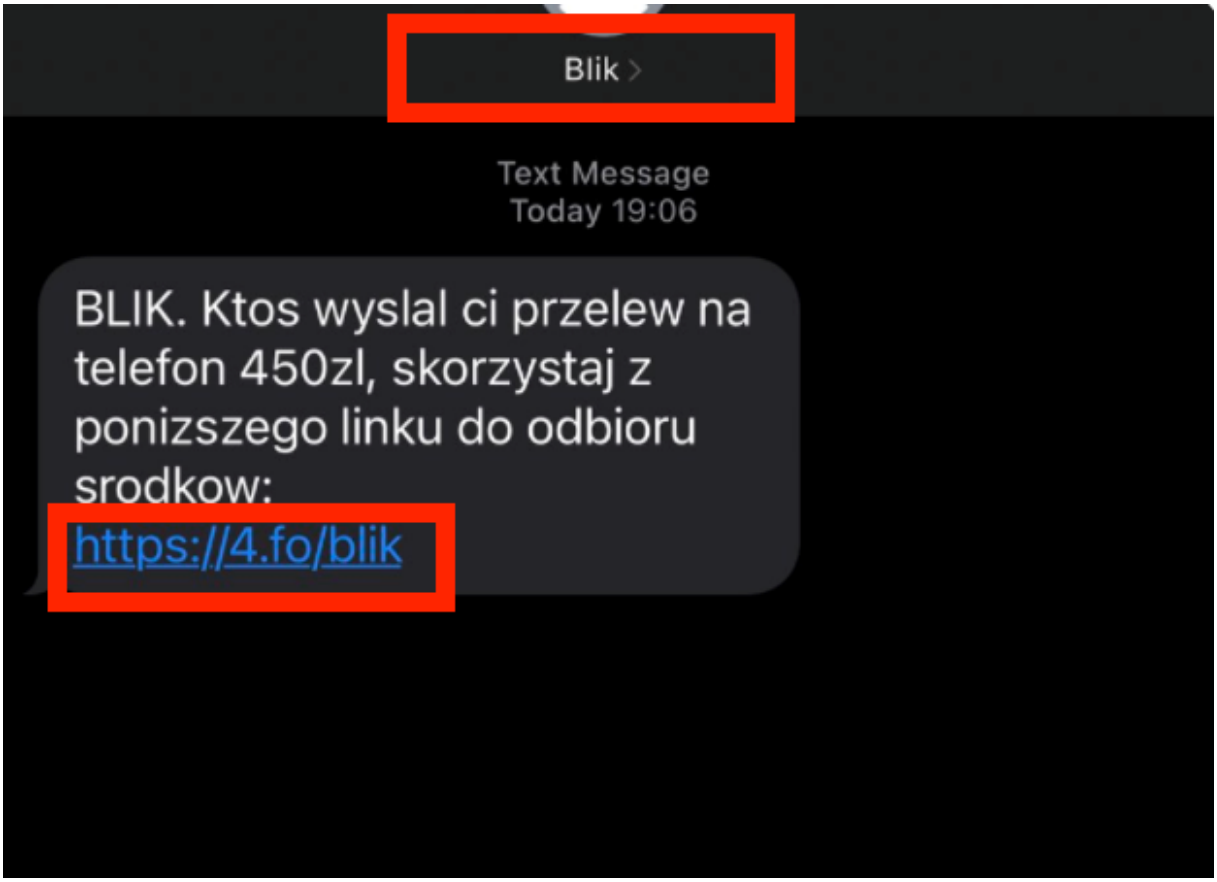
rozłącz się i skontaktuj się z bankiem.
Pamiętaj – nigdy nie podawaj przez telefon nadmiarowych informacji. Nie zdradzaj szczegółów swoich transakcji. Nie oddzwaniaj na połączenie, z którego wcześniej rozmawiałeś z podejrzanym rozmówcą!

Jeżeli masz wątpliwości – skontaktuj się osobiście z placówką banku lub zadzwoń do nas na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia). Nasze numery kontaktowe znajdziesz na www.sgb.pl/kontakt lub na stronie do logowania https://sgb24.pl/frontend-web/app/auth.html#/content/login. Zawsze też ręcznie wpisuj pełen adres strony banku w pasku adresu przeglądarki (znajduje się u góry okna z otwartą przeglądarką internetową).
Kontakt z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

31.01.2022 Uważaj na fałszywe SMS-y dotyczące usługi BLIK!

Dotarł do Ciebie SMS o poniższej lub podobnej treści?



Uważaj! To oszustwo!
Oszuści wysyłają SMS-y z informacją o przelewie 450 złotych przesłanych za pomocą BLIKA na Twój telefon. Do wiadomości dołączony jest link, który kieruje na fałszywą stronę, gdzie rzekomo masz odebrać pieniądze. Celem oszustów jest pozyskanie Twoich danych do logowania do bankowości.
Gdy otworzysz link pojawi się okienko z wyborem Twojego banku. Ta strona, jak i strona wybranego banku jest fałszywa. Jeśli podasz tam swoje dane – trafią one bezpośrednio do oszusta.
Jeśli podejrzewasz, że padłeś ofiarą oszustwa przerwij transakcję i skontaktuj się z nami:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

17-01-2022 - OSZUSTWO "Zwrot 300 zł za szczepienie" - ostrzeżenie

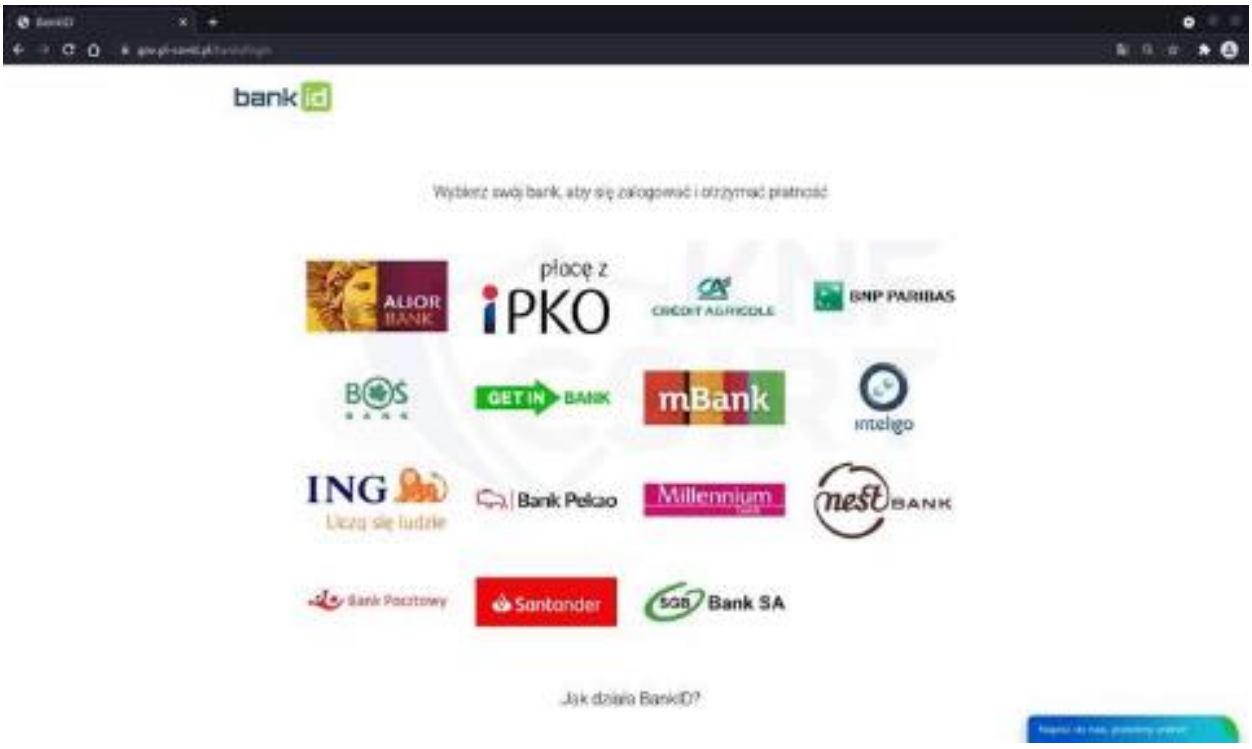
Szanowni Państwo,

Ostrzegamy przed fałszywą stroną, na której oszuści oferują zwrot 300 zł za szczepienie. Jeżeli wprowadzone tam zostanie hasło do banku, trafi ono bezpośrednio do oszustów, którzy wykorzystają je do kradzieży środków.

Wygląd strony jest łudząco podobny do rządowych witryn. Użyto na niej polskiego godła i napisu "gov.pl", używanego przez państwowe instytucje. Na stronie możemy przeczytać: "Odbierz 300 zł za szczepienie od Prezydenta Andrzeja Dudy". Pieniądze mają pochodzić z nieistniejącego programu "Wsparcie", uruchomionego rzekomo 12 stycznia 2022 roku. Oszukańcza strona informuje, że otrzymają je "wszyscy Polacy, którzy przeszli pełen cykl szczepienia".

Niebezpieczna strona:
gov.pl-covid[.]pl


gov.pl
BankID
Sposób weryfikacji obywateli za pośrednictwem polskich banków w celu świadczenia usług administracyjnych i innych przez Internet
Korzystamy z międzynarodowego doświadczenia
1 Obywatel wybiera "Zaloguj się za pomocą BankID".
2 W oknie, które się otworzy, wybierz swój bank.
3 Potwierdź zgodę na podanie loginu i hasła swojego banku internetowego.
4 Wprowadź hasło z SMS (w przypadku niektórych banków drugi etap autoryzacji może się różnić).
5 Potwierdzenie wypłaty. Obywatel otrzymuje wypłatę 300 zł.
Zaloguj się za pomocą BankID →


bankid
Wybierz swój bank, aby się zalogować i otrzymać płatność
ALIOR BANK
płacę z iPKO
CREDIT AGRICOLE
BNP PARIBAS
BOŚ BANK
GETIN BANK
mBank
inteligo
ING Liczą się ludzie
Bank Pekao
Millennium
nest BANK
Bank Pocztowy
Santander
SGB Bank SA
Jak działa BankID?

11.01.2022 Ostrzegamy o oszustwach na portalach OLX/Vinted/Allegro

Sprzedajesz coś przez OLX, Vinted czy Allegro? Wystawiasz ogłoszenie o sprzedaży, a kupujący kontaktuje się z Tobą za pomocą komunikatora (np. WhatsApp) i chce kupić przedmiot? Później możesz dostać od niego link na WhatsAppie do rzekomego odbioru pieniędzy:

albo instrukcję wraz z linkiem na Twój adres e-mail:

Uważaj! To oszustwo. Link prowadzi do fałszywej strony, na której masz ujawnić swoje dane do logowania. Ta strona łudząco przypomina stronę logowania do Twojego Banku. Jeśli ujawnisz na niej swój login, hasło oraz kod SMS – te dane trafią bezpośrednio do oszusta.
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!

Nie podawaj żadnych kodów z wiadomości SMS od banku!
Możesz dostać wiadomość z kodem SMS dotyczącym aktywacji aplikacji mobilnej na nowym urządzeniu. To oszust próbuje na swoim urządzeniu aktywować aplikację mobilną. Jeśli mu się to uda – będzie mógł zmienić limity dla Twojej karty, limity przelewów oraz aktywować usługę BLIK i w ten sposób wyprowadzić pieniądze z Twojego konta.

Zadbaj o to, na co masz wpływ
Jeśli Twoja intuicja podpowiada Ci, że przedstawiona okazja jest podejrzana – wycofaj się z niej.

Pamiętaj:

- czytaj SMS-y od Banku. Zwracaj uwagę na to, co autoryzujesz. Jeśli w treści SMS-a informujemy, że aktywujesz aplikację SGB mobile – a tego nie zlecasz, to właściwie pewne, że na Twoim koncie bankowym jest zalogowany oszust.
- nie otwieraj linków, które rzekomo mają pozwolić na odbiór pieniędzy za wystawiony przez Ciebie przedmiot.
- rozliczaj się bezpośrednio przez dany portal. Uważaj na próby nawiązania kontaktu poza portalem czy aplikacją, np. WhatsApp, e-mail.

Jeśli podejrzewasz, że padłeś ofiarą oszustwa przerwij transakcję i skontaktuj się z nami:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

13.12.2021 Ostrzegamy o kolejnych oszustwach w internecie

Najpierw pomyśl, potem… nie rób!

Chcesz sprzedać swój towar za pomocą popularnych serwisów internetowych np. OLX/Vinted? Wystawiasz ogłoszenie o sprzedaży. 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 oraz dane do logowania.

- 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!

- Nie podawaj żadnych kodów z wiadomości SMS od banku!

Możesz dostać wiadomość z kodem SMS dotyczącym aktywacji aplikacji mobilnej na nowym urządzeniu. To oszust próbuje na swoim urządzeniu aktywować aplikację mobilną. Jeśli mu się to uda – będzie mógł zmienić limity dla Twojej karty, limity przelewów oraz aktywować usługę BLIK i w ten sposób wyprowadzić środki finansowe z Twojego konta.

- Zadbaj o to, na co masz wpływ

Wielkimi krokami zbliżają się Święta, a więc czas wzmożonych zakupów. Bądź uważny i ostrożny, 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: https://zbp.pl/aktualnosci/wydarzenia/Bezpieczne-zakupy-przedswiateczne.

02.12.2021 Uważaj na próby wyłudzenia poufnych danych przez telefon – przestępcy podszywają się pod pracowników banków lub różnych zaufanych instytucji (np. policjantów)!

Ponownie ostrzegamy przed przestępcami, którzy podają się za pracowników banku lub innych zaufanych instytucji (np. policjantów). Oszuści podają się za pracowników SGB-Banku pod pretekstem weryfikacji podejrzanego logowania czy transakcji. Proszą o instalację oprogramowania, które pozwala na przejęcie kontroli nad pulpitem, np. Any Desk, TeamViewer.

Próbują podszywać się również pod pracowników zaufanych instytucji (np. policjantów). Informują o zagrożeniu finansów na koncie. Proszą o przekazanie pieniędzy na „konto techniczne", na którym będą bezpieczne. Nie rób tego!

Przestępcy mogą korzystać z techniki tzw. spoofingu numeru telefonu, w taki sposób, by na Twoim telefonie wyświetlił się numer infolinii banku lub zaufanego pracownika banku. W rzeczywistości ich celem jest m.in. zdobycie danych do logowania czy narzędzia autoryzacyjnego lub Twoich innych, równie cennych danych.

Przypominamy, że pracownik banku podczas rozmowy telefonicznej nigdy nie poprosi Cię o:

- podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji,
- instalację jakiegokolwiek oprogramowania na Twoim komputerze lub telefonie.

W przypadku, gdy:

- odbierzesz podejrzany telefon lub wiadomość tekstową od osoby podającej się za pracownika banku lub instytucji zaufanej,
- masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych,
- podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie

rozłącz się i skontaktuj się z bankiem.

Pamiętaj – nigdy nie podawaj przez telefon nadmiarowych informacji. Nie zdradzaj szczegółów swoich transakcji. Nie oddzwaniaj na połączenie, z którego wcześniej rozmawiałeś z podejrzanym rozmówcą!

Jeżeli masz wątpliwości – skontaktuj się osobiście z placówką banku lub zadzwoń do nas na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia). Nasze numery kontaktowe znajdziesz na www.sgb.pl/kontakt lub na stronie do logowania https://sgb24.pl/frontend-web/app/auth.html#/content/login. Zawsze też ręcznie wpisuj pełen adres strony banku w pasku adresu przeglądarki (znajduje się u góry okna z otwartą przeglądarką internetową).
Kontakt z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

01.10.2021 Uważaj na próby wyłudzenia poufnych danych przez telefon – przestępcy podszywają się pod pracowników banków!

Ponownie ostrzegamy przed przestępcami, którzy podają się za pracowników banku. Obecnie z reguły są to osoby o wschodnio brzmiącym akcencie. Podają się za pracowników SGB-Banku pod pretekstem weryfikacji podejrzanego logowania czy transakcji i proszą o instalację oprogramowania Any Desk. Przestępcy mogą korzystać z techniki tzw. spoofingu numeru telefonu, w taki sposób, by na Twoim telefonie wyświetlił się numer infolinii banku lub zaufanego pracownika banku. W rzeczywistości celem oszustów jest m.in. zdobycie danych do logowania czy narzędzia autoryzacyjnego lub Twoich innych, równie cennych danych.
Przypominamy, że pracownik banku podczas rozmowy telefonicznej nigdy nie poprosi Cię o:

- podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji

- instalację jakiegokolwiek oprogramowania na Twoim komputerze lub telefonie.

W przypadku, gdy:

- odbierzesz podejrzany telefon od osoby podającej się za pracownika banku
- masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych
- podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie

skontaktuj się z bankiem!
Pamiętaj – nigdy nie podawaj przez telefon nadmiarowych informacji. Nie zdradzaj szczegółów swoich transakcji.

Jeżeli masz wątpliwości – skontaktuj się osobiście z placówką banku lub zadzwoń do nas na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia).

Kontakt z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

24.09.2021 Uważaj na fałszywe SMS-y o skierowaniu na kwarantannę lub zgubionych dokumentach!

Ostrzegamy o masowo rozsyłanych SMS-ach, które informują o skierowaniu na kwarantannę albo zgubionych dokumentach.

Wiadomości w nazwie mają nadpis Kwarantanna, a w treści znajduje się link do strony nakłaniającej do pobrania fałszywej aplikacji Flash Player. Jeśli zainstalujesz aplikację z linku, zainfekujesz swój smartfon z systemem Android złośliwym oprogramowaniem. W efekcie oszuści uzyskają dostęp

do wrażliwych danych z Twojego telefonu, m.in. danych uwierzytelniających do bankowości mobilnej.
Pamiętaj, że samo kliknięcie w link z wiadomości SMS – bez pobrania i zainstalowania aplikacji, nie stanowi zagrożenia dla Twojego telefonu. Jeśli jednak aplikacja została przez Ciebie zainstalowana, to jak najszybciej wyłącz smartfon. Następnie z innego telefonu skontaktuj się z Infolinią SGB: 800 88 88 88.
Zachowaj czujność i uważaj na fałszywe SMS-y. Warto ostrzec również rodzinę i znajomych.

W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

13.09.2021 Uwaga na wiadomości e-mail zawierające załączniki lub linki (powiązane z podatnością CVE-2021-40444 w Microsoft Office)

Ostrzegamy o kampaniach phishingowych, które wykorzystują złośliwe oprogramowanie oparte na luce w oprogramowaniu Microsoft Office (CVE-2021-40444).

Atakujący mogą próbować nakłaniać użytkowników do uruchomienia złośliwego pliku, korzystając z metod opartych na socjotechnice. Najczęściej stosowaną metodą jest atak polegający na rozsyłaniu e-mailowych wiadomości ze złośliwym załącznikiem lub linkiem do pobrania złośliwej treści.
Mogą to być e-maile podszywające się pod istniejące – zaufane organizacje, a także wiadomości, których celem jest np. zainteresowanie odbiorcy.

Jeśli uruchomisz plik zawierający złośliwe oprogramowanie, zainfekujesz urządzenie i umożliwisz wykonanie dowolnego kodu na swoim komputerze.

W praktyce doprowadzi to do przejęcia Twojej stacji roboczej przez atakujących.

Prosimy – zachowaj szczególną ostrożności podczas otwierania korespondencji elektronicznej, zwłaszcza załączników i linków. Nie otwieraj i usuwaj wiadomości, które budzą Twoje podejrzenia.
W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

13.05.2021 Ostrzegamy przed kolejnymi stronami podszywającymi się pod SGB24

Informujemy, że w dalszym ciągu pojawiają się strony, za pośrednictwem których przestępcy podszywają się pod stronę Bankowości Internetowej SGB24.

Przypominamy:

- Wpisuj w pasku adresu przeglądarki pełny adres strony logowania do Bankowości Internetowej SGB24 – 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://sgb24.pl/). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla sgb24.pl przez firmę DigiCert. Możesz to sprawdzić, klikając w kłódkę. Podczas korzystania z Bankowości Internetowej sprawdzaj regularnie, czy na pasku adresu przeglądarki widnieje domena sgb24.pl (https://sgb24.pl/ – po drugim i trzecim “ukośniku” od lewej strony musi występować wyłącznie domena sgb24.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 Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

16.04.2021 Uwaga na SMS „Twoja paczka została zatrzymana przez służby celne”

Ostrzegamy przed kampanią, w której przestępcy rozsyłają fałszywe SMS-y informujące o zatrzymaniu przesyłki przez służby celne.

Linki znajdujące się w SMS-ach kierują do strony, która udaje firmę kurierską i „zachęca” do pobrania aplikacji śledzącej przesyłkę.

W rzeczywistości aplikacja to szkodliwe oprogramowanie, które umożliwia atakującym m.in. przejmowanie funkcji wysyłania i odbierania wiadomości SMS w celu kradzieży środków z konta bankowego.

W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

26.03.2021 Uwaga na próby wyłudzenia poufnych danych przez telefon – podszywanie się pod pracowników Banku nadal groźne!

Ponownie ostrzegamy przed przestępcami podającymi się za pracowników banku. Osoby te przez telefon wyłudzają poufne dane dotyczące haseł, kodów PIN/SMS. Jak to robią? Informują rozmówcę, że dane te potrzebne są do zwiększenia bezpieczeństwa lub przeprowadzany jest test działania bankowości. Przestępcy mogą korzystać z techniki tzw. spoofingu numeru telefonu, w taki sposób, by w Waszym telefonie wyświetlił się numer infolinii Banku lub zaufanego pracownika Banku! Dla uwiarygodnienia swojej legendy mogą podawać się za pracowników IT lub bezpieczeństwa.

W rzeczywistości celem oszustów jest m.in. zdobycie danych do logowania/narzędzia autoryzacyjnego lub innych cennych danych, które nie powinny być upublicznione osobom postronnym!

Przypominamy, że pracownik Banku podczas rozmowy telefonicznej nigdy nie poprosi Cię o podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji. Pracownik również w rozmowie telefonicznej nie poprosi o instalację jakiegokolwiek oprogramowania na Twoim komputerze lub telefonie.

W przypadku, gdy:

- odbierzesz podejrzany telefon od osoby podającej się za pracownika banku,
- masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych,
- podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie,

skontaktuj się z bankiem!

Pamiętaj – nie podawaj nigdy przez telefon nadmiarowych informacji, nie zdradzaj szczegółów swoich transakcji. Jeżeli masz wątpliwości – skontaktuj się osobiście z placówką Banku lub zadzwoń do nas na znany Tobie numer telefonu (koniecznie wybierz numer ręcznie, najlepiej korzystając z innego urządzenia).

25.03.2021 Uwaga na fałszywe serwisy internetowe, które oferują kryptowaluty i inwestycje na rynku Forex

Ostrzegamy przed próbami oszustw przy inwestowaniu w kryptowaluty oraz na rynkach Forex i zachęcamy do zapoznania się z komunikatem Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP:

https://zbp.pl/Aktualnosci/Wydarzenia/Uwazaj-na-oszukancze-serwisy-internetowe,-ktore-oferuja-kryptowaluty-i-inwestycje-na-rynku-Forex.

W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

05.02.2021 Uwaga na oszustów podszywających się pod pracowników Call Center SGB-Banku SA

Odebrałeś telefon od nieznajomego, który podaje się za pracownika „działu technicznego” Banku?

Wypytuje Cię o poufne dane Twojej karty płatniczej czy prosi o podanie loginu i hasła do bankowości internetowej?

Nakłania do instalacji programu do zdalnej obsługi Twojego urządzenia, z którego logujesz się do bankowości elektronicznej? A na brak zgody na taką instalację informuje, że poniesiesz tego skutki, że będziesz odpowiadał za utratę pieniędzy?

Podczas rozmowy przekonuje, że Twoje pieniądze nie są bezpieczne, bez interwencji „pracownika działu technicznego”?

Wypytuje przy tej okazji o Twoje dokumenty, zwyczaje zakupowe?

Możesz być pewny, że to oszustwo! Przestępcy potrzebują tych informacji, by dostać się do Twoich pieniędzy z rachunku, a nawet ukraść Twoją tożsamość, by móc potem zawierać umowy kredytowe w Twoim imieniu.

Pamiętaj, że oszuści, aby wzbudzić swoją wiarygodność, mogą nawet podszyć się pod prawdziwy numer telefonu z Banku.

Jak możesz zatroszczyć się o siebie, gdy otrzymałeś telefon od oszusta?

- Rozłącz się.
- Upewnij się, że istotnie połączenie zostało przerwane.
- Zadzwoń do Banku na nr telefonu dostępny na stronie internetowej Banku i przedstaw sprawę.
- Zgłoś sprawę organom ścigania, gdy ujawniłeś poufne informacje o sobie lub zainstalowałeś aplikację wskazaną przez oszusta.
- Przed ponownym korzystaniem z bankowości internetowej – przy użyciu nowych środków dostępu – upewnij się, że urządzenie, z którego korzystasz jest wolne od wszelkich podejrzanych instalacji oraz zabezpieczone aktualnym oprogramowaniem antywirusowym.

Klienci zwykle czują, że rozmowa z rzekomym pracownikiem nie odpowiadała standardom instytucji, którą jakoby reprezentuje oszust, była nietypowa a zadawane pytania powodowały dyskomfort.
To intuicja – zaufaj jej. Nie ujawniaj swoich poufnych danych, zadbaj o siebie i nie daj się oszukać!

07.12.2020 Uwaga na fałszywe sklepy internetowe

Zbliżający się okres Świąt to czas, w którym pojawiają się różnego rodzaju fałszywe sklepy internetowe. Celem takich działań, pod pretekstem sprzedaży produktów (często po bardzo atrakcyjnych cenach), jest np. wyłudzenie danych kart płatniczych.

Szczególną uwagę warto zwrócić na:

- niedostępność danej metody płatności,
- brak szyfrowanego połączenia (SSL),
- błąd certyfikatu SSL,
- podejrzaną nazwę domeny,

- niepoprawną polszczyznę.

Oszuści podszywają się również (phishing) pod istniejące, znane sklepy, przyciągając Klientów mocno zaniżonymi cenami oferowanych produktów. Dlatego zawsze należy zwracać uwagę na domenę widoczną w pasku adresu – przestępcy tworzą nazwy, które łudząco przypominają oryginał.

Warto zwrócić uwagę także na komunikaty wyświetlane na stronie sklepu. Chcąc sprawdzić wybrane dane o sklepie, np. kontakt, regulamin, formy płatności itd. prezentowany jest komunikat: „trwają prace serwisowe, spróbuj ponownie później".

Co więcej, w fałszywym sklepie zazwyczaj mamy tylko jedną opcję płatności – kartą płatniczą przez internet. Sklep internetowy za zakupiony towar powinien oferować kilka metod płatności np. za pośrednictwem systemów szybkich płatności m.in. PayU, Dotpay, Przelewy24 oraz opcję płatności przy odbiorze zamówienia.

Jeśli sklep, w którym zdecydowałeś się zrobić zakupy oferuje tylko jedną metodę płatności, lepiej zrezygnuj z zakupów.

Jeśli wybierzesz metodę płatności kartą – zweryfikuj na jakiej stronie wpisujesz jej dane. Zawsze warto również porównywać ceny w kilku sklepach lub korzystać np. z internetowych porównywarek cen.

W przypadku jakichkolwiek podejrzeń dot. autentyczności sklepu lub oferty należy zrezygnować z zakupów.

W razie jakichkolwiek wątpliwości skontaktuj się z Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

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.

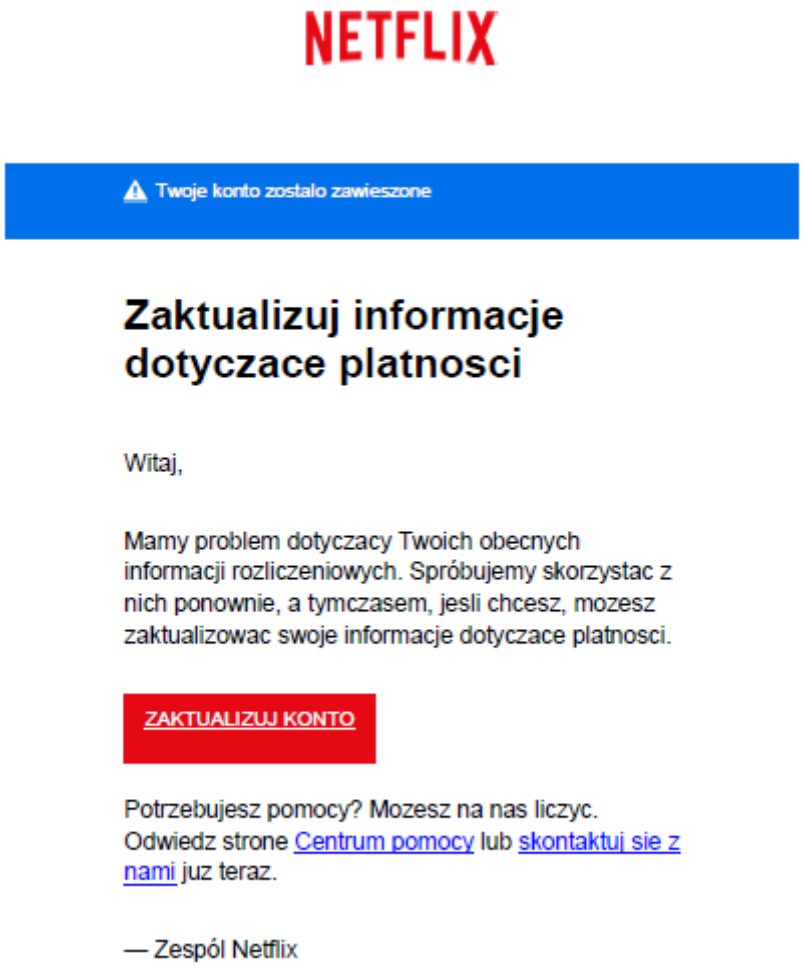
Koniecznie zapoznaj się z ostrzeżeniami Związku Banków Polskich: www.zbp.pl/dla-klientow/bezpieczne-bankowanie/bezpieczne-zakupy-przez-internet

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 Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

12.10.2020 Ostrzegamy przed kolejnymi stronami podszywającymi się pod SGB24

Informujemy, że w dalszym ciągu pojawiają się strony, za pośrednictwem których przestępcy podszywają się pod stronę Bankowości Internetowej SGB24.

Przypominamy:

- Wpisuj w pasku adresu przeglądarki pełny adres strony logowania do Bankowości Internetowej SGB24 – 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://sgb24.pl/). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla sgb24.pl przez firmę DigiCert. Możesz to sprawdzić, klikając w kłódkę. Podczas korzystania z Bankowości Internetowej sprawdzaj regularnie, czy na pasku adresu przeglądarki widnieje domena sgb24.pl (https://sgb24.pl/ – po drugim i trzecim “ukośniku” od lewej strony musi występować wyłącznie domena sgb24.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 Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

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 SGB24 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 sgb24.pl. Po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla sgb24.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 Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

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 sgb24.pl. Po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla sgb24.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 Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

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 Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- +48 61 647 28 46 (z telefonów komórkowych i z za granicy; opłata zgodna z taryfą operatora)

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:

- 800 88 88 88 (bezpłatne połączenie)
- +48 61 647 28 46 (z telefonów komórkowych i z za granicy; opłata zgodna z taryfą operatora)

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:

- 800 88 88 88 (bezpłatne połączenie)
- +48 61 647 28 46 (z telefonów komórkowych i z za granicy; opłata zgodna z taryfą operatora)

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 sgb24.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.

26.09.2019 r. Ostrzegamy przed atakami na Bankowość Elektroniczną

Szanowny Kliencie,

Wraz z wprowadzeniem 14 września 2019 r. nowego sposobu logowania do Bankowości Elektronicznej mogą pojawić się ataki wykonywane przez przestępców, mające na celu wyłudzenie poufnych danych.

Poprzez fałszywe strony Banku lub internetowych operatorów płatności np. PayU osoby nieuprawnione mogą uzyskać poufne informacje umożliwiające im dostęp do Twojego rachunku za pośrednictwem Kanałów Elektronicznych.

Przypominamy:

- Zawsze sprawdzaj, czy adres strony do logowania jest prawidłowym adresem Bankowości Elektronicznej Twojego banku, czy rozpoczyna się od https:// oraz czy połączenie z bankiem jest szyfrowane (obok paska adresowego musi być widoczny symbol zamkniętej kłódki).
- Jeżeli korzystasz z autoryzacji transakcji za pośrednictwem Kodu SMS przed jej potwierdzeniem dokładnie przeczytaj treść całej wiadomości SMS otrzymanej z Banku. Sprawdź czy zlecałeś osobiście taką transakcję lub operację i porównaj czy jest ona zgodna ze złożoną przez Ciebie dyspozycją. W szczególności w przypadku autoryzowania przelewów lub tworzenia szablonów zweryfikuj, czy podana w wiadomości SMS kwota transakcji oraz numer rachunku konta odbiorcy są zgodne z wprowadzanymi przez Ciebie danymi.
- Nigdy nie loguj się do Bankowości Elektronicznej za pośrednictwem otrzymanego w wiadomości e-mail lub sms linku.

Więcej informacji znajdą Państwo na stronie ZBP

02.09.2019 r. Uwaga na próby wyłudzenia poufnych danych przez telefon

Ostrzegamy, przed przestępcami podającymi się za pracowników banku. Osoby te przez telefon wyłudzają poufne dane dotyczące haseł, kodów PIN/SMS informując rozmówcę, że dane te potrzebne są do zwiększenia bezpieczeństwa lub przeprowadzany jest test działania bankowości.

W rzeczywistości celem oszustów jest zdobycie danych do logowania/narzędzia autoryzacyjnego.

Przypominamy!

Pracownik Banku podczas rozmowy telefonicznej nigdy nie poprosi Cię o podanie mu haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji.

W przypadku gdy odbierzesz podejrzany telefon od osoby podającej się za pracownika banku i masz jakiekolwiek wątpliwości czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych, jak również w każdym innym przypadku, w którym podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie, skontaktuj się z bankiem.

16.05.2019 r. Uwaga na fałszywe strony udające pośredników szybkich płatności!

Ostrzegamy przed fałszywymi stronami udającymi pośredników szybkich płatności.

https://zbp.pl/wydarzenia/archiwum/wydarzenia/2019/maj/uwaga-na-falszywe-strony-udajace-posrednikow-szybkich-platnosci

27.02.2019 r. Uwaga na fałszywe maile z informacją o wszczęciu kontroli z Urzędu Skarbowego!

Uwaga na fałszywe maile z informacją o wszczęciu kontroli z Urzędu Skarbowego!

Szanowni Klienci!

Ostrzegamy przed kampanią internetową, w której przestępcy wykorzystując komunikację e-mail podszywają się pod Urząd Skarbowy. W treści maila znajduje się spakowany załącznik (najczęściej archiwum z rozszerzeniem .tar) zawierający złośliwe oprogramowanie. Otwarcie tego dokumentu jest bardzo niebezpieczne i grozi zainfekowaniem komputera złośliwym oprogramowaniem!

Poniżej przykładowa treść wiadomości:

Nadawca (pole Od): URZĄD SKARBOWY

Temat: INFORMACJA O ZAMIARZE WSZCZĘCIA KONTROLI SKARBOWEJ
Nadawca: URZĄD SKARBOWY
Do:

Urząd Skarbowy odczytać zawiadomienie o zamiarze zainicjować kontroli w dniu 18.04.2019r. Wobec braku możliwości ustawienia kontaktu telefonicznego w dniach 4-7.04.2019r. i nie zastania podatnika w jego siedzibie w dniu 6.04.2019r. w celu ustalenia terminu wszczęcia kontroli. Urząd Skarbowy wyznacza termin zainicjować kontroli na 29.04.2019r. o godz. 9.00.

Jednoczesnie Urzqd Skarbowy informuje, ze zgodnie z art. 92a ustawy z dnia 13 pazdziernika 1998r. (Dz. U. z 2007 r., Nr 11, poz.74 z p6zn. zm.) w zwiqzku art. 80 ust. 1 ustawy z 2 lipca 2004 r. o swobodzie dziatalnosci gospodarczej (Dz. U. z 2007 r.. Nr 155, poz. 1095 z pozn. zm.) czynnosci kontrolnych dokonuje si$ w obecnosci kontrolowanego lub osoby przez niego upowaznionej. Oznacza to ze w wyzej wymienionym terminie jest Pani/Pan zobowiązana do obecnosci w siedzibie swojej Firmy i wspofpracy z inspektorem kontroli. Ponadto zgodnie z art. 80 ust. 3 ustawy o swobodzie dziatalnosci gospodarczej jest Pani/Pan zobowiązuje do pisemnego wskazania osoby upowaznionej do reprezentowania Pani/Pana w trakcie kontroli, w szczegolnosci w czasie Pani/Pana nieobecnosci.

Jest Pani/Pan zobowiązania do przygotowania wszystkich potrzebnych dokumentow zwiqzanych z prowadzone przez Pani/Pana Firm wymienionych w załączniku(dokumenty.rar).

Nieobecnosc Pani/Pana moze zostac uznana za stan wyczerpuje znamiona wykroczenia okreslonego w art. 98 ust. 1 pkt 3 ustawy z 13 pazdziernika 1998 r. (Dz. U. z 2007 r., Nr 11, poz. 74 z pozn. zm.).

INSPEKTOR KONTROLI

Urząd Skarbowy

mgr Marian Jakubowski

26.07.2018 r. Nowe zagrożenie - kradzież środków z rachunku „na kartę SIM”

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

Schemat ataku:

- W pierwszej kolejności przestępcy pozyskują dane osobowe swojej ofiary oraz środki dostępu do Bankowości Elektronicznej (ID i hasło). Dane te pozyskują poprzez wcześniejsze zainfekowanie urządzenia złośliwym oprogramowaniem (oraz także fałszywe ogłoszenia o pracę, załączniki do fałszywych maili, phishing, nieuprawniony dostęp do konta pocztowego, itp.)
- 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:

- 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.

- ZAPOBIEGAJ:

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.

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. 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.

Jeśli podejrzewasz, że Twój telefon został zainfekowany:

– usuń złośliwe oprogramowanie poprzez przywrócenie ustawień fabrycznych w telefonie oraz skontaktuj się w tym celu z operatorem sieci komórkowej (lub serwisem Twojego telefonu),

– koniecznie szybko zmień hasło do Bankowości Elektronicznej

Dostępu do Bankowości Elektronicznej chroń poprzez używanie unikalnego hasła (nie zapisuj go w swoim telefonie, tablecie oraz komputerze) – innego, jak do poczty elektronicznej, portali społecznościowych itp.

21.06.2018 r. Uwaga na nowe zagrożenia w sieci

W Internecie pojawiają się kolejne wersje złośliwego oprogramowania, które zainstalowane na komputerze Użytkownika logującego się do Bankowości Elektronicznej wykradają m.in. dane uwierzytelniające do logowania.

Do zainfekowania urządzeń, z których Użytkownicy łączą się z Internetem, dochodzi najczęściej w wyniku otwierania załączników do fałszywych e-maili.

Temat wiadomości najczęściej odnosi się do kwestii związanych z rozliczeniami i płatnościami i przybiera treść taką, jak np. „Faktury”, „Zaległe faktury”, „Potwierdzenie transakcji”, „Wezwanie do zapłaty”, „Nota księgowa”, co ma zwrócić uwagę odbiorcy i uśpić jego czujność. Maile wysyłane są z wielu adresów, z których każdy posiada polskojęzyczne imię i nazwisko oraz podpis wraz z nazwą firmy.

Przykładowa wiadomość:

-------- Oryginalna wiadomość --------
Od: Marek Lisowski <informatyk@garwolin.nazwa.pl>
Data: 21.06.2018 01:38 (GMT+01:00)
Do: @sgb.pl>
Temat: Faktury

Witam,

W załączniku przesyłam dane do faktur i rozliczenia.

Z poważaniem,
Marek Lisowski
Biuro Ekoprzedsiębiorstwo sp. z o.o.

Wiadomości zawierają załączniki z archiwami .*zip, .*rar (przykładowa nazwa pliku plik fa04285379785.rar)

Otwarcie – rozpakowanie załącznika infekuje komputer, na którym załącznik jest otwierany, groźnym wirusem, umożliwiającym kradzież poufnych danych Klienta.

Prosimy o zachowanie szczególnej ostrożności podczas otwierania korespondencji elektronicznej (zwłaszcza załączników i linków w e-mailach).

Rekomendujemy nie otwieranie i usuwanie wiadomości, których się nie spodziewamy oraz tych budzących podejrzenia w szczególności nie należy pobierać i otwierać załączników w formie plików zarchiwizowanych [spakowanych] (.*zip, .*rar)

14.12.2017 r. Uwaga podczas otwierania korespondencji elektronicznej!

Szanowny Kliencie

W ostatnim czasie zaobserwowano nową kampanię złośliwego oprogramowania.

Przestępcy wykorzystują przedświąteczny czas w którym Internauci dokonują zwiększonej ilości zakupów do dystrybucji wiadomości e-mail zawierających złośliwe załączniki. W tej kampanii przestępcy podszywają się pod znane firmy kurierskie. Otwarcie takiego załącznika uruchamia złośliwy kod, który szyfruje pliki na komputerze i w zamian za ich odszyfrowanie żąda zapłaty.

Prosimy o zachowanie szczególnej ostrożności podczas otwierania korespondencji elektronicznej (zwłaszcza załączników i linków w wiadomości).

5.12.2017 r. Uwaga na fałszywe sklepy internetowe

Szanowny Kliencie,

Ostatnie miesiące roku w związku z nadchodzącym okresem Świąt są szczególnym momentem, w którym pojawiają się różnego rodzaju fałszywe sklepy internetowe. Celem takich sklepów pod pretekstem sprzedaży produktów (często po atrakcyjnych cenach) jest wyłudzenie danych kart płatniczych.

Szczególnie uwagę powinny zwrócić podczas poruszania się na podejrzanej witrynie internetowej wszelkie informacje związane z niedostępnością danej metody płatności, brak szyfrowanego połączenia (SSL) lub błąd certyfikatu SSL, podejrzana nazwa domeny i niepoprawna polszczyzna. Przypominamy tym samym o zachowanie szczególnej ostrożności przy wykonywaniu płatności online.

W przypadku jakichkolwiek podejrzeń, prosimy o niezwłoczny kontakt z naszym zespołem Call Center (800 888 888 / (+48) 61 647 28 46) oraz o sprawdzenie swojej historii transakcji pod kątem podejrzanych wpisów.

30.11.2017 r. Uwaga na fałszywe faktury, które przypominają autentyczne dokumenty, jakie otrzymujecie Państwo od swoich kontrahentów

Szanowny Kliencie,

Nasz zespół bezpieczeństwa obecnie zaobserwował zwiększoną ilość ataków typu BEC (Business Email Compromise). Ataki te polegają m.in. na podszywaniu się pod zaufaną osobę lub firmę, np. Państwa kontrahenta i wysyłaniu w jego imieniu wezwania do zapłaty np. w postaci faktury. W tak przygotowanej fakturze (zazwyczaj w formie pliku elektronicznego) dane do przelewu zostały w odpowiedni sposób spreparowane, najczęściej poprzez podmianę numeru rachunku bankowego. Jedną z technik wykorzystywanych przez przestępców, w celu dostarczenia spreparowanych wiadomości e-mail może być wcześniejsze włamanie się na Państwa skrzynkę (lub skrzynki) poczty elektronicznej i obserwacja przebiegu korespondencji elektronicznej (np. z kontrahentami), w celu dokładnego przygotowania fałszywej faktury.. Faktura taka przypomina oryginalne dokumenty!

Prosimy o zwiększenie czujności podczas realizacji płatności na podstawie otrzymywanych faktur, zwłaszcza w formie elektronicznego załącznika poczty e-mail. Sugerujemy każdorazowe sprawdzenie numeru rachunku bankowego, na który ma zostać wykonana płatność, a w przypadku uzasadnionych wątpliwości (np. nagłej zmiany numeru rachunku), nawiązanie kontaktu z kontrahentem poprzez zaufany kanał komunikacji (np. dotychczas używany do komunikacji numer telefonu). Prosimy również o zwrócenie szczególnej uwagi na wszelkie informacje, które mogą przypominać autentyczną korespondencję z Państwa kontrahentami, dotyczące zmian kontaktowych numerów telefonów, adresów e-mail, czy numerów rachunków bankowych.

5.10.2017 r. Próby wyłudzania informacji o klientach przez telefon

Szanowny Kliencie,

w ostatnim czasie odnotowuje się zwiększoną liczbę prób wyłudzenia informacji o klientach poprzez rozmowy telefoniczne. Oszuści bardzo często podają się za pracownika Banku, kancelarii prawnej lub firmy współpracującej z Bankiem. Celem oszustów jest pozyskanie informacji o loginie, haśle a także o kodzie SMS, lub danych osobowych. Posiadając ten komplet danych oszuści zmieniają numer telefonu w profilu klienta i od tego momentu wszystkie SMS z kodami służącymi do autoryzacji transakcji wysyłane są na numer oszusta.

Więcej informacji znajdą Państwo pod adresem www: https://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci

20.09.2017 r. Uwaga na podejrzane sklepy internetowe

Szanowny Kliencie,

w Internecie pojawiły się sklepy, w których podczas dokonywania zakupów dochodzi do phishingu (wyłudzenia danych). Wspomniane sklepy dostępne są pod domenami innymi, niż polskie domeny .pl (np. eu, czy biz) Poniżej opisujemy przebieg takiego ataku:

- Klient po złożeniu zamówienia w sklepie internetowym otrzymuje wiadomość e-mail wysłaną przez sklep, w celu potwierdzenia realizacji zamówienia.
- W otrzymanej wiadomości e-mail Klient dostaje informację o opłacie oraz sposobie przesyłki (przesyłka pobraniowa kurierska).
- W informacji finalnej płatność ma nastąpić w momencie odbioru zamówionego towaru przez Klienta, jednak po niedługim czasie na skrzynkę pocztową trafia kolejny e-mail (sfałszowany) od kuriera, który sugeruje płatność online i przenosi Klienta do strony phishingowej.

- Strona wyłudzająca dane jest przygotowana w taki sposób, aby Klient podał swoje poświadczenia dostępu do bankowości elektronicznej oraz kod SMS potwierdzający transakcję „zapłaty”.
- W tym samym czasie atakujący loguje się na konto Klienta w bankowości elektronicznej (za pomocą skradzionych w ten sposób danych) i dodaje nowy szablon przelewu. W następnym kroku przestępcy, logując się na Konto Klienta, realizują faktyczny przelew.

W przypadku jakichkolwiek podejrzeń, prosimy o niezwłoczny kontakt z naszym zespołem Call Center (800 888 888 / (+48) 61 647 28 46) oraz o sprawdzenie swojej listy szablonów pod kątem prawidłowych numerów kont bankowych, jak i podejrzanych wpisów.

05.09.2017 r. Aktualizacja do komunikatu z dn. 04.08.2017: Atak phishingowy na bankowość elektroniczną

Szanowny Kliencie,

obserwujemy pojawienie się kolejnych stron phishingowych, które podszywają się pod witryny WWW systemu płatniczego Dotpay.

Poniżej przykładowa grafika systemu stworzonego przez przestępców, dzięki któremu wyłudzane mogą być dane dotyczące Twojej tożsamości oraz dane kart płatniczych.

Prosimy o zachowanie szczególnej ostrożności (oraz szczególnie zwrócenie uwagi na podejrzane działanie systemów płatności online, np. informacja o niedostępności danej metody płatniczej lub niedostępności Banku, podejrzana nazwa domeny w adresie przeglądarki) przy wykonywaniu płatności online.

04.08.2017 r. Atak phishingowy na bankowość elektroniczną

Szanowny Kliencie,

w ciągu ostatnich dni pojawiła się seria ataków mających na celu wyłudzenie środków dostępu do Bankowości Elektronicznej, za pomocą fałszywych stron mogących przypominać m.in. strony Bankowości Elektronicznej SGB oraz Dotpay. Poprzez fałszywe strony oszuści pozyskiwali nazwę użytkownika oraz hasło dostępowe do Bankowości Elektronicznej.

Następnie przestępcy po udanym zalogowaniu z wykorzystaniem skradzionych poświadczeń dostępu próbowali dodać lub zmodyfikować szablony.
Prosimy o wzmożoną czujność w zakresie potwierdzania (np. za pomocą kodu SMS) zlecenia dyspozycji przelewu oraz zmiany lub dodania kontrahenta na Państwa koncie. W przypadku jakichkolwiek podejrzeń, prosimy o niezwłoczny kontakt z naszym zespołem Call Center(800 888 888 / (+48) 61 647 28 46) oraz o sprawdzenie swojej listy szablonów pod kątem prawidłowych numerów kont bankowych, jak i podejrzanych wpisów.

Pamiętaj:

Sprawdź, czy adres strony do logowania jest adresem bankowości elektronicznej Twojego banku, czy rozpoczyna się od https:// oraz czy połączenie z bankiem jest szyfrowane (obok paska adresowego musi być widoczny symbol zamkniętej kłódki). Adres WWW Bankowości Elektronicznej dla Klientów indywidualnych SGB24 zaczyna się od: https://sgb24.pl/

Jeżeli korzystasz z autoryzacji transakcji za pośrednictwem Kodu SMS przed jej potwierdzeniem dokładnie przeczytaj treść całej wiadomości SMS otrzymanej z Banku. Sprawdź czy zlecałeś osobiście taką transakcję lub operację i porównaj czy jest ona zgodna ze złożoną przez Ciebie dyspozycją. W szczególności w przypadku autoryzowania przelewów lub tworzenia szablonów zweryfikuj, czy podana w wiadomości SMS kwota transakcji oraz numer rachunku konta odbiorcy są zgodne z wprowadzanymi przez Ciebie danymi.

05.05.2017 r. Ostrzeżenie o kampanii phishingowej (wiadomości e-mail od zaufanych nadawców)

Szanowny Kliencie,

w Internecie pojawiają się kolejne wersje złośliwego oprogramowania rozsyłanego poprzez wiadomości e-mail (kampania phishingowa). Fałszywe wiadomości w polu nadawca („OD”) zawierają najczęściej adres e-mail, należący do zaufanego nadawcy.

Złośliwe oprogramowanie uruchomione na komputerze użytkownika korzystającego z systemu Bankowości Elektronicznej, może być wykorzystywane do realizacji nieuprawnionych operacji z rachunków.

Do zainfekowania urządzeń dochodzi najczęściej w wyniku otwierania załączników do fałszywych e-maili, zawierających np. informacje o konieczności zapłaty za fakturę, telefon lub przesyłkę kurierską. Otwarcie załącznika uruchamia złośliwy kod, który infekuje komputer. Malware umożliwia kradzież poufnych danych Klienta m.in. wykorzystywanych do logowania do serwisu Bankowości Elektronicznej, a także wystawienie komunikatów o podanie kodów z karty kodów jednorazowych, kodu SMS lub Kodu z tokena.
W efekcie Klient może nieświadomie dokonać autoryzacji nieuprawnionych operacji z własnego rachunku.

Informacje

Szanowny Kliencie,

Bezpieczeństwo w Bankowości Elektronicznej zależy również od Ciebie. Zachowaj czujność, uważnie czytaj całą treść wiadomości z Kodem SMS.

Jeżeli korzystasz z autoryzacji transakcji za pośrednictwem Kodu SMS przed jej potwierdzeniem dokładnie przeczytaj treść całej wiadomości SMS otrzymanej z Banku.Sprawdź czy zlecałeś osobiście taką transakcję lub operację i porównaj czy jest ona zgodna ze złożoną przez Ciebie dyspozycją. W szczególności w przypadku autoryzowania przelewów lub tworzenia szablonów zweryfikuj, czy podana w wiadomości SMS kwota transakcji oraz numer rachunku konta odbiorcy są zgodne z wprowadzanymi przez Ciebie danymi.

Pamiętaj, że cyberprzestępcy stosują różne techniki i narzędzia ataków. W przypadku zainfekowania urządzenia, z którego korzystasz w Bankowości Elektronicznej złośliwym oprogramowaniem cyberprzestępcy mogą dokonać nieuprawnionych transakcji z Twojego rachunku np. zmieniając numer rachunku konta odbiorcy.

Jeżeli korzystasz z autoryzacji transakcji za pośrednictwem Kodu SMS w treści całej wiadomości otrzymanej z Banku zweryfikujesz czego transakcja dotyczy, na jaki numer rachunku konta odbiorcy ma być wykonana i na jaką kwotę.

Więcej informacji

Więcej informacji o aktualnych zagrożeniach znajdziecie Państwo na stronach WWW:
Związku Banków Polskich
Związku Banków Polskich – Bezpieczny Bank
Urzędu Komisji Nadzoru Finansowego
CERT Orange