

ZASADY ZAPOBIEGANIA OSZUSTWOM

I. Uważaj na manipulacje przestępców

1. Jeżeli otrzymasz połączenie telefoniczne budzące Twoje podejrzania, nie kontynuuj rozmowy — **rozłącz się**.
2. Jeżeli podczas rozmowy telefonicznej lub w e-mailu zostaniesz poinformowany, że na Twoje dane — bez Twojej wiedzy — złożono wniosek kredytowy lub o pożyczkę, zapytaj rozmówcę, w jakim banku lub firmie pożyczkowej miało to miejsce. **Pod żadnym pozorem nie podawaj jakichkolwiek danych ani nazw instytucji finansowych z których korzystasz.** Prawdopodobnie oszuści próbują w ten sposób wyłudzić informacje oraz Twoje dane metodą „na fałszywy wniosek”. **Rozłącz się i nie odbieraj kolejnych połączeń** w tej sprawie. Samodzielnie znajdź numer telefonu na oficjalnej stronie internetowej i skontaktuj się z bankiem bądź firmą pożyczkową, w której rzekomo miało miejsce podejrzane zdarzenie, aby zweryfikować jego prawdziwość.
3. Oszuści mogą podszywać się pod różne banki lub aplikacje, w tym np. BIK czy mObywatel 2.0, i wysyłać SMS z informacją o weryfikacji Twojego numeru PESEL w związku z rzekomą umową kredytową. Następnie dzwonią, udając pracownika BIK lub banku, aby wykorzystać niepokój wzbudzony tą wiadomością. **Nie wykonuj poleceń oszustów i najlepiej zakończ rozmowę.** Działając pod presją, możesz ujawnić swoje dane, które sprawcy wykorzystają do przejęcia pieniędzy. Prawdziwy SMS z mObywatel 2.0 dotyczący numeru PESEL nie zawiera powodu weryfikacji ani żadnych linków — wskazuje wyłącznie datę, godzinę oraz nazwę podmiotu, który dokonał sprawdzenia.
4. Jeśli ktoś faktycznie złoży wniosek o kredyt na Twoje dane, otrzymasz Alert BIK — pod warunkiem, że wcześniej wykupiłeś tę płatną usługę w Biurze Informacji Kredytowej (BIK). Wiarygodność SMS-z Alertem BIK potwierdź, logując się do swojego konta w BIK, gdzie znajdziesz listę wysłanych do Ciebie alertów i powiadomień. **PAMIĘTAJ — pracownicy BIK nie dzwonią do Klientów, aby interweniować w sprawie wyłudzeń.**
5. Jeżeli chcesz uniknąć sytuacji, w której ktoś mógłby wyłudzić w bankach kredyt na Twoje dane albo założyć rachunek bankowy, **zastrzeż bezpłatnie swój numer PESEL.** Zastrzeżenia można dokonać: w aplikacji mObywatel 2.0, na stronie internetowej www.gov.pl lub osobiście w urzędzie gminy. W dowolnym momencie, w taki sam sposób, możesz odwołać zastrzeżenie numeru PESEL.
6. Jeżeli ktoś zaoferuje Ci pożyczkę pod warunkiem wcześniejszej wpłaty przez Ciebie pieniędzy, oznacza to, że prawdopodobnie masz do czynienia z oszustwem.
7. Chronić swoje dane osobowe, w tym te zawarte w dokumentach tożsamości. W przypadku ich ujawnienia bezpłatnie zastrzeż dokument w urzędzie gminy, przez Internet (z wykorzystaniem

profilu zaufanego, certyfikatu kwalifikowanego lub e-dowodu), w aplikacji mObywatel 2.0 lub w banku. Jeśli padłeś ofiarą kradzieży dokumentu, zgłoś sprawę na Policji.

8. Przestępcy mogą podszywać się pod dowolny numer telefonu — jest to tzw. **spoofing** czyli maskowanie prawdziwego numeru telefonicznego, z którego dzwonią lub wysyłają wiadomości SMS. Mogą sprawić, że na Twoim telefonie wyświetli się ustawiony przez nich dowolny numer, w tym numer telefonu instytucji, banku lub osoby, którą znasz. Maskowanie numerów dotyczy wyłącznie połączeń i wiadomości SMS przychodzących, gdy to oszuści się kontaktują. Nie ma możliwości podszywania się pod numery instytucji lub osób w przypadku, gdy to Ty inicjujesz połączenie telefoniczne.
9. **PRACOWNICY DZIAŁU BEZPIECZEŃSTWA BANKU NIE KONTAKTUJĄ SIĘ BEZPOŚREDNIO Z KLIENTAMI.**
10. **UWAŻAJ** na e-maile od nadawców podszywających się pod przedstawicieli znanych firm lub instytucji państwowych np. Generalnego Inspektora Informacji Finansowej (GIIF). **Nie klikaj w linki, nie otwieraj załączników i nie odpowiadaj na takie wiadomości.** W pierwszej kolejności skontaktuj się z daną instytucją, aby zweryfikować, czy wiadomość nie pochodzi od oszustów. Dane kontaktowe instytucji wyszukuj wyłącznie na ich oficjalnych stronach internetowych.
11. **UWAŻAJ** na przestępców podających się za maklerów, brokerów giełdowych lub doradców ekonomicznych, którzy nakłaniają do inwestycji — szczególnie w: kryptowaluty, bitcoin, sztuczną inteligencję (AI) akcje Orlen, Tauron, BalticPipe lub inne bazujące na chwytliwych hasłach — zapewniając o szybkich, wysokich zyskach, bez żadnego ryzyka. Oszuści uwiarygadniają się poprzez profesjonalnie wyglądające serwisy informacyjne i kampanie marketingowe, a także rozpowszechniają zmanipulowane reklamy oraz filmy ze znanymi osobami zachwalającymi fałszywe inwestycje. Nie klikaj w te reklamy i pod żadnym pozorem nie uzupełniaj formularzy zgłoszeniowych. Przestępcy nawiązują kontakt i namawiają do dobrowolnych wpłat, a następnie nakłaniają swoje ofiary do instalowania oprogramowania pulpitu zdalnego (np. AnyDesk, Quick Support, TeamViewer, Splashtop SOS). Dzięki temu przejmują kontrolę nad urządzeniem, w tym nad dostępem do bankowości elektronicznej, co skutkuje kradzieżą pieniędzy z rachunku bankowego.
12. Jeżeli ktokolwiek zadzwoni do Ciebie, wyśle SMS lub wiadomość przez komunikator, podając się za bliską osobę, która rzekomo pilnie potrzebuje pieniędzy, **rozłącz się i samodzielnie skontaktuj z tą osobą**, aby zweryfikować informację. To samo dotyczy telefonów od fałszywych policjantów lub funkcjonariuszy innych służb, np. Centralnego Biura Śledczego Policji, którzy namawiają

do przekazania gotówki w ramach rzekomej policyjnej prowokacji mającej na celu ujęcie przestępców. **Taki telefon oznacza próbę oszustwa.**

13. Jeżeli wchodzisz na stronę internetową, szczególnie związaną z wykonywaniem płatności (np. sklepu lub banku) **zawsze sprawdzaj**, czy adres w górnym pasku (tzw. URL) jest zgodny z oryginalnym, czy też jedynie się pod niego podszywa (np. poprzez użycie w adresie nieprawidłowych liter, znaków lub domen).
14. Jeżeli sprzedajesz towary w Internecie, **czekaj na przelew** od kupującego i nie wykonuj dodatkowych czynności np. dopłacania niewielkich kwot do przesyłki czy podawania danych karty płatniczej lub danych logowania do bankowości elektronicznej, ponieważ możesz paść ofiarą oszustwa metodą „na OLX” lub „na InPost” (szczególnie przy kontakcie z kupującym przez komunikator WhatsApp).
15. Jeśli otrzymasz e-mail lub SMS dotyczący rzekomej konieczności uregulowania dopłaty, np. za energię elektryczną lub przesyłkę pocztową bądź kurierską, **nie reaguj i nie klikaj w linki**, jeżeli zostały w nich zawarte — możesz w ten sposób stracić pieniądze. Najlepiej skontaktuj się z daną instytucją, korzystając z numeru infolinii podanego na jej oficjalnej stronie internetowej, aby potwierdzić prawdziwość otrzymanej wiadomości.

II. Chroń dostęp do swoich pieniędzy

1. Stosuj wyłącznie legalne programy antywirusowe na swoich urządzeniach, aby chronić je przed szkodliwym oprogramowaniem.
2. Regularnie instaluj aktualizacje niezbędne do prawidłowego działania oprogramowania antywirusowego.
3. **NIKOMU nie podawaj danych logowania do bankowości elektronicznej oraz chroń dane z karty płatniczej (kod CVC, datę ważności i numer karty).**
4. Pod żadnym pozorem, nie instaluj ani nie korzystaj na swoim urządzeniu z aplikacji pulpitu zdalnego (np. AnyDesk, Quick Support, TeamViewer, Splashtop SOS), rzekomo mającej pomóc w obsłudze Twoich finansów. Takie aplikacje umożliwiają przejęcie kontroli nad zawartością urządzenia i mogą posłużyć do kradzieży danych oraz środków z rachunku bankowego. Zarówno banki, jak i inne instytucje zaufania publicznego nie nakłaniają swoich Klientów do instalowania takich aplikacji ani do korzystania z pulpitu zdalnego w jakiejkolwiek formie.
5. **NIE ZAPISUJ HASEŁ w przeglądarkach internetowych.**
6. **NIE KLIKAJ W LINKI** otrzymane (SMS-em lub e-mailem) z nieznanych źródeł — mogą one zainfekować Twoje urządzenie.

7. Jeżeli obawiasz się, że ktoś przejął kontrolę nad Twoją bankowością elektroniczną, po zalogowaniu na stronie plusbank24.pl wybierz w górnej części ekranu zakładkę „Mój profil”, a następnie w menu po lewej stronie kliknij „**Ustawienia dostępu**”. W nowym oknie możesz zablokować dostęp do kanału Internet, Telefon/SMS oraz do aplikacji mobilnej na wszystkich urządzeniach.
8. Jeżeli podejrzewasz, że w bankowości elektronicznej dodano urządzenie mobilne bez Twojej zgody, po zalogowaniu na stronie plusbank24.pl wybierz w górnej części ekranu zakładkę „Mój profil”, a następnie w pionowym menu „**Urządzenia mobilne**”. Jeżeli nie rozpoznajesz wskazanego urządzenia, wybierz opcję „**Usuń**”.
9. **Ogranicz dzienny limit oraz limit pojedynczej transakcji w bankowości elektronicznej i aplikacji mobilnej, dostosowując je do własnych potrzeb.** Aby zmienić limit transakcji w bankowości elektronicznej plusbank24 skontaktuj się z infolinią Banku pod numerem telefonu: **61 846 14 61 lub 801 44 55 66** (opłata za połączenie zgodnie z taryfą operatora) lub udaj się do najbliższego Oddziału Partnerskiego PLUS BANK S.A. Limit pojedynczej transakcji w aplikacji mobilnej możesz zmienić samodzielnie po zalogowaniu się do bankowości elektronicznej i wybraniu zakładki „**Ustawienia**”.
10. **Nie wyszukuj** strony logowania Banku w wyszukiwarce internetowej. Dane logowania do bankowości elektronicznej plusbank24 wprowadzaj po wpisaniu w pasku adresu: **plusbank24.pl**
11. Przed wprowadzeniem hasła otrzymanego w wiadomości SMS do zatwierdzenia przelewu w bankowości elektronicznej **ZAWSZE SPRAWDZAJ**, czy treść wiadomości jest zgodna z Twoją dyspozycją — w szczególności kwota i końcówka numeru rachunku bankowego odbiorcy.
12. Zapoznawaj się z komunikatami bezpieczeństwa, które Bank cyklicznie przesyła do Ciebie w bankowości elektronicznej.

III. Zgłaszaj podejrzenia

1. W przypadku jakichkolwiek podejrzeń lub wątpliwości dotyczących bezpieczeństwa Twoich pieniędzy niezwłocznie skontaktuj się z Bankiem, dzwoniąc na numer infolinii: **61 846 14 61 lub 801 44 55 66, która jest czynna od poniedziałku do soboty w godzinach 9:00-21:00** (opłata za połączenie wg cennika operatora). Możesz też wysłać wiadomość do Banku w swojej bankowości elektronicznej, albo udać się do najbliższego Oddziału Partnerskiego Banku.
2. Podejrzane e-maile, złośliwe domeny, fałszywe sklepy internetowe i inne próby podszywania się możesz zgłosić do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK na stronie internetowej: incydent.cert.pl

3. Jeżeli otrzymasz podejrzaną wiadomość SMS z linkami, możesz przesłać ją **w niezmienionej formie tekstowej** na bezpłatny numer telefonu **8080**, obsługiwany przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK (pamiętaj, że **nie może** to być MMS w postaci zrzutu ekranu). Jeżeli czujesz się pokrzywdzony, nawet samym faktem kontaktu ze strony oszustów, **niezwłocznie zgłoś sprawę na Policję**.

IV. PAMIĘTAJ– OSZUŚCI DZIAŁAJĄ WG SCHEMATU:

1. Wywołać silny stres i poczucie zagrożenia.
2. Wyłudzić dane i informacje.
3. Wyłączyć zdolność racjonalnego myślenia i oceny sytuacji.
4. Wywołać działanie pod presją czasu i stałą kontrolą (przez cały czas trwania połączenia telefonicznego oszusta z pokrzywdzonym).
5. Nakłonić do szybkich i nieprzemyślanych działań (np. instalowania złośliwych aplikacji, ujawnienia danych, które powinny być chronione, realizacji przelewów), skutkujących wyłudzeniem lub kradzieżą pieniędzy).