



infoDOK

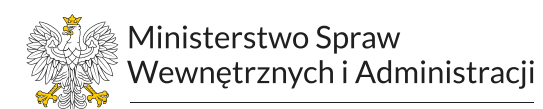
Raport o dokumentach

IV kwartał 2023 r.

/ 56. edycja /

Kampania Informacyjna Systemu
DOKUMENTY ZASTRZEŻONE

Patronat honorowy



Współpraca



Patronat



Organizator



Kampania informacyjna Systemu DOKUMENTY ZASTRZEŻONE

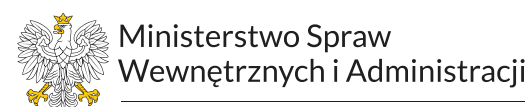
Akcja trwa od 16 lipca 2008 r. Celem jest informowanie o potrzebie zastrzegania utraconych dokumentów, gdyż wiedza w tym zakresie była zbyt ograniczona.

Rozpowszechniane są informacje o Systemie DZ w aspekcie korzyści i bezpieczeństwa osób, które utraciły dokumenty tożsamości. Istnieje bowiem możliwość uniknięcia szeregu przykrych konsekwencji mogących powstać w wyniku kradzieży tożsamości.

System DOKUMENTY ZASTRZEŻONE Związku Banków Polskich to ogólnopolska baza milionów skradzionych i zagubionych dokumentów. Chroni przed wyłudzeniami z użyciem cudzej tożsamości.

Zastrzegać powinni wszyscy – nie tylko klienci banków. To najważniejszy krok, który trzeba natychmiast zrobić, gdy utracimy np. dowód osobisty, paszport czy prawo jazdy. W kilka minut dane są dostępne dla wszystkich banków, operatorów telefonii komórkowych oraz tysięcy innych firm.

Patronat honorowy



Współpraca



Patronat



Organizator



Partnerzy



Patroni medialni



W Systemie uczestniczą wszystkie polskie banki oraz szereg innych firm i instytucji. Pokazane powyżej logotypy banków przedstawiają wybranych Uczestników Systemu, którzy przystąpili do dodatkowej, społecznej Kampanii Informacyjnej. Ich szczególne potraktowanie w niniejszym materiale jest wyrazem podziękowania ze strony Związku Banków Polskich za wkład w promocję idei zabezpieczenia nas wszystkich przed przestępstwami z wykorzystaniem kradzionych dokumentów.

4

Wstęp

5

Raport w liczbach

6

W skrócie:
Zgubiłem lub ukradziono mi dokumenty – co mam zrobić?

7

Liczba zastrzeżonych dokumentów tożsamości

8

Łączna liczba i kwota udaremnionych prób wyłudzeń kredytów

9

Liczba zastrzeżonych dokumentów tożsamości oraz ogólna liczba przestępstw

10

Liczba udaremnionych prób wyłudzeń – wg. województw

11

Łączna kwota udaremnionych prób wyłudzeń – wg. województw

12

Średnia kwota udaremnionych prób wyłudzeń – wg. województw

13

Największe kwoty prób wyłudzeń kredytów

14

Kapanie społeczne

16

Prawdziwe historie

Opracowanie Raportu:

Grzegorz Kondek
tel. (22) 48 68 426
e-mail: grzegorz.kondek@cpb.pl

Emilia Ożarowska
tel. (22) 48 68 426
e-mail: emilia.ozarowska@cpb.pl

Wstęp

Szanowni Państwo,
zapraszam do lektury **56. wydania raportu infoDOK** – od już 14 lat omawiamy tematykę związaną z zastrzeganiem kradzionych i zgubionych dokumentów tożsamości oraz próbach ich nielegalnego wykorzystania.

W latach 2008–2023:

- » baza Systemu DOKUMENTY ZASTRZEŻONE urosła do **2.476.116 szt.** dokumentów (rekordowy był IV kwartał 2019 r., gdy zastrzeżono 56.686 szt.)
- » próbowano wyłudzić **117,8 tysięcy kredytów na łączną kwotę 5,8 miliarda zł**
- » rekordowa próba wyłudzenia opiewała na **25 milionów zł**
- » aż **718 prób** dotyczyło kwot równych lub większych niż **1 mln zł**
- » **20.015 prób** dotyczyło kwot równych **1 tys. zł** lub niższych

Przejdźmy do analizy szczegółowych danych z IV kwartału 2023 r. Na koniec grudnia 2023 r. wielkość Centralnej Bazy Danych Systemu DZ wyniosła **2,476.116 szt. dokumentów**. W ostatnich trzech miesiącach odnotowano wzrost o **51,5 tysiąca nowych zastrzeżeń** (str. 7) – to **28% więcej** niż rok temu, a w skali całego badania to 2. najwyższy wynik kwartalny od 2008 r. Statystycznie do bazy trafiało codziennie 560 dokumentów. **W całym 2023 r. zastrzeżono łącznie 177,8 tys. szt. – to rekordowy jak dotąd wynik roczny.**

W IV kwartale 2023 r. **próbowano wyłudzić 2.739 kredytów, na łączną kwotę 88,3 mln zł**. O ile łączna kwota jest bardzo zbliżona do 14-letniej średniej (90,5 mln zł), to już **liczba prób wyłudzeń była najwyższa w historii** i pobiła dotychczasowy rekord o 5,9%.

Podobnie było w skali całego 2023 r.: 9.730 to także najwyższy wynik zanotowany od 2008 r. W Q4 2023 r. tradycyjnie najwięcej przypadków prób wyłudzeń odnotowano w województwach dolnośląskim, śląskim i mazowieckim (str. 10).

W IV kwartale 2023 r. odnotowano **16 prób wyłudzeń na bardzo wysokie kwoty 1 mln zł**. Te kwoty z łącznej puli 2,7 tys. prób wyłudzeń w tym kwartale to aż 18% z sumy wszystkich pieniędzy, które chciano w tym czasie ukraść.

Polecam część opisową – prezentujemy tam przede wszystkim ważne komunikaty z kampanii społecznych ZBP i Policji dot. bezpieczeństwa (str. 14–15) oraz krótkie opisy prawdziwych zdarzeń pochodzących z kronik policyjnych (str. 16 i kolejne).

Zapraszam do lektury Raportu infoDOK!

Grzegorz Kondek

Koordynator Kampanii Informacyjnej
Systemu DOKUMENTY ZASTRZEŻONE



Raport w liczbach

2 476 116

stan na 31 grudnia 2023 r.

przyrost w IV kwartale 2023

Liczba dokumentów tożsamości w Centralnej Bazy Danych Systemu DOKUMENTY ZASTRZEŻONE



51 520

IV kwartał 2023 r.

177 762

ostatnich 12 miesięcy

Liczba zastrzeżonych dokumentów tożsamości

[w szt.]



2 739

IV kwartał 2023 r.

9 730

ostatnich 12 miesięcy

Liczba udaremnionych prób wyłudzeń kredytów

[w szt.]



88,3 mln

IV kwartał 2023 r.

296,1 mln

ostatnich 12 miesięcy

Łączna kwota udaremnionych prób wyłudzeń kredytów

[w zł]



18,7 tys.

IV kwartał 2023 r.

17,7 tys.

ostatnich 12 miesięcy

Średnia kwota udaremnionych prób wyłudzeń kredytów

[w zł]



1,0 mln

IV kwartał 2023 r.

2,0 mln

ostatnich 12 miesięcy

Kwota największej udaremnionej próby wyłudzenia kredytu

[w zł]

Raport w liczbach

56. Raport o dokumentach infoDOK
(IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich
Źródło danych: Związek Banków Polskich
oraz Biuro Informacji Kredytowej

Co robić w przypadku utraty dokumentów?

1

Zastrzec dokumenty w banku

Najłatwiej to zrobić w swoim oddziale osobiście, a w wielu bankach także telefonicznie pod numerem **828 828 828**. Kto nie ma rachunku, może iść do banku przyjmującego zastrzeżenia od wszystkich (lista: www.DokumentyZastrzezone.pl).

Można także skorzystać z www.bik.pl (jeżeli ktoś miał tam założone wcześniej konto na utracony dokument).

2

Zgłosić się do najbliższej jednostki policji

Należy to zrobić tylko jeżeli dokumenty zostały utracone w wyniku przestępstwa (np. kradzież).

3

Zawiadomić gminę lub placówkę konsularną

Udajemy się tam w celu wyrobienia nowego dokumentu.

Jak to działa?

Wystarczy zgłosić dokument w jednym banku, aby dane automatycznie przekazano do Centralnej Bazy Danych, a następnie rozesłano do wszystkich banków, operatorów telefonii komórkowych oraz tysięcy innych firm i instytucji korzystających z Systemu DZ.

Dokumenty można zastrzegać nie tylko osobiście. Większość banków przyjmuje zgłoszenia telefonicznie (od swoich klientów), a część wprowadziła taką funkcję również do bankowości elektronicznej.

Jeżeli ktoś spróbuje posłużyć się zastrzeżonym dokumentem, operacja zostanie zablokowana, a do wyjaśnienia sprawy wzywana jest Policja.

Kiedy należy zastrzegać?

Trzeba to zrobić zarówno w przypadku zgubienia, jak i utraty dokumentu w wyniku kradzieży. Niezależnie od przyczyny, bardzo ważne jest, aby zareagować możliwie jak najszybciej, żeby nikomu nieuczciwemu nie dać szansy na wykorzystanie dokumentu do celów przestępczych.

Jakie dokumenty?

Najważniejsze są: dowód osobisty, paszport oraz prawo jazdy.

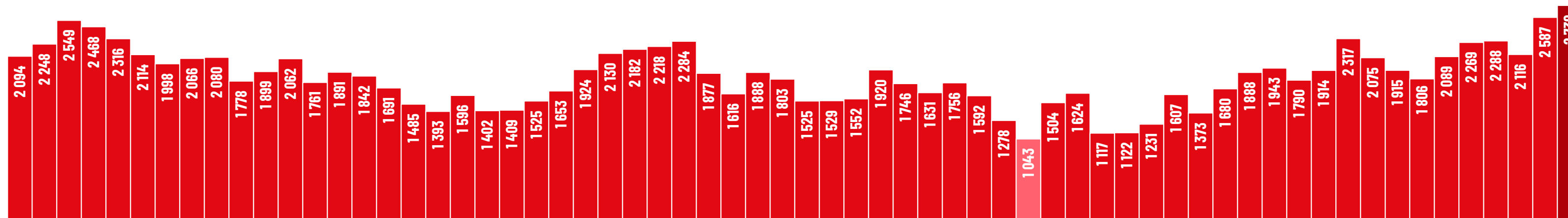
Dlaczego należy zastrzegać?

- Dziennie zdarza się kilkadziesiąt prób posłużenia się cudzym lub podrobionym dokumentem. Przykłady najczęstszych przestępstw:
- wyłudzenia kredytów i pożyczek,
 - unikanie opłat, kradzieże wyposażenia (wynajem mieszkań i pokoi hotelowych),
 - kradzieże wynajętych samochodów lub innych rzeczy,
 - zakładanie fikcyjnych firm (przestępstwa kredytowe i podatkowe).

Liczby i kwoty udaremnionych prób wyłudzeń kredytów

Liczby prób wyłudzeń kredytów

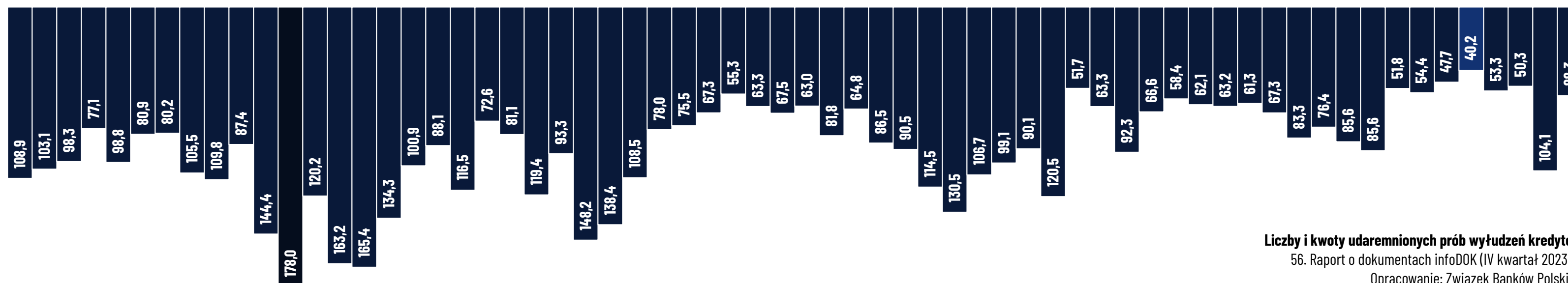
[szt.]



9 359	8 494	7 819	7 185	5 876	6 511	8 814	7 184	6 526	6 725	5 449	5 077	6 884	8 096	8 079	9 730
2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04	01 02 03 04
387,3	365,4	519,5	583,1	378,0	442,0	400,4	253,3	296,0	442,2	361,5	280,6	253,8	336,6	194,1	296,1

Łączne kwoty prób wyłudzeń kredytów

[mln zł]



Liczby i kwoty udaremnionych prób wyłudzeń kredytów

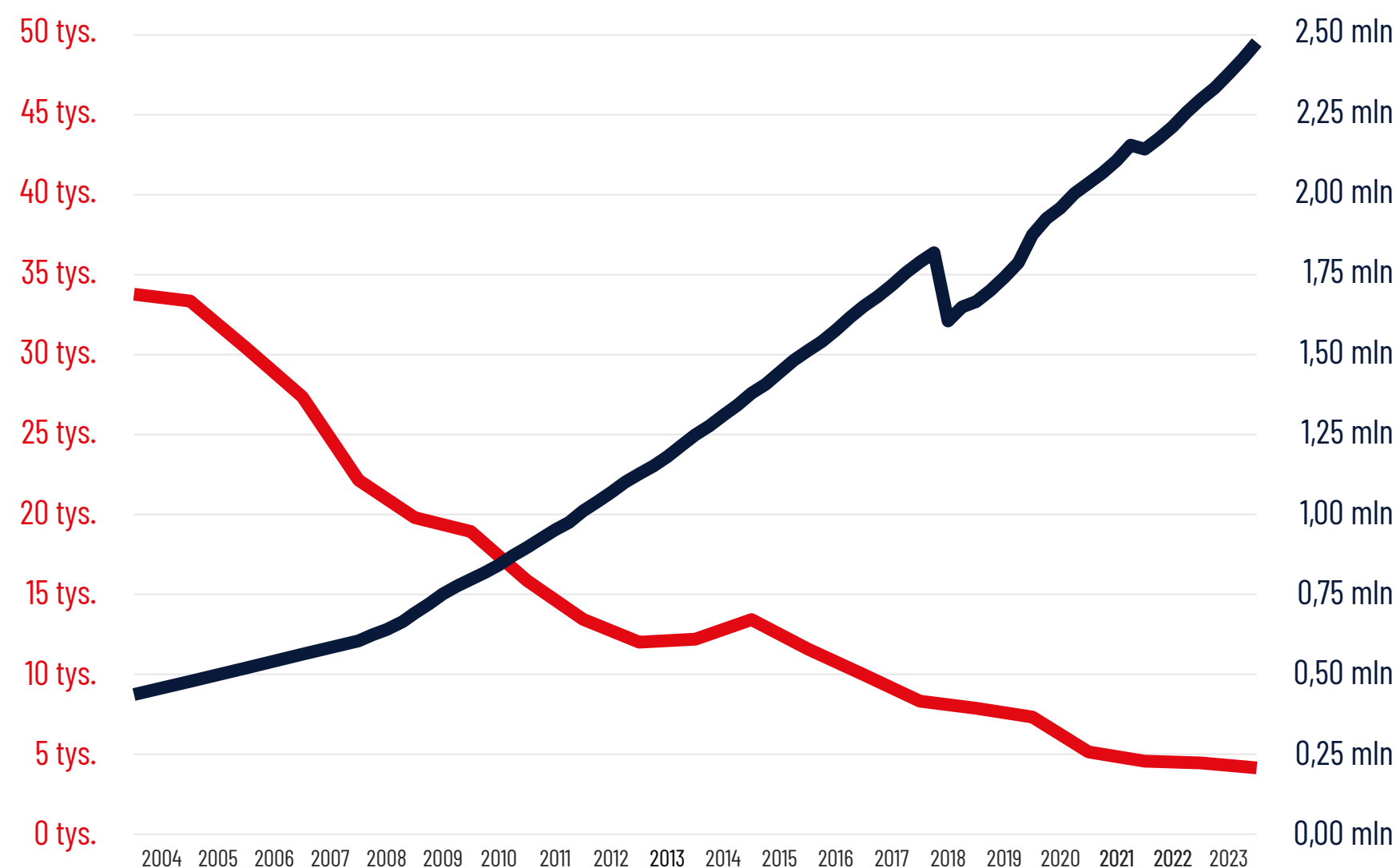
56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich

Źródło danych: Biuro Informacji Kredytowej

Liczby zastrzeżonych dokumentów tożsamości oraz ogólne liczby przestępstw związanych z dokumentami

Postępowanie się dokumentami innej osoby (art. 275 § 1-2 KK)



Liczba zastrzeżonych dokumentów tożsamości w Systemie DZ oraz ogólne liczby przestępstw związanych z dokumentami

56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Źródło danych: Związek Banków Polskich oraz Komenda Główna Policji

Postępowanie się dokumentami innej osoby, Podrabianie dokumentów, Liczba zastrzeżonych dokumentów (System DZ)

Rok	Postępowanie się dokumentami innej osoby	Podrabianie dokumentów	Liczba zastrzeżonych dokumentów (System DZ)
2003	33 775	36 381	436 778
2004	33 350	43 456	480 006
2005	30 391	39 870	530 862
2006	27 322	36 230	590 693
2007	22 087	33 801	661 083
2008	19 729	30 772	743 894
2009	18 854	32 770	848 205
2010	15 770	35 060	950 095
2011	13 332	36 025	1 059 237
2012	11 896	29 588	1 173 562
2013	12 084	30 331	1 294 248
2014	13 316	30 392	1 422 406
2015	11 616	26 988	1 553 238
2016	10 004	28 324	1 690 925
2017	8 336	23 794	1 827 020
2018	7 889	22 906	1 704 839
2019	7 339	20 077	1 881 393
2020	5 142	17 998	2 038 229
2021	4 561	15 530	2 142 582
2022	4 454	19 701	2 298 354
2023	4 145	14 706	2 476 116

Wielkość bazy danych Systemu DZ oraz ogólne liczby przestępstw związanych z dokumentami

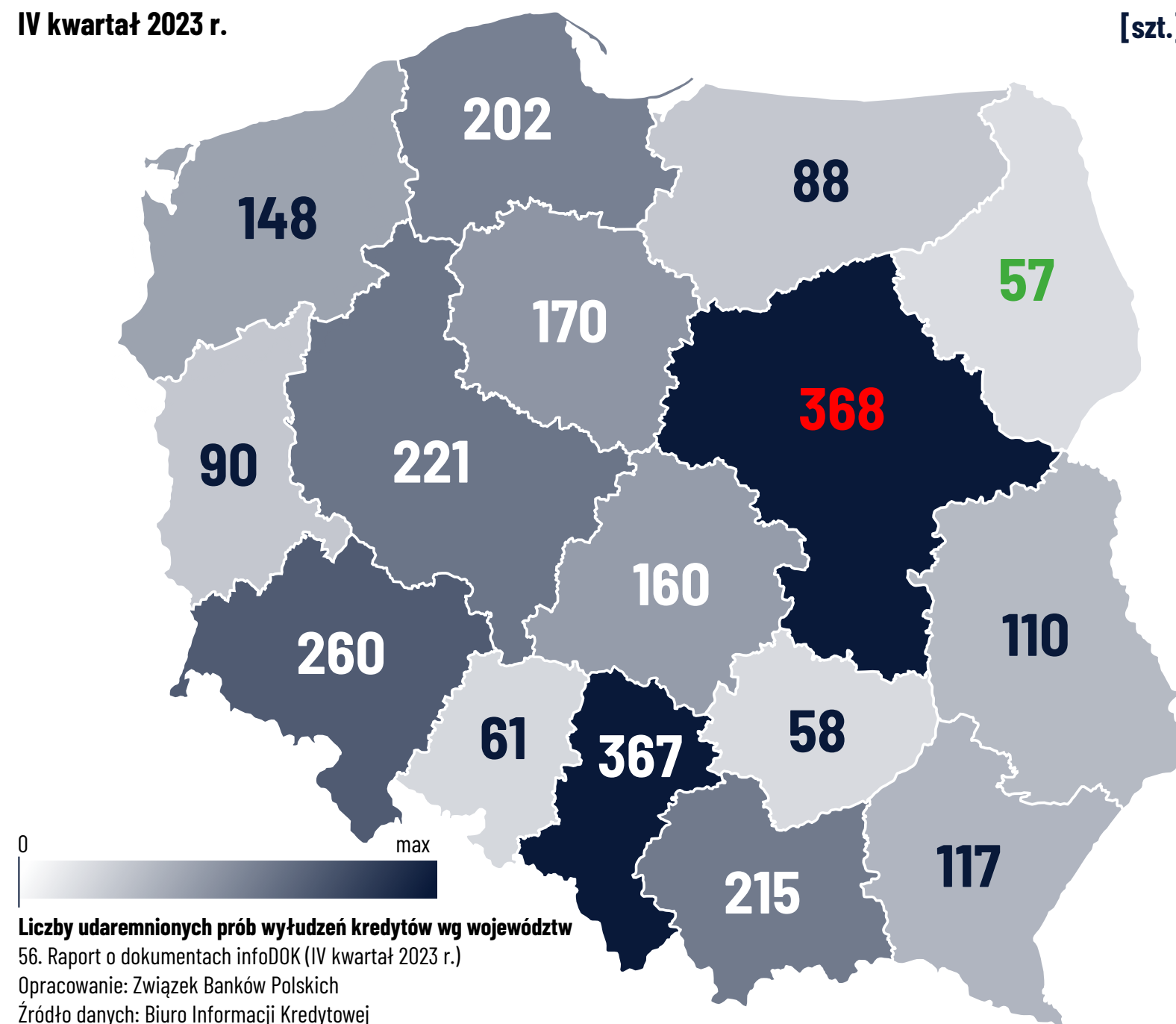
56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Źródło danych: Związek Banków Polskich oraz Komenda Główna Policji

Liczby udaremnionych prób wyłudzeń wg województw

IV kwartał 2023 r.

[szt.]



Liczby udaremnionych prób wyłudzeń kredytów wg województw

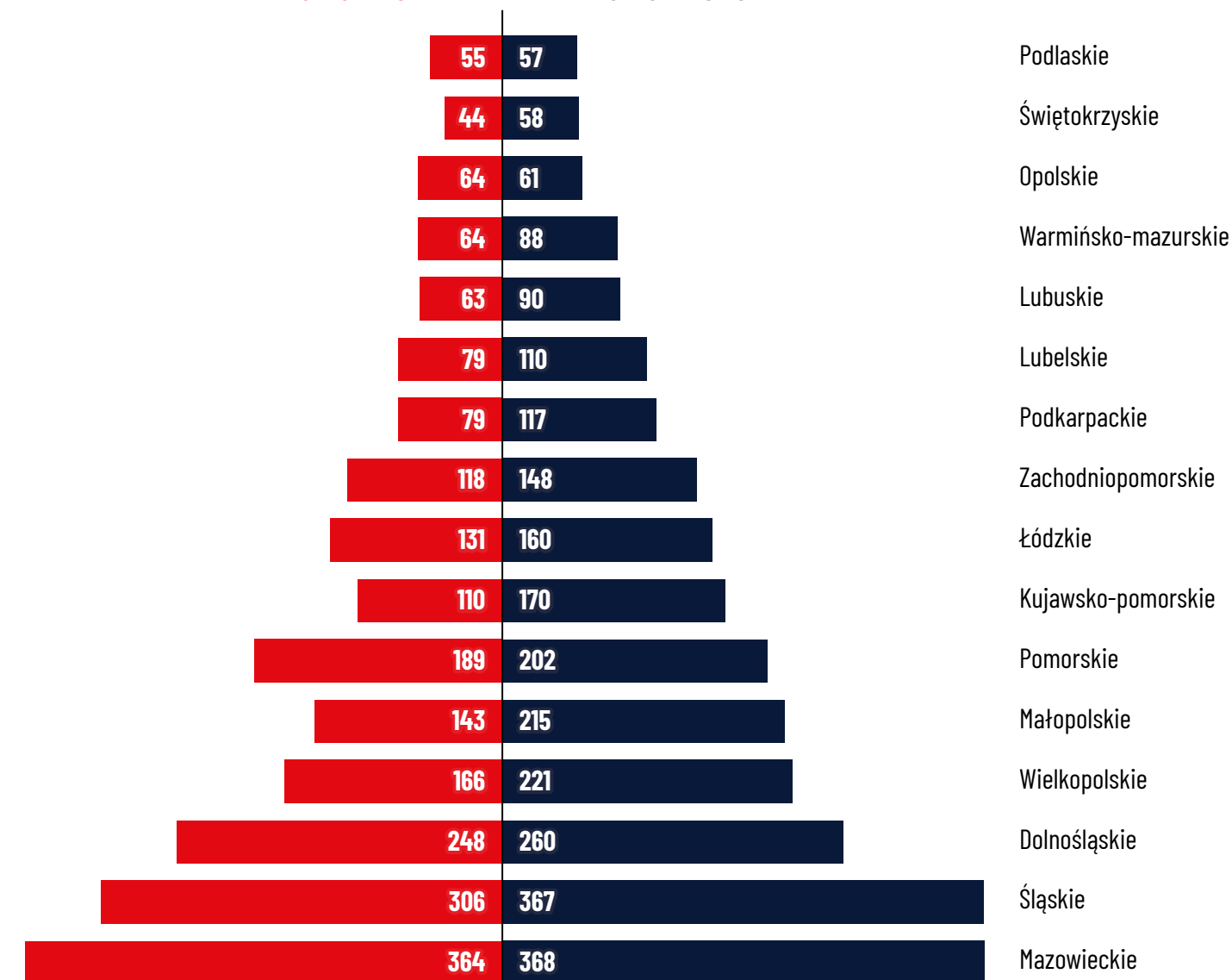
56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich

Źródło danych: Biuro Informacji Kredytowej

IV kwartał 2022 r.

IV kwartał 2023 r.



[mln zł]

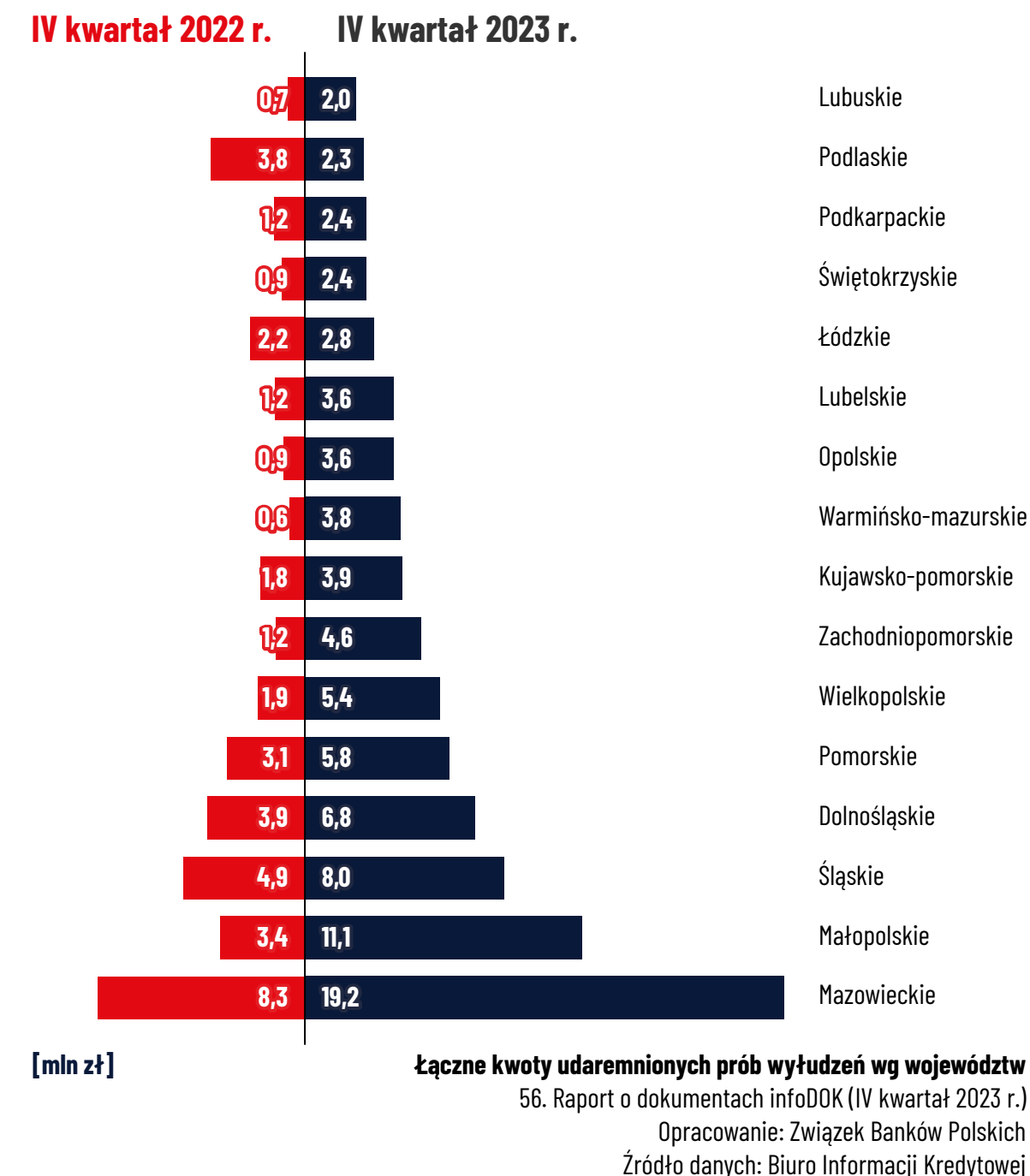
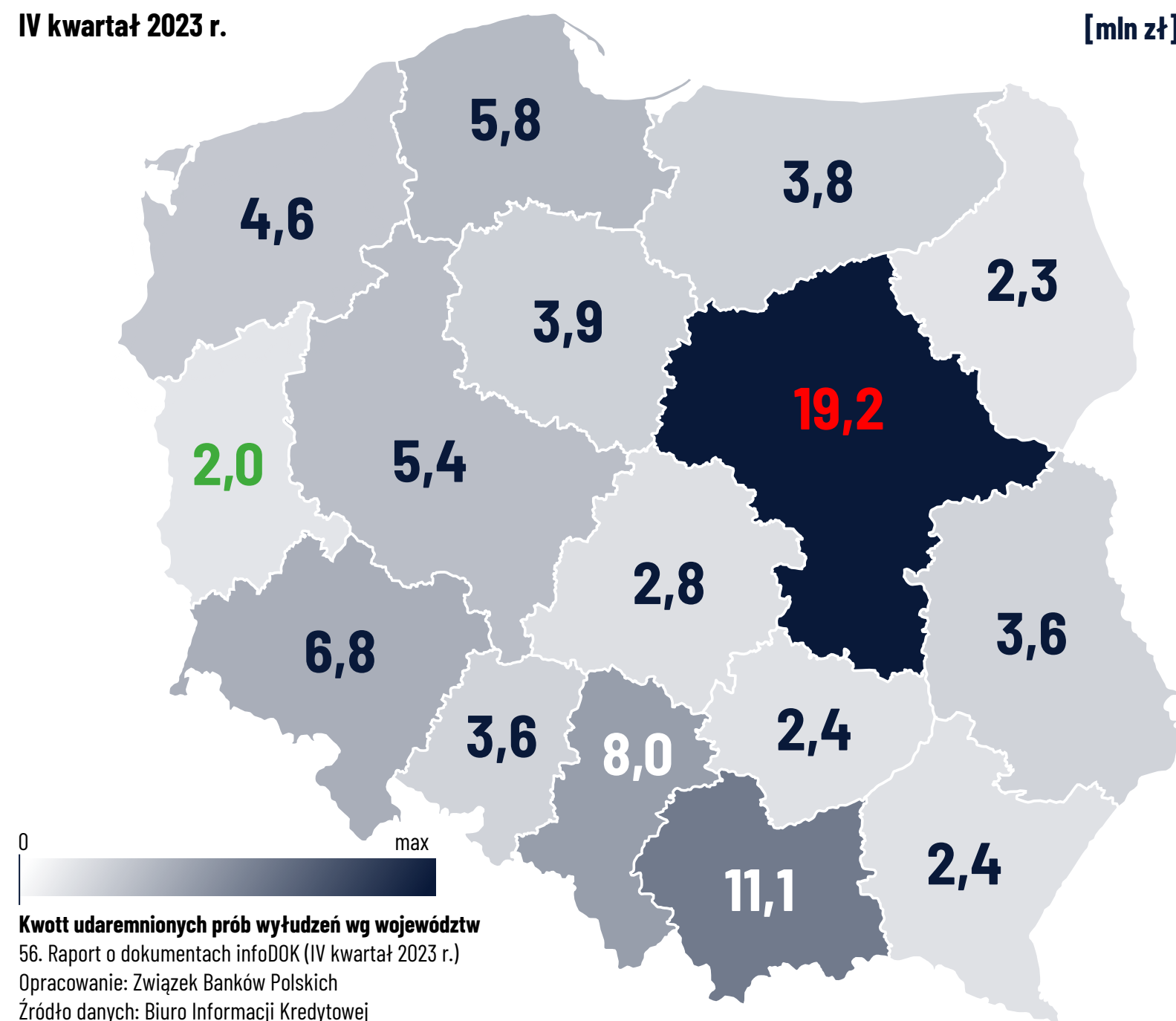
Liczby udaremnionych prób wyłudzeń kredytów wg województw

56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich

Źródło danych: Biuro Informacji Kredytowej

Kwoty udaremnionych prób wyłudzeń wg województw

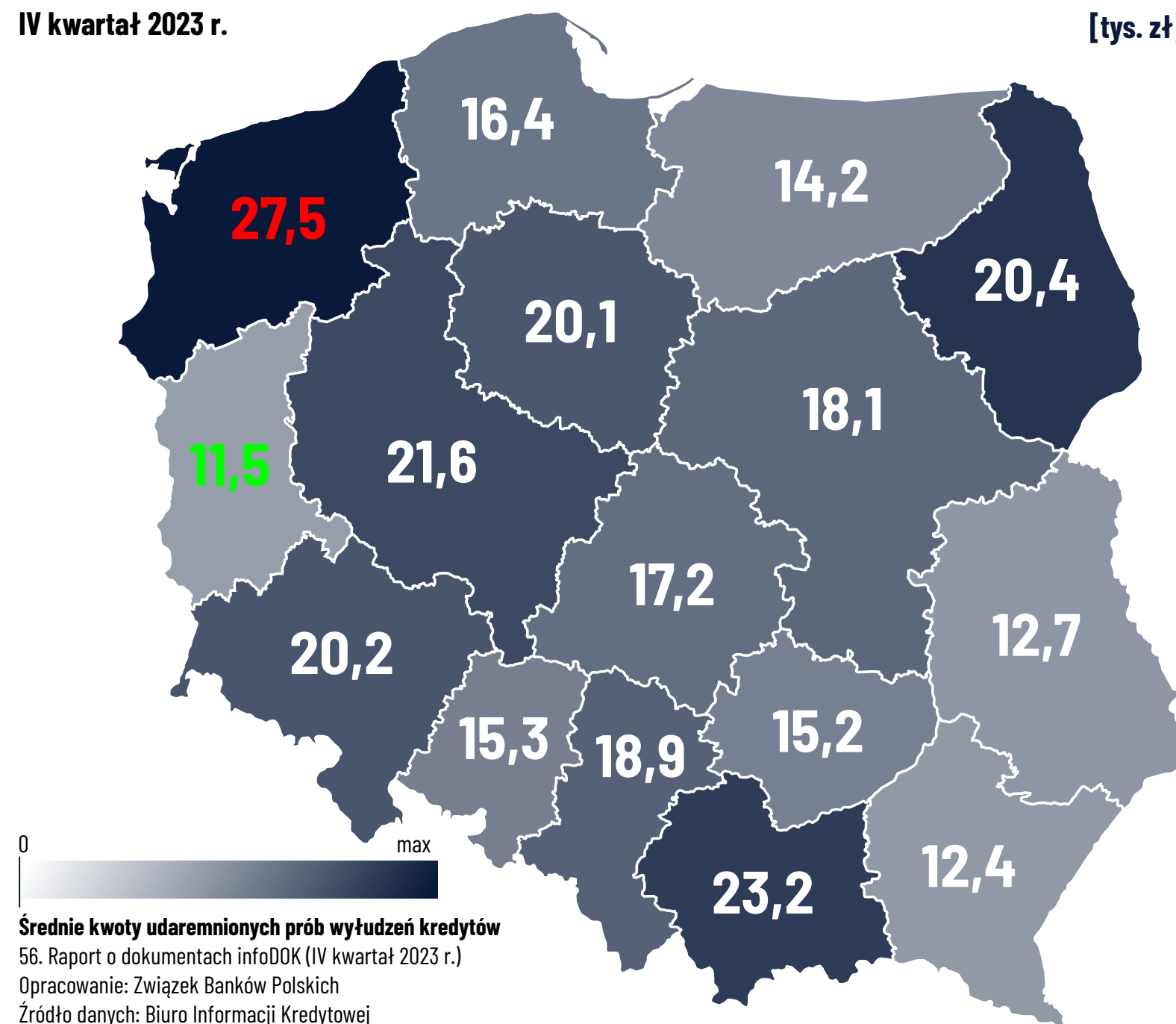


Średnie kwoty udaremnionych prób wyłudzeń kredytów wg województw

Przy wyliczeniu zostały odrzucone najbardziej ekstremalne wyniki (największe kwoty równe lub większe niż 500 000 zł), które mogły w znaczny sposób wpłynąć na średnią kwotę udaremnionych prób wyłudzeń w poszczególnych województwach.

IV kwartał 2023 r.

[tys. zł]



Średnie kwoty udaremnionych prób wyłudzeń kredytów

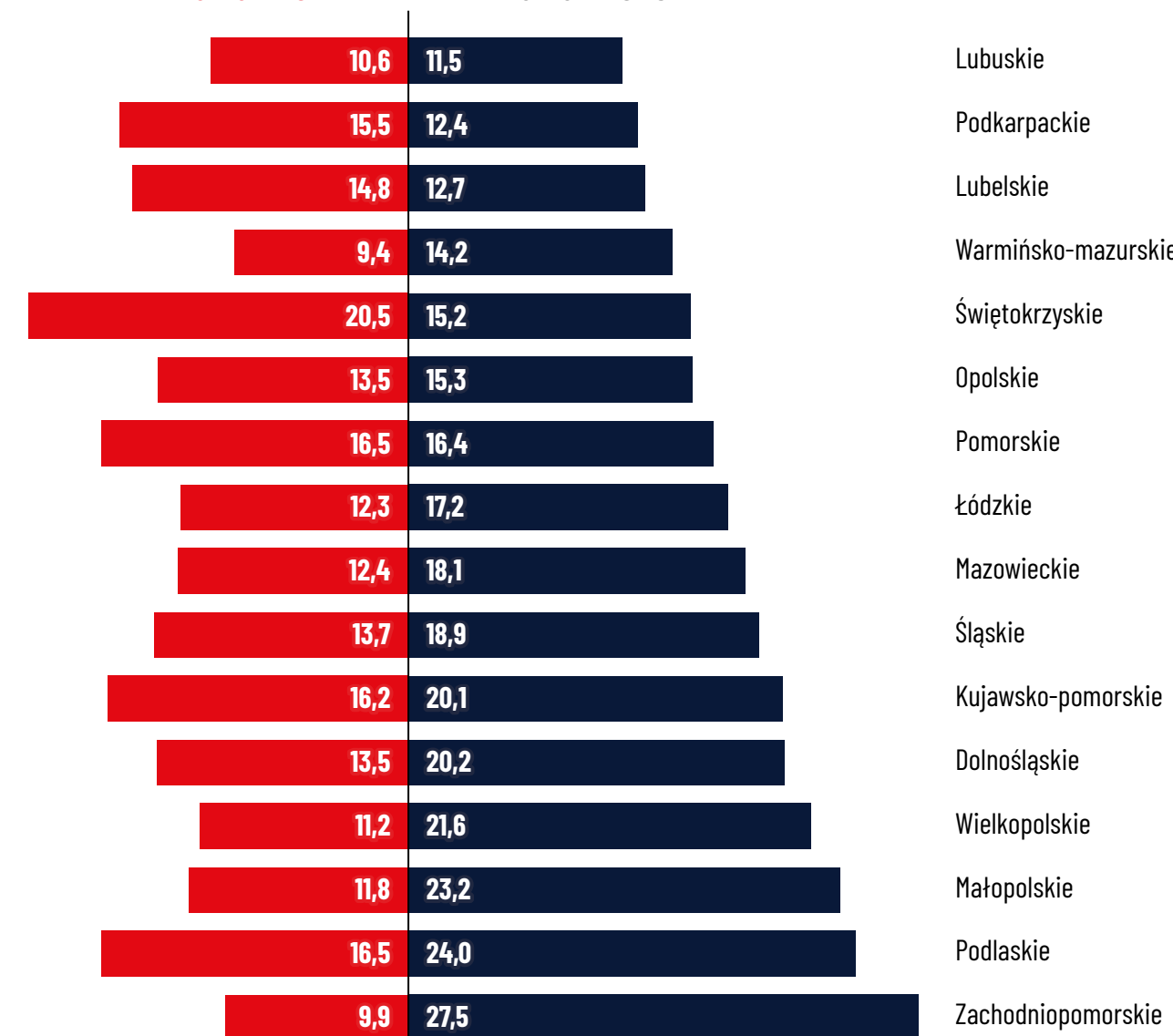
56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich

Źródło danych: Biuro Informacji Kredytowej

IV kwartał 2022 r.

IV kwartał 2023 r.



[tys. zł]

Średnie kwoty udaremnionych prób wyłudzeń kredytów wg województw

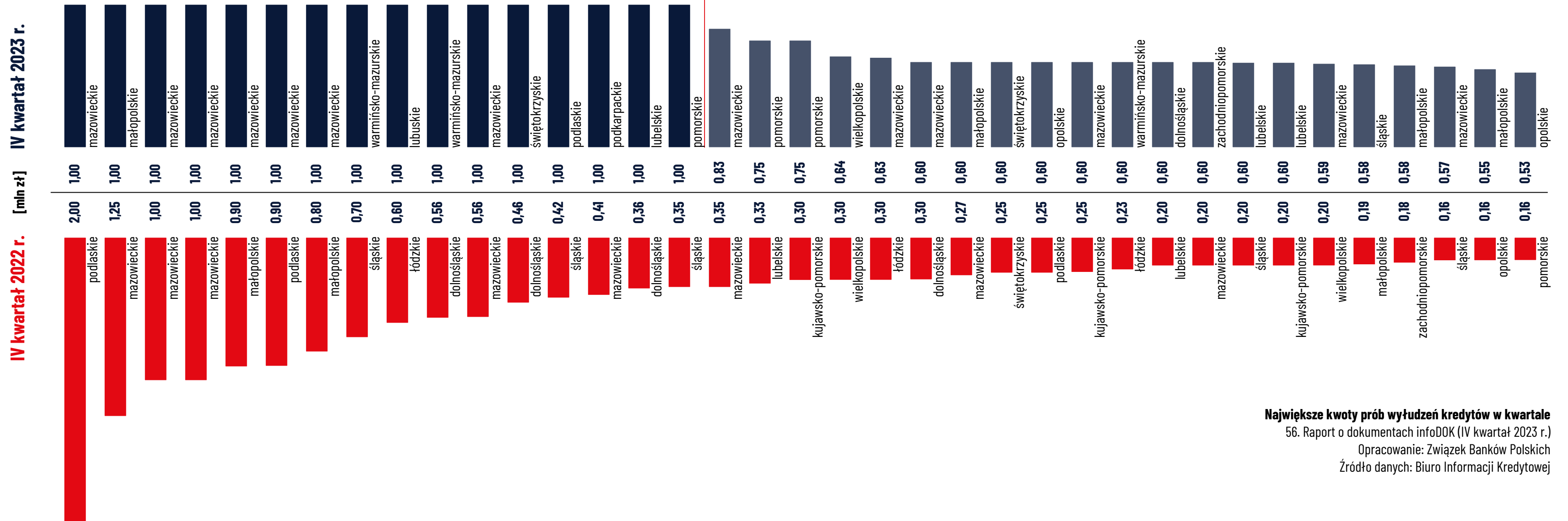
56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich

Źródło danych: Biuro Informacji Kredytowej

Największe kwoty prób wyłudzeń kredytów w IV kwartale 2023 w por. do IV kwartału 2022 r.

16 największych kwot z 2,7 tys. prób wyłudzeń w IV kwartale 2023 r. odpowiada za 18% z sumy wszystkich pieniędzy, które chciano ukraść



Największe kwoty prób wyłudzeń kredytów w kwartale

56. Raport o dokumentach infoDOK (IV kwartał 2023 r.)

Opracowanie: Związek Banków Polskich

Źródło danych: Biuro Informacji Kredytowej

Eksperyment społeczny w ramach kampanii „Cyberbezpieczeństwo – prostsze niż myślisz”

Związek Banków Polskich wspólnie z Super Expressem, Komendą Główną Policji i Bankowym Centrum Cyberbezpieczeństwa zorganizował eksperyment społeczny w ramach kampanii „Cyberbezpieczeństwo – prostsze niż myślisz”. W ramach eksperymentu na stronie Super Expressu zostały zamieszczone banery zachęcające internautów do kliknięcia i skorzystania ze specjalnej oferty zakupowej czy szybkiego zarobku.

Banery przypominały rzeczywiste oferty sprzętu AGD, sklepów odzieżowych oraz reklam inwestycyjnych, np. w kryptowaluty. Elementem prowokacji było pozyskanie potencjalnych klientów i uzyskanie od nich dorozumianej zgody na przekazanie danych wrażliwych (PESEL). Celem akcji było uświadomienie Polaków i zobrazowanie im zagrożeń, jakie czyhają w świecie cyfrowym.

W ciągu dwóch tygodni ponad 14 tysięcy osób kliknęło w fałszywą reklamę i było gotowych podać swoje dane w celu skorzystania ze wskazanych ofert. Klienci w żaden sposób nie weryfikowali pochodzenia reklamy ani firmy za nią stojącej. Gdy internauci klikali w baner, zamiast obiecanych markowych butów czy super taniego sprzętu AGD, ukazywał im się film, który rozpoczął się słowami: „To nie jest gra – to prawdziwe życie”. **Film (link do materiału zawarty jest w widocznym obok kodzie QR) zawierał opis najbardziej popularnych sposobów wyłudzenia danych wrażliwych. Pokazywał jak bronić się przed wyłudzeniami.**

– Świadomość zagrożeń, które płyną z cyberprzestępczości jest bardzo niska. Dlatego wszystkie działania, które mają na celu uświadamiać, że oferty, które



dla przeciętnego Kowalskiego brzmią nierealistycznie, są oszustwem. Nie ma niczego za darmo. Obietnice, że wystarczy kilka kliknięć, żeby zyskać kilka tysięcy, wysyp fałszywych reklam, często z udziałem celebrytów, czy polityków bez ich zgody i wiedzy, są próbą wyłudzenia danych. Te reklamy pojawiają się na serwerach państw spoza UE. Będziemy wszystkimi możliwymi środkami starać się dotrzeć do świadomości klientów obrazując im zagrożenia związane z cyberprzestępczością. Podobnie reklamy, które odnoszą się do inwestycji z kryptowalutami, w znaczącej większości są fałszywe. Podobnie jak dziwnie wyglądające telefony, gdy ktoś próbuje się podszyc pod bank, próbując wywołać panikę u klienta, że jego środki są zagrożone i musi nagle przelać środki pieniężne. Jeśli mamy jakikolwiek cień wątpliwości, czy rzeczywiście dzwoni do nas pracownik banku, rozłączmy się i zadzwońmy na infolinię banku. – mówi dr Tadeusz Białek, prezes Związku Banków Polskich.

Na zakończenie eksperymentu, akcja została opisana w drukowanym wydaniu Super Expressu w nakładzie ok. 100 000 egzemplarzy. W publikacji został załączony poradnik, wskazujący czytelnikom w prosty sposób, jak dbać o cyberbezpieczeństwo.

Wyniki prowokacji pokazują, że edukacja w obszarze cyberbezpieczeństwa i działania promujące bezpieczeństwo cyfrowe są nadal bardzo potrzebne.

Po więcej informacji na temat cyberbezpieczeństwa zapraszamy na stronę – **BankiwPolsce.pl/Cyberbezpieczenstwo**.

Uważaj na SMS'y dotyczące rzekomych dopłat do przesyłek kurierskich lub zmiany danych adresowych dotyczących przesyłki

Komunikat Komendy Głównej Policji, FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP i Centralnego Biura Zwalczenia Cyberprzestępczości.

Licho niestety nie śpi – również podczas zakupów online. Kiedy myślisz, że wszystko masz pod kontrolą, nagle dostajesz wiadomość SMS. To informacja o nieoczekiwanej dopłacie do przesyłki lub zmianie adresu dostawy... Oblewa cię zimny pot „przecież teściowa marzyła o szalu, który zamówiłam online”. Niepokój przeradza się w przerażenie, które zaczyna wyłączać racjonalne myślenie i chłodny osąd sytuacji.

Klikasz w link przesyłany w wiadomości, otwiera się strona, zaczynasz aktualizować dane: adres, e-mail, numer telefonu. Ostatnie kliknięcia, jeszcze tylko podam: imię i nazwisko, numer karty płatniczej, data jej ważności i kod CVV, ...uff zaraz będzie można odetchnąć, „ostatnia prosta” – kliknę przycisk „wyślij” i pożar będzie zgaszony, ale czy aby na pewno?

Stop! Zatrzymujesz się na chwilę, czy to na pewno jest bezpieczne? Może to jakieś oszustwo? Szukasz informacji na temat tego rodzaju wiadomości, sprawdzasz, czy inni nie padli ofiarą tego typu przestępstw?

Bingo! Docierasz do informacji, że to bardzo popularne oszustwo, którego celem jest wyłudzenie danych z karty płatniczej, danych do logowania w serwisach bankowości internetowej a w konsekwencji można stracić wszystkie pieniądze, a nawet więcej. Inni piszą, że w ten sposób oszuści uzyskali dostęp do ich bankowości elektronicznej, dodali „urządzenie zaufane” przestępców lub utworzyli wirtualną kartę na telefonie – a wszystko to w wyniku ich lekkomyślności!

Zanim wykonasz jakikolwiek krok, szczególnie ten, który może zagrozić Twojemu bezpieczeństwu zatrzymaj się, weź 3 głębokie wdechy i:

- nie klikaj w linki w wiadomości SMS!
- przeczytaj bardzo uważnie treść komunikatu SMS, otrzymany z banku!
- nie przekazuj kodów otrzymanych od banków w wiadomościach SMS lub kodów BLIK!
- nie podawaj danych wrażliwych!
- obserwuj zamówiony towar wyłącznie za pomocą oficjalnej strony internetowej firmy kurierskiej lub jej aplikacji!

Ostrożność jest równie istotna, jak zakupy. Ostatecznie, unikasz przekazania danych wrażliwych, a przesyłki trafiają do Ciebie.

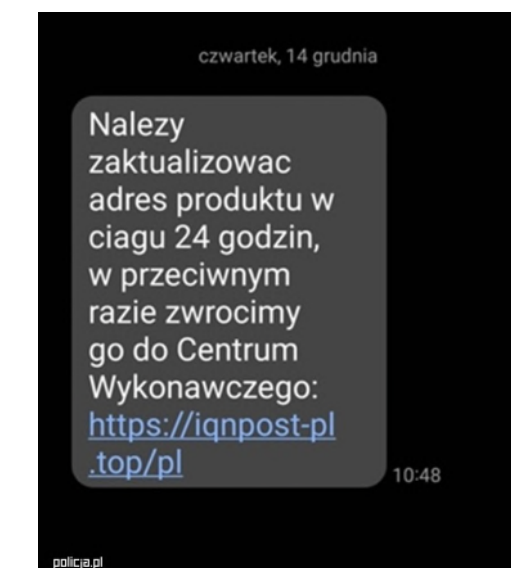
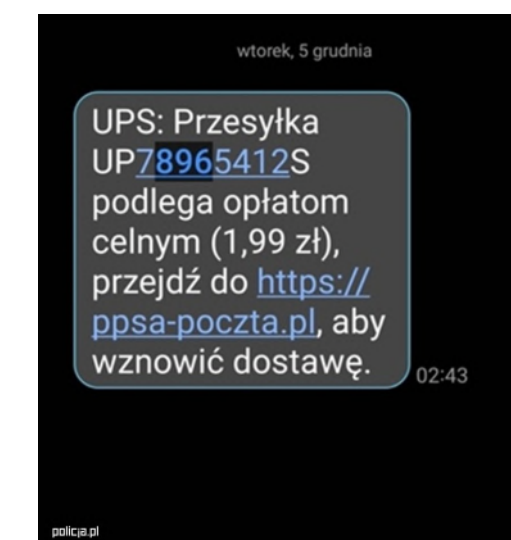
Jeśli padł(aś\eś) ofiarą przestępstwa, to w zależności od jego rodzaju natychmiast:

- skontaktuj się ze swoim bankiem,
- zmień hasło do swojej bankowości internetowej i aplikacji mobilnej;
- zastrzeż skompromitowaną kartę płatniczą – dzwoniąc na numer 828 828 828;
- złóż zawiadomienie o popełnieniu przestępstwa na policji lub w prokuraturze;
- zastrzeż skompromitowany dokument potwierdzający Twoją tożsamość i wystąp o wydanie nowego.

Komenda Główna Policji
oraz Centralne Biuro Zwalczenia Cyberprzestępczości FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP – Centrum Wymiany i Analiz Informacji Sektora Finansowego

Kampanie społeczne

zbp.pl / policja.pl



Uwierzyła fałszywemu policjantowi – straciła 42 tysiące złotych

6 września 2023 r.

Dolnośląscy policjanci wielokrotnie ostrzegali przed oszustami posługującymi się metodą między innymi na policjanta. Niestety jak pokazał wczorajszy dzień, nie wszystkie osoby zdają sobie sprawę z powyższego zagrożenia.

We wtorek, 5 września do Komisariatu Policji w Gryfowie Śląskim zgłosiła się 71-letnia kobieta, która została oszukana i straciła 42 tysiące złotych. Sposób działania przestępców był kolejny raz powielony i niestety kolejny raz skuteczny.

Starsza pani otrzymała telefon od mężczyzny podającego się za policjanta. Przedstawił się z imienia i nazwiska oraz podał swój stopień służbowy. Mężczyzna twierdził, że prowadzą policyjną akcję mającą na celu zatrzymanie sprawcy, który próbował włamać się na konto bankowe seniorki. Jej pieniądze nadal były zagrożone, nakazał udać się do placówki bankowej, wypłacić i przekazać pieniądze osobie, która po nie przyjdzie. Celem zweryfikowania autentyczności prowadzonej akcji mężczyzna powiedział, by kobieta na telefonie wybrała numer 112. Wówczas odezwał się inny mężczyzna, potwierdzając wiarygodność policjanta i całego zdarzenia.

71-latka udała się do banku, skąd wypłaciła 42 tysiące złotych. Po powrocie do domu przyszła do niej obca kobieta, której przekazała gotówkę. Jak obiecywał fałszywy policjant, pieniądze miała odzyskać 5 września. Niestety do tego nie doszło, a wtedy kobieta zdała sobie sprawę, że padła ofiarą oszusta.



Prawdziwe historie

policja.pl

Jak nie stać się ofiarą oszustów?

- Przede wszystkim należy zachować ostrożność.
- Prawdziwi policjanci NIGDY nie informują o prowadzonych przez siebie sprawach telefonicznie i nigdy nie proszą też o przekazanie pieniędzy nieznanemu osobie.
- Policjanci nigdy nie telefonują, że przyjdą lub wyślą kogoś innego do nas, aby odebrać pieniądze np. na pomoc dla syna.
- W takich sytuacjach możemy mieć pewność, że mamy do czynienia z oszustami.
- W szczególności pamiętajmy o tym, że w momencie, kiedy ktoś będzie chciał nas oszukać, podając się przez telefon, za policjanta – zakończmy rozmowę telefoniczną!
- Nie wdawajmy się w rozmowę z oszustem. Jeżeli nie wiemy, jak zareagować powiedzmy o podejrzanym telefonie komuś z bliskich. Kolejne połączenia telefoniczne wykonujemy z innego aparatu.
- Pamiętajmy o tym, że jeśli ktoś prosi o pieniądze przez telefon, to wtedy nie podejmujemy żadnych pochopnych działań.
- Nie informujemy nikogo telefonicznie o ilości pieniędzy, które mamy w domu lub jakie przechowujemy na koncie. Nie wypłacamy z banku wszystkich oszczędności.
- Zachowując spokój, zadzwońmy do kogoś z rodziny i zapytajmy o to czy osoba, która prosiła nas o pomoc, rzeczywiście jej potrzebuje.
- Pamiętajmy, że nikt nie będzie nam miał za złe tego, że zachowujemy się rozsądnie. Nie ulegajmy presji czasu wywieranej przez oszustów.

KWP we Wrocławiu

Oszukani na „lekarza z Jemenu”. Dzięki działaniom Policji i prokuratury nie stracili swoich pieniędzy

12 października 2023 r.

Oszuści nie mają żadnych skrupułów. Stosują różne metody i w różny sposób wpływają na nasze emocje, po ty, aby wyłudzić od nas pieniądze. Ofiarą oszusta internetowego padła 60-letnia mieszkanka powiatu złotoryjskiego i jej znajomy, od którego pożyczyła 35 tysięcy złotych. Kobieta w Internecie poznała osobę podającą się za polskiego lekarza pracującego na co dzień w Jemenie, państwie położonym na Półwyspie Arabskim. Dzięki pożyczonym pieniądzom miała opłacić i odebrać paczkę należącą do lekarza. Ja można się domyślić, okazało się, że kobieta padła ofiarą oszusta!

Do Komendy Powiatowej Policji w Złotoryi zgłosili się lokalni mieszkańcy, którzy poinformowali, że prawdopodobnie padli ofiarą oszusta. W rozmowie z funkcjonariuszami 60-latką oświadczyła, że za pośrednictwem portalu społecznościowego nawiązała kontakt z mężczyzną podającym się za polskiego lekarza, który przebywa w Jemenie. Miał on tam pomagać ludziom dotkniętym wojną. Relacja pomiędzy nimi utrzymywała się dość długo, a korespondowali za pośrednictwem komunikatora internetowego oraz poczty elektronicznej.

Po jakimś czasie mężczyzna poprosił kobietę o odbiór paczki w jego imieniu, w której miały się znajdować oszczędności i dokumenty. Paczkę miała dostarczyć firma kurierska, jednak konieczne było uiszczenie opłat celnych. W tym celu „lekarz” poprosił 60-latkę o przelew 35 tysięcy złotych. Kobieta nie posiadała tak dużej sumy pieniędzy, więc poprosiła o pożyczkę znajomego. 63-latek przelał tą kwotę na wskazane przez kobietę konto. Po kilku godzinach otrzymał informację z banku, że mógł paść ofiarą oszusta.

Natychmiast złożył reklamację w banku, po czym wspólnie ze znajomą zgłosili się do Komendy Powiatowej Policji w Złotoryi. Funkcjonariusze na podstawie przeprowadzonych ustaleń natychmiast wystąpili do prokuratury o wydanie postanowienia o blokadzie środków na rachunku bankowym. Dzięki błyskawicznym działaniom mężczyzna odzyskał całość kwoty. W tej sprawie policjanci będą prowadzili dalsze czynności.

Opisujemy tą historię, po to, aby przestrzec mieszkańców przed podobnymi sytuacjami. Pamiętajmy, że w przypadku oszustw internetowych bardzo ważny jest czas. Jeśli zorientowaliśmy się, że pieniądze zostały przesłane na konto oszusta możemy cofnąć operację bankową, pod warunkiem że nie została ona jeszcze zaksięgowana. W tym celu kontaktujemy się z bankiem. Jeśli na anulowanie zlecenia jest już za późno, to możemy złożyć reklamację w banku. Zgłaszając sprawę na Policji, funkcjonariusz także może zwrócić się do prokuratora o blokadę środków finansowych. Jednak w każdej z powyższych sytuacji liczy się czas, jaki upłynął od wpłaty pieniędzy.

Nawiązując kontakty na odległość zawsze kierujmy się zasadą ograniczonego zaufania. Nie dajmy się oszukać!

KWP we Wrocławiu / kc

Prawdziwe historie

policja.pl



Oszukany „na pracownika banku” stracił ponad 130 000 zł

21 grudnia 2023 r.

Oszust podszywając się pod pracownika banku wmówił 52-latkowi, że ktoś zaciągnął kredyt na jego rachunku. Wmówił również, że doszło do włamania na konto i zgromadzone tam oszczędności są zagrożone. Obiecał także pomóc w anulowaniu pożyczki. Nieświadomy oszustwa 52-latek za namową przestępcy w telefonie zainstalował aplikację do zdalnej obsługi urządzenia i przekazywał oszustowi otrzymywane z banku kody. Przestępcy szybko to wykorzystali i wyprowadzili z jego rachunku ponad 137 000 zł.



52-letni mieszkaniec powiatu zamojskiego odebrał połączenie. Telefonujący mężczyzna przedstawił się jako pracownik banku. Zapytał, czy 52-latek składał wniosek o kredyt. Kiedy zaprzeczył poinformował go, że doszło do włamania na konto i zgromadzone tam oszczędności są zagrożone. Zapewniał też, że zobowiązanie można anulować. W tym celu zalecił, aby zainstalować w telefonie platformę do wideokonferencji oraz aplikację do zdalnej obsługi urządzenia. 52-latek wykonał polecenia. Następnym krokiem do zabezpieczenia oszczędności miało być przekazywanie rozmówcy otrzymywanych z banku sms-ów z kodami. Nieświadomy oszustwa pokrzywdzony łącznie przekazał 17 takich kodów.

W tym czasie 52-latek miał zablokowany dostęp do rachunku i nie widział, jakie operacje są tam realizowane. Dopiero, kiedy żona wróciła do domu powiadomiła go, że na ich wspólnym rachunku realizowane są przelewy bankowe. Natychmiast pojechali do banku, aby anulować te transakcje. Niestety okazało się, że przestępcy wyprowadzając pieniądze z konta zlecali tak zwane szybkie wypłaty i nie można było już ich zablokować. Oszuści ze wspólnego konta 52-latka i jego żony wypłacili łącznie ponad 137 000 złotych. Sprawę pokrzywdzony zgłosił policjantom.

Oszuści dzwonią do potencjalnych pokrzywdzonych i fałszywie informują o podejrzanych przelewach, próbach włamań na konto, czy też zaciągniętych przez kogoś pożyczkach.

Wykorzystując strach posiadacza rachunku przed utratą oszczędności zalecają instalację programów do zdalnej obsługi urządzenia, zalecają też przekazywanie otrzymywanych kodów, które w rzeczywistości służą do potwierdzenia transakcji bankowych. W takich sytuacjach nie należy działać pochopnie. Każdą tego typu wiadomość trzeba wcześniej bardzo skrupulatnie sprawdzić. Najlepiej osobiście udać się do placówki banku i porozmawiać z prawdziwym bankowcem.

Aspirant sztabowy
Dorota Krukowska-Bubiło



NOWOCZESNE

ZARZĄDZANIE BIZNESEM

www.nzb.pl



Ponad
120
szkół wyższych



Ponad
390 000
studentów



Ponad
2 700
wykładów
(stacjonarnych oraz online)



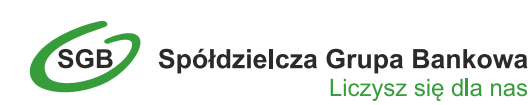
Blisko
430
konferencji



Ponad
600
stref edukacyjnych



Program współpracy szkół wyższych i sektora finansowego



System
DOKUMENTY
ZASTRZEŻONE

www.DokumentyZastrzezone.pl



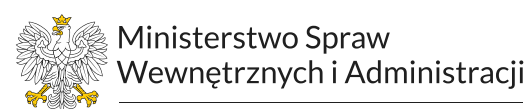
UTRACIŁEŚ DOKUMENTY?

Zastrzeż je w banku!

**NIE POZWÓL UKRAŚĆ
SWOJEJ TOŻSAMOŚCI!**

Kampania Informacyjna
Systemu **DOKUMENTY ZASTRZEŻONE**

Patronat honorowy



Patronat



Współpraca



Organizator



Patroni medialni



Partnerzy

