

BEZPIECZNY SENIOR

Głos SENIORA



NR 62 | ISSN 2299-6990 | www.glosseniara.pl

WYDANIE SPECJALNE – „STOP MANIPULACJI – NIE DAJ SIĘ OSZUKAĆ!”



OSZUSTWO NA WĘGIEL



OSZUSTWO NA WNUCZKA



ZASADY
CYBERBEZPIECZEŃSTWA



JAK SIĘ WYCOFAĆ
Z NIEKORZYSTNEJ
UMOWY?



STOP MANIPULACJI – NIE DAJ SIĘ OSZUKAĆ!

MANKO
STOWARZYSZENIE

KARTA SENIORA
OGÓLNOPOLSKA

GMINA PRZYJAZNA
Seniorom

MIRS
Międzynarodowy Instytut
Rozwoju Społecznego

AKTYWNI+
Projekt dofinansowany ze środków rządowego
programu wieloletniego na rzecz Osób Starszych
„Aktywni+” na lata 2021–2025
Edycja 2022

ADRES REDAKCJI

os. Urocz 12, 31-953 Kraków
Tel./faks 12 429 37 28
www.glosseniora.pl

REDAKTOR NACZELNY

Łukasz Salwarowski
salwarowski@manko.pl

REDAKTOR WYDANIA

Anna Kot
ogs@manko.pl,
konkurs@manko.pl

ZESPÓŁ REDAKCYJNY

Ewa Hołota
Anna Kot
Sylvia Krawczyk
Michał Majchrzak
Michał Białewicz
Marek Pilch
Ewelina Florczak

RADA PROGRAMOWA

Przewodniczący
– dr Krzysztof Czarnobilski

MARKETING

Michał Białewicz
marketing@manko.pl

PROMOCJA I PR

Ewa Hołota
programoks@manko.pl
Magdalena Mika
promocja@manko.pl
pr@manko.pl

PRENUMERATA

kontakt@manko.pl

GMINA PRZYJAZNA SENIOROM

Dorota Seweryn
gps@manko.pl
510 001 166

Agnieszka Nowak
kartaseniorka@manko.pl
519 127 178

SKŁAD GRAFICZNY

Sławomir Wolsza

NAKŁAD

30 tysięcy egzemplarzy

DRUK

INTROMAX Drukarnia
Offsetowa
Kraków, ul. Biskupińska 21

NA OKŁADCE: WIRGINIA WIKI SZMYT
– DJ WIKI

LISTOPAD 2022

SPIS TREŚCI**BEZPIECZNY SENIOR****Rodzaje oszustw:**

Phishing	4
Spoofing	5
Na fotowoltaikę	6
Na węgiel	7
Na 14 emeryturę	8
Na BLIK	9
Amerykański żołnierz mówi „Kocham Cię”	10
Na niezapłacone rachunki	11
Na telefon z zagranicy	12
Na fałszywe sklepy internetowe	13
Na firmy medyczne	14
Na kuriera, firmy kurierskie i paczkę	15
Na pomoc dla Ukrainy	16
Na spadek	17
Na nieistniejącego zwierzaka	18
Na wnuczka	19

Oszustwa w mediach społecznościowych	20
---	----

**PREZENTACJE
SPRZEDAŻOWE**

Tricki sprzedażowe	22
Techniki manipulacji	23
Czekamy na zmiany prawne!	24
Nie wynajmuj lokalu dla oszustów!	25

Jak nie ulec manipulacji na prezentacji sprzedażowej?	26
--	----

Jak się wycofać z niekorzystnej umowy?	27
---	----

Wzór odstąpienia od umowy zawartej na odległość	28
--	----

Wzór odstąpienia od umowy kredytu	29
--	----

**GMINA PRZYJAZNA
SENIOROM**

Zostań Gminą Przyjazną Seniorom!	30
--	----

**ZASADY
CYBERBEZPIECZEŃSTWA**



Szanowni Państwo

Oddajemy w Wasze ręce specjalne wydanie Głosu Seniora, poświęcone w całości bezpieczeństwu osób starszych i naszej kampanii „Bezpieczny Senior – Stop Manipulacji, Nie daj się oszukać!“. Jednym z najważniejszych obszarów naszej działalności jako Stowarzyszenia MANKO – Głosu Seniora jest edukacja w zakresie zdrowia, prawa i bezpieczeństwa osób starszych. Od 7 lat uświadamiamy i przestrzegamy Seniorów, chroniąc ich przed manipulacją i demaskując najnowsze techniki oszustw. W kwietniu 2022 roku zainaugurowaliśmy kolejną edycję kampanii **Bezpieczny Senior – STOP MANIPULACJI, NIE DAJ SIĘ OSZUKAĆ**, którą prowadzimy we współpracy z Ministerstwem Rodziny i Polityki Społecznej.

Według oficjalnych danych przestępcy, dzięki różnego rodzaju oszustwom, wyciągają z kont bankowych lub portfeli Seniorów ponad 100 milionów złotych rocznie. Dlatego edukacja osób starszych w obszarze bezpieczeństwa jest konieczna i wręcz obowiązkowa. Jako Stowarzyszenie MANKO - Głos Seniora działamy w kooperacji z organizacjami partnerskimi, naszymi ambasadorami, gminami, które przystąpiły do naszego programu Gmina Przyjazna Seniorom, a także z Urzędem Komunikacji Elektronicznej. Dzięki tej współpracy mamy aktualną wiedzę o najnowszych sposobach i modyfikacjach oszustw.

Nie od dziś wiadomo, że oszuści wykorzystują łatwość Seniorów na wielu płaszczyznach. Do tej pory wymyślili mnóstwo różnych modyfikacji technik manipulacyjnych jak: fałszywe strony internetowe, wiadomości SMS, e-mail, zbiórki pieniędzy, podejrzane linki, a także oszustwa na wnuczka, na fotowoltaikę, na 14 emeryturę, na BLIK, na spadek, na nieistniejącego zwierza,

na fałszywe sklepy internetowe, na telefon z zagranicy, na niezapłacone rachunki i wiele innych. I tę wiedzę chcemy i powinniśmy przekazywać Seniorom oraz ich rodzinom. Temu służy między innymi to specjalne wydanie Ogólnopolskiego Głosu Seniora (nr 62).

Kampania społeczna „Bezpieczny Senior – Stop manipulacji, Nie daj się oszukać” to także działania prewencyjne przed dokonywaniem zakupów w warunkach, które nie sprzyjają roważnemu podjęciu decyzji przez konsumentów. Goście zaproszeni na tego typu spotkania (pokazy, prezentacje, bezpłatne badania) nie są informowani o ich handlowym celu i bywają wprowadzani w błąd, co do właściwości produktów. W trakcie spotkań jest wywierana presja i nieetyczny nacisk na potencjalnych klientów. Klienci po zakupie nie otrzymują wszystkich dokumentów ani nie są informowani o swych prawach.

W związku z licznymi, powtarzającymi się przypadkami oszustw, których ofiarami stają się osoby starsze, samotnie mieszkające i łatwowiernie odnoszące się do nieznajomych, uświadamiamy oraz apelujemy o ostrożność i zdrowy rozsądek w kontaktach z potencjalnymi oszustami!

Każdy z Was może zostać ambasadorem naszej kampanii i edukować bliskich, znajomych i sąsiadów. Zapraszamy do współpracy!

Bądźcie z nami – Solidarni z Seniorami!

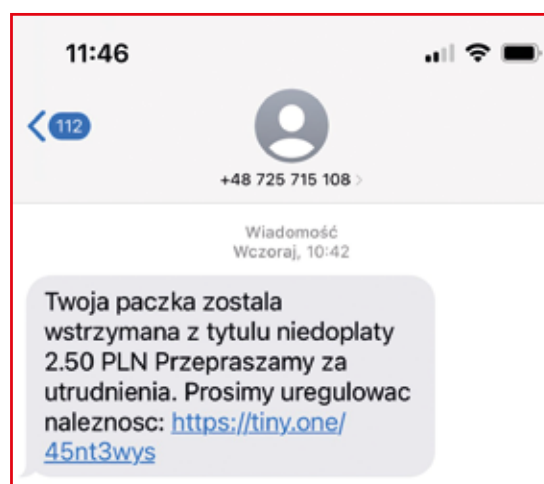

Łukasz Salwarowski

PHISHING

Phishing jest przebiegłą metodą oszustwa internetowego, za pośrednictwem którego przestępca podszycia się pod jakąś osobę lub instytucję. Phishing ma też inną nazwę: password harvesting fishing. To tzw. łowienie haseł, którego celem jest wykradanie numerów kart kredytowych, haseł do logowania oraz innych poufnych informacji za pośrednictwem różnego rodzaju

wiadomości e-mail może zawierać informację, że dana firma ma problemy prawne i trzeba kliknąć w link, aby uzyskać więcej informacji. Link ten przenosi ofiarę na stronę, na której należy wpisać wszystkie ważne dane dotyczące firmy, takie jak identyfikator podatkowy czy numery kont bankowych.

SMISHING – to rodzaj ataku wykorzystujący komunikatory tekstowe lub SMS-y. Popularną techniką smishingu jest wystanie na telefon komórkowy wiadomości SMS zawierającej linki do kliknięcia lub numer do oddzwonienia. Przykładem smishingu jest wiadomość SMS wyglądająca jakby została wysłana przez bank. Zawiera ona informację, że doszło do ataku na konto



technik. Najczęściej oszuści wysyłają swoje wiadomości na wszystkie adresy e-mail, jakie uda im się zdobyć. Treść wiadomości najczęściej informuje o tym, że doszło do włamania na konto i należy szybko zareagować, klikając na podany odnośnik, czyli link.

RODZAJE PHISHINGU

Wyróżnia się zarówno klasyczne ataki phishingowe z wykorzystaniem poczty elektronicznej czy wiadomości SMS, jak i bardziej wyszukane odmiany, takie jak: spear phishing, whaling, vishing czy smishing. Wszystkim przyświeca jednak jeden cel – **ukraść dane użytkownika**.

SPEAR PHISHING – to atak ukierunkowany na konkretną grupę osób lub typ osób, np. administratorów systemu firmy. Personalizacja wiadomości e-mail wywołuje u użytkownika wrażenie, że zna adresata – prywatną osobę bądź instytucję. Treść takich wiadomości odwołuje się do osobistych informacji czy wspólnego znajomego. Podszycanie się pod znajomych ma na celu np. wyłudzenie haseł.

WHALING – to jeszcze precyzyjniejszy rodzaj ataku phishingowego, ponieważ celem ataków są dyrektorzy generalni, dyrektorzy finansowi i wszyscy inni dyrektorzy w branży lub konkretnej firmie. Whalingowa

i trzeba natychmiast zadzwonić pod podany numer. Haker prosi o weryfikację numeru konta bankowego, SSN itd. Kiedy otrzyma te informacje, przejmuje kontrolę nad kontem bankowym.

VISHING – to kradzież wrażliwych danych osobowych lub firmowych. Ten rodzaj ataku jest przeprowadzany za pośrednictwem połączenia głosowego. Typowy atak vishingowy to telefon od osoby podającej się za przedstawiciela firmy np. Microsoft, który informuje, że na komputerze użytkownika wykryto wirus. Ofiara jest proszona o podanie danych karty kredytowej, aby oszust mógł zainstalować zaktualizowaną wersję programu antywirusowego na jego komputerze. Od tej pory haker posiada wszystkie dane karty kredytowej ofiary. A w dodatku – nakłonił ją do zainstalowania złośliwego oprogramowania na jej komputerze, które wykradnie np. dane dostępu do konta bankowego.

PAMIĘTAJ

Nie klikaj w podejrzaną linki. Sprawdzaj nagłówki wiadomości mailowych i adresy e-mail. Zanim wpiszesz swoje dane na stronie www, dokładnie sprawdź jej adres URL. Sprawdź czy adres nie zawiera np. dodatkowych liter czy cyfr.

SPOOFING

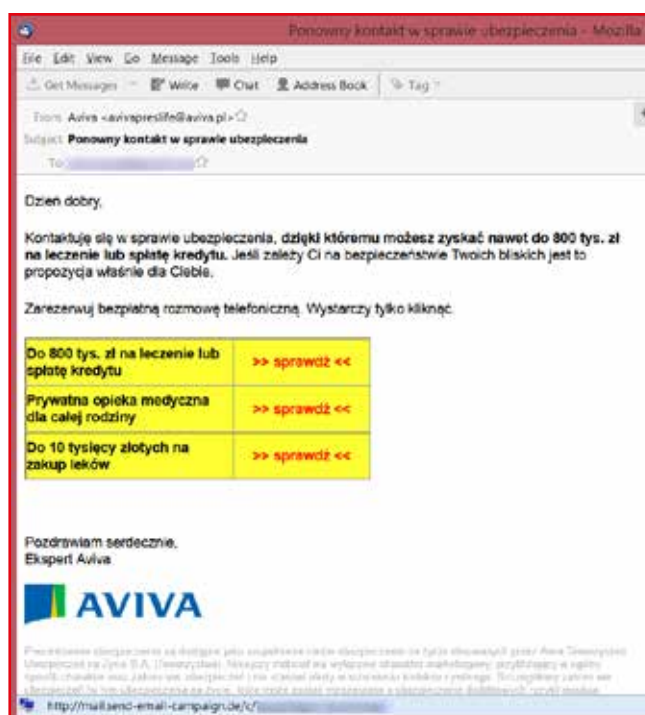
To rodzaj oszustwa, którego celem jest podszywanie się pod inne osoby lub podmioty czy instytucje w celu pozyskania danych wrażliwych oraz zainstalowanie szkodliwego oprogramowania na smartfonie lub komputerze ofiary. Ofiarami spoofingu są nie tylko osoby fizyczne, ale również firmy, których zasoby powinny być szczególnie chronione, bo na serwerach firmowych przechowywane są także dane klientów. W wyniku spoofingu poszkodowane są dwie osoby – oszukaną osobą lub firmą oraz podmiot, pod który podszył się oszust.

RODZAJE SPOOFINGU

Wyróżniamy kilka rodzajów spoofingu: e-mailowy, telefoniczny, przez aplikację czy spoofing URL.

SPOOFING E-MAIL

W tej metodzie przestępcy tworzą niemal identyczny adres mailowy, jaki ma dowolny adresat w Twojej skrzynce e-mail. Rozsyłają wiadomości e-mail imitujące te otrzymywane z zaufanych adresów – od banków, klientów czy współpracowników. Oszuści mogą zmienić wygląd nagłówków i adres wiadomości w taki sposób, że odbiorcy trudno będzie ją odróżnić od prawdziwej. Wiadomości zawierają zazwyczaj odnośniki lub linki do innych stron czy formularzy, które przenoszą użytkownika na zainfekowaną stronę.



SPOOFING TELEFONICZNY

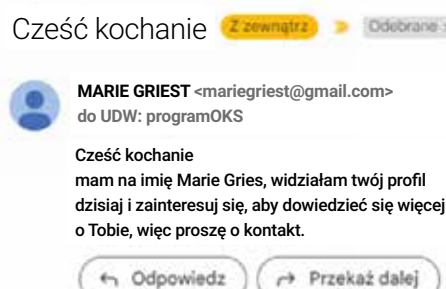
To metoda polegająca na podszyciu się pod wybrany numer telefonu, czyli wykorzystanie go jako własnego identyfikatora. W Internecie jest mnóstwo narzędzi, które w prosty sposób pozwalają wybrać połączenie na dowolny numer i wyświetlić na telefonie odbiorcy znany mu identyfikator – nazwę banku lub zaufanego kontaktu. Oszusta trudno jest namierzyć, bo może podszyć się pod bliską osobę, członka rodziny, przyjaciela lub – w warunkach biznesowych – naszego kontrahenta. Oszust może poprosić np. o wykonanie płatności lub przestanie poufnych danych.

SPOOFING PRZEZ APLIKACJE

Na spoofing przez aplikację narażone są osoby i firmy korzystające z portali ogłoszeniowych jak np. OLX. Aplikacje tego rodzaju nie mają zaprojektowanych procedur sprzedażowych, ograniczających kontakt obu stron transakcji. W celu sprzedaży produktów i usług konieczna jest zazwyczaj rozmowa w przygotowanym przez platformę komunikatorze. Dzięki temu przestępcy mogą w prosty sposób podszywać się pod inne osoby i firmy oraz rozsyłać zainfekowane linki, które wyłudzą dane lub instalują szkodliwe oprogramowanie.

SPOOFING URL

Oszust tworzy odpowiednik autentycznej strony internetowej (np. banku) i przesyła do niej link korzystając ze spoofingu mailowego lub SMS-owego.



Jeśli otworzysz link, będzie mógł wejść w posiadanie Twoich danych do logowania lub zainfekować Twój komputer.

PAMIĘTAJ

Bądź czujny i ostrożny podczas rozmowy telefonicznej. W przypadku jakichkolwiek wątpliwości skontaktuj się bezpośrednio z infolinią banku lub innej instytucji i zweryfikuj czy połączenie pochodziło od zaufanego źródła. Nie klikaj w podejrzane linki i sprawdzaj adresy URL, zanim wejdiesz na stronę www.

OSZUSTWO

NA FOTOWOLTAIKĘ

W związku z ogromnym zainteresowaniem fotowoltaiką pojawiają się też doniesienia o oszustwach, których ofiarami są osoby rozważające zakup paneli fotowoltaicznych. W dobie rozwoju odnawialnych źródeł energii na rynku można znaleźć przedsiębiorstwa, które doradzają i montują tego typu urządzenia. Niestety wśród rzetelnych firm mogą znaleźć się także nieuczciwe. Oszuści mogą próbować skłonić nas do zawarcia umowy, która przyniesie dla nas niekorzystne efekty lub zamontowania dużo większej instalacji umożliwiającej późniejszy montaż klimatyzacji czy elektrycznego źródła ogrzewania. Często to strata pieniędzy wpłaconych na poczet realizacji inwestycji, zaciągnięcie zobowiązania celem pokrycia kosztów zakupu, który nie zostanie zrealizowany, a także przekazanie danych osobowych, które mogą być wykorzystane dla przestępców.

NA CO POWINNIŚMY ZWRÓCIĆ UWAGĘ?

Naszą czujność powinna wzbudzić chęć szybko go podpisywania umowy, przewidziany błyskawiczny montaż instalacji oraz korzystniejsza oferta niż u innych wykonawców. Należy pamiętać, że wszystkie przestępstwa mają wspólny mianownik – pieniądze. Potencjalny klient jest narażony na niebezpieczeństwo polegające na wyłudzeniu znacznych kwot z przeznaczeniem na zaliczkę na poczet realizacji inwestycji, do której w efekcie może nie dojść. Oszuści najczęściej używają argumentów cenowych, aby zwabić potencjalną ofiarę i wzbudzić zaufanie. Pamiętajmy, że oferty znacznie tańsze od konkurencyjnych mogą, a nawet powinny wzbudzić podejrzenia. Zdarza się również, że wybrany wykonawca namawia nas do zaciągania kredytów lub pobiera wysokie zaliczki, po czym znika z pieniędzmi, nie realizując zleceń. Kolejną nieuczciwą praktyką jest proponowanie klientom us-

ługi w postaci płatnego audytu nieruchomości przed montażem paneli, podczas gdy takiej inspekcji dokonuje się nieodpłatnie.

JAK NIE DAĆ SIĘ OSZUKAĆ?

Przed podpisaniem umowy należy sprawdzić wiarygodność firmy i opinie na jej temat. Negatywne komentarze czy niekompletne informacje na stronie internetowej powinny wzbudzić naszą czujność. Warto pamiętać, że o wiarygodności przedsiębiorstwa w dużej mierze świadczą udane realizacje. Wykonawca powinien zapewniać kompleksową usługę, która zawiera wykonanie audytu, wybór najlepszych rozwiązań, zakup i dostarczenie niezbędnych elementów oraz montaż instalacji PV. Należy także zweryfikować czy firma montująca instalacje posiada certyfikaty potwierdzające kwalifikacje instalatorów OZE oraz polisę OC związaną z wykonywanymi usługami. Realizacja inwestycji fotowoltaicznej powinna także podlegać ubezpieczeniu, a wykonawca powinien udzielać gwarancji na swoje usługi.

PAMIĘTAJ

Stosuj teorię ograniczonego zaufania! Bez względu na to, jak korzystnie brzmi oferta w ustach konsultanta, zanim zdecydujesz się na podpisanie umowy, dokładnie prześwietl całą firmę. Poproś o pomoc dzieci, wnuki bądź znajomych.



OSZUSTWO

NA WĘGIEL

Przez sytuację społeczno-ekonomiczną na świecie, tani węgiel jest dziś najbardziej poszukiwanym towarem w Polsce. Wielu mieszkańców szuka jak najtańszego węgla na zimę, aby ogrzać swoje domy. Niestety chęć kupna opału wykorzystują oszuści, którzy oferują węgiel w bardzo korzystnej cenie i obiecują szybką dostawę. W rzeczywistości to naciągacze, którzy w nielegalny sposób wzbo- gacają się dzięki naszej łatwowier- ności i niewiedzy. Nie da się ukryć, że trudności z zakupem opału, jego wysokie ceny i długi czas oczeki- wania na dostawę stworzyły dobre warunki do oszukiwania metodą na węgiel. Z tego względu, coraz wię- cej osób daje się złapać na oferty fikcyjnych firm lub podszywanie się pod istniejące spółki.

JAK DZIAŁAJĄ OSZUŚCI?

Oszuści pobierają zaliczki za węgiel i nie wywiązują się z umo- wy. Kupujący w ogóle nie dostaje zamówionego surow- ca lub zamiast niego dostaje pomalowane na czarno kamienie. Wiele oszustw tego typu opiera się na tym samym schemacie. Ofara ma wpłacić zaliczkę za opał, a fikcyjna firma obiecuje dostarczenie pelletu, eko- groszku lub węgla po okazyjnej cenie, ale dopiero po wpłacie całej należności lub zaliczki. Niestety pomimo zapłaty – węgiel nie dociera do klienta. Ale na tym nie koniec – samo ogłoszenie lub strona internetowa oszu- stów, jak i ich numery telefonów kontaktowych, znikają po pewnym czasie. Może się też zdarzyć, że fałszywi sprzedawcy zastosują metodę bez zaliczki. W takiej sy- tuacji dowiemy się, że nasze zlecenie będzie zrealizo- wane w późniejszym terminie. Tym sposobem oszuści zachęcają nas do wpłaty zaliczki na wskazane konto. Kolejną metodą wykorzystywaną przez oszustów jest podszywanie się pod strony internetowe firm zajmu- jących się wydobywaniem lub sprzedażą opału. Oszuści, podszywając się pod spółki zajmujące się sprzedażą węgla lub innego źródła energii, starają się wyłudzić



dane do logowania np. do kont bankowych lub kont społecznościowych czy systemów biznesowych.

Nie bądźmy bezwzględnie ufni, że każde ogłoszenie jest prawdziwe i wiarygodne. Osoby zamieszczające ta- kie oferty robią to dla zysku, a gdy uda im się kogoś naciągnąć szybko urywają kontakt.

PAMIĘTAJ



Staraj się kupować u sprawdzonych i wiarygodnych sprze- dawców. Sprawdzaj autentyczność stron www oferujących sprzedaż opału. Uważaj na tanie oferty i atrakcyjne oka- zje – oszuści lubią kusić niską ceną. Zachowaj szczególną ostrożność przy składaniu zamówień na węgiel. Sprawdzaj wiarygodność sprzedawcy i firmy, którą reprezentuje. Przy odbiorze sprawdź produkt – uważaj na „farbowany wę- giel”. W miarę możliwości – płać przy odbiorze.

OSZUSTWO

NA 14 EMERYTURĘ

25 sierpnia na konta emerytów trafiły 14 emerytury, a oszuści nieustannie wymyślają nowe metody na wyłudzenie danych osobowych czy bankowych. Okazją do oszustwa stała się dla nich także wypłata dodatkowego świadczenia. W związku z rozpoczęciem wypłat – oszuści zaczęli podejmować próby wykorzystania tej sytuacji i oszukania seniorów. Pod pretekstem pomocy przy wypełnianiu wniosku – wyłudniają dane wrażliwe i pieniądze. Pamiętajmy, że oferta pomocy w wypełnieniu wniosku, żądanie danych osobowych lub bankowych powinna być sygnałem ostrzegawczym. Pracownicy ZUS nie składają telefonicznych, osobistych propozycji płatnego czy też darmowego wypełnienia wniosku o czternastą emeryturę. Nie proponują pomocy przy wypełnianiu wniosku. Nie odwiedzają emerytów i rencistów w ich domach. Seniorzy mogą spodziewać się takiej wizyty tylko w dwóch przypadkach, ale zawsze wcześniej są o niej informowani. W pierwszym przypadku – z okazji jubileuszu ukończenia 100 urodzin, w drugim – gdy ubiegają się np. o rentę z tytułu niezdolności do pracy, czy świadczenie uzupełniające dla osób niezdolnych do samodzielnej egzystencji, a ich stan zdrowia nie pozwala dotrzeć na badanie do placówki ZUS.

Zakład Ubezpieczeń Społecznych przypomina, że żeby otrzymać świadczenie, nie trzeba wypełniać żadnych dokumentów! Bo wypłata 14. emerytury odbywa się z automatu. Otrzymają ją każdy, kogo podstawowa emerytura lub renta nie przekracza 4188,44 zł brutto. „Czternasta emerytura będzie wypłacana z urzędu, czyli nie jest konieczne składanie żadnego wniosku w tym zakresie. Pragnę podkreślić to bardzo wyraźnie i uczulić na wszelkie próby oszustwa. Nikt nie ma prawa żądać od emerytów i rencistów wypełniania żadnych formularzy, wniosków, wysyłania żadnych smsów czy jakichkolwiek innych czynności” – powiedziała Minister Rodziny i Polityki Społecznej Marlena Małag.

JAK DZIAŁAJĄ OSZUŚCI?

Oszuści podają się za urzędników ZUS-u i wmawiają seniorom, że przyszedli pomóc w wypełnieniu formalności związanych z 14 emeryturą. A następnie okradają. Jest to nowy sposób oszustów na wykorzystanie łatwowierności seniorów.

PAMIĘTAJ

Nie trzeba składać żadnych wniosków, by otrzymać 14 emeryturę. Świadczenie jest wypłacane z urzędu. Ostrzegaj swoich bliskich seniorów przed oszustami. Pieniądze w ramach 14 emerytury są wypłacane razem z emeryturą lub rentą, tą samą drogą. Nie wpuszczaj do domu nieznajomych osób. Jeżeli są to osoby, podające się np. za pracowników ZUS-u, to jak najszybciej zadzwoń do najbliższej placówki zakładu i zapytaj o zgodność danych. Jeśli tożsamość takiej osoby budzi wątpliwości, to zawiadom Policję i najbliższą placówkę ZUS. Jeżeli ktokolwiek do nas zadzwoni i poprosi lub zażąda żebyśmy przekazali pieniądze komukolwiek lub je przelali – powinna nam się zapalić czerwona lampka! Już wtedy powinniśmy wiedzieć, że mamy do czynienia z oszustwem i że osoba, z którą rozmawiamy, to przestępca. W takiej sytuacji, kiedy już mamy podejrzenie, że rozmawiamy z przestępcą, powinniśmy się rozłączyć i jak najszybciej powiadomić o tym najbliższą jednostkę policji lub zadzwonić pod numer alarmowy 112.



OSZUSTWO

NA BLIK

BLIK to metoda płatności, dzięki której szybko i łatwo zapłacisz w sklepie i przez internet, a dodatkowo wpłacisz i wypłacisz gotówkę. Z BLIKiem możesz też natychmiastowo rozliczyć się ze znajomym, używając zaledwie jego numeru telefonu. Do płatności BLIKiem nie potrzebujesz karty płatniczej ani portfela. BLIK, choć jest bezpiecznym środkiem płatności, bardzo często zachęca oszustów do korzystania z niego w celu wyłudzenia pieniędzy. Oszustwo na BLIK polega na wyłudzeniu kodu do płatności, najczęściej z wykorzystaniem komunikatorów, bądź kont w serwisach społecznościowych. Z potencjalną ofiarą kontaktuje się cyberprzestępca i podszywając się pod członka rodziny lub znajomego prosi o pilną pożyczkę. Aby zrealizować swój cel namawia do wygenerowania kodu płatności telefonem, a następnie przestania go „znajomemu”.

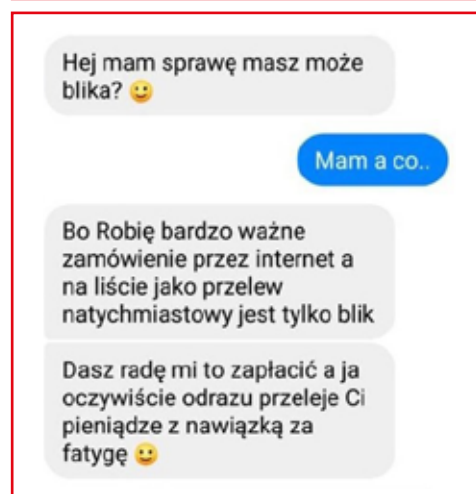
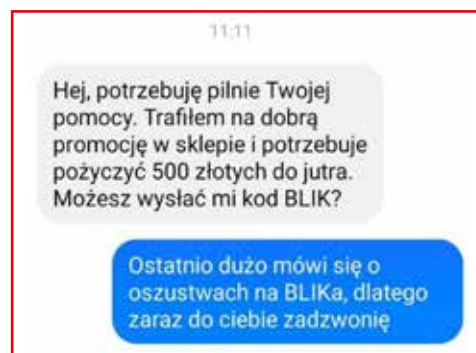
JAK DZIAŁAJĄ OSZUŚCI?

Jest kilka schematów działania oszustów.

NA POŻYCZKĘ – gdzie przestępca włamuje się na konto w mediach społecznościowych rodziny ofiary. Píše o potrzebie pilnej pożyczki na niewielką kwotę i wygenerowanie kodu BLIK. Pieniądże obiecuje zwrócić za kilka dni.

NA KRADZIEŻ LUB ZGUBIENIE PORTFELA – oszust kontaktuje się z ofiarą i przekonuje, że zgubił portfel lub został mu skradziony, a potrzebuje gotówki. Przekonuje, że sprawa jest pilna, bo musi za coś zapłacić. W takich okolicznościach trzeba działać szybko, a w grę wchodzi także emocje, dlatego ofiara nie weryfikuje tożsamości ani okoliczności osoby kontaktującej się z nią.

NA PRACOWNIKA BANKU – z ofiarą kontaktuje się oszust podający się za pracownika banku. W rozmowie telefonicznej informuje, że wykryto próbę zaciągnięcia zobowiązania na rachunek tej osoby. Aby potwierdzić tożsamość klienta, prosi o podanie informacji dotyczących stanu rachunku, wysokości zgromadzonych środków itd. Nieświadoma ofiara udziela wszystkich informacji. Następnie przestępca prosi o wygenerowanie kodu BLIK, który pomoże w zdemaskowaniu oszusta. Kod ten służy jej do pobrania pieniędzy z bankomatu.



ZAKUP NA OLX – ofiara wystawia na OLX produkt do sprzedaży i dostaje w aplikacji WhatsApp wiadomość od oszusta, który podszywa się pod potencjalnego klienta. Píše, że chciałby kupić produkt przez Paczkomat InPost. Ofiara odpisuje, że nie ma problemu i po chwili otrzymuje odpowiedź, że klient zaraz zapłaci. Po kilku minutach przychodzi SMS od InPost z linkiem do potwierdzenia. Ofiara kilka w odnośnik i przechodzi na stronę firmy kurierskiej. Aby otrzymać pieniądze, ofiara musi wpisać dane karty bankowej, na którą wpłyną środki. W kolejnym oknie pojawia się już tylko prośba o wpisanie kodu BLIK i potwierdzenie wypłaty.

PAMIĘTAJ



Kiedy ktoś prosi Cię o kod BLIK – nie działaj pochopnie. Najlepiej zadzwoń do tej osoby i upewnij się, że to właśnie ona go potrzebuje, a nie oszust. Zawsze sprawdzaj, komu

wysyłasz kody do płatności mobilnych. Nigdy nie przekazuj pieniędzy obcym osobom. Nie podawaj szczegółowych danych przez telefon, nawet kiedy bank rzekomo ich wymaga (pracownicy banku i tak mają je w systemie). Przed potwierdzeniem transakcji BLIK sprawdź kilka razy, ile wynosi kwota i do kogo ona trafi. Nie klikaj w linki otrzymywane od nieznanym numerów. Przed zalogowaniem się na konto w banku, dwa razy upewnij się, że adres strony jest właściwy.

OSZUSTWO

AMERYKAŃSKI ŻOŁNIERZ MÓWI „KOCHAM CIĘ”

Jedną z metod używanych przez przestępców jest oszustwo „na amerykańskiego żołnierza” lub weterana wojennego. Oszust wyszukuje w sieci samotne osoby i nawiązuje z nimi kontakt. Postępując się



zdjęciami z sieci, przedstawia się najczęściej jako amerykański żołnierz, który aktualnie jest na misji, poza granicami swojego kraju. Oszust poprzez regularny kontakt i przedstawienie fałszywych historii z życia zdobywa zaufanie ofiary, tworzy więź przyjaźni a nawet miłości, a następnie prosi o pomoc finansową na zakup biletu lub bardzo drogie leczenie. Gdy ofiara oszustwa prześle pieniądze na konto przestępcy, zostaje bez ukochanego i bez pieniędzy. Ostatnio pojawiły się także oszustki podające się za „lekarki z amerykańskiej armii”. Te z kolei wyłudzały pieniądze od samotnych mężczyzn.

JAK DZIAŁAJĄ OSZUŚCI?

Internetowi oszuści przedstawiają się jako amerykańscy żołnierze będący na misji lub jako weterani wojenni. Korespondują z kobietami, wzbudzają zaufanie, zaprzyjaźniają się, a następnie np. pod pretekstem chęci przyjazdu do Polski, wymyślają różne historie, z których wynika, że aby doszło do spotkania lub odebrania bardzo drogiej paczki, kobiety muszą wesprzeć finansowo „wojskowego” lub zapłacić za cło. Oczywiście, oszust zapewnia, że wszystkie koszty, jakie poniesie kobieta będą jej zwrócone i to z pokazną nawiązką. Oczywiście oszuści przedstawiają różne legendy. Począwszy od zablokowanych, z różnych przyczyn kont bankowych, poprzez opłatę celną za paczkę, która „utknęła” gdzieś na granicy. Warto podkreślić, że owe opłaty, sięgają kwot rzędu kilkunastu, a nawet kilkudziesięciu tysięcy złotych. Zmanipulowane kobiety wykonują bezmyślnie polecenia internetowego amanta, który podając przeróżne konta bankowe, zarejestrowane w różnych częściach świata, wyłudza w ten sposób znaczne sumy pieniędzy. Wiele kobiet aby pomóc „żołnierzowi” zaciąga kredyty bankowe. Oszuści zazwyczaj unikają rozmów telefonicznych i wskazywania miejsc, z których pochodzą. Ich konta na profilach społecznościowych nie zawierają żadnych informacji osobistych, zdjęć z rodziną, miejsca pracy czy zamieszkania. Poprzez regularny kontakt i przedstawianie fałszywych historii z życia – zdobywają zaufanie ofiary, a następnie proszą o pomoc finansową na zakup biletu lub na pokrycie opłat za przestanie paczki czy nagłej operacji.



PAMIĘTAJ

Zachowaj szczególną ostrożność w kontaktach z osobami poznanymi przez Internet – nigdy nie mamy pewności, kto znajduje się po drugiej stronie monitora. Bądź ostrożny, gdy poznana przez internet osoba prosi Cię o pieniądze. Nie ulegaj chwilowemu zauroczeniu czy presji czasu i nie przekazuj pieniędzy nieznanym osobom.

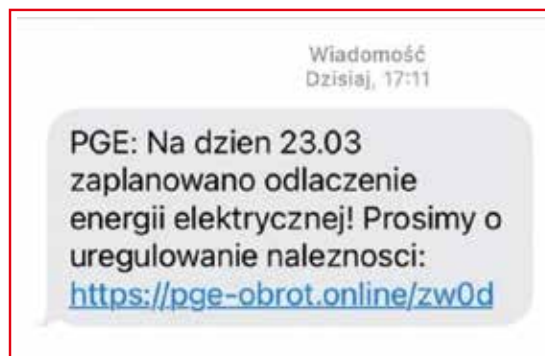
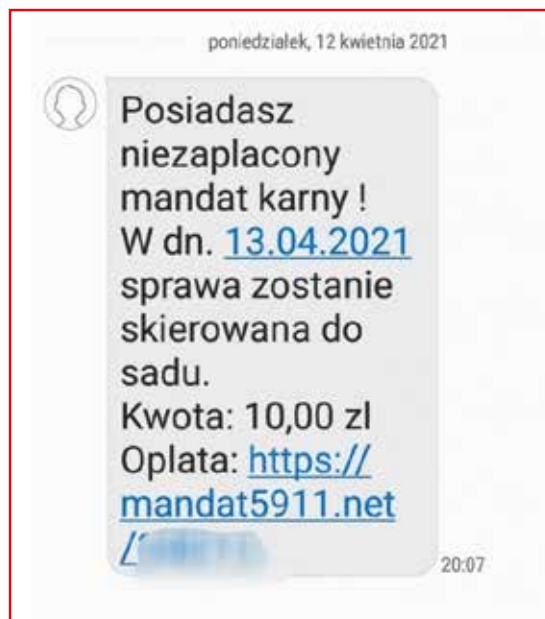
OSZUSTWO

NA NIEZAPŁACONE RACHUNKI

Oszuści nie próżnują. Cały czas wymyślają nowe metody, by wyciągnąć od nas pieniądze, ale też wracają do znanych sposobów np. pod pozorem odłączenia energii elektrycznej oczekują uregulowania należności. Fatszywe powiadomienia SMS zawierają także komunikat o możliwości opłacenia należności bezpośrednio poprzez link, szybki przelew lub BLIK. Na pierwszy rzut oka wszystko wygląda jak zwykła wiadomość tekstowa wysłana od dostawcy energii elektrycznej. Jej treść jest krótka, ale starannie przemyślana. Oszuści już dawno odkryli, że skuteczność ich ataków często zależy od samych ofiar i ich podatności na manipulację. Cyberprzestępcy bardzo chętnie sięgają po metody socjotechniczne, które bazują na wywoływaniu określonych emocji u odbiorcy – szczególnie silnego strachu. Ofiary widząc informację o nieopłaconych rachunkach mogą wpadać w panikę, że nie będą mogły oświetlić domu, umyć się czy ugotować obiadu. Kwoty, które rzekomo mają zapłacić, są zazwyczaj bardzo niskie. A to sprawia, że odbiorca chcąc mieć wszystko uregulowane, klika w niebezpieczny link i przez to nieświadomie infekuje swoje urządzenie złośliwym oprogramowaniem.

JAK DZIAŁAJĄ OSZUŚCI?

Oszuści podszywają się pod dostawców energii, gazu, wody itd. Wysyłają fatszywe wiadomości SMS z informacją o planowanym wyłączeniu prądu/wody/gazu w związku z rzekomo nieuregulowanymi płatnościami i linkiem do ich opłacenia. Nieświadoma i zaniepokojona ofiara klika w link, myśląc, że płaci za wodę/prąd/gaz. Wówczas – bez naszej wiedzy i zgody – może zostać zainstalowane na naszym telefonie złośliwe oprogramowanie, które może wykraść z naszego urządzenia takie informacje, jak dane logowania do bankowości mobilnej czy dane kart płatniczych.



W konsekwencji, oszuści mogą dostać się do naszych kont bankowych, wykraść pieniądze i nasze dane.

PAMIĘTAJ

Bądź ostrożny, nie daj się zwodzić na sprawdzone i wyszukane metody oszustów. Zachowaj czujność przy wszelkich transakcjach, z jakimi spotykasz się na co dzień i dbaj o swoje dane.

Nie otwieraj podejrzanych linków. Jeżeli nie jesteś pewien, kto jest nadawcą wiadomości – zweryfikuj to, zanim podejmiesz jakiegokolwiek działanie. Gdy otrzymasz podejrzaną wiadomość – jak najszybciej skontaktuj się z infolinią lub z prawdziwym nadawcą i wyjaśnij sprawę. Jeżeli jednak nie korzystasz z usług firmy, pod którą podszywają się oszuści, od razu usuń wiadomość.

Pamiętaj, że jeden błąd może Cię kosztować naprawdę dużo.

OSZUSTWO

NA TELEFON Z ZAGRANICY

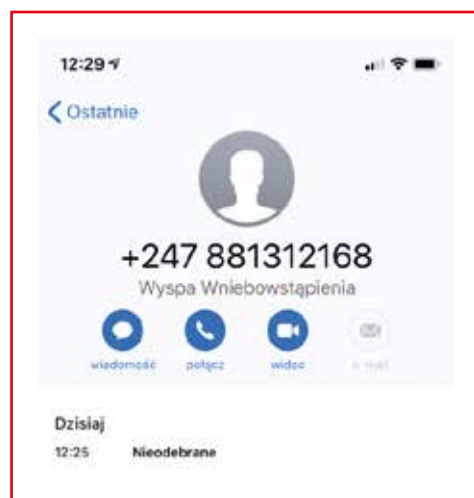


Zadzwonił do Ciebie nieznany numer? Uważaj! To mogą być oszuści z zagranicy. Odebranie lub oddzwonienie może kosztować kilka, a czasem nawet kilkadziesiąt tysięcy złotych. Nawet jeśli masz rodzinę za granicą i do siebie dzwonicie, musisz zachować ostrożność. Numer z zagranicy wyświetlony w aparacie telefonu jest bardzo długi, ale często początek może wyglądać na znajomy numer z Polski. Oszuści dobierają zagraniczne numery tak, aby udawały polskie prefiksy. Numery krajowe (komórkowe i stacjonarne) mają 9 cyfr w formacie XXX-XXX-XXX np.: 603-XXX-XXX lub 81Y-YYY-YYY (z prefiksem Polski +48 – 11 cyfr), natomiast numery zagraniczne są z reguły dłuższe, nawet 14 cyfrowe. Oszuści stosują dodatkowy podstęp. Gdy oddzwaniamy pod „podejrzany” numer, w słuchawce słyszymy różne dźwięki sugerujące wybieranie numeru i połączenia albo oczekiwanie na odebranie telefonu po drugiej stronie, a w rzeczywistości połączenie już trwa a kosztowne sekundy są naliczane.

JAK DZIAŁAJĄ OSZUŚCI?

Przestępcy zwykle dzwonią w nocy. Przychodzący numer najczęściej to tzw. „głuchy telefon” trwający bardzo krótko. Oszuści wykonują połączenia z numerów międzynarodowych na polskie numery w nadziei, że adresat tych połączeń automatycznie oddzwoni na numer, z którego połączenie zostało wykonane. W ten sposób wykorzystują naturalną skłonność abonentów do oddzwaniania na nieodebrane połączenia. Mechanizm działania oszustów opiera się przede wszystkim na nieuwadze użytkowników. Sprawcy liczą na to, że abonent oddzwoni, co kończy się dla niego naliczeniem wysokich opłat – jak za połączenie międzynarodowe. W sytuacji, kiedy oddzwonimy na taki numer usłyszy-

my sygnał rozłączenia. Warto pamiętać, że dopóki samemu się nie rozłączymy (nie naciśniemy symbolu czerwonej słuchawki), połączenie jest kontynuowane, a operator nalicza wysokie opłaty. Oszuści stosują dźwięk udający rozłączenie, przez co myślimy, że połączenie zostało zakończone. Odkładamy telefon, a czas połączenia międzynarodowego cały czas jest naliczany, nawet przez kilka godzin! W konsekwencji zapłacimy nawet kilkadziesiąt tysięcy złotych!



PAMIĘTAJ

Gdy zobaczysz, że dzwonił do Ciebie ktoś z nieznanego i długiego numeru – policz cyfry. Jeśli jest ich więcej niż 9 (11 cyfr z prefiksem +48) – nie oddzwaniaj i nie pisz SMS-a. Zignoruj takie połączenie. Jeśli nie spodziewasz się telefonu z zagranicy, a wyświetlony na Twoim telefonie numer jest zadziwiająco długi – po prostu nie odbieraj. Możesz też sprawdzić numer w internecie i włączyć u swojego operatora sieci komórkowej wszystkie blokady dotyczące podejrzanych połączeń.

OSZUSTWO NA FAŁSZYWE SKLEPY INTERNETOWE

Zakupy w sklepie internetowym można zrobić w każdym miejscu i w każdym czasie. Wystarczy dostęp do internetu. Również dla przestępców jest to kolejne miejsce, gdzie mogą wykorzystać roztargnienie, nieostrożność i pośpiech kupujących. Fałszywy sklep internetowy to nie tylko ryzyko kupna nieistniejącego produktu i strata pieniędzy. Za pośrednictwem fałszywej strony www przestępcy mogą wyczerpić nasze konto bankowe. Myślimy, że płacimy za produkt, a faktycznie udostępniamy przestępcom dane logowania do naszego konta bankowego. W ciągu miesiąca takich fałszywych sklepów może powstać nawet kilkaset. Zazwyczaj działają przez tydzień lub dwa i nagle znikają... wraz z naszymi pieniędzmi. Nigdy nie wysyłają opłaconego przez nas produktu. Banery reklamowe sklepów pojawiają się w mediach społecznościowych czy na ulubionych stronach. Kuszą niższymi cenami, specjalnymi kuponami rabatowymi i wyprzedażami. Oczywiście, nie wszystkie sklepy, które nęcą promocjami i zniżkami, będą próbowały nas naciągnąć. Jednak przed sfinalizowaniem zakupu warto sprawdzić kilka detali, aby mieć pewność, że wysyłamy pieniądze do wiarygodnego sklepu, a produkt na pewno do nas dotrze.

JAK DZIAŁAJĄ OSZUŚCI?

Najczęściej wszystko zaczyna się od linka w mediach społecznościowych, czy wiadomości SMS lub na komunikatorze. Dowiadujemy się tam o świetnej ofercie, której nie można przegapić. Innym razem trafiamy na reklamę sklepu na poczytnym portalu internetowym, czy na zaufanym blogu lub serwisie www. Pamiętajmy, że cyberprzestępca może wykupić reklamę swojego fałszywego sklepu praktycznie wszędzie. Fałszywe sklepy oferują najczęściej markowe produkty (np. sprzęt elektroniczny) w bardzo okazjowych cenach. Stosują przy tym sztuczki, które mają nas skłonić do szybkiego złożenia zamówienia, aby skorzystać z okazji.

Jak rozpoznać fałszywy sklep internetowy?

1. Zwróć uwagę na ceny. Jeżeli są podejrzanie niskie – nie daj się zwieść. Nie wierz w to, że ktoś da Ci coś za darmo albo za 30% ceny rynkowej.
2. Sprawdź informacje o sklepie. Jeżeli nie wiesz np. gdzie jest siedziba firmy – nie kupuj!
3. Nie decyduj się na zakup, jeżeli nie ma możliwości płatności przy odbiorze zamówienia (za pobraniem). Obecnie nie ma



praktycznego wytłumaczenia dla rezygnacji z tej formy płatności.

4. Kontakt ze sklepem jest słaby lub nie ma go wcale? Nie kupuj! Jeśli sklep długo odpowiada na wysyłane zapytania to także warto być ostrożnym.
5. Sprawdź, jak wygląda witryna sklepu internetowego – czy znajduje się na niej regulamin, polityka prywatności, a w nich informacja, kto jest właścicielem sklepu i administratorem danych osobowych. Brak takich dokumentów, albo trudności z ich odszukaniem na stronie to czerwona lampka ostrzegawcza!
6. Nie kupuj, jeżeli nie ma opinii i informacji o sklepie w internecie albo są same pozytywne komentarze, które pojawiły się w krótkim czasie.
7. Widzisz błędy i literówki? Nie kupuj! Fałszywe sklepy zakładają często przestępcy z zagranicy i korzystają przy tłumaczeniu np. z automatycznych translatorów. Takie praktyki powinny zwrócić Twoją uwagę.

PAMIĘTAJ

Zwróć uwagę na wszystkie szczegóły, które opisaliśmy powyżej. Zwłaszcza wtedy, gdy robisz zakupy w tym sklepie internetowym po raz pierwszy. Bądź ostrożny i nieufny podczas zakupów w sieci.

OSZUSTWO

NA FIRMY MEDYCZNE

Przedstawiciele firm medycznych oferują seniorom abonament medyczny, czyli szybki i łatwy dostęp do lekarzy i badań, ale za duże pieniądze. Seniorzy, którzy im uwierzą, a nie mają funduszy na pakiet – biorą kredyt. Po czym zostają bez lekarzy i z długami. Tak właśnie działa oszustwo na firmy medyczne. Nieuczciwe praktyki oparte są na obietnicach związanych z pakietami medycznymi i dostępem do lekarzy specjalistów. Seniorzy, którzy decydują się skorzystać z pozornie atrakcyjnej oferty leczenia, narażają się na poważne problemy finansowe.

JAK DZIAŁAJĄ OSZUŚCI?

Oszuści często obierają sobie za cel osoby starsze i samotne. Zaczyna się od telefonu z propozycją bezpłatnego badania, następnie jest rzeczowa rozmowa o stanie zdrowia, aż wreszcie – złożenie atrakcyjnej oferty pakietu medycznego z dostępem do wielu specjalistów i badań. Niekiedy uda się nawet umówić na kilka wizyt, ale potem firma znika. Wraz z naszymi pieniędzmi. Przestępcy, podszywający się pod przedstawicieli firmy medycznej, często wykorzystują zdenerwowanie klientów i podsuwają do podpisania umowy o pakiety medyczne, po czym udają się z nimi do pobliskiego banku, którego pracownicy „od ręki” udzielają wysokoprocentowych kredytów na pokrycie kosztów pakietu medycznego.

Koszty poszczególnych pakietów medycznych zazwyczaj wynoszą od kilku **do kilkunastu tysięcy złotych**. Fałszywa klinika posiada w swojej ofercie zakup pakietów medycznych z nielimitowanym dostępem do lekarzy specjalistów i badań. Przedstawiciele zatrudniają takie osoby, przy czym liczba zatrudnionych lekarzy, zakres ich specjalności oraz faktycznie realizowane usługi – nie odpowiadają tym określonym w pakietach i umowach. Przedstawiciele spółki niekiedy uruchamiają też call-center oraz za pomocą ulotek z zaproszeniem na bezpłatne badania – zachęcają seniorów do skorzystania z usług. Organizują też w salach konferencyjnych oraz w klubach seniora spotkania, których głównym celem jest zawieranie umów na usługi medyczne. Pozyskanemu w ten sposób klientowi klinika wykonuje powierzchowne badania diagnostyczne, po czym informuje o poważnym stanie zdrowia i konieczności natychmiastowego podjęcia leczenia, którego brak może być groźny dla życia i zdrowia. Z uwagi na oferowanie tego typu usług, liczba klientów spółki stale rośnie, a wraz z nią liczba poszkodowanych. Klienci dopiero w domu orientują się jaką umowę podpisali, w związku z czym większość z nich podej-



muje próbę odstąpienia od nich. Nie trudno się domyślić, że oświadczenia o odstąpieniu od umowy nie są uznawane, a klienci są zbywani lub ich wnioski są odrzucane w oparciu o opracowany wcześniej regulamin i szablon.



PAMIĘTAJ

Nie podejmuj decyzji pod wpływem impulsu. Czytaj dokładnie wszystkie dokumenty, które zamierzasz podpisać. Jeśli odebrałeś podejrzany telefon – zweryfikuj wiarygodność podanych informacji dotyczących oferty opieki medycznej. Pracownicy służb zdrowia nie dzwonią do potencjalnych pacjentów w celu umówienia na zabiegi bez wcześniejszego dostarczenia im skierowania na takie usługi medyczne.

OSZUSTWO

NA KURIERA, FIRMY KURIERSKIE I PACZKĘ

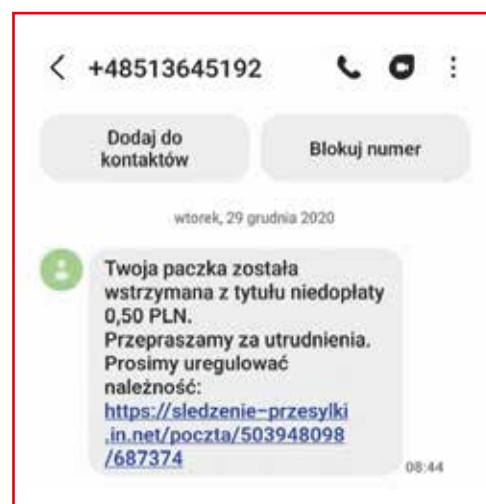
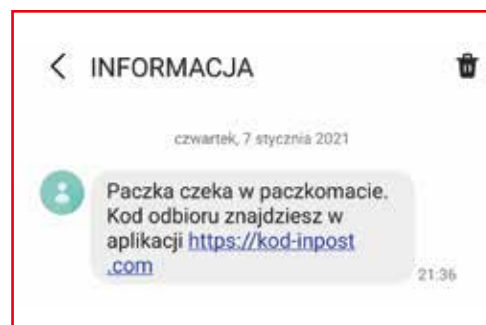
Oszuści ciągle modyfikują swoje metody działania i korzystają z każdej nadarzającej się okazji, aby wprowadzić w błąd i wykorzystać zaufanie nieświadomych osób. Coraz chętniej podszywają się pod firmy kurierskie i wysyłają SMS-y z informacją o konieczności dopłaty do przesyłki. Zazwyczaj kwota, jaką należy wpłacić, jest bardzo niska – w granicach 1 zł. W wiadomości podany jest także link, który przekierowuje potencjalną ofiarę na stronę łudząco podobną do strony banku bądź operatora płatności, gdzie nieświadoma osoba wprowadza wrażliwe dane dotyczące konta takie jak: login czy hasło i umożliwia tym samym przechwycenie tych danych przez oszustów. Warto dodać, że ten typ oszustwa często pojawia się w okresach świątecznych. A zatem wtedy, gdy składamy najczęściej zamówień.

JAK DZIAŁAJĄ OSZUŚCI?

Oszustwo na paczkę/kuriera/firmę kurierską w każdym przypadku wygląda podobnie, ale schematy działania są dwa.

Pierwszy scenariusz opiera się na masowym wysyłaniu grupie potencjalnych ofiar wiadomości SMS z informacją o nieudanej próbie dostarczenia paczki. W treści wiadomości SMS znajduje się link, który przekierowuje na stronę założoną przez oszustów. Jeśli ofiara faktycznie zamawiała paczkę to może łatwo złapać się na taką informację i kliknąć w przesłany przez przestępców link. Zwykle istnieje konieczność dopłacenia za przesyłkę. Jest to oczywista próba wyłudzenia wrażliwych danych, w tym loginu i hasła do logowania w bankowości internetowej. Przestępcy również wskazują na konieczność instalowania „aplikacji”, która w rzeczywistości jest złośliwym oprogramowaniem.

W drugim scenariuszu – kurier zjawia się u nas i informuje, że ma dla nas paczkę zamówioną za pobraniem. Najczęściej na koszt kilkuset złotych. Na paczce jest nasze imię, nazwisko i adres. Nadawcą jest firma „Y”, której nie znamy i od której nic nigdy nie zamawialiśmy. Pan, który dostarcza paczkę oświadcza, że jego zadaniem jest tylko dostarczenie paczki i pobranie pieniędzy, ale skoro mamy wątpliwości, można je wyjaśnić od ręki telefonicznie. Kurier pyta, czy może zadzwonić od nas do firmy i wyjaśnić sytuację. My wpuszczamy kuriera do domu i udostępniamy nasz telefon. Kieruje nami chęć jak najszybszego wyjaśnienia sprawy. Kurier dzwoni (przeważnie ok. 1 minuty) i niby sprawdza w firmie, czy nie zaistniała pomyłka. Informuje nas, że faktycznie jest to pomyłka, po czym przeprosza i wychodzi. Po miesiącu przychodzi rachunek telefoniczny nawet na kilkadziesiąt tysięcy złotych. Jak to możliwe? Kurier wykręcił numer telefonu stacjonarnego, który jest zainstalowany gdzieś w wynajętym mieszkaniu, najczęściej na fałszywą umowę. W tym właśnie mieszkaniu stoi małe niepozorne urządzenie, które natychmiast dokonuje przekierowań jak się tylko do niego dodzwonisz.



PAMIĘTAJ

Nigdy nie klikaj linków przesłanych w wiadomościach SMS. Szczególnie, gdy wzbudzają w Tobie chociaż cień wątpliwości. Nie instaluj nieznanych aplikacji na telefonie lub innym urządzeniu, za pomocą którego korzystasz z bankowości mobilnej. Nigdy nie podawaj haseł, PIN-ów ani kodów dostępu na stronach, do których link przyszedł w wiadomości SMS. Nie wykonuj transakcji, gdy cokolwiek wzbudza Twoje wątpliwości. Nie przyjmuj paczek od podejrzanych firm. Nie pozwalaj korzystać z telefonu nieznanym.

OSZUSTWO NA POMOC DLA UKRAINY

Ze względu na sytuację na Ukrainie w ostatnim czasie pojawiło się kilka nowych technik manipulacji i oszustw. Jak się okazuje, jest wiele osób chcących skorzystać na cierpieniu naszych wschodnich sąsiadów. Fałszywe strony internetowe organizacji charytatywnych i maile z prośbami o pomoc finansową to niektóre z metod, jakimi posługują się oszuści polujący na nieświadomych darczyńców. Emocjonalne wpisy, fałszywe apele o solidarność z narodem Ukrainy lub wezwania do pomocy w finansowaniu wysiłków obronnych służą oszustom do wyłudzenia pieniędzy.

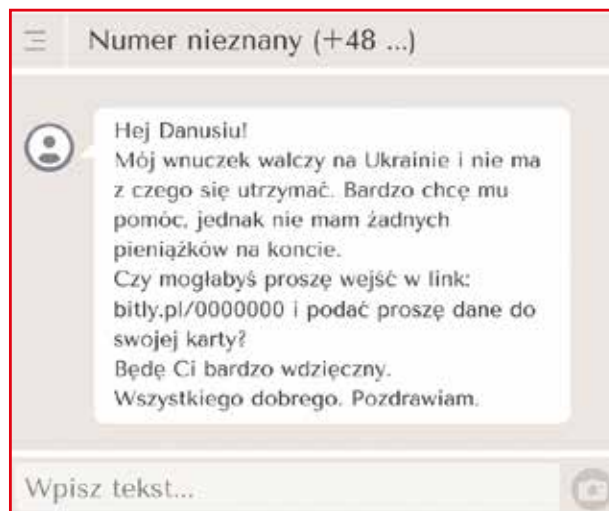
JAK DZIAŁAJĄ OSZUŚCI?

Jest kilka schematów według których działają oszuści wykorzystując sytuację w Ukrainie.

1. Oszuści wysyłają wiadomości SMS, mailowe lub w mediach społecznościowych od rzekomych ofiar wojny na Ukrainie, które zostały bez środków do życia. Proszą w nich o pomoc finansową. W wiadomościach najczęściej jest link, który po kliknięciu zamienia się w panel do logowania w mediach społecznościowych. Logując się, podajemy swoje dane przestępcom. W ten sposób cyberprzestępcy przejmują nasze konta.
2. Przestępcy przygotowują także fałszywe zbiórki, których celem jest kradzież pieniędzy z kont osób, które chcą pomóc. Na popu-

PAMIĘTAJ

Sprawdź dokładnie, zanim przekażesz środki organizacji charytatywnej – najlepiej wspierać znane organizacje, które posiadają historię pracy w terenie i współpracują z potwierdzonymi partnerami działającymi w Ukrainie. Pieniądze przekazuj za pośrednictwem oficjalnej strony internetowej organizacji lub zwróć się bezpośrednio do organizacji charytatywnej po wskazówki. Uważaj na prośby o przelew pieniędzy lub wysłanie kart podarunkowych. Organizacje charytatywne zwykle nie proszą o tego rodzaju „darowizny”. Nie klikaj w linki i nie pobieraj załączników w niechcianych wiadomościach e-mail lub wiadomościach z mediów społecznościowych, zwłaszcza z nieznanych źródeł i takich, które zwiększają poczucie niepokoju. Pamiętaj, że oszuści mogą próbować nakłonić Cię do nieświadomego pobrania złośliwego oprogramowania na Twoje urządzenie. Podchodź sceptycznie do postów w mediach społecznościowych, które promują organizację charytatywną, chyba że potwierdzisz, że organizacja jest legalna.



larnych komunikatorach lub serwisach wysyłają wiadomości z prośbą o dołączenie do zbiórki i wpłatę środków na rzecz pomocy Ukrainie.

3. Pojawiło się także wiele fałszywych postów z linkami, które kierują do filmów dotyczących inwazji na ukraińskie miasta. Po kliknięciu w link zostajemy przekierowani do strony przypominającej serwisu informacyjne. Jednak aby móc obejrzeć film – musimy się zalogować podając swoje dane. Takie konto może im posłużyć do dalszego rozpowszechniania fałszywych treści i kradzieży środków. W takiej sytuacji oszust podszywa się pod właściciela profilu i prosi znajomych o przekazanie mu funduszy.
4. Cyberoszuści mogą także dzwonić do ofiar i podawać się za policjantów, pracowników banku, przedstawicieli służb mundurowych czy urzędników działających na rzecz Ukrainy. Proponują zabezpieczenie naszego dobytku, które w obliczu toczącej się wojny na Ukrainie, może być zagrożone. Podczas rozmowy próbują wyłudzić dane i pieniądze.

OSZUSTWO

NA SPADEK

To wersja oszustwa nigeryjskiego oparta na długotrwałej grze psychologicznej. Ten rodzaj oszustwa zwykle ma postać oficjalnego e-maila lub listu od osoby podającej się za prawnika (czasami z zagranicy), w którym informuje się, że osoba, o takim samym nazwisku jak Ty umarła, a swój ogromny majątek w pozostawionym testamencie przekazała Tobie. Fortunę ofiara może podjąć w banku po dopełnieniu kilku formalności i opłaceniu różnych należności, które są niczym w porównaniu z olbrzymim spadkiem. Podobnie, jak w przypadku innych oszustw nigeryjskich, oszuści uwiarygodniają całą historię przesyłając pocztą elektroniczną spreparowane certyfikaty i kopie potwierdzeń przelewów.

JAK DZIAŁAJĄ OSZUŚCI?

Oszuści tworzą fikcyjne opowieści podając się np. za amerykańskich lekarzy czy żołnierzy stacjonujących w Syrii lub Iraku i proszą o odbiór paczki z dużą gotówką, po którą przyjadą do Polski. Ich historie opierają się również na odzyskaniu pieniędzy z zablokowanego konta uchodzący politycznego, wygraniu ogrom-

nej kwoty pieniędzy w jednej z loterii któregoś europejskiego kraju czy też dziedziczeniu ogromnej fortuny po zmarłym krewnym o którego istnieniu powiadomił pełnomocnik jego rodziny. Przestępca, który podaje się za pełnomocnika lub prawnika rodziny zmarłego, kontaktuje się z ofiarą najczęściej wykorzystując do tego pocztę elektroniczną. W korespondencji informuje potencjalną ofiarę, że jest jedynym żyjącym spadkobiercą dalekiego krewnego, który niedawno zmarł, a z uwagi na to, że nie pozostawił potomstwa, swój ogromny majątek w pozostawionym testamencie przepisał jednemu mu znanemu krewnemu, czyli wytypowanej już ofierze oszustwa. Oszuści mają na celu jak najdłuższe zwodzenie ofiary i wytudzenie jak największej kwoty pieniędzy. Ofiara zamiast zyskać fortunę, sukcesywnie traci coraz większe sumy, dopóki nie zorientuje się, iż padła ofiarą poczyniła oszusta.



PAMIĘTAJ

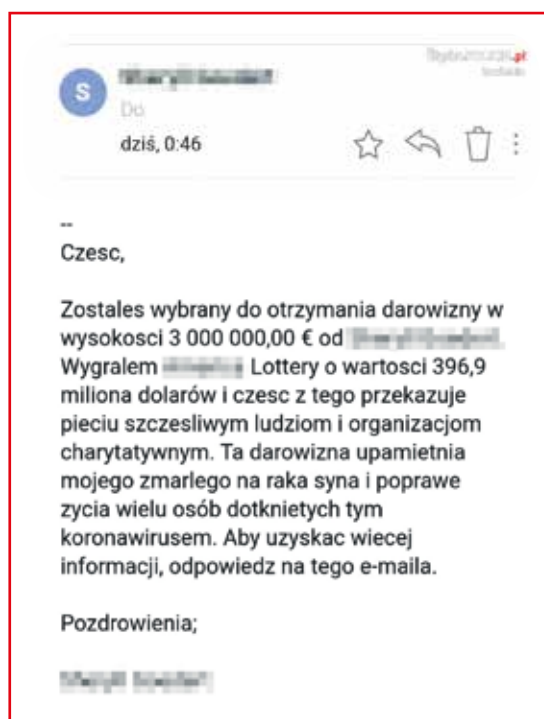


Jeżeli ktoś proponuje Ci dużą kwotę pieniędzy, bądź pewny, że to oszustwo. Nigdy nie udostępniaj wrażliwych danych, takich jak PESEL, czy skan dowodu osobistego, haseł do bankowości, PIN-ów. Jeśli ktoś za przekazanie nam jakiejś kwoty pieniędzy żąda opłat manipulacyjnych, powinno to wzbudzić nasze wątpliwości. Zachowaj szczególną ostrożność w kontaktach z osobami poznanymi przez Internet, zwłaszcza takimi, które proszą o pieniądze. Pamiętaj, że certyfikaty wystawiane przez różne instytucje, to dokumenty, które tak jak dokumenty identyfikacyjne, papiery wartościowe i banknoty, mają odpowiednie zabezpieczenia, takie jak hologramy, recto-verso, czy mikrodruk, które po wykonaniu skanowania (digitalizacji obrazu), tracą swoje właściwości, a tym samym przesłany nam skan certyfikatu nie ma żadnej wartości i wagi prawnej.

Jeżeli zostałeś wybrany na pomocnika w odzyskaniu pieniędzy przez uchodząc politycznego i za to masz otrzymać miliony dolarów – możesz być pewny, że to oszustwo.

Jeżeli zostałeś zwycięzcą zagranicznej loterii, w której nie brałeś udziału i nawet o niej nie słyszałeś, to śmiało możesz potraktować tą informację jako spam i od razu przekierować ją do kosza.

Jeżeli niespodziewanie otrzymasz wiadomość o milionach dolarów w spadku po krewnym, o którym nie miałeś pojęcia, to też więcej niż pewne, że to oszustwo.



OSZUSTWO

NA NIEISTNIEJĄCEGO ZWIERZAKA



Czy ogłoszenie oddania rasowego kota lub psa nie wzbudza podejrzeń? Czy ktoś mógłby oddać za darmo zwierzę, które może sprzedać nawet za kilka tysięcy złotych? Nie! Są jednak osoby, które się na to nabierają i przez swoją naiwność stają się ofiarą oszustwa. Zgodnie z artykułem 10a ust. 1 ustawy o ochronie zwierząt, zabrania się sprzedaży zwierząt domowych poza miejscami ich chowu lub hodowli, na przykład za pośrednictwem internetu. Dlatego często można trafić na ogłoszenia, w których zwierzęta są oferowane za darmo, a w trakcie konwersacji okazuje się, że jednak jakieś (zazwyczaj niemałe) koszty trzeba ponieść.

JAK DZIAŁAJĄ OSZUŚCI?

Schemat zazwyczaj jest taki sam. Przeglądasz ogłoszenia na jednym z portali ogłoszeniowych. Zdjęcie uroczego psa przykuwa Twoją uwagę wraz z informacją, że ktoś chce go oddać za darmo. Wydaje Ci się, że to świetna okazja, bo przecież taki pies kosztuje kilka tysięcy złotych. Nie zastawiając się długo – szybko piszesz wiadomość do sprzedawcy, bo wskazany numer jest zazwyczaj błędny. Następnie otrzymujesz odpowiedź z prośbą o przeniesienie konwersacji na ko-



munikator. Zgadzasz się i otrzymujesz kilka fotografii pieska i informacje, jaki jest wyjątkowy. Dopytujesz się więc, jak go możesz odebrać. Okazuje się, że właściciel wyjechał wraz z psem za granicę – ze względów zawodowych, i teraz nie ma się kto nim zajmować. Piesek potrzebuje troskliwej opieki i nowego domu, gdzie zazna miłości. Jesteś zdecydowany. Jedyne co musisz zrobić, to zapłacić 500 zł za usługi profesjonalnej agencji, która przywiezie Ci pieska do domu. Podajesz adres i przelewasz pieniądze. Następnie kontakt ze strony „sprzedającego” może się powtórzyć jeszcze kilka razy wraz z prośbą o dopłatę np. za przetłumaczenie dokumentów do przewozu zwierząt z zagranicy, albo za dodatkowe szczepienie. Zatem rachunek może być o wiele wyższy. Na tym koniec historii – kontakt ze sprzedającym się urywa, a Ty już wiesz, że padłeś ofiarą oszustwa.

PAMIĘTAJ

Nie licz na okazje! Nikt nie oddaje wartościowych rzeczy lub rasowych zwierząt za darmo! Nie łudź się, że ktoś pomylił numer telefonu. To specjalny zabieg, abyś nie mógł zadzwonić. Podczas korzystania z portali ogłoszeniowych kieruj się zasadą ograniczonego zaufania. Korespondencja powinna być prowadzona za pośrednictwem danego portalu i nie zaleca się nawiązywać kontaktu za pośrednictwem komunikatorów. Zwróć uwagę na pisownię w korespondencji. Jeżeli wygląda na tłumaczoną przez translator, możesz mieć obawy, że to oszustwo. Nie klikaj w zewnętrzne linki do płatności. Transakcja powinna być rozliczona w serwisie – o ile to możliwe. Unikaj bezpośrednich transakcji, szczególnie na zagraniczne rachunki. Jeśli zauważysz podejrzaną ogłoszenie – poinformuj serwis o naruszeniu, który powinien niezwłocznie usunąć takie ogłoszenie. Takie zachowanie pozwoli ustrzec inne osoby przed oszustwem. Internet to ogrom możliwości, ale również zagrożeń. Bądź świadomy – sprawdź, zastanów się i nie licz na niesamowite okazje! Pamiętaj – schroniska są pełne zwierzątek, które można przygarnąć zupełnie za darmo.

OSZUSTWO

NA WNUCZKA

Dla seniorów rodzina jest najważniejsza, dlatego oszustwa z nią związane są najpopularniejsze. Pomiędzy wielu kampanii społecznych i ostrzeżeń ze strony policji czy mediów, seniorzy wciąż dają się nabrać na „wnuczka”. Oszuści podszywają się pod kogoś zaufanego, np. członka rodziny. Cel jest jeden – wyłudzenie pieniędzy lub kradzież innych wartości, np. sprzętu, biżuterii, dokumentów. Oszust podszywający się pod kogoś bliskiego, mówi że miał wypadek i może trafić do więzienia. Jeśli jednak wpłaci mu kaucję w wysokości kilku lub kilkunastu tysięcy złotych to zostanie zwolniony. Bywa też, że oszust dzwoni do starszej osoby w imieniu rzekomego wnuczka lub innego członka rodziny i prosi o szybką pożyczkę.

JAK DZIAŁAJĄ OSZUŚCI?

Choć najczęściej używa się określenia na wnuczka, oszust może podszyć się pod innego członka rodziny lub bliskiego znajomego. Scenariusze zazwyczaj wyglądają podobnie. Upatrzona ofiara (zazwyczaj osoba starsza lub samotna) odbiera telefon wykonany od rzekomego członka rodziny. Rozmówca, zapytany o zmieniony głos, tłumaczy się przeziębieniem, zmęczeniem. Prawdopodobnie nawet nie

zna imienia osoby, pod którą się podszywa, dlatego nie przedstawia się („to ja, babciu”). Podczas rozmowy szybko porusza temat pożyczki. Chodzi o jak najszybsze dostarczenie mu pieniędzy. Jako powód najczęściej podaje:

- **ZADŁUŻENIE** – oszust mówi, że wziął pożyczkę, którą musi szybko spłacić, albo nie ma pieniędzy na ratę kredytu.
- **OKUP** – oszust podszywa się pod wnuczka lub syna i twierdzi, że został porwany i potrzebuje pieniędzy na okup.
- **WYPADEK** – złodziej opowiada historię o spowodowanym przez niego wypadku drogowym i mówi, że szybko potrzebuje pieniędzy, aby uniknąć konsekwencji, których domaga się ofiara.
- **INWESTYCJA** – rzekomy wnuk przekonuje, że pilnie potrzebuje określonej kwoty na inwestycję, która wkrótce się zwróci z ogromnym zyskiem.
- **OPERACJA** – podszywający się pod krewnego złodziej przekonuje, że musi poddać się poważnej operacji i natychmiast potrzebne są mu pieniądze na zabieg.

PAMIĘTAJ



Nigdy nie przekazuj pieniędzy osobom, których nie znasz. Nie ufaj osobom, które telefonicznie podają się za krewnych lub ich przyjaciół. Zawsze po otrzymaniu podobnego jak powyżej telefonu zadzwoń do wnuczka lub krewnego, żeby potwierdzić informację. Jeśli to możliwe – spotkaj się z nim. Jeśli nie rozpoznajesz głosu, odłóż słuchawkę – oszuści wywierają silny nacisk i presję, mają doświadczenie w manipulowaniu ludźmi, więc im szybciej zakończysz rozmowę, tym lepiej. Jeśli masz przekazać pieniądze komuś z rodziny, rób to tylko osobiście – bardzo charakterystyczne dla oszustw „na wnuczka” jest przysyłanie pośrednika, który ma odebrać pieniądze. Nie dawaj gotówki ani cennych rzeczy w ręce kogoś, kogo nie znasz. Odbierając telefon z prośbą o pieniądze nigdy nie mów ile masz gotówki i staraj się nie udzielać żadnych informacji osobistych. O całej sprawie powiadom Policję.



OSZUSTWA W MEDIACH SPOŁECZNOŚCIOWYCH

Dużo czytamy o oszustwach względem osób starszych, np. za pomocą metody na wnuczka. Wciąż jednak niewiele mówi się o wyłudzeniach za pomocą mediów społecznościowych. Warto mieć na uwadze, że oszuści, bez względu na wiek ofiar, próbują wyłudzić informacje i pieniądze. I niestety, w bardzo wielu przypadkach im się to udaje. Metod jest naprawdę sporo, jednak najpopularniejszymi są fałszywe profile i newsy na Facebook'u, konkursy w social mediach oraz akcja „Zobacz kto widział Twój profil”.

„ZOBACZ KTO WIDZIAŁ TWÓJ PROFIL”

Oszustwo ma na celu wyłudzenie poufnych danych. Prześiępca wysyła nam link do pobrania aplikacji, pod którą możesz zobaczyć kto podglądał Twój profil. Następnie poprzez aplikację zyskuję Twoje hasło i login do Facebook'a. A od tego już tylko krok np. od prób wyłudzenia pieniędzy od znajomych. **Zapamiętaj – nie ma możliwości sprawdzenia kto odwiedzał Twój profil na Facebook'u!**

FAŁSZYWE PROFILE, NEWSY NA FACEBOOK'U

SCAM to oszustwo, polegające na tworzeniu fałszywych informacji i profili na Facebook'u w celu wzbudzeniu czyjejś ciekawości w konkretnym celu, np. pozyskania danych lub wyłudzenia pieniędzy.

JAK ZIDENTYFIKOWAĆ SCAM POST?

Post posiada szokujący, intrygujący, absurdalny tytuł, a także zdjęcie, które ma zwrócić naszą uwagę. Taka notka posiada krótki komentarz typu „Nie wierzę”, „To niemożliwe”, „Zobacz sami!”, „To-

jest szokujące”, który ma podsyć naszą ciekawość. Oszuści w tym przypadku wykorzystują także autorytet – często nazwy ich stron są zbliżone do tych nam znanych np. centrum-wiadomosci24.pl, tvnnewsy24.pl, polsat24h.pl.

KONKURSY W SOCIAL MEDIACH

Konkursy to jeden z najpopularniejszych sposobów na wyłudzenia. Najczęściej możemy w nich wygrać smartfony, pieniądze, drogi sprzęt, wyjazdy za granicę i inne atrakcje. A jedyne, co musimy zrobić, to kliknąć w link i podać swoje dane osobowe. Ale to nie wszystko w tym temacie. Zdarza się również, że „wygrywając” coś, jesteśmy poproszeni o wniesienie stosownych opłat, np. na pokrycie podatku. Zdarza się też, że ofiary bardzo często otrzymują stosowny czek. Niestety, bez możliwości wypłacenia z niego funduszy.

PAMIĘTAJ

Zawsze bądź podejrzliwy względem osób poznanych w sieci. Zwłaszcza wtedy, gdy nie jesteś do końca pewny, kim dana osoba jest. Jeżeli nie jesteś pewny czystych intencji tej osoby – ogranicz z nią kontakt. Możesz również zgłosić się z tym problemem na Policję i szukać wsparcia wśród innych osób, które również zostały poddane próbie wyłudzeń. Pamiętaj – nie wszystko co widzimy w mediach społecznościowych jest dobre i nie wszyscy ludzie chcą dla nas dobrze. Warto oprzeć się pokusom, aby ewentualnie konsekwencje naszych złych decyzji nie ciągnęły się za nami długie lata. Dlatego za każdym razem, gdy zdecydujesz się np. na udział w jakimkolwiek konkursie – zapoznaj się najpierw z regulaminem. Jeżeli takowy nie istnieje – odpuść. Jest wówczas ogromna szansa na to, że dany konkurs nie jest legalny lub po prostu nie istnieje. A jedyne co możesz zyskać, to niepokój i wiele prób odzyskania pieniędzy.



PREZENTACJE SPRZEDAŻOWE



Każdego dnia w Polsce odbywa się kilkadziesiąt pokazów i prezentacji sprzedażowych, na których głównie osoby starsze są zachęcane do zakupu produktów wątpliwej jakości i pochodzenia po zawyżonych cenach oraz wprowadzane w błąd na temat ich rzekomego leczniczego działania. Sprzedaż ta odbywa się poza stałymi punktami sprzedaży detalicznej. Zazwyczaj ma miejsce w domu klienta, podczas prezentacji lub wycieczki zorganizowanej przez przedsiębiorcę. Pokazy organizowane są najczęściej w dobrych, ekskluzywnych hotelach, restauracjach lub sanatoriach.

SPOSOBY ZAPRASZANIA GOŚCI NA POKAZY I PREZENTACJE SPRZEDAŻOWE

- Telefoniczne/Telemarketing
- Zaproszenia wysyłane pocztą
- Ulotki informacyjne
- Ogłoszenia na klatkach schodowych

NA CO JESTEŚMY ZAPRASZANI?

- Darmowe badania (podczas których często zostaje ujawniony problem zdrowotny w rozwiązaniu którego ma pomóc oferowany przez sprzedawcę produkt)
- Bezpłatne konsultacje ze specjalistami
- Darmowy masaż
- Wykłady zdrowotne na temat zdrowego stylu życia, ekologicznego gotowania itp.
- Odbiór darmowego, „cennego” prezentu typu: ekspres do kawy, robot kuchenny, tablet, telewizor, żelazko, waga, grill, suszarka, wiertarka, ciśnieniomierz, pulsoksymetr. Zwykle są to jednak drobne upominki, które nijak mają się do tego, o czym był informowany klient. Można je odebrać na końcu trwającej często do 3-4 godzin prezentacji.

Zaproszeni goście nie są najczęściej informowani o handlowym celu spotkania. Na pokazach prezentowane są produkty mające ułatwiać funkcjonowanie w domu, pomóc w utrzymaniu dobrego zdrowia, a także wspomóc leczenie. Gości często wprowadza się w błąd, co do właściwości oferowanych produktów. Podczas spotkania często zakazuje się używania telefonów komórkowych.

PRZEBIEG PREZENTACJI

- Prezenter to przeważnie elegancka, miła, młoda osoba, która kojarzy się z dobrym wnuczkem lub amantem.
- Swobodna atmosfera, aby klient nie odniósł wrażenia, że cokolwiek będzie sprzedawane
- Każdy ma czuć się wyjątkowo i mieć świadomość, że uczestniczenie w spotkaniu jest okazją i wyróżnieniem
- Uśmiechy i komplementy w odpowiednich momentach
- Często osoba prowadząca podaje się za eksperta
- Prezentacje ilustrowane są filmami z wypowiedziami fachowców i znanych osób
- Często pokazuje się certyfikaty, mające potwierdzać wiarygodność produktu oraz jego wyjątkowość
- Brawa i oklaski zebranych sterowane przez ukrytych, podstawionych klientów.

DLACZEGO KUPUJEMY NA PREZENTACJACH?

Podczas prezentacji produktów stosowane są nieznane „zwyktemu” człowiekowi triki handlowe i techniki wywierania wpływu mające podnosić wartość oferowanych produktów i skutecznie przekonać nas do ich zakupu. Za ich pomocą sprzedawcy wywołują w nas potrzebę zakupu oferowanych produktów oraz przekonują nas, że zakup jest rozsądny i opłacalny, nawet jeżeli tak nie jest, a my tak naprawdę go nie potrzebujemy lub nas na niego nie stać.

PAMIĘTAJ

Jeżeli ktoś zaprasza Cię na prezentację – najlepiej odmów już na etapie rozmowy telefonicznej. Gdy ktoś zaprasza na pokaz, po odbiór nagrody lub na wręczenie kuponu powiedz, że nie jesteś zainteresowany i się rozłącz. Możesz także poprosić o usunięcie Twojego numeru telefonu z bazy danych. Jeżeli telemarketer dalej będzie Cię nękał telefonami, możesz powiedzieć, że zgłosisz sprawę na policję.

TRICKI SPRZEDAŻOWE

GRATIS

Do usługi lub produktu za określoną cenę dodawane jest coś za darmo. Ten gratis ma wywołać wrażenie dodatkowej atrakcji. Takie działanie obniża nasze wymagania co do produktu czy usługi i spora grupa ludzi jest skłonna skorzystać z takiej „okazji”, mimo drobnych wad produktu/usługi, które dostrzegła wcześniej.

UKRYTE KOSZTY

Najpierw jesteśmy zainteresowani towarem, a gdy osoba, której manipulacja dotyczy bezpośrednio, zdecyduje się na podpisanie umowy czy kupna towaru – manipulator zaczyna ujawniać ukryte, dodatkowe koszty. Skoro już wystarczająco ktoś „nakręcił się” na dany produkt lub usługę, to trudniej mu będzie z niej zrezygnować. Mimo ukrytych kosztów.

BEZINTERESOWNOŚĆ

Skuteczna metoda, w której ktoś bezinteresownie zachwala produkt np. jesteśmy w trakcie zakupów, a z boku odzywa się niby „przypadkowy przechodzień”, który w bezinteresowny sposób zachwala produkt. Kupujemy go nie wiedząc, że przechodzień jest podstawiony.

METODA „NISKA PIŁKA”

Manipulator przedstawia propozycję, która jest niesamowicie dla nas korzystna. Tuż przed realizacją okazuje się jednak, że nastąpiło nieporozumienie albo pomyłka – w konsekwencji towar lub usługa, o której mowa jest droższa.

WYTWORZENIE W ROZMÓWCY POCZUCIA WYJĄTKOWOŚCI

Przedstawienie konsumenta jako wybrańca losu znanymi i utartymi frazesami, jak: „Jest Pani wyjątkowa!”, „Jest Pani tego warta!”, „Wygrała Pani telewizor!”

METODA „DRZWIAMI W TWARZ”

Metoda polegająca na tym, że najpierw wysuwa się bardzo dużą prośbę, a po niej docelowo małą, na której zależy manipulatorowi, żeby została spełniona.



TECHNIKI MANIPULACJI

REGUŁA WZAJEMNOŚCI

Jeśli Ty zrobisz dla mnie coś dobrego, to ja także zrobię coś dobrego dla Ciebie. Jesteśmy kuszeni do przyścia na spotkania rzekomo bezpłatnym prezentem, poczęstunkiem czy badaniami. Podświadomie czujemy się zobowiązani i wdzięczni. A jak można się odwdziżyć? Spełnić prośbę i kupić coś od tej osoby, która nas zaprosiła. Niestety często się okazuje, że te rzeczy są nam zupełnie niepotrzebne. W dodatku – mają bardzo wysoką cenę.

SPOŁECZNY DOWÓD SŁUSZNOŚCI

Jeżeli inni ludzie zachowują się w dany sposób oznacza to, że jest on właściwy i przez to – ja również będę tak postępował. Kiedy podczas prezentacji sprzedażowej większość zgromadzonych osób potwierdza, że dany produkt się sprawdza i jest wart swojej ceny, to nie chcemy wyróżniać się z tłumu i mówić, że jest wręcz przeciwnie. Przecież wszyscy nie mogą się mylić. Tymczasem Ci, co polecają i przytakują, to najczęściej osoby zmanipulowane albo podstawione.

LUBIENIA I SYMPATII

Jeżeli Cię lubię, to chętnie spełnię Twoją prośbę. Prezenterzy zawsze częstują nas komplementami i nam schlebiają. Na prezentacjach dowiadujemy się np. że mamy na imię jak najukochańsza babcia, żona, siostra czy mama prowadzącego spotkanie. Należy być ostrożnym przy wszystkich próbach pochlebstw, bo miły i szarmancki nie znaczy uczciwy.

WPŁYWU AUTORYTETU

Jeżeli uważam Cię za autorytet, to chętniej spełnię Twoją prośbę. Dlatego prezenterzy często powołują się na opinie ekspertów, profesorów i doktorów. Doskonale wiedzą, że podczas prezentacji nie możesz tego sprawdzić i wykorzystują to. Innym przykładem są aktorzy w przebraniu lekarza lub matki 4 dzieci, która zna się na rzeczy.

NIEDOSTĘPNOŚCI

Inaczej decydowanie się tu i teraz. Taka okazja się nie powtórzy. Mamy tyle zamówień, że nie nadążamy z produkcją. Są zapisy i listy rezerwowe. Jeżeli coś jest rzadkie lub trudno osiągalne, to pewnie jest dobre. Najczęściej mija się to z prawdą. Ma nas to jedynie skusić do skorzystania z okazji, jaka już nigdy się nie powtórzy. Z tego powodu często nabieramy się na oferty „last minute”, limitowane edycje, artykuły kolekcjonerskie i trudno dostępne.

ZAANGAŻOWANIA I KONSEKWENCJI

Jeżeli zaangażowałem się w coś, to będę kontynuował to działanie, ponieważ chcę być postrzegany jako osoba konsekwentna i nie chcę stracić już zainwestowanego czasu, energii i pieniędzy. Dlatego bardzo często umowy są skonstruowane tak, aby rezygnacja oznaczała stratę tak dużą, że nie opłaca się z niej wycofać.



CZEKAMY NA ZMIANY PRAWNE!

Mimo naszych apeli, programów i działań nadal trwają oszukańcze prezentacje sprzedażowe. Oszuści w dalszym ciągu ukrywają handlowy cel spotkania, dzwonią do seniorów wbrew ich woli, zapraszają na spotkania i wabia ich z pozoru wartościowymi, darmowymi prezentami. A właściciele hoteli, restauracji, sanatoriów, domów kultury nadal wynajmują powierzchnie oszustom. Bo liczy się tylko chęć zysku kosztem starszych, schorowanych osób. Dlaczego nic się nie dzieje? Dlaczego seniorzy są narażani na takie niebezpieczeństwo? Czekamy na zmiany prawne! Czekamy na zdecydowane działania, aby zatrzymać ten proceder!

Co prawda, 26 maja 2022 roku został wprowadzony zakaz sprzedaży wyrobów medycznych poza lokalem przedsiębiorstwa, czyli między innymi na pokazach i prezentacjach sprzedażowych, ale to niewiele zmieniło. Czekamy na zmiany prawne, które wyeliminują między innymi możliwość wynajmu powierzchni na prezentacje, selekcję uczestników na początku spotkania, możliwość udzielania kredytów poza stacjonarną placówką bankową, zgłoszenie prezentacji 14 dni przed jej planowanym terminem do lokalnego Rzecznika Praw Konsumenta, nakaz rejestrowania video prezentacji i przechowywania zapisu przez okres 5 lat, nakazu ujawnienia w zaproszeniu handlowego celu spotkania oraz produktów, które będą sprzedawane, a tym samym wprowadzenie odpowiedzialności karnej za ukrywanie takiego celu, a także oferowanie produktów, których się potem nie otrzymuje.



STOWARZYSZENIE MANKO – GŁOS SENIORA APELUJE:

- o nie wynajmowanie powierzchni podejrzany i niesprawdzonym firmom na spotkania sprzedażowe. Narażenie na oszustwo osób starszych nie jest tego warte!
- o zakaz selekcji uczestników przed spotkaniem. Jedną z wielu nieuczciwych metod organizatorów jest wybranie jak najstarszych, najbardziej schorowanych, najmniej świadomych i z łatwością poddających się manipulacji osób. Bo właśnie takie najłatwiej oszukać!
- o wydłużenie do 30 dni terminu na odstąpienie od umowy dla transakcji zawartych podczas wycieczki lub nieumówionej wizyty przedsiębiorcy w domu konsumenta,
- o możliwość odstąpienia od umów o świadczenie usług zdrowotnych zawieranych poza lokalem przedsiębiorstwa lub na odległość. Chodzi o tzw. umowy obejmujące abonymenty medyczne,
- o zakaz udzielania kredytów/pożyczek poza stacjonarną placówką bankową np. na prezentacji czy wycieczce,
- o wprowadzenie obowiązku zgłoszenia prezentacji 14 dni przed jej planowanym terminem do lokalnego Rzecznika Praw Konsumenta i innych instytucji kontrolnych,
- o wprowadzenie nakazu rejestrowania video prezentacji i przechowywania zapisu przez okres 5 lat ,
- o wprowadzenie nakazu ujawnienia w zaproszeniu handlowego celu spotkania oraz produktów, które będą sprzedawane, a tym samym wprowadzenie odpowiedzialności karnej za ukrywanie handlowego celu spotkań,
- wprowadzenie odpowiedzialności karnej za oferowanie prezentów za samo przyjscie na spotkanie, których potem się nie otrzymuje. Są one tylko wabikiem, mającym skusić ofiarę do przyjscia na spotkanie.

NIE WYNAJMUJ LOKALU DLA OSZUSTÓW!

Jednym ze sposobów skutecznej manipulacji na słynnych oszukańczych spotkaniach sprzedażowych jest wynajęcie wiarygodnego miejsca na takie spotkanie! Oszuści organizujący pokazy często wynajmują lokal w wiarygodnym miejscu – w hotelu, restauracji, sanatorium, domu kultury czy na plebanii. Uwiarygadniają się w ten sposób przed zaproszonymi „gośćmi”. Zaproszeni liczą, że w tak poważnym miejscu nic im nie grozi, bo właściciel na pewno sprawdził tę firmę i na pewno nie wynająłby swojej powierzchni dla oszustów. Niestety często mija się to z prawdą!

Właściciel lokalu wynajmuje go każdemu, kto mu zapłaci i nic więcej go nie interesuje. Liczy się tylko zysk.

Dlatego od lat apelujemy do przedsiębiorców i samorządów – **NIE WYNAJMUJcie LOKALU PODEJRZANYM FIRMOM**, które mogą oszukać Waszych gości! Nie warto zarobić paręset złotych i pozwolić, aby w Twoim lokalu manipulowano i oszukiwano ludzi. Zostań partnerem kampanii i zdeklaruj, że jesteś przyjazny seniorom i tym samym nie wynajmujesz lokalu dla podejrzanych firm. Do naszej kampanii przystąpiło już kilkaset obiektów – hoteli, uzdrowisk i instytucji kultury. Dołącz do nas i edukuj, przestrzegaj innych! Są z nami między innymi hotele Gromada Centrum, Hotele Arche, Nadwiślańska Agencja Turystyczna, Gabinety Rehabilitacyjne Rudek, Uzdrowisko Busko-Zdrój, Uzdrowisko Ciechocinek, Uzdrowisko Nałęczów.



NA RZECZ BEZPIECZEŃSTWA SENIORÓW W POLSCE



- Ponad **300** warsztatów stacjonarnych, w których wzięło udział ponad **15 000** seniorów
- Ponad **30** warsztatów online, z których skorzystało ponad 100 000 Seniorów
- **15** konferencji prasowych, w wielu miejscach w Polsce
- Produkcja i emisja 3 spotów promocyjnych (dotarcie do ponad **2 milionów** Seniorów)
- Kilkadziesiąt audycji w mediach ogólnopolskich – TVP, Polsat, Radio Zet itd.



JAK NIE ULEC MANIPULACJI NA PREZENTACJI SPRZEDAŻOWEJ?

Liczy się przede wszystkim czas! Im szybciej podejmiesz działanie, tym lepiej dla Ciebie. Jeżeli jesteś osobą starszą – zwróć się o pomoc do swoich dzieci, wnuków, sąsiadów lub znajomych. Młodsze osoby pomogą Ci wybrać z sytuacji. Brak działania często oznacza trudne do przewidzenia konsekwencje!



PAMIĘTAJ!

- ➔ Nie ma niczego za darmo! Żadna firma nie działa charytatywnie!
- ➔ Pośpiech jest złym doradcą. Nie ulegaj pokusie prezentów i promocji. Nie podpisuj niczego bez spokojnego zastanowienia się nad zakupem! Daj sobie czas! Najlepiej nie podpisuj żadnych dokumentów, dopóki nie skonsultujesz się z bliskimi.
- ➔ Uważaj na hasła: bezpłatne badania, prezenty, gratisy, niepowtarzalne okazje. To tylko kuszące wabiki, które mają Cię skłonić do wyjścia z domu i udziału w pozornie atrakcyjnym spotkaniu. W rzeczywistości chodzi o prezentację oferty handlowej i skłonienie Cię do podpisania umowy kupna-sprzedaży produktów w horrendalnych cenach i na kredyty!
- ➔ Zanim coś kupisz i podpiszesz – poradź się kogoś bliskiego! Czy Twoje dzieci i znajomi również uważają, że produkt/usługa jest w dobrej cenie?
- ➔ Prezentowane produkty są często nawet kilkanaście razy droższe, od takich samych lub podobnej jakości, oferowanych w sklepach!
- ➔ Porównaj oferty. Poproś dzieci lub wnuki o sprawdzenie w internecie cen podobnych produktów oraz opinii o firmie organizującej pokaz.
- ➔ Przed zakupem sprzętu medycznego poproś o radę swojego lekarza rodzinnego.
- ➔ Przeczytaj uważnie warunki umowy, którą podpisujesz i zażądaj kopii każdego podpisanego przed siebie dokumentu.
- ➔ Nie podpisuj umów, których nie rozumiesz!
- ➔ Nie dawaj dowodu osobistego obcym!
- ➔ Bądź ostrożny. Często dzieci muszą spłacać kredyty rodziców. Tu chodzi o duże pieniądze!

JAK SIĘ WYCOFAĆ Z NIEKORZYSTNEJ UMOWY?

Kupiłeś garnki, pościel lub inne przedmioty na pokazie a teraz chcesz je zwrócić? Pamiętaj, że **masz do tego prawo w ciągu 14 dni!** Jeżeli dokonałeś zakupu na pokazie możesz odstąpić od umowy w terminie 14 dni kalendarzowych od odebrania towaru. Zakup produktów dokonany na prezentacji jest uznawany za **umowę zawartą poza lokalem przedsiębiorcy**. Dzieje się tak dlatego, że firmy organizujące pokazy wynajmują na ten cel lokale nie będące ich własnością np. sale w hotelach.

JAK ODSZTAĆ OD UMOWY?

- Aby odstąpić od umowy wystarczy, że złożysz sprzedawcy oświadczenie na piśmie. Taki formularz odstąpienia od umowy powinien Ci dostarczyć sprzedawca, ale możesz je także napisać samodzielnie (wzór znajduje się na końcu tego folderu).
- Do zachowania 14-dniowego terminu wystarczy wysłanie oświadczenia przed jego upływem.
- W przypadku odstąpienia od umowy sprzedawca nie może pobrać od Ciebie żadnych opłat z tym związanych.
- W ciągu kolejnych 14 dni po odstąpieniu od umowy musisz, na swój koszt, zwrócić sprzedawcy zakupiony towar.
- Sprzedawca powinien zwrócić Ci pieniądze za towar i koszt jego dostarczenia, nie później niż w ciągu 14 dni od dnia otrzymania oświadczenia o odstąpieniu od umowy. Może jednak się wstrzymać ze zwrotem należności do czasu, gdy otrzyma od Ciebie towar.
- W przypadku odstąpienia przez Ciebie od umowy zawartej poza lokalem przedsiębiorcy – taką umowę uważa się za niezawartą i jesteś zwolniony z wszelkich zobowiązań.
- Sprzedawca powinien zwrócić Ci pieniądze w takiej formie, jakiej Ty użyłeś przy zakupie, chyba że zgodziłeś się na inną formę zwrotu.
- Rozwiązanie umowy sprzedaży powoduje wygaśnięcie powiązanych z nią umów, np. umowy kredytu lub ubezpieczenia.

WAŻNE

Obowiązkiem sprzedawcy jest poinformowanie współpracujących z nim podmiotów o wygaśnięciu umowy. O prawie do odstąpienia od umowy sprzedawca powinien Cię poinformować. Jeżeli tego nie zrobił, możesz **odstąpić od umowy przez 12 miesięcy**. Jeśli jednak w ciągu tego roku sprzedawca przekaze Ci tę informację, od tego momentu masz na rezygnację tylko 14 dni.

PAMIĘTAJ

- Jeżeli podpisałeś umowę na zakup produktów na prezentacji, to **w ciągu 14 dni od jej zawarcia możesz z niej zrezygnować** bez podania przyczyny!
- Wyślij sprzedawcy **oświadczenie o odstąpieniu od umowy**. Taki formularz odstąpienia od umowy powinien dostarczyć sprzedawca. Wzór pisma znajdziesz również na końcu tego folderu.
- Poinformuj bank, że rezygnujesz z kredytu, jeśli był on częścią umowy, a towar kupiłeś na raty.
- Zwróć towar sprzedawcy. Pamiętaj, że **rozpakowanie i użycie produktu nie pozbawia Cię prawa do odstąpienia od umowy**. Możesz zrobić to osobiście lub wysłać pocztą na adres sprzedawcy.
- Korespondencję wysyłaj listami poleconymi za potwierdzeniem odbioru.



JEŻELI MASZ PROBLEM:

Skorzystaj z pomocy **Powiatowego Rzecznika Praw Konsumenta**.

Skorzystaj z pomocy prawnika. Dowiedz się, gdzie w Twojej okolicy znajdują się **Punkty Nieodpłatnej Pomocy Prawnej**.

Jeżeli w jakikolwiek sposób czujesz się zagrożony zaistniałą sytuacją, zgłoś problem **Policji** lub w **Prokuraturze**. Instytucje państwowe są po to, aby Ci pomóc!



Wzór 1

Miejscowość, data

.....

.....

.....

Imię i nazwisko konsumenta(-ów)

Adres konsumenta(-ów)

Nazwa i adres przedsiębiorcy

**Oświadczenie
o odstąpieniu od umowy zawartej na odległość
lub poza lokalem przedsiębiorstwa**

Ja/My (*).....niniejszym informuję/informujemy(*) o moim/naszym(*)
odstąpieniu od umowy sprzedaży następujących rzeczy(*)
umowy dostawy następujących rzeczy(*)
umowy o dzieło polegającej na wykonaniu następujących rzeczy/o świadczenie następującej
usługi(*).....

Data zawarcia umowy¹/odbioru²(*).....

.....

Podpis konsumenta(-ów)

(*) Niepotrzebne skreślić

¹ podać, jeżeli umowa dotyczyła świadczenia usług

² podać, jeżeli umowa dotyczyła zakupu towaru



Wzór 2

Data, miejscowość:.....

.....
Imię i Nazwisko

.....
Adres zamieszkania

.....
Numer PESEL

.....
Seria i numer dowodu osobistego

.....
Numer klienta

.....
Nazwa kredytodawcy

.....
Adres kredytodawcy

Odstąpienie od umowy kredytu

Oświadczam, że na podstawie art. 53 ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim (Dz. U. Nr 126 poz. 715 z późn. zm.) odstępuję od umowy kredytu o numerze..... zawartej dnia..... z firmą.....

.....
(czytelny podpis)

ZOSTAŃ GMINĄ PRZYJAZNĄ

Już 200 samorządów przyłączyło do Programu Gmina Przyjazna Seniorom i wydało lokalną edycję Ogólnopolskiej Karty Seniora w swojej gminie. Dzięki temu już ponad 550 000 seniorów może korzystać ze zniżek w ponad 3000 punktów w całej Polsce.

3000 punktów (uzdrowiska, ośrodki zdrowia, instytucje kultury i firmy usługowe). Zniżki, przy okazaniu Ogólnopolskiej Karty Seniora, sięgają od 10 - 50%, a na wyjeździe do sanatorium można zaoszczędzić nawet do 300 zł.

CZYM JEST OGÓLNOPOLSKA KARTA SENIORA?

Program Ogólnopolska Karta Seniora, którego organizatorem jest Stowarzyszenie MANKO – Głos Seniora, powstał z myślą o osobach starszych. Program ma na celu aktywizację oraz edukację seniorów z zakresu zdrowia, prawa, ekonomii i bezpieczeństwa. W całej Polsce już 550 000 seniorów posiada Ogólnopolską Kartę Seniora, a honoruje ją

KTO I W JAKI SPOSÓB MOŻE PRZYSTĄPIĆ DO PROGRAMU GMINA PRZYJAZNA SENIOROM?

Celem Programu jest wsparcie samorządu w rozwoju skutecznej polityki senioralnej – aktywizacji i edukacji seniorów z zakresu zdrowia, ekonomii, bezpieczeństwa czy nowych mediów. Każdy samorząd może dołączyć do Programu, wydać lokalną edycję Ogólnopolskiej Karty Seniora i otrzymać cer-

PARTNERZY PROGRAMU GMINA PRZYJAZNA SENIOROM



SENIOROM!

tyfikat Gminy Przyjaznej Seniorom. Warunkiem przystąpienia do Programu Gmina Przyjazna Seniorom jest m.in. wydanie lokalnej edycji Ogólnopolskiej Karty Seniora z herbem danej miejscowości oraz udział w naszych kampaniach m.in.: Stop Manipulacji - Nie daj się oszukać, Zażywaj leki bezpiecznie, Szkoła Przyjazna Seniorom, Poznaj swojego sąsiada seniora czy Stylowi Seniorzy. Projekt ma na celu również aktywizację lokalnych przedsiębiorców i seniorów, którzy współtworzą Program, poprzez pozyskiwanie nowych punktów honorujących Ogólnopolską Kartę Seniora oraz dystrybuowanie karty osobom niezrzeszonym i nieaktywnym.

PODPISZ DEKLARACJĘ I PRZYSTĄP DO KAMPANII „STOP MANIPULACJI, NIE DAJ SIĘ OSZUKAĆ!”

Jedną z kampanii realizowaną w partnerskim samorządzie w ramach Programu Gmina Przyjazna Seniorom jest kampania „Stop Manipulacji, nie daj się oszukać!”. Głównym jej celem jest edukacja w obszarze oszczędności, ekonomii, praw konsumenta, manipulacyjnych technik sprzedaży i bezpieczeństwa. Projekt skierowany jest do seniorów, samorządów i przedsiębiorców. Kampania zakłada edukację gmin, uzdrowisk i hoteli, aby nie wynajmowały powierzchni pod nieetyczne praktyki biznesowe i promowały bezpieczeństwo wśród swoich mieszkańców i gości. Aby przystąpić do kampanii, wystarczy odesłać skanem bądź pocztą wypełnioną deklarację udziału w kampanii. Jeśli Samorząd podejmie decyzję o dołączeniu do kampanii, otrzyma certyfikat partnerstwa, a informacja ta zostanie umieszczona na wszelkich nośnikach medialnych kampanii.

W celu uzyskania dodatkowych informacji prosimy o kontakt pod nr tel. 12 429 37 28 lub mailowo – kartaseniara@manko.pl.

PARTNERZY PROGRAMU GMINA PRZYJAZNA SENIOROM





ZASADY CYBERBEZPIECZEŃSTWA

1

Nie otwieraj załączników z niepewnych źródeł i nie klikaj w podejrzone linki.

2

Sprawdzaj dokładnie adresy stron www, a także ich certyfikaty.

3

Twórz skomplikowane hasła i trudne do odgadnięcia przez postronne osoby.

4

Nie używaj tego samego hasła do różnych kont oraz nie zapisuj haseł na kartkach ani w plikach na komputerze.

5

Nie podawaj i nie wysyłaj swoich loginów i haseł innym osobom.

6

Nie loguj się do bankowości elektronicznej podczas korzystania z publicznych, niezabezpieczonych sieci Wi-Fi.

7

Nie korzystaj z bankowości elektronicznej na urządzeniach publicznych np. w hotelach czy kafejkach.

8

Czytaj potwierdzenia SMS przed zatwierdzeniem transakcji płatniczej.

9

Regularnie aktualizuj system, aplikacje, przeglądarkę oraz oprogramowanie antywirusowe.

10

Nie podłączaj do swojego sprzętu zewnętrznych nośników danych typu Pendrive, co do których bezpieczeństwa nie masz pewności.

11

Stosuj się do ustalonych przez bank zasad bezpieczeństwa zamieszczonych na stronie. Jeśli coś odbiega od normy, to przerwijmy transakcję i skontaktujmy się z bankiem.

12

Kupuj tylko w takich sklepach internetowych, gdzie jest szyfrowane połączenie, czyli gdzie widzisz kłódkę i odpowiedni certyfikat.

13

Jeśli „bank” pyta Cię o hasła, czy też inne poufne dane, np. kod PIN do karty płatniczej – nie odpowiadaj! Na pewno nie jest to bank!

14

Skanuj od czasu do czasu swój komputer, szczególnie przed zalogowaniem się na stronę banku.

15

Zmieniaj regularnie hasła do swojego komputera, a także hasła dostępu do konta internetowego.

16

Cały czas bądź czujny i stosuj zasadę ograniczonego zaufania.

Numer karty:



MIRS
Międzynarodowy Instytut
Rozwoju Społecznego



KARTA SENIORA
OGÓLNOPOLSKA

FORMULARZ ZGŁOSZENIOWY DLA UCZESTNIKÓW PROGRAMU „OGÓLNOPOLSKA KARTA SENIORA”*

Proszę o przyjęcie mnie w poczet uczestników programu „Ogólnopolska Karta Seniora”. Oświadczam, że znane mi są postanowienia Regulaminu zamieszczonego na stronie www.glosseniora.pl. Jednocześnie zobowiązuję się do jego przestrzegania.

PROSZĘ WYPEŁNIĆ PISMEM DRUKOWANYM

Miejscowość:

Data:

d	d	m	m	r	r	r	r

DANE OSOBOWE

Imię (imiona):

Nazwisko:

Płeć: M:

☐

K:

☐
Miejscowość
urodzenia:
Data
urodzenia:

d	d	m	m	r	r	r	r

DANE KONTAKTOWE

Ulica:

Numer domu:

Numer
lokalu:

Miejscowość:

Kod pocztowy:

 -

Województwo:

Numer
telefonu:

stacjonarny:

☐

komórkowy:

☐

Adres e-mail:

Okres ważności karty:

1 rok – 35 zł
☐
2 lata – 50 zł
☐

OŚWIADCZENIE O WYRAŻENIU ZGODY

Oświadczam, iż wyrażam dobrowolną i wyraźną zgodę na przetwarzanie przez Administratora, tj. Międzynarodowy Instytut Rozwoju Społecznego sp. z o.o. (MIRS) z siedzibą przy ul. Siarczki 16, 30-698 Kraków moich danych osobowych

w celu otrzymywania od Międzynarodowego Instytutu Rozwoju Społecznego sp. z o.o. drogą elektroniczną na wskazany przeze mnie w Formularzu adres e-mail informacji handlowych, dotyczących usług oferowanych przez Międzynarodowy Instytut Rozwoju Społecznego sp. z o.o. oraz jego partnerów, np. wydarzeń organizowanych dla seniorów, informacji o partnerach MIRS-u honorujących Kartę Seniora i oferowanych przez nich zniżek w ramach Karty Seniora, w rozumieniu ustawy o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r.

☐ TAK

☐ NIE

w celu przekazywania przez Międzynarodowy Instytut Rozwoju Społecznego sp. z o.o. treści, dotyczących oferty MIRS-u na podany przeze mnie w Formularzu numer telefonu, w tym przy użyciu automatycznych systemów wywołujących w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

☐ TAK

☐ NIE

Jednocześnie oświadczam, że moja zgoda spełnia wszystkie warunki o których mowa w art. 7 RODO, tj. przysługuje mi możliwość jej wycofania w każdym czasie, zapytanie o zgodę zostało mi przedstawione w wyraźnej i zrozumiałej formie.

Zapoznałam/em się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych. Klauzula informacyjna dotycząca przetwarzania danych osobowych OGÓLNOPOLSKA KARTA SENIORA jest dołączona do niniejszego formularza, która jest również dostępna na stronie internetowej www.glosseniora.pl oraz zobowiązuję się do uiszczenia wyżej zaznaczonej kwoty gotówką lub przelewem na rachunek bankowy Międzynarodowego Instytutu Rozwoju Społecznego sp. z o.o. o numerze: 96 2490 0005 0000 4530 7190 0865 (Alior Bank)

.....
Data, podpis osoby zamawiającej Kartę Seniora

* WYPEŁNIONY PISMEM DRUKOWANYM FORMULARZ PROSIMY ODESŁAĆ POCZTĄ TRADYCYJNĄ WRAZ Z ZAŁĄCZONYM POTWIERDZENIEM PRZELEWU/PRZEKAZU NA ADRES REDAKCJI „GŁOS SENIORA” (os. Urocze 12, 31-953 KRAKÓW).

POZNAJ SWOJEGO SĄSIADA - SENIORA



Seniorze, chętnie Ci pomogę!

Zrobię zakupy, wykupię leki, wyprowadzę psa

IMIĘ

TELEFON

Pomóż nam szerzyć dobro i rozwieś plakat u siebie!
Możesz go pobrać ze strony www.glosseniara.pl/poznaj-sasiada

ORGANIZATORZY KAMPANII:



www.glosseniara.pl



www.adameddlaseniara.pl

ORGANIZATORZY KAMPANII



TRWAJĄCE KAMPANIE



PATRONI HONOROWI



WSPÓFINANSOWANIE



ZOSTAŃ AMBASADOREM KAMPAanii



Stowarzyszenie MANKO Międzynarodowy Instytut Rozwoju Społecznego

Os. Urocze 12, 31-953 Kraków

☎ tel. +48 12 429 37 28, +48 12 644 59 22

🌐 www.glosseniora.pl

🌐 niedajmysieoszukac.pl

📘 www.facebook.com/GlosSeniora

@ kontakt@manko.pl