BEZPIECZNY SENIOR

Głos SENIORA

KARTA SENIORA OGÓLNOPOLSKA

NR 74 | LISTOPAD 2024 | ISSN 2299-6990 | www.glosseniora.pl

WYDANIE SPECJALNE – FOLDER „STOP MANIPULACJI – NIE DAJ SIĘ OSZUKAĆ!"

POZNAJ ZASADY CYBERBEZPIECZEŃSTWA

JAK OSZUŚCI UŻYWAJĄ SZTUCZNEJ INTELIGENCJI?

AMERYKAŃSKI ŻOŁNIERZ MÓWI „KOCHAM CIĘ"

DRODZY SENIORZY, BĄDŹCIE CZUJNI

MAŁGORZATA SZEPTYCKA

KARTA SENIORA OGÓLNOPOLSKA

MIRS Międzynarodowy Instytut Rozwoju Społecznego

GMINA PRZYJAZNA Seniorom

AKTYWNI+

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

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

REDAKTOR NACZELNY
Łukasz Salwarowski
salwarowski@manko.pl

REDAKTOR WYDANIA
Justyna Śmiertka
ogs@manko.pl

ZESPÓŁ REDAKCYJNY
Ewa Hołota
Sylwia Krawczyk
Michał Majchrzak

WSPÓŁPRACA
Małgorzata Szeptycka
Małgorzata Miś
Natalia Gajecka
Michał Modro
Oliwia Gissel

RADA PROGRAMOWA
Przewodniczący
dr Krzysztof Czarnobilski

DYREKTOR BIURA
Ewa Hołota
programoks@manko.pl

MARKETING
Marcin Sołtys
firmyoks@manko.pl
marketing@manko.pl

PROMOCJA I PR
Szymon Kubik
promocja@manko.pl

PRENUMERATA
kontakt@manko.pl

GMINA PRZYJAZNA SENIOROM
Anna Gressel
gps@manko.pl, 507 634 147

Agnieszka Nowak
kartaseniora@manko.pl, 519 127 178

Aleksandra Dzik
gminaprzyjaznaseniorom@manko.pl

SKŁAD GRAFICZNY
Sławomir Wolsza

NAKŁAD
32 000 szt.

DRUK
INTROMAX Drukarnia Offsetowa
Kraków, ul. Biskupińska 21

FOT. NA OKŁADCE: GRZEGORZ GOŁĘBIOWSKI, TELEWIZJA PULS

www.glosseniora.pl

MIRS Międzynarodowy Instytut Rozwoju Społecznego

Głos Seniora
www.glosseniora.pl

SPIS TREŚCI

AKTYWNI+

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

Szanowni Państwo,

żyjemy w świecie, w którym Internet stał się nieodzownym elementem naszej codzienności. Oczywiście w sposób niemal nieograniczony korzystamy z jego dobrodziejstw: płacimy rachunki, robimy zakupy bez wychodzenia z domu, mamy dostęp do informacji z ostatniej chwili. Mimo tego do wszystkiego trzeba podchodzić z głową, ponieważ Internet niesie za sobą także wiele zagrożeń.

Z tego względu listopadowy numer jest specjalny, a wydaje go przedsiębiorstwo społeczne Międzynarodowy Instytut Rozwoju Społecznego we współpracy z Głosem Seniora – przy wsparciu finansowym pozyskanym z programu „Aktywni+". Został w całości poświęcony bezpieczeństwu osób starszych. W przeważającej części dotyczy oszustw internetowych, które stają się coraz popularniejsze w dobie rozwijającej się technologii i sztucznej inteligencji. Uwzględniliśmy wiele metod: spoofing, phishing, oszustwo na kody QR, kradzież tożsamości i haseł, oszustwo na kryptowaluty, oszustwa na inwestycje czy oszustwa na fałszywe opinie. Czy jest sposób na to, aby się przed nimi uchronić? Podstawa to przede wszystkim edukacja osób, które dopiero zapoznają się z nowoczesną technologią i uczą się korzystać z Internetu. Bezpieczeństwo seniorów w sieci to nie tylko świadomość dotycząca występowania coraz to nowszych sposobów na wyłudzanie danych i pieniędzy, ale także troska o higienę cyfrową – nieumiejętne korzystanie z Internetu może wyrobić wiele szkód zarówno materialnych, jak i tych powiązanych ze sferą psychiczną. Przekazywanie wiedzy o tym, jak nie zatracić się w wirtualnym świecie, jest celem najnowszej kampanii „Oderwij się od ekranu i żyj" organizowanej przez Stowarzyszenie MANKO i Fundację Tomorrow Offline.

W przypadku bezpiecznego korzystania z Internetu szczególną ostrożność należy zachować podczas zakupów, ponieważ zewsząd otaczają nas niezwykle korzystne rabaty i krzykliwe reklamy obiecujące szybkie korzyści i oszczędności. Takie informacje najczęściej odsyłają do sfałszowanych stron i formularzy – te z kolei prowadzą wprost w sidła oszustów. Cennymi uwagami na temat radzenia sobie z nieuczciwymi sprzedawcami podzielili się nasi eksperci, czyli adwokat Natalia Gajecka oraz członkowie Rady ds. Polityki Senioralnej przy minister ds. polityki senioralnej Marzenie Okle-Drewnowicz: radca prawny Michał Modro i prezes Stowarzyszenia Ochrony Konsumentów „Aquila", Małgorzata Miś.

Chociaż skupiliśmy się na bezpieczeństwie cyfrowym, nie oznacza to, że pominęliśmy tradycyjne sposoby oszukiwania seniorów, które wciąż z powodzeniem są wykorzystywane przez przestępców. Oszustwo na telefon z zagranicy, oszustwo na paczkę kurierską czy słynna metoda na wnuczka – dzięki sztucznej inteligencji stare metody zyskały drugie życie. Nie mogliśmy również pominąć oszukańczych prezentacji sprzedażowych. Warto sprawdzić, jak się przed nimi ustrzec.

Edukacja o bezpieczeństwie jest flagowym celem naszej kampanii „Stop manipulacji – nie daj się oszukać", którą prowadzimy już od 10 lat pod patronatem honorowym minister ds. polityki senioralnej Marzeny Okły-Drewnowicz i minister rodziny, pracy i polityki społecznej Agnieszki Dziemianowicz-Bąk. W ramach niej Stowarzyszenie MANKO przeprowadziło 40 konferencji i 400 warsztatów, wydało 4 foldery edukacyjne i nagrało 4 spoty wideo oraz 15 webinarów. Dzięki współpracy z Urzędem Komunikacji Elektronicznej, Małopolską Wojewódzką Radą Bezpieczeństwa Drogowego, Polskim Towarzystwem Opieki Farmaceutycznej, Fundacją SeniorApp, Stowarzyszeniem Ochrony Konsumentów „Aquila" i Fundacją Tomorrow Offline chcemy na bieżąco informować Was o szeroko pojętym bezpieczeństwie: cyfrowym, drogowym, lekowym i konsumenckim. Pamiętajcie jednak, że każdy z Was może zostać ambasadorem naszej kampanii, a tym samym edukować rodzinę, znajomych, sąsiadów czy członków swojej organizacji.

Zapraszamy do współpracy – chętnie przekażemy Wam materiały w wersji tradycyjnej i elektronicznej. Współpracujmy, bo razem można więcej. Solidarni z Seniorami – razem damy radę!

Łukasz Salwarowski

PARTNERZY

KAMPANIA „STOP MANIPULACJI – NIE DAJ SIĘ OSZUKAĆ”

Dlaczego edukowanie osób starszych i ich najbliższych w zakresie wszechobecnych oszustw i manipulacji powinno być jednym z priorytetów polskich władz i organizacji? Wystarczy przyjrzeć się przerażającym statystykom. Według danych Naukowej i Akademickiej Sieci tylko w samym 2023 roku cyberprzestępcy zajmujący się oszustwami telefonicznymi wyłudzili ponad 141 milionów złotych od 3500 seniorów. A doskonale wiemy, że metod jest o wiele więcej, tak więc i straty są bardziej dotkliwe. Dlatego od 10 lat Stowarzyszenie MANKO i Głos Seniora prowadzą kampanię „Stop manipulacji – nie daj się oszukać”, w ramach której przeprowadzono 40 konferencji i 400 warsztatów, wydano 4 foldery edukacyjne i nagrano 4 spoty wideo oraz 15 webinarów.

Niemal każdego dnia dochodzą do nas informacje o kolejnych ofiarach podstępnych oszustw i interwencjach służb. Na Śląsku mundurowi aresztowali grupę przestępczą, która okradła około 70 seniorów. Oszuści najpierw podawali się za pracowników Głównego Urzędu Statystycznego i pozyskiwali potrzebne dane osobowe, a także informacje na temat członków rodziny. Następnie metodą „na lekarza” przekonywali ofiary, że są zakażone koronawirusem i muszą pokryć koszty leku ratującego życie. Tym sposobem grupa wzbogaciła się o 2,5 miliona złotych.

We wrześniu małopolska policja zatrzymała 11 przestępców, którzy dokonali blisko 40 oszustw metodą „na legendę” w województwach: małopolskim, śląskim i podkarpackim na kwotę co najmniej 1,5 miliona złotych. Oszukany 73-latek z Nowej Huty zgłosił wyłudzenie 100 tysięcy złotych, dzięki czemu sukcesywnie przechwytywano kolejne osoby zamieszane w podstępne kradzieże.

W gminie Słubice starsze małżeństwo przekazało oszustom 40 tysięcy. Zadzwoniła do nich rzekoma córka, aby poinformować, że zostaje w szpitalu na noc. W międzyczasie wymusiła natychmiastową pożyczkę, a po pieniądze przyszedł nieznajomy mężczyzna. Małżeństwo w emocjach nie zauważyło, że ich prawdziwa córka podczas zajścia cały czas była w domu, na innym piętrze.

KAMPANIA „STOP MANIPULACJI – NIE DAJ SIĘ OSZUKAĆ” TO WAŻNA INICJATYWA

Kampania Stowarzyszenia MANKO jest odpowiedzią na bieżące problemy w zakresie bezpieczeństwa, z którymi borykają się osoby starsze. Jak widać, sposobów na oszustwa nie brakuje, a nawet ich przybywa – a to głównie za sprawą rozwijającej się technologii i sztucznej inteligencji, która zaskakuje możliwościami. Dzisiaj z łatwością można wygenerować zdjęcie lub film w ciągu kilku sekund, a poziom zaawansowania utrudnia rozpoznanie, co jest prawdą, a co wykreowaną (nie)rzeczywistością.

Kampania „Bezpieczny Senior. Stop manipulacji – nie daj się oszukać” organizowana pod patronatem minister ds. polityki senioralnej Marzeny Okły-Drewnowicz ma na celu przestrzeganie przed oszustwami, dlatego Stowarzyszenie MANKO organizuje konferencje i wystąpienia w całej Polsce. W tym roku byliśmy w: Muszynie, Krynicy, Łysomicach, Łodzi, Bieczu, Harmężach, Skawinie, Andrychowie, Tarnowie, Krynicy-Zdroju, Olsztynie, Gdańsku, Poznaniu, Cieszynie, Mikołowie, Gdowie, Wrocławiu i Sejmie Rzeczypospolitej Polskiej w Warszawie, by edukować najstarszych członków naszego społeczeństwa. W kampanię zaangażowane są również samorządy zrzeszone w programie „Gmina Przyjazna Seniorom”, firmy honorujące Ogólnopolską Kartę Seniora i Urząd Komunikacji Elektronicznej.

Nie zwalniamy tempa i już dziś zapraszamy kolejne podmioty do bycia partnerem lub ambasadorem kampanii „Stop manipulacji – nie daj się oszukać”. Wszelkie próby oszustwa prosimy zgłaszać na adres e-mail: **ogs@manko.pl**, na adres redakcji: os. Urocze 12, 31-953 Kraków lub pod numerem telefonu (12) 429 37 28.

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

NASZE DZIAŁANIA

Stowarzyszenie MANKO – Głos Seniora od 25 lat organizuje skuteczne kampanie i programy społeczne, które zyskały uznanie nie tylko w Polsce, ale także za granicą. Działania organizacji w znaczącym stopniu opierają się na edukacji i aktywizacji osób starszych, a także ich najbliższych. Przez lata zostaliśmy uhonorowani wieloma nagrodami i wyróżnieniami: Srebrnym Krzyżem Zasługi od Prezydenta Rzeczypospolitej Polskiej, Amicus Hominum i Kryształami Soli od Marszałka Województwa Małopolskiego, Złotymi Spinaczami, Białym Krukiem, Laurami Magellana, Medalem Obywatelskim oraz tytułami „Lider Wolontariatu", „Lider Zmian" i „Lodołamacz".

Stowarzyszenie MANKO obrało szczególny cel: zmiana świata na bardziej przyjazny seniorom. Nie bez powodu grupą docelową stali się najstarsi członkowie naszego społeczeństwa – według prognoz w ciągu najbliższych 25 lat udział osób powyżej 60 roku życia wzrośnie do 40%. Z powodzeniem więc nasza organizacja zajmuje się polityką senioralną od 2010 roku. W 2012 roku ukazał się pierwszy numer ogólnopolskiego magazynu Głos Seniora. Dzisiaj jest wydawany w nakładzie 35–40 tysięcy egzemplarzy.

Dzięki prężnemu rozwojowi i doświadczeniu nasi przedstawiciele zasiadają w Radzie Organizacji Pacjentów przy Rzeczniku Praw Pacjenta, Radzie Dostępności przy Ministerstwie Funduszy i Polityki Regionalnej, Radzie ds. Polityki Senioralnej przy Minister ds. Polityki Senioralnej w KPRM.

ZMIENIAMY ŚWIAT NA LEPSZY

Stowarzyszenie MANKO z sukcesem przeprowadziło kampanie: „Lokal bez papierosa", „Polska bez dymu", „Nie pal przy dziecku" i „Palenie jest słabe", które doprowadziły do wprowadzenia zakazu palenia tytoniu w miejscach publicznych, dzięki czemu zmniejszyła się liczba zgonów z powodu biernego palenia w Polsce. Następne przeprowadzone kampanie wiązały się z profilaktyką HIV/AIDS: „RyzyKochania" i „Przetestuj się"; pigułkami gwałtu: „Pilnuj drinka"; czy ekologią: „Eko-Segregacja". Warto wspomnieć również o obecnych inicjatywach, takich jak: „Zażywaj leki bezpiecznie", „Noś odblaski i żyj" oraz „Bezpieczny Senior. Stop manipulacji – nie daj się oszukać".

NIE TYLKO KARTA ZNIŻKOWA

Flagowym projektem grupy MANKO jest program „Ogólnopolska Karta Seniora" zrzeszający już ponad 620 tysięcy seniorów, 4 tysiące firm oraz 280 gmin, które stały się partnerami programu „Gmina Przyjazna Seniorom". Ogólnopolska Karta Seniora to jeden z najważniejszych długofalowych programów, dzięki któremu wspieramy polskich seniorów i promujemy firmy honorujące kartę. Upoważnia do zniżek w tysiącach punktów w całym kraju, ma również „moc" aktywizacji, gdyż wielu posiadaczy OKS dystrybuuje kartę do osób samotnych i niezrzeszonych, a także pozyskuje kolejne firmy do partnerstwa.

KORZYSTAJ Z ŻYCIA

Jako Stowarzyszenie MANKO organizujemy największą imprezę dla osób starszych w Europie. XI Międzynarodowe Senioralia w Krakowie zyskały rekordową frekwencję, w Parku Jordana zjawiło się bowiem 6 tysięcy seniorów z 115 miast i 7 państw. Idea aktywizacji kryje się również za licznymi konkursami Głosu Seniora, tj. „Stylowi seniorzy", „Senior działkowiec", „Zwierzak lekiem na samotność", „Miłość po 60-tce", „Podziel się swoją twórczością", „Patriotyczny Głos Seniora" oraz „Prześlij nam swój przepis".

Po więcej informacji zapraszamy na stronę **www.glosseniora.pl** i do kontaktu pod numerem 12 429 37 28.

DRODZY SENIORZY, BĄDŹCIE CZUJNI

Niemal codziennie gości na ekranach polskich telewizorów. Widzowie pokochali ją za rolę Beaty Barskiej w serialu „Lombard. Życie pod zastaw", za którą została nominowana w plebiscycie „Telekamery Tele Tygodnia" 2024 w kategorii „aktorka". Niedawno osiągnęła wiek emerytalny, ale nie zwalnia tempa. O swojej karierze, przepisie na dobrą kondycję i radach dotyczących bezpieczeństwa opowiedziała MAŁGORZATA SZEPTYCKA.

FOT. GRZEGORZ GOŁĘBIOWSKI, TELEWIZJA PULS

Kiedy zaczęła się Pani przygoda z aktorstwem?

Jak to najczęściej bywa, pierwszą osobą, która zauważyła mój potencjał, była moja mama. Któregoś dnia wróciła z pracy i oznajmiła, że zapisała mnie na balet do Wrocławskiego Teatrzyku Tańca Klasycznego „Arabeska". Może wpływ na moje wybory miały również geny. Mój stryjeczny dziadek Leon Niewiadomski był wybitnym przedwojennym artystą związanym przez długie lata z Operą Wileńską. Przez wiele lat występowałam z Akademickim Zespołem Pieśni i Tańca „Jedliniok". I pewnie zostałabym członkinią któregoś z reprezentacyjnych polskich zespołów pieśni i tańca, gdybym na swojej drodze nie spotkała pana Krzysztofa Kowalewskiego, który dostrzegł we mnie aktorski potencjał i nakłonił do złożenia egzaminów w Wyższej Szkole Teatralnej. I stało się – w 1983 roku rozpoczęłam studia w PWST we Wrocławiu.

Co w branży filmowej fascynuje Panią najbardziej?

Kocham swój zawód i wszystkie jego odsłony: teatr, film, lektorowanie oraz pracę edukacyjną jako nauczycielka aktorstwa i wymowy scenicznej. W każdej formie odnajduję coś wspaniałego i wartościowego. Film i serial dają mi poczucie misji. Codzienna obecność w domach widzów to ogromne zobowiązanie i odpowiedzialność za to, co proponujemy, za treści, jakie płyną z ekranu.

Niezwykle istotna jest dla mnie praca w teatrze. Od wielu lat jestem aktorką Wrocławskiego Teatru Komedia. Praca w tym miejscu to czysta przyjemność, ciągły rozwój i bezpośredni kontakt z publicznością. Wspomniałam również o pracy pedagoga. To kolejny aspekt mojej działalności artystycznej – kształcenie nowych kadr aktorskich. Dzielę się z młodzieżą swoimi doświadczeniami, umiejętnościami i wiedzą, oni zaś odwdzięczają się spontanicznością i „zarażają" mnie młodością.

Jako lektor od wielu lat nagrywam dla Grupy Radiowej Agora, Mikrofoniki czy Sound Media Studio. Uważam, że aktor, który z założenia musi wcielać się w różne postaci, powinien też być zawodowo wszechstronny, uniwersalny. Gdy nie ma propozycji ról filmowych, można skoncentrować się na nagraniach lektorskich, pracy edukacyjnej czy na teatrze. Z całego serca zapraszam do Wrocławskiego Teatru Komedia na wszystkie spektakle, ale szczególnie na naszą ostatnią premierę „Sex dla opornych". To piękna sztuka o dojrzałym małżeństwie dokonującym rozrachunku z przeszłością. Trochę zabawna, trochę wzruszająca i refleksyjna.

Jakie wydarzenie zawodowe lub prywatne miało na Panią szczególny wpływ?

Wydarzenie, które wpłynęło na każdy aspekt mojego życia, to udział w serialu „Lombard. Życie pod zastaw". Staliśmy się jedną wielką i wspierającą się rodziną, a serial jest w pewnym stopniu moim domem. To ogromna przyjemność być częścią tego projektu. Bywać w Państwa domach, rozweselać, radzić, wzruszać. Dzięki „Lombardowi..." spotkałam wielu wspania-

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

łych i szlachetnych ludzi, m.in. niezapomnianego Aleksandra Dobę czy panią Erin Dąbską, prezeskę Fundacji Telewizji Puls „Pod Dębem", która tak wiele robi dla seniorów, a przede wszystkim Zbigniewa Buczkowskiego (mojego serialowego małżonka) – wspaniałego aktora i niezawodnego kolegę.

Jaka jest Pani recepta na zdrowie fizyczne i psychiczne?

Któregoś dnia obliczyłam, że ponad trzy razy objechałam kulę ziemską na rowerze – i to nie elektrycznym! Ruch jest dla mnie podstawą zachowania dobrej kondycji fizycznej i psychicznej. To dawka endorfin, które mają zbawienny wpływ na naszą psychikę.

Między innymi poprzez rolę w serialu „Lombard. Życie pod zastaw" pomaga Pani edukować widzów na temat bezpieczeństwa. Dlaczego wzięła Pani udział w akcji #ZnamTeNumery?

Szczerze? Dopiero akcja #ZnamTeNumery uświadomiła mi rangę problemu. Goszcząc codziennie w domach naszych widzów, poczułam się w jakimś stopniu za nich odpowiedzialna – za ich spokój i bezpieczeństwo. Dzięki udziałowi w tej akcji mogę wyrazić również swoją wdzięczność.

Media często manipulują wizerunkiem znanych osób. Czy kiedykolwiek dziennikarze przekłamywali informacje na Pani temat? Jak Pani temu zaradziła?

Nie zdarzyła mi się taka sytuacja. Pilnuję tego, żeby każdy wywiad był przeze mnie autoryzowany. A może po prostu moje życie nie jest na tyle atrakcyjne. Żadnych skandali, tylko praca, wnuki, dom. To stanowi sens mojego „senioralnego" życia. Cóż tu można przekłamać?

Aktywność zawodowa seniorów to remedium na przedwczesną niesamodzielność. Czy popiera Pani naszą kampanię „Pracodawca przyjazny seniorom"?

Jak wspominałam, w tym roku stałam się szczęśliwą pracującą emerytką. Drodzy pracodawcy, dajcie szansę emerytom, bądźcie przyjaźni seniorom. Ja na swojej drodze takich właśnie pracodawców spotkałam. Nie bądźcie gorsi!

Co by poradziła Pani czytelnikom Głosu Seniora, którzy stali się ofiarą oszustów?

Drodzy, bądźcie czujni! Kierujcie się zasadą ograniczonego zaufania. Tym bardziej, że ofiarami oszustw stają się również ludzie młodzi. Oszuści są bardzo przebiegli. Jeśli tylko poczujecie, że coś jest nie tak, natychmiast zawiadomcie odpowiednie służby. Nie klikajcie w podejrzane linki. Ignorujcie reklamy oferujące „duży i szybki zysk", bo to najczęściej pułapki, które mają za zadanie wykorzystać naszą łatwowierność i dobre serce. I oczywiście śledźcie wszystkie akcje dotyczące tego, jak uniknąć oszustwa, tj. kampanię „Stop manipulacji – nie daj się oszukać" Głosu Seniora i akcję #ZnamTeNumery, którą zainicjowała Telewizja Puls wraz z Komendą Główną Policji i wspomnianą już Fundacją Telewizji Puls „Pod Dębem". Zrobimy wszystko, żeby was ochronić! Poznajcie (kolejne) numery oszustów i nie dajcie się nabrać!

FOT. PAWEŁ JAKUBEK. TELEWIZJA PULS

SPOOFING – PODSZYWANIE SIĘ

Spoofing [czyt. spufing] to rodzaj oszustwa, którego celem jest podszywanie się pod inne osoby, podmioty lub instytucje w celu pozyskania danych wrażliwych oraz zainstalowanie szkodliwego oprogramowania na smartfonie lub komputerze ofiary.

Pani Janina dostała wiadomość e-mail z prośbą o zaktualizowanie danych logowania do Internetowego Konta Pacjenta. Wiadomość nie wzbudziła żadnych podejrzeń, tym bardziej że przyszła od banku – właśnie taką formę logowania do IKP wybrała seniorka. Kliknęła link i trafiła na fałszywą stronę internetową, dzięki czemu oszuści zdobyli poufne dane.

FAŁSZYWY E-MAIL

W tym przypadku oszuści zakładają adres e-mail podobny do tego, który już znajduje się w twojej skrzynce. Następnie przesyłają wiadomości imitujące te otrzymywane z zaufanych adresów – od banków, klientów, członków rodziny czy współpracowników. Oszuści mogą zmienić wygląd nagłówków i adres wiadomości w taki sposób, że odbiorcy będzie trudno odróżnić ją od prawdziwej. Treść zawiera zazwyczaj odnośniki lub linki do innych stron czy formularzy, które przenoszą użytkownika na zawirusowaną stronę. Coraz częściej jednak takie wiadomości oznaczane są na czerwono jako SPAM, co ułatwia weryfikację.

PODRABIANY ADRES URL

Oszust podrabia adres prawdziwej strony internetowej (np. banku) i przesyła do niej link SMS-em lub na skrzynkę e-mail. Kiedy niczego nieświadomy odbiorca otworzy link, najprawdopodobniej oszust przechwyci dane logowania albo zainfekuje komputer.

PLATFORMY SPRZEDAŻOWE

Ten rodzaj spoofingu dotyczy najczęściej firm i osób korzystających z platform sprzedażowych i portali ogłoszeniowych: Allegro, OLX, Vinted czy Marketplace. Aby doszło do transakcji, najczęściej konieczna jest rozmowa poprzez komunikator. To idealna okazja dla oszustów, aby podszywać się pod inne osoby i rozesłać podejrzane linki, które następnie prowadzą do wyłudzenia danych lub zainstalowania złośliwego oprogramowania.

FAŁSZYWA NAZWA ROZMÓWCY

Metoda polega na przypisywaniu dowolnemu numerowi telefonu wybranego przez oszusta identyfikatora. Dzięki temu przestępcy mogą zadzwonić do ofiary z podejrzanego numeru, a i tak na wyświetlaczu pokaże się nazwa banku czy urzędu, z którego korzysta. Oszusta trudno jest namierzyć, bo może podszyć się pod bliską osobę, członka rodziny, przyjaciela lub partnera biznesowego. Nieuczciwy rozmówca najczęściej prosi o wykonanie płatności lub przesłanie poufnych danych.

SENIORZE, 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 wejdziesz na stronę www.

GRATULACJE Z OKAZJI DAROWIZNY

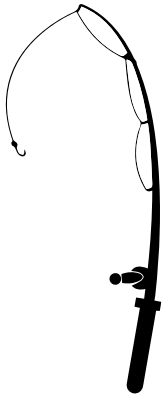
Trust<order@mwprem.net> 16 paź 2024, 04:04 (9 dni temu)

Witaj, masz darowiznę w wysokości €10 000 000 euro. Wygrałem amerykańską loterię o wartości 768,4 miliona dolarów i część z niej przekazuję pięciu szczęśliwcom i organizacji charytatywnej Orphanages. Skontaktuj się ze mną, aby uzyskać więcej informacji na temat odbioru pieniędzy z mojej darowizny: < mrgoodluck372@gmail.com > https://www.tiktok.com/@mr__good_luck

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

PHISHING – ŁOWIENIE HASEŁ

Phishing [czyt. fiszing] to przebiegła metoda oszustwa internetowego umożliwiającego podszywanie się pod znajomą osobę lub instytucję. To inaczej łowienie haseł, którego celem jest wykradanie numerów kart kredytowych, haseł do logowania oraz innych poufnych informacji za pośrednictwem różnych technik. Najczęściej oszuści wysyłają swoje wiadomości na wszystkie adresy e-mail, jakie uda im się zdobyć. W przeważającej części treść wiadomości informuje o tym, że doszło do włamania na konto i należy szybko zareagować, a zatem kliknąć w podany odnośnik. Phishing oparty jest więc na manipulacji emocjonalnej.



Pan Andrzej uwielbia śledzić aukcje na OLX i jest mistrzem okazji, dlatego często wyręcza bliskich w zakupach na tej platformie. Obiecał również ukochanemu wnukowi kupno wymarzonego roweru, o ile znajdzie się odpowiedni. Pewnego dnia dostał wiadomość na WhatsAppie, w której rzekomy wnuczek przesyła link do oferty i błaga, by dziadek zamówił rower jak najszybciej, bo ten model szybko się sprzedaje. Nie zastanawiając się, senior dokonał transakcji po kliknięciu fałszywego linku, a z jego konta zniknęło 5 tysięcy złotych.

SMISHING [CZYT. SMISZING] – ŁOWIENIE PRZEZ KOMUNIKATORY I SMS-Y

To atak, do którego potrzeba komunikatorów tekstowych lub SMS-a. Popularną techniką smishingu jest wysłanie na telefon komórkowy **wiadomości SMS zawierającej linki do kliknięcia lub numer do oddzwonienia**. Oszuści najczęściej podszywają się pod bank. W wiadomości przekazują, że został zarejestrowany podejrzany ruch na koncie i trzeba natychmiast zadzwonić pod podany numer. Haker prosi o weryfikację numeru konta bankowego, a kiedy otrzyma tę informację, przejmuje nad nim kontrolę.

WHALING [CZYT. ŁOLING] – OSZUSTWA WOBEC FIRM

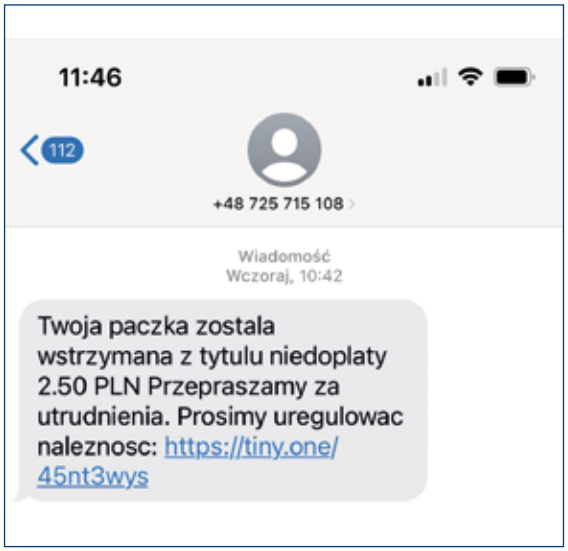
W tym przypadku celem stają się wyżej postawione osoby, np. dyrektorzy generalni czy finansowi. Oszuści przesyłają wiadomość e-mail informującą o tym, że firma ma problemy prawne i trzeba przejść do danej strony internetowej, aby dowiedzieć się więcej. Link ten przenosi ofiarę na stronę, na której należy wpisać wszystkie ważne dane dotyczące firmy, takie jak identyfikator podatkowy czy numery kont bankowych.

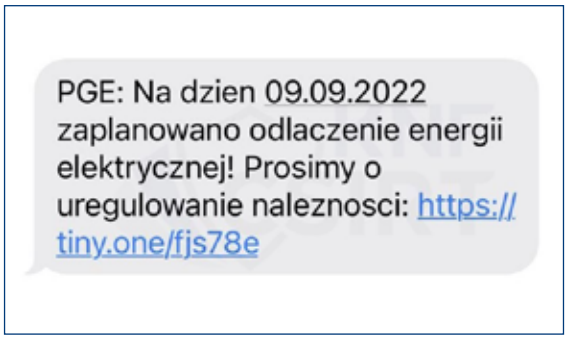
VISHING [CZYT. WISZING] – OSZUSTWA ZA POŚREDNICTWEM POŁĄCZENIA GŁOSOWEGO

Vishing to kradzież wrażliwych danych osobowych lub firmowych za pośrednictwem **połączenia głosowego**. Przestępca podszywa się pod przedstawicieli różnego rodzaju instytucji zaufania publicznego: banki, policję, urząd skarbowy czy firmy telekomunikacyjne. Próbuje wyłudzić poufne informacje, opisując sytuację wywołującą w rozmówcy stres lub zaskoczenie: awarię urządzeń, niewykonany przelew, próbę wyłudzenia kredytu, atak hakerski.

JAK SIĘ UCHRONIĆ? ABC BEZPIECZEŃSTWA

- Nie klikaj w podejrzane linki.
- Sprawdzaj dokładnie treść wiadomości SMS i adresy e-mail.
- Sprawdzaj adres URL.
- Zwróć uwagę, czy adresy nie zawierają zbędnych liter czy cyfr.
- Nie oddzwaniaj na numer, na który dzwonił oszust.
- Zainstaluj oprogramowanie antywirusowe, które pomaga zidentyfikować podejrzane numery. Poproś bliskich o pomoc.





JAK OSZUŚCI UŻYWAJĄ SZTUCZNEJ INTELIGENCJI?

Sztuczna inteligencja stała się nie tylko ogromną szansą, lecz także zagrożeniem. Jej rozwój daje oszustom spore pole do popisu. Chociaż internauci zwracają coraz większą uwagę na to, z czym mają do czynienia w sieci, dla wielu cyberoszustów nielegalne praktyki to wciąż bułka z masłem. Właśnie dlatego należy stale zapoznawać się z najnowszymi oszustwami internetowymi. Ta edukacja jest szczególnie ważna w przypadku osób starszych, które nierzadko nie są w stanie nadążyć za nowinkami w świecie Internetu.

OSZUSTWA INTERNETOWE

W ciągu ostatnich lat oszustwa znacznie się rozwinęły, a to za sprawą sztucznej inteligencji. Czym są oszustwa internetowe? To fałszywe programy, których celem jest wyłudzenie pieniędzy lub poufnych informacji od poszczególnych osób i całych organizacji. Niestety coraz trudniej je wykryć, a co za tym idzie – uniknąć.

Do najczęstszych sposobów należy phishing (łowienie haseł) bądź fałszywe połączenia. W dobie sztucznej inteligencji z łatwością można kreować nieprawdziwe informacje, aby ukraść czyjąś tożsamość i stworzyć fałszywy profil choćby na portalach społecznościowych czy randkowych. Sztuczna inteligencja „pomaga" przestępcom podrabiać wizerunek. Dotyczy to zarówno głosu, jak i całej twarzy. Aby oszuści mogli się pod nas podszyć, wystarczy kilkunastosekundowe nagranie naszej rzeczywistej mowy. Z kolei stworzenie filmu, w którym główną rolę odgrywa nasze fikcyjne ja, również nie stanowi dziś żadnego problemu. Niedawno Internet został zalany podobnymi filmikami z udziałem polityków, aktorów, piosenkarzy… Z pozoru zabawne – w rzeczywistością mogą wyrządzić wiele krzywdy.

Ostatnio wiele emocji wywołała wiadomość o tym, że audycje Off Radia Kraków poprowadzą sztucznie wykreowani dziennikarze: Jakub Zieliński (22-letni student inżynierii akustycznej), Emilia Nowak (20-letnia studentka dziennikarstwa) oraz Alex Szulc (23-letni student psychologii). Redaktor naczelny przedstawił decyzję jako eksperyment badawczo-medialny, który miałby dać odpowiedź, jakie skutki dla kultury i mediów przyniesie rozwój sztucznej inteligencji. Projekt wzbudził ogromny sprzeciw, choć szybko został zakończony. Nic dziwnego – jako gościa audycji na temat tegorocznej Literackiej Nagrody Nobla zaproszono… nieżyjącą już Wisławę Szymborską.

CZYM KIERUJĄ SIĘ OSZUŚCI INTERNETOWI?

Najważniejszym czynnikiem decydującym o powodzeniu oszustów internetowych są emocje, którymi kierują się internauci. Przestępcy wykorzystują nadmierne zaufanie ludzi, ich strach czy ekscytację. Jak zatem działają?

- Oszuści podszywają się pod znaną nam osobę lub renomowaną firmę, aby zdobyć zaufanie ofiary. Najczęściej czynią to za pomocą platform, takich jak: poczta e-mail, media społecznościowe, SMS-y i aplikacje randkowe.
- Podstępnie skłaniają ofiarę do podania wrażliwych danych: logowania, finansowych, adresu.
- Gdy oszustw uzyska potrzebne informacje, wykorzystuje je do szkodliwych celów, takich jak: kradzież tożsamości czy wyłudzenie pieniędzy.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

KRADZIEŻ TOŻSAMOŚCI

Kradzież tożsamości to przestępstwo polegające na uzyskaniu danych osobowych lub wrażliwych informacji, aby następnie wykorzystać je do nielegalnych działań w imieniu ofiary. Złodzieje tożsamości zazwyczaj polują na hasła, numery kart kredytowych, numery ubezpieczenia, imię i nazwisko, data urodzenia, numer PESEL czy adres zamieszkania.

Starsze małżeństwo planowało zawrzeć nową umowę z jedną z sieci telekomunikacyjnych, która oferowała atrakcyjne warunki. Niedługo po rozmowie na adres e-mail przyszła prośba o przesłanie skanu lub zdjęcia dowodów osobistych, aby umowa zaczęła obowiązywać. Po czasie okazało się, że oszuści wykorzystali ich zdjęcia i założyli fałszywą zbiórkę, z której opisu wynika, że seniorzy na skutek pożaru stracili dach nad głową.

Oszuści ubiegają się o pożyczkę, przejmują profile na portalach społecznościowych, robią zakupy on-line, aktywują płatne subskrypcje, wystawiają fałszywe faktury, a także docierają do dokumentacji medycznej i finansowej poszkodowanej osoby. Należy wspomnieć również o zakładaniu nowych kont bankowych, posługiwaniu się kontami walutowymi oraz działaniu na giełdach kryptowalutowych, co przy nieumiejętnym działaniu może mieć katastrofalne skutki.

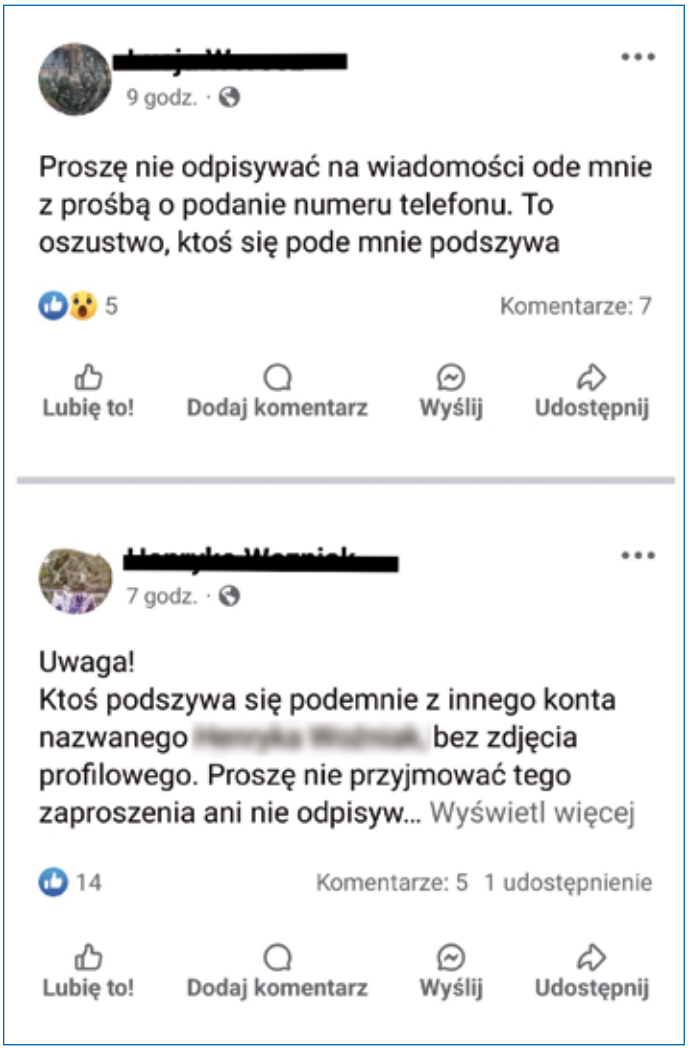
Podszywanie się ułatwiają publiczne profile na wszelkich portalach, które dla wielu oszustów są jak otwarta księga. Poszkodowani mogą więc w bardzo krótkim czasie ponieść ogromne straty finansowe z powodu nieautoryzowanych wypłat czy też zakupów w sklepach internetowych.

JAK UCHRONIĆ SIĘ PRZED KRADZIEŻĄ TOŻSAMOŚCI?

Jeżeli mamy zamiar korzystać z danych osobowych on-line, musimy być pewni, że korzystamy z bezpiecznego połączenia, czyli sieci domowej i firmowej lub z danych komórkowych. Najlepiej unikać sieci publicznych, które nie są zabezpieczone hasłem.

O CZYM WARTO JESZCZE PAMIĘTAĆ?

- **Zabezpiecz swój sprzęt przed złośliwym oprogramowaniem.** Zainstaluj aktualne oprogramowanie antywirusowe.
- **Unikaj podejrzanych wiadomości i stron internetowych, sprawdzaj dokładnie adres.**
- **Zwróć uwagę na hasła.** Najlepiej wybierać długie i trudne frazy, skorzystać z uwierzytelniania dwuskładnikowego i ustawiać inne hasło dla każdego kolejnego konta.
- **Sprawdzaj swoje konta bankowe pod kątem podejrzanej aktywności.**
- **Monitoruj wrażliwe dane.** Jeżeli dokumenty zawierające dane osobowe nie są już potrzebne, należy zniszczyć je w bezpieczny sposób. Powinieneś je również trwale usunąć z urządzeń, które sprzedajemy lub których się pozbywamy.
- **Nie wrzucaj wszystkiego do sieci.** Wszelkie zdjęcia i filmy, nawet te niepozorne, są cennym źródłem informacji dla oszustów.
- **Pobieraj aplikacje tylko z zaufanych stron.**
- **Regularnie aktualizuj system operacyjny, przeglądarkę stron i aplikacje.**
- **Zastrzeż PESEL** – więcej informacji na stronie 50.



DEEPFAKE – ZMANIPULOWA

Deepfake jest techniką polegającą na wykorzystywaniu sztucznej inteligencji do kreowania fałszywych obrazów, filmów lub dźwięku, które wydają się niezwykle prawdziwe. Ze względu na możliwość tworzenia wiarygodnych, aczkolwiek fałszywych materiałów, rosną obawy dotyczące dezinformacji, zniesławienia, szantażu, manipulacji politycznych czy naruszenia prywatności.

Seniorka z powiatu zamojskiego przekazała 700 tysięcy złotych mężczyźnie podającemu się za adwokata, aby pomóc córce, która rzekomo potrąciła kobietę w ciąży za granicą. Starsza kobieta rozpoznała głos córki, choć to nie była ona. Oszuści zapewne wykorzystali sztuczną inteligencję do podrobienia głosu, co uwiarygodniło komunikat.

Nazwa deepfake pochodzi od dwóch angielskich słów: *deep* – 'głęboki' [czyt. dip] i *fake* – 'fałszywy' [czyt. fejk]. Aby wyprodukować nieprawdziwe filmy i zdjęcia, nie trzeba dysponować specjalnymi umiejętnościami ani być specjalistą zajmującym się informatyką. Wprost przeciwnie – aplikacje deepfake najczęściej są bardzo intuicyjne w obsłudze, do tego coraz tańsze, a niekiedy nawet bezpłatne. Oczywiście trzeba poświęcić chwilę, aby wytrenować sieć na wielu prawdziwych nagraniach. Algorytm musi wyłapać, jak osoba, której kradnie się wizerunek, wygląda z różnych stron i jakie są jej charakterystyczne ruchy. Dzięki takiej technologii oszuści mogą umieścić dowolną osobę (od sławnych ludzi po sąsiadów mijanych na klatce schodowej) w sztucznie wyreżyserowanej sytuacji. Tak naprawdę ogranicza ich wyłącznie wyobraźnia.

NA CZYM NAJCZĘŚCIEJ POLEGA DEEPFAKE?

W praktyce deepfake najczęściej polega na:

- **zmianie twarzy** – twarz jednej osoby zostaje zastąpiona twarzą tej drugiej. Algorytmy analizują zarówno mimikę, jak i ruchy, co pozwala na stworzenie bardzo realistycznego złudzenia;
- **synchronizacji ruchu ust z dźwiękiem** – ruchy ust osoby przedstawionej na wideo są dopasowywane do nagrania głosu kogoś innego. Tym sposobem usłyszymy coś, czego nigdy dana osoba tak naprawdę nie powiedziała;
- **zmianach w głosie** – za pomocą syntetyzatora mowy manipuluje się głosem, tak by brzmiał łudząco podobnie do głosu innej osoby.

PRZYKŁADY WYKORZYSTANIA TECHNOLOGII DEEPFAKE

Internet jest kopalnią sfabrykowanych filmów i zdjęć. Jednym z najbardziej znanych przykładów jest sfabrykowane wideo ukazujące prezydenta Wołodymyra Zełenskiego, który tuż po wybuchu wojny na Ukrainie ogłasza w mediach społecznościowych kapitulację wojsk ukraińskich. Wojna pomiędzy Rosją a Ukrainą udowodniła, że w dzisiejszych czasach niebagatelną rolę odgrywa tzw. wojna informacyjna siejąca panikę i zamęt w społeczeństwie.

KLONOWANIE GŁOSU

Spośród wymienionych sposobów wykorzystania sztucznej inteligencji wielkie zagrożenie niesie za sobą klonowanie głosu. Do tego wystarczy kilkunastosekundowe nagranie naszej rzeczywistej mowy. Zwłaszcza starsze osoby mogą mieć problem z rozróżnieniem prawdziwej rozmowy i sztucznie wygenerowanego komunikatu bazującego na głosie bliskiej osoby. W tym przypadku tzw. metoda na wnuczka staje się niezwykle skuteczna – w końcu oszust będzie brzmieć jak prawdziwy członek rodziny. Dzięki nowoczesnej technologii oszuści są jeszcze bardziej przekonujący, dlatego zdobywają pełne zaufanie niczego nieświadomych bliskich.

Czy da się rozpoznać klonowany głos? Chociaż silne emocje odczuwane przez seniora podczas próby wyłudzenia pieniędzy mogą uniemożliwić zidentyfikowanie wypowiedzi warto zapamiętać kilka szczegółów:

- **niepoprawna intonacja** – zwróć uwagę, czy zdania się nie urywają albo czy między słowami nie ma zbyt długich przerw. Sztucznie wygenerowany głos będzie również pozbawiony emocji;
- **brak błędów** – sklonowany głos jest zbyt płynny i nie zawiera przerywników;
- **oddech** – w wypowiedziach nie słychać wdechów i wydechów.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

NE ZDJĘCIA I WIDEO

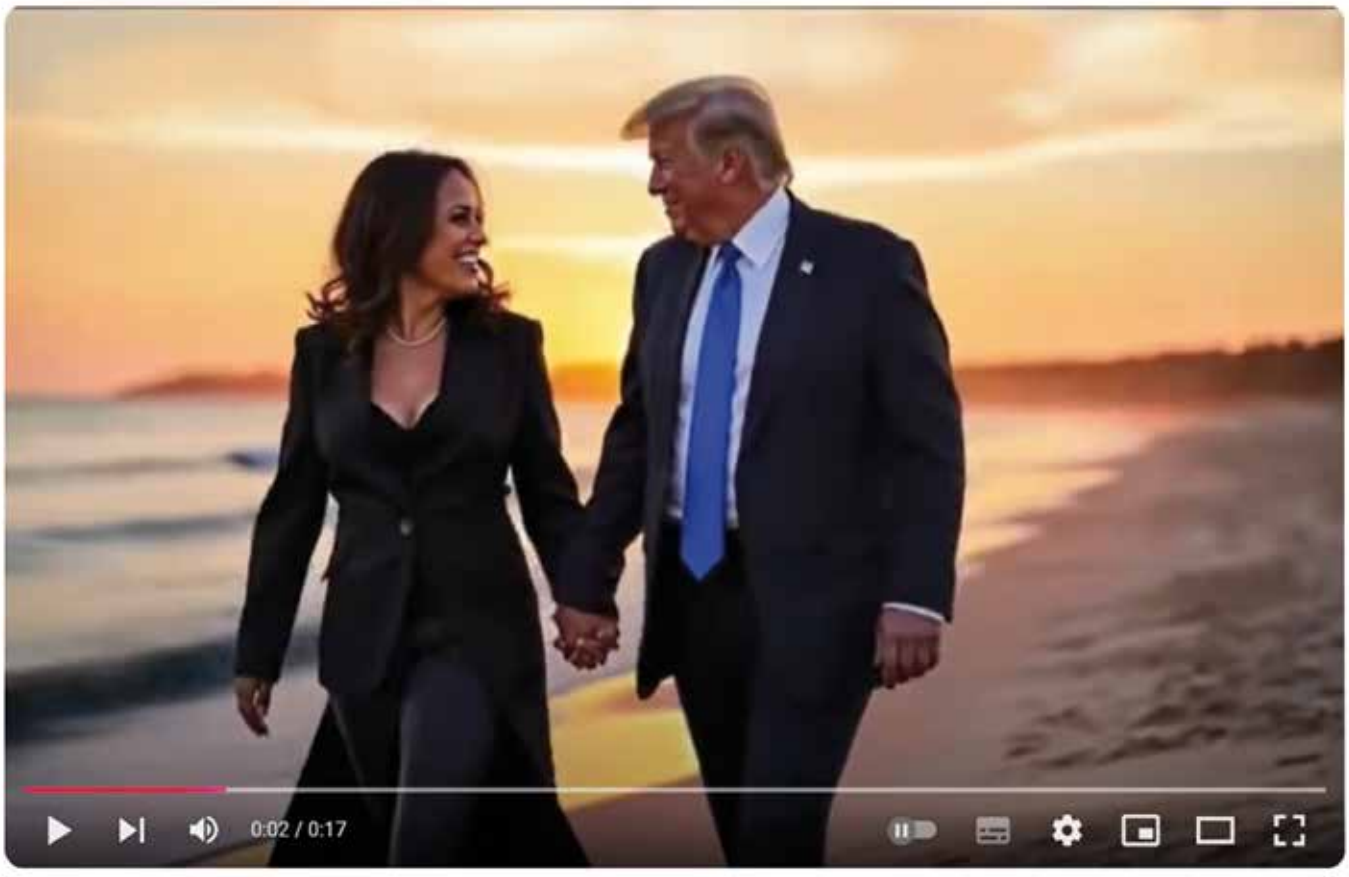
Aby zweryfikować tożsamość rozmówcy, należy zadać mu osobiste pytanie, na które znają odpowiedź tylko osoby z najbliższego kręgu. Można również posłużyć się sekretnym słowem ustalonym z członkami rodziny, a najlepiej rozłączyć się i zadzwonić pod właściwy numer do osoby, pod którą podszywają się oszuści.

Jeśli senior jest aktywny w mediach społecznościowych, powinien zadbać szczególnie o ustawienia prywatności, tak aby kontrolować, kto ma dostęp do jego danych. Sugeruje się także, aby ograniczyć publikowanie postów wyłącznie dla wąskiego grona znajomych.

CZUJNOŚĆ PRZEDE WSZYSTKIM

W dzisiejszych czasach nie powinniśmy uznawać materiałów zamieszczanych w sieci za rzetelne i wiarygodne źródło informacji. Trzeba być szczególnie czujnym, kiedy próbujemy rozpoznać, czy oglądany właśnie film przedstawia prawdziwe sytuacje.

Co warto zrobić? Użytkownicy powinni sprawdzić, czy ruch warg postaci występujących w danej produkcji jest zsynchronizowany z wypowiadanymi słowami i czy wygląda naturalnie. Należy także zwrócić uwagę na jakość nagrania, ponieważ te wykorzystujące deepfake zazwyczaj są o wiele gorsze, co znacząco utrudnia rozpoznanie. Jednakże na takich filmach sporadycznie mogą pojawiać się błędy, np. przebijanie oryginalnych kadrów, nienaturalne ruchy oczu, nienaturalnie padający cień na obrazie, nierównomierny kolor skóry, rzadkie mruganie, mimika niedopasowana do treści komunikatu, nienaturalne proporcje ciała czy nienaturalne ułożenie głowy w stosunku do reszty.



Czy Donald Trump i Kamala Harris mają dziecko?! 😳🤣

PODCZAS KAMPANII WYBORCZEJ W STANACH ZJEDNOCZONYCH INTERNAUCI STWORZYLI FAŁSZYWY FILMIK PRZEDSTAWIAJĄCY KANDYDATÓW NA PREZYDENTA: DONALDA TRUMPA I KAMALĘ HARRIS JAKO SZCZĘŚLIWĄ PARĘ. W RZECZYWISTOŚCI SĄ RYWALAMI. W TYM PRZYPADKU O TECHNICE DEEPFAKE ŚWIADCZY M.IN. KIEPSKA JAKOŚĆ OBRAZU. CHOCIAŻ NIEMAL DLA WSZYSTKICH MOŻE WYDAWAĆ SIĘ OCZYWISTE, ŻE KADRY NIE SĄ PRAWDZIWE, SAMO POWSTANIE TAKIEGO NAGRANIA NADAŁO TEGOROCZNEJ KAMPANII INNY WYMIAR.

JAK OSZUŚCI WYKORZYSTUJĄ PROGRAMY IMITUJĄCE LUDZKĄ ROZMOWĘ?

Chatbot [czyt. czatbot] jest programem imitującym ludzką rozmowę (pisaną lub mówioną), który daje błyskawiczne odpowiedzi na niemal każde pytanie. Jego nazwa pochodzi od słów *chat* – 'rozmowa' i *bot* – 'robot'. Chociaż rzekomo czerpie wiedzę z ogromnej bazy danych, trzeba mieć na uwadze, że w Internecie jest pełno niezweryfikowanych treści oraz fałszywych informacji. Należy unikać zwłaszcza porad dotyczących zdrowia: chatboty mogą generować odpowiedzi wprowadzające w błąd na temat praktyk niebezpiecznych nawet dla życia użytkowników.

Wnuczka pani Haliny nauczyła ją korzystać z popularnego chatbota. Od tamtej pory seniorka jest zafascynowana możliwościami sztucznej inteligencji: z jego pomocą pisze wiersze, szuka przepisów na nowe ciasta. Niestety zaczęła na nim za bardzo polegać i prosić o polecenie leków oraz suplementów na jej dolegliwości. Wirtualny asystent podsunął drogie specyfiki na podejrzanych stronach internetowych, ale seniorka – przekonana o wspaniałych właściwościach – złożyła zamówienie. Tym sposobem straciła kilkaset złotych na leki, które mają znikome działanie.

Wirtualni asystenci przechowują liczne informacje: transkrypcję rozmów, informacje o urządzeniu, lokalizację, nawet aktywność w mediach społecznościowych. Gromadzenie tych szczegółów pozwala firmom udoskonalanie modeli językowych. Wielu internautów „zaprzyjaźnia" się z chatbotem, a przez to ujawnia prywatne dane, które następnie mogą być podstępnie wykorzystane, m.in. do kradzieży tożsamości.

Chatboty są zdolne do stworzenia fałszywych stron internetowych, które będą łudząco podobne do tych rzeczywistych. Co w takim przypadku może zdradzać oszustów? Wszelkiego rodzaju błędy ortograficzne i składniowe zazwyczaj świadczą o tym, że zostały nieumiejętnie przetłumaczone z innego języka.

JAKICH INFORMACJI NIE UDOSTĘPNIAĆ W TRAKCIE ROZMOWY ZE SZTUCZNYM ASYSTENTEM?

Długie rozmowy są pułapką zwłaszcza dla seniorów, którym doskwiera samotność, zwłaszcza że coraz więcej osób starszych korzysta z dobrodziejstw Internetu. Łatwo jednak zatracić się w wirtualnej przyjaźni, a to może mieć przykre konsekwencje. Trzeba zatem pamiętać, by w trakcie wymiany zdań nie podawać: imienia i nazwiska, adresu i numeru telefonu, daty urodzenia, numeru ubezpieczenia społecznego i kart płatniczych, nazw użytkowników i haseł do platform społecznościowych i sklepów on-line, kodów PIN, poufnych informacji dotyczących miejsca pracy, a także swoich przemyśleń. Informacje o poglądach i osobistych doświadczeniach mogą posłużyć do szantażu emocjonalnego.

Korzystaj, ale z głową – nie przekazuj poufnych danych i nie wierz we wszystko, co napisze chatbot.

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

ZŁODZIEJE HASEŁ

Programy wykradające hasła to złośliwe oprogramowanie, które nieświadomie można zainstalować na swoim komputerze lub smartfonie. Najczęściej ich źródłem są zainfekowane pliki pobrane jako załączniki z podejrzanych wiadomości e-mail. Oczywiście mają na celu wykradanie poufnych informacji, takich jak hasła czy dane logowania.

65-latka w ramach newslettera dostała wiadomość z informacją, że słynna organizacja działająca na rzecz seniorów rozplanowała warsztaty do końca roku. W załączniku przesłano broszurę, w której podano rozpiskę najbliższych wydarzeń. Seniorka pobrała zainfekowany plik, a wraz z nim – nielegalny program przechwytujący hasło do jej konta.

Coraz więcej użytkowników zdaje sobie sprawę, że proste i przewidywalne hasło nie wystarcza. W tym temacie trzeba uświadamiać przede wszystkim osoby starsze, które niejednokrotnie ze względu na problemy z pamięcią mogą nie chcieć tworzyć trudnych kombinacji. Mimo wszystko używanie silnych haseł jest niezbędne do tego, by chronić własną tożsamość.

JAK DZIAŁAJĄ PROGRAMY WYKRADAJĄCE HASŁA?

Takie narzędzia przede wszystkim zdobywają informacje o nazwie użytkownika i hasłach, które są przechowywane na urządzeniu. Takie poufne dane są następnie sprzedawane innym cyberprzestępcom do nieuczciwych celów: kradzieży tożsamości i pieniędzy czy kupowania nielegalnych produktów.

Jak sprawdzić, czy padliśmy ofiarą takiego oszustwa? Najlepiej używać zaktualizowanego oprogramowania antywirusowego. Jeśli program wykradający hasła zostanie wykryty, trzeba natychmiast go wyczyścić i usunąć z urządzenia.

DOBRE HASŁO TO PODSTAWA

Oprócz aktualnego oprogramowania antywirusowego warto zadbać o właściwe hasło.

- Specjaliści ds. cyberbezpieczeństwa sugerują, by hasła tworzyć z trzech losowych i niepowiązanych ze sobą słów, np. „klawiszpasektermos" lub „niedzielakrzywecukier". Można dobrać frazy zapadające w pamięć, ale nie takie, które są łatwe do odgadnięcia lub ściśle wiążą się z najbliższym otoczeniem osoby zagrożonej atakiem.
- Hasło powinno mieć co najmniej 8 znaków, w tym kombinację małych i wielkich liter, liczb oraz znaków specjalnych. Im dłuższe, tym trudniej je złamać. Nie korzystaj z sekwencji kolejnych liter lub cyfr.
- Do stworzenia hasła możesz użyć pierwszych liter ulubionego cytatu lub piosenki, a wybrane litery zastąpić podobnymi znakami, np. „@" zamiast „a", „$" zamiast „S", „!" zamiast „i".
- Unikaj oczywistych informacji. Hasło, które zawiera imię i nazwisko czy daty urodzenia, najprawdopodobniej zostanie sprawdzone w pierwszej kolejności.
- Nie używaj tego samego hasła do wielu kont, ponieważ staniesz się bardziej podatny na ataki hakerskie. Unikalność hasła jest ważna również wtedy, gdy dojdzie do nieprawidłowości na stronach internetowych, z których usług korzystamy. Wycieki danych są coraz częstszym zjawiskiem, a ostatnio taka sytuacja miała miejsce choćby w jednej z internetowych aptek i znanym sklepie jubilerskim.
- Nie wpisuj hasła, gdy ktoś zagląda przez ramię, i nie wysyłaj go w wiadomościach e-mail i SMS. Unikaj także logowania się na cudzym sprzęcie.
- Stosuj dwuetapowe uwierzytelnianie – choć może się wydawać, że jest ono skomplikowane, nic bardziej mylnego.

FAŁSZYWE REKLAMY I MANIPULOWANIE OPINIAMI

W dobie cyfryzacji i dynamicznego rozwoju mediów internetowych seniorzy stają się narażeni również na manipulację przybierającą formę fałszywych reklam oraz opinii. Podstawą takich oszustw jest stworzenie przekonującego obrazu lub opisu produktu i usługi, który ma zachęcić konsumenta do zakupu. Jak wiadomo, ze względu na starzejące się społeczeństwo osoby starsze są uważane za coraz bardziej atrakcyjną grupę docelową dla marketerów.

Ostatnimi czasy oszuści ukradli wizerunek znanego z telewizji doktora Michała Sutkowskiego, by rozpromować preparat nieznanego pochodzenia. Sztuczna inteligencja pomogła stworzyć wywiady, w których lekarz zachwala działanie leków: kardiologicznych, zwalczających pasożyty i na cukrzycę. W filmikach przekonuje on, że apteki oszukują pacjentów, a cudowne specyfiki zwalczą wszystkie objawy choroby. Pod nagraniem oszuści zamieścili link do strony internetowej, gdzie znajdują się komentarze osób zadowolonych z zakupu. Witryna umożliwia zamówienie leku, a po podaniu swojego imienia i numeru telefonu z zainteresowanym kontaktuje się konsultant.

Oszuści zazwyczaj celują w produkty popularne wśród seniorów. W sieci znajdziemy więc reklamy suplementów diety, produktów poprawiających pamięć, usług medycznych, a nawet kontrowersyjnych lekarstw – zazwyczaj mają dawać szybkie i spektakularne efekty, co oczywiście jest kłamstwem. Niestety z pomocą sztucznej inteligencji oszuści często wykorzystują wizerunek znanych specjalistów lub celebrytów, dzięki czemu komunikat staje się bardziej wiarygodny.

Należy pamiętać, że polskie prawo zabrania lekarzom reklamowania produktów leczniczych i leków, aktorom natomiast – wcielania się w lekarzy, by zapromować dany specyfik. Oszuści jednak wykorzystują zarówno nieświadomość konsumentów, jak i autorytet znanych osób.

Podejrzane suplementy diety i środki lecznicze to niejedyne, co przestępcy próbują „sprzedać" nieświadomym seniorom. Należy wspomnieć o inwestycjach przeznaczonych tylko dla osób starszych, drogich kursach i szkoleniach on-line mających poprawić ich kompetencje cyfrowe, a także ubezpieczeniach zdrowotnych, które tylko pozornie nie zawierają żadnych kruczków.

FAŁSZYWE RECENZJE

Problem stanowią fałszywe recenzje wystawiane przez tzw. boty (program stworzony do wykonywania powtarzalnych zadań). Dotyka on wiele popularnych platform sprzedażowych, ale też małe sklepy internetowe, które starają się walczyć z tym zjawiskiem, by nie stracić zaufania klientów. Jednakże w wielu przypadkach oszuści tworzą osobne strony internetowe i zamieszczają sztucznie wykreowane pozytywne recenzje, by w ten sposób nakłonić użytkowników do zakupu produktów, których albo nie ma, albo ich cena jest znacząco zawyżona. W ostatnich tygodniach pojawia się również coraz więcej reklam – przeważnie sklepów odzieżowych – informujących odbiorców o czyszczeniu magazynów z powodu zamknięcia się firmy. Takie posty mają za zadanie wywołać określone emocje: współczucie czy empatię, dzięki czemu internauci są bardziej skłonni do odwiedzenia strony internetowej i zrobienia zakupów. Niestety informacja o upadku marki jest tylko fałszywą informacją, a post o „upadku" firmy widnieje w sieci długie tygodnie.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA KRYPTOWALUTY

Oszustwo na kryptowaluty polega na wyłudzeniu cyfrowej wersji tradycyjnego pieniądza (takie pieniądze są niezależne od inflacji i dodruku) poprzez różne metody manipulacji i podszywania się. Główny cel oszustwa to nakłonienie ofiary, aby przekazała swoje kryptowaluty lub umożliwiła dostęp do portfela, w którym są przechowywane. Drugim celem natomiast jest nakłanianie do zakupu takiej formy pieniądza na platformach inwestycyjnych.

56-latka mieszkająca w powiecie sztumskim straciła ponad 40 tysięcy złotych, bo myślała, że inwestuje w cyfrowe złoto. Na popularnej platformie internetowej zobaczyła reklamę firmy zajmującej się kryptowalutami. Wypełniła formularz kontaktowy, który wymagał od niej podania dokładnych danych osobowych. Następnie przelała pieniądze, aby zainwestować w wirtualną walutę. W międzyczasie rozmawiała na komunikatorze z rzekomym pracownikiem firmy. Mężczyzna zapewniał ją, że dzięki tak wysokiej wpłacie jej zyski powiększą się o wiele szybciej.

Podobny schemat działania został wykorzystany w przypadku 70-latki. Seniorka uwierzyła w internetową reklamę, która przekierowała ją do formularza. Tym razem oszuści namówili kobietę do zainstalowania aplikacji na telefon. W ten sposób zyskali dostęp do jej konta bankowego, a wraz z nim – 120 tysięcy złotych. Również 66-letnia mieszkanka Bydgoszczy pozbyła się ponad 100 tysięcy złotych. Przez 3 miesiące wpłacała pieniądze na konto w Luksemburgu, aby zainwestować na giełdzie. Oczywiście cała kwota przepadła.

W wielu przypadkach procedura popełniania przestępstwa polega na stworzeniu Centrum Obsługi Klienta (call center) i nakłanianiu przez „doradców" do instalowania programu zdalnej obsługi komputera. Ofiary nie mają pojęcia, że taki krok wcale nie jest wyręczeniem i ułatwieniem, ale próbą dotarcia do danych przechowywanych na urządzeniu. Oszuści przeprowadzają szereg operacji finansowych przy użyciu zagranicznych kantorów internetowych oraz giełd inwestycyjnych i kłamią co do możliwości zarobku.

Oszustwa na kryptowaluty są też możliwe poprzez spoofing telefoniczny – dzięki specjalnym programom cyberprzestępcy ukrywają swój numer, więc wyświetla się on jako anonimowy. Podczas działania wykorzystują dane kart bankowych: numer karty, datę ważności i kod CVV/CVC, a to wszystko pod pretekstem weryfikacji danych w celu założenia konta na platformie.

WIRTUALNE WALUTY W GRACH

Coraz więcej seniorów gra w gry komputerowe, by w ten sposób trenować umysł. W dobie Internetu bardzo popularne są gry on-line, a większość z nich jest dostępna za darmo. Czasem jednak trzeba wykupić dodatkowy wirtualny przedmiot, co pozwala zwiększyć szansę w grze na przeżycie. To oszustom otwiera drzwi do kolejnego przestępstwa. Senior może dostać powiadomienie, że musi zweryfikować swoje konto, w przeciwnym wypadku zostanie ono wyłączone. Niektórzy poświęcają sporo czasu na uzbieranie potrzebnych i cennych przedmiotów w grze, dlatego podają dane logowania, aby nie stracić swoich zbiorów.

W przypadku inwestowania na giełdach i w kryptowaluty trzeba być szczególnie ostrożnym. Jeśli ktoś obiecuje szybki zarobek w kilku krokach – najprawdopodobniej jest to oszustwo.

OSZUSTWA NA APLIKACJĘ SPRZEDAŻOWĄ TEMU

Temu jest obecnie jedną z najbardziej popularnych platform sprzedażowych na całym świecie. A to wszystko dzięki szerokiemu asortymentowi i bardzo atrakcyjnym cenom, które w dobie rosnących wydatków są niezwykle kuszące. Jak można się domyślić, jakość produktów pozostawia wiele do życzenia, jednakże względy finansowe zdecydowanie przemawiają do milionów klientów na całym świecie, również tych starszych.

Marketing tej platformy jest rozbudowany, dzięki czemu reklamy przedstawiające ofertę Temu pokazują się niemal na każdym kroku – również w telewizji. Niestety popularność aplikacji przyciągnęła także wielu oszustów, którzy wykorzystują „sławę" Temu do okradania ludzi i wprowadzania ich w błąd.

OSZUSTWA POPRZEZ E-MAIL

Cyberprzestępcy wykorzystują skrzynkę pocztową do rozsyłania fałszywych wiadomości e-mail, których nadawcą jest pracownik Temu. W treści mogą znajdywać się informacje o nagrodzie, rabatach lub darmowych produktach, jednakże klient najpierw musi wypełnić ankietę lub dopłacić za wysyłkę. W rzeczywistości oszuści próbują w ten sposób przechwycić dane karty płatniczej lub zainstalować na komputerze złośliwe oprogramowanie. Aby uniknąć oszustwa, sprawdź adres e-mail nadawcy. W przypadku sklepu Temu brzmi on „temuemail.com". Mimo wszystko powstrzymaj się od otwierania jakichkolwiek linków.

PODSZYWANIE SIĘ POD PRACOWNIKA BIURA OBSŁUGI KLIENTA

Oszuści podszywają się pod przedstawicieli obsługi klienta, by wzbudzić większe zaufanie, a tym samym wyłudzić dane osobowe. Tym razem nie tylko wysyłają wiadomość e-mail, ale także kontaktują się telefonicznie z informacją, że muszą rozwiązać problem z zamówieniem. Pamiętaj, że prawdziwi przedstawiciele nie będą wypytywać cię o konkretne dane i to bez powodu.

OSZUSTWO NA KARTĘ PODARUNKOWĄ TEMU

Cyberprzestępcy wykorzystują media społecznościowe, by reklamować na nich darmowe karty podarunkowe do sklepu Temu. Nie ma jednego sposobu: mogą informować o atrakcyjnych promocjach, zachęcać do zainstalowania aplikacji i zrobienie zakupów on-line, a nawet namówić do grania w gry. W ten sposób rzekomo zdobędzie się kartę. Jeżeli natrafiłeś w sieci na reklamę obiecującą coś za darmo, w większości przypadków nie ma to nic wspólnego z rzeczywistością i służy do wykradania osobistych informacji oraz pieniędzy.

WYKORZYSTANIE CELEBRYTÓW

Technologia deepfake, czyli manipulowanie obrazem i dźwiękiem, umożliwia oszustom przygotować taką reklamę, w której popularny aktor czy wokalista zachwala dany produkt, a następnie zachęca do przejścia na stronę internetową podlinkowaną w opisie. Słowa włożone w usta znanej osobowości stają się bardziej przekonujące i wzbudzają większe zaufanie.

PODRÓBKI

Również na oficjalnej stronie sklepu Temu senior jest narażony na oszukańcze działanie. Nieuczciwi sprzedawcy wystawiają na aukcję wadliwe podróbki, które nawet mogą szkodzić zdrowiu potencjalnych nabywców.

Szukaj zweryfikowanych sprzedawców (z odznaką , Wszystkie opinie są weryfikowane) sprawdzaj opinie o nich i o produkcie, ogranicz drogie zakupy, by w przypadku oszustwa stracić jak najmniej pieniędzy.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWA INWESTYCYJNE

Na platformach społecznościowych pojawia się coraz więcej reklam namawiających odbiorców do inwestycji. Z pomocą sztucznej inteligencji oszuści wykorzystują wizerunek celebrytów i logotypy instytucji, aby uwiarygodnić przekaz. Cyberoszuści wykorzystują brak wiedzy potencjalnych inwestorów na temat różnorakich form inwestycji i ryzyka, jakie za sobą niosą.

Oszuści najczęściej umieszczają reklamę fałszywych inwestycji w mediach społecznościowych i na wielu stronach internetowych. Umieszczają na niej kuszące hasła, takie jak „bezpieczna inwestycja", „zysk bez ryzyka" czy „gwarancja szybkiego zarobku".

JAK DZIAŁA OSZUSTWO NA INWESTYCJĘ?

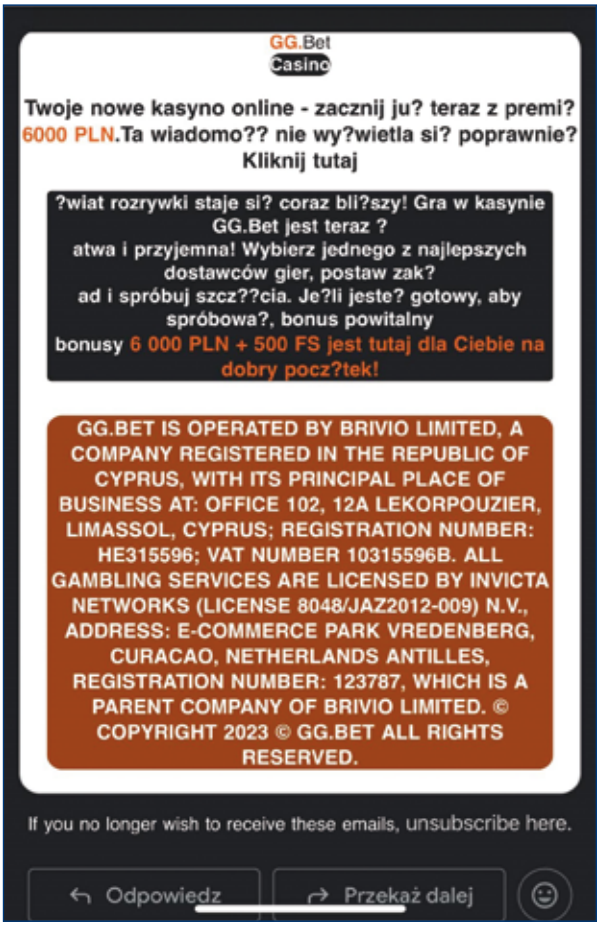
Oczywiście reklama fałszywej inwestycji zawiera link, który prowadzi do zewnętrznej strony. Następnie osoba jest proszona o podanie swoich danych kontaktowych, aby się zarejestrować albo zainstalować specjalną aplikację do inwestowania. Kiedy oszust zdobędzie potrzebne informacje, kontaktuje się z ofiarą telefonicznie i podaje się za brokera lub konsultanta. Opowiada o korzyściach wynikających z zainwestowania niewielkich pieniędzy, opowiada również o inspirujących historiach innych ludzi. W ten sposób próbuje zmanipulować rozmówcę do przelania środków.

Następnie oszust podaje numer rachunku do płatności. Po kilkukrotnie zrealizowanych przelewach przestępca zasila konto ofiary drobnymi kwotami, aby uśpić czujność inwestora. W rzeczywistości są to środki pozyskane od innych oszukanych osób. Przestępcy często posługują się również wizualizacją wyników inwestycji zamieszczaną na fałszywych platformach. Kiedy ofiara chce wypłacić zyski i zakończyć inwestycję, oszuści oferują pomoc w wypłacie i proponują zainstalowanie programu do zdalnego zarządzania pulpitem. Po spełnieniu życzenia inwestor loguje się do bankowości internetowej – tym sposobem wszystkie dane są widoczne. Właśnie w taki sposób 70-letnia mieszkanka powiatu bielskiego straciła prawie 90 tysięcy złotych.

W zależności od wariantu oszustwa przestępcy mogą poprosić o przesłanie skanu dowodu osobistego.

INWESTYCJA W STACJE BENZYNOWE ORLEN

Fałszywe ogłoszenia gwarantują także szybki zarobek po zainwestowaniu w akcje spółek Grupy ORLEN albo w budowę stacji paliw. Reklama zawiera przerobione logo spółki i często zmodyfikowaną nazwę. Należy więc zwrócić uwagę, czy nie brakuje jakiejś litery. Aby zweryfikować profil, warto sprawdzić liczbę obserwujących – jeśli jest niewielka, najprawdopodobniej mamy do czynienia z fałszywym kontem. Takie posty prowadzą do stron niepowiązanych z ORLENEM, zawierają błędy językowe i przedstawiają kiepskiej jakości fotomontaże, których grupa na co dzień nie wykorzystuje w swoim przekazie. Firma informuje, że ORLEN zachęca do inwestowania wyłącznie poprzez oficjalne kanały: orlen.pl, orlenwportfelu.pl lub na zweryfikowanym profilu w mediach społecznościowych.



QUISHING – OSZUSTWO NA KODY QR

Kody QR to kody, które po zeskanowaniu natychmiastowo przenoszą na daną stronę internetową. Coraz częściej są one stosowane nie tylko w sieci, ale także w restauracjach (wyświetlenie menu), firmach (informacje o produktach i ofertach specjalnych) czy w przychodniach (opis kampanii), a nawet w aplikacji mObywatel (kod potwierdzający szczepienie przeciw COVID-19). Choć jest to wygodne rozwiązanie, może przysporzyć wiele kłopotów.

Coraz częściej oszuści wykorzystują kody QR do kradzieży danych osobowych. Taka sytuacja spotkała 50-letnią mieszkankę powiatu płońskiego, która po zeskanowaniu kodu straciła niemal 4 tysiące złotych. Co więcej, ktoś próbował wziąć na nią kredyt w wysokości 40 tysięcy złotych.

Jak do tego doszło? Skorzystała z popularnego serwisu ogłoszeniowego, aby wystawić na sprzedaż buty sportowe. Niedługo później dostała SMS z informacją o tym, że ktoś postanowił je kupić. Za pośrednictwem komunikatora w serwisie fałszywy kupujący przesłał kod QR, za pomocą którego kobieta miała odebrać przelew. Sytuacja nie wzbudziła w niej żadnych podejrzeń i uznała to za unowocześnienie procesu transakcji, ponieważ od bardzo dawna nie korzystała z wybranej przez siebie platformy sprzedażowej. Po zeskanowaniu kodu została przeniesiona na fałszywą stronę. Wybrała bank, zalogowała się na swoje konto, a następnie wpisała kody liczbowe, które dostała poprzez wiadomość SMS. Mieszkanka powiatu płońskiego zorientowała się dopiero wtedy, gdy dane zbyt długo się ładowały i sprawdziła bankowość elektroniczną na komputerze. Niestety w ciągu tych paru chwil straciła lokatę i 3800 złotych. Kobieta zadzwoniła na infolinię banku, by zablokować konto, i wtedy dowiedziała się, że oszuści nie tylko skradli jej oszczędności, ale również próbowali wziąć kredyt.

UWAŻAJ!

Jeżeli zeskanujesz podrobiony kod, najprawdopodobniej zostaniesz odesłany na fałszywą stronę banku, sklepu lub innych instytucji. Celem oszustów jest kradzież danych użytkowników lub zainstalowanie złośliwego oprogramowania, które wyrządzi wielu szkód na przejętym sprzęcie. Po zeskanowaniu kodu QR przestępca może uzyskać dostęp do wszelakich haseł, zapisanych i wysyłanych wiadomości, listy kontaktów i osobistych informacji.

Aby ochronić się przed tego typu działaniem, trzeba przede wszystkim wyłączyć funkcję automatycznego skanowania kodów QR. Bądź niezwykle ostrożny, jeśli na stronie widnieje prośba o pobranie pliku czy aplikacji lub aktualizację aplikacji – podobnie w przypadku przenoszenia się do bramek płatności lub na stronę banku. Stałeś się ofiarą podstępnego działania? Niezwłocznie zgłoś się na policję, do Urzędu Ochrony Konkurencji i Konsumentów oraz organizacji broniących praw konsumentów.

JAK ROZPOZNAĆ FAŁSZYWY KOD QR?

Jeśli mamy do czynienia z kodem w fizycznej formie – na przykład naklejką – zwróć uwagę na jego stan. W miejscach publicznych oszuści z łatwością mogą go podmienić. Sprawdź więc, czy w miejscu naklejenia znaku nic nie zostało zdarte.

Na większości telefonów wyświetla się adres strony internetowej, do której prowadzi kod QR. Pamiętaj, na początku powinny znajdować się zamknięta kłódka i fragment „https://".

Ten kod QR przeniesie Cię do naszej strony internetowej www.glosseniora.pl – zapraszamy.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

ZASADY CYBERBEZPIECZEŃSTWA

1. Nie otwieraj załączników z niepewnych źródeł i nie klikaj w podejrzane linki.
2. Zwróć uwagę na adres strony i sprawdź, czy na pasku znajduje się ikonka zamkniętej kłódki.
3. Wymyślaj trudne hasła – z kombinacją wielkich i małych liter, cyfr i znaków specjalnych (np. &, $, #, @).
4. Regularnie zmieniaj hasło, a więc przynajmniej raz w roku.
5. Pamiętaj, aby nie używać jednego hasła do różnych kont i platform oraz nie zapisywać go na komputerze. Nie zostawiaj także na kartce w widocznym miejscu.
6. Pod żadnym pozorem nie podawaj i nie wysyłaj innym swoich danych osobowych, loginów i haseł.
7. Korzystaj wyłącznie z zabezpieczonych sieci, czyli takich, do których dostęp jest blokowany przez hasło.
8. Nie rób przelewów ani nie loguj się do bankowości elektronicznej na urządzeniach dostępnych w miejscach publicznych.
9. Po zakończonej sesji wyloguj się, zamknięcie przeglądarki nie wystarczy.
10. Włącz weryfikację dwuetapową, która jest dodatkowym zabezpieczeniem polegającym na wpisywaniu kodu wysłanego SMS-em.
11. Pamiętaj o aktualizowaniu oprogramowania antywirusowego. Jeśli masz z tym kłopot – poproś bliskiego o pomoc.
12. Nie klikaj w reklamy pojawiające się na pulpicie lub w przeglądarce.
13. Nie podawaj swoich danych osobowych w odpowiedzi na nieznane wiadomości e-mail lub SMS.
14. Nie wierz we wszystko, co widzisz i słyszysz – sztuczna inteligencja fabrykuje obrazy i wideo.
15. Bądź czujny i stosuj zasadę ograniczonego zaufania.
16. Nie daj się wyprowadzić z równowagi, kiedy oszuści straszą konsekwencjami (utratą zdrowia, życia czy funduszy) lub kuszą niepowtarzalną okazją i ceną.

UWAGA NA FAKESHIPPING POD

Internet stał się miejscem, gdzie coraz częściej robimy zakupy. Jest to rozwiązanie wygodne i często tańsze niż tradycyjne sklepy, jednak wraz z rozwojem handlu internetowego pojawiają się nowe zagrożenia. Seniorzy, podobnie jak wszyscy inni konsumenci, mogą paść ofiarą nieuczciwych sprzedawców. Powyższe zjawisko to fakeshipping [czyt. fejksziping], a jego nazwa pochodzi od *fake* – 'fałszywy' i *shipping* – 'wysyłka'. Dlatego przygotowaliśmy garść porad, które pomogą bezpiecznie poruszać się w świecie zakupów internetowych.

JAK ODRÓŻNIĆ NIEUCZCIWY SKLEP?

W Internecie funkcjonuje wiele różnych modeli sprzedaży. Jednym z nich są tradycyjne sklepy internetowe, które handlują swoim towarem. Coraz popularniejsze stają się modele, które opierają się na podobnej zasadzie, towar jednak nie jest wysyłany od sprzedawcy, tylko prosto z hurtowni lub od producenta. Najczęstszym przykładem takiego sposobu sprzedaży jest tzw. dropshipping (metoda realizacji zakupów). Jest to całkowicie legalny model, zgodnie z którym sprzedawca prowadzi oficjalny sklep internetowy i współpracuje z zaufanymi dostawcami, choć nie ma własnego magazynu. Co najważniejsze, bierze pełną odpowiedzialność za sprzedawany towar i dba o prawa klienta.

Zupełnie inaczej działa model, który nazwaliśmy fakeshippingiem (Izba Gospodarki Elektronicznej nazywa go pozornym dropshippingiem). To oczywiście nieuczciwy model sprzedaży. Sprzedawcy stosujący tę metodę tylko udają polskie sklepy, a w rzeczywistości zamawiają w imieniu klienta produkty z krajów azjatyckich, najczęściej z Chin, i podają się za pośredników. Próbują przy tym unikać odpowiedzialności za towar i często utrudniają składanie reklamacji. To właśnie przed takimi nieuczciwymi praktykami chcemy przestrzec.

NA CO SZCZEGÓLNIE UWAŻAĆ?

Pierwszym sygnałem ostrzegawczym są wyjątkowo niskie ceny. Jeśli jakiś produkt kosztuje znacznie mniej niż w innych sklepach, powinno to wzbudzić naszą czujność. Pamiętajmy, że żaden uczciwy sprzedawca nie będzie sprzedawał towaru ze stratą.

Kolejną rzeczą, na którą warto zwrócić uwagę, jest brak polskiego adresu firmy. Każdy legalnie działający sklep internetowy ma obowiązek podać swój polski adres, numer telefonu oraz dane rejestrowe firmy, takie jak NIP, KRS czy

REGON. Jeśli brakuje tych informacji, lepiej zrezygnować z zakupów.

Warto też dokładnie czytać regulamin sklepu. Jeżeli znajdziemy informację, że sklep jest tylko „pośrednikiem", a towar wysyła „zewnętrzny dostawca", najprawdopodobniej mamy do czynienia z fakeshippingiem.

JAKIE SĄ ZAGROŻENIA ZWIĄZANE Z FAKESHIPPINGIEM?

Kupując w nieuczciwym sklepie, narażamy się na wiele problemów. Przede wszystkim nasze dane osobowe trafiają poza Unię Europejską, gdzie nie chronią ich europejskie przepisy RODO. Oznacza to, że mogą zostać wykorzystane w sposób, którego sobie nie życzymy.

Problemy pojawiają się też z samą przesyłką. Czas oczekiwania na towar może się wydłużyć nawet do kilku miesięcy, a nierzadko nigdy do nas nie dociera. W wielu przypadkach musimy uregulować dodatkowe opłaty celne i podatki. Istnieje też duże ryzyko otrzymania podróbki zamiast oryginalnego produktu.

Największe problemy pojawiają się jednak w momencie, gdy chcemy złożyć reklamację lub zwrócić towar. W przypadku fakeshippingu może się okazać, że zostaniemy odesłani do sprzedawcy z Azji i to z nim będziemy musieli załatwiać wszystkie sprawy związane z reklamacją. W takiej sytuacji brak znajomości języka chińskiego może być najmniejszym z potencjalnych problemów. Już samo odesłanie towaru może być droższe niż sam towar.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

CZAS ZAKUPÓW W INTERNECIE

BEZPIECZNE ZAKUPY W MEDIACH SPOŁECZNOŚCIOWYCH

Osobny rozdział należy poświęcić zakupom przez portale społecznościowe, takie jak Facebook czy Instagram. Tutaj ryzyko oszustwa jest szczególnie wysokie, ponieważ platformy te nie posiadają zabezpieczeń typowych dla profesjonalnych sklepów internetowych. Trudno też zweryfikować prawdziwego sprzedawcę, a w razie oszustwa praktycznie niemożliwe jest odzyskanie pieniędzy.

Jeśli jednak zdecydujemy się na zakupy w mediach społecznościowych, warto stosować kilka podstawowych zasad bezpieczeństwa. Kupujmy tylko od sprzedawców, którzy mają dużo pozytywnych opinii od innych klientów. Unikajmy przedpłat na konto, wybierajmy opcję płatności przy odbiorze. W ten sposób minimalizujemy ryzyko oszustwa.

ZASADY BEZPIECZNYCH ZAKUPÓW

Przed dokonaniem zakupu zawsze warto poświęcić chwilę na sprawdzenie sprzedawcy. Poszukajmy w Internecie opinii o sklepie, sprawdźmy, czy adres strony zaczyna się od „https://", dokładnie przeczytajmy regulamin. Jeśli mamy jakiekolwiek wątpliwości, skonsultujmy się z rodziną lub znajomymi.

Podczas robienia zakupów pamiętajmy o zachowywaniu wszelkich potwierdzeń i dokumentacji. Zapisujmy lub drukujmy potwierdzenia zamówień, róbmy zrzuty ekranu ofert, zachowujmy korespondencję ze sprzedawcą. Te materiały mogą okazać się bezcenne w przypadku ewentualnych problemów.

CO ZROBIĆ, GDY PADLIŚMY OFIARĄ OSZUSTWA?

Jeśli mimo zachowania ostrożności zostaliśmy oszukani, najważniejsze jest szybkie działanie. W pierwszej kolejności należy skontaktować się ze swoim bankiem – czasem możliwe jest jeszcze zablokowanie przelewu. Następnie powinniśmy zgłosić sprawę na policję i zachować wszystkie dowody oszustwa.

Warto też skorzystać z pomocy miejskiego lub powiatowego rzecznika konsumentów lub doświadczonej organizacji konsumenckiej oraz powiadomić rodzinę o zaistniałej sytuacji.

PAMIĘTAJ!

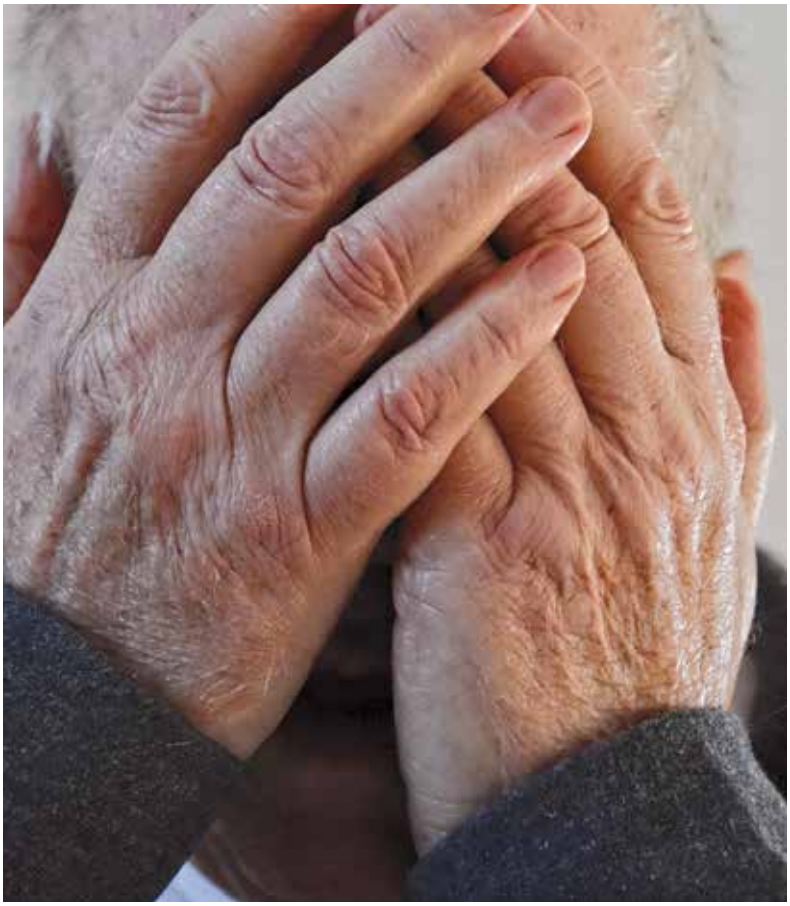
Zakupy w Internecie mogą być bezpieczne, jeśli zachowamy odpowiednią ostrożność. Nie dajmy się zwieść wyjątkowo niskim cenom ani naciskom na szybką decyzję. Kierujmy się zasadą ograniczonego zaufania i pamiętajmy, że nasze bezpieczeństwo jest ważniejsze niż okazja cenowa. A przede wszystkim nie wstydźmy się prosić o pomoc. Jeśli coś wzbudza nasze wątpliwości lub nie jesteśmy pewni, jak postąpić, zawsze możemy zwrócić się do młodszych członków rodziny lub zaufanych znajomych.

Jako Stowarzyszenie Ochrony Konsumentów „Aquila" na bieżąco monitorujemy działalność sklepów internetowych i pracujemy nad narzędziami, które ułatwią bezpieczne zakupy. Mamy nadzieję, że już wkrótce przedstawimy wam wyniki naszych działań.

MAŁGORZATA MIŚ
PREZES STOWARZYSZENIA OCHRONY KONSUMENTÓW „AQUILA"

OSZUSTWO NA WCZEŚNIEJSZĄ EMERYTURĘ

Seniorzy czekają na podwójną waloryzację emerytur i rent, ale najwcześniej dojdzie do niej najprawdopodobniej dopiero w 2026 roku. Jak zapowiedział rząd, świadczenia wzrosną, jednakże podwyżka będzie mniej znacząca niż w poprzednich dwóch latach. Z prognoz wynika, że w przyszłym roku waloryzacja wyniesie 5,52%, a zatem najniższa emerytura wyniesie 1879,27 złotych (dzisiaj jest to 1780,96 złotych). Dezinformację związaną z kwestią podwójnej waloryzacji wykorzystują oszuści, którzy podejmują próby wyłudzenia danych osobowych w zamian za rzekomą wcześniejszą wypłatę świadczenia.



Oszuści oferują pomoc przy wypełnianiu wniosku, co już powinno wzbudzić nasze podejrzenia. Pracownicy ZUS nie składają telefonicznych i osobistych propozycji pomocy ani płatnego, ani darmowego wypełnienia wniosku. Również nie odwiedzają emerytów i rencistów w ich miejscu zamieszkania. Seniorzy mogą spodziewać się takiej wizyty tylko w dwóch przypadkach: z okazji setnych urodzin oraz gdy ubiegają się o rentę z tytułu niezdolności do pracy lub świadczenie uzupełniające dla osób niezdolnych do samodzielnej egzystencji, a ich stan zdrowia nie pozwala na przeprowadzenie badania w placówce ZUS-u.

Warto również pamiętać, że przede wszystkim nie trzeba wypełniać żadnych wniosków, aby dodatkowa emerytura oraz środki po waloryzacji wpłynęły na konto. Podobnie jest w przypadku świadczenia honorowego dla stulatków, które wynosi 6246,13 złotych i również będzie podlegało waloryzacji. Każde wprowadzenie takich dodatków stwarza oszustom idealną okazję do podejmowania próby wyłudzenia danych osobowych i pieniędzy.

Seniorze – nie wpuszczaj do domu nieznajomych osób. Jeżeli ktoś podaje się za pracowników ZUS-u, zadzwoń do najbliższej placówki zakładu i zapytaj o zgodność danych. W przypadku rozmowy telefonicznej rozłącz się i zawiadom rodzinę oraz policję.

FAŁSZYWA STRONA ZUS-U

W przypadku emerytur oszuści nie ograniczają się jedynie do tradycyjnych metod. Z pomocą sztucznej inteligencji stworzyli fałszywą stronę internetową ZUS-u i ukradli tożsamość, by założyć na Facebooku łudząco podobny profil placówki. To właśnie na nim pojawiły się reklamy zachęcające do inwestycji, która miałaby zagwarantować emeryturę już w wieku 50 lat. Zgodnie z treścią posta wystarczyło zainwestować 1000 złotych. Oszuści wykorzystali nawet wizerunek byłej prezes ZUS – prof. Gertrudy Uścińskiej, która została odwołana na początku roku. W tym przypadku schemat działania jest podobny. Ofiara, skuszona możliwością wcześniejszej emerytury, klika w link zamieszczony na profilu na portalu społecznościowym. Zostaje przekierowana na fałszywą stronę ZUS-u, gdzie wypełnia formularz i robi przelew. Tym sposobem hakerzy przejmują jej dane i środki na koncie.

Przypominamy – nie klikaj w podejrzane linki i nie pobieraj załączników niewiadomego pochodzenia. Fałszywi pracownicy ZUS-u tylko chcą wyłudzić informacje, a następnie pozbawić cię oszczędności życia.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA URZĄD SKARBOWY I APLIKACJĘ mObywatel

W ostatnim czasie oszuści wyłudzają cenne dane osobowe z wykorzystaniem fałszywego profilu elektronicznej wersji Urzędu Skarbowego. Cyfrowy Urząd Skarbowy ułatwia załatwianie wielu spraw bez wychodzenia z domu. Niestety powszechność takiego rozwiązania wykorzystują cyberprzestępcy.

Chociaż podatek w Polsce rozliczaliśmy kilka dobrych miesięcy temu, oszustom nie przeszkadza to w powoływaniu się na Urząd Skarbowy. Wielu podatników wciąż dostaje niepokojące wiadomości SMS lub e-mail o treści: „Masz bezpieczną wiadomość dotyczącą Twojego podatku dochodowego od osób fizycznych za rok 2023, wejdź na stronę https://login-gov-pl.surge.sh/-dTH=0CGuJetzHV, aby ją przeczytać i zabezpieczyć uwierzytelnienie przy użyciu swojego profilu zaufanego". Już na pierwszy rzut oka adres strony wygląda podejrzanie.

JAK USTRZEC SIĘ PRZED OSZUSTWEM?

Oszuści nie dość, że kradną tożsamość, to posługują się metodą phishingu. Zachęcają do otworzenia niebezpiecznego linku pod przykrywką uwierzytelnienia wiadomości z użyciem Profilu Zaufanego w aplikacji mObywatel lub na stronie internetowej. Link przenosi ofiarę do fałszywej strony, na której znajduje się formularz do wprowadzenia danych niezbędnych do logowania.

Po otrzymaniu podobnej wiadomości najlepiej nie klikać w link. Jeśli nawet przez przypadek trafisz na zewnętrzną stronę, pod żadnym pozorem nie podawaj żadnych informacji i natychmiast zamknij stronę. Po takim incydencie warto przeskanować urządzenie zaktualizowanym programem antywirusowym, by sprawdzić, czy nie wkradł się wirus.

W przypadku wpisania danych osobowych i haseł, zmień te informacje jak najszybciej. Włącz również uwierzytelnianie dwuskładnikowe na wszystkich kontach. Uzyskanie dostępu do Profilu Zaufanego pozwala oszustom na wgląd w szczegółowe dane z rządowego rejestru, a co za tym idzie – na składanie wniosków lub zmianę poleceń w imieniu okradzionej osoby.

JAK ZABEZPIECZYĆ APLIKACJĘ MOBYWATEL?

Próba kradzieży danych osobowych albo zgubienie telefonu, na której zainstalowałeś aplikację mObywatel, może przysporzyć wielu kłopotów. Jeżeli dojdzie do takiej sytuacji, dobrze jest aktywować aplikację na innym urządzeniu – dzięki temu dotychczasowa wersja przestanie być aktywna i nikt nie zobaczy zawartych w niej informacji.

Konto na stronie mObywatel można zablokować również po zgłoszeniu sprawy na infolinii pod numerem 42 253 54 74.

Tym sposobem wykwalifikowany pracownik zweryfikuje prośbę i poinstruuje, co zrobić, by dokumenty przestały być widoczne na zgubionym bądź skradzionym telefonie.

Warto wiedzieć, że mObywatel umożliwia zgłaszanie podejrzanych wiadomości SMS i e-mail, złośliwe reklamy czy fałszywe strony internetowe. Jak zgłosić incydent?

- Uruchom aplikację mObywatel i zaloguj się do niej.
- W sekcji „Usługi" wybierz pozycję „Bezpiecznie w sieci".
- Po przejściu do zakładki możesz włączyć powiadomienia o zagrożeniach i zgłosić podejrzaną stronę czy wiadomość.
- Wybierz kategorię oszustwa i postępuj zgodnie z poleceniami na ekranie. Instrukcje mogą się różnić w zależności od rodzaju zgłoszenia.

OSZUSTWO NA LEGENDĘ

Oszustwa na legendę to przestępstwa, w których oszust podszywa się pod kogoś, kim nie jest. Najbardziej popularną metodą jest oszustwo na wnuczka – rzekomy członek naszej rodziny potrzebuje sporej kwoty, by pokryć różne zobowiązania. Jak to działa w praktyce? Oszust dzwoni do potencjalnej ofiary i mówi, że spowodował wypadek i potrzebuje pieniędzy, by wpłacić kaucję. Jednakże w dobie sztucznej inteligencji stara metoda zyskała drugie życie i niestety jest bardziej skuteczna.

Do tej pory oszusta można było zdemaskować – najczęściej zdradzał go głos wcale niepodobny do głosu bliskiej osoby, za którą podawał się przestępca. Niestety rozwój sztucznej inteligencji pozwala na modelowanie głosu w tak dokładny sposób, że oszustwo na wnuczka stało się groźne jak nigdy dotąd.

Narzędzia do klonowania głosu dostępne są w Internecie już za kilkadziesiąt złotych za kilka minut nagrania. To wystarczy, by senior uwierzył, że naprawdę ma do czynienia z członkiem rodziny, który potrzebuje pomocy. Co więcej, oszust nie tylko może spreparować głos dowolnej osoby, ale także przygotować wideo z jej udziałem i wysłać do osoby starszej. Taka metoda jeszcze bardziej uwiarygadnia przekaz i wywołuje u seniora bardzo silne emocje, a te zaburzają zdolność logicznego myślenia.

W JAKIEJ SPRAWIE „WNUCZEK" DZWONI NAJCZĘŚCIEJ?

W przypadku tej metody oszuści zawsze mają jeden cel – wyłudzenie pieniędzy. W trakcie rozmowy przestępca unika rozmów uwzględniających dokładne szczegóły, ponieważ w przeważającej części ich nie zna: ani imienia babci/dziadka, ani imienia osoby, pod którą się podszywa. W jakim interesie rzekomi wnuczkowie dzwonią najczęściej?

- WYPADEK – złodziej opowiada historię o spowodowanym przez niego wypadku drogowym i mówi, że szybko potrzebuje pieniędzy, aby uniknąć konsekwencji.
- INWESTYCJA – rzekomy wnuk przekonuje, że pilnie potrzebuje określonej kwoty na inwestycję, która wkrótce się zwróci z ogromnym zyskiem.
- ZADŁUŻENIE – oszust mówi, że wziął pożyczkę, a nie ma pieniędzy na spłatę bieżącej raty kredytu.
- OPERACJA – podszywający się pod krewnego złodziej przekonuje, że musi poddać się poważnej operacji i natychmiast potrzebne są mu pieniądze na zabieg.
- OKUP – oszust podszywa się pod wnuczka lub syna i twierdzi, że został porwany i potrzebuje pieniędzy na okup. Jednocześnie wysyła sfałszowane wideo, na którym widać, jak ktoś go szarpie lub wiąże liną.

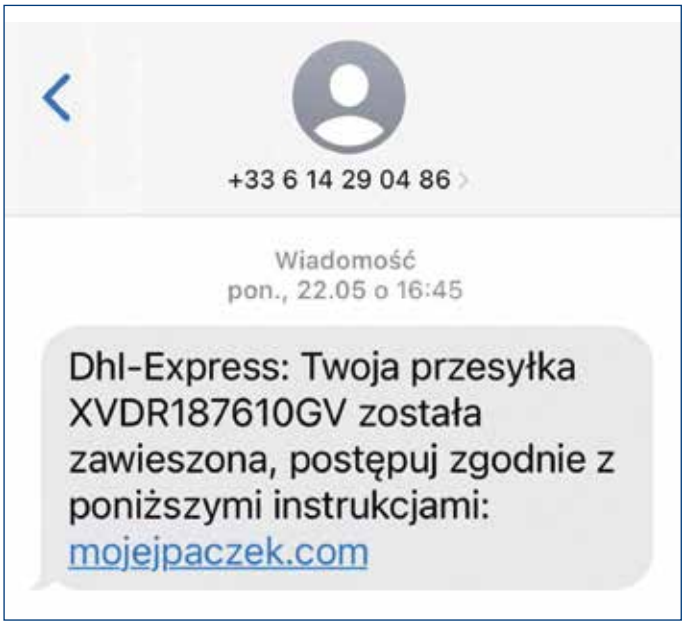
PAMIĘTAJ!

Nie ufaj osobom, które telefonicznie podają się za krewnych lub przyjaciół. Zawsze po otrzymaniu podejrzanego telefonu zadzwoń do prawdziwego członka rodziny, żeby potwierdzić informację. Jeśli nie rozpoznajesz głosu, odłóż słuchawkę. Oszuści wywierają silny nacisk i presję, bo mają doświadczenie w manipulowaniu ludźmi, więc im szybciej zakończysz rozmowę, tym lepiej. Charakterystyczne dla oszustw na wnuczka jest wysyłanie po pieniądze pośredników. Nigdy nie przekazuj pieniędzy nieznajomym! Jeżeli musisz przekazać pieniądze, rób to tylko osobiście. W trakcie rozmowy nigdy nie podawaj, ile gotówki masz przy sobie. Na koniec zgłoś sprawę na policję – nie wstydź się. Pamiętaj również, że metoda na legendę to nie tylko podszywanie się pod wnuczka. Zadzwonić może każdy: policjant, adwokat, córka czy sąsiad. Bądź czujny.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA PACZKĘ KURIERSKĄ I BLIK

Oszuści nie przestają podszywać się pod firmy kurierskie. Wciąż wysyłają SMS-y i wiadomości e-mail z informacją o konieczności dopłaty do przesyłki. Niekiedy przesyłają również komunikat, że odbiorca podał błędny adres, co uniemożliwia kurierowi doręczenie paczki. W treści znajduje się link, który przekierowuje ofiarę na stronę łudząco podobną do strony przewoźnika lub do bramki płatności. Inną metodą jest również wykorzystanie linków do pobrania aplikacji firmy kurierskiej.



Tym sposobem potencjalna ofiara wprowadza wrażliwe dane dotyczące konta bankowego, czyli login, hasło i PIN. Warto zachować ostrożność szczególnie w najbliższym czasie – zbliżają się święta Bożego Narodzenia i zapewne wiele osób zdecyduje się na internetowe zakupy, by wręczyć bliskim prezent pod choinkę. W szale świątecznych przygotowań możesz nawet nie zwrócić uwagi na to, że wiadomość jest podejrzana. Pamiętaj, czytaj treść dokładnie! Oszustwo na dopłatę do paczki kurierskiej to klasyczny przejaw phishingu (str. 9). Link podany w SMS-ie lub wiadomości e-mail prowadzi do niebezpiecznej domeny, na której oszuści domagają się danych osobowych i informacji o kartach płatniczych.

W niektórych przypadkach fałszywy nadawca nie każe nam klikać w link, tylko wypełnić luki w załączonym dokumencie. W rzeczywistości nie pobieramy załącznika, a program potrafiący przechwytywać loginy, hasła, wykonywać zrzuty ekranu, a nawet rejestrować to, które klawisze na urządzeniu naciskamy. Warto popatrzeć na listę odbiorców – jeżeli znajduje się na niej wiele osób, wzrasta ryzyko zagrożenia.

ODBIÓR PACZKI

Oszuści posługują się również tradycyjnymi metodami i przychodzą do domu ofiary. Rzekomy kurier informuje, że przywiózł paczkę zamówioną za pobraniem, a kwota najczęściej wynosi kilkaset złotych. Oczywiście na opakowaniu znajdują się nasze dane: imię, nazwisko i adres. Chociaż nic nie zamawialiśmy i nie znamy nawet nazwy firmy, wpuszczamy do siebie kuriera, który chce zadzwonić do firmy i wyjaśnić sytuację. Kurier pożycza nasz telefon, by skontaktować się z nadawcą. Zazwyczaj rozmowa trwa około minuty. Okazuje się, że przesyłka naprawdę trafiła do niewłaściwej osoby, po czym wychodzi, a my po jakimś czasie dostajemy rachunek na ogromną kwotę, bo kurier specjalnie wykonał drogie połączenie.

PŁATNOŚĆ BLIK-iem

Niejednokrotnie za zamówienie płacimy BLIK-iem. To szybka metoda płatności, która polega na przepisaniu kodu z aplikacji bankowej do zrealizowania transakcji. Niestety ta metoda również służy oszustom do okradania niczego nieświadomych seniorów. Jednym z najczęstszych sposobów jest podszywanie się pod bliską nam osobę, ponieważ w takiej sytuacji pożyczenie drobnej kwoty nie będzie wzbudzać podejrzeń. Wyłudzacz przesyła wiadomość, że potrzebuje pomocy, bo ma problem z opłaceniem zamówienia. Prosi też o podanie kodu BLIK z obietnicą, że wkrótce zwróci pieniądze. Często w grę wchodzą emocje i szybkość reakcji, dlatego osoba nie weryfikuje prawdziwej tożsamości oszusta. Jeśli przestępca roześle taką wiadomość do kilkunastu osób, może szybko się wzbogacić.

ZAPAMIĘTAJ!

Kiedy ktoś prosi Cię o kod BLIK, najlepiej zadzwoń do tej osoby. Zawsze sprawdzaj, komu wysyłasz kody do płatności mobilnych i nigdy nie przekazuj pieniędzy obcym. Nie podawaj szczegółowych danych przez telefon, nawet kiedy bank rzekomo ich wymaga. Przed potwierdzeniem transakcji BLIK sprawdź kilka razy, ile wynosi kwota i do kogo ona trafi.

OSZUSTWO NA ODSZKODOWANIE ZA KREDYT WE FRANKACH

Sprawa kredytu we frankach wciąż budzi wiele kontrowersji. Takie zobowiązanie zaciągnięte we frankach szwajcarskich miało przynieść o wiele więcej korzyści niż wzięcie kredytu w złotówkach. W 2015 roku kurs waluty poszybował w górę, przez co wysokość raty wzrosła dwukrotnie. Frankowicze zaczęli pozywać banki, w których wzięli kredyt, a za powód podawali wprowadzenie w błąd przez pracowników instytucji oraz samodzielne określenie kursu obcej waluty, co jest sprzeczne z powszechną praktyką.

Niestety trudną sytuację frankowiczów wykorzystują oszuści. Wysyłają wiadomości e-mail albo dzwonią z propozycją pomocy w uzyskaniu odszkodowania od banku, w którym rozmówca zaciągnął kredyt. Twierdzą, że za niewielką opłatą są w stanie rozwiązać problem finansowy. Kiedy zmanipulowania osoba wyraża zainteresowanie ofertą, oszuści proszą o podanie danych osobowych oraz dostęp do bankowości elektronicznej. Bardzo często przestępcy dobierają ofiary przypadkowo i nie wiedzą, czy dana osoba na pewno wzięła kredyt we frankach.

Innym sposobem jest informowanie o już przyznanym odszkodowaniu. Oszust dopytuje najpierw, czy na pewno nikt wcześniej nie zwrócił tych środków. W trakcie rozmowy fałszywy doradca próbuje wyciągnąć jak najwięcej szczegółów – nazwę banku, numer konta, imię i nazwisko, a także miejsce zamieszkania. Jeśli całkowicie zdobędzie zaufanie ofiary, może pozyskać informacje nawet na temat sposobu prowadzenia mediacji z bankiem albo przebiegu sprawy sądowej, w wyniku której kredyt miał zostać unieważniony. Wszelkie dane, o jakich dowie się sprawca, mogą być wykorzystane do wzięcia pożyczki lub zawarcia umowy kupna/sprzedaży albo najmu w imieniu ofiary.

Warto wiedzieć, że nie da się wywalczyć odszkodowania jedynie poprzez kontakt telefoniczny, ponieważ banki są zobowiązane do podtrzymywania drogi oficjalnej. Jeżeli decydują się na rozmowę przez telefon, muszą przeprowadzić obustronny proces weryfikacji tożsamości.

NA CO ZWRÓCIĆ UWAGĘ PODCZAS ROZMOWY TELEFONICZNEJ?

Senior powinien zwrócić uwagę, czy osoba po drugiej stronie słuchawki się przedstawiła. Na wypadek gdyby o tym zapomniała, warto jej przypomnieć, by podała dokładnie i wyraźnie swoje imię i nazwisko oraz nazwę firmy. Oczywiście nie wolno potwierdzać żadnych danych, które sugeruje fałszywy doradca. Najlepiej również dopytać, skąd wziął wszelkie informacje i nasz numer telefonu. Wtedy najczęściej oszust się rozłącza, bo obawia się zdemaskowania i zgłoszenia sprawy na policję.

WYSYŁANIE OFERT POPRZEZ E-MAIL

Oczywiście oszuści stosują także phishing (tzw. łowienie haseł) i rozsyłają niebezpieczne wiadomości e-mail ofertę, zgodnie z którą frankowicz nie musi występować o odszkodowanie do sądu, a otrzyma gotówkę od rzekomej firmy od ręki. Żeby poznać więcej informacji, potencjalna ofiara musi udostępnić swoje dane adresowe i często również umowę z bankiem. Innym razem fałszywi konsultanci obiecują bezpłatne negocjowanie ugody z bankiem. Wszystko po to, by wyłudzić dane, które następnie są przez nich wykorzystywane albo sprzedawane w ciemnej stronie Internetu (tzw. Darknet).

GDZIE ZGŁOSIĆ SPRAWĘ?

Podejrzane telefony oraz wiadomości SMS czy e-mail można zgłaszać pod adresem pod numerem 8080 lub na stronie **https://incydent.cert.pl/**, na której trzeba wypełnić formularz, załączyć wiadomość i wysłać do zweryfikowania.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA „NIE JESTEM ROBOTEM"

Wyobraźnia cyberprzestępców nie przestaje zaskakiwać. Do kolejnych sposobów phishingu dołączyło oszustwo, które polega na sfałszowaniu systemu weryfikacji użytkownika CAPTCHA. Choć nazwa może brzmieć obco, jako użytkownicy Internetu spotykamy się z nią niemal codziennie. Mowa o potwierdzeniu pojawiającym się na wielu stronach internetowych, że nie jesteśmy robotami.

Sama prośba o potwierdzenie, że użytkownik jest człowiekiem, nie wzbudzi w ofierze podejrzeń, bo to częste rozwiązanie stosowane przez wielu sprzedawców. Takie działanie chroni dany serwis przed niepożądanymi treściami czy botami, które zostawiają niezweryfikowane opinie, a te z kolei mogą wpłynąć negatywnie na wizerunek sklepu. Najczęściej polega to na zaznaczeniu okienka obok hasła „Nie jestem robotem", a następnie wykonaniu prostego testu zgodnie z poleceniem „Wybierz wszystkie obrazki, na których są (...)". W przeważającej części są to zdjęcia ukazujące sygnalizację świetlną, motocykle czy rowery. Zdarza się również, że weryfikacja jest równoznaczna z przepisaniem zniekształconego wyrazu do odpowiedniego pola.

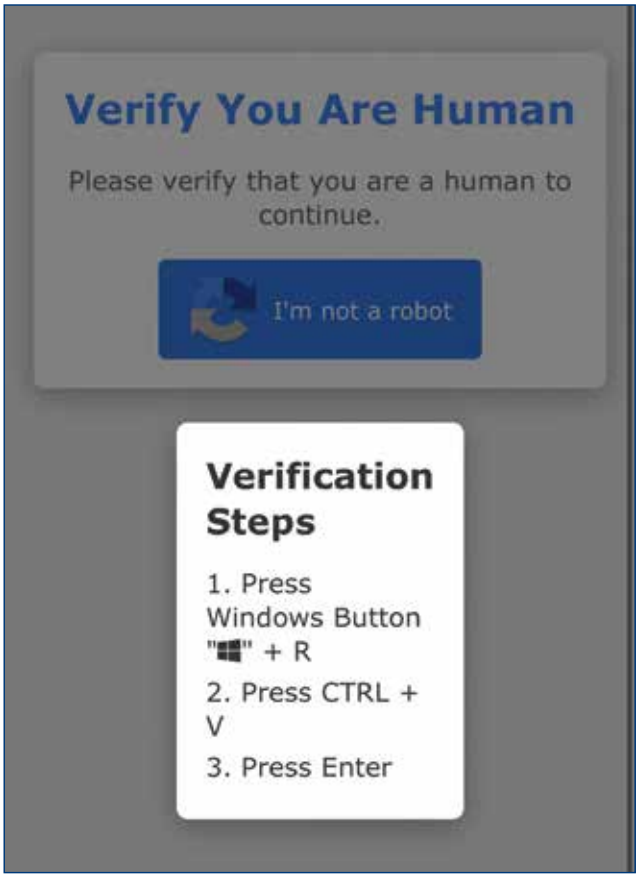
Fałszywy komunikat na ogół nie dotyczy sprawdzonych i godnych zaufania stron. Jak już wiadomo, w Internecie pojawia się mnóstwo reklam oferujących fałszywe inwestycje czy podejrzane produkty w niewiarygodnie niskich cenach i najczęściej kierują one użytkownika na zewnętrzną stronę. W takim przypadku oszuści stosują dowolne chwyty, byle tylko zdobyć dane i pieniądze potencjalnej ofiary. I najczęściej w takich niesprawdzonych zakamarkach Internetu cyberprzestępcy podszywają się pod system weryfikacji CAPTCHA.

ZAZNACZANIE OKIENEK NIE WYSTARCZY

W przypadku tego oszustwa przepisywanie ciągu znaków i wybieranie odpowiedniej sekwencji obrazków nie wystarcza. Kiedy ofiara wejdzie na fałszywą stronę, wyświetli się jej opcja weryfikacji, jednakże okienko będzie się różniło od tego, które pojawia się zazwyczaj. Pod hasłem „Nie jestem robotem" pojawi się polecenie wymagające naciśnięcia kombinacji klawiszy Windows (na dole po lewej stronie klawiatury – ikonka okna) i R. W kolejnym kroku trzeba użyć skrótu CTRL + V (czyli komenda „kopiuj"), a na końcu wcisnąć Enter, żeby zatwierdzić działanie. Po takiej czynności uruchamia się kod, który zostaje automatycznie skopiowany przez fałszywą stronę internetową. Umożliwia to cyberprzestępcom zainstalowanie złośliwego oprogramowania na naszym komputerze lub telefonie.

Tym sposobem oszuści mogą wejść w posiadanie wszelkich danych osobowych, haseł, loginów, odczytywać zawartość ekranu. Nie ma bezpośredniego sposobu na to, by ochronić się przed powyższym atakiem – kluczem jest ostrożność, świadomość i edukacja.

NA PRAWDZIWEJ STRONIE PO ZAZNACZENIU OPCJI „NIE JESTEM ROBOTEM" WYŚWIETLI SIĘ SEKWENCJA OBRAZKÓW DO WYBORU. CZASAMI WYSTARCZA TYLKO PIERWSZY KROK, BY PRZEJŚĆ DO STRONY.



NA SFAŁSZOWANEJ STRONIE PO ZAZNACZENIU OPCJI „NIE JESTEM ROBOTEM" WYŚWIETLI SIĘ DODATKOWE POLECENIE, ZGODNIE Z KTÓRYM UŻYTKOWNIK MA NACISNĄĆ OKREŚLONĄ KOMBINACJĘ KLAWISZY. JEŚLI ZOBACZYSZ TAKĄ KOMENDĘ, NATYCHMIAST WYJDŹ ZE STRONY.

OBEJRZYJ SPOTY „STOP MANIPULACJI – NIE DAJ SIĘ OSZUKAĆ"

W ramach kampanii „Stop manipulacji – nie daj się oszukać" Stowarzyszenie MANKO – Głos Seniora nagrało 4 spoty edukacyjne. Forma krótkich treściwych filmików bardzo dobrze się przyjęła wśród naszych odbiorców. Spoty szybko rozeszły się po Internecie, a ich oglądalność dobiła do 155 tysięcy wyświetleń!

Spot kampanii społecznej „Stop manipulacji, nie kupuj na prezentacji" poruszył bardzo ważny problem popularności nieetycznych pokazów handlowych. Podczas oszukańczych prezentacji seniorzy są naciągani na kupno produktów niewartych swojej ceny lub na wzięcie pożyczek, których spłata ciągnie się latami. W spocie wzięli udział ambasadorzy Głosu Seniora: Marek Pilch, DJ Wika, Barbara Maciejewska i Hanna Piekarska.

Na temat zaproszeń na prezentację sprzedażową pod pretekstem wygranej sprzętu medycznego nagraliśmy także spot z gościnnym udziałem ambasadora Zdzisława Wasiaka – króla III edycji Sanatorium Miłości. Spot jest dostępny również w języku migowym.

Kolejny spot z DJ Wiką w roli głównej dotyczył fałszywych wiadomości SMS i e-mail, które w ostatnich latach wręcz zalały Polaków. Ambasadorka przestrzegła przed podejrzanymi komunikatami o rzekomych niedopłatach za prąd, mandat, podatek czy paczkę kurierską.

Dużym problem zwłaszcza wśród samotnych seniorów jest oszustwo na amerykańskiego żołnierza. Dzięki miłym słówkom i rzewnym opowieściom manipulują starszymi kobietami, które w efekcie przelewają oszustowi swoje oszczędności. W spocie pod tytułem „Amerykański żołnierz mówi «Kocham cię»" wystąpili ambasadorzy Jagoda Bogusiewicz i Wojciech Kałkusiński.

Spoty można obejrzeć na naszym kanale Głos Seniora TV – **www.youtube.com/@GlosSenioraTV** oraz pod linkami:

- **https://www.youtube.com/watch?v=4rrvmolztsA**
- **https://www.youtube.com/watch?v=NAqnF0quCpk**
- **https://www.youtube.com/watch?v=-S-tzZ7ZUW8**
- **https://www.youtube.com/watch?v=V_ygLetIxjA**

Stop manipulacji, nie daj się oszukać! - spot promocyjny z DJ Wiką z językiem migowym

STOWARZYSZENIE MANKO W PROGRAMIE „INTERWENCJA"

Starsze małżeństwo z Warszawy zostało oszukane przez komis z Tomaszowa Lubelskiego. Seniorzy kupili samochód, aby ułatwić sobie opiekę nad synem z niepełnosprawnością, jednak pojazd zepsuł się już w drodze powrotnej. Mimo że właściciel zobowiązał się pokryć koszty naprawy, słuch po nim zaginął. Sprawą zainteresował się Polsat – do programu „Interwencja" jako eksperta zaproszono między innymi prezesa Stowarzyszenia MANKO Łukasza Salwarowskiego.

Rodzina miała pojechać nowym samochodem do sanatorium w Darłówku. Potrzebowała większego auta, po tym jak poprzednie się zepsuło. Niestety właściciel komisu zataił wiele informacji: przede wszystkim samochód był powypadkowy. Po przejechaniu 50 kilometrów zapaliły się kontrolki, zagotował się akumulator i wylał kwas. Początkowo właściciel chciał pomóc, ale kiedy pojawiły się kolejne usterki, przestał odbierać telefon.

Niestety to jedno z wielu rodzajów oszustw, które spotykają łatwowiernych seniorów. Prezes Łukasz Salwarowski podkreśla, że w dobie coraz to nowszych sposobów na oszustwa, trzeba być szczególnie czujnym:

– To nieuczciwe i manipulacyjne zachowanie, przykład na wykorzystywanie słabości konsumenta. Sprzedawca ma obowiązek naprawić, zmniejszyć cenę albo oddać całość wpłaconej kwoty.

W ramach kampanii „Stop manipulacji – nie daj się oszukać" Stowarzyszenie MANKO uczula na wszelkie podejrzane zachowania i szerzy wiedzę na temat podstępnych technik manipulacji. Więcej informacji na temat naszych działań znajdziecie na stronie **www.gloseniora.pl**. Bądźcie na bieżąco.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

AMERYKAŃSKI ŻOŁNIERZ MÓWI „KOCHAM CIĘ"

Oszustwo na amerykańskiego żołnierza lub weterana wojennego jest jedną z powszechniejszych metod, jeśli chodzi o sposoby oszukiwania za pośrednictwem mediów społecznościowych i wszelkich komunikatorów.

Oszust wyszukuje w sieci samotne osoby i nawiązuje z nimi kontakt. W tym przypadku podaje się za amerykańskiego żołnierza, który kończy służbę i jako osoba samotna – często wdowiec – szuka prawdziwej miłości. Ma polskie korzenie, więc na starość chce się przenieść się do Polski, gdzie u boku ukochanej spędzi jesień swojego życia. Posługuje się fałszywymi zdjęciami, które przedstawiają silnego mężczyznę w kwiecie wieku.

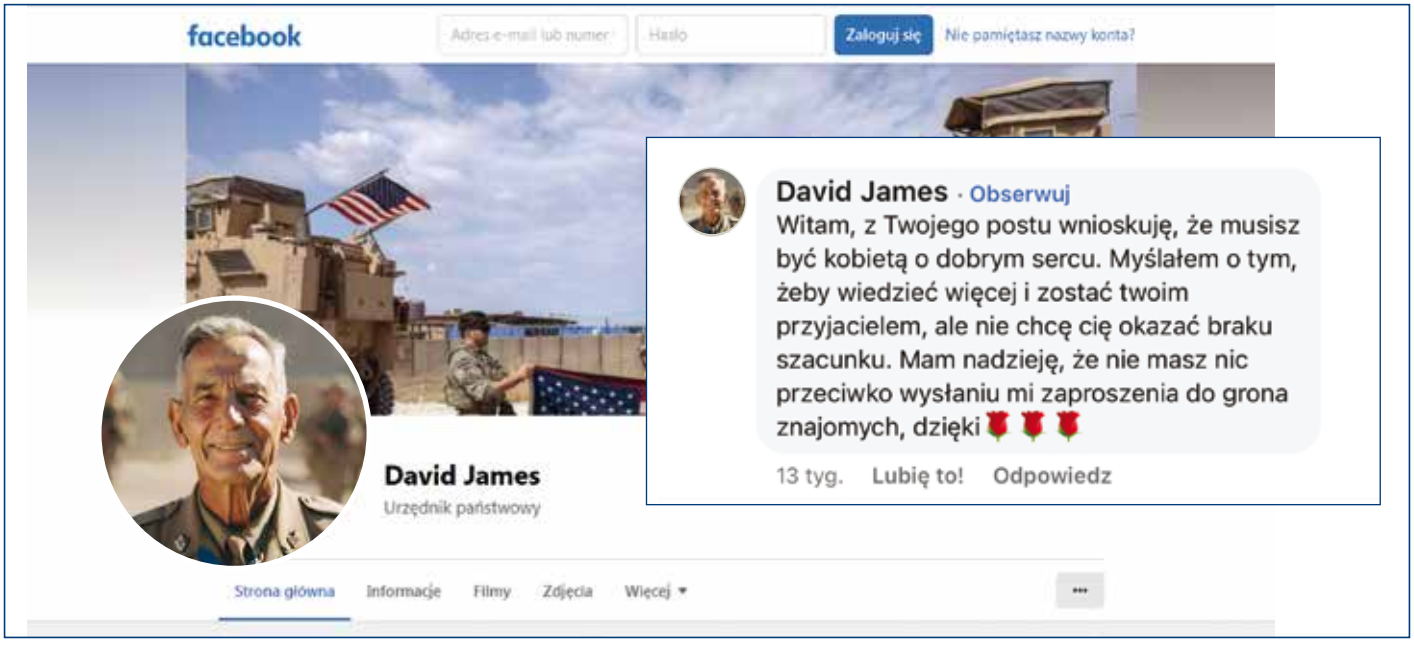
Rozmowy trwają nawet miesiącami. W tym czasie oszust zdobywa zaufanie i sympatię ofiary. Opowiada o swoim życiu – historie są łzawe i wzbudzają litość – oraz przesyła zdjęcia, a z czasem decyduje się na wyznanie sympatii, przyjaźni i wreszcie miłości. Następnie prosi o pomoc finansową na zakup biletu lub bardzo drogie leczenie. Gdy ofiara oszustwa prześle pieniądze na konto przestępcy, zostaje i bez ukochanego, i bez pieniędzy. Ostatnio pojawiły się także oszustki podające się za lekarki z amerykańskiej armii. Te z kolei wyłudzają pieniądze od mężczyzn.

„Żołnierze z Ameryki" mają różne metody wyłudzania pieniędzy. Jednym razem ukochany wysyła paczkę z kosztownościami, po czym ofiara dostaje fałszywy telefon z granicy, że trzeba opłacić cło, a następnym – żołnierz został ranny podczas ostatniej akcji lub uległ wypadkowi i potrzebuje pomocy finansowej. Oczywiście istnieje wiele możliwości, aby wykorzystać szantaż emocjonalny. Niektórzy oszuści podający się za żołnierzy opowiadają nieprzyjemne historie i wysyłają zdjęcia z pola walki, co wzbudza litości i chęć pomocy. Tym sposobem najczęściej to kobiety niejednokrotnie tracą oszczędności swojego życia.

Żołnierz to niejedyny zawód, na który powołują się przestępcy. W październiku mieszkanka powiatu cieszyńskiego straciła 50 tysięcy złotych, ponieważ chciała opłacić powrót amerykańskiego lekarza pracującego w Niemczech. Oszust przekonał ją, że jego aktywa są zamrożone i potrzebuje pomocy. To przykłady tzw. oszustw nigeryjskich – przestępcy na portalach społecznościowych, randkowych i aukcyjnych zawierają znajomość z przypadkowymi osobami, by zdobyć ich zaufanie, a następnie wyłudzić pieniądze za pomocą technik manipulacji.

JAK NIE DAĆ SIĘ ZWIEŚĆ?

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



TELEFON Z ZAGRANICY

W dalszym ciągu tradycyjne oszustwa telefoniczne nie tracą na popularności, ale oszuści wykorzystują dodatkowo aplikację WhatsApp. Jak już wiadomo, przestępcy mogą wykorzystywać specjalne programy do wykonania anonimowego połączenia lub przypisania danego numeru do numeru zupełnie innej osoby. Trzeba również uważać na nieznane numery. W wielu przypadkach mogą kontaktować się z tobą oszuści z zagranicy. Zachowaj szczególną ostrożność!

Odebranie lub oddzwonienie może kosztować kilka, a nawet kilkadziesiąt tysięcy złotych. Masz rodzinę za granicą i często rozmawiacie przez telefon? Na pewno już kojarzysz numer bliskiej osoby, ale nadal musisz być czujny. Zagraniczny numer, który się wyświetla na ekranie smartfona jest bardzo długi, ale często jego początek może wyglądać na znajomy numer z Polski. Oszuści specjalnie tak dobierają zagraniczne numery, aby wyglądały jak polskie numery kierunkowe (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 – w rzeczywistości połączenie już trwa, a kosztowne sekundy są naliczane.

JAK WYGLĄDA SCHEMAT DZIAŁANIA OSZUSTÓW?

Przestępcy zwykle dzwonią w nocy. Przychodzący numer najczęściej to tzw. głuchy telefon, który trwa bardzo krótko. Oszuści wykonują połączenia z numerów międzynarodowych na polskie numery w nadziei, że adresat tych połączeń automatycznie oddzwoni na ich numer. W ten sposób wykorzystują naturalną skłonność abonentów do oddzwaniania na nieodebrane połączenia. Podstawą działania oszustów jest nieuwaga użytkowników. Ze względu na połączenie międzynarodowe naliczają się bardzo wysokie opłaty. Kiedy oddzwonimy na taki numer, usłyszymy sygnał rozłączenia. Warto pamiętać, że dopóki sami nie naciśniemy symbolu czerwonej słuchawki, połączenie trwa, a operator nalicza wysokie opłaty. Ofiara odkłada telefon, myśląc, że rozmowa została zakończona, tymczasem opłaty naliczają się nawet przez następne kilka godzin. W konsekwencji nieświadoma niczego osoba może zapłacić nawet kilkadziesiąt tysięcy złotych!

NA CO ZWRÓCIĆ UWAGĘ?

Gdy zobaczysz, że ktoś dzwonił z nieznanego i długiego numeru – policz cyfry. Zwróć uwagę na początek, jeśli jest inny niż **+48** i numer ma więcej niż 9 cyfr (lub 11 z prefiksem), nie oddzwaniaj i nie pisz SMS-a. Najlepiej zignoruj takie połączenie. Spodziewasz się telefonu z zagranicy, ale wyświetlany numer wydaje się zadziwiająco długi? Mimo wszystko nie odbieraj i spróbuj skontaktować się z rodziną za pośrednictwem komunikatora. Pamiętaj również, że w dowolnym momencie możesz sprawdzić numer w Internecie. Użytkownicy często wypisują podejrzane numery i oznaczają, w jakim celu rozmówca nawiązywał kontakt. Włącz u swojego operatora sieci komórkowej wszelkie blokady dotyczące nieznanych numerów. W wielu smartfonach automatycznie jest wprowadzona funkcja, która podświetla podejrzane połączenia na czerwono i podpisuje jako SPAM.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA DOFINANSOWANIE I DOTACJĘ

Jak już wiemy, zakupy przez Internet stały się codziennością, również dla wielu seniorów. Nie bez powodu – nie trzeba dźwigać ciężkich toreb, a same produkty bywają o wiele tańsze niż w sklepach stacjonarnych. Oszuści wykorzystują tę sytuację i próbują naciągnąć osoby starsze na zakup produktów w kuszącej cenie. O nieuczciwych sprzedawcach internetowych pisaliśmy na stronach 22–23. Jednakże tym razem w grę wchodzą fałszywe dofinansowania oraz dotacje.

Jak działają oszuści? Po zakupie w Internecie suplementów, leków, witamin czy innych wyrobów medycznych po naprawdę okazjonalnej cenie zostaje dostarczona paczka bez żadnej instrukcji obsługi ani ulotki. Senior korzysta z zakupionej rzeczy i po jakimś czasie odzywa się do niego rzekomy przedstawiciel firmy, w której nabył dany produkt. Oszust informuje, że jeżeli klient nie zamówi u nich kolejnego egzemplarza zakupionego wcześniej produktu, będzie musiał płacić wysoką karę. Jak wmawia sprzedawca, poprzednim razem klient zamówił dofinansowany produkt, ale warunkiem podtrzymania tak niskiej ceny było wykupienie całej kuracji lub serii.

Zasłaniają się regulaminem, który kupujący podpisał, a tym samym – zgodził się na warunki. Innym wytłumaczeniem jest zrzucenie winy na zagranicznego producenta. Kiedy senior zażąda przedstawienia regulaminu, oszuści nagle zbijają pierwotnie wywołaną cenę. Nie daj się nabrać! Te „dofinansowane" wyroby w rzeczywistości można dostać w aptece za kilkanaście złotych.

CO Z DOTACJĄ?

Idea aktywizacji zawodowej po 60 roku życia jest niezmiernie ważna i pokazuje również, że nigdy nie jest za późno na spełnianie marzeń. Przy otwieraniu własnego biznesu nie brakuje przeszkód, ale i wsparcia ze strony instytucji, które oferują dotacje. Niestety ten obszar również stał się polem do popisu dla oszustów. Wiele osób decyduje się na pomoc profesjonalnych doradców, by ominąć zawiłości urzędowej mowy. Jednakże w Internecie pojawili się fałszywi doradcy, którzy oferują sprzedaż już wypełnionych lub pustych dokumentów za niewielkie kwoty, co czyni ogłoszenie bardziej atrakcyjnym. Natomiast takie wnioski są ogólnodostępne i nie trzeba za nie płacić.

Kolejnym sposobem jest celowe błędne wypełnienie formularza – oszuści wpisują wyposażenie, które nie spełnia warunków dotacji, albo kopiują całe fragmenty z innych wniosków, co skutkuje plagiatem. Nieuczciwi doradcy niejednokrotnie powołują się na współpracę z Ministerstwem Funduszy i Polityki Regionalnej lub Polską Agencję Rozwoju Przedsiębiorczości. Jeszcze niedawno, podszywając się pod PARP, przesyłali fałszywe umowy z informacją o oczekiwaniu na wpłatę na wskazany numer konta pod pretekstem poręczenia albo zabezpieczenia wsparcia projektu przez agencję.

Podobny schemat działania może dotyczyć innych rodzajów dotacji, niekoniecznie związanych z zakładaniem firmy. Pamiętaj, czytaj dokładnie wiadomości e-mail i nie otwieraj podejrzanych załączników. Jeżeli ktoś oferuje pomóc w wypełnianiu wniosku, sprawdź, czy na Internecie nie znajdują się przykładowe wnioski.

FAŁSZYWY ZNAK TOWAROWY

Oszuści czyhają nie tylko na samotnych i schorowanych seniorów, ale także tych przedsiębiorczych, którzy mimo wieku emerytalnego nie przestają pracować, a nawet prowadzą własny biznes. Jak już wiadomo, jednym z oszustw jest sprzedawanie za drobne kwoty ogólnodostępnych wniosków o dotacje na firmę. Kolejnym sposobem oszukiwania właścicieli jest kradzież znaku towarowego.

Oszuści podszywający się pod pewne przedsiębiorstwo nawiązują kontakt z twoją firmą poprzez wiadomość e-mail, którą wysyłają na pocztę służbową. W treści znajduje się propozycja współpracy – wszystko wydaje się w porządku. Przedstawiciel fałszywej firmy jest miły i przekonujący, a przede wszystkim zależy mu na długotrwałej relacji biznesowej.

Zachwala tak samą firmę, jak i projekt, który w niedalekiej przyszłości ma zostać rozpoczęty. Oczywiście idea jest mu bardzo bliska, więc chce pomóc w realizacji. Kiedy potencjalna ofiara opowiada o przedsięwzięciu ze szczegółami, tym bardziej nalega na wspólne działanie. Zgadzasz się na zaproponowane warunki, podpisujesz wszystkie dokumenty i porozumienia. Początkowo współpraca nie budzi zastrzeżeń – oszust angażuje się w inicjatywę, proponuje kolejne pomysły, projektuje grafiki, konsultuje każdy krok. Mimo wszystko stawiacie na pierwotny program.

W momencie gdy wszystko wydaje się gotowe – logo, plakat czy hasło – okazuje się, że nie możesz wykorzystać żadnego z tych elementów. W trakcie procesu powstawania projektu oszust wszystko zastrzega, czyli zgłasza do Urzędu Patentowego RP znak patentowy i to jako swój pomysł. Tym sposobem zostajesz pozbawiony prawa do posługiwania się efektami autorskiego projektu. Za to fałszywy wspólnik może czerpać z nich korzyści majątkowe i szantażować cię, że jeśli nie przekażesz mu określonej kwoty zarobionej na projekcie, on poinformuje twoich kontrahentów o „kradzieży" pomysłu i znaku towarowego, który został zastrzeżony. Niestety Urząd Ochrony Konkurencji i Konsumentów nie weryfikuje zgłaszanych znaków.

NA CO ZWRÓCIĆ UWAGĘ PRZY NAWIĄZYWANIU WSPÓŁPRACY Z NIEZNANĄ FIRMĄ?

Przede wszystkim stosuj się do zasady ograniczonego zaufania. Zanim podpiszesz jakiekolwiek dokumenty, skontroluj potencjalnego współpracownika i firmę, której jest właścicielem. Poczytaj opinie w Internecie i dopytaj znajomych z branży, czy ktoś miał do czynienia z przedstawicielami wspomnianej firmy. Najlepiej weryfikuj nadawcę już na etapie otrzymania wiadomości e-mail. Nie udostępniaj osobom trzecim autorskich pomysłów albo zastrzeż je jak najszybciej, zanim zrobi to ktoś niepowołany.

PROŚBA O PRZELEW

Następnym sposobem na oszukanie przedsiębiorców jest wysyłanie pism lub wiadomości e-mail oczekujących na przedłużenie ważności znaku towarowego lub domeny (nazwy www strony twojej firmy). Pismo imituje list od Urzędu Patentowego lub firmy rejestrujące domeny (nazwy stron internetowych) i zawiera wszystkie potrzebne pieczątki, podstawę prawną i znak wodny. Na dokumencie znajduje się numer konta, na który trzeba przelać pieniądze z tytułu opłat urzędowych. Należy pamiętać, że dane adresowe podmiotów zgłaszających znaki towarowe nie są dostępne, tak więc oszust pozyskuje je we własnym zakresie. Co powinno cię zaniepokoić, jeśli dostaniesz taki list? Głównie kwota podana w obcej walucie i rachunek zarejestrowany w zagranicznym banku. Pojawia się także błąd w przywołanych paragrafach. Warto też porównać numer konta do informacji podanych na oficjalnej stronie Urzędu Patentowego lub rejestratora.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

FAŁSZYWE ZBIÓRKI DLA POWODZIAN

Po tragedii, jaka we wrześniu spotkała mieszkańców Dolnego Śląska, oszuści nie przestają wykorzystywać dobrego serca Polaków i ich chęci pomocy. Cyberprzestępcy za pomocą phishingu (tj. podszywanie się pod firmy, znajome osoby i wysyłanie wiadomości z linkami) tworzą fałszywe zbiórki na portalach takich jak Zrzutka.pl, które zachęcają do wsparcia powodzian, a w rzeczywistości są próbą wyłudzenia pieniędzy. Ale to niejedyny sposób na oszustwo. Za pomocą mediów społecznościowych podszywają się pod znajomych potrzebujących wsparcia finansowego. Co ważne, dla oszustów każda tragedia jest okazją do wyłudzenia pieniędzy – nie tylko wrześniowa powódź.

W tym przypadku oszuści najczęściej posługują się fałszywymi zbiórkami i stronami internetowymi, które do złudzenia przypominają witryny fundacji oraz organizacji charytatywnych. W obliczu wrześniowych powodzi Centralne Biuro Zwalczania Cyberprzestępczości wykryło **150 fałszywych** zbiórek pieniężnych, z których środki rzekomo miały być przeznaczone na poszkodowanych mieszkańców.

Chociaż od powodzi minęło przeszło 2 miesiące, przestępcy nie odpuszczają. Jeden z fałszywych organizatorów założył zbiórkę pod hasłem „Odrobina uśmiechu! Zrzutka na zabawki dla dzieci z Barda". Wykorzystał do tego zdjęcia najmłodszych, by wzbudzić współczucie wśród odbiorców. Władze tamtejszej szkoły nie miały o niczym pojęcia i mimo że Prokuratura Okręgowa we Wrocławiu zna imię i nazwisko oszusta, najprawdopodobniej one również nie są prawdziwe.

FAŁSZYWY ALERT RCB

Ten rodzaj oszustwa jest szczególnie niebezpieczny – przestępcy wykorzystują moment, kiedy Rządowe Centrum Bezpieczeństwa rozsyła najwięcej alertów. Właśnie wtedy wysyłają wiadomości SMS z fałszywym ostrzeżeniem, w którym znajduje się link kierujący na zainfekowane strony internetowe. To z kolei pozwala na przejęcie kontroli nad urządzeniem i zdobycie danych osobowych, a w ostateczności – kradzież pieniędzy z konta bankowego. Warto wiedzieć, że prawdziwe alerty RCB nie mają w treści żadnych linków. Jeżeli nie masz pewności co do prawdziwości informacji otrzymanej SMS-em, wejdź na oficjalną stronę Rządowego Centrum Bezpieczeństwa.

JAK NIE DAĆ SIĘ OSZUKAĆ?

Na rządowym Portalu Zbiórek Publicznych Ministerstwa Spraw Wewnętrznych i Administracji pod adresem **www.zbiorki.gov.pl** sprawdź, czy zbiórka jest legalna.

- Dokładnie czytaj opis zbiórki.
- Nie przelewaj pieniędzy na numer konta podany w wiadomości SMS czy e-mail.
- Jeśli ktoś prosi o pomoc finansową przez telefon – bądź szczególnie ostrożny.
- W razie wątpliwości skontaktuj się z organizatorem zbiórki i dopytaj o szczegóły.
- Nie postępuj pochopnie, kiedy nagle dostaniesz wiadomość z prośbą o pomoc. Oszuści specjalnie wywierają presję czasu.
- Pod żadnym pozorem nie przekazuj pieniędzy lub innych środków rzeczowych nieznajomym osobom, które przyjdą do ciebie do domu.
- Nie daj się zmanipulować wywołującym emocje zdjęciom dzieci i osób starszych, którym bezduszni oszuści nie chcą pomóc, tylko przede wszystkim żerują na ich tragedii.


Dziś jestem już tylko tą starszą panią,
samotną w Święta...
Czy możesz pomóc?
Ufunduj świąteczne spotkanie na
podarujwigilie.pl
i spraw świąteczny cud.
Podaruj Wigilię
Konto akcji wigilijnej:
83 1600 1462 1818 9539 9000 0002
PATRONAT
Głos SENIORA
MEDIALNY
Stowarzyszenie
mali bracia Ubogich
przyjaciele osób starszych


FUNDACJA
DIGNUM
partnerem akcji jest
Głos SENIORA
GODNY POSIŁEK
Cześć!
Znasz seniora w Warszawie lub
okolicach, który jest w trudnej sytuacji?
Dostarczymy darmowe posiłki w
ramach pomocy.
biuro@fundacja-dignum.org
726 289 555 wtorki i czwartki
w godz. 11.00-15.00
Możesz dowiedzieć się
więcej o naszych
działaniach tutaj:

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

HIGIENA CYFROWA TO TROSKA O WŁASNE BEZPIECZEŃSTWO

Korzystanie z Internetu przynosi wiele korzyści, ale może też wiązać się z pewnym ryzykiem. Zwiększanie świadomości na temat zagrożeń to cel kampanii „Oderwij się od ekranu i żyj", która jest organizowana przez Stowarzyszenie MANKO i Fundację Tomorrow Offline. Jak dbać o swoje zdrowie psychiczne podczas surfowania w sieci i oglądania telewizji? W dalszej części artykułu znajdują się proste porady oraz praktyczne wskazówki.

CO TO JEST HIGIENA CYFROWA?

Higiena cyfrowa to zbiór zasad, które pomagają korzystać z Internetu i telewizji w sposób bezpieczny, zdrowy i intencjonalny. Spędzanie wielu godzin przed ekranem może powodować zmęczenie oraz problemy z koncentracją i pamięcią. Przebodźcowanie, czyli nadmiar informacji, potrafi również wywoływać stres. Ograniczenie czasu on-line natomiast poprawia samopoczucie i sen.

NEGATYWNE SKUTKI NADMIERNEGO KORZYSTANIA Z INTERNETU I TELEWIZJI

Nadmierne korzystanie z urządzeń ekranowych może prowadzić do wielu negatywnych skutków zdrowotnych i psychicznych. Przede wszystkim długotrwałe patrzenie na ekran powoduje zmęczenie oczu, suchość i podrażnienia, a także może przyczyniać się do pogorszenia wzroku. Spędzanie wielu godzin on-line często wpływa negatywnie na sen, ponieważ światło emitowane przez ekrany zakłóca naturalny rytm dobowy.

Nadmierna aktywność cyfrowa może również zwiększać poziom stresu, powodować trudności z koncentracją oraz prowadzić do poczucia izolacji społecznej i obniżenia samopoczucia.

JAK OGRANICZYĆ CZAS PRZED EKRANEM?

- **Ustal limity korzystania z urządzeń**, aby zapobiec zmęczeniu oczu i poprawić samopoczucie. Pamiętaj, aby co godzinę oderwać wzrok od ekranu na kilka minut. Przejdź się po pokoju lub spójrz w dal za okno.
- **Zrezygnuj z używania telefonu**, komputera lub telewizora co najmniej dwie godziny przed snem. Dzięki temu poprawisz jakość snu i zmniejszysz problemy z zasypianiem.
- **Określ strefy wolne od ekranów** i wybierz, w których pomieszczeniach nie korzystasz z Internetu i telewizji.

Higiena cyfrowa to klucz do zdrowego i zrównoważonego życia w nowoczesnym świecie. Świadome korzystanie z technologii pomaga zachować równowagę między światem on-line a codziennym życiem, wspierając nasze zdrowie fizyczne i psychiczne. Wprowadzenie prostych nawyków, takich jak ograniczanie czasu spędzanego przed ekranem czy regularne przerwy, może znacznie poprawić jakość życia. Dbając o higienę cyfrową, nie tylko chronimy siebie przed negatywnymi skutkami nadmiernej ekspozycji na ekrany, ale też uczymy się lepiej korzystać z dobrodziejstw technologii, a także czerpać z nich korzyści bez szkody dla naszego zdrowia.

Dbanie o higienę cyfrową i bezpieczeństwo w sieci to podstawa. Proste zasady: silne hasła, aktualizacje czy przerwy od Internetu mogą pomóc ci bezpiecznie korzystać z nowych technologii i cieszyć się spokojem ducha.

OLIWIA GISSEL
PROFILAKTYK
SPECJALISTA DS. ZDROWIA PUBLICZNEGO
WICEPREZES FUNDACJI TOMORROW OFFLINE

OSZUSTWO NA MIESZKANIE

Osoby starsze coraz częściej padają ofiarą oszustw, których podstawą jest chęć przejęcia mieszkania. Dzięki popularności platform ogłoszeniowych przestępcy żerują na nieświadomych seniorach. Jednakże przykładów oszustw na mieszkanie jest o wiele więcej.

Oszuści zazwyczaj wykorzystują trzy schematy działania:

- **mieszkanie za pożyczkę** – oszust zamieszcza ogłoszenie, w którym oferuje pożyczkę pod zastaw nieruchomości jako pomoc w wyjściu z kiepskiej sytuacji finansowej. To sposób kuszenia zwłaszcza starszych, schorowanych i zadłużonych seniorów. Przestępca okłamuje klientów co do warunków umowy zawieranej u fałszywego notariusza. Zmienia dane swojej firmy i wpisy w księgach wieczystych, a tym samym staje się nowym właścicielem. Czasami oszust proponuje również mniejsze mieszkanie i dopłacanie różnicy, jednakże nowe lokum okazuje się ruderą;
- **mieszkanie za opiekę** – oszust pojawia się w życiu samotnego seniora i nawiązuje z nim więź. Pod wpływem manipulacji zyskuje dostęp do konta bankowego, aby opłacać bieżące zakupy i rachunki. Kiedy zyska pełne zaufanie seniora, podstępem każe podpisać mu umowę dożywocia, dzięki czemu nie tylko wzbogaca się o mieszkanie, ale też o wszystkie oszczędności oszukanej osoby;
- **mieszkanie za alkohol** – przestępca wybiera seniora z uzależnieniem alkoholowym i problemami finansowymi. Zaprzyjaźnia się z ofiarą, robi zakupy, po czasie przynosi też alkohol. Oczywiście zmanipulowany senior podpisuje notarialne oświadczenie, że ich „znajomy" staje się pełnomocnikiem w zarządzaniu nieruchomością. Czasami jednak mieszkanie nie wystarcza – oszust podaje seniorowi zatruty alkohol i przejmuje wszystko.

NA WYNAJEM

W przypadku rynku nieruchomości nie brakuje różnorakich metod oszustwa. Oprócz wymienionych jednym z nich jest fałszywa oferta na wynajem. Przestępca zamieszcza ogłoszenie na portalu sprzedażowym, takim jak OLX, że oferuje wynajem mieszkania. W trakcie rozmowy telefonicznej ustala warunki umowy i prosi o zaliczkę, aby potwierdzić umowę. Senior robi przelew na 500–3000 złotych, ale po wpłacie kontakt z właścicielem się urywa.

ODWRÓCONA HIPOTEKA

W ostatnim czasie w telewizji i w Internecie pojawiła się reklama funduszu hipotecznego, w której para emerytów przekonuje o tym, że przepisanie mieszkania na rzecz funduszu hipotecznego jest właściwą decyzją. Na czym to polega? Senior może mieszkać w swoim domu do końca życia, po czym nieruchomość trafi w ręce firmy. Oczywiście po zawarciu umowy firma jest zobowiązana wypłacać co miesiąc określoną kwotę.

Z odwróconej hipoteki najczęściej korzystają samotni seniorzy, bez spadkobierców. Zgodnie z reklamą dodatkowy fundusz z hipoteki ma znacząco ułatwić jesień życia i pozwolić seniorowi na przyjemności, na które dotąd nie mógł sobie pozwolić. Zgodnie z raportem Związku Przedsiębiorstw Finansowych z odwróconej hipoteki najczęściej korzystają osoby w wieku 75–80 lat, a w zeszłym roku wysokość wypłaty miesięcznej renty na rzecz seniora w ramach funduszu wyniosła 1033 złote. Można więc stwierdzić, że obietnica spełnienia przyjemności za tę kwotę przy wydatkach, jakie musi ponosić większość osób w wieku emerytalnym, jest na wyrost.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA PRACOWNIKA BANKU

Oszustwo na pracownika banku to jedna z popularniejszych i skuteczniejszych metod wyłudzania danych osobowych i pieniędzy. Przestępcy najpierw podszywają się pod osoby reprezentujące bank, w którym senior założył rachunek. Następnie przekonują do podania poufnych informacji i czyszczą konto.

66-letni mieszkaniec powiatu radomskiego stracił 340 tysięcy złotych, ponieważ oszust podający się za pracownika banku poinformował go, że środki zgromadzone na koncie są zagrożone. Jedyną formą „ratunku" było przelanie ich na inny rachunek bankowy – senior tak też zrobił. Z kolei 59-letnia mieszkanka powiatu ostródzkiego na polecenie fałszywego konsultanta bankowego udostępniła dane logowania do aplikacji bankowej i pod wpływem manipulacji podała kody potwierdzające transakcję. Tym sposobem straciła 50 tysięcy złotych.

Oszuści podszywają się pod oficjalne numery banków, by dzwonić do potencjalnych ofiar. Zazwyczaj trzymają się przygotowanego wcześniej skryptu rozmowy, co sprawia, że konwersacja nie brzmi naturalnie i swobodnie. Coraz częściej kontaktują się za pomocą SMS-a lub wiadomości e-mail. Aby wywołać u rozmówcy silne emocje, informują o podejrzanej transakcji na koncie: wielokrotnym logowaniu przez inną osobę, kradzieży pieniędzy, zmianie danych osobowych czy zaciągnięciu zobowiązania. Niczego nieświadoma, ale za to przerażona osoba pod presją czasu podaje swoje imię i nazwisko, login, hasło i nawet numer PESEL w celu rzekomej weryfikacji. W wielu przypadkach, zwłaszcza podczas rozmowy telefonicznej, nawet kiedy senior poda błędne dane, oszuści mogą podziękować za „pomyślną weryfikację" – to zdradza zamiary fałszywego pracownika banku.

Do czego nakłaniają cyberprzestępcy bankowi? Do pobrania aplikacji, która okazuje się złośliwym oprogramowaniem pozwalającym przejąć kontrolę nad urządzeniem; natychmiastowego przelania pieniędzy na rachunek techniczny, by „zabezpieczyć" zagrożone środki; podania kodu otrzymanego w wiadomości SMS, który jest potrzebny do autoryzacji; wypłacenia pieniędzy z bankomatu, a następnie wpłacenia ich za pomocą wpłatomatu na podany przez nich rachunek.

ZWERYFIKUJ PRACOWNIKA BANKU

Jak zweryfikować pracownika banku? Poproś o podanie imienia i nazwiska, nazwy banku, adresu placówki i oddziału, z którego dzwoni, a następnie się rozłącz. Na oficjalnej infolinii banku dopytaj, czy sytuacja przedstawiona przez rzekomego pracownika jest prawdziwa i czy twoje środki są zagrożone.

Pamiętaj, by nie podawać przez telefon danych logowania do bankowości internetowej i nie udostępniać danych karty płatniczej. Nie udostępniaj także kodu BLIK nieznajomemu, a jeśli masz wątpliwości co do tożsamości pracownika banku – przerwij rozmowę telefoniczną. W przypadku wiadomości e-mail nie klikaj w linki i nie pobieraj wątpliwych załączników. I co ważne, nie wpłacaj pieniędzy na awaryjny rachunek techniczny, ponieważ prawdziwy pracownik banku nigdy cię o to nie poprosi.

MAŁOPOLSKA
Projekt zrealizowano przy wsparciu finansowym Województwa Małopolskiego

HACKING – KRADZIEŻ DANYCH Z SYSTEMU KOMPUTERA

Jak już wiadomo, SPOOFING [czyt. spufing] to technika mająca na celu oszustwo polegające na podszywaniu się pod inną osobę, urządzenie lub serwer. Choć w literaturze brakuje powszechnie obowiązującej definicji hackingu, to większość autorów przyjmuje, że HACKING [czyt. haking] oznacza bezprawne wejście do systemu komputera w celu kradzieży informacji.

HISTORIA PANA TOMASZA

Pan Tomasz ma 67 lat. Jest aktywny, ma smartfon i komputer, na których często korzysta z Internetu – między innymi przegląda serwisy informacyjne. Pewnego dnia zadzwoniła do niego kobieta i przedstawiła się jako osoba reprezentująca dużą firmę finansową. Wyjaśniła, że pan Tomasz w czasie przeglądania stron internetowych zaakceptował regulamin serwisu finansowego, a serwis ten prowadził w jego imieniu transakcje w kryptowalutach. Jednakże pan Tomasz nie pamięta takiej okoliczności.

Pani wyjaśniła, że to zdarza się dość często, ale nie ma się czym martwić, bo serwis zarobił w jego imieniu 6700 zł i chce mu te pieniądze wypłacić. Przypomniała tylko, że od takiej kwoty trzeba zapłacić podatek. Kiedy pan Tomasz chciał podać swój rachunek bankowy, pani poleciła zainstalować specjalną aplikację, przez którą może przekazać środki finansowe. W tym momencie pan Tomasz wystraszył się i rozłączył. Sprawdził, że kobieta próbowała dzwonić do niego jeszcze kilka razy, ale on już nie odebrał.

Czy postąpił właściwie? Zdecydowanie tak. W tym przypadku mamy do czynienia z klasycznym przykładem tzw. **SPOOFINGU** lub **HACKINGU.** W opisanej sytuacji przestępcy uzyskaliby zdalny dostęp do programów używanych przez pana Tomasza poprzez zainstalowanie aplikacji na urządzeniu z Internetem. W ten sposób mogliby pozbawić go wszystkich oszczędności.

HISTORIA PANI MAGDY

Pani Magda ma 72 lata. Na urodziny dostała od swoich dzieci smartfon – wykorzystuje go głównie do rozmów telefonicznych. Koleżanka, która mieszka w sąsiednim bloku, pochwaliła się, że zaczęła robić zakupy w Internecie. Nie dość, że ceny są o wiele niższe, to jeszcze kurier przywozi jej wszystko do domu.

Pani Magdzie było wstyd, że ona nie jest tak zaradna, dlatego postanowiła sprawdzić możliwość takich zakupów na własną rękę. Przeglądała oferty wielu sklepów. Jeden wydawał się szczególnie interesujący, oferował bowiem ceny produktów niższe o 60–70%. Pani Magda oczyma wyobraźni widziała, ile zaoszczędzi i jakie prezenty kupi wnukom. Strona sklepu wymagała podania wielu danych osobowych, w tym danych do rachunku bankowego, aby zapłacić za zakupy. Pani Magda uznała, że to całkowicie uzasadnione... Niestety padła ofiarą oszustów, którzy podszyli się pod sklep internetowy w celu wyłudzenia danych do rachunku bankowego pani Magdy.

PAMIĘTAJ:

- nigdy nie instaluj oprogramowania z nieznanych i niezaufanych źródeł,
- nigdy nie podawaj danych do logowania do swojego rachunku bankowego (loginu i hasła),
- w życiu nie ma niespodziewanych i darmowych okazji,
- jeżeli coś kosztuje znacznie mniej niż zwykle, jest to podejrzane,
- jeżeli ktoś proponuje ci szybkie i łatwe pieniądze lub prezenty, powinno to wzbudzić twoje podejrzenia.

NIGDY NIE JEST ZA PÓŹNO NA EDUKACJĘ

Zwracaj uwagę na komunikaty, jakie otrzymujesz od swojego banku na temat bezpieczeństwa. Nie wstydź się pytać o radę lub pomoc innych – sąsiadów, dzieci, wnuków, przyjaciół.

MICHAŁ MODRO
RADCA PRAWNY, ZASTĘPCA PRZEWODNICZĄCEGO RADY POLITYKI SENIORALNEJ

SIŁA RĘKOJMI

Zdarza się, że kupione przez nas sprzęty elektroniczne, AGD czy inne produkty psują się niedługo po zakupie. Nie każdy jednak wie, iż taki sprzęt można skutecznie reklamować i uzyskać bezpłatną naprawę lub wymianę.

Pani Anna kupiła nowe buty do biegania, ale już po pierwszym treningu podeszwa okazała się wadliwa. Twarda część wbijała się w stopę tak mocno, że utrudniało to chodzenie. Sprzedawca nie uznał reklamacji i sprawa trafiła do sądu. Ze względu na istotę wady i czas jej ukazania się sąd nakazał sprzedawcy oddać całość ceny, a na dodatek pokryć koszty rozprawy sądowej.

W polskim prawie są przewidziane dwa rodzaje reklamacji wadliwych rzeczy:

- **gwarancja**, w ramach której odpowiedzialność za wadliwy towar spoczywa na producencie towaru;
- **rękojmia** – wówczas kierujemy nasze roszczenia do sprzedawcy towaru.

Spośród podanych rozwiązań instytucja rękojmi jest znacznie powszechniejsza i korzystniejsza dla konsumenta.

CZYM JEST WADLIWY TOWAR?

Jeżeli sprzedana rzecz ma wadę, sprzedawca jest odpowiedzialny względem kupującego przez 2 lata od daty sprzedaży, a zatem nie może odmówić przyjęcia reklamacji, jeżeli nie wynika to wprost z przepisów.

Wada rzeczy polega na niezgodności sprzedanego produktu z umową. Niezgodność następuje wtedy, gdy rzecz:

1) nie ma właściwości typowych dla rzeczy tego rodzaju;
2) nie ma właściwości, o których sprzedawca zapewnił kupującego poprzez pokazanie próbki lub wzoru;
3) nie nadaje się do celu, na którym zależało kupującemu przy zawarciu umowy ze sprzedawcą, a sprzedawca nie miał zastrzeżeń co do takiego przeznaczenia towaru;
4) została wydana w stanie niezupełnym, niekompletnym.

Wadliwość rzeczy może także wystąpić wtedy, kiedy sprzedawca lub osoba upoważniona przez sprzedawcę nieprawidłowo zamontuje lub uruchomi daną rzecz. Sytuacja wygląda podobnie, gdy kupujący uszkodzi rzecz, mimo że postąpił zgodnie z instrukcją otrzymaną od sprzedawcy.

NA CZYM POLEGA RĘKOJMIA?

Jeżeli sprzedana rzecz ma wadę, kupujący może żądać od sprzedawcy usunięcia wady (naprawy) albo wymiany rzeczy na towar wolny od wad, a sprzedawca jest do tego zobowiązany. W przypadku wystąpienia wady po raz pierwszy sprzedawca ma prawo jedynie naprawić uszkodzoną rzecz, chociaż kupujący żądałby wymiany produktu na nowy. Jednakże przy kolejnych reklamacjach tej samej wady sprzedawca ma już obowiązek wydać nowy towar. Co istotne, okres 2 lat odpowiedzialności sprzedawcy zaczyna biec na nowo zarówno po naprawie (w części, w jakiej dokonano naprawy), jak i wymianie na nowy.

Niewywiązanie się z obowiązku naprawy lub wymiany wadliwej rzeczy zostało przedstawione w programie „Interwencja". Właściciel komisu samochodowego tym sposobem oszukał starsze małżeństwo, które potrzebowało nowego pojazdu, aby usprawnić sobie opiekę nad synem z niepełnosprawnością. Chociaż zarówno ten przykład, jak i podany na początku sugeruje inaczej, zdecydowana większość reklamacji jest uznawana przez sprzedawców niemal od razu, ponieważ w ten sposób firma dba o swój wizerunek.

Koszty naprawy lub wymiany rzeczy – w szczególności koszty opłat pocztowych, przewozu, robocizny i materiałów – ponosi sprzedawca. Co jest istotne, nie ma wymogu prawnego, by przedstawić paragon lub fakturę, jeżeli zgłaszamy reklamację z tytułu rękojmi. Niemniej zawsze rekomenduję przechowywanie dowodów sprzedaży przez okres 2 lat od zakupu.

NATALIA GAJECKA
ADWOKAT

UWAGA NA PREZENTACJE SPRZEDAŻOWE
NIE DAJ SIĘ OSZUKAĆ!

W Internecie znajdziemy wiele wskazówek na temat tego, jak powinna wyglądać dobra i skuteczna prezentacja sprzedażowa. Nie brakuje również specjalistów, dla których marketing i kontakt z klientem nie mają żadnych tajemnic, a za pomocą odpowiednio dobranych słów są w stanie namówić do transakcji nawet najbardziej opornych. Niestety w Polsce prezentacje sprzedażowe nie kojarzą się najlepiej. Wręcz przeciwnie – każdego dnia odbywa się mnóstwo takich spotkań, aby naciągnąć seniorów na produkty i usługi niewarte swojej ceny.

Nie bez powodu nieuczciwi sprzedawcy na swoje ofiary wybierają osoby starsze. Zazwyczaj odwołują się do emocji kupującego, a seniorzy często nie zdają sobie sprawy, jakie sztuczki stosują oszuści. W ten sposób zostają namówieni do kupna za drogich garnków, robotów kuchennych i innych przedmiotów, ponieważ „to jedyna taka okazja". Pokazy najczęściej są organizowane w hotelach, restauracjach, sanatoriach, a w ostatnim czasie nawet w domu klienta.

Na forach nie brakuje historii o oszukanych seniorach:

– Jakiś czas temu oszukali moją mamę, która „wygrała" masę produktów. Poszła na bezpłatną spirometrię, a wyszła z długiem w wysokości 12 tysięcy złotych. Zupełnie nie była tego świadoma, dopiero w domu przejrzała teczkę od sprzedawcy i się zdziwiła. Kiedy się zorientowała, chciała wszystko oddać, ale oszuści powiedzieli, że to była promocja i nie ma zwrotów. Teraz mama musi spłacać dług przez 3 lata – pisze jedna z internautek.

W JAKI SPOSÓB NACIĄGACZE KONTAKTUJĄ SIĘ Z KLIENTAMI?

Zazwyczaj fałszywi sprzedawcy nawiązują kontakt telefoniczny, w wielu przypadkach jednak wysyłają wiadomości SMS lub e-mail, rozdają również ulotki i plakaty informacyjne.

Oczywiście oszuści dobierają produkt i usługę w ten sposób, aby wpasować się w potrzeby osób starszych. Oprócz prezentacji, na których sprzedają artykuły domowe (np. żelazko, czajnik, noże, narzędzia), nieuczciwi handlowcy zapraszają na: darmowe badania (a te w ostateczności albo się nie odbywają, albo wymuszają na seniorze kupno drogiego specyfiku rozwiązującego jego problem zdrowotny), konsultacje ze specjalistami czy wykłady na temat zdrowego stylu życia itd. Zaproszeni goście nie są informowani o celach marketingowych, a w trakcie spotkania nie mogą korzystać z telefonów.

JAK WYGLĄDA OSZUKAŃCZA PREZENTACJA SPRZEDAŻOWA?

Przede wszystkim liczy się pierwsze wrażenie, dlatego prezenter wygląda elegancko i ma miłe usposobienie. Handlowiec często podaje się za eksperta w dziedzinie, opowiada o swoim doświadczeniu i przedstawia opinie rzekomo zadowolonych klientów. W trakcie spotkania panuje swobodna atmosfera, co wzbudza zaufanie seniorów. Sprzedawcy zapewniają również, że takie pokazy są zarezerwowane dla nielicznych, a to pozwala poczuć się wyjątkowo. Nie brakuje także opowieści o osobistych doświadczeniach z danym produktem, którego stosowanie popiera wielu fachowców.

JAK ZAREAGOWAĆ?

Nie przyjmuj zaproszenia na prezentację najlepiej już w trakcie pierwszej rozmowy. Jeśli zrezygnujesz w późniejszym terminie i to bez przekonania, oszuści mogą podsyłać ci dodatkowe informacje, w których będą używać słownictwa nacechowanego emocjonalnie. Poproś o usunięcie twojego numeru telefonu z bazy danych, a w przypadku nieustannych propozycji powiedz, że zgłosisz sprawę na policję.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

TECHNIKI SPRZEDAŻY I MANIPULACJI

Techniki sprzedaży to narzędzia umożliwiające nawiązywanie kontaktów i budowanie relacji z klientem, a przede wszystkim – zwłaszcza w przypadku oszukańczych prezentacji sprzedażowych – do zakupu konkretnego produktu lub usługi. W sprzedaży pomagają również techniki manipulacji, które mają oddziaływać na podświadomość i emocje człowieka. Zarówno technik sprzedaży, jak i manipulacji jest mnóstwo – warto poznać najważniejsze.

TOROWANIE Sprzedawca przyzwyczaja klienta do wysokich cen przy pomocy eksponowania równie wysokich liczb. Przez to narzuca określony schemat myślenia.

DRZWIAMI W TWARZ Handlowiec najpierw podaje wygórowaną cenę, którą klient na pewno zakwestionuje, by później zaproponować znacznie niższą – choć w przypadku oszustw wciąż nieadekwatną do wartości produktu.

ZA DARMO Sprzedawca daje poczucie, że klient nie dostanie rabatu bez dodatkowych warunków. Tym sposobem odbiera okazję do dalszych negocjacji cenowych.

ZMĘCZENIE CZASEM Gospodarze spotkania szczegółowo tłumaczą klientowi wszelkie kwestie i grają na czas. Podejmowanie pobocznych wątków i maksymalne skupienie się na mało istotnych kwestiach sprawiają, że dana osoba nie będzie mieć już energii na zbijanie ceny i chce jak najszybciej zakończyć sprawę.

WIELU KUPUJĄCYCH NARAZ Sprzedawca daje do zrozumienia, że na ten sam produkt jest jeszcze wielu chętnych, którzy o cenę się nie targują. Tym sposobem senior podejmie decyzję w sposób impulsywny – byle stać się szczęśliwym posiadaczem prezentowanego produktu.

GRATIS Do usługi lub produktu za określoną cenę dodawane jest coś za darmo. Takie działanie obniża nasze wymagania co do produktu czy usługi. Wiele osób z chęcią skorzysta z takiej okazji, nawet pomimo drobnych wad produktu/usługi.

NISKA PIŁKA Manipulator przedstawia propozycję, która jest niesamowicie dla nas korzystna. Tuż przed realizacją okazuje się jednak, że nastąpiło nieporozumienie albo pomyłka – w konsekwencji przedmiot ma o wiele wyższą cenę lub aby go otrzymać za darmo, musimy kupić coś innego.

AUTORYTET Prezenterzy często powołują się na opinie ekspertów, bo doskonale wiedzą, że podczas prezentacji nie można tego sprawdzić. Poparcie autorytetu w postaci specjalisty lub sławnej osoby czyni przedmiot bardziej wiarygodnym.

NIEDOSTĘPNOŚĆ Sprzedawcy zapewniają, że taka okazja już się nie powtórzy, a sam produkt wywołał wielkie zainteresowanie, dlatego szybko znika z półek. To wzbudza w nas przeświadczenie, że również chcielibyśmy być posiadaczami wyjątkowej rzeczy.

SPOŁECZNY DOWÓD SŁUSZNOŚCI Jeżeli podczas oszukańczej prezentacji sprzedażowej większość potwierdza, że produkt spełnia swoją funkcję i jest wart swojej ceny, to nie chcemy odstawać od reszty grupy. Najczęściej jednak w trakcie spotkania na sali siedzą podstawione osoby.

NIE DAJ SIĘ ZMANIPULOWAĆ NA PREZENTACJI SPRZEDAŻOWEJ

W ciągu ostatniego roku Urząd Ochrony Konkurencji i Konsumentów przeprowadził 27 kontroli pokazów, podczas których firmy próbowały sprzedać konsumentom swoje produkty i usługi. Konsekwencją tych działań było złożenie zawiadomienia w sprawie ośmiu firm – trzy z nich zostały ukarane grzywną o łącznej wysokości niemal 4 milionów złotych. Największe kary spotkały firmy, które zapraszały na badanie zdrowotne, a organizowały prezentacje sprzedażowe.

Oszuści wykorzystują problemy zdrowotne seniorów oraz brak wiedzy na temat aktualnych przepisów prawnych. Właśnie dlatego edukacja i uświadamianie muszą być priorytetem, aby osoby starsze unikały oszukańczych pokazów oraz – jeśli już na nich się znajdą – zawierania niekorzystnych umów.

JAK UCHRONIĆ SIĘ PRZED ZMANIPULOWANIEM NA PREZENTACJACH SPRZEDAŻOWYCH?

- Uważaj na obietnice dotyczące niepowtarzalnych okazji, przeprowadzenia bezpłatnych badań, wręczania prezentów i gratisów. To tylko słowa bez pokrycia, które brzmią kusząco. Pozornie atrakcyjne spotkanie w rzeczywistości jest prezentacją oferty handlowej. Celem oszustów jest nakłonienie do podpisania umowy kupna-sprzedaży produktów w wygórowanych cenach i często na kredyt.
- Pamiętaj, że żadna firma nie działa charytatywnie, więc „za darmo" musi mieć drugie dno – podobnie to wygląda w przypadku oszustw internetowych.
- Jeżeli już znalazłeś się na prezentacji, nie podpisuj niczego bez zastanowienia się nad zakupem! Przeczytaj bardzo uważnie umowę, a najlepiej nie kupuj niczego, dopóki nie zasięgniesz rady bliskich.
- Zażądaj kopii dokumentów dla siebie.
- Oferowane produkty najczęściej są o wiele tańsze, niż wskazują na to zapewnienia handlowca. Wielokrotnie cena nie idzie w parze z jakością. Sprawdź, ile zapłacisz za podobny produkt w innych sklepach.
- Znajdź w Internecie opinie na temat produktów lub poproś bliskiego o pomoc. Sprawdź także opinie o samej firmie, która zorganizowała prezentację sprzedażową.
- Przed zakupem sprzętu medycznego poproś o radę swojego lekarza rodzinnego.
- Nie podpisuj umów, których nie rozumiesz. Bardzo często umowy są konstruowane specjalnie w sposób zawiły zwłaszcza dla osób starszych.
- Nie dawaj dowodu osobistego obcym, nie przekazuj danych na żadnych notatkach. Sprawdź, czy nikt nie zagląda ci przez ramię.
- Bądź czujny. Nieuwaga może wiele kosztować – niejednokrotnie na pokazach ludzie dobrowolnie pozbywają się oszczędności życia, kiedy zostaną zmanipulowani.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

JAK ODSTĄPIĆ OD NIEKORZYSTNEJ UMOWY

W maju 2022 roku został wprowadzony zakaz sprzedaży wyrobów medycznych poza lokalem przedsiębiorstwa, czyli między innymi na prezentacjach sprzedażowych. Z kolei od stycznia 2023 roku obowiązują przepisy, zgodnie z którymi firmy organizujące pokazy handlowe nie mogą przyjmować płatności przed upływem terminu na odstąpienie umowy oraz zawierać umów dotyczących usług finansowych, np. kredytów.

JAK ODSTĄPIĆ OD NIEKORZYSTNEJ UMOWY?

Warto pamiętać, że zawieranie (podpisywanie) umów podczas spotkania w miejscach takich jak restauracje czy hotele jest niezgodne z prawem.

- Jeśli jednak oszuści w dokumencie wpisali mieszkanie jako miejsce zawarcia umowy, chociaż odbyło się to gdzie indziej, możesz od niej odstąpić w czasie:
  - 30 dni – w przypadku umowy zawartej podczas nieumówionej wizyty przedsiębiorcy w miejscu zamieszkania konsumenta albo podczas wycieczki,
  - 14 dni – w przypadku pozostałych umów (również zawartych przez Internet) lub podczas umówionej wizyty w domu konsumenta. Początek biegu terminu na odstąpienie od umowy poza lokalem przedsiębiorstwa (14 lub 30 dni) liczy się od dnia zawarcia umowy.
- Sprzedawcy należy wysłać oświadczenie o odstąpieniu od umowy. Taki formularz powinien dostarczyć sprzedawca, wzory można znaleźć również w sieci, a także w tym wydaniu na stronach 55–56.
- Jeśli częścią umowy było zawarcie kredytu (kupno na raty), poinformuj bank o odstąpieniu od umowy, by nie zdążył pobrać pieniędzy z konta.
- Towar należy zwrócić sprzedawcy. Nawet jeśli otworzysz i rozpakujesz produkt, w dalszym ciągu możesz go zwrócić. Zwrotu można dokonać osobiście albo wysłać pocztą na adres sprzedawcy.
- Korespondencję wysyłaj listami poleconymi za potwierdzeniem odbioru. Aby mieć pewność, że list dotarł do odbiorcy, skorzystaj z możliwości poinformowania SMS-em.
- Należy pamiętać, że w wypadku jakichkolwiek problemów warto skontaktować się z Powiatowym Rzecznikiem Praw Konsumenta lub skorzystać z darmowej porady prawnej.

TO MUSI SIĘ ZMIENIĆ!

Pomimo stopniowych zmian w prawie dotyczących ochrony konsumentów wciąż wiele praktyk budzi wątpliwości. Apelujemy zatem o:

- niewynajmowanie powierzchni podejrzanym i niesprawdzonym firmom na spotkania sprzedażowe przeprowadzane w hotelach i restauracjach,
- wydłużenie terminu na odstąpienie od umowy kupna-sprzedaży do 30 dni,
- zakaz udzielania kredytów/pożyczek poza stacjonarną placówką bankową,
- wprowadzenie obowiązku zgłoszenia prezentacji 14 dni przed jej planowanym terminem do lokalnego Rzecznika Praw Konsumenta lub innych instytucji kontrolnych,
- wprowadzenie nakazu uwzględnienia w zaproszeniu informacji o handlowym celu spotkania i produktach, które będą sprzedawane, a w razie niewywiązywania się z obowiązku – nałożenie kary na nieuczciwego handlowca,
- wprowadzenie odpowiedzialności karnej za oferowanie prezentów za samo przyjście na spotkanie, których się potem nie otrzymuje,
- zakaz wyłudzania danych teleadresowych od seniorów oraz wykorzystywania tych informacji przez firmy call center.

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

OSZUSTWO NA SAMOCHÓD ZASTĘPCZY

Jeśli zepsuje ci się ubezpieczony samochód, zgodnie z umową na czas naprawy możesz otrzymać samochód zastępczy. Dostarcza go twój ubezpieczyciel lub autoserwis. Okazuje się jednak, że ta powszechna na całym świecie praktyka również jest okazją do wyłudzania pieniędzy i oszukiwania ludzi.

Mieliśmy kolizję, więc zgodnie z instrukcją zgłosiliśmy ją do firmy ubezpieczeniowej. Nasz zepsuty samochód został odholowany do warsztatu, a ubezpieczyciel obiecał dać samochód zastępczy. Agentka dostarczyła go późnym wieczorem – było zupełnie ciemno, a do tego padał deszcz. Co więcej, zaparkowała w złym miejscu, tak że inni nie mogli przejeżdżać obok – to spowodowało stres i pośpiech przy odbiorze. Szybko podsunęła nam tablet i kazała podpisać odbiór samochodu. Nie dała nam nawet szansy, aby zapoznać się z tym, co podpisujemy. Kazała jedynie oddać samochód w takim stanie, w jakim go dostarczyła: „Oczywiście nie musicie go myć, tylko zatankujcie bak do takiego samego zasięgu, czyli 450 km".

Następnego dnia z samego rana wyjechaliśmy na ważne spotkanie do Warszawy. Dopiero w trasie firma przesłała nam na pocztę e-mail dziesięciostronicową umowę. Okazało się, że nie jest to samochód od ubezpieczyciela, tylko od nieznanej nam firmy wypożyczającej samochody. Z kolei podpisany na tablecie dokument nie był odbiorem samochodu, a umową wypożyczenia – i to nie z naszą firmą, ale z osobą prywatną, która przyjęła pojazd. Nic już nie mogliśmy zrobić, skoro samochodem pojechaliśmy daleko w trasę.

Po kilku dniach dostaliśmy informację o konieczności wymiany samochodu na inny samochód zastępczy. Kiedy kolejny agent przyjechał podmienić auto, kazał zapłacić za mycie i dotankowanie. Stwierdził, że nie wykupiliśmy pakietu „myjnia", a co do tankowania – liczy się nie zasięg paliwa, tylko jego ilość w baku. Zaprotestowaliśmy, bo chociaż poprzednia agentka wprowadziła nas w błąd, jego zdaniem dalej byliśmy zobowiązani do zapłaty za tankowanie, paliwo i mycie. Mimo wszystko nie daliśmy się zastraszyć i samochód sami dotankowaliśmy na najbliższej stacji. Powiedzieliśmy również, że to agentka kazała nie myć pojazdu (są świadkowie), który sama zaparkowała na ulicy pełnej błota i liści. Wtedy agent odpuścił. Następnie zaczął wnikliwie przyglądać się blacharce samochodu. Kiedy znalazł biały nalot na słupku drzwi, kazał nam zapłacić za rzekomo nową szkodę. Nie mogliśmy potwierdzić, że to nasza wina, skoro przy oddawaniu samochodu nikt nie dał nam szansy sprawdzić, w jakim stanie jest auto. Poza tym samochód zastępczy powinien mieć ubezpieczenie, które obejmuje taki przypadek. Jak się okazało, zgodnie z umową zawartą z wypożyczalnią musimy dopłacić tak zwany wkład własny do szkody w wysokości 1850 złotych. Oczywiście zaprotestowaliśmy, zwłaszcza że nalot starliśmy zwykłą szmatką.

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

Zaledwie w tym fragmencie można wymienić aż pięć sposobów na próbę wyłudzenia pieniędzy:

1. na mycie;
2. na dotankowanie (ilość paliwa, a nie zasięg);
3. na nieistniejącą szkodę;
4. szkodę, której nie można zweryfikować ani nikomu przypisać;
5. na nie w pełni ubezpieczony samochód.

Po oględzinach pierwszego samochodu agent podstawił drugi. Tym razem próbował nas przekonać, że nie musimy przeglądać pojazdu, bo jest czysty i ma wiele szkód, które zostały odhaczone na tablecie. Nauczeni jego wcześniejszą nieuczciwością, zaczęliśmy przyglądać się blacharce. Co się wtedy stało? Jak można się domyślić, znaleźliśmy kilka nowych szkód (obtarć i zarysowań). Oczywiście nie zostały one wcześniej odnotowane na tablecie, agent je zaznaczył dopiero w tamtym momencie. Dodatkowo w bagażniku był piasek, więc zmienił oznaczenie samochodu z „czysty" na „brudny". Jaki z tego morał? Gdybyśmy wtedy nie przejrzeli samochodu dokładnie, zapewne wypożyczalnia kazałaby nam dopłacić za szkody, które w rzeczywistości wyrządził ktoś inny.

Po kolejnych sześciu dniach oddawaliśmy drugi samochód zastępczy. Agent doszukał się rysy na reflektorze, ale nie mieliśmy pewności, czy nie została zrobiona jeszcze przed poprzednim odbiorem. Nie zaakceptowaliśmy więc próby przypisania nam winy. Co stało się dalej? Po tygodniu dostaliśmy fakturę do zapłacenia: 1850 złotych za wyrządzenie szkody i 1500 złotych za brak dokumentacji szkody. Oczywiście złożyliśmy skargę i do ubezpieczyciela, i do wypożyczalni za oszukańcze, karygodne praktyki. Ta sytuacja rodzi wiele pytań:

- Dlaczego dostaliśmy samochód nie od ubezpieczyciela, tylko od niezweryfikowanej, nieznanej nam firmy?
- Dlaczego samochód był przekazany w nocy, a potwierdzenie odbioru podpisane na tablecie okazało się niekorzystną dla nas umową z wypożyczalnią?
- Dlaczego umowy nie zawiera się z właścicielem uszkodzonego i ubezpieczonego samochodu, tylko z osobą, która odbiera samochód?
- Dlaczego nie ma możliwości zapoznania się z umową przed jej podpisaniem? Czy pospieszne podsunięcie tabletu na parkingu to forma wiarygodnego podpisania dziesięciostronicowej umowy?
- Dlaczego klient nie dostaje informacji i możliwości dokładnego przeglądu samochodu, aby w pełni ocenić jego stan?
- Dlaczego samochód zastępczy nie jest ubezpieczony, a klient nie otrzymuje takiej informacji ani od ubezpieczyciela, ani od agenta wypożyczalni?
- Dlaczego klient nie został poinformowany o możliwości dokupienia ubezpieczenia samochodu, aby pojazd był całkowicie ubezpieczony, a klient nie musiał płacić kary za nowo powstałe szkody z własnej kieszeni?
- Dlaczego klient jest obciążany karą za brak dokumentacji szkody, jeśli klient o niej nie wiedział, kiedy oddawał samochód? W jaki sposób miał dostarczyć dokumentację, jeśli nie wiedział o szkodzie?
- Dlaczego ubezpieczyciel, który chwali się odznaką „Przyjazny klientowi", odrzuca wszelkie pretensje i twierdzi, że agenci przekazali wszystkie informacje?
- Czyj interes reprezentuje ubezpieczyciel – swojego klienta, który mu zaufał i ubezpieczył u niego samochód, czy wypożyczalni, która bez wiedzy i zgody klienta niespodziewanie podstawia mu samochód w nocy po dom?

JAK SIĘ UCHRONIĆ PRZED OSZUSTWEM – PORADY

- **Jeśli potrzebujesz samochodu zastępczego, upewnij się, czy jest on w pełni ubezpieczony.**
- **Jeśli nie – nie wypożyczaj takiego pojazdu lub dopłać za pełne ubezpieczenie.**
- **Zrób dokładne zdjęcia samochodu, licznika i bagażnika.**
- **Zatankuj tuż przed oddaniem samochodu.**
- **Upewnij się, czy samochód jest czysty. Dopytaj również agenta, kto jest odpowiedzialny za mycie pojazdu przed oddaniem.**

AKTYWNI+
Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

CHCEMY KIBICOWAĆ POLAKOM

Od lat wiadomo, że sport łączy ludzi – integruje, emocjonuje, jest tematem spotkań i dyskusji. Na mecze chodzimy całymi rodzinami i z przyjaciółmi, a jeśli nie mamy takiej możliwości, sportowe zmagania śledzimy z wypiekami na twarzy przed telewizorami. Oglądanie meczów Polaków i naszych reprezentantów dodaje nam sensu życia, którego wielu osobom wraz z wiekiem zaczyna brakować. To jest także promocja uprawiania sportu, motywacja do ruchu fizycznego i powrotu do formy sprzed lat. Wspólne kibicowanie to również doskonały sposób na integrację międzypokoleniową, bo na kanapie zasiadają dziadkowie, rodzice i dzieci. Tymczasem od wielu lat ta możliwość jest nam odbierana! W jaki sposób mamy kibicować Polakom?

Aby obejrzeć transmisję meczu, w większości przypadków trzeba wykupić specjalny abonament. W zależności od platformy jego cena waha się pomiędzy 30 a 70 złotych za miesiąc. Wielu z nas ma ograniczony budżet i nie potrafi biegle obchodzić się z technologią. Zostajemy przez to pozbawieni dostępu do meczów naszych ulubionych drużyn.

Przenoszenie większości transmisji na płatne serwisy to dyskryminacja cyfrowa i odcinanie nas od ważnego elementu aktywizacyjnego. W końcu kibicowanie, czyli obstawianie wyniku czy przewidywanie ruchów graczy, poprawia naszą kondycję psychiczną.

Oprócz telewizji publicznej pozostałe kanały wymagają opłacenia abonamentu lub dostępu do Internetu, a nie każdy z nas może sobie na to pozwolić. Ligę Mistrzów obejrzymy w Polsat Sport Premium, mecze Igi Świątek na Canal+, a mecze reprezentacji siatkówki w Lidze Narodów – na płatnym kanale TVP Sport. Podobnie dzieje się w przypadku piłkarskiej Ekstraklasy. Tylko jedno spotkanie z każdej kolejki jest transmitowane w TVP (poza meczami 1 ligi).

Chcemy pełnej dostępności do meczów naszych reprezentantów w publicznej, bezpłatnej telewizji! Dostęp do kultury i rozrywki powinien być podstawowym prawem dla wszystkich, a nie luksusem dla wybranych.

Pozwólcie nam, seniorom, cieszyć się sportem i kibicować Polakom wraz z dziećmi i wnukami.

ODDAJCIE NAM STÓŁ DO PING-PONGA

Z placu zabaw w Grębałowie na ul. Stycznej zniknął stół do ping-ponga oraz jedna z bramek do gry w piłki nożną. Jak się okazało, nie był to żaden akt wandalizmu, a zaplanowane działanie. Z takiej decyzji nie są zadowoleni zwłaszcza rodzice i nauczyciele, którzy do parku miejskiego przychodzili z najmłodszymi. Chociaż dzięki tym sprzętom dzieci mogły urozmaicić wyjście do parku i aktywnie spędzić czas, zdaniem Zarządu Zieleni Miejskiej stół i bramka piłkarska stwarzały niebezpieczeństwo.

Sytuacja wydaje się kuriozalna. Skoro sprzęty uznano za zagrożenie dla dzieci, dlaczego zdemontowano tylko jedną bramkę, jeśli są dwie? Trudno wytłumaczyć taki powód uczniom, zwłaszcza że na terenach innych parków czy placów zabaw można korzystać z powyższych bez problemu.

Te proste obiekty miały ogromne znaczenie dla lokalnej społeczności – zwłaszcza dla młodzieży i rodzin z dziećmi, a nawet starszych, którzy na emeryturze chcą podtrzymywać dobrą kondycję fizyczną. Usunięcie sprzętu nie tylko obniża jakość infrastruktury parku, ale ogranicza swobodę mieszkańców do korzystania z przestrzeni przeznaczonej do rekreacji.

W odpowiedzi na pytanie od mieszkańców o zasadność usunięcia stołu i bramki zastępca prezydenta Krakowa uzasadnia, że sprzęty były niewłaściwie użytkowane, co generowało konflikty sąsiedzkie – krakowianie zgłaszali nadużywanie alkoholu i hałas na terenie parku.

Czy naprawdę przyczyną był stół do tenisa i jedna bramka piłkarska? W końcu pić można na zwykłej ławce i na otwartej przestrzeni. Modernizacja placu zabaw została ujęta w pracach projektowych na kolejne lata. Do czasu realizacji dzieci i seniorzy z Grębałowa zostają z niczym.

JAN Z KRAKOWA

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

STOP DYSKRYMINACJI TOALETOWEJ

Z wiekiem rośnie częstotliwość korzystania z toalety, przez co dla wielu osób starszych wyjście na zakupy czy do urzędu musi być przemyślaną wyprawą. Ale problem nietrzymania moczu nie jest jedyną kwestią, która powstrzymuje seniorów przed swobodnym poruszaniem się w przestrzeni publicznej. Winowajcami są także ograniczony dostęp do publicznych toalet oraz wysokie opłaty za skorzystanie z nich. To skandal, by w XXI wieku brakowało tak podstawowych rzeczy, dlatego priorytetem stała się realizacja kampanii „Toalety ratują życie".

W szczególności osoby starsze, rodziny z dziećmi oraz osoby z niepełnosprawnością zmagają się z trudnościami związanymi z brakiem tego rodzaju udogodnień w przestrzeni publicznej. Brak publicznych toalet często skutkuje niekomfortowymi i krępującymi sytuacjami.

Przypominamy, że nietrzymanie moczu występuje u ponad 50% kobiet po 60 roku życia. W przypadku zespołu pęcherza nadreaktywnego konieczność częstokrotnego i natychmiastowego korzystania z toalety w ciągu dnia jest kluczowa dla chorych. Ich brak ma swoje konsekwencje – seniorzy izolują się od społeczeństwa i wycofują z wszelkich aktywności wymagających wyjścia z domu.

Przeraża również obojętność pracowników wielu dyskontów, w których pobliżu nie znajduje się żadna toaleta. Najczęściej nie pozwalają na skorzystanie z niej nawet w naprawdę trudnych sytuacjach i zasłaniają się przepisami. Apelujemy do decydentów o wprowadzenie **obowiązku** stawiania toalet dla klientów i osób „z zewnątrz" w istniejących i nowo budowanych dużych sklepach, kościołach, parkach i dworcach.

Jeśli byliście świadkami lub ofiarami dyskryminacji toaletowej, prosimy o przesłanie takiej informacji: mailem na adres **ogs@manko.pl**, pocztą na adres **os. Urocze 12, 31-953 Kraków** lub telefonicznie pod numerem **12 429 37 28**.

OBNIŻMY CENY PRYWATNYCH WIZYT LEKARSKICH

Zgodnie z danymi statystycznymi na wizytę u specjalisty przyjmującego w ramach Narodowego Funduszu Zdrowia czeka się długie 12 miesięcy. Rozwiązaniem wydaje się pójście na prywatną konsultację – niestety nie w Polsce, gdzie cena takiej wizyty wynosi nawet 800 złotych. Lekarze zasługują na godną płacę, ale powinna ona uwzględniać otaczające nas realia. Czy seniora, który ma najniższą emeryturę i wymaga natychmiastowego leczenia, stać na taką wizytę?

Dostęp do opieki medycznej to jedno z podstawowych praw człowieka, ale sytuacja w publicznej ochronie zdrowia zmusza pacjentów do szukania pomocy w prywatnych gabinetach, gdzie czas oczekiwania na specjalistę jest o wiele krótszy. Jednakże w wielu przypadkach seniorzy rezygnują nawet z takiego rodzaju konsultacji, a to ze względu na horrendalne kwoty. Niestety to może prowadzić do pogorszenia stanu zdrowia seniora lub rezygnacji z innych podstawowych potrzeb na rzecz leczenia.

– Wykształcili się z naszych podatków i na bezpłatnych uczelniach państwowych, a teraz liczą za wizytę od nas, seniorów, nawet 700 złotych? To jest chore i nieetyczne – mówi nam pani Dorota z Mazowsza.

Według badań Głównego Urzędu Statystycznego w zeszłym roku Polacy wydali na prywatną opiekę medyczną około 44 miliardy złotych. Brakuje nie tylko terminów do publicznych gabinetów, ale także samych lekarzy, w tym geriatrów – w naszym kraju jest ich niewiele ponad 500.

Apelujemy do decydentów o skuteczną interwencję i regulację cen prywatnych wizyt lekarskich, z kolei od lekarzy oczekujemy przyzwoitości i uczciwości. Nie można stawiać seniorów pod ścianą – tu chodzi o ich życie i zdrowie, a niekiedy nawet przetrwanie z dnia na dzień. Po wydaniu kolosalnej kwoty na kilkunastominutową, ale niezbędną konsultację seniorowi zostają grosze na opłacenie rachunków i zakup lekarstw oraz jedzenia.

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO
NIW
Organizacje Poradnicze
SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU WSPIERANIA ROZWOJU ORGANIZACJI PORADNICZYCH NA LATA 2022–2033

SENIORZE, ZASTRZEŻ PESEL

W listopadzie zeszłego roku Ministerstwo Cyfryzacji wprowadziło usługę „Zastrzeż PESEL", a od czerwca 2024 roku wszelkie instytucje finansowe, notariusze oraz operatorzy komunikacyjni są zobowiązani do sprawdzenia Rejestrów Zastrzeżeń Numerów PESEL, zanim podpiszą z kimś umowę lub udzielą mu pożyczki. Z możliwości zastrzeżenia PESEL-u może skorzystać każda osoba pełnoletnia i to bez podawania przyczyny. Akcja promująca zastrzeganie numeru została zainaugurowana na konferencji z udziałem ministra cyfryzacji Krzysztofa Gawkowskiego i minister ds. polityki senioralnej Marzeny Okły-Drewnowicz, która poparła kampanię.

Głównym celem oszustów jest pozyskanie danych osobowych. Sztuczna inteligencja pozwala im na przeprowadzenie coraz doskonalszych ataków. Do tej pory rozpoznanie fałszywej strony internetowej było możliwe, ale dziś bywa to problematyczne. Nie trzeba jednak korzystać z Internetu, by paść ofiarą hakerów. Skarbnicą danych osobowych i wrażliwych są m.in. placówki medyczne, w których poziom zabezpieczeń pozostawia wiele do życzenia.

GDZIE I JAK ZASTRZEC PESEL?

PESEL można wielokrotnie zastrzegać nie tylko za pomocą aplikacji mObywatel, ale także w serwisie internetowym mObywatel oraz w urzędzie gminy. Jednak opcja mObywatel pozwala na bezterminowe cofnięcie zastrzeżenia numeru PESEL, ustawienie daty automatycznego zastrzeżenia, a także sprawdzenie, które firmy i instytucje szukały informacji o naszym PESEL-u i z jakiego powodu. Mimo wszystko Ministerstwo Cyfryzacji zaleca, by numer był zastrzeżony cały czas.

Zastrzeżenie PESEL-u nie wpływa na:

- sprawy urzędowe (wzięcie ślubu, zameldowanie się czy wyrobienie dokumentów),
- sprawy zdrowotne (wizyty u lekarza, pobyt w szpitalu czy wykupienie recepty),
- udział w wyborach,
- ważność dokumentów (dowodu osobistego, paszportu czy prawa jazdy),
- korzystanie z profilu zaufanego,
- podróżowanie (przekraczanie granicy, podróże lotnicze czy kupowanie biletów lotniczych),
- wykonywanie czynności służbowych (podpisywanie umów w pracy),
- korzystanie z usług poczty (Poczta Polska może ubiegać się o dostęp do weryfikacji zastrzeżenia w rejestrze, ale nie ma takiego obowiązku ustawowego).

ZASTRZEŻENIE MOŻNA COFNĄĆ

Zastrzeżenie można cofnąć w każdej chwili zarówno w aplikacji i na stronie internetowej, jak i w urzędzie gminy. Taka decyzja jest bezterminowa (dopóki nie postanowimy zastrzec go ponownie) lub czasowa (następuje automatyczne zastrzeżenie). Należy pamiętać, że zmiana statusu może nastąpić dopiero po 30 minutach od poprzedniego zastrzeżenia.

Kiedy warto cofnąć zastrzeżenie? Kiedy chcemy załatwić ważną sprawę lub podpisać umowę z:

- firmami i instytucjami finansowymi: umowa o kredyt, pożyczkę, zakup z płatnością ratalną czy leasing,
- notariuszami: umowa o kupnie lub sprzedaży nieruchomości,
- operatorami telekomunikacyjnymi: prośba o kopię karty SIM.

SENIORZE, ZASTRZEŻ PESEL

Decyzja o zastrzeżeniu numeru PESEL to przejaw troski o własne bezpieczeństwo, a także finanse. W sytuacji gdy oszuści zaciągną kredyt lub inne zobowiązanie na osobę, która zastrzegła PESEL, instytucja finansowa nie może domagać się spłaty od pokrzywdzonej osoby.

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO
NIW
Organizacje Poradnicze
SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU WSPIERANIA ROZWOJU ORGANIZACJI PORADNICZYCH NA LATA 2022–2033

ZAŻYWAJ LEKI BEZPIECZNIE

Aż 1,5 mln seniorów w Polsce nadużywa leków. Nadmierne dawkowanie ma wiele negatywnych konsekwencji: zatrucia, uszkodzenie organów, uzależnienie oraz marnotrawstwo pieniędzy. Zażywanie kilku lekarstw jednocześnie podnosi ryzyko groźnych powikłań i niepożądanych interakcji albo neutralizowania ich działania. Przyjmowanie już 4 medykamentów sprawia, że ryzyko wynosi 38%. W przypadku 7 i 10 lekarstw to zagrożenie wzrasta kolejno do 82% i 100%.

Trzeba temu przeciwdziałać, aby podnosić świadomość i jakość życia polskich seniorów. W edukowaniu osób starszych pomaga kampania pn. „Zażywaj leki bezpiecznie", która 8 lat temu została zainicjowana przez Stowarzyszenie MANKO – Głos Seniora. Jest realizowana we współpracy z Polskim Towarzystwem Opieki Farmaceutycznej, Minister ds. Polityki Senioralnej i Rzecznikiem Praw Pacjenta. Poprzez wykłady i warsztaty promujemy rozsądne zażywanie leków, prowadzenie dzienniczka lekowego oraz przeprowadzanie przeglądu lekowego dla osób powyżej 60 roku życia. Ta usługa jest wykonywana przez farmaceutów współpracujących z lekarzami rodzinnymi i polega na spotkaniu z pacjentem oraz zebraniu szczegółowego wywiadu medycznego. Farmaceuci pomagają również we właściwym stosowaniu leków. Pacjent na spotkanie przynosi torbę ze wszystkimi przyjmowanymi medykamentami (lekami na receptę i bez recepty, suplementami diety, preparatami pochodzenia naturalnego), aby konsultant przygotował indywidualny plan opieki.

Nadużywanie leków i suplementów to problem zwany polipragmazją. Nasila się on między innymi na skutek atrakcyjnych reklam w mediach obiecujących natychmiastowe działanie. Brak edukacji w tym zakresie potwierdzają badania dotyczące spożywania produktów aptecznych, zgodnie z którymi nasz kraj jest w czołówce rankingu uwzględniającym państwa europejskie. W polskich aptekach zostawiamy rocznie aż 50 mld złotych, z tego 25 mld złotych wydajemy na leki bez recepty, a 5 mld złotych – na suplementy. Wśród leków bez recepty prym wiodą produkty na przeziębienie, leki przeciwbólowe, wspomagające przemianę materii, uspokajające i na żołądek. To zdecydowanie negatywny aspekt samoleczenia, które – choć służy pacjentowi i systemowi – musi być odpowiedzialne.

W zeszłym roku zaprezentowano wyniki Pilotażowego Przeglądu Lekowego, do którego dołączyło również Stowarzyszenie MANKO. Był on koordynowany przez prof. Agnieszkę Neumann-Podczaską z Uniwersytetu Medycznego w Poznaniu. Na podstawie Rozporządzenia Ministra Zdrowia udało się zaangażować 75 aptek i 850 pacjentów w całym kraju. Jak się okazało, uczestnicy zażywali średnio 16 medykamentów dziennie. Po przeglądzie aż 80% pacjentów przyznało, że czuje się lepiej.

Bezpieczeństwo lekowe to temat wielokrotnie podejmowany przez Stowarzyszenie MANKO – Głos Seniora w ramach kampanii „Bezpieczny Senior" podczas wydarzeń w całej Polsce, m.in. w Warszawie, Łodzi, Gdańsku, Bydgoszczy, Muszynie, Piwnicznej, Łysomicach, Bieczu, Harmężach, Skawinie czy Andrychowie. Ostatnimi czasy prezes Stowarzyszenia MANKO i Międzynarodowego Instytutu Rozwoju Społecznego, Łukasz Salwarowski, miał okazję zaprezentować ten wykład podczas Konferencji w Sejmie RP oraz podczas Targów VIVA Seniorzy na Międzynarodowych Targach Poznańskich. W ramach kampanii wydaliśmy ponad 50 tysięcy dzienniczków lekowych, nagraliśmy 4 spoty wideo, zorganizowaliśmy 40 konferencji i 400 warsztatów. Kampania „Zażywaj leki bezpiecznie" będzie kontynuowana w kolejnych latach. Zapraszamy do współpracy, bo razem możemy więcej.

JAKIE SPRAWY ZAŁATWIĆ PO ŚMIERCI BLISKIEJ OSOBY?

Nie każdy wie, jakie formalności trzeba załatwić po śmierci bliskiej osoby. Okazuje się, że to nie tylko kwestia uzyskania aktu zgonu i zorganizowania pogrzebu, ale także uregulowanie spraw konsumenckich zmarłego.

Warto pamiętać o możliwości ubiegania się o świadczenia na wypadek zgonu:

- **zasiłek pogrzebowy** – jest wypłacany przez ZUS osobom lub podmiotom, które zorganizowały i opłaciły pogrzeb. Obecnie wynosi 4000 złotych;
- **odprawa pośmiertna** – świadczenie przewidziane dla rodziny osoby, która w chwili śmierci była zatrudniona lub pobierała zasiłek z tytułu niezdolności do pracy z powodu choroby. Jest zależne od stażu zatrudnienia oraz liczby osób, którym przysługuje renta rodzinna, i wypłacane przez pracodawcę. Przy zatrudnieniu krótszym niż 10 lat odprawa wynosi tyle co miesięczne wynagrodzenie, przy zatrudnieniu równym 10 lat odprawa to trzykrotność wynagrodzenia, a przy zatrudnieniu równym 15 lat odprawa to sześciokrotność wynagrodzenia;
- **renta rodzinna** – świadczenie przysługujące małżonkowi, dzieciom i rodzicom osoby zmarłej, jeśli przed śmiercią dana osoba miała przyznane prawo do emerytury lub renty;
- **ubezpieczenie na wypadek śmierci** – świadczenie wypłacane przez firmę ubezpieczeniową, jeśli zmarły zawarł wcześniej umowę ubezpieczenia na życie.

ZOBOWIĄZANIA KONSUMENCKIE

Jeżeli zmarły miał zobowiązania wobec jakichś podmiotów i podpisał z nimi umowy, trzeba poinformować je o zgonie, ponieważ dostawcy usług nie otrzymują informacji o śmierci klienta z urzędu. W przeciwnym wypadku dana placówka wciąż może wystawiać faktury na nazwisko zmarłego.

Należy zamknąć konto bankowe, które należało do osoby zmarłej. Do zablokowania najczęściej wystarczy akt zgonu, jednakże do odblokowania może być potrzebny dokument wydany przez sąd o stwierdzeniu nabycia spadku. W przypadku kredytu i pożyczki zobowiązanie jest traktowane jako część tego spadku. Najlepiej dokładnie sprawdzić dokumentację zmarłego, w której znajdzie się kolejność poszczególnych etapów procesu zakończenia zobowiązań.

Jeśli zmarły założył polisę na życie i Otwarty Fundusz Emerytalny, pieniądze dziedziczą spadkobiercy. Podobnie wygląda sytuacja z mieszkaniem – należy się spadkobiercy, a jeżeli zmarły nie zostawił testamentu, to w pierwszej kolejności lokum dziedziczy małżonek i dzieci zmarłego.

W dzisiejszych czasach istotną kwestią stały się serwisy społecznościowe. Członek rodziny może zamknąć profil zmarłego, wystarczy zgłosić się do administracji portalu i dostarczyć akt zgonu.

TECZKA Z NAJWAŻNIEJSZYMI DOKUMENTAMI

Przed śmiercią warto sporządzić listę istotnych informacji oraz dokumentów, które ułatwią załatwienie wszelkich informacji po naszej śmierci. Najlepiej założyć teczkę i ją podpisać. Co powinno się w niej znaleźć: opis – co znajduje się w teczce; najważniejsze kontakty – numery osób upoważnionych do odbioru dokumentacji czy wizyt w szpitalu; testament; informacje o emeryturze i innych świadczeniach, w tym o polisie na życie; kontakt do pracodawcy; lista banków, w których otworzyłeś rachunek i zaciągnąłeś pożyczki czy kredyty; dane o prywatnych pożyczkach – lista osób i kwoty do oddania; akt notarialny potwierdzający własność nieruchomości; kopia dokumentów samochodu; login i hasło do urządzeń i skrzynek pocztowych oraz do profili społecznościowych; oświadczenie o ewentualnej zgodzie na pobranie organów do przeszczepu. Aktualizuj informacje raz do roku i wpisuj datę ostatniej aktualizacji. To ułatwi bliskim załatwianie wszystkich spraw po twojej śmierci.

Więcej informacji znajduje się w poradniku „O czym pamiętać po stracie bliskiej osoby" wydanym przez Urząd Ochrony Konkurencji i Konsumentów. Jest dostępny na stronie **https://uokik.gov.pl/smierc-bliskiej-osoby-a-prawne-formalnosci**.

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024

NOŚ ODBLASKI I ŻYJ

Stowarzyszenie MANKO – Głos Seniora od lat promuje edukację z zakresu bezpieczeństwa konsumenckiego, lekowego oraz drogowego w ramach kampanii „Bezpieczny Senior. Stop manipulacji – nie daj się oszukać!". W obszarze bezpieczeństwa drogowego zorganizowaliśmy kampanię „Noś odblaski i żyj" w partnerstwie z Małopolską Wojewódzką Radą Bezpieczeństwa Ruchu Drogowego oraz pokaz mody „Bezpiecznie, stylowo, odblaskowo". Należy podkreślić, że musimy być uważni nie tylko jako piesi, ale także jako kierowcy – właśnie dlatego zapoczątkowaliśmy akcję „Zostań mobilnym ambasadorem Głosu Seniora".

W ostatnich latach około 30% poszkodowanych na drogach stanowią osoby powyżej 65 roku życia. Jeżeli wziąć pod uwagę tylko pieszych i rowerzystów, seniorzy to aż połowa wszystkich ofiar. Niestety co roku to właśnie osoby starsze najczęściej ulegają wypadkom drogowym, dlatego ważna jest edukacja i uświadamianie na temat przestrzegania przepisów i widoczności na drodze.

Jako Stowarzyszenie MANKO – Głos Seniora czynimy to poprzez liczne kampanie, m.in. „Noś odblaski i żyj". W ramach akcji cyklicznie organizowane są pokazy mody Stylowych Seniorów Głosu Seniora pod hasłem „Bezpiecznie, stylowo, odblaskowo". To doskonała forma promowania odblaskowych ubrań, które ratują życie. W ostatnim czasie taka wersja pokazu mody w wykonaniu ambasadorów Głosu Seniora zyskała zainteresowanie na wielu ważnych wydarzeniach i imprezach. Seniorzy zaprezentowali się podczas: konferencji „Bezpieczny Senior" w Sejmie Rzeczypospolitej Polskiej, XI Międzynarodowych Senioraliów w Krakowie, IV Nowohuckich Senioraliów, III Wielickich Senioraliów czy konferencji w Gdowie i Szczurowej.

Uczestnicy pokazów udowodnili, że noszenie kolorów jest modne – żywe odcienie nie tylko dodają energii, ale także poprawiają widoczność seniora na drodze. Podczas wieczornych spacerów unikaj szarych, stonowanych odcieni, postaw na jaskrawe barwy. Wyróżnianie się z tłumu to nic złego, a wręcz przeciwnie – może uratować życie. Jeżeli nie chcesz zakładać całego stroju w wyraźnych kolorach, pamiętaj choćby o jednym elemencie, np. odblaskowej opasce. Warto wiedzieć, że w ciemnych ubraniach jesteśmy widoczni zaledwie z odległości 20–30 metrów. Samochód poruszający się z prędkością 90 km/h taki dystans pokonuje w mgnieniu oka, kierowca nie zdąży więc zareagować, a tym bardziej bezpiecznie wyminąć. Jeżeli pieszy założy odblask, kierujący pojazdem dostrzeże go z odległości pięciokrotnie dalszej. Trzeba pamiętać także o tym, aby element odblaskowy był widoczny dla kierujących z obydwóch stron.

Ostrożność dotyczy nie tylko pieszych, lecz także kierowców. Aby propagować bezpieczną jazdę, rozpoczęliśmy akcję „Mobilny ambasador Głosu Seniora". Inicjatywa ma pokazać, że seniorzy dbają o bezpieczeństwo zarówno swoje, jak i innych. Seniorze, jeśli jeździsz bezpiecznie i chcesz promować Ogólnopolską Kartę Seniora, zgłoś się do nas! Dostaniesz magnesy i nasze magazyny, które możesz podarować bliskim i sąsiadom. Czekamy na Wasze zgłoszenia na adres: **ogs@manko.pl**.

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 umowy[1]/odbioru[2](*)……..…….

……
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.) ostępuję od umowy kredytu o numerze…… zawartej dnia…… z firmą……

……
(czytelny podpis)

ZAMÓW PRENUMERATĘ

OGÓLNOPOLSKIEGO MAGAZYNU GŁOS SENIORA

RODZAJ PRENUMERATY:

12 zł* – jeden wybrany egzemplarz

60 zł* – 6 kolejnych numerów

W wartość prenumeraty wliczona jest wysyłka listem ekonomicznym.
Jak zamówić prenumeratę? Wejdź na:

https://glosseniora.pl/prenumerata/

wydrukuj i wypełnij formularz, ureguluj opłatę, załącz potwierdzenie wpłaty i wyślij na adres **os. Urocze 12, 31–953 Kraków** lub adres e-mail **kontakt@manko.pl**.

OGÓLNOPOLSKA KARTA SENIORA

Seniorze, jeśli ukończyłeś 60 lat, zostań członkiem wspierającym Stowarzyszenia MANKO i odbierz Ogólnopolską Kartę Seniora. Ciesz się ze zniżek w ponad 4000 punktach w całej Polsce. Opłata członkowska wynosi: 35 zł na rok i 50 zł na 2 lata.

JAK ZAMÓWIĆ KARTĘ? Wejdź na:

https://glosseniora.pl/ogolnopolska-karta-seniora/

wydrukuj i wypełnij formularz, ureguluj opłatę członkowską, załącz potwierdzenie wpłaty i wyślij na adres **os. Urocze 12, 31–953 Kraków** lub adres e-mail **poczta@manko.pl**.

WESPRZYJ DZIAŁALNOŚĆ „GŁOSU SENIORA" DAROWIZNĄ

DOWÓD/POKWITOWANIE DLA ZLECENIODAWCY

nr rachunku odbiorcy
66 2490 0005 0000 4600 9366 4184

odbiorca:
Stowarzyszenie MANKO
os. Urocze 12
31-953 Kraków

kwota:

zleceniodawca:

tytułem:

stempel dzienny

opłata:

nazwa odbiorcy
Stowarzyszenie MANKO

nazwa odbiorcy cd.
os. Urocze 12, 31-953 Kraków

nr rachunku odbiorcy
6 6 2 4 9 0 0 0 0 5 0 0 0 0 4 6 0 0 9 3 6 6 4 1 8 4

waluta: W X PLN

kwota:

nr rachunku zleceniodawcy (przelew) / kwota słownie (wpłata)

nazwa zleceniodawcy

nazwa zleceniodawcy c.d.

tytułem
Darowizna na cele statutowe

tytułem cd.
- Głos Seniora

06

Opłata:

pieczęć, data i podpis(y) zleceniodawcy

DRUK WYGENEROWANO ZA POMOCĄ www.dmr.vot.pl/posk

Numer karty:

FORMULARZ DLA OSÓB CHCĄCYCH PRZYSTĄPIĆ DO PROGRAMU OGÓLNOPOLSKA KARTA SENIORA*

Ja niżej podpisany, po zapoznaniu się z Regulaminem Ogólnopolskiej Karty Seniora opisującym tego Programu, wyrażam chęć Uczestnictwa w tym Programie. Oświadczam, że wiem, że udział w tym Programie jest możliwy wyłącznie pod warunkiem przystąpienia w poczet członków wspierających Stowarzyszenie Manko i właśnie dlatego uprzejmie proszę o przyjęcie mojej osoby w poczet członków wspierających.

PROSZĘ WYPEŁNIC 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:

Deklaruję opłacenie składki członkowskiej z góry za: **1 rok – 35 zł** ☐ **2 lata – 50 zł** ☐

OŚWIADCZENIE O WYRAŻENIU ZGODY

Oświadczam, iż wyrażam dobrowolną i wyraźną zgodę na przetwarzanie przez Administratora, tj. Stowarzyszenie MANKO oraz Partnera operacyjnego Programu tj. Międzynarodowy Instytut Rozwoju Społecznego sp. z o.o. (MIRS), z siedzibami przy os. Uroczym 12, 31-953 Kraków, moich danych osobowych

w celu otrzymywania od Stowarzyszenia MANKO i 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 Stowarzyszenie MANKO i Międzynarodowy Instytut Rozwoju Społecznego sp. z o.o. oraz ich partnerów, np. wydarzeń organizowanych dla seniorów, informacji o partnerach Programu 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. 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. ☐ TAK ☐ NIE

w celu przekazywania przez Stowarzyszenie MANKO i Międzynarodowy Instytut Rozwoju Społecznego sp. z o.o. treści, dotyczących oferty Stowarzyszenia i MIRSu oraz Partnerów Programu 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 w ramach programu 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 Stowarzyszenia MANKO o numerze: 80 2490 0005 0000 4600 0004 0502 (Alior Bank)**

.....
Data, podpis

* 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).

KOPALNIA SOLI
BOCHNIA

Odkryj podziemne atrakcje

Podziemny Skarb Małopolski

Kopalnia Soli Bochnia, najstarsza kopalnia soli kamiennej w Polsce, jest wyjątkowym zabytkiem kultury i techniki, położonym zaledwie 40 km od Krakowa. Założona w 1248 roku, stanowiła przez wieki jedno z głównych źródeł bogactwa Królestwa Polskiego. Dziś, wpisana na Listę Światowego Dziedzictwa UNESCO, zachwyca nie tylko historycznym znaczeniem, ale także unikatowym pięknem podziemnych korytarzy i komór. Podczas zwiedzania można podziwiać zabytkowe wyrobiska, kaplice wykute w soli oraz dowiedzieć się więcej o procesie wydobycia soli. Zwiedzanie kopalni to niezwykła podróż w czasie, która z pewnością zapadnie w pamięć.

Honorujemy Ogólnopolską Kartę Seniora!

Posiadacze Karty otrzymują 30% zniżki na zwiedzanie Trasy Turystycznej z Ekspozycją Multimedialną, 3-godzinny Pobyt Rekreacyjny w Komorze Ważyn oraz Pobyt Nocny.

Informacja i rezerwacja:

Biuro Obsługi Klienta:

tel. 14 692 67 52, 14 692 67 54

www.kopalnia-bochnia.pl

Głos SENIORA

OBYWATELSKI KONGRES ORGANIZACJI SENIORSKICH I LIDERÓW SENIORALNYCH *Głosu Seniora*

AKADEMIA EKONOMICZNO-HUMANISTYCZNA W WARSZAWIE
KAMPUS VIZJA PARK, AULA GŁÓWNA 234
OKOPOWA 59, 01-043 WARSZAWA

10 GRUDNIA 2024

REJESTRACJA: 9:00
START: 10:00

OBOWIĄZKOWE ZAPISY NA:
www.glosseniora.pl/ObywatelskiGlosSeniora

ORGANIZATOR:

MANKO STOWARZYSZENIE

PARTNERZY:

POLSKIE TOWARZYSTWO OPIEKI FARMACEUTYCZNEJ

AKADEMIA EKONOMICZNO-HUMANISTYCZNA W WARSZAWIE

INSTYTUT SENIORALNY

WSPÓŁFINANSOWANIE:

AKTYWNI+

Zadanie publiczne jest współfinansowane ze środków otrzymanych od Zleceniodawcy w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025. Edycja 2024


Twój procent...
ma znaczenie.
1,5%
Przekaż 1,5% podatku Stowarzyszeniu MANKO - Głos Seniora na Fundusz Wsparcia Samotnych i Oszukanych Seniorów.
KRS: 0000225549
Głos Seniora
- od 15 lat z myślą o osobach starszych
MANKO
STOWARZYSZENIE