SENIOR ONLINE

Kilka słów o bezpieczeństwie osób starszych

AKTYWNI+

Ministerstwo Rodziny i Polityki Społecznej

FUNDACJA Wiedzy Obywatelskiej

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025.

SENIOR ONLINE
KILKA SŁÓW O BEZPIECZEŃSTWIE OSÓB STARSZYCH

Z myślą o starości. Z misją dla seniorów!

Redakcja: Oskar Jurek
Redakcja językowa: Aleksandra Pszczoła
Projekt okładki: PINK PIXELS Ewa Prokop Rodzoń
Skład i łamanie: PINK PIXELS Ewa Prokop-Rodzoń

ISBN 978-83-67976-03-9

Wydawca: Fundacja Misji Obywatelskiej
Ropa 354, 38–312 Ropa
tel. + 48 694 919 498
kontakt@fmo.com.pl

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025.

Rzeszów, 2023

FUNDACJA
Misji Obywatelskiej

SENIOR ONLINE
KILKA SŁÓW O BEZPIECZEŃSTWIE OSÓB STARSZYCH

Z myślą o starości. Z misją dla seniorów!

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025.

AKTYWNI+

Ministerstwo Rodziny i Polityki Społecznej

Spis treści

Wstęp

Szanowni Państwo,

Fundacja Misji Obywatelskiej oddaje w Państwa ręce broszurę pt. ***SENIOR ONLINE. KILKA SŁÓW O BEZPIECZEŃSTWIE OSÓB STARSZYCH.***

Internet, nowoczesne technologie dają wiele możliwości, które jeszcze do niedawna były czymś niewyobrażalnym i odległym w ludzkiej rzeczywiści. Dziś w każdej chwili bez względu na miejsce i godzinę możemy połączyć się z dowolną osobą na świecie, przejrzeć wybrany przez siebie serwis informacyjny, zrobić zakupy, opłacić rachunki, pracować bądź obejrzeć ulubiony serial.

Niestety nowoczesne technologie, tak jak każde inne narzędzia są wykorzystywane przez przestępców do kradzieży wrażliwych danych.

Seniorzy są grupą osób szczególnie narażonych na działania przestępców ze względu na fakt, że uważają oni osoby starsze za łatwowierne.

Niniejsza broszura nie ma na celu zniechęcić Cię do korzystania z Internetu i nowoczesnych technologii. Wręcz przeciwnie! Ma ona na celu przedstawić Ci główne zagrożenia występujące w tym obszarze, które ułatwią Tobie bezpieczne korzystania z Internetu i nowoczesnych technologii w codziennym życiu.

Kilka słów o Fundacji

Fundacja Misji Obywatelskiej jest owocem efektywnej współpracy grupy młodych osób, mających na celu dobro, a także rozwój i bezpieczeństwo Ojczyzny.

Działalność organizacji opiera się na trzech filarach. **Pierwszym** jest **wymiar społeczny**, mający aktywizować grupy społeczne, w szczególności dzieci, młodzież, a także seniorów. **Drugim** filarem jest **działalność ekspercka** w zakresie bezpieczeństwa, prawa, ekonomii oraz gospodarki, natomiast **trzeci** stanowi wymiar **medialny** w zakresie budowania i prowadzenia mediów obywatelskich oraz dialogu społecznego.

Główne cele:

- wspieranie, promowanie i podtrzymywanie tradycji narodowej,
- pielęgnowanie polskości oraz rozwoju świadomości narodowej, obywatelskiej, cywilizacyjnej i kulturowej.

Adam Poręba, Oskar Jurek, Antoni Myjak

O projekcie słów kilka

Z myślą o starości. Z misją dla seniorów! to projekt realizowany przez **Fundację Misji Obywatelskiej** tworzoną przez grupę młodych osób działających na rzecz rozwoju społeczeństwa obywatelskiego w południowo-wschodniej Polsce.

Jego celem jest zwiększenie uczestnictwa seniorów we wszystkich dziedzinach życia społecznego poprzez wzmacnianie trwałych relacji międzypokoleniowych, kształtowanie empatycznych postaw wobec seniorów, upowszechnienie pozytywnego wizerunku osób starszych oraz zwiększenie ich wiedzy i świadomości na liczne zagrożenia.

Projekt jest realizowany dzięki wsparciu Ministerstwa Rodziny i Polityki Społecznej.

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych ,,Aktywni+'' na lata 2021-2025.

Projekty Fundacji Misji Obywatelskiej

■ **Projekt pn. „Przystanek – Czas na Podkarpacką Młodzież!"** – został zaadresowany do młodzieży w wieku 15–29 lat działającej na terenie województwa podkarpackiego. Projekt zakładał zwiększenie zaangażowania młodzieży i młodzieżowych organizacji pozarządowych w życie publiczne przez wsparcie inicjatyw młodzieżowych, a także wzrost ich znaczenia w życiu publicznym i wzmocnienia instytucjonalnego. Wykorzystany został mechanizm regrantingu, który umożliwi skuteczne dotarcie do podmiotów lokalnych i wspieranie młodzieżowych rad i sejmików, samorządów studenckich i uczniowskich czy uczelnianych organizacji studenckich i doktoranckich.

■ **„Szanse na deglomerację Polski na przykładzie powiatu gorlickiego i jasielskiego"** – celem projektu była diagnoza sytuacji społeczno-ekonomicznej powiatów jasielskiego i gorlickiego w odniesieniu do pozostawania ludzi aktywnych zawodowo na ich terytorium lub powrotów po skończonej edukacji. Ponadto założenia projektu ukierunkowane są na poznanie subiektywnej opinii mieszkańców dwóch ww. powiatów na temat ich życia, oczekiwań, perspektyw zawodowych, działań państwa i samorządu zmierzających do poprawy jakości życia, zbadanie uwarunkowań pozwalających na powrót młodych ludzi, którzy wyjechali na studia lub do pracy do dużych miast, a także przedstawienie sytuacji w Gorlicach i Jaśle na tle dawnych miast wojewódzkich Krosna i Nowego Sącza.

■ **Projekt pn. „Z myślą o starości. Z misją dla seniorów!"** – zakładał zwiększenie uczestnictwa seniorów we wszystkich dziedzinach życia społecznego poprzez wzmacnianie trwałych relacji międzypoko-

leniowych, kształtowanie empatycznych postaw wobec seniorów, upowszechnienie pozytywnego wizerunku osób starszych oraz zwiększenie ich wiedzy i świadomości na liczne zagrożenia (bezpieczeństwo). Cel ten został osiągnięty poprzez realizację projektu składającego się z cyklu szkoleniowego (bezpieczeństwo zdrowotne, prawne, społeczne, cyfrowe i internetowe), które było wsparte spotkaniami z specjalistami i doradztwem. Został również zorganizowany wolontariat dla seniorów, spotkania międzypokoleniowe oraz kampania kształtująca empatyczne postawy wobec osób starszych oraz upowszechniania pozytywnego wizerunku seniorów. Projekt skierowany został skierowany do osób starszych i realizowany był na terenie województwa podkarpackiego.

- **„Międzynarodowy Dzień Dziecka w Rzeszowie (2023)** – miał na celu przede wszystkim propagowanie idei braterstwa i zrozumienia pomiędzy dziećmi całego świata, jak również promowanie działań na rzecz ich pomyślnego rozwoju. Wspieranie wymienionych idei nabywa szczególnego znaczenia w sytuacji, kiedy w sąsiadującym z województwem podkarpackim kraju trwa od ponad roku pełnoskalowy konflikt zbrojny. Wydarzenie miało charakter prospołeczny i proedukacyjny. Pierwszy aspekt miał na celu nauczeniu dzieci tolerancji, która w przyszłości z pewnością będzie owocowała wzajemnym zrozumieniem i dialogiem. Z kolei drugi aspekt odnosi się do poznawania różnych kultur i zwyczajów. Warto zaznaczyć, że podczas wydarzenia pojawiły się także stoiska promocyjno-edukacyjne, w tym dotyczące pierwszej pomocy. Współorganizatorami wydarzenia byli: Fundusz Narodów Zjednoczonych na rzecz Dzieci , UNICEF, UNHCR, IOM.

- **„Historia oczami Podkarpacia. Wolność po podkarpacku”** – miał na celu wzrost wiedzy uczestników na temat historii, polskiego dziedzictwa kulturowego oraz myśli społeczno-politycznej. Na realizowane przez Fundację Misji Obywatelskiej przedsięwzięcie składał się cykl wywiadów, seminariów, konkursu historycznego, debaty oraz wyjść do instytucji kultury. Wywiady i seminaria umożliwią odbiorcom

zadania zapoznanie się z opinią profesjonalistów, którzy na co dzień zajmują się działalnością naukową lub praktyczną w omawianych obszarach. Z kolei konkurs historyczny wraz z debatą miał za zadanie aktywnie włączyć uczestników w realizację projektu. Spoiwem działań były wyjścia do instytucji kultury mające na celu kształtowanie tożsamości narodowej, propagowanie odpowiednich postaw patriotycznych.

■ **Projekt „Z myślą o Ukrainie!”** – skierowany został do uchodźców przybywających zza naszej wschodniej granicy, którzy znaleźli schronienie przedwojną w Domu Seniora „Maria” w miejscowości Wapienne w powiecie gorlickim. W ramach darowizny otrzymanej ze środków Fundacji ORLEN zostały zakupione i przekazane uchodźcom z Ukrainy wsparcie pierwszej potrzeby: odzież, środki higieniczne i żywność. Zadanie realizowane latem 2022 roku objęło pomocą grupę 70 uchodźców z Ukrainy – dzieci, kobiet, osób starszych.

Bezpieczna bankowość. Jak zadbać o swoje bezpieczeństwo finansowe?

Pewnie każdy z nas spotkał się z takim powiedzeniem „masz to jak w banku". Powiedzenie to oznacza, że coś jest pewnego tak jak bezpieczeństwo naszych środków finansowych we wspomnianej instytucji. Czasy napadów na banki – przynajmniej w znanej nam formie – odeszły do lamusa. A czy to jest równoznaczne z tym, że przestępcy odpuścili chęć bezprawnego przejęcia naszych pieniędzy? Niekoniecznie.

Jako społeczeństwo jesteśmy przyzwyczajeni do tego, że wynagrodzenie lub emerytura wpływają nam na rachunek bankowy. Już jesteśmy obyci z dokonywaniem płatności kartą, do wykonywania przelewów za pomocą bankowości elektronicznej bądź podawania danych z karty, aby korzystać z dodatkowych udogodnień lub usług np. w formie comiesięcznego abonamentu.

Przestępcy z duchem czasów dostosowują narzędzia i metody do panującej rzeczywistości. Czasem nie muszą wiele w tym zakresie robić. Wystarczy nasz błąd, nasze zaniechanie, nasza łatwowierności, aby stać się ofiarą przestępstwa.

Nieraz nawet chwila nieuwagi wystarczy, że klikając w przypadkowy link stracimy oszczędności swojego życia. Dlatego bardzo ważne jest, żeby pamiętać jak ostrożnie posługiwać się swoimi danymi poufnymi w Internecie. Niestety nie ma zabezpieczeń nie do złamania, ale celem

zabezpieczeń jest utrudnienie pracy przestępcy na tyle, aby skupił się na innym celu. Nawet najlepsze hasła i oprogramowania nie pomogą nam, jeżeli sami zaprosimy złodzieja na nasze konto np. odpowiadając na podejrzane wiadomości.

PRZYKŁAD

W czerwcu 2023 r. podkarpacka Policja poinformowała, że 50 latek z powiatu ropczycko-sędziszowskiego stracił 20 tys. zł podając swoje dane do logowania w banku. Mężczyzna chciał sprzedać dziecięcy rower na jednym z popularnych portali sprzedażowych. Przestępca podał się za zainteresowanego klienta wysyłając 50-cio latkowi formularz za pośrednictwem linku. Mężczyzna za pośrednictwem formularza wpisał dane do logowania w banku zatwierdzając dane. Sytuacja ta doprowadziła do starty 20 tys. zł.

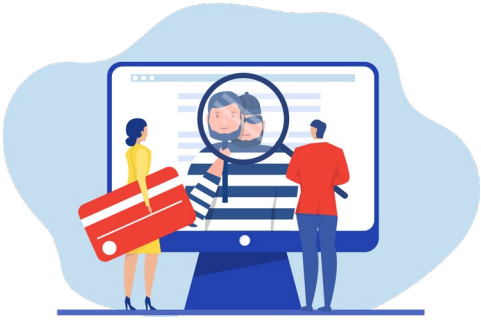
ZAPAMIĘTAJ!

Podczas korzystania z bankowości elektronicznej pamiętaj, aby:

- nie dokonywać płatności poprzez otwartą sieć Wi-Fi,
- upewnić się, czy strona lub aplikacja, przez którą logujemy się do banku jest autoryzowana (cyberprzestępcy tworzą fałszywe strony internetowe lub aplikacje podszywające się pod nasz bank),
- przelewu dokonywać z aktualnego systemu operacyjnego,
- nie podawać nikomu swoich danych do logowania,
- zweryfikować odbiorcę przelewu,
- korzystać z dodatkowej weryfikacji (np. kod SMS),
- nie korzystać z podejrzanych formularzy logowania lub formularzy przesłanych w linku.

To nie byłam ja! O tym, jak skradziono Ci tożsamość w Internecie.

Kiedy zgubimy portfel z dokumentami oraz kartami kredytowymi niezwłocznie zgłaszamy ten fakt na Policję, a wszystkie dokumenty oraz karty płatnicze zastrzegamy. Robimy to w obawie, aby przestępcy nie wykorzystali naszej tożsamości lub środków finansowych do celów niepożądanych przez nas.



Niestety nie przywiązujemy takiej uwagi przy korzystaniu z telefonu, komputera czy Internetu. Nasza czujność jest mniejsza niż w świecie realnym, ponieważ nie dopuszczamy do siebie myśli, że to ja mogę być celem przestępcy. Słysząc informacje w mediach o kolejnej ofierze cyberprzestępstwa wmawiamy sobie „ja jestem bezpieczny", „to mnie nie dotyczy", „to było oczywiste, że tak się skończy". Takie myślenie jest nieodpowiedzialne i niebezpieczne. W końcu zaniechanie też może nas słono kosztować.

Ostatnio coraz częściej słyszymy, że dane konkretnego serwisu wyciekły przez atak hakerski lub złe zabezpieczenia. Może się wydawać, że wyciek hasła i e-maila do serwisu nie jest niczym strasznym, jednak w rzeczywistości on mieć dużo konserwacji. Przykładowo wycieka Twój adres email i hasło do jakiegoś sklepu internetowego, co samym w sobie

może nie jest niczym strasznym. Ale załóżmy, że korzystasz z tego samego hasła do wielu portali, więc bardzo łatwo przestępcy mogą dostać się już do kont, gdzie udostępniasz bardziej poufne informacje takie jak np. adres zamieszkania, PESEL, numer karty kredytowej, wszystko czym dzieliłeś się z innymi osobami przez Internet.

Również mając sam dostęp do Twojego e-mail hakerzy łatwo mogą uzyskać dostęp do innych kont, wybierając opcję „zapomniałem hasła" i zmieniając hasła do Twoich kont, jednocześnie pozbawiając Ciebie dostępu do nich. W ten sposób hakerzy mając dużo danych o Tobie, mogą z łatwością się podszyć pod Ciebie w różnych miejscach, a nawet wziąć kredyt na Twoje dane. Dlatego niezwykle ważne jest, żeby dbać o swoje dane w Internecie.

ZAPAMIĘTAJ!

Korzystając z Internetu pamiętaj, aby:

- mieć osobne hasła do wszystkich usług,
- założyć osobnego e-maila do stron zakupowych,
- nie podawać danych, które nie są potrzebne,
- nie udostępniać numeru PESEL, kart oraz PIN-ów,
- chronić się przed SPAMEM,
- nie wchodzić w podejrzane wiadomości od znajomych, banków czy firm energetycznych - lepiej do nich zadzwonić i potwierdzić wysłanie wiadomości,
- nie pobierać podejrzanych aplikacji,
- zmieniać hasła co jakiś czas i trzymać je w bezpieczny miejscu.

Ciekawy ten komentarz! Kilka słów o doxingu

Doxing jest jednym z nowszych zagrożeń cybernetycznych związanych z naruszeniem naszej prywatności. Zjawisko to polega na wyszukiwaniu, zbieraniu i gromadzeniu informacji wrażliwych na temat danej osoby w celu ich rozpowszechniania w Internecie. Zazwyczaj są to informacje prywatne, które mogą upokorzyć potencjalną ofiarę czy zaszkodzić jej w życiu prywatnym albo zawodowym. Doxing głównie opiera się na fakcie, że większość z nas przechowuje i udostępnia dane na swój temat w Internecie. Dane takie są chronione różnymi poziomami zabezpieczeń, a w niektórych przypadkach i bez zabezpieczeń. Po znalezieniu tych danych zostają one szybko zabezpieczone i użyte przeciwko nam.

Wiele osób uważa, że w Internecie jesteśmy anonimowi, jednak nic bardziej mylnego, każde nasze działania zostawiają po sobie ślad, a istnieje wiele sposobów, dzięki którym możemy zostać zidentyfikowani w Internecie. Oprawca zazwyczaj wyszukuje dane przez legalne źródła, w których sami udostępniliśmy informacje o sobie – są to zazwyczaj media społecznościowe, blogi, fora internetowe czy strony firmowe. Głównie są to informacje o naszym imieniu i nazwisku, adresie zamieszkania, numerze telefonu, orientacji seksualnej, poglądach politycznych, miejscu pracy lub szkoły, a nawet mogą to być ośmieszające filmy bądź zdjęcia, na których nas widać. Doxing w ten sposób może łatwo doprowadzić

do kradzieży tożsamości, dlatego bardzo ważne jest, gdzie i jakie dane udostępniamy o sobie w Internecie.

ZAPAMIĘTAJ!

Korzystając z Internetu pamiętaj, żeby:

- nie udostępniać dużej ilości informacji dotyczących życia prywatnego i zawodowego,
- usunąć konta społecznościowe, których dawno nie używałeś i ich niepotrzebujesz,
- zmienić ustawienia prywatności w mediach społecznościowych na konta prywatne,
- ustawiać inne pseudonimy na każdym koncie,
- korzystać z możliwości zapominania haseł przez wyszukiwarkę,
- używać silnych haseł do kont,
- tworzyć odrębne e-maile do odrębnych celów takich jak cele zawodowe, prywatne i spamowe,
- pozbyć się ze znajomych starych, nieaktywnych czy podejrzanych kont,
- uważać na quizy online i inne strony, w których podajesz dużo informacji o sobie.

Babciu, przelej mi BLIKiem!

BLIK brzmi trochę strasznie, jednak nic bardziej mylnego, albowiem jest to system płatności mobilnych, który pozwala użytkownikom smartfonów płacenie bezgotówkowe w sklepach, wypłacanie i wpłacanie gotówki w bankomatach, realizowanie szybkich przelewów na numer telefonu oraz generowanie czeków z cyfrowym kodem. Kody BLIK są systemem działającym po połączeniu z Internetem. Każdy kod to 6 cyfrowa unikalna kombinacja, która jest ważna przez 2 minuty od wygenerowania.

Model płatności na podstawie kodu BLIK przebiega w następującysposób:

1. Uruchamiamy aplikację bankową i wybieramy opcję BLIK, gdzie generowany jest kod.
2. Wprowadzamy wygenerowany kod w punkcie akceptacji takim jak terminal, bankomat czy strona internetowa.
3. Teraz następuje przekazanie kodu autoryzanta przez akceptanta za pośrednictwem agenta rozliczeniowego do spółki Polskiego Standardu Płatności.
4. Kod zostaje weryfikowany przez PSP, rozpoznany przez bank, w którym go wygenerowaliśmy i przekazany bankowi do autoryzacji.
5. Bank odsyła autoryzacje do PSP, który za pośrednictwem agenta rozliczeniowego przekazuję ją do akceptacji.
6. Potwierdzamy transakcje w aplikacji bankowej, zazwyczaj przez wpisanie PINu, który mamy ustawiony w aplikacji bankowej.

Cały proces zajmuje kilkanaście sekund i w praktyce jest dość łatwy, i intuicyjny. Tylko musimy pamiętać, że nie każdy sklep ma jeszcze możliwość płacenia BLIKiem więc warto przed zrobieniem zakupów zapytać, czy jest taka możliwość.

Ze względu, iż usługa bazuje na jednorazowych 6-cyfrowych kodach jest to naprawdę bezpieczna metoda płatności. Nawet jeżeli ktoś pozna nasz kod, to straci on za chwilę ważność i osoba postronna nie będzie mgła go wykorzystać ponownie, szczególnie biorąc pod uwagę, że każdą transakcje musimy osobiście potwierdzić w aplikacji bankowej.

Mimo, iż BLIK jest stosunkowo bezpieczną metodą dokonywania płatności, to niestety również jest wykorzystywany do wyłudzeń pieniędzy. Oszuści wykorzystują BLIKa w następujące sposoby:

- **Pilna pożyczka** – przestępca po włamaniu się na konto w mediach społecznościowej bliskiej osoby ofiary pisze o potrzebuje pilnej pożyczki na niewielką kwotę i wygenerowanie kodu BLIK. Pożyczkę obiecuje zwrócić za kilka dni, a że znamy tą osobę to nie widzimy nic podejrzanego.
- **Zgubienie lub kradzież portfela** – przestępca kontaktuje się z ofiarą informując o zgubieniu lub kradzieży portfela, a musi on pilnie dokonać zapłaty np. za zakupy. Wchodzi tu gra na emocjach ofiary przekonując ją, że sprawa jest pilna, bo czeka w kolejce i zaraz jego kolej na płatność. Pod wpływem nacisku przestępcy ofiara również działa szybko i bez zastanowienia się oraz weryfikacji podaje kod BLIK.
- **Pracownik Banku** – rzekomy pracownik banku kontaktuje się z ofiarą informując ją, że wykryto próbę zaciągnięcia kredytu

na rachunek tej osoby. W celu potwierdzenia tożsamości klienta, zwraca się z prośbą o podanie informacji dotyczących stanu rachunku czy wysokości zgromadzonych środków na koncie. W pierwszej chwili po takim telefonie w ofierze pojawia się niepokój więc nieświadoma podaje wszystkie informacje. Po czym na prośbę rzekomego pracownika generuje kod BLIK, który ma pomóc w zdemaskowania oszusta. Jednak kod ten posłuży do wybrania pieniędzy z bankomatu na koszt ofiary.

- **Zakup na OLX/Vinted** – ofiara wystawia produkt na sprzedaż przez OLX/Vinted, po czym zgłasza się potencjalny kupiec, od którego dostaje wiadomość, że jest on zainteresowany zakupem produktu np. przez Inpost. Po chwili spływa odpowiedź z linkiem do potwierdzenia zakupu. Ofiara klikając w odnośnik przechodzi na rzekomą stronę firmy kurierskiej, gdzie, aby otrzymać pieniądze za produkt, musi wpisać dane karty bankowej, na którą wpłyną środki. Po wpisaniu danych pojawia się tylko prośba o wpisanie kodu BLIK i potwierdzenie wypłaty, co wiąże się z kradzieżą naszych środków z konta zamiast wpłatą. W tym wypadku bardzo ważne jest, że nie wchodzić w żadne linki, które nam druga osoba wysyła, tylko robić to np. bezpośrednio przez aplikację, która posiada wszelkie zabezpieczenia.

ZAPAMIĘTAJ!

Korzystając z BLIKa pamiętaj o tym, aby:

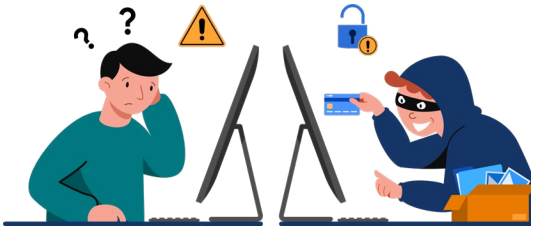
- nie podawać prywatnych danych przez telefon, nawet pracownikom banku, ponieważ mają je w systemie,
- jeżeli ktoś bliski prosi Cię o pożyczkę przez kod BLIK najpierw zadzwonić do tej osoby w celu potwierdzenia jej tożsamości,
- zanim potwierdzisz transakcję BLIK dokładnie sprawdzić, ile wynosi kwota transakcji i do kogo ona trafia,
- nie klikać w nieznane linki otrzymane od obcych osób czy numerów, prawdopodobnie przeniosą Cię one do stron wyłudzających pieniądze,
- przed zalogowaniem się na stronę banku, upewnić się czy adres strony jes twłaściwy,
- nie logować się danymi poufnymi u kogoś na telefonie czy w miejscach publicznych, korzystając z Wi-Fi do którego każdy ma dostęp.

Pomocy, moja ukochana córka umiera! Zbieramy na operację

Przeglądając informacje dostępne w Internecie wcześniej czy później natrafimy na internetową zbiórkę. Zdecydowana większość z nich, jak w codziennym życiu dotyczy wsparcia finansowego w walce z chorobą, powrotem do zdrowia bądź inną sytuacją losową, która diametralnie zmieniła życie danej osoby lub jej rodziny.

Wiele zbiórek prowadzonych w Internecie jest zweryfikowanych i prowadzonych na szczytne cele. W zdecydowanej większości administratorzy danego portalu (strony internetowej) weryfikują organizatora zbiórki.

Niestety dochodzi do sytuacji, w których przestępcy próbują zmniejszyć naszą czujność i wykorzystać nasze współczucie do swoich niecnych, partykularnych interesów tworząc fikcyjne, fałszywe zbiórki pod przykrywą dobroczynności.



Istotne znaczenie ma fakt, że przestępcy odpowiednio nazywają zbiórkę, tak aby zwracała naszą uwagę. Dalej w treści zbiórki uwiarygadniają opis np. zamieszczając zdjęcia. Podkreślić trzeba, że tworzone zbiórki są na mało znanych stronach lub na stronach internetowych podszywających się pod znane witryny internetowe specjalizujące się w faktycznym niesieniu pomocy.

Coraz częściej pojawiają się również prośby o wsparcie danej osoby, która opisuje swoją ciężką i ckliwą historię w poście na portalu spo-

łecznościowym. Post ten często nie jest przez nikogo sprawdzany, a np. podawany dalej ze względu na poruszającą historię. W tym przypadku często emocje zaczynają górować nad zdrowym rozsądkiem i pojawia się chęć pomocy. Często również oszust w wiadomościach prywatnej jeszcze bardziej opisuje swoją ciężką sytuację zachęcając do pomocy, czy nawet do przekazania drobnej sumy. Jednak po wysłaniu pieniędzy takiej osobie profil zazwyczaj znika wraz z pieniędzmi, które przekazaliśmy. Dlatego bardzo ważne jest, aby przekazywać pieniądze tylko na sprawdzone zbiórki np. poprzez strony siepomaga.pl lub pomagam.pl, ewentualnie dokładnie sprawdzać osobę, która prosi o pomoc.

PRZYKŁAD

Według informacji opublikowanych przez Komendę Stołeczną Policji w 2021 r. policjanci z Wydziału do walki z Cyberprzestępczością KSP zatrzymali 33-latka, który założył fałszywą zbiórkę na rzecz poszkodowanej w pożarze rodziny. Oszust w ramach zbiórki zebrał rzekomo dla poszkodowanej rodziny ponad 54 tys. zł.

ZAPAMIĘTAJ!

Chcąc wesprzeć daną zbiórkę internetową, pamiętaj, aby:

- nie klikać podejrzanych linków,
- zweryfikować czy strona internetowa nie podszywa się pod inną witrynę internetową lub zbiórkę,
- nie przekazywać środków finansowych podejrzanym osobom lub organizmom, w szczególności, gdy ich profil działalności jest trudny do określenia,
- zachować czujność i włączyć krytyczne myślenie.

SMS: Dopłać 2,39 do przesyłki. Poznaj phishing

Każdy wędkarz wie, aby ryba brała musi być dobra przynęta. Wyobraźmy sobie, że wędkarzem jest cyberprzestępca, rybą jesteśmy my, natomiast przynętą jest nasza łatwowierność i nieuwaga.

Phising to metoda wykorzystywana przez cyberprzestępców polegająca na przejęciu od ofiary danych takich jak loginy i hasła, numery kont, danych kart kredytowych. Podczas oszustw phishingowych, cyberprzestępcy wykorzystują adresy e-mail, SMSy lub inne wiadomości tekstowe podając się za zaufane podmioty lub osoby.

Podczas ataku phishingowego cyberprzestępca będzie podawał się za zaufaną osobę lub podmiot (np. firmę), gdzie za pośrednictwem m.in. wiadomości e-mail, SMS będzie chciał wyłudzić nasze dane.

Podkreślić trzeba, że cyberprzestępcy podszywają się m.in. pod urzędy administracji, kontrahentów, firmy kurierskie, operatorów telekomunikacyjnych, a nawet naszych znajomych. Cyberprzestępcy przygotowują fałszywe wiadomości phishingowe tak, aby wyglądały na autentyczne. Dlatego konieczne jest uważne zwracanie uwagi na detale otrzymywanych wiadomości.

Phishing jest zatem metodą bazującą na socjotechnice, ponieważ ma na celu wykorzystanie naszego zaufania do działań zgodnych z zamiarem

przestępcy. Słowo „phish” wymawia się tak samo jak słowo „fish” (ryba). Stąd analogia do wędkarstwa.

PRZYKŁAD

Według informacji przekazanych przez podkarpacką Policję 45-letni mieszkaniec powiatu przemyskiego stał się ofiarą phishingu. Otóż otrzymał wiadomość e-mail – jak mu się wydawało – od swojego kontrahenta z informacją o tym, że zmienił numer rachunku bankowego do przelewów. Nowe konto było w innym kraju niż siedziba firmy, z którą współpracował, lecz nie zaniepokoiło go to, ponieważ współpracuje on z wieloma zagranicznymi firmami z różnych krajów i zdarzało się, że te przedsiębiorstwa miały konta w różnych bankach na świecie. Niestety składając nowe zamówienie w kwocie 10 tys. dolarów dokonał przelewu na fałszywe konto. Okazało się, że firma nie zmieniła numeru konta bankowego.

ZAPAMIĘTAJ!

Zwróć uwagę na:

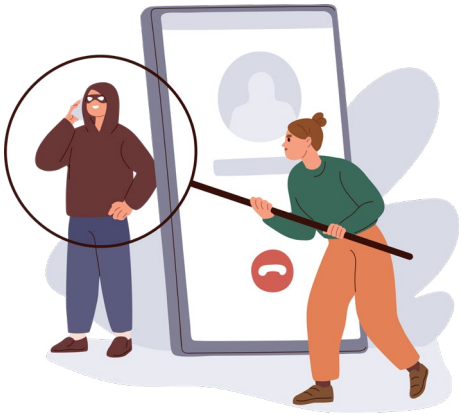
- gramatykę, interpunkcję, pisownie (np. brak polskich znaków „ą", „ć", „ę" itd.) otrzymywanych wiadomości,
- wiadomości zachęcające do pilnego i szybkiego działania, gdzie konsekwencją może być blokada konta, wyłączenie prądu itp.,
- informację, które mogą wskazywać na dziwny adres e-mail, nazwy, imię i nazwisko,
- otrzymany link (np. zamiast „allegro.pl" jest „allegro.eu"),
- załączniki do wiadomości.

Pamiętaj, że twój bank ani inna instytucja nie powinna prosić Cię o podanie danych osobowych w wiadomości e-mail. Możesz to sprawdzić dzwoniąc na infolinię prosząc o zweryfikowanie, czy dany e-mail został wysłany przez jej pracownika.

Pani Magdaleno, proszę zapoznać się z przesłaną wiadomością. O spoofingu słów kilka.

Nieraz spotkaliśmy się z sytuacją, kiedy dzwonił do nas przedstawiciel banku chcący zaoferować kredyt lub inną ofertę na atrakcyjnych warunkach. Jesteśmy przyzwyczajeni, że przedstawiciel naszego banku lub innego podmiotu zadzwoni do nas z ofertą raz na jakiś czas.

Wyobraźmy sobie teraz sytuację, w której dzwoni do nas cyberprzestępca podając się za pracownika naszego banku. Na ekranie telefonu wyświetla się numer banku. Osoba po drugiej stronie słuchawki próbuje wmówić nam, że doszło do włamania na nasze konto i trzeba szybko reagować. W trosce o bezpieczeństwo naszych pieniędzy działamy w emocjach. Podajemy cyberprzestępcy nasze wrażliwe dane, o które nikt nie powinien pytać. Nakłania nas on do instalacji oprogramowania, które ma nas rzekomo ochronić. Niestety w ten sposób staliśmy się ofiarą spoofingu.



Spoofing jest bardzo podobną metodą do phishingu, ponieważ przede wszystkim bazuje na emocjach. Cyberprzestępca próbuje wmówić nam jakąś sytuację i każą szybko reagować nie dając nam czasu na zastanowienie się. Ponadto cyberprzestępcy wykorzystują narzędzia, przez które łatwo nas zmanipulować m.in. wspomniany numer telefonu,

który wyświetlając się podaje się za kogoś kogo znamy, a w rzeczywistości numer, z którego wykonywane połączenie do nas jest zupełnie inny.

W ramach spoofingu cyberprzestępcy podają się za pracowników banków, ubezpieczycieli, nawet policjantów. Wykorzystują wiele metod, które ułatwiają wprowadzenie nas w błąd m.in. podszywają się w wiadomościach e-mail pod znane nam osoby, manipulują numerem telefonu, a nawet tworzą fikcyjne strony internetowe podające się pod powszechnienie znane nam witryny internetowe.

Coraz częściej również pojawiają się informacje o wykorzystaniu np. starszych bezbronnych osób podając się za przyjaciela wnuczka, znajomego, czy nawet przedstawiciela policji. Obieramy telefon, w którym ktoś nas informuje, że bliska dla nas osoba uległa wypadkowi i potrzebuje pilnie pieniędzy, żeby zacząć leczenie. Albo dzwoni do nas rzekomy funkcjonariusz policji, który mówi, iż była próba włamania na nasze konto bankowe i nasze fundusze są zagrożone, w celu ochrony trzeba je wybrać po czym przekazać w jakimś miejscu „policji" w celu ich zabezpieczenia. W pierwszej chwili pojawia się przerażenie, strach o bliską nam osobę czy nasze fundusze, jednak mimo wszystko trzeba odstawić emocje na bok i przemyśleć sytuacje na spokojnie.

Służby publiczne nigdy nie będą nas prosić o oddanie swoich pieniędzy w celu ochrony, a jeżeli dzwoni osoba podająca się za przyjaciela wnuczka to pod żadnym pozorem nie wolno przekazywać jej pieniędzy, najlepiej w takiej sytuacji skontaktować się i spotkać się z naszą bliską osobą i sprawdzić czy na pewno to ona potrzebuje tych pieniędzy.

PRZYKŁAD

W październiku 2021 r. podkarpacka policja poinformowała, że mieszkaniec powiatu sanockiego stał się ofiarą spoofingu tracąc kilkanaście tysięcy złotych. Cyberprzestępca wykorzystał oprogramowanie, które umożliwiło zmianę nazwy i numery telefonu u osoby odbierającej połączenie, a następnie podał się za pracownika banku. Wmówił on mężczyźnie, że dokonano próby włamania na jego konto. Nieświadomy niebezpieczeństwa mężczyzna wykonywał dalsze instrukcje cyberprzestępcy podającego się za pracownika banku. Ostatecznie, mieszkaniec powiatu sanockiego stracił kilkanaście tysięcy złotych.

ZAPAMIĘTAJ!

- zachowaj ostrożność i włącz zasadę ograniczonego zaufania,
- nikomu nie podawaj przez Internet swoich danych osobowych, loginów oraz haseł,
- upewnij się, czy nie jesteś celem cyberprzestępcy np. dzwoniąc do banku, czy faktycznie rozmawiałeś z ich pracownikiem,
- aktualizuj oprogramowanie swoich urządzeń,
- dbaj o bezpieczeństwo swoich haseł, np. stosując weryfikację dwuetapową,
- potwierdź tożsamość osoby, która prosi Cię o pieniądze czy hasła, najlepiej przez spotkanie z nią,
- zwracaj uwagę na szczegóły np. czy zdania są składne, czy występują polskie znaki diakrytyczne „ą”, „ę” itp.

No dobrze, ale logowałem się przez stronę. Oblicza pharmingu

Robienie zakupów przez Internet jest coraz bardziej popularną metodą. Szukamy w wyszukiwarce interesującego nas produktu, a następnie dokonujemy płatności wskazując adres dostawy. Podobny schemat dotyczy zlecenia płatności w bankowości elektronicznej. A co, gdyby, strona, przez którą dokonujemy płatności lub podajemy dane do logowania jest tak naprawdę fałszywa? Poznaj pharming.

Pharming jest jedną z najniebezpieczniejszych form cyberataków wykorzystywanych przez hakerów. Cyberprzestępcy za pośrednictwem złośliwego oprogramowania przekierowują nas do fałszywych stron internetowych celem przejęcia naszych wrażliwych danych. Z kolei my myślimy, że dokonujemy czynności na tej prawdziwej.

Hakerzy w atakach pharmingowych wykorzystują złośliwy kod, który zmienia informacje o adresie IP, co błędnie kieruje użytkowników do fałszywych stron internetowych bez ich wiedzy i zgody. Po wejściu na fałszywą witrynę internetową cyberprzestępcy próbują uzyskać dostęp do informacji osobistych lub finansowych albo wykorzystają fałszywą witrynę do zainfekowania naszego urządzenia wirusami lub innymi złośliwymi oprogramowaniami.

Ma to istotne znaczenie podczas próby zalogowania się przez użytkownika.

JAK ROZPOZNAĆ PHARMING?

Atak pharmingowy jest trudny do wykrycia, niemniej jednak istnieją sposoby na jego zidentyfikowanie. Należy zwrócić szczególną uwagę na:

- adres URL strony internetowej, czy nie ma różnic i błędów w nazwie strony (np. zamiast www.fmo.com.pl jest www.fno.com.xz),
- upewnienie się, że strona posiada protokół „https", a nie „http". Ma to kluczowe znaczenie, bowiem litera „s" oznacza, że strona jest bezpieczna.
- drobne zmiany w wyglądzie strony internetowej, z której często korzystamy.

ZAPAMIĘTAJ!

Korzystając ze stron internetowych pamiętaj, aby:

- być świadomym możliwego zagrożenia,
- posiadać aktualne i sprawdzone oprogramowanie antywirusowe,
- używać bezpiecznej przeglądarki internetowej.

Dobra, skorzystam z kodu QR. Nieciekawe konsekwencje quishingu

A tak naprawdę czym jest ten cały kod QR? Jest to rodzaj kwadratowego obrazu składającego się z czarno-białych wzorów (przypomina kod kreskowy), który przeznaczony jest do skanowania za pomocą aparatu w urządzeniach mobilnych. Po zeskanowaniu kod QR kieruje użytkownika do strony internetowej lub może zainicjować połączenie telefoniczne, wysłanie wiadomości tekstowej bądź ułatwić dokonanie płatności. Podkreślić trzeba, że na popularność kodów QR wpłynęła pandemia COVID-19, dzięki którym użytkownicy mogli bezkontaktowo otrzymać na telefon interesujące ich informacje np. zamiast tradycyjnej karty menu w restauracji, gość mógł zeskanować kod QR i wyświetlić menu restauracji na swoim telefonie.

Cyberprzestępcy nie pozostają w tyle i idą z duchem czasu. Ich cele nie zmieniają się od lat, lecz dostosowują swoje metody do panującej i zmieniającej się rzeczywistości. Dlatego wraz z wzrostem popularności kodów QR powstała nowa metoda – quishing. Nazwa „quishing" pochodzi od połączenia „QR" i „phisingu".

Quishing to rodzaj oszustwa, w którym cyberprzestępca tworzy spreparowany kod QR, wykorzystywany w wiadomościach phishingowych wysłanych za pomocą poczty e-mail. Niczego nieświadomy konsument, otwierając taką wiadomość widzi dość wiarygodną treść e-maila z kodem QR, który np. prowadzi do odbioru nagrody czy wykonania płatności. Po zeskanowaniu takiego

kodu przekierowani zostajemy na fałszywą stronę, gdzie zostają zbierane nasze dane uwierzytelniające albo do strony z wirusem lub złośliwym oprogramowaniem, którego pobieranie rozpoczyna się od razu po zeskanowaniu kodu. Kody QR możemy również spotkać na ulicach czy w jakiś miejscach, które zostały tam specjalnie zostawione, aby zaskoczyć potencjalną ofiarę, która z ciekawości zeskanuje kod.

PRZYKŁAD

W październiku br. 29 latek za pośrednictwem popularnej strony internetowej wystawił na sprzedaż kartę graficzną, po czym otrzymał wiadomość od kobiety zainteresowanej zakupem, gdzie uzgodnili, że paczka zostanie wysłana przesyłką kurierska po otrzymaniu przez mężczyznę pieniędzy. Aby transakcja przebiegła sprawniej, kobieta wysłała sprzedającemu kod QR, który po zeskanowaniu, wybraniu konta i zalogowaniu na nie, miał przekazać mężczyźnie pieniądze. Po zalogowaniu do bankowości mężczyzna zobaczył komunikat „przetwarzanie danych" jednocześnie odbierając telefon od osoby podającej się za kuriera w celu ustalenia przyjazdu po paczkę. Po zerwaniu połączenia, 29-latek zobaczył, że na jego koncie zostało wykonane kilka transakcji na łączną kwotę 7 600 zł.

ZAPAMIĘTAJ!

Widząc jakiś kod QR warto pamiętać, aby:

- upewnić się, kto jest adresatem danej wiadomości,
- sprawdzić czy ulotka, którą właśnie znaleźliśmy nie wyglądapodejrzanie,
- nie skanować kodów QR, w celu sprawdzenia, gdzie on nas przeniesie.

Dobrze, że mogłem Ci pomóc. Dziadku, ale nie rozmawialiśmy. Czym jestdeepfake?

Deepfake to rodzaj sztucznej inteligencji wykorzystywanej do tworzenia przekonujących obrazów oraz oszustw audio i wideo. Termin ten opisuje zarówno technologię, jak i wynikającą z niej fałszywą treść i jest połączeniem głębokiego uczenia się i podróbki. Deepfake często przekształcają istniejącą treść źródłową, gdzie jedna osoba zostaje zamieniona na drugą. Tworzą także całkowicie oryginalne treści, w których ktoś robi lub mówi coś, czego nie zrobił lub nie powiedział.

Najprościej mówiąc deepfake wykorzystuje sztuczną inteligencję do tworzenia nowych materiałów wideo lub audio, przedstawiających coś co w rzeczywistości się nie wydarzyło. Widea deepfake wygenerowane zostają po to, aby przekonać osoby oglądające nagranie, że ktoś zrobił coś, co w rzeczywistości nie miało miejsca, wprowadzając drugą stronę w błąd. Powszechnie możemy mieć styczność z deepfakes poprzez doświadczenie szantażu i szkody dla reputacji, w sytuacji, gdy oszust publikuje obraz sytuacji nielegalnej czy kompromitującej, w której bierzemy udział. Takie filmy i zdjęcia służą do wymuszenia ofiary, zrujnowania jej reputacji, zemsty lub cyberprzemocy.

PRZYKŁAD

W 2018 roku belgijska partia polityczna opublikowała wideo, na którym Donald Trump wygłasza przemówienie wzywając Belgię do wycofania się z paryskiego porozumienia klimatycznego. W rzeczywistości Trump nigdy nie wykonał takiej przemowy.

ZAPAMIĘTAJ!

Aby wykryć deepfake trzeba zwrócić uwagę na kilka cech takich jak:

- szczegóły, które są zamazane lub niewyraźne, niedociągnięcia, patrząc na skórę lub włosy postaci oraz jej twarz, która może być bardziej rozmyta niż otoczenie,
- oświetlenie, czy wygląda ono naturalnie? Algorytmy deepfake zazwyczaj zachowują oświetlenie z klipów, które zostały użyte już jako oświetlenia z klipów, co nie pasuje do oświetlenia w docelowym nagraniu,
- słowa i dźwięki, które nie pasują do obrazów, głos w takim wypadku nie będzie pasować do osoby,
- źródło, z którego otrzymaliśmy zdjęcie czy nagranie,
- czy film/zdjęcie wygląda normalnie po powiększeniu.

O, darmowe WiFi!
O Sniffing, mamyCię!

Jadąc pociągiem, komunikacją miejską, robiąc zakupy lub jedząc obiad w restauracji nadchodzi moment na chęć skorzystania z Internetu. Pokusa jest o tyle większa, kiedy jest możliwość skorzystania z otwartej sieci WiFi.

Sniffing w dosłownym tłumaczeniu z angielskiego oznacza „węszenie", a sam atak polega na „podsłuchiwaniu", a więc przechwytywaniu pakietów danych wędrujących przez sieć. Snifferem nazywamy oprogramowanie lub urządzenie służące do podsłuchu. Wystarczy, zainstalować sniffera na dowolnym urządzeniu w danej sieci (takiej jak WiFi) aby móc monitorować przysłane w niej informacje. Zazwyczaj możemy się z nim spotkać w publicznie dostępnych sieciach WiFi w miejscach takich jak galerie, bary, uczelnie, poczekalnie czy hotele. Wykrycie sniffera niestety jest dość ciężkie, albowiem nie obciąża on nadmiernie sieci i nie powoduje spowolnienia jej działania. Oszust w ten sposób może bez problemu filtrować wszystkie dostępne informacje i korzystać z nich w dowolny sposób, bez wiedzy nieświadomego użytkownika telefonu. Teoretycznie można korzystać z programów wykrywających podsłuch sieciowy, jednak w rzeczywistości sniffing nadal pozostaje jedną z najbardziej nieuchwytnych form pozyskiwania informacji i brakuje w 100 % skutecznego sposobu na jego wykrycie. Jednak nadal można skutecznie zapobiegać przed staniem się ofiarą sniffingu.

ZAPAMIĘTAJ!

Korzystając z Internetu:

- nie łącz się z publicznymi hotspotami Wi-Fi, gdyż jest to najlepsze środowisko do przeprowadzania ataków na Twoje dane,
- nie wchodź w podejrzane odnośniki, łatwo w ten sposób stracić wszystkie nasze dane,
- korzystaj tylko z bezpiecznych i szyfrowanych komunikatorów i serwisów pocztowych, więc nie używaj dziwnych i podejrzanych stron,
- sprawdzaj adresy stron, których używasz, odwiedzając witrynę internetową zobacz, czy jej adres zaczyna się od HTTPS, jeżeli tak to znaczy, że jest ona certyfikowana i bezpieczna, a przesyłane przez nią dane są szyfrowane.

Krótkie podsumowanie

Jak wiadomo Internet daje nam dużo różnych możliwości, od wyszukiwania danych po zdalną pracę bez wychodzenia z domu. Prawie wszystkie działania jakie podejmujemy opierają się na dostępie do Internetu co powoduje, że jest on dostępny w naszym życiu niemal nieustannie. Nawet komunikacja z innymi osobami coraz bardziej się opiera się na dostępie do Internetu. Większość z nas, już teraz, nie wyobraża sobie życia bez dostępu do Internetu.

Mając tak wiele możliwości, które daje nam Internet, musimy cały czas pamiętać by rozsądnie z niego korzystać.

Mimo, iż wszystkie zawarte tu informacje początkowo mogą wydawać się niezrozumiałe i przerażające, to właśnie dzięki przestrzeganiu zasad tu zawartych możemy bezpiecznie korzystać z możliwości Internetu i zobaczyć jak dużo daje on nam możliwości, jeżeli tylko będziemy rozważnie z niego korzystać.

Przestępcy rozwijają się wraz z rozwojem Internetu, dlatego ważne jest abyście byli świadomi różnych zagrożeń, na które możemy się natknąć i umieli przed nimi zapobiegać. Niniejsza broszura na pewno pozwoli Wam uniknąć zagrożeń wynikających z korzystania z Internetu.

Projekt pn. „Z myślą o starości. Z misją o przyszłości!" to odpowiedź Fundacji Misji Obywatelskiej na rosnące potrzeby i problemy związane z wciąż niską wiedzą i świadomością osób starszych na liczne zagrożenia występujące w przestrzeni cyfrowej, prawnej, zdrowotnej oraz społecznej. Stanowi to istotne wyzwanie w dobie starzejącego się społeczeństwa, jak również jego polaryzacji.

Celem projektu jest zatem, zwiększenie uczestnictwa seniorów we wszystkich dziedzinach życia społecznego poprzez wzmacnianie trwałych relacji międzypokoleniowych, kształtowanie empatycznych postaw wobec seniorów, upowszechnienie pozytywnego wizerunku osób starszych oraz zwiększenie ich wiedzy i świadomości na liczne zagrożenia.

Projekt składa się z cyklu szkoleniowego, którego zakres tematyczny obejmuje bezpieczeństwo zdrowotne, prawne, cyfrowe oraz społeczne. Cykl szkoleniowy jest wsparty spotkaniami ze specjalistami, świadczeniem doradztwa oraz prowadzeniem spotkań międzypokoleniowych i wolontariatu senioralnego. Spoiwem projektu jest kampania kształtująca empatyczne postawy wobec osób starszych oraz upowszechniająca pozytywny wizerunek seniora.

AKTYWNI+
Ministerstwo Rodziny i Polityki Społecznej
Z WIELĄ O STAROŚCI Z MISJĄ DLA SENIORÓW
FUNDACJA Misji Obywatelskiej

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025.