7
2023/2024

AKTYWNY SENIOR

KAMPANIA #HALO TU CYBERBEZPIECZNY SENIOR!

PRZYKŁAD OSZUSTWA NA „PRACOWNIKA BANKU”

Patron
ZWIĄZEK BANKÓW POLSKICH

Organizator
WARSZAWSKI INSTYTUT BANKOWOŚCI

Drodzy Seniorzy!

Oddajemy w Państwa ręce kolejny numer biuletynu informacyjno-edukacyjnego „Aktywny Senior". W tym wydaniu skupimy się na zagadnieniach dotyczących bezpieczeństwa seniorów w przestrzeni wirtualnej, ale także w bankowości i finansach.

Obecnie nowe technologie, takie jak internet, bankowość elektroniczna i mobilna, telefon komórkowy czy różne aplikacje na smartfona pomagają nam w życiu codziennym, służą do szybkiego i wygodnego realizowania różnych spraw. Ale to co dla jednych osób jest pożytecznym narzędziem do funkcjonowania we współczesnym świecie i ułatwianiem sobie życia, dla drugich stanowi furtkę do nadużyć, oszustw i przestępstw.

Z badania pt. „InfoSenior" Warszawskiego Instytutu Bankowości (przeprowadzonego w 2023r.) wynika, że z bankowości elektronicznej lub mobilnej korzysta już 82% seniorów, a tylko 55% z nich przeciętnie ocenia swój poziom wiedzy na temat bezpiecznego korzystania z Internetu, w tym bankowości internetowej. Osoby starsze częściej są narażone na ataki i oszustwa online. Badanie pokazuje, że 62% seniorów miało styczność (bezpośrednio lub w swoim otoczeniu) z próbami wyłudzenia pieniędzy w przestrzeni cyfrowej. W związku z tym ważne jest, aby seniorzy byli świadomi zagrożeń związanych z cyberprzestrzenią i wiedzieli, jak ochronić siebie, swoje dane i pieniądze.

Stąd tegoroczny biuletyn wydajemy pod hasłem „Bezpieczny senior to wyedukowany senior." Wspólnie z Partnerami projektu edukacyjnego „Bezpieczeństwo w Cyberprzestrzeni" przygotowaliśmy szereg artykułów, wskazówek i praktycznych porad, jak bezpiecznie korzystać z nowych technologii i nie paść ofiarą oszustów. Mamy nadzieję, że przekazana wiedza pozwoli Państwu być bezpiecznym.

Życzymy ciekawej lektury!
Redakcja Aktywnego Seniora

redakcja wydania: Aleksandra Czyrkowska,
materiały Partnerów projektu edukacyjnego
„Bezpieczeństwo w Cyberprzestrzeni"

W NUMERZE:

Kampania edukacyjna #Halo! Tu cyberbezpieczny Senior!

Warszawski Instytut Bankowości wspólnie z NASK-PIB oraz Centralnym Biurem Zwalczania Cyberprzestępczości w Policji organizuje kampanię edukacyjną pt. #Halo! Tu bezpieczny Senior. Akcja ma na celu zwiększenie wiedzy seniorów na temat różnych oszustw internetowych i telefonicznych, a także pokazanie socjotechnik i manipulacji stosowanych przez przestępców. Kampania rozpoczęła się z okazji Dnia Seniora oraz Europejskiego Miesiąca Cyberbezpieczeństwa (październik), a zakończy w Dniu Babci i Dziadka 2024r.

Jaki jest mechanizm oszustw telefonicznych?

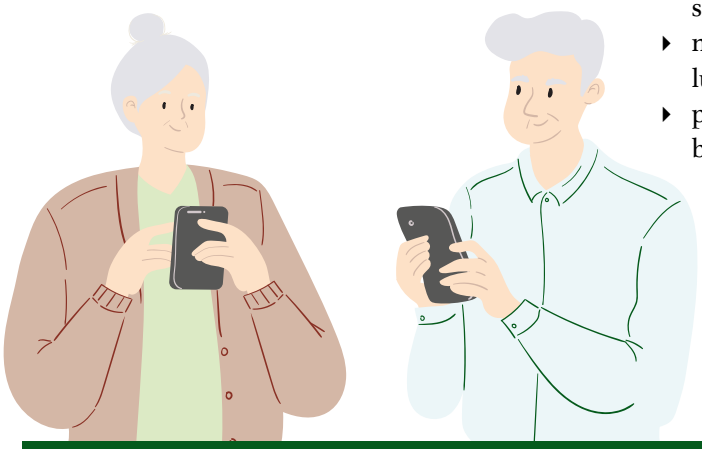
Dzwoniący oszuści przedstawiają zmyśloną, ale bardzo wiarygodną historię i liczą, że senior w nią uwierzy i będzie postępować zgodnie z ich poleceniami – bardzo często kończy się to przekazaniem pieniędzy. Przestępcy mogą podszywać się pod dowolną osobę, np.:

- członka rodziny,
- policjanta lub prokuratora,
- pracownika banku lub innej instytucji.

Jakie metody stosują oszuści podczas rozmów telefonicznych?

Będą próbować manipulować seniorem m.in. poprzez:

- wywieranie nacisku, aby szybko podjąć działania i pilnie przekazać pieniądze,
- wzbudzanie lęku i niepokoju np. mówiąc, że ktoś włamał się na konto bankowe i próbuje skraść pieniądze,
- prośby, aby dla dobra sprawy nikomu nie mówić o rozmowie,
- wykonywanie kilku telefonów w krótkich odstępach czasu – aby uniemożliwić zweryfikowanie sprawy,
- nakłanianie do instalowania aplikacji na telefonie lub komputerze,
- poinformowanie, że zaufana osoba przyjdzie i odbierze pieniądze.



KAMPANIA #HALO! TU BEZPIECZNY SENIOR! ZOSTAŁA PODZIELONA NA DWIE CZĘŚCI

W pierwszym etapie kampanii została przygotowana ulotka i plakat.
Ulotka, czyli kieszonkowa ściąga dla seniora, zawiera najważniejsze informacje ostrzegające przed telefonicznymi oszustami, w tym:

- Kiedy zachować szczególną czujność?
- O czym warto zawsze pamiętać?
- Co zrobić, gdy odbierze się telefon?

Ulotkę można pobrać na stronie projektu „Bankowcy dla Edukacji": **www.bde.wib.org.pl** – w zakładce: Materiały – Do pobrania

Druga część kampanii to cykl artykułów opisujących najczęściej występujące oszustwa internetowe i telefoniczne wymierzone w seniorów, takie jak np. wyłudzanie poufnych danych (tzw. *phishing*) czy podszywanie się pod zaufane podmioty (tzw. *spoofing*).
Publikacje będą ukazywać się cyklicznie, co miesiąc – od listopada 2023 r. do stycznia 2024 r.:

- na stronie internetowej Europejskiego Miesiąca Cyberbezpieczeństwa: **www.bezpiecznymiesiac.pl**
- na stronie projektu „Bankowcy dla Edukacji": **www.bde.wib.org.pl**
- na Facebooku Warszawskiego Instytut Bankowości i FB ECSM-u.

Oszustwa telefoniczne „na pracownika banku” – jak to wygląda w praktyce?

Dzwonię do Pani/Pana w bardzo ważnej sprawie. Telefon z banku – czy aby na pewno?

Jesteś w domu, nagle dzwoni telefon komórkowy, odbierasz. Osoba dzwoniąca przedstawia się i mówi, że dzwoni z banku z działu bezpieczeństwa i chciałaby przekazać bardzo ważną sprawę. Informuje, że doszło do ataku cyberprzestępcy na Twoim koncie bankowym i trzeba natychmiast zareagować, gdyż Twoje oszczędności są zagrożone!

Tak zazwyczaj zaczyna się rozmowa, która powinna wzbudzić Twoją czujność. To scenariusz oszustwa na tzw. „pracownika banku” – to jedna z ulubionych metod wyłudzania pieniędzy od seniorów przez telefon. Ten sposób kradzieży doczekał się licznych modyfikacji, m.in. z użyciem kodów BLIK.

Dzwoniąca osoba z banku twierdzi, że oszczędności można uchronić przed kradzieżą cyberprzestępcy, ale musisz szybko podjąć działania prewencyjne – przez telefon powie Ci, co masz po kolei zrobić. Nie zastanawiając się, zgadzasz się na szybkie zabezpieczenie Twoich pieniędzy. Pracownik z działu bezpieczeństwa proponuje, aby szybko udać się do bankomatu i wypłacić oszczędności, a następnie za pomocą kodów BLIK, które Ci przekaże, wpłacić te pieniądze we wskazanym wpłatomacie. Osoba dzwoniąca podkreśla, że to jedyny sposób na uratowanie oszczędności i że trzeba działać natychmiastowo, ale ważne jest, aby być ciągle na łączach telefonicznych. Podejmujesz zatem szybkie działania, lecisz do bankomatu i wypłacasz pieniądze z konta, a następnie wpłacasz we wskazanym wpłatomacie. Informujesz przez telefon o dokonanych czynnościach, a konsultant bankowy potwierdza, że teraz Twoje pieniądze są bezpieczne i rozłącza się. Ty wracasz do domu, zaglądasz na swoje e-konto, a tam nie ma nic – zostałeś/aś oszukany/a!

Jak zatem uchronić się od telefonicznych oszustw?

Należy mieć na uwadze, że to od nas samych zależy czy „pomożemy” przestępcom dokonać kradzieży. Tak jak w przypadku opisanego powyżej scenariusza oszustwa – to my sami autoryzujemy wszystkie działania podczas tego typu oszustw, przez co przestępca nie musi bezpośrednio atakować naszego konta bankowego.

Powyżej opisany scenariusz oszustwa to niestety tylko jeden z kilku telefonicznych metod wyłudzania pieniędzy przez telefon. Jeśli otrzymasz niespodziewany telefon od wnuczka, policjanta, prokuratora, ze szpitala czy nawet z ZUS z prośbą o szybkie wypłacanie pieniędzy z konta – zachowaj czujność i zastanów się czy nie jest to przypadkiem oszustwo. Nie reaguj spontanicznie, odłóż słuchawkę i na spokojnie przeanalizuj rozmowę, skonsultuj sytuację z bliskimi!

Seniorze nie daj się złowić! Czym jest phishing i jak się przed nim bronić?

Podstawowym oszustwem internetowym jest tzw. *phishing* – jest to angielskie sformułowanie, które oznacza „łowienie haseł". Nie bez przyczyny oszustwo jest tak nazwane, gdyż żeby zrozumieć jego mechanizm, najprościej porównać je do wędkowania. W prawdziwym życiu wędkarze łowią ryby w wodzie, natomiast oszuści internetowi próbują złowić Twoje dane osobowe i poufne informacje w sieci.

Jaki jest mechanizm phishingu?

Oszuści zarzucają na nas przynętę – wiadomość, w której informują o wygranej, nieopłaconej fakturze lub innej sytuacji, która ma nakłonić do kliknięcia w przesłany link lub podjęcia innych, szkodliwych dla nas działań. Taka wiadomość może być wysłana do nas poprzez fałszywe e-maile, sms-y lub komunikaty internetowe, które wyglądają, jakby pochodziły od rzeczywistych firm lub instytucji, takich jak banki, sklepy internetowe czy serwisy społecznościowe. W fałszywych wiadomościach, które do złudzenia przypominają te prawdziwe, oszuści namawiają do kliknięcia w link, który prowadzi do podrobionej strony logowania. Jeśli podamy tam swoje prywatne dane, przestępcy będą mogli je wykorzystać, a dysponując naszymi danymi, mogą np. ukraść pieniądze z naszego konta bankowego.

W jaki sposób możemy rozpoznać taką wiadomość?

- Dokładnie przeczytaj treść wiadomości i sprawdź czy nie zawiera błędów językowych i stylistycznych, literówek.
- Nawet jeśli wiadomość wydaje się być prawdziwa, zweryfikuj nadawcę – należy sprawdzić adres e-mail, z którego pochodzi wiadomość.
- Jeśli informacja pochodzi z banku, a w e-mailu od nadawcy po znaku @ jest inna nazwa niż nazwa banku to prawdopodobnie jest to oszustwo. Warto samodzielnie zadzwonić do firmy lub instytucji, która się z nami rzekomo kontaktuje i wyjaśnić sprawę telefonicznie lub w najbliższej placówce.
- Uważaj na wiadomości, które wykorzystują Twoje emocje (np. stres, lęk, presję czasu) i namawiają do podjęcia natychmiastowych działań.
- Jeśli coś wydaje się podejrzane lub zbyt dobre, aby było prawdziwe, zachowaj daleko idącą ostrożność i nie działaj na podstawie takich wiadomości.

Jak się chronić przed fałszywymi wiadomościami?

- Nie otwieraj wiadomości e-mail lub wiadomości tekstowych od nieznanych nadawców, osób, których nie znasz. Nie klikaj w przesłane do Ciebie linki i nie otwieraj załączników!
- Stosuj silne, długie i bezpieczne hasła. Pamiętaj, aby Twoje hasła nie zawierały informacji o Tobie ani Twoich bliskich. Do każdej usługi internetowej stosuj inne hasło.
- Zachowaj ostrożność w mediach społecznościowych! Bądź rozważna/y podczas przyjmowania zaproszeń od nieznanych osób na platformach społecznościowych. Unikaj udostępniania poufnych informacji publicznie na swoim profilu.
- Regularnie aktualizuj system operacyjny, przeglądarki internetowe i oprogramowanie antywirusowe, aby być chronionym przed lukami bezpieczeństwa.
- Nie lekceważ komunikatów i alertów bezpieczeństwa, jakie wyświetlają się podczas korzystania z sieci.
- Naucz się rozpoznawać znaki ostrzegawcze wiadomości phishingowych i podziel się tą wiedzą z rodziną i przyjaciółmi – edukuj innych!

Materiał przygotowany w ramach kampanii pt. #Halo! Tu cyberbezpieczny Senior! przygotowanej przez NASK, Centralne Biuro Zwalczania Cyberprzestępczości w Policji oraz Warszawski Instytut Bankowości.

Zagrożenie w sieci niejedną ma postać – seniorze uważaj na dezinformację!

NASK

Z badania Warszawskiego Instytutu Bankowości i Związku Banków Polskich pt. „Postawy Polaków wobec cyberbezpieczeństwa" wynika, że Polacy coraz częściej wskazują problem dezinformacji jako duże zagrożenie w cyberprzestrzeni. Jednakże tylko 39% badanych Polaków stwierdza, że sprawdza wiarygodność informacji, a 42% przyznaje, że robi to nieregularnie. 9 na 10 ankietowanych osób przyznaje, że jest potrzeba większej edukacji cyfrowej.

Warsztaty „Plotka też może być groźna – czyli o dezinformacji dla seniorów" na Uniwersytetach Trzeciego Wieku

Idąc tropem potrzeby edukacji w zakresie cyberbezpieczeństwa, Warszawski Instytut Bankowości (WIB) wspólnie z NASK-PIB (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy) organizuje wykłady warsztatowe na temat dezinformacji na Uniwersytetach Trzeciego Wieku w całej Polsce. WIB jest organizatorem warsztatów, a prowadzący wykłady to przedstawiciele Zespołu Budowania Odporności na Zagrożenia w Przestrzeni Informacyjnej NASK-PIB.

Cykl wykładów dla słuchaczy UTW pt. „Plotka też może być groźna – czyli o dezinformacji dla seniorów" WIB rozpoczął w październiku 2023 r. z okazji Europejskiego Miesiąca Cyberbezpieczeństwa. Wykłady mają charakter warsztatowy – na zajęciach poruszane są tematy bliskie seniorom. Zależy nam, aby w ciekawy i praktyczny sposób ukazać zagrożenia, które niesie ze sobą dezinformacja, tak aby seniorzy potrafili odróżniać opinię lub plotkę od prawdziwej informacji oraz wiedzieli, gdzie mają szukać wiarygodnych źródeł.

Wykłady dla seniorów na Uniwersytetach Trzeciego Wieku organizowane są w ramach Programu sektorowego „Bankowcy dla Edukacji", w tym także Projektu „Bezpieczeństwo w Cyberprzestrzeni".

Chcesz zorganizować wykład z tematu cyberbezpieczeństwa/dezinformacji na swoim UTW – napisz emaila na adres:

aczyrkowska@wib.org.pl

Seniorze uważaj na fałszywych znajomych w social mediach!

DAGMA
BEZPIECZEŃSTWO IT

Oszustwa popełniane przez osoby, które nie są tymi, za kogo się podają, to nadal jedno z największych zagrożeń w mediach społecznościowych.

W województwie lubuskim policja zdemaskowała oszustów działających metodą „na wygraną w konkursie". Kobieta z Gliwic straciła ponad 2 tys. złotych po tym, jak przez Messengera otrzymała prośbę od „swojego" chłopaka o przesłanie kodu BLIK. Z kolei jeden z samorządowców z województwa kujawsko-pomorskiego poinformował o profilu wykorzystującym jego wizerunek do zachęcania do inwestycji w kryptowaluty.

Co łączy te przypadki cyberoszustw? We wszystkich tych przypadkach cyberprzestępcy wykorzystywali fałszywe konta w mediach społecznościowych.

– *Oszuści często wykorzystują profile zarejestrowane i zarządzane przez automaty do zasypywania użytkowników atrakcyjnymi treściami, fałszywymi propozycjami matrymonialnymi, nienaturalnie korzystnymi ofertami handlowymi czy aplikacjami typu „sprawdź, kto oglądał twój profil". Kliknięcie w zawarty w nich link może skutkować pobraniem złośliwego oprogramowania lub dobrowolnym przekazaniem danych osobowych, np. jeśli następnie wypełnimy fałszywą ankietę. W ten sposób można stracić pieniądze i dane albo stać się ofiarą rozbudowanego oszustwa matrymonialnego lub finansowego* – wyjaśnia Kamil Sadkowski, analityk laboratorium antywirusowego ESET.

Jak się uchronić przed oszustwami w Social Mediach?

– *Przede wszystkim powinniśmy nauczyć się dostrzegać sygnały alarmowe świadczące o tym, że osoba, która wchodzi z nami w interakcję, nie jest tym, za kogo się podaje. Ważna jest także aktywność użytkowników i zgłaszanie podejrzanych kont do administratorów platform społecznościowych. Bardzo dobrą praktyką jest również odpowiednie ustawienie prywatności naszego profilu i nieprzyjmowanie zaproszeń od osób, których w rzeczywistości nie znamy* – tłumaczy Kamil Sadkowski.

Jak rozpoznać „fałszywych przyjaciół” w Social Mediach?

TOP 10 WSKAZÓWEK EKSPERTÓW ESET:

1. **Nietypowy życiorys.**
   Fałszywe konta mogą mieć opisy i bio, które są pobierane z innych miejsc, kopiowane i łączone. Często prowadzi to do błędów językowych. Zwróć także uwagę m.in. na literówki, nadmierne użycie emotikon i dziwny, sztuczny język, który może wskazywać na bota.

2. **Oszuści snujący intrygi.**
   Oszuści mogą wykorzystywać fałszywe profile w mediach społecznościowych, podobnie jak na portalach randkowych, w celu nawiązania romantycznej relacji online z ofiarą, a w kolejnym kroku proszą o przesłanie im pieniędzy. Warto przede wszystkim weryfikować ich zdjęcia profilowe przy użyciu wyszukiwarki obrazów i rezygnować z konwersacji jak tylko dostrzeżemy podejrzane zachowania.

3. **Brak proporcji pomiędzy „obserwującymi” a „obserwowanymi”.**
   To sygnał alarmowy, szczególnie na Instagramie, gdzie konta spamerskie automatycznie obserwują setki lub tysiące użytkowników, ale niewielu z nich ma jakichkolwiek własnych obserwatorów.

4. **Wykorzystanie zdjęcia profilowego bliskich znajomych.**
   Jednym z mechanizmów stosowanych powszechnie przez oszustów jest klonowanie kont naszych bliskich znajomych lub rodziny. Następnie wysyłają oni fałszywą wiadomość np. z informacją o kłopotach finansowych i prośbą o pieniądze. Na ten typ oszustwa nadal nabiera się niestety wielu użytkowników. Zawsze należy zatem dokładnie zweryfikować konto, które się z nami kontaktuje, szczególnie z jakąś nietypową prośbą. Trzeba także sprawdzić, za pośrednictwem innej metody kontaktu, np. telefonicznie, czy znajomy naprawdę wysłał do nas taką wiadomość.

5. **Spam w wiadomościach bezpośrednich.**
   Oszuści często wykorzystują wiadomości prywatne do rozsyłania fałszywych ofert, zachęcając użytkowników do przesyłania takiego spamu dalej lub klikania w szkodliwe linki. Do szerzenia tego typu komunikatów wykorzystywane są fałszywe konta, a tematyka wiadomości może być różna: od oszustw związanych i inwestycjami w kryptowaluty, po fałszywe oferty sprzedaży.

6. **Brak oznaczenia potwierdzającego weryfikację konta.**
   Instagram, Facebook, TikTok i X (Twitter) mają oznaczenia pozwalające na zidentyfikowanie autentyczności kont firm czy osób publicznych. Jeśli widzisz konto, rzekomo należące do jakiejś znanej organizacji lub osoby, ale nie zawiera ono takiego elementu, prawdopodobnie jest to oszustwo.

7. **Częstotliwość aktywności.**
   Fałszywe konta często publikują mnóstwo treści za jednym razem, często z podobnymi lub identycznymi podpisami, a następnie milkną. Mogą też w ogóle nie publikować. Należy więc sprawdzać ilość, jakość i częstotliwość postów i weryfikować czy u osób, które się z nami kontaktują, wygląda ona naturalnie.

8. **Oferty darmowych prezentów.**
   Uważaj na konta, które oferują prezenty i/lub gotówkę, na przykład w zamian za wypełnienie ankiety. Tego typu fałszywe profile często podszywają się pod znane marki i są tworzone głównie w celu kradzieży danych osobowych użytkowników social mediów.

9. **Mocno przecenione produkty.**
   Fałszywe konta mogą również promować luksusowe przedmioty, które zostały mocno przecenione. Pamiętaj, że jeśli coś jest zbyt piękne, by mogło być prawdziwe, to zazwyczaj takie jest.

10. **Przypadkowe komentarze.**
    Jeśli konto zostawia komentarze pod twoimi postami, niezwiązane z ich treścią, najprawdopodobniej także jest fałszywe.

Jak bezpiecznie kupować w internecie podczas promocji?

Takie miesiące jak listopad i grudzień to czas wzmożonych promocji zakupowych i świątecznych ofert. Sklepy kuszą promocjami, również te internetowe. Na stałe do naszych kalendarzy wpisały się takie dni, jak Black Friday czy Cyber Monday. Niestety to także okazja dla oszustów, którzy mogą wysyłać do nas swoje „kosmiczne" promocje i tworzyć fałszywe strony udające sklepy internetowe.

Na co zwrócić uwagę podczas zakupów w sieci?

- Najważniejsze to nie wierzyć w „kosmiczne" promocje, gdy oferowany towar lub usługa są w znacząco niższej cenie niż w innych sklepach.
- Warto sprawdzać sklepy internetowe i czytać opinie na ich temat.
- Wiarygodność sklepów zwiększa to, jeśli udostępniają regulamin, różne formy płatności i kontaktu.
- Można również sprawdzać dane przedsiębiorcy prowadzącego sklep w ogólnodostępnych rejestrach działalności gospodarczej.
- Należy uważać na wiadomości, w których ktoś wysyła link i przekonuje, że musimy dopłacić drobną kwotę do paczki. To charakterystyczny scenariusz oszustów.

Płacąc kartami, pamiętajmy o kilku sprawach

- Nigdy nie należy udostępniać danych kart płatniczych osobom trzecim ani pozostawiać kart bez opieki.
- Nie należy podawać danych karty, jeśli strona internetowa, na której trzeba to zrobić, budzi wątpliwości.
- Za zakupy w internecie warto płacić kartą płatniczą, m.in. ze względu na usługę chargeback, która umożliwia odzyskanie pieniędzy, np. w sytuacji nieotrzymania zamówionego produktu.
- Warto ustawić w bankowości internetowej rozsądne limity transakcji i wypłat gotówki kartami, aby w ten sposób ograniczyć ewentualne straty.
- Banki w swojej ofercie mają powiadomienia o realizowanych transakcjach, np. w aplikacji mobilnej. Dzięki nim mamy większą kontrolę. Jeśli jakakolwiek transakcja budzi wątpliwości, należy jak najszybciej skontaktować się z infolinią banku.

Bądźmy zatem czujni i rozsądni korzystając z wszelkich promocji, aby z pośpiechu i ekscytacji niską ceną nie dać złapać się na sztuczki cyberprzestępców.

Recepta na szybkie i bezpieczne zakupy VISA

Co możemy zrobić, by upewnić się, że nasze zakupy będą bezpieczne? Sprawdź, zanim klikniesz

W czasie zakupów online i dostaw możemy otrzymywać różne wiadomości. Są to na przykład: potwierdzenie dokonania transakcji czy informacja od kuriera. W takich wiadomościach czasami znajdują się linki. Zanim w nie klikniemy, warto upewnić się, czy wiadomość przyszła do nas z właściwego adresu. Nawet jeden zmieniony znak, np. „0" zamiast „o" powinien sprawić, że zapali nam się czerwona lampka. Warto być także czujnym, gdy dostaniemy SMS od firmy kurierskiej, że musimy dopłacić kilka złotych do naszej przesyłki, klikając w podany link. Takie i podobne sytuacje mogą być próbą oszustwa, dlatego powinniśmy na nie uważać, szczególnie jeżeli nadawcy wymagają od nas szybkiego działania i dążą do wywołania silnych emocji.

Zakupy w sklepie internetowym, którego nie znamy

Sklep sklepowi nierówny – czasem korzystamy z takich, które znają wszyscy, innym razem kupujemy w niszowych, na które można trafić, szukając atrakcyjnych cen czy bardzo nietypowych produktów. Gdy znajdziemy się na stronie jakiegoś sklepu po raz pierwszy lub z jakiegoś powodu nie budzi naszego zaufania, warto przed zakupami przejrzeć jego regulamin. Szczególną uwagę należy zwrócić na sekcje dotyczące dostawy oraz reklamacje. Kolejny krok to przejrzenie komentarzy i ocen dotyczących tego sklepu, które dość łatwo można znaleźć w internecie.

Już po decyzji o zakupie warto także sprawdzić, czy w miejscach na stronie, gdzie podawane są dane (dane karty czy dane adresowe) sklep zapewnia szyfrowanie połączenia. W adresie internetowym przed adresem sklepu powinno pojawić się „**https://**", któremu towarzyszyć powinien znak kłódki.

Telefonem za produkt

Płatności wykonywane telefonem są łatwe, szybkie i bezpieczne. Choć wygląda na to, że tego typu urządzenia na dobre zagościły w naszym codziennym życiu, wciąż są osoby, dla których to nowość. Większość smartfonów i smartwatchy pozwala już teraz na płatności mobilne, a kartę Visa można dodać do nich w kilku prostych krokach.

1. Dodaj swoją kartę Visa do aplikacji lub „portfela" na smartfonie lub smartwatchu. W przypadku wielu urządzeń wystarczy wykonać czynność podobną do robienia zdjęcia, która pozwala szybko załadować kartę do „portfela" na smartfonie, a następnie samodzielnie podać jedynie kod CVV2, który znajduje się na jej odwrocie. Proces ten nie zawsze będzie wyglądał tak samo, ze względu na różnice w systemach operacyjnych zainstalowanych na smartfonach.
2. W Polsce wszystkie terminale płatnicze przyjmują płatności zbliżeniowe, więc nie ma obawy, że nie będzie można z tej opcji skorzystać.
3. Przy najbliższej okazji, gdy będziesz w sklepie, zamiast wyjmować swój portfel i kartę, sięgnij po telefon. Wystarczy zbliżyć urządzenie do terminala, wcześniej potwierdzając płatność odciskiem swojego palca lub pozwalając telefonowi zeskanować swoją twarz. W niektórych sytuacjach niezbędne może okazać się również wprowadzenie numeru PIN w celu autoryzacji transakcji.

Telefonem można zapłacić także w internecie. Przykładem może być usługa Visa Mobile. To szybki i bezpieczny sposób dokonywania płatności online. Po założeniu konta i dodaniu karty Visa, jedyne co trzeba zrobić, by wykonać płatność, to wybrać Visa Mobile spośród dostępnych metod płatności, wpisać numer telefonu, a następnie potwierdzić w aplikacji. Sama płatność zajmuje zaledwie kilka chwil.

Bezpieczne płatności Visa w internecie

Wszystkie płatności Visa przy wykorzystaniu smartfona, smartwatcha lub tabletu są chronione tak samo, jak każda inna transakcja kartą Visa. Posiadacze kart mogą być pewni, że nikt nie będzie miał dostępu do ich danych wrażliwych, ponieważ po zapisaniu informacji o karcie w portfelu mobilnym, Visa zastępuje je unikalnym ciągiem cyfr, tzw. tokenem cyfrowym.

Warto również wiedzieć, że płatność kartą Visa, także tą dodaną do smartfona, objęta jest dodatkową ochroną, tzw. chargeback. Można skorzystać z tego mechanizmu w razie problemów z zakupem (np. gdy towar nie dotarł, jest niezgodny z opisem, wadliwy, uszkodzony lub po prostu nie jesteśmy zadowoleni z rezultatu rozpatrzenia reklamacji). Pierwszym krokiem powinna być próba rozwiązania problemu poprzez kontakt ze sprzedawcą. Jeśli nie da się załatwić sprawy polubownie, bank, który wydał kartę Visa, może podjąć próbę odzyskania środków od banku sprzedawcy.

Nowoczesny senior bankuje online

Bankowość internetowa i mobilna umożliwiają sprawdzanie obecnego salda na rachunku oraz historii transakcji i operacji na nim wykonanych. Możesz przeglądać historię transakcji według ram czasowych, kwoty, typu oraz słowa kluczowego. To również najszybszy sposób sprawdzenia, czy np. wpłynęło wynagrodzenie, emerytura lub inny przelew. Użytkownik konta może także zobaczyć transakcje zlecone z datą przyszłą, zlecenia stałe, nadchodzącą spłatę karty kredytowej oraz raty kredytu. Co więcej, szereg aplikacji bankowych na telefon pozwala podejrzeć bieżące saldo konta nawet bez potrzeby logowania do aplikacji. Wystarczy, że w ustawieniach aplikacji ustawisz taką opcję. Aplikacje najczęściej pozwalają wybrać rachunek, którego saldo ma być widoczne w podglądzie, oraz zdecydować, czy wartość ma być kwotowa, czy procentowa. Dzięki temu można sprawdzić także ostatnie transakcje na kilku kontach.

Po zalogowaniu się do mobilnej aplikacji bankowej, na głównym ekranie zobaczysz wszystkie swoje konta, karty oraz ich bieżące saldo. W dalszej części tego rozdziału krok po kroku opiszemy, jak otworzyć konto online w banku przez aplikację mobilną na smartfonie, a także pokażemy, jak łatwo zalogować się do swojego rachunku bankowego.

Płacisz rachunki online

Możesz skorzystać z bankowości internetowej swojego banku lub z aplikacji mobilnej, aby opłacić rachunki online. Możesz także skonfigurować stałych odbiorców swoich płatności, do których najczęściej wykonujesz przelewy. Mogą to być nie tylko twoi bliscy czy znajomi – warto dodać tam dostawców usług (prąd, gaz, internet, kablówka, telefon itp.). Dzięki temu przy kolejnym przelewie wybierzesz odbiorcę z listy, zamiast wpisywać numer jego konta od nowa. A jeśli zaznaczysz, że jest to odbiorca zaufany, nie będzie trzeba za każdym razem autoryzować przelewu, czyli potwierdzać przelewu smsKodem, tokenem lub Mobilną autoryzacją. W bankowości internetowej można ustawić tzw. polecenie zapłaty – cykliczną płatność automatyczną w tej samej kwocie, np. co miesiąc. Ta funkcja jest przydatna w przypadku rachunków, takich jak opłata za internet, raty za samochód lub polisa ubezpieczeniowa, czy opłaty za subskrypcje w serwisach streamingowych, które nie zmieniają się z miesiąca na miesiąc.

Przelewasz pieniądze między kontami

Dzięki bankowości online możesz o dowolnej porze wysłać pieniądze ze swojego rachunku bankowego znajomym i rodzinie. Jeśli odbiorca przelewu ma konto w tym samym banku co ty, przelew zostanie wykonany jako wewnętrzny, a odbiorca powinien otrzymać pieniądze w kilka chwil. Jeśli oprócz konta osobistego posiadasz również rachunek oszczędnościowy, możesz w łatwy sposób przelewać środki między tymi kontami. Jest to zdecydowanie wygodniejsze i szybsze niż osobista wizyta banku i zlecenie przelewu bądź wypłata gotówki z bankomatu. Pamiętaj, że zazwyczaj jeden przelew w miesiącu

Więcej informacji z zakresu poruszania się po cyfrowym świecie znajdziesz w publikacji „Nowoczesny senior. Przewodnik po cyfrowym świecie – 2023” dostępnej na stronach **www.digitalpoland.org/publikacje** oraz **www.polskabezgotowkowa.pl/badania-i-analizy**

z konta oszczędnościowego na rachunek bieżący jest bezpłatny. Za każdy następny może obowiązywać dodatkowa opłata. Aby zrobić przelew w aplikacji mobilnej, po zalogowaniu do aplikacji należy wybrać odpowiednią opcję płatności, wybrać rachunek lub wpisać dane odbiorcy rachunku, a po upewnieniu się, że dane się zgadzają, należy zatwierdzić operację.

Jesteś zawsze na bieżąco

Kolejną zaletą bankowości internetowej i aplikacji mobilnej jest możliwość skonfigurowania powiadomień. Dzięki nim możesz być na bieżąco z wieloma sprawami, które dzieją się na twoim koncie i karcie. Możesz otrzymywać powiadomienia, np. o zmianie salda czy przekroczeniu limitu środków na karcie przez SMS-a, e-maila lub w aplikacji mobilnej. Bank poinformuje cię też o nieudanym logowaniu czy innych zdarzeniach na koncie i karcie. Alerty nie tylko informują oraz pozwalają szybko zweryfikować to, co dzieje się z twoimi finansami. Dzięki temu możesz natychmiast skontaktować się z bankiem i wyjaśnić wątpliwości.

Zarządzasz swoimi finansami

Za pomocą bankowości internetowej możesz również załatwić wiele spraw, np. doładować telefon na kartę, opłacić parking, opłacić przejazd autostradą, kupić bilet komunikacji miejskiej, na pociąg czy autobus, zasilać konta na platformach subskrypcyjnych z filmami, serialami, muzyką, grami, zalogować się do Profilu Zaufanego, zachowywać zdjęcia paragonów, złożyć wniosek w programach 500+ lub Dobry Start.

Masz bank w telefonie dzięki aplikacji mobilnej

Większość banków oferuje aplikację mobilną, dzięki której masz stały dostęp do konta i najważniejszych funkcji w swoim smartfonie. Możesz szybko sprawdzić stan swojego konta, gdy robisz zakupy, czy przelać środki z innego konta, aby nie przekroczyć salda. W aplikacji mobilnej możesz również zakupić walutę po atrakcyjnym kursie wymiany i od razu masz ją na swoim koncie. Ponadto w aplikacji aktywujesz, zastrzeżesz lub zablokujesz kartę. Możesz również łatwo ustawić nowy PIN lub zmienić limity transakcji na karcie. Nie musisz już chodzić do oddziału banku, by założyć w nim kolejne/dodatkowe konto i korzystać z niego w bankowości mobilnej. Możesz to zrobić całkowicie zdalnie i cieszyć się od razu dostępem do konta w smartfonie. Dla części usług może być najpierw wymagane podpisanie dokumentów w oddziale banku. Pamiętaj, że bank rozwija swoje usługi i co jakiś czas może być konieczna aktualizacja aplikacji. Zawsze zrób to przez oficjalny sklep: Sklep Play lub App Store, w zależności od rodzaju telefonu, jaki posiadasz.

Seniorzy mogą budować swój dodatkowy kapitał na emeryturze

Funkcjonujący w Polsce od wielu lat repartycyjny system emerytalny (I filar) opiera się na założeniu, że pracująca część społeczeństwa poprzez odprowadzanie składek na bieżąco „finansuje" świadczenia obecnych emerytów i rencistów. Taki system pozostaje stabilny, jeśli liczba osób pracujących pokrywa się z będącymi na emeryturze. W przypadku niekorzystnych zmian demograficznych, którymi są m.in. starzenie się społeczeństwa czy też rekordowo niski przyrost naturalny, może on ulec destabilizacji i niestety, co już obserwujemy od kilku lat, może również wpływać na niższą wartość wypłacanych emerytur. Analizując wysokość świadczeń wypłacanych przez Zakład Ubezpieczeń Społecznych po marcowej waloryzacji można zauważyć, że największy odsetek emerytur (13,8%) to emerytury w przedziale wysokości od 2200 zł do 2600 zł. Oczywiście, aby mieć więcej środków do dyspozycji trzeba w miarę możliwości samodzielnie odkładać pieniądze.

Gdzie odkładać pieniądze na emeryturze?

Będąc tuż przed emeryturą lub mając już wypłacane świadczenia emerytalne warto zastanowić się i rozważyć skorzystanie z jednej lub kilku dostępnych na rynku rozmaitych opcji pozwalających samodzielnie zabezpieczyć swoją przyszłość, a przy tym skorzystać z ulg podatkowych.

Taką możliwość dają dobrowolne programy finansowe składające się na tzw. III filar emerytalny, a są to:

- Pracownicze Programy Emerytalne (PPE),
- Pracownicze Plany Kapitałowe (PPK),
- Indywidualne Konta Emerytalne (IKE),
- Indywidualne Konta Zabezpieczenia Emerytalnego (IKZE).

PPE pozwala budować dodatkową emeryturę przy udziale pracodawcy i dobrowolnych składek pracownika, z kolei w PPK gromadzony kapitał pochodzi z trzech źródeł – od pracodawcy, pracownika oraz

państwa. Oba programy prowadzone są przez wybraną instytucję finansową.

A czym są i jak funkcjonują indywidualne konta?

Choć nazwy obu kont są niemal identyczne - Indywidualne Konto Emerytalne oraz Indywidualne Konto Zabezpieczenia Emerytalnego - to jednak występują między nimi dość istotne różnice.

IKE jest dostępne w Polsce od 2005 roku i zostało utworzone na wzór amerykańskiego konta IRA (*Individual Retirement Account*). Z IKZE wiąże się nieco krótsza historia (można je zakładać od 2012 roku), ale z założenia jest to podobny do IKE instrument, który umożliwia jego właścicielowi samodzielnie gromadzić dodatkowy kapitał na przyszłość. Co istotne, nie ma żadnych przeciwwskazań do posiadania obu kont jednocześnie.

Najpierw o podobieństwach...

Co ważne, ani w ustawie o podatku dochodowym od osób fizycznych, ani w ustawie o IKE i IKZE nie ma przepisów, które zabraniają emerytom i rencistom zakładania i gromadzenia swoich oszczędności w ramach kont IKE oraz IKZE. Tym samym dla tej grupy osób również istnieje możliwość odliczenia wpłat na IKZE od podstawy opodatkowania lub otwarcia IKE (np. z myślą o swoich wnukach), z jednoczesnym zwolnieniem z podatku od zysków kapitałowych tzw. podatku Belki.

Są natomiast ograniczenia dotyczące minimalnego wieku. Konta mogą otworzyć osoby, które ukończyły 16 lat. W zależności od osobistych preferencji oba programy mogą przybierać różne formy np. w przypadku PKO TFI jest to inwestowanie w fundusze inwestycyjne. Z punktu widzenia właściciela konta, ważne jest to, aby były to produkty finansowe pomnażające kapitał w długim horyzoncie czasowym i najlepiej osiągające stopy zwrotu przewyższające poziom inflacji. Gromadzony w ten sposób prywatny kapitał jest w razie śmierci właściciela w pełni dziedziczony przez spadkobierców lub przez osoby uposażone wskazane w umowie np. dzieci lub wnuki.

...A teraz o licznych różnicach

Posiadaczy IKE oraz IKZE obowiązują ustawowe limity wpłat, co oznacza, że jeśli zostanie przekroczony ich górny próg, to instytucja finansowa zwróci im nadpłatę. Wysokość limitu uzależniona jest od prognozowanego przeciętnego wynagrodzenia miesięcznego. W przypadku IKE jest to trzykrotność tej pensji – w 2023 roku jest to kwota 20 805 zł.

W IKZE wyznaczone są dwa limity wpłat. Podstawowy obejmuje pracowników etatowych oraz zatrudnionych na umowach cywilno-prawnych. Jest liczony jako 1,2-krotności przeciętnej prognozowanej pensji i w tym roku wynosi 8 322 zł. Nieco wyższy limit wpłat na IKZE wyznaczono przedsiębiorcom – jest to 1,8-krotności prognozowanego wynagrodzenia czyli w 2023 roku – 12 483 zł. Liczba dokonanych wpłat oraz to czy powyższe limity wykorzysta się w pełni zależy wyłącznie od decyzji posiadacza konta.

Następna różnica dotyczy wieku właściciela konta i tego kiedy może wypłacić swoje pieniądze z zachowaniem ustawowych ulg podatkowych. W IKE jest to wiek 60 lat lub 55, jeśli mamy prawo do tzw. wcześniejszej emerytury. Warunkiem jest również dokonywanie wpłat przez co najmniej 5 lat kalendarzowych lub wpłacenie ponad połowy wartości wszystkich wpłat do 5 lat przed dniem złożenia wniosku o wypłatę. Właściciel IKZE musi natomiast osiągnąć 65. rok życia i dokonywać wpłat przez co najmniej 5 lat kalendarzowych. Spełniając powyższe warunki zgromadzone środki można wypłacić jednorazowo lub w ratach. Oczywiście nie oznacza to, że nie można wypłacić pieniędzy wcześniej (wręcz w każdej chwili), ale wtedy może to być zdecydowanie mniej opłacalne, głównie z powodu utraty ulg podatkowych. Nie ma natomiast górnej granicy wiekowej i może to być np. 80, 90 lub nawet 100 lat.

Koniec roku – pamiętaj o wpłacie na indywidualne konto emerytalne!
Zbliża się końcówka 2023 roku, która zwykle mobilizuje właścicieli tych kont do dokonania wpłat do pełnej wysokości obowiązujących w danym roku limitów. Jeśli masz już indywidualne konto(a) emerytalne, to nie zapomnij tego zrobić. W ten sposób w pełni korzystasz z przysługujących ulg. Jednocześnie pamiętaj, że rozłożenie wpłat na tygodnie lub miesiące na zasadzie tzw. stałego zlecenia, pozwala uśrednić cenę zakupu wybranych przez Ciebie produktów finansowych.

Na jakie ulgi podatkowe można liczyć?

Ulgi podatkowe to kluczowa zachęta do skorzystania z IKE oraz IKZE i jednocześnie mocno je różniąca. Pod warunkiem osiągnięcia wskazanego powyżej wieku tj. 55 lub 60 lat w IKE zgromadzone oszczędności nie są objęte 19-procentowym podatkiem od zysków kapitałowych tzw. podatkiem Belki. Jeśli posiadacz IKZE osiągnie wiek 65 lat to również i on może liczyć na zwolnienie z podatku od zysków kapitałowych, ale nie jest to jedyna ulga przysługująca mu w ramach skorzystania z tego wariantu oszczędzania.

Kolejną, jak nie najważniejszą, korzyścią podatkową IKZE jest bowiem możliwość odliczania wpłat na konto IKZE od podstawy opodatkowania podatkiem od osób fizycznych. Dzięki takiej konstrukcji programu wielu podatników ma możliwość obniżenia podatku PIT poprzez odliczenie kwoty, która została wpłacona na konto IKZE w roku poprzednim. Wpłacając pełną kwotę na IKZE w ramach tegorocznego limitu podatnik „zaoszczędza" na podatku nawet 2 663,04 zł. Jeszcze korzystniej wygląda to wśród osób prowadzących pozarolniczą działalność. Przy wpłacie równej limitowi w 2023 roku ich podatek może być niższy nawet o 3 995 zł. W momencie wypłaty wszystkich pieniędzy zgromadzonych na IKZE (po osiągnięciu 65. roku życia) jego posiadacz zapłaci 10-procentowy zryczałtowany podatek dochodowy. W końcowym rozrachunku może to być jednak opłacalne, szczególnie kiedy co roku istnieje możliwość obniżania podatku dochodowego, a od wypracowanych zysków nie będzie również pobierany podatek od zysków kapitałowych (tzw. podatek Belki).

Jakie są konsekwencje dokonania wcześniejszej wypłaty (zwrotu)?

Co istotne, zarówno IKE, jak i IKZE daje właścicielom możliwość wypłaty środków w każdej chwili. Decydując się na wcześniejszą wypłatę z IKE można wypłacić całość zgromadzonych pieniędzy lub ich część, co wiąże się z koniecznością zapłaty podatku od zysków kapitałowych (tzw. podatku Belki). W przypadku IKZE nie można wypłacić części środków, a jedynie całość. Co ważne – wypłacana kwota zwrotu nie jest obciążona podatkiem od zysków, ale ich wcześniejsze wycofanie (przed 65. rokiem życia) wymusza na właścicielu konieczność samodzielnego odprowadzenia podatku dochodowego przy rozliczaniu swojego PIT. W praktyce wypłacane środki są traktowane w danym roku podatkowym jako dodatkowy przychód. Nie ulega wątpliwości, że przed podjęciem decyzji o wcześniejszym „skonsumowaniu" gromadzonych środków należy dokonać wnikliwej analizy czy taki wariant faktycznie będzie się opłacał.

Z danych KNF wynika, że zainteresowanie Polaków IKE i IKZE systematycznie rośnie. Wybierając tę formę oszczędzania na przyszłość można dołączyć do grona blisko 1,3 mln posiadaczy dobrowolnych i prywatnych kont IKE i/lub IKZE, którzy według stanu na 30 czerwca 2023 roku gromadzili już na swoich kontach łącznie 23,392 mld złotych.

I na koniec rzecz najważniejsza z punktu widzenia seniora – skoro nie ma górnych ograniczeń wiekowych przy oszczędzaniu poprzez IKE i IKZE to jest to jedna z korzystnych podatkowo możliwości rozpoczęcie czy też kontynowania oszczędzania pieniędzy dla siebie lub też dla swoich pokoleniowych następców (np. dzieci czy wnuków). Nawet krótki czas oszczędzania w późniejszym okresie życia przynosi właścicielom dodatkowe korzyści finansowe.

Wszystkie osoby, które do tej pory nie doświadczyły jeszcze korzyści wynikających z posiadania kont IKE i/lub IKZE zachęcamy do ich założenia. W bardzo prosty i szybki sposób można tego dokonać z PKO TFI i jeszcze w tym roku rozpocząć oszczędzanie z preferencjami podatkowymi.

Wystarczy wejść na stronę PKO TFI i zapoznać się ze szczegółowymi zasadami:
www.pkotfi.pl/pakiet-emerytalny-pkotfi/

Artur Stypka, Manager Regionalny PKO TFI S.A.

Dzień Seniora w ZUS

Dzień Seniora to ważna i potrzebna społecznie inicjatywa, która na stałe wpisała się w kalendarz cyklicznych wydarzeń organizowanych corocznie przez Zakład Ubezpieczeń Społecznych.

Współorganizatorem akcji jest Polski Związek Emerytów, Rencistów i Inwalidów, a działania w ramach obchodów Dnia Seniora organizowane są zarówno przez ZUS, jak i Partnerów tego wydarzenia, a także przez lokalne instytucje działające na rzecz osób starszych. W 2023 roku Warszawski Instytut Bankowości ponownie został Partnerem Dnia Seniora w ZUS.

W 2023 roku Dzień Seniora w ZUS odbywał się w październiku i listopadzie pod hasłem „Senior manager ds. własnego bezpieczeństwa". Organizowane były następujące wydarzenia:

- spotkania i konsultacje,
- prelekcje, panele dyskusyjne,
- stoiska informacyjne,
- porady specjalistów z ZUS i ekspertów.

Wszystkie informacje o Dniu Seniora oraz innych inicjatywach ZUS są dostępne na stronie **www.zus.pl**

Warszawski Instytut Bankowości w ramach obchodów Dnia Seniora w ZUS zorganizował w dniu 30 listopada warsztaty edukacyjne w formie grywalizacji dla seniorów Uniwersytetu Trzeciego Wieku w Górze Kalwarii. Do wydarzenia WIB pt. „Bezpieczny senior to wyedukowany senior" dołączył III Oddział ZUS w Warszawie, Inspektorat w Piasecznie oraz Komenda Powiatowa Policji w Piasecznie.

Wydarzenie dla słuchaczy UTW w Ośrodku Kultury w Górze Kalwarii składał się z 3 części:

- spotkania z przedstawicielem Komendy Powiatowej Policji w Piasecznie na temat bezpieczeństwa seniorów,
- warsztatów WIB w formie gry edukacyjnej w zakresie bezpieczeństwa seniorów w cyberprzestrzeni,
- stoiska i quizu ZUS – podniesienie wiedzy na temat ZUS i jego działalności na rzecz seniorów, jak np. elektroniczne formy kontaktu, usługi ZUS czy bezgotówkowa forma pobierania świadczeń.

Warsztaty edukacyjne WIB miały na celu rozwinąć wśród seniorów umiejętność rozpoznawania zagrożeń online i zwiększyć ich poczucie bezpieczeństwa w korzystaniu z nowych technologii.

Biuletyn „Aktywny Senior” jest wydawany w ramach programu „Bankowcy dla Edukacji”

BANKOWCY DLA EDUKACJI
program sektorowy

O programie „Bankowcy dla Edukacji” (BdE)

Program BdE został uruchomiony w 2016 roku przez Związek Banków Polskich i Fundację Warszawski Instytut Bankowości. To wspólna inicjatywa banków i firm infrastruktury bankowej realizowana we współpracy z instytucjami publicznymi, samorządami, organizacjami pozarządowymi i mediami. Łącznie uczestniczyło w nim ponad 800 podmiotów.

Jednym z głównych założeń przy inicjowaniu Programu BdE było dotarcie z treściami edukacyjnymi do jak największej grupy odbiorców, niezależnie od wieku czy profesji. Edukacja ekonomiczna i bezpieczeństwo cyfrowe są niezwykle ważne na każdym etapie życia, a dynamicznie zmieniająca się rzeczywistość sprawia, że obszar tematyczny edukacji stale się powiększa. Stąd program skierowany jest do grup odbiorców w różnym wieku: uczniów, studentów, dorosłych, przedstawicieli różnych grup zawodowych i seniorów.

Najważniejsze działania i inicjatywy projektu Aktywny Senior:

- wykłady i webinary z udziałem ekspertów, w tym wykłady na Uniwersytetach Trzeciego Wieku,
- konferencje i spotkania online,
- raport „InfoSenior”,
- poradniki i materiały informacyjne,
- biuletyny i newslettery,
- broszury edukacyjne,
- kampania filmowa „Bankowcy dla CyberEdukacji”.

Dla Uniwersytetów Trzeciego Wieku i organizacji senioralnych uczestniczących w Programie BdE wszystkie działania są BEZPŁATNE.

Skorzystaj z naszych propozycji dla siebie i innych – dziel się zdobytą wiedzą z rodziną i znajomymi!

Fundacja Warszawski Instytut Bankowości stale rozwija zakres działań na rzecz seniorów, organizuje własne wydarzenia, jak i przyłącza się do nowych inicjatyw. W listopadzie 2023 r. Warszawski Instytut Bankowości dołączył do Koalicji Cyfrowi Seniorzy zrzeszającej 24 organizacje (łącznie z WIB), w tym największe izby, związki, federacje oraz fundacje działające na rzecz rozwoju nowych technologii i szeroko pojętej cyfryzacji. Celem Koalicji Cyfrowi Seniorzy jest m.in. zbudowanie największej w Polsce platformy edukacyjnej cyfrowiseniorzy.pl, która pozwoli seniorom zdobywać wiedzę i rozwijać kluczowe umiejętności do sprawnego funkcjonowania w świecie cyfrowym. Koalicję Cyfrowi Seniorzy zainicjowała Fundacja Digital Poland. W ramach funkcjonowania Koalicji zaplanowano m.in. doradztwo (infolinia z poradami) oraz kampanie edukacyjne ukierunkowane na potrzeby osób w starszym wieku.

Chcesz być na bieżąco z naszymi działaniami skierowanymi do seniorów oraz inicjatywami podejmowanymi w ramach Koalicji Cyfrowi Seniorzy – odwiedzaj nasze strony internetowe:

- Program Bankowcy dla Edukacji **www.bde.wib.org.pl**
- Warszawskiego Instytutu Bankowości **www.wib.org.pl**

Masz pytania? Chcesz rozpocząć współpracę i przyłączyć się do naszych działań?
Napisz do nas email: seniorzy@wib.org.pl