AKTYWNY SENIOR

© 2025

WYDAWCA: WARSZAWSKI INSTYTUT BANKOWOŚCI

W RAMACH PROJEKTU: AKTYWNY SENIOR

W RAMACHH PROGRAMU: BANKOWCY DLA EDUKACJI program sektorowy

Drodzy *Seniorzy!*

Oddajemy w Państwa ręce kolejny numer biuletynu informacyjno-edukacyjnego „Aktywny Senior”, publikowanego w tym roku pod hasłem „Seniorze bądź ostrożny – sztuczna inteligencja to nie tylko wsparcie człowieka!”. Niniejsze wydanie ma zatem charakter głównie poradnikowy i porusza tematy dotyczące nowych technologii i związanych z nimi zagrożeń.

Współczesne rozwiązania technologiczne, takie jak np. sztuczna inteligencja (AI), coraz śmielej wkraczają do życia człowieka, m.in. stosowane są w medycynie, przemyśle, dziennikarstwie czy grafice. Ale to co dla jednych osób jest pożytecznym narzędziem ułatwiającym pracę, dla drugich – stanowi furtkę do oszustw i przestępstw. Z badania Warszawskiego Instytutu Bankowości pt. „Postawy Polaków wobec cyberbezpieczeństwa” przeprowadzonego w czerwcu 2024 roku wynika, że blisko połowa badanych (49%) uważa, że sztuczna inteligencja jest zarówno szansą, jak i zagrożeniem dla człowieka.

Natomiast badanie „Seniorzy w świecie cyfrowych finansów” zrealizowane w I połowie stycznia 2025 roku (z okazji Dnia Babci i Dziadka) pokazuje, że obecnie osoby starszego pokolenia stają się coraz bardziej cyfrowe i coraz częściej korzystają z technologicznych rozwiązań, używając ich m.in. jako środka płatniczego. Aż 76% respondentów zadeklarowało, że korzysta z bankowości internetowej a 86% swoje codzienne zakupy opłaca kartami płatniczymi z kolei prawie połowa (45%) korzysta z płatności za pomocą BLIK-a.

Jak widać, cyfrowe rozwiązania płatnicze wkraczają obecnie do świata seniorów. Dlatego ważne jest, aby starsze osoby były świadome zagrożeń związanych z cyberprzestrzenią, a także by wiedziały, jak chronić siebie, swoje dane i pieniądze.

Stąd 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”

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

W numerze:

NASK

Poradnik „#Halo! Tu cyberbezpieczny Senior!”

Cyfryzacja postępuje w zawrotnym tempie, a cyberprzestępstwa stają się coraz większym wyzwaniem, zwłaszcza dla seniorów, którzy nie zawsze wiedzą, jak rozpoznać zagrożenie. Oszuści wykorzystują brak świadomości użytkowników sieci, dlatego ważne, by seniorzy mieli odpowiednie narzędzia i wiedzę, jak skutecznie chronić się przed internetowymi pułapkami.

Dlatego trzy instytucje, tj. Naukowa i Akademicka Sieć Komputerowa (NASK) – Państwowy Instytut Badawczy, Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) oraz Fundacja Warszawski Instytut Bankowości (WIB) połączyły siły i przygotowały kompleksowy poradnik „#Halo! Tu cyberbezpieczny Senior!”. Dzięki zawartym w poradniku praktycznym wskazówkom i przykładom starsze osoby zyskają wiedzę, która pomoże im bezpiecznie korzystać z internetu i unikać cyfrowych oszustów.

Publikacja poradnika zbiegła się z obchodzonym w zeszłym roku Światowym Dniem Seniora.

Wierzymy, że nasz poradnik pomoże seniorom z większą śmiałością i poczuciem bezpieczeństwa eksplorować internet. Edukacja cyfrowa chroni przed oszustwami, ale – co równie ważne – daje poczucie niezależności. Dzięki internetowi seniorzy mogą aktywnie uczestniczyć w życiu społecznym, mieć łatwy dostęp do informacji, pozostać w kontakcie z bliskimi i korzystać z różnych usług online, bez względu na wiek i stan zdrowia

– zauważa Beata Frankiewicz, specjalistka ds. budowania cyberświadomości w instytucie NASK

ROŚNIE LICZBA CYBERPRZESTĘPSTW

Liczba cyberprzestępstw w Polsce rośnie w ostatnich latach, co odzwierciedlają dane zespołu CERT Polska działającego w NASK, który w tym roku obsłużył już ponad 80 tysięcy incydentów bezpieczeństwa, przekraczając tym samym wynik zeszłoroczny. Rosnąca liczba odnotowanych incydentów oznacza także wzrost świadomości Polaków na temat cyberzagrożeń, co przekłada się na liczbę zgłoszeń do CERT Polska (cert@cert.pl lub sms na nr 8080). Chcemy, żeby także seniorzy rozpoznawali zagrożenia i aktywnie je zgłaszali, a poradnik „#Halo! Tu cyberbezpieczny Senior!” z pewnością zwiększy wiedzę na temat niebezpieczeństw czyhających w internecie.

WZROST KOMPETENCJI CYFROWYCH SENIORÓW ZWIĘKSZA ICH ODPORNOŚĆ NA OSZUSTWA

Badania przeprowadzone przez Główny Urząd Statystyczny w 2022 pokazują, że aż 29,9 proc. osób w wieku 60-74 nigdy nie korzystało z internetu. Niski poziom kompetencji cyfrowych sprawia, że seniorzy stają się łatwym celem dla cyberoszustów. Eksperci wskazują, że edukacja seniorów w zakresie cyberbezpieczeństwa jest kluczowa, szczególnie w czasach, gdy coraz więcej usług, takich jak bankowość czy administracja, przenosi się do internetu.

Z badania WIB „Seniorzy w świecie cyfrowych finansów” przeprowadzoneg w połowie stycznia 2025 r. wynika, że 76 proc. aktywnych cyfrowo seniorów korzysta z bankowości internetowej i 61 proc.

używa bankowości mobilnej. Z jednej strony ta otwartość seniorów na nowinki technologiczne cieszy, z drugiej zaś - cyfrowy świat to również przestrzeń dla przestępców. Stąd tak ważne jest dostarczanie tej grupie rzetelnej wiedzy o zagrożeniach, jakie mogą napotkać w sieci

– podkreśla Aleksandra Czyrkowska, koordynatorka projektów edukacyjnych w Warszawskim Instytucie Bankowości.

ABC CYBERBEZPIECZEŃSTWA

Poradnik „#Halo! Tu cyberbezpieczny Senior!" w przystępny sposób przybliża kluczowe zasady bezpieczeństwa online – od sposobów rozpoznawania oszustw internetowych, przez sprawdzanie autentyczności wiadomości, po dobre praktyki w ochronie danych. Znajdziemy w nim liczne przykłady oraz praktyczne porady, jak dbać o swoje dane w sieci, a także linki do dodatkowych źródeł, które pomogą bezpiecznie korzystać z internetu.

Takie publikacje są potrzebne, aby uzmysławiać, że przestępcy asymilują się z cyfrowym światem, są tam obecni i czyhają na możliwość dokonania oszustwa, również wymierzonego w osoby starsze. Kolorowe ilustracje w internecie, komunikaty zachęcające do „kliknięcia" powodują, że możemy wejść na stronę stworzoną przez oszusta, który używając różnych sposobów, podszywa się pod kogoś innego. Jego celem jest wyłudzenie od nas danych bądź nakłonienie do wykonania jakiegoś zadania, np. przelewu. W ten sposób możemy stracić oszczędności całego życia

– dodaje asp. Monika Przestrzelska z zespołu prasowego CBZC.•

Poradnik można pobrać na stronie internetowej pod linkiem:

https://bde.wib.org.pl/wp-content/uploads/2025/01/Poradnik__Halo__Tu_cyberbezpieczny_Senior.pdf

oraz skanując kod QR:

Dzięki licencji CC BY-NC (Creative Commons, Uznanie autorstwa, Użycie niekomercyjne) poradnik jest dostępny dla wszystkich instytucji przyjaznych seniorom, które mogą go swobodnie wykorzystywać w swojej działalności, wspierając edukację seniorów w zakresie cyberbezpieczeństwa.

Dezinformacja

– czy jesteśmy w stanie odróżnić ją od informacji w czasach używania nowych technologii i rozwoju sztucznej inteligencji?

Dzięki coraz bardziej zaawansowanym algorytmom technologicznym stosowanym przez sztuczną inteligencję (z ang. AI) możliwe jest generowanie realistycznych obrazów, filmów i dźwięków, które imitują prawdziwe osoby i wydarzenia. Skutki tych technologii to zarówno wyłudzenia finansowe, jak i manipulacja opinią publiczną na masową skalę oraz szerzenie dezinformacji. Deepfake (czyt. dipfejk) czy klonowanie głosu z powodzeniem wchodzą również do świata polityki, gdzie zmanipulowane nagrania video przedstawiają wypowiedzi polityków, które nigdy nie zostały wypowiedziane.

SZTUCZNA INTELIGENCJA I DEEPFAKE – CZYLI JAKĄ „PRAWDĘ" WIDZIMY?

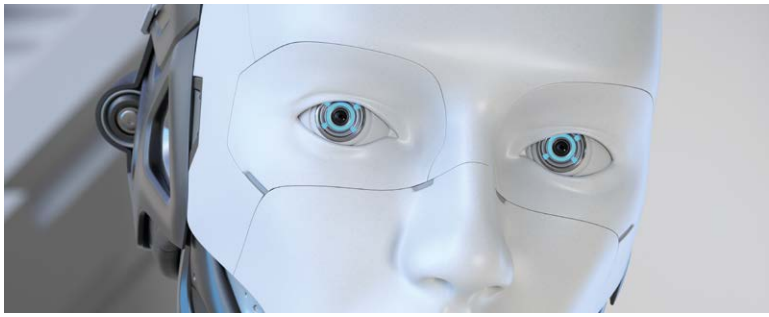
Technologia deepfake wykorzystuje zaawansowane modele uczenia maszynowego do analizy ogromnych ilości danych wizualnych i dźwiękowych. Dzięki temu możliwe jest stworzenie materiałów, które realistycznie imitują wizerunek i głos konkretnej osoby. Przykładowo, zaledwie kilkuminutowy materiał wideo wystarczy, aby stworzyć „klona" czyjegoś wizerunku, który może mówić lub wykonywać dowolne czynności. Wideo deepfake często wykorzystują technikę zamiany twarzy (ang. face swapping), która pozwala „nałożyć" twarz jednej osoby na ciało innej. Z kolei klonowanie głosu umożliwia generowanie dźwięków i wypowiedzi brzmiących niemal identycznie jak oryginalne, co jest możliwe dzięki zaawansowanej analizie próbek dźwięku.

Niezwykle niepokojącym aspektem jest fakt, że narzędzia do tworzenia deepfake'ów stają się coraz bardziej powszechne i łatwo dostępne. Istnieją aplikacje i platformy, które umożliwiają tworzenie takich materiałów bez konieczności posiadania zaawansowanej wiedzy technicznej. Przestępcy mogą w ciągu kilku minut stworzyć realistyczne nagranie wideo, które oszuka zarówno ludzi, jak i tradycyjne systemy weryfikacji.

FAŁSZYWE PRZEKAZY W DOBIE SZTUCZNEJ INTELIGENCJI

Głośne przykłady prób dezinformacji przy użyciu sztucznej inteligencji można wymieniać bez końca. To nie tylko zdjęcia tulących się do siebie Donalda Trumpa i Anthonego Fauciego, papież Franciszek w puchowej designerskiej kurtce, czy też spreparowane, wzbudzające strach zdjęcia ukazujące zniszczenia wywołane przez tą, czy inną stronę konfliktu zbrojnego.

To także potencjalnie niegroźne materiały wideo, które mają wyłudzać pieniądze, jak choćby materiał wideo pt.: „Samotna mama z Warszawy została milionerką dzięki aplikacji blogera Mr. Beast". Film podszywa się pod materiały tworzone przez TVP, a Marek Czyż ma w nim zachęcać do pobrania aplikacji hazardowej. W materiale pojawia się „zwyciężczyni" oraz wspomniany influencer, a dla uwiarygodnienia rzekomych przychodów także wizerunek PKO BP i jego aplikacji bankowej. Film kończy się zachętą do klikania w osadzony w nim link i „wejścia do gry". Oczywiście jest to fałszywy materiał, ale oszustwa tego typu są coraz częstsze.



DLACZEGO FAŁSZYWY PRZEKAZ JEST SKUTECZNY?

Twórcy dezinformacji poszli tropem, że najbardziej podobają się nam przecież piosenki, które znamy. Dlatego cyberprzestępcy często wykorzystują autorytet znanych osób publicznych, celebrytów lub marek, aby budować wiarygodność swoich oszustw. W kampaniach phishingowych oszuści podszywają się pod znane firmy, takie jak banki, serwisy streamingowe czy nawet media, jak TVP. W ten sposób zwiększają szansę na to, że ofiary uwierzą w autentyczność wiadomości. To już buduje skuteczność.

Łatwiej też manipuluje się odbiorcami, kiedy w grę wchodzi wzbudzanie emocji i snucie wiarygodnych historii. Ludzie są bardziej podatni na manipulację, gdy komunikaty są zaprojektowane tak, aby wzbudzać silne emocje – strach, współczucie lub chęć pomocy. Oszustwa takie jak „wirtualne porwania" bazują na strachu rodziców, którym przedstawia się zmanipulowane nagranie ukazujące ich dziecko w niebezpieczeństwie. Tego typu sytuacje są możliwe dzięki zastosowaniu technologii klonowania głosu oraz realistycznych narracji. Fałszywe przekazy często wykorzystują tzw. efekt halo – ludzie są bardziej skłonni uwierzyć w informacje, jeśli są one związane z autorytetem. Może to być zarówno znana osoba, jak i instytucja lub marka, której ufają.

DLACZEGO FAŁSZYWE PRZEKAZY SĄ CORAZ BARDZIEJ WIARYGODNE?

Kluczowym pytaniem wydaje się być nie to, dlaczego ulegamy dezinformacji, ale dlaczego jest ona tak skuteczna. Niewątpliwie postęp w dziedzinie sztucznej inteligencji sprawia, że materiały generowane przez AI są coraz trudniejsze do odróżnienia od autentycznych. Deepfake potrafi odwzorować mimikę, ton głosu, a nawet kontekstowe wypowiedzi, które pasują do danego materiału. Na rynku widać też rozwój narzędzi AI do tworzenia zmanipulowanych treści. Algorytmy AI, takie jak generatory tekstu, mogą tworzyć przekonujące narracje i konteksty, które uwiarygodniają fałszywe treści. To sprawia, że nawet wysoce sceptyczni użytkownicy internetu mogą zostać wprowadzeni w błąd. Natomiast media społecznościowe umożliwiające rozprzestrzenianie treści w ciągu kilku minut na całym świecie, przyczyniają się do rozpowszechniania fałszywych informacji. Czytając przykładowo posta na Facebooku, raczej nie zastanawiamy się czy zamieszczona tam treść jest prawdziwa i przyjmujemy, że przekazywana treść jest wiarygodna – stąd właśnie tzw. z angielskiego „fake newsy" (czyt. fejk niusy) zyskują popularność na platformach społecznościowych zanim zostaną w ogóle zweryfikowane.•

NASK

Znana twarz w reklamie?

Uważaj na oszustwa z użyciem sztucznej inteligencji (AI), która generuje zmanipulowane przekazy audio-video.

Wyobraź sobie, że przeglądasz internet, a znana osoba np. aktor, piosenkarz, sportowiec czy polityk z przekonaniem opowiada o inwestycji, która odmieniła jej życie.

„Wystarczyło tylko wpłacić niewielką sumę, by pomnożyć swoje pieniądze – to naprawdę działa!" – zapewnia ktoś, kogo dobrze znasz z telewizji lub mediów społecznościowych. Wydaje się, że nie masz powodów, by kwestionować prawdziwość tego, co widzisz i słyszysz. Przecież tak znane osoby nie narażałyby swojej reputacji, promując coś nieuczciwego. Myślisz: „Jeśli on to poleca, to musi być sprawdzone i bezpieczne".

Tymczasem osoby, które widzisz w nagraniu, nie mają nic wspólnego z reklamowaną „inwestycją". To jedynie iluzja – perfekcyjnie spreparowane nagranie stworzone przez sztuczną inteligencję (AI) po to, by zdobyć Twoje zaufanie. Wizerunek tych osób często jest bezprawnie wykorzystany przez oszustów i zmanipulowany za pomocą zaawansowanej technologii, która nazywa się z angielskiego deepfake (czyt. dipfejk).

DEEPFAKE, CZYLI SZTUKA ILUZJI

Efekt jest zdumiewający. Widzisz znaną twarz, słyszysz charakterystyczny głos, a wypowiedź pełna jest autentycznych emocji. Technologia deepfake, oparta na algorytmach sztucznej inteligencji, potrafi odwzorować mimikę, gesty i ton głosu z niezwykłą precyzją. Realizm jest tak przekonujący, że nawet osoby dobrze zaznajomione z tym zagadnieniem mogą mieć trudności z rozpoznaniem oszustwa. Przykłady takich fałszywych materiałów można zobaczyć na oficjalnym kanale NASK na YouTube.

ZBYT PIĘKNE, BY MOGŁO BYĆ PRAWDZIWE

Reklama prowadzi Cię na profesjonalnie wyglądającą stronę internetową, gdzie wszystko zdaje się potwierdzać autentyczność oferty: wykresy, historie sukcesów „innych inwestorów", a nawet „profesjonalna" obsługa klienta, która chętnie odpowiada na pytania. Oszuści dopracowują swoje materiały w najdrobniejszych szczegółach – fałszywe logo renomowanych firm, spreparowane artykuły prasowe czy rzekome wywiady budują iluzję wiarygodności.

NIE DAJ SIĘ ZWIEŚĆ POZOROM!

W takich sytuacjach łatwo stracić czujność, zwłaszcza gdy przekaz odwołuje się do emocji i nadziei na poprawę finansów. Oszuści często stosują presję czasu, zachęcając do natychmiastowego działania hasłami w stylu: „Oferta dostępna tylko dziś!" czy „Nie przegap swojej szansy na miliony!". Manipulacje tego rodzaju mają na celu wymuszenie szybkiej, nieprzemyślanej decyzji.

Takie triki mogą sprawić, że uwierzysz w pozornie atrakcyjne i bezpieczne inwestycje, takie jak kryptowaluty, metale szlachetne czy nieruchomości w przekonaniu, że dokonujesz właściwego wyboru. Niestety, gdy zorientujesz się, że to oszustwo, na odzyskanie utraconych pieniędzy może być już za późno.

SPRAWDZAJ ZANIM ZAUFASZ!

Każde działanie związane z inwestowaniem wiąże się z ryzykiem. Dlatego zanim podejmiesz decyzję, dokładnie zweryfikuj:

- dane rejestrowe firmy, która ma pośredniczyć w inwestycjach, tj. czy na stronie są dostępne takie informacje jak: adres firmy, NIP oraz dane kontaktowe tj. e-mail, telefon;
- historię firmy: posiadając numer NIP możesz zweryfikować historię firmy w Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEDIG) lub w Krajowym Rejestrze Sądowym (KRS);
- listę podmiotów objętych nadzorem Komisji Nadzoru Finansowego (KNF): to oficjalny spis firm i instytucji finansowych działających w Polsce, które podlegają regularnej kontroli KNF. Daje to pewność, że przestrzegają prawa i działają zgodnie z wysokimi standardami, dbając o interesy swoich klientów.

Przed podjęciem decyzji, warto także skonsultować się z najbliższymi lub zaufanym doradcą finansowym. Dodatkowa opinia może pomóc zidentyfikować potencjalne zagrożenia i uniknąć kosztownych błędów.

TWÓJ NAJWAŻNIEJSZY SOJUSZNIK – ZDROWY ROZSĄDEK

W świecie, gdzie technologia może oszukiwać zmysły, krytyczne myślenie i ostrożność to najlepsza obrona przed oszustami. Pamiętaj, że uczciwe inwestycje nie wymagają presji czasu, a rzetelni doradcy szanują Twoje prawo do przemyślenia decyzji. Jeśli ktoś naciska na natychmiastowe działanie, potraktuj to jako sygnał ostrzegawczy. Twoja czujność i rozwaga są bronią, której oszuści nie potrafią złamać. •

Oszustwo inwestycyjne

– na czym polega i jak się przed nim chronić?

Jednym z przykładów coraz częściej stosowanych nowych sposobów oszustw w internecie jest tzw. „oszustwo na inwestycje". Proponowane inwestycje są przedstawiane jako dochodowe, jednak ostatecznie bogacą się tylko oszuści. Potencjalni klienci są zachęcani wizją szybkiego zysku poprzez reklamy, w których nierzadko wykorzystywany jest bezprawnie wizerunek osób publicznych z pierwszych stron gazet. Niestety w takich przypadkach ofiary oszustw tracą bardzo wysokie kwoty, chcąc zainwestować swoje oszczędności, jak również wykorzystując środki z kredytów.

OSZUŚCI WYKORZYSTUJĄ RÓŻNE TECHNIKI, ŻEBY UWIARYGODNIĆ SWOJĄ OFERTĘ, TJ.:

- **profesjonalne reklamy w mediach społecznościowych i na stronach internetowych,**
- **szybki kontakt z zainteresowanym ofertą klientem,**
- **podszywanie się pod maklerów i brokerów giełdowych oraz ekspertów od produktów inwestycyjnych.**

Oferta inwestycji jest zazwyczaj przedstawiana bardzo profesjonalnie, przez co klient nie orientuje się, że ma do czynienia z oszustwem. Aby uwiarygodnić propozycję inwestycji, proponowana jest również „aplikacja inwestorska", gdzie klient ma swoje indywidualne konto, na którym może obserwować, jak firma inwestycyjna pomnaża pieniądze klienta - to dodatkowa sugestia, że mamy do czynienia z realną inwestycją, która w rzeczywistości jest oszustwem.

JAK WYGLĄDA OSZUSTWO INWESTYCYJNE W PRAKTYCE?

Najczęściej oszust kontaktuje się telefonicznie, mailowo lub przez media społecznościowe. Oferuje możliwość zainwestowania w produkty finansowe, jak na przykład kryptowaluty, co ma przynieść bardzo wysokie zyski w krótkim czasie jednocześnie przy niskim ryzyku inwestycyjnym. Bardzo często, fałszywe oferty są również opublikowane na specjalnie przygotowanych serwisach lub w mediach społecznościowych, np. na Facebooku. Kiedy już klient przekonał się do inwestycji, oszust nakłania go do samodzielnego wykonania transakcji lub do udostępnienia swojego urządzenia np. telefonu, na którym realizowane są transakcje (za pośrednictwem aplikacji służących do udostępniania zdalnego pulpitu lub innych komunikatorów), dzięki którym oszust może wykonać transakcje bez wiedzy klienta.

Drugim, równie istotnym elementem oszustwa na inwestycje jest sytuacja, w której rachunek klienta może zostać wykorzystany do dalszych transferów pieniężnych i w rezultacie klient bierze udział w przestępstwie polegającym na tzw. „praniu" pieniędzy pochodzących z nielegalnych źródeł. W ten sposób oszuści tworzą poczucie, że klient zarabia na swojej inwestycji, którą warto pomnażać.

Oszustwo na inwestycje może trwać przez dłuższy okres czasu. Kiedy klient próbuje wypłacić pieniądze z inwestycji lub zaczyna coś podejrzewać, kontakt z domniemanym „doradcą" urywa się, a zainwestowane środki, jak i zysk nie pojawiają się na rachunku klienta.

JAK SIĘ UCHRONIĆ? →

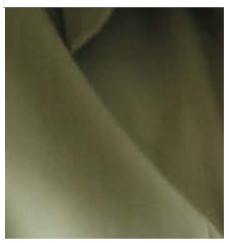
Jeśli masz podejrzenie, że to oszustwo, **zadzwoń na policję** i zgłoś niezwłocznie reklamację w swoim banku.

Sprawdź firmę, z którą chcesz podjąć współpracę w zakresie inwestycji w kilku źródłach. Czytaj opinie innych osób o danej firmie. Oszukani klienci często sami publikują ostrzeżenia przed nieuczciwymi podmiotami.

Uważaj na reklamy szybkiego zysku w internecie i mediach społecznościowych.

Nigdy nie podawaj loginu i hasła do bankowości internetowej czy danych swojej karty płatniczej (numer karty, CVV, data ważności) – te informacje są poufne, powinny być znane tylko Tobie.

Nie instaluj dodatkowego oprogramowania (np. Any Desk, Team Viewer, SplashTop) na urządzeniach, z których logujesz się do aplikacji bankowej.



Nie działaj w pośpiechu i pod wpływem impulsu.

Podmioty oferujące inwestycje muszą mieć zezwolenie na prowadzenie takiej działalności. **Firmy, które w Polsce są objęte nadzorem KNF znajdziesz w wyszukiwarce podmiotów nadzorowanych:** *www.knf.gov.pl/podmioty/wyszukiwarka_podmiotow.*

Jeśli otrzymasz przelew z obcego rachunku/od innej osoby, którego się nie spodziewasz nie przekazuj go dalej. **Jeśli to zrobisz, weźmiesz udział w przestępstwie.** Zgłoś sprawę w banku, w którym masz rachunek – możesz to zrobić w formie reklamacji.

Sprawdzaj listę ostrzeżeń publicznych KNF – tam znajdziesz komunikaty o podejrzanych firmach, które działają bez zezwolenia KNF: *www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne.*

Co możemy zrobić, by być bezpiecznym,
gdy korzystamy z internetu i podczas zakupów?

W polskim kalendarzu zakupowym istnieją różne specyficzne okresy skłaniające nas do podejmowania szybkich decyzji, np. przed świętami (Wielkanoc, Boże Narodzenie) czy innymi wydarzeniami handlowymi typu Hallowen czy Black Friday. To także dobra okazja, aby przypomnieć, że podczas „gorączki" zakupów, mogą pojawić się też przestępcy, którzy za pomocą różnych technik manipulacyjnych mogą nas oszukać.

OSZUŚCI POSZUKUJĄ NOWYCH NARZĘDZI, A JEDNOCZEŚNIE STOSUJĄ STARE SZTUCZKI

Jakie sytuacje powinny wzbudzać szczególną uważność i jakie są obecnie najpopularniejsze metody działania przestępców?

Oszustwa polegające na budowaniu relacji

Metoda ta określana po angielsku jako „pig butchering" (czyt. „pig buczering") wykorzystuję potrzebę bliskości, jaką odczuwamy szczególnie w Walentynki czy Nowy Rok. Przestępcy nawiązują ze swoimi ofiarami relacje, np. romantyczne w mediach społecznościowych i na portalach randkowych lub przyjaźnie rozpoczynające się od przypadkowej wiadomości na komunikatorze. Następnie przekonują je do zainwestowania w nieistniejące platformy wymiany kryptowalut, wykorzystując możliwości sztucznej inteligencji do tworzenia przekonujących komunikatów.

Metoda „na spadek"

Osoba będąca celem oszustwa jest powiadamiana o spadku pozostawionym rzekomo przez dalekiego krewnego. Przy czym zawiadomienie takie często pochodzi od wiarygodnie wyglądającej kancelarii prawnej, czy innego profesjonalnego podmiotu. Ostrzegawcza lampka powinna nam się zapalić, gdy proszeni jesteśmy o dyskrecję, sprawa jest pilna, mamy podać dane osobowe, a przyszłe zyski uzależnione są od zrealizowania wstępnej płatności.

Wyłudzenie pomocy humanitarnej

Żerując na ludzkich tragediach, oszuści proszą o pieniądze od niczego niepodejrzewających darczyńców, udając organizacje charytatywne prowadzące zbiórki w mediach społecznościowych.

Podszywanie się pod sklep internetowy

Oszuści tworzą fałszywe witryny online, oferując popularne produkty w przystępnej cenie. Celem takiego działania jest wyłudzenie informacji dotyczących płatności. Zamówienie zostanie wprawdzie zrealizowane przez rzeczywiście istniejących sprzedawców, ale informacje dotyczące płatności trafiają w niepowołane ręce.

W JAKI SPOSÓB ROZPOZNAĆ OSZUSTWO?

1.

SPRAWDZAJ WIADOMOŚCI POD KĄTEM BŁĘDÓW ORTOGRAFICZNYCH

– niespójności w języku użytym w danej wiadomości (np. w SMS-ie, komunikatorze czy w emailu), takie jak: błędy gramatyczne, układ słów lub różnice między nazwiskiem nadawcy a podanym linkiem do strony internetowej, mogą wskazywać na oszustwo. Jeśli otrzymasz wiadomość od firmy lub osoby znikąd, bądź czujny w sprawdzaniu tych błędów.

2.

BĄDŹ OSTROŻNY WOBEC WIADOMOŚCI NAKŁANIAJĄCYCH DO PILNEGO DZIAŁANIA

– język zachęcający do podjęcia pilnych działań jest powszechną taktyką używaną w fałszywych komunikatach. Zwracaj uwagę na frazy takie jak „wyślij (…) tutaj" lub „kliknij (…) poniżej" albo nieokreślone ramy czasowe, takie jak „w ciągu 48 godzin" lub „do jutra rano". Zawsze poświęć czas, aby rozważyć, czy wiadomość jest autentyczna. Jeśli uważasz, że jest fałszywa, ważne jest, aby nie klikać żadnych linków, aby uniknąć potencjalnego przekazania swoich danych osobowych przestępcom.

3.

UWAŻAJ NA PODEJRZANE PROŚBY

– oszuści często kuszą, podkreślając problem (np. prosząc o przełożenie dostawy) lub składając kuszącą ofertę (np. sugerując, że wygrałeś nagrodę). Pomyśl o swoich ostatnich kontaktach z tą organizacją lub osobą. Jeśli nie rozpoznajesz problemu, który masz rozwiązać, lub oferty, na którą masz zareagować, może to być oszustwo. Jeśli nie jesteś pewien, nie klikaj żadnych linków ani nie kontaktuj się z nadawcą w żaden sposób.

4.

ZWERYFIKUJ, CZY OSOBY, Z KTÓRYMI ROZMAWIASZ SĄ TYMI, ZA KTÓRYCH SIĘ PODAJĄ

– oszuści często starają się przekonać Cię o swojej wiarygodności, czasami używając słów i fraz, które możesz znaleźć w autentycznych komunikatach. Może być trudno odróżnić, więc jeśli nie jesteś pewien, możesz sprawdzić, używając innej formy komunikacji niż ta, którą użyli, aby się z Tobą skontaktować. Na przykład, jeśli otrzymasz SMS z prośbą o informacje bankowe, spróbuj wysłać e-maila lub skontaktować się bezpośrednio z firmą przez czat internetowy, aby sprawdzić, czy to prawdziwa prośba.

5.

SPRAWDŹ WIADOMOŚĆ Z KIMŚ, KOMU UFASZ

– prawdziwi ludzie są świetni w rozumieniu języka i komunikacji w kontekstach społecznych. Może to zabrzmieć oczywiście, ale jeśli nie jesteś pewien autentyczności wiadomości, warto omówić ją z kimś, komu ufasz. Mogą również otrzymać podobną wiadomość i mogą pomóc doradzić, jakie działania podjąć. Dzielenie się swoim doświadczeniem może również uratować kogoś innego przed padnięciem ofiarą.

SENIORZE BĄDŹ BEZPIECZNY PODCZAS ZAKUPÓW

Visa dba, aby płacący jej kartą mogli cieszyć się spokojem ducha, zapewniając różne zabezpieczenia podczas płatności, także tych w internecie. Używa wielu warstw zabezpieczeń, aby zapobiegać oszustwom, chroni dane i pomaga w odzyskaniu pieniędzy, jeśli ktoś użyje karty Visa bez zgody jej właściciela.•

Aktywny, czyli bezpieczny senior i seniorka.

Internet to wspaniałe narzędzie dla każdego bez względu na wiek. Korzystajmy z niego, ale jednocześnie pamiętajmy o tym, aby zachowywać najwyższe standardy bezpieczeństwa, bo przecież chodzi o nasze poufne informacje i pieniądze – radzi Michał Mazur, ekspert ds. cyberbezpieczeństwa w Departamencie Wykrywania Cyberzagrożeń i Fraudów Transakcyjnych Santander Bank Polska.

FAŁSZYWE TELEFONY Z „BANKU"

Podejrzane połączenia telefoniczne są już z nami od dłuższego czasu. Oszuści bardzo często podszywają się pod pracowników banku, policję czy rodzinę. Dlatego powinniśmy być bardzo czujni, kiedy ktoś przekonuje nas, że nasze pieniądze są w niebezpieczeństwie, albo że coś złego stało się naszym najbliższym. Nigdy nie działajmy pod presją czasu ani nie przekazujmy pieniędzy lub informacji nieznanym osobom. Warto sprawdzić, czy bank, w którym mamy konto, oferuje funkcjonalność weryfikacji pracownika, który dzwoni do nas z jakąś sprawą. A w rodzinie można ustalić tzw. hasło bezpieczeństwa. Kiedy będziemy mieli wątpliwość, że dzwoni do nas np. wnuczek, zapytajmy go o to hasło.

ODPOWIEDZIALNE ZAKUPY ONLINE

Kupowanie w internecie jest łatwe i wygodne. Trzeba jednak pamiętać, że również podczas zakupów online mogą czyhać na nas cyberprzestępcy. Zbyt dobre okazje czy promocje mogą okazać się zwykłym oszustwem. Musimy uważać na fałszywe reklamy w internecie oraz nieprawdziwe czy nieuczciwe sklepy. Najlepiej kupować w miejscach sprawdzonych, wiarygodnych i pamiętać o kilku poniższych wskazówkach.

- Warto czytać komentarze i opinie – sklepy „krzaki" mogą mieć niewiele komentarzy, które zostały wystawione na potrzeby oszustwa.
- Warto sprawdzić, czy sklep ma regulamin, dostępne różne formy kontaktu – działalność gospodarczą można znaleźć w publicznej bazie CEIDG
- Tylko jedna opcja zapłaty w sklepie, np. przelew na konto, to mocny sygnał ostrzegawczy.
- Lepiej zrezygnować z zakupu, jeśli dany towar jest np. sporo tańszy niż w kilku innych sklepach internetowych.
- Nie należy klikać w linki, które wysyłają nieznane osoby i nakłaniają do kliknięcia pod pretekstem płatności za zakupiony towar.
- Za zakupy w internecie najlepiej płacić kartą, aby w określonych sytuacjach móc skorzystać z usługi chargeback*

**dodatkowa ochrona płatności, np. w sytuacji, kiedy nie otrzymasz zamówionego produktu, jest on uszkodzony lub niezgodny z opisem.*

BEZPIECZNIEJSZE BANKOWANIE

Niezależnie od tego, jakie sztuczki stosują cyberoszuści, warto też sprawdzić, jakie zabezpieczenia daje nam nasz bank, kiedy korzystamy z konta w internecie. Oto kilka wskazówek dotyczących zabezpieczeń stosowanych przez banki, na które warto zwrócić uwagę.

- Logowanie do banku – dodatkowe czynnik logowania czyli np. kod z SMS-a, który podajemy po haśle to powinien być standard. Możemy też sprawdzić czy banki nie mają innych funkcjonalności, np. obrazek bezpieczeństwa, który zawsze będzie pojawiał się przy logowaniu. Jeśli go zabraknie, najlepiej wtedy skontaktować się z bankiem.

- Limity transakcji i wypłat gotówki – dobrze, aby były one dostosowane do naszych potrzeb. Samodzielna zmiana limitów zwykle jest możliwa i łatwa do wykonania, więc w każdej chwili, kiedy musimy zrobić większą transakcję, możemy limit podwyższyć, a następnie wrócić do niższego.

- Banki oferują też alerty, które poinformują nas o realizowanych transakcjach. Jeśli jakaś będzie budziła nasze wątpliwości, to jak najszybciej należy skontaktować się z bankiem.

- Aplikacja mobilna – jeśli „bankujemy" na telefonie, to koniecznie róbmy to przez oficjalną aplikację banku, którą ściągamy tylko ze sklepu z aplikacjami, np. Google Play, App Store.

- Zabezpieczmy telefon hasłem, a jeśli mamy taką możliwość, to również biometrią (tj. poprzez odcisk palca czy skan twarzy).

- Czytajmy i najlepiej przesyłajmy znajomym i najbliższym materiały edukacyjne, które przygotowują banki, ponieważ nasze bezpieczeństwo zależy przede wszystkim od nas. Jeśli znamy metody przestępców, łatwiej się przed nimi uchronić.

Nie daj się oszukać!

Proste zasady, jak rozpoznać manipulacje stosowane przez oszustów.

Oszustwa to niestety codzienność, zwłaszcza w świecie, gdzie technologia odgrywa coraz większą rolę. Oszuści sprytnie wykorzystują telefony i internet, by wyłudzić nasze dane czy pieniądze. Wystarczy znać kilka zasad, by nie dać się nabrać. Oszustwa bazujące na manipulacji i działające przeważnie na emocjach – znane jako socjotechnika – to coraz częstsza forma wyłudzania danych i pieniędzy. Seniorzy jako doświadczeni życiowo są szczególnie cenni dla oszustów, którzy starają się wykorzystać ich zaufanie i poczucie odpowiedzialności.

JAK MOŻE MANIPULOWAĆ NAMI OSZUST?

Metoda pośpiechu i presji

stosuje takie wyrażenia jak np. „To pilne! Proszę działać natychmiast!" – nie daj się wciągnąć w takie szybkie tempo podejmowania ważnych decyzji. Daj sobie czas na zastanowienie.

Podszywanie się pod autorytet

oszuści często podszywają się pod ekspertów i mówią o „ważnych regulacjach" czy „działaniach operacyjnych".

Podszywanie się pod autorytet

oszuści mogą próbować wzbudzić Twoje zaufanie, stosując niepodważalne wyrażenia, np. „Na pewno zależy Panu/Pani na bezpieczeństwie".

CO ROBIĆ W TRUDNYCH SYTUACJACH?

ROZŁĄCZ SIĘ
– to najlepsze rozwiązanie, jeśli rozmowa wydaje Ci się podejrzana.

ZADAWAJ PYTANIA
– oszuści często gubią się, gdy prosisz o szczegóły.

NIE DAJ SIĘ ZMANIPULOWAĆ
– nawet jeśli rozmówca mówi przekonująco, miej z tyłu głowy, że to może być oszustwo.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA:

1. **NIGDY NIE PODAWAJ POUFNYCH DANYCH PRZEZ TELEFON**
– numer PESEL, dowodu osobistego czy karty płatniczej to informacje, które musisz chronić;

2. **NIE PODAWAJ KODU BLIK PRZEZ TELEFON**
– ten kod służy do płatności, a nie do „weryfikacji";

3. **NIE KLIKAJ W PODEJRZANE LINKI**
– zwłaszcza jeśli przychodzą w SMS-ie czy e-mailu od nieznanych nadawców.

PAMIĘTAJ – INSTYTUCJE TAKIE JAK BANK I POLICJA NIGDY:

- nie poproszą Cię o wykonanie przelewu na „bezpieczne konto",
- nie będą wymagać podania kodu BLIK czy danych osobowych przez telefon,
- nie będą oczekiwać „wsparcia finansowego" dla swoich działań.

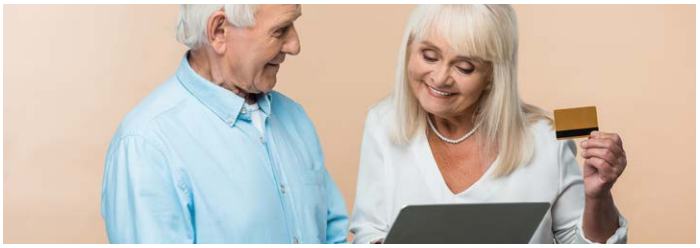
Jeśli coś wydaje się podejrzane, rozłącz się i skontaktuj bezpośrednio z daną instytucją, używając oficjalnego numeru. To jedyny sposób, by upewnić się, że rozmawiasz z prawdziwym pracownikiem.

Zamiast ulec presji, zawsze zachowaj zdrowy rozsądek. Twoje bezpieczeństwo jest najważniejsze – nie bój się kwestionować informacji, które otrzymujesz. Dzięki ostrożności i rozwadze możesz uniknąć problemów i cieszyć się spokojem każdego dnia.•

Bankowość elektroniczna

– jak korzystać z niej bezpiecznie?

Korzystanie z bankowości internetowej to duża wygoda – możesz sprawdzić stan konta, zrobić przelew czy zapłacić rachunki bez wychodzenia z domu. Aby jednak robić to bezpiecznie, warto znać kilka prostych zasad. Ten poradnik pomoże Ci poruszać się po świecie bankowości elektronicznej z pewnością i spokojem.



ZAWSZE KORZYSTAJ Z WŁASNEGO URZĄDZENIA

Kiedy chcesz zalogować się do swojego konta, rób to tylko na swoim komputerze, tablecie lub telefonie. Korzystanie z urządzeń w miejscach publicznych, takich jak biblioteka, może być ryzykowne – takie sprzęty nie zawsze są dobrze zabezpieczone. Jeśli musisz zalogować się do banku poza domem, skorzystaj z własnego telefonu i połączenia komórkowego, a nie z darmowego Wi-Fi w kawiarni.

AKTUALIZACJE TO TWOI SPRZYMIERZEŃCY

Każdy komputer, tablet czy telefon ma swoje oprogramowanie, które regularnie wymaga aktualizacji. Te uaktualnienia to nie tylko nowe funkcje, ale przede wszystkim poprawki zabezpieczeń. Dzięki nim Twoje urządzenie jest mniej podatne na ataki hakerów. Włącz automatyczne aktualizacje, aby mieć pewność, że wszystko jest zawsze na bieżąco.

SILNE HASŁO – TWOJE CYFROWE KLUCZE

Twoje hasło to klucz do konta – powinno być jak najsilniejsze, aby nikt nie mógł go złamać. Dobre hasło powinno mieć przynajmniej 12 znaków i zawierać różne elementy: duże i małe litery, cyfry oraz znaki specjalne, takie jak „@”, „#” czy „!”.

Unikaj prostych haseł, takich jak Twoje imię, data urodzenia czy popularne kombinacje typu „123456” lub „haslo”. Te łatwo zgadnąć, a Twoje konto może stać się celem ataku.

Każde konto powinno mieć swoje hasło – inne do banku, inne do poczty czy mediów społecznościowych. Jeśli używasz jednego hasła wszędzie, złamanie go daje przestępcom dostęp do wszystkich Twoich danych.

Jeśli obawiasz się, że zapomnisz hasła, możesz skorzystać z menedżera haseł – to aplikacja, która zapisze i bezpiecznie przechowa Twoje hasła. Pamiętaj, aby nikomu nie udostępniać swoich haseł!

KORZYSTAJ Z APLIKACJI MOBILNYCH

Jeśli masz smartfon, warto zainstalować aplikację swojego banku. Aplikacje oferują dodatkowe funkcje, takie jak powiadomienia o transakcjach czy szybkie logowanie za pomocą biometrii (np. odcisku palca lub rozpoznawania twarzy). Pamiętaj, aby aplikacje bankowe pobierać tylko z oficjalnych sklepów, takich jak Google Play czy App Store.

KORZYSTAJ Z APLIKACJI MOBILNYCH

Regularne kontrolowanie konta to ważny nawyk. Sprawdzaj historię transakcji, aby upewnić się, że wszystkie operacje zostały wykonane przez Ciebie. Jeśli zauważysz coś podejrzanego – np. wypłatę pieniędzy, której nie dokonywałeś – natychmiast skontaktuj się z bankiem.

NIE ZAPOMINAJ O WYLOGOWANIU

Po zakończeniu korzystania z bankowości internetowej zawsze kliknij „Wyloguj". Zamknięcie okna przeglądarki nie wystarcza – sesja może nadal być aktywna, co stanowi ryzyko. Nigdy nie zapisuj danych logowania w przeglądarce, zwłaszcza na urządzeniach, z których korzysta więcej osób.

UWAŻAJ NA WIADOMOŚCI OD OSZUSTÓW

Bank nigdy nie poprosi Cię o podanie hasła, numeru PIN ani innych poufnych danych przez telefon, SMS czy e-mail. Jeśli dostaniesz taką wiadomość, zachowaj czujność i zadzwoń do swojego banku, korzystając z numeru podanego na ich stronie internetowej. Nie klikaj w podejrzane linki w wiadomościach e-mail ani SMS-ach – mogą prowadzić na strony, które próbują wyłudzić Twoje dane.

EDUKUJ SIĘ I PYTAJ

Świat technologii zmienia się bardzo szybko, ale nie musisz być w tym sam. Banki i różne organizacje często prowadzą szkolenia i warsztaty dla seniorów, gdzie możesz nauczyć się korzystania z bankowości internetowej.

Nie bój się pytać – zarówno doradców w banku, jak i bliskich. Dla nich to chwila, a Tobie może dać to dużo pewności siebie.

Bankowość elektroniczna może ułatwić życie, ale wymaga ostrożności. Warto pamiętać o podstawowych zasadach, aby korzystać z niej bezpiecznie. Bądź czujny, korzystaj z nowoczesnych zabezpieczeń i nie bój się pytać o pomoc, jeśli masz wątpliwości. Twoje bezpieczeństwo jest najważniejsze!•

Bezpieczny senior to wyedukowany senior
– wydarzenia edukacyjne WIB

Fundacja Warszawski Instytut Bankowości (WIB) nieustannie angażuje się w edukację cyfrową seniorów, dbając o ich bezpieczeństwo online. W ramach projektów edukacyjnych „Bezpieczeństwo w Cyberprzestrzeni" oraz „Aktywny Senior" organizuje wykłady i spotkania oraz warsztaty na Uniwersytetach III Wieku, podczas których edukuje seniorów, jak chronić się przed zagrożeniami w sieci i bezpiecznie korzystać z usług cyfrowych, w tym bankowości internetowej i mobilnej oraz płatności elektronicznych.

W minionym 2024 r. warto wyróżnić spotkanie edukacyjne pt. „Cyfrowy senior – aktywny, edukowany, bezpieczny" organizowanym w ramach VIII Kongresu Edukacji Finansowej i Przedsiębiorczości w warszawskim Centrum Aktywności Międzypokoleniowej „Nowolipie". Eksperci z instytucji partnerskich przedstawili seniorom pigułkę wiedzy na temat bezpiecznego poruszania się w sieci i ochrony przed możliwymi zagrożeniami, Pani Prezes Krajowego Instytutu Gospodarki Senioralnej – p. Marzena Rudnicka opowiedziała o świadomym korzystaniu z zasobów internetowych i metodach zdobywania rzetelnej wiedzy, Wiceprezes Warszawskiego Instytutu Bankowości – p. Michał Polak zaprezentował wyniki opracowanego przez WIB badania opinii publicznej pt. „Seniorzy w świecie cyfrowych finansów" (edycja badania z 2024r.), w tym w jaki sposób nowoczesny senior płaci bezgotówkowo, a gość specjalny Beata Borucka – influencerka „Mądra Babcia" zachęcała uczestników spotkania do aktywizacji cyfrowej, w tym rozwijania pasji za pomocą internetu czy sposobów przekształcania swoich zainteresowań w formę zarobku online.

Spotkanie edukacyjne pt. „Cyfrowy senior – aktywny, edukowany, bezpieczny" organizowane w ramach VIII Kongresu Edukacji Finansowej i Przedsiębiorczości w warszawskim Centrum Aktywności Międzypokoleniowej „Nowolipie".

Wykłady na Uniwersytetach III Wieku w ramach kampanii pod patronatem Ministerstwa Cyfryzacji pn. „Aktywnie w sieci".

Spotkanie edukacyjne pt. „Cyfrowy senior – aktywny, edukowany, bezpieczny" organizowane w ramach VIII Kongresu Edukacji Finansowej i Przedsiębiorczości w warszawskim Centrum Aktywności Międzypokoleniowej „Nowolipie".

Ciekawym wydarzeniem, do którego włączył się w 2024 r. Warszawski Instytut Bankowości było również spotkanie edukacyjne organizowane przez PKO Bank Polski z Powstańcami Warszawskimi w warszawskiej Rotundzie PKO. Podczas wydarzenia, Wiceprezes WIB przedstawił na podstawie badania „Seniorzy w świecie cyfrowych finansów" wizerunek współczesnego seniora, który obecnie coraz śmielej porusza się po cyfrowym świecie, również tym finansowym, coraz chętniej płaci kartami płatniczymi i używa smartfonu do obsługi bankowości, a zakupy w sieci opłaca BLIK-iem. Natomiast zespół ekspertów z PKO Banku Polskiego wraz naczelnikiem Wydziału Nadzoru i Koordynacji Centralnego Biura Zwalczania Cyberprzestępczości w Warszawie podzielili się wskazówkami, jak rozpoznać fałszywe maile i SMS-y, unikać phishingu, bezpiecznie logować się do bankowości internetowej, korzystać z aplikacji mobilnych i chronić dane w przestrzeni publicznej.

Warto również podkreślić, że WIB wraz z instytucjami partnerskimi, np. z NASK – Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym organizuje wykłady na Uniwersytetach III Wieku, dotyczących zasad bezpiecznego poruszania się w przestrzeni cyfrowej, a także w zakresie rozpoznawania dezinformacji. Dodatkowo w 2024 r. NASK został partnerem merytorycznym kampanii pod patronatem Ministerstwa Cyfryzacji pn. „Aktywnie w sieci", w której edukowaliśmy seniorów na temat bezpiecznego korzystania z narzędzi e-administracji i funkcjonalności aplikacji mObywatel.•

Spotkanie edukacyjne organizowane przez PKO Bank Polski z Powstańcami Warszawskimi w warszawskiej Rotundzie PKO.

Kampania edukacyjna „@ktywnie w sieci”

pod patronatem Ministerstwa Cyfryzacji

Fundacja Warszawski Instytut Bankowości we współpracy z Ministerstwem Cyfryzacji oraz Naukową Akademicką Siecią Komputerową (NASK) przeprowadziła przy okazji Europejskiego Miesiąca Cyberbezpieczeństwa w 2024 r. kampanię edukacyjną pn. „@ktywnie w sieci”.

Jej głównym celem było wsparcie procesu podnoszenia wiedzy i kształtowania właściwych postaw społeczeństwa w zakresie aktywnego i bezpiecznego korzystania z nowoczesnych, cyfrowych narzędzi dostępnych za pośrednictwem administracji publicznej i sektora bankowego. Kampania miała charakter ogólnopolski, a jej koncepcja zakładała bezpośrednie dotarcie przede wszystkim do dzieci i młodzieży, studentów oraz pracowników uczelni, ale także seniorów.

W ramach kampanii WIB i NASK przeprowadzili trzy wykłady na Uniwersytetach III Wieku, tj. na Politechnice Warszawskiej, w Szkole Głównej Handlowej w Warszawie oraz w Hajnówce w woj. podlaskim. Podczas spotkań z seniorami omówiono m.in. takie zagadnienia jak: bezpieczne korzystanie z usług e-administracji, korzyści wynikające z używania aplikacji mObywatel, w tym funkcji „Zastrzeż PESEL” i „Bezpiecznie w sieci” oraz jak chronić swoją prywatność i wizerunek w sieci.

O programie „Bankowcy dla Edukacji”

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 różnych grup odbiorców w różnych 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 „Seniorzy w świecie cyfrowych finansów” *(dawniej: „InfoSenior”)*
- poradniki i materiały informacyjne
- biuletyny i newslettery
- broszury edukacyjne
- kampania filmowa „Bankowcy dla CyberEdukacji”
- kampania edukacyjna „Seniorze – spotkajmy się w sieci” i „#Halo! Tu cyberbezpieczny senior”.

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

Chcesz być na bieżąco z naszymi działaniami skierowanymi do seniorów – odwiedzaj nasze strony internetowe:

Program Bankowcy dla Edukacji	Fundacja Warszawski Instytut Bankowości
www.bde.wib.org.pl	www.wib.org.pl

Masz pytania, chcesz rozpocząć współpracę i przyłączyć się do naszych działań – napisz do nas email:

seniorzy@wib.org.pl
lub aczyrkowska@wib.org.pl

Biuletyn „Aktywny Senior" jest wydawany w ramach programu „Bankowcy dla Edukacji", którego Patronem jest Związek Banków Polskich

BANKOWCY DLA EDUKACJI
program sektorowy

ZWIĄZEK BANKÓW POLSKICH