



Ministerstwo Rodziny
i Polityki Społecznej



e-SENIOR 2.0
OSZUSTWA
INTERNETOWE
SKIEROWANE DO
SENIORÓW



*Witam Państwa
serdecznie,*



Broszura, którą trzymają Państwo w rękach, została przygotowana przez Fundację „Idea dla Ciebie” jako część projektu „e-SENIOR 2.0” współfinansowanego przez Ministerstwo Rodziny i Polityki Społecznej w ramach Programu Wieloletniego na rzecz Osób Starszych „Aktywni+” na lata 2021–2025. Edycja 2023. Projekt ten dedykowany jest zarówno dla osób, które nie miały do tej pory do czynienia z urządzeniami takimi jak bankomat, komputer, tablet, czy smartfon, jak również dla tych, które są na początku tej drogi. Celem tego projektu jest przede wszystkim przedstawienie Seniorom podstawowych zasad bezpieczeństwa dotyczącego użytkowania tych urządzeń. Zapraszam Państwa do zapoznania się z niniejszą publikacją, w której w prosty i przystępny sposób przedstawione zostaną podstawowe informacje związane z zasadami bezpieczeństwa Seniorów podczas korzystania z internetu.

Z wyrazami szacunku,

Agnieszka Janczura

Prezes Fundacji "Idea dla Ciebie"



Dziękuję wszystkim, którzy nauczyli mnie wytrwałości w dążeniu do celu i odwagi w podejmowaniu decyzji. Dżę wiem, jak wielką wartość ma przyjań i jak ważne jest dzielenie się wiedzą i doświadczeniem. Patrz szerzej. Mierz daleko. Odkrywaj nowe horyzonty...

Agnieszka Janeczura



Idea dla Ciebie

@ideadlaciebie · 1,11 tys. subskrybentów · 145 filmów

Ideą naszej Fundacji jest inspirowanie do zmian i odkrywania nowych możliwości niezależ... >

ideadlaciebie.org/wspieraja-nas

Subskrybuj

Główna Wideo Shorts Playlisty Społeczność Kanały Informacje 🔍

Zapraszam na kanał YouTube „Idea dla Ciebie”, na którym znajdują Państwo filmy przygotowane z myślą o Seniorach pod następującymi tytułami:

1. Jak bezpiecznie korzystać z bankomatu?
2. Oszustwa internetowe skierowane do seniorów.
3. Bankowe konto internetowe - zasady bezpieczeństwa.
4. Podstawy Worda dla seniorów.
5. Podstawy Excela dla seniorów.

www.e-senior.org.pl

Na stronie internetowej www.e-senior.org.pl również znajdują Państwo powyższe filmy, ale także niniejszy skrypt do samodzielnego pobrania i wydrukowania. Zapraszam.

KILKA SŁÓW WSTĘPU

W dzisiejszych czasach korzystanie z internetu stało się nieodłączną częścią naszego życia. Daje nam to wiele korzyści, ale jednocześnie niesie za sobą pewne zagrożenia. Dlatego ważne jest, aby być świadomym tych zagrożeń i umieć je rozpoznać oraz unikać.

Osoby starsze, które dorastały w czasach bez dostępu do Internetu i smartfonów, są szczególnie narażone na działania oszustów. Często nie zdajemy sobie sprawy, jak łatwo i szybko można zostać oszukanym przy użyciu nowoczesnych technologii. Statystyki pokazują, że liczba ataków cyberprzestępczych wymierzonych w seniorów rośnie z roku na rok, a oszuści stają się coraz bardziej kreatywni w swoich działaniach.

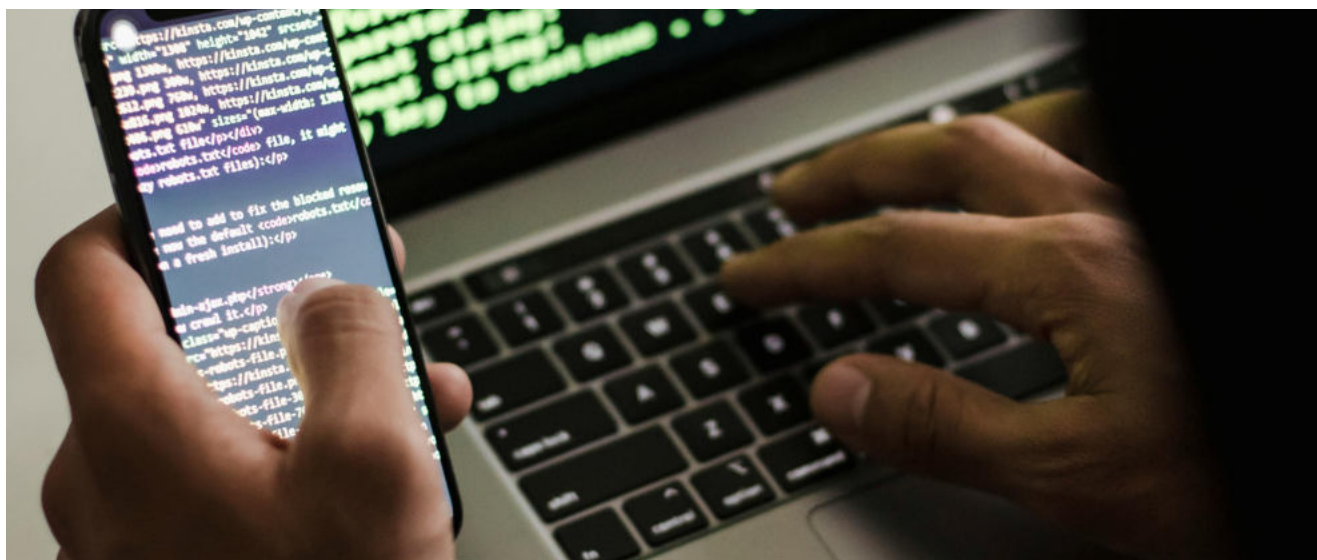


Uważaj na zagrożenia w internecie

Hakerzy doskonale zdają sobie sprawę z tego, że wiele osób starszych nie posiada odpowiedniej wiedzy i świadomości, jeśli chodzi o korzystanie z internetu. Wykorzystują to, aby wyłudzić pieniądze lub dane poufne.

Osoby starsze są częstym celem ataków oszustów. Ufność i uczciwość, które często są charakterystyczne dla tej grupy wiekowej, są wykorzystywane przez przestępców. Dlatego tak ważne jest, aby zdawać sobie sprawę z metod, jakie wykorzystują oszuści. Na kolejnych stronach przedstawionych zostanie kilka najpopularniejszych sposobów wykorzystywanych przez oszustów, których warto być świadomym, aby uchronić się przed takimi sytuacjami.

Oszuści internetowi są nieustannie w pogoni za nowymi sposobami oszukiwania osób, szczególnie starszych. Ich skuteczność polega na umiejętnym wykorzystywaniu emocji, takich jak strach, lęk, troska o kogoś bliskiego czy nawet radość z nieoczekiwanej wygranej. Manipulując, starają się doprowadzić do szybkiego działania pod naciskiem i presją czasu. Dlatego ważne jest, aby być świadomym ich metod i zachować czujność.



Jak oszuści internetowi WYKORZYSTUJĄ NASZE EMOCJE?



Oszuści internetowi stosują różne techniki manipulacyjne, aby osiągnąć swoje cele. Poniżej przedstawiamy kilka z nich, na które należy być szczególnie czujnym:

1. Wzbudzanie LĘKU lub NIEPOKOJU

Często dzwoniąc do starszej osoby, oszuści podają się za pracownika banku lub policji i informują np. o włamaniu na jej konto. W ten sposób starają się sprowokować strach i lęk, aby ta podjęła szybkie działania. Należy pamiętać, że żaden prawdziwy pracownik instytucji finansowej czy organu ścigania nie prosi o przekazanie pieniędzy telefonicznie.

2. Nacisk na SZYBKIE DZIAŁANIE i SZYBKIE PRZEKAZANIE PIENIĘDZY

Oszuści starają się wyrzucić presję na seniorze, aby ten działał szybko i przekazał im pieniądze. Często podają konkretne terminy mówiąc, że należy się z nich wywiązać. Pamiętajmy, że żadna legalna instytucja nie nakazuje takich działań i zawsze warto zasięgnąć porady przed podjęciem jakichkolwiek kroków.



3. Prośba o ZACHOWANIE TAJEMNICY

Oszuści często mówią seniorom, że rozmowa jest poufna i nie powinna być nikomu donoszona. To ma zmusić osoby starsze do zachowania informacji tylko dla siebie, uniemożliwiając tym samym zweryfikowanie prawdziwości sytuacji przez osobę trzecią. W takiej sytuacji należy pamiętać, że ważne jest konsultowanie się z zaufanymi osobami lub służbami odpowiedzialnymi za bezpieczeństwo.

4. Informowanie o PRZYJŚCIU ZAUFANEJ OSOBY

Oszuści często podają, że zaufana osoba przyjdzie i odbierze pieniądze. Chcą tym samym wprowadzić ofiarę w błąd, że cała sytuacja jest legalna i kontrolowana. Należy pamiętać, że prawdziwa zaufana osoba nie będzie prosić o przekazanie jakichkolwiek środków finansowych.



5. Wykonywanie WIELU TELEFONÓW w krótkim czasie

Oszuści dokonując kilku połączeń telefonicznych w krótkich odstępach czasu, utrudniają ofierze sprawdzenie prawdziwości ich twierdzeń. Starają się tym samym wyeliminować możliwość weryfikacji sytuacji i manipulować umysłem seniora. W takiej sytuacji warto odłożyć telefon na bok i skonsultować się z innymi osobami przed podjęciem jakichkolwiek działań.

6. Nakłanianie do ZAINSTALOWANIA SPECJALNEJ APLIKACJI

Nakłanianie do instalowania aplikacji: Często oszuści sugerują starszym osobom, że muszą zainstalować specjalną aplikację na swoim telefonie lub komputerze w celu ochrony. Pamiętajmy, że nie jest to dobrze znana praktyka i należy zachować szczególną ostrożność przed pobieraniem i instalowaniem nieznanych aplikacji.

POZNAJ 11 NAJCZĘSTSZYCH OSZUSTW SKIEROWANYCH DO OSÓB STARSZYCH

1. FAŁSZYWE NAGRODY

Schemat tego ataku jest prosty – ofiara otrzymuje informację, że wygrała nagrodę rzeczową, wycieczkę lub dużą kwotę pieniędzy, ale z powodu biurokracji musi uiścić stosunkowo niewielką opłatę, aby ją odebrać.

W drugim wariantcie oszukany ma podać dane osobowe i bankowe, aby wygrana została “przesłana” (co oczywiście nigdy nie następuje). Dane te są z kolei wykorzystywane, by włamać się na konto bankowe lub podszyć się pod cudzą tożsamość, np. w celu wzięcia kredytu lub założenia fałszywej firmy.

Oszustwo może przybierać różne formy – np. baneru na stronie internetowej informującego, że jesteś milionowym gościem lub e-maila z informacją, że wygrałeś na loterii. Niezależnie od tego, jaką drogą oszust się kontaktuje, jego celem jest uzyskanie w ten sposób korzyści finansowej.



2. PODSZYWANIE SIĘ POD POLICJĘ lub inne służby

Przestępcy często wykorzystują podszywanie się pod policję lub inne służby w celu zastraszenia swoich ofiar. Wydawałoby się, że taka metoda jest rzadka, ale niestety nie jest to prawda. W ostatnich latach liczba przypadków tego typu przestępstw znacznie wzrosła, a ofiarami padają zarówno zwykli obywatele, jak i korporacje.

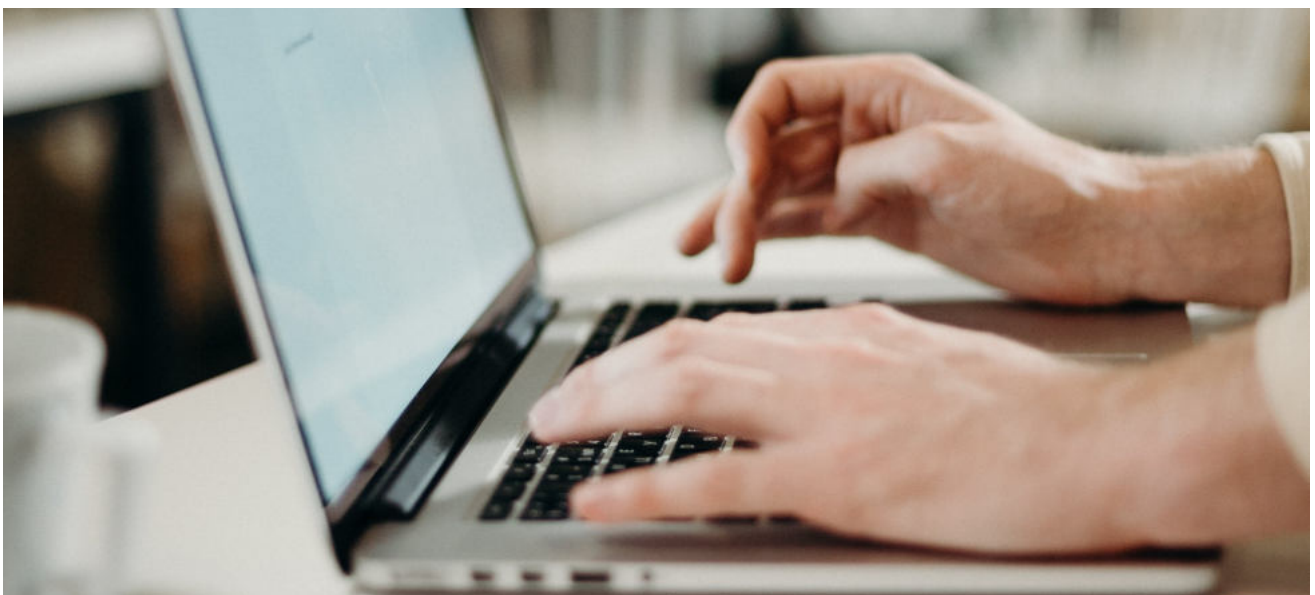
Jeden z popularnych scenariuszy to oszustwo, które dotyczy osób starszych. Starsza osoba otrzymuje maila, w którym informuje się ją, że na jej komputerze zostały znalezione nielegalne materiały lub że odtworzyła lub pobrała nielegalny film. Oczywiście, takie wiadomości są fałszywe, ale przestępcy liczą na to, że starsza osoba uwierzy im bez zastanowienia.

Gdy ofiara da się nabrać i uwierzy w fałszywe oskarżenia, przestępcy żądają od niej zapłacenia określonej kwoty, aby uniknąć aresztowania lub innej kary. Należy zauważyć, że podszywanie się pod służby jest przede wszystkim możliwe dzięki rozwijającym się technologiom. Przestępcy potrafią tak manipulować informacjami, że wyglądają one na autentyczne. Wiadomości mogą pochodzić z adresów e-mail, które wydają się być oficjalne lub numerów telefonów, które wyświetlają nazwy instytucji publicznych. Żadna rzeczywista służba ani instytucja nigdy nie wysyłałaby takich informacji drogą elektroniczną. Jeśli otrzymamy podejrzany e-mail lub telefon, zawsze powinniśmy skonsultować się z prawdziwymi służbami, aby sprawdzić autentyczność wiadomości. Służby ścigające nigdy nie będą nas kontaktować drogą elektroniczną w sprawach takich jak popełnienie przestępstwa.

3. KRADZIEŻ DANYCH OSOBOWYCH - phishing

Phishing polega na wykorzystaniu wiadomości elektronicznych, które mają na celu oszustwo i wykradanie poufnych informacji. Oszuści starają się "nabrać" użytkowników internetu, wykorzystując różne techniki manipulacji. Ich głównym celem jest nakłonienie odbiorcy do kliknięcia w podejrzany link lub skorzystania z zainfekowanej strony, która ładząco przypomina autentyczną witrynę, np. banku czy serwisu handlowego.

Najpopularniejszą metodą jest wysyłka fałszywych e-maili, których nadawcy podszywają się pod różne instytucje, takie jak firmy telekomunikacyjne czy banki. Phishing wykorzystuje także inne kanały komunikacji, takie jak wiadomości SMS czy portale społecznościowe. Kiedy użytkownik kliknie w podejrzany link lub poda swoje dane na fałszywej stronie, oszuści uzyskują dostęp do wartościowych informacji. Mogą to być dane do logowania, numery kont bankowych, informacje na temat kart kredytowych czy inne dane osobowe. Posiadając te informacje, przestępcy mogą dokonywać nielegalnych transakcji finansowych lub wykorzystać je w inny sposób.



4. OBIETNICA DUŻEGO ZWROTU Z INWESTYCJI



Coraz częściej słyszy się o oszustwach inwestycyjnych, które są ukierunkowane na starsze osoby. Oferty obiecujące duży zwrot z inwestycji, ale po przekazaniu pieniędzy Senior już nigdy więcej ich nie zobaczy – to przykład typowego oszustwa, które przyprawia starsze osoby o straty finansowe oraz ogromny stres.

Jak więc uchronić się przed tego typu szkodliwymi działaniami? Przede wszystkim należy uświadomić sobie, że należy być czujnym i strzec się obietnic wysokich zysków bez ryzyka. Trzeba pamiętać, że to, co wydaje się zbyt piękne, zwykle nie jest prawdziwe. Kolejnym ważnym aspektem jest unikanie ofert, które wywierają presję na szybkie kupowanie lub zawierają silnie ograniczone czasowo warunki. Oszuści często stosują takie metody manipulacji, aby skłonić starsze osoby do podjęcia pochopnych decyzji i przekazania swoich oszczędności. Dlatego warto pamiętać, że prawdziwe inwestycje wymagają czasu na dokładne zastanowienie się i konsultację z ekspertami. Podsumowując, osoby starsze powinny być szczególnie ostrożne w zakresie inwestycji, zwłaszcza gdy obiecują one szybki i łatwy zysk.

5. FAŁSZYWA POMOC TECHNICZNA

Oszuści podszywają się pod legalne firmy i kontaktują się telefonicznie lub za pomocą wiadomości udając, że mają pełnomocnictwo do udzielania wsparcia technicznego. Najczęściej wymyślają nieistniejący problem na naszym komputerze i przekonują nas, że musimy podjąć konkretne kroki, które ich zdaniem naprawią problem.

Niestety, te "kroki" są ukierunkowane na uzyskanie zdalnego dostępu do naszego komputera lub na wykradzenie naszych danych osobowych i finansowych. Jeśli uwierzymy w tę mistyfikację, możemy paść ofiarą kradzieży tożsamości, utraty oszczędności, a nawet szantażu.

6. OSZUSTWA DOTYCZĄCE LEKARSTW

Oszustwa dotyczące produktów leczniczych to poważny problem, który dotyka przede wszystkim starsze osoby. Jego skutki mogą być katastrofalne dla zdrowia i życia. Seniorzy powinni być świadomi, że nielegalne praktyki handlowe na rynku produktów leczniczych stają się coraz bardziej powszechne. Oszuści wykorzystują zaufanie i nieświadomość swoich ofiar, które często są właśnie w starszym wieku. Musimy być ostrożni, zawsze sprawdzać źródło i autentyczność oferowanych produktów.



7. OSZUSTWO "NA WNUCZKA"

Oszustwo na wnuczka/członka rodziny to jedno z najbardziej groźnych i powszechnych oszustw, które mają miejsce obecnie. Jego celem jest wyłudzenie informacji lub pieniędzy od starszych osób poprzez podszywanie się pod ich krewnego, najczęściej wnuka. Ten rodzaj przestępstwa może mieć miejsce zarówno poprzez telefon, jak i przez internet. Przestępcy działają w sposób bardzo przemyślany. Tworzą na przykład duplikat konta wnuczka na mediach społecznościowych i kontaktują się z dziadkiem czy babcią, prosząc o pomoc. Opowiadają historię o kłopotach, jakie ich spotkały (na przykład zostali okradzeni na zagranicznych wakacjach) i potrzebują pilnie pieniędzy, aby wyjść z powstałej sytuacji. Podkreślają, że jest to pilne oraz że nie chcą się zwracać do swoich rodziców ze wstydu.

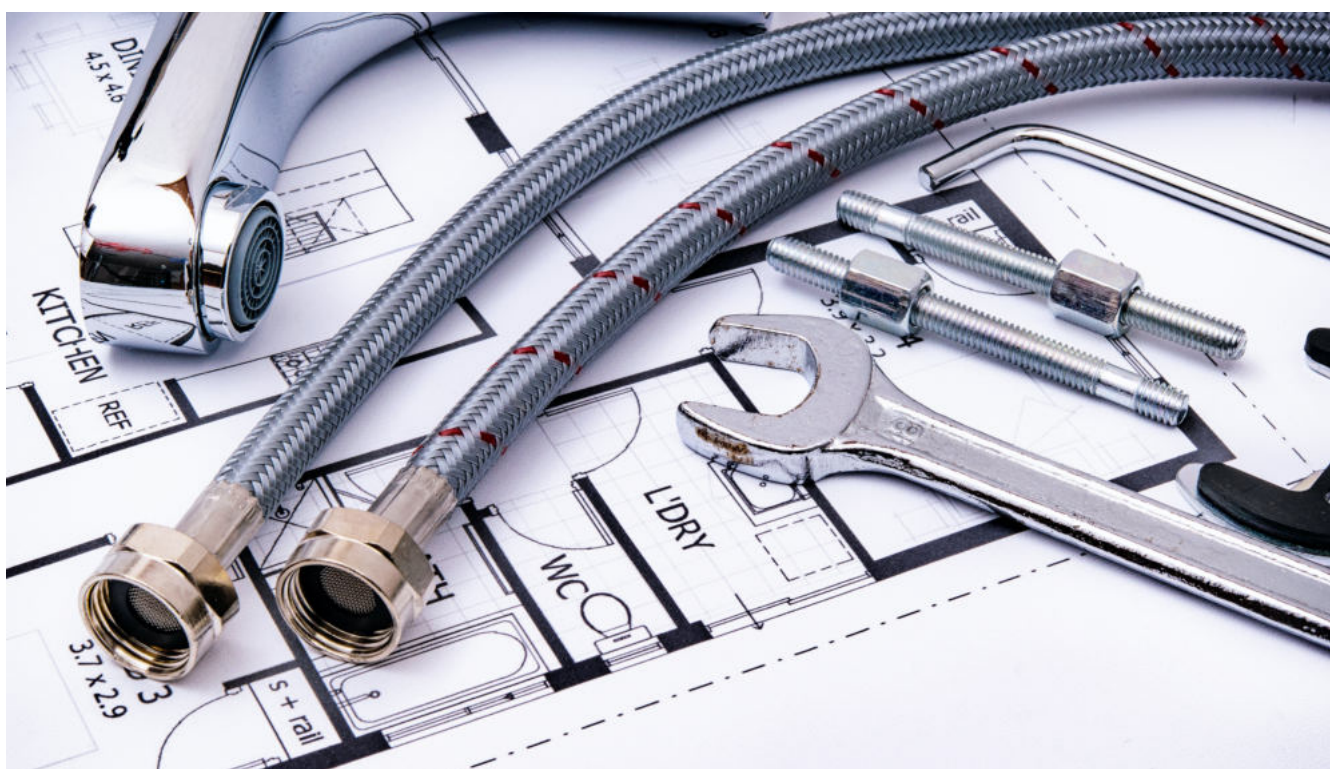
To jedna z perfidnych metod oszustw seniorów, ponieważ bazuje na strachu o bezpieczeństwo bliskich. Przestępca dzwoni i podaje się za członka rodziny, najczęściej wnuczka, który spowodował wypadek i potrzebuje natychmiastowego wsparcia finansowego na opłacenie kosztów "oczyszczenia z zarzutów". Innym scenariuszem jest udawanie osoby ciężko chorej i zdesperowanej. Oszust stara się wzbudzić współczucie, opowiadając przekonująco o chorobie, własnej lub kogoś z rodziny, i prosi o pieniądze na leczenie.

Jak jednak nie paść ofiarą tych oszustw? To proste - zadzwoń do rzekomej osoby bliskiej, która znajduje się w kłopotliwej sytuacji i potrzebuje wsparcia finansowego. Krótka rozmowa może uchronić cię przed utratą zgromadzonych oszczędności życia.

8. OSZUSTWA REMONTOWE

Oszuści działający w branży remontowej mają wiele sposobów na wyłudzenie pieniędzy. Jednym z nich jest prośba o przesłanie zaliczki w celu zarezerwowania terminu. Niestety, po otrzymaniu pieniędzy kontakt często zostaje całkowicie zerwany. Inni oszuści nawet udają się do domu ofiary, wyłudzając większe kwoty pieniędzy, aby po pewnym czasie zniknąć bez śladu.

Jak więc skutecznie uchronić się przed tego typu przekrętami? Przede wszystkim zawsze warto robić dokładne badania dotyczące wybranej firmy. Sprawdzanie opinii innych klientów, wyszukiwanie informacji na temat firmy w internecie oraz kontaktowanie się z jej dotychczasowymi klientami mogą dostarczyć wielu cennych wskazówek i wiedzy na temat rzetelności danej firmy. Warto także zasięgnąć opinii osób, które korzystały z usług remontowych w przeszłości, gdyż mogą mieć cenne doświadczenia i wskazać na godne zaufania firmy.



9. FAŁSZYWE ZBIÓRKI CHARYTATYWNE

W dzisiejszych czasach, kiedy coraz więcej osób potrzebuje pomocy charytatywnej, niestety pojawia się także coraz więcej oszustów, którzy wykorzystują dobre intencje ludzi w celach własnego zysku. Szczególnie narażone na tego typu działania są osoby starsze, które często są bardziej ufne i chętnie angażują się w pomoc potrzebującym.

Podstawową zasadą jest zdrowa rezerwa i ostrożność. Osoby starsze powinny zdawać sobie sprawę, że oszuści coraz częściej podszywają się pod zaufane organizacje charytatywne. W ten sposób przekonują swoje ofiary, że są godnymi zaufania, aby przekazały im swoje darowizny. Niestety zdarza się, że te pieniądze nie trafiają tam, gdzie powinny, lecz prosto do kieszeni oszustów.

10. FAŁSZYWY SKLEP INTERNETOWY/BANK

Jednym z ich najskuteczniejszych narzędzi wykorzystywanym przez oszustów są fałszywe witryny internetowe, które wyglądają jak oryginalne strony logowania do banków, sklepów internetowych czy portali społecznościowych. Sprawdźmy, jak można je rozpoznać i uniknąć nieprzyjemnych niespodzianek. Największą wskazówką, że mamy do czynienia z próbą wyłudzenia, jest drobna różnica w zapisie adresu www. Oszuści często dodają myślniki, kropki lub zmieniają pojedyncze litery w adresie, aby wprowadzić nas w błąd. Warto zwrócić na to uwagę i dokładnie sprawdzić adres, zanim podamy jakiegokolwiek dane osobowe czy bankowe.

Oszuści wiedzą też, że niskie ceny przyciągają klientów, dlatego często oferują produkty po znacznie niższych cenach niż konkurencja. Niestety, po dokonaniu płatności okazuje się, że kontakt z sprzedawcą urywa się, a otrzymany produkt jest podróbką lub niskiej jakości.

11. OSZUSTWA RANDKOWE

W dobie rozwoju technologii i coraz bardziej powszechnego korzystania z internetu, coraz więcej osób szuka miłości i przyjaźni online. Niestety, wraz z tym także rośnie liczba oszustw randkowych, które mają na celu wyłudzenie pieniędzy. Fałszywe profile w mediach społecznościowych czy na portalach randkowych stają się coraz bardziej wyrafinowane, przez co trudno jest odróżnić prawdziwe osoby od oszustów.

Oszustwa randkowe są szczególnie podstępne, gdy fałszywy randkowiec zdobędzie zaufanie lub nawet miłość ofiary. Wtedy zaczyna prosić o poufne informacje lub o pomoc finansową, np. na pokrycie kosztów podróży lub leczenia. Sytuacja wydaje się tak realna, że wiele osób daje się nabrać na tę manipulację.





The best free stock photos & videos shared by talented creators.

Search for free photos and videos

Suggest: research, beauty, computer, wine, island, early, more

Home Discover Videos Leaderboard Challenges

Stack of books and magazines, including one titled "2018".



FUNDACJA "IDEA DLA CIEBIE"

Ignaców 14a

63-507 Kobyla Góra

www.ideadlaciebie.org