#Halo!

Tu cyberbezpieczny Senior

Poradnik
dla seniorów
2024

CBZC

NASK

WIB WARSZAWSKI INSTYTUT BANKOWOŚCI

Projekt finansowany ze środków
Ministra Cyfryzacji

Redakcja:
Beata Frankiewicz

Autorki:
Beata Frankiewicz
Katarzyna Grabowska
Katarzyna Koletyńska
Anna Kwaśnik

Opieka merytoryczna:
Zuzanna Polak
dr Agnieszka Wrońska

Redakcja językowa, korekta:
Katarzyna Nakonieczna

Opracowanie graficzne i skład:
Beata Frankiewicz

Państwowy Instytut Badawczy NASK

Warszawa 2024

ISBN: 978-83-65448-94-1

Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

#Halo!

Tu cyberbezpieczny Senior

SPIS TREŚCI

Wprowadzenie

Pamiętasz czasy, kiedy wszystko trzeba było załatwiać osobiście? Kolejki na poczcie, wycieczki do banku, a żeby porozmawiać z kimś z daleka, trzeba było zamawiać międzymiastową lub napisać list i cierpliwie czekać na odpowiedź. Ach, to były inne czasy! A teraz?

Teraz wystarczy jedno kliknięcie i możesz zrobić zakupy, umówić wizytę u lekarza, załatwić sprawy urzędowe bez wychodzenia z domu, porozmawiać z wnukami przez wideorozmowę a nawet... znaleźć swoją drugą połówkę! Tak, dobrze czytasz – internet otwiera drzwi do całego świata!

Ale – jak to w życiu bywa – w tej beczce miodu jest też łyżka dziegciu. W cyfrowym świecie podobnie jak w rzeczywistym, można natknąć się na nieuczciwych ludzi i różne zagrożenia.

Dlatego warto znać zasady, które pomogą Ci bezpiecznie poruszać się po tej cyfrowej autostradzie. W Poradniku opowiemy jak chronić swoje dane, nie dać się oszukać i o czym warto pamiętać, by korzystać z nowych technologii w pełni bezpiecznie.

Gotowy na podróż po świecie cyber, czyli świecie nowych technologii i internetu? Zaczynamy!

Cyberoszustwa, czyli co?

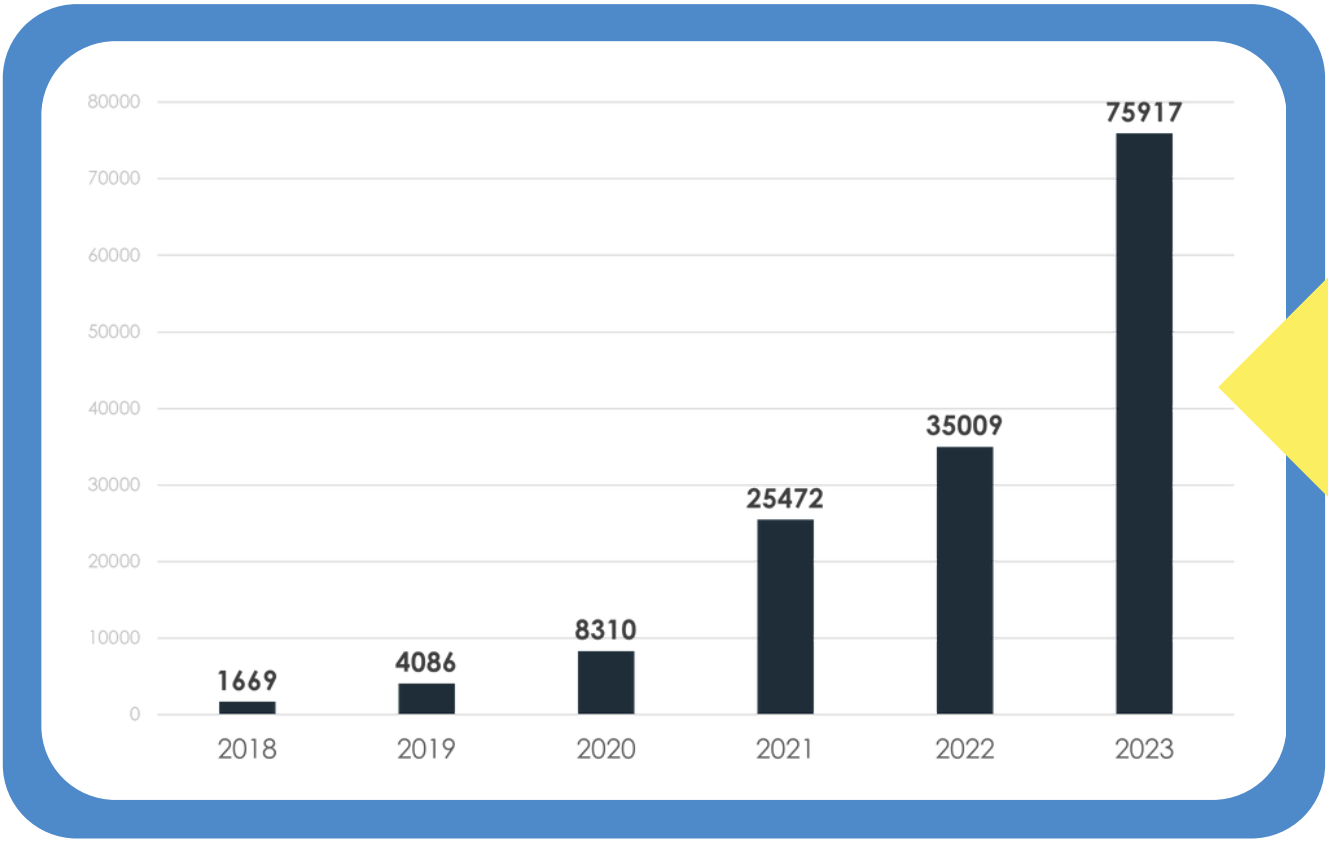
Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- jaka jest skala oszust komputerowych w Polsce,
- jak działają cyberoszuści,
- czym jest socjotechnika,
- jakie są podstawowe elementy socjotechniki.

Skala oszustw

Z roku na rok rośnie liczba przestępstw związanych z nielegalną działalnością w internecie. Dotyka to coraz większej liczby osób, w tym także seniorów.

W 2023 roku w porównaniu do 2022 roku liczba oszustw komputerowych wzrosła dwukrotnie. Jest to wzrost z 35 tysięcy do 75 tysięcy przypadków. Poniższy wykres ilustruje tę zmianę.



Źródło: Raporty roczne z działalności CERT POLSKA

Cyberprzestępcy, czyli osoby, które wykorzystują internet i nowe technologie do oszukiwania oraz zdobywania poufnych informacji, mogą uzyskać dostęp do kont bankowych i wykradać z nich pieniądze. Takie działania są nielegalne i mogą prowadzić do poważnych konsekwencji.

Jak działają cyberprzestępcy?

Kradzież pieniędzy i danych wrażliwych,
to przestępstwa,
które istnieją od lat i wciąż
stanowią poważne zagrożenie.

Przestępcy mogą wykorzystać Twoje dane m.in. do kradzieży tożsamości, uzyskania dostępu do kont bankowych, oszustw finansowych, a także do zakładania fałszywych profili, które mogą posłużyć do popełnienia kolejnych przestępstw.

Cyberprzestępcy mogą próbować nakłonić Cię do:

- **wykonania** przelewu,
- **przekazania** poufnych danych i informacji, np. kodów autoryzacyjnych, danych do logowania, haseł,
- **zainstalowania** oprogramowania umożliwiającego przejęcie kontroli nad Twoim urządzeniem.

Mogą wykorzystywać różne formy kontaktu m.in.:

wiadomości e-mail

połączenia telefoniczne

wiadomości SMS

Czym jest socjotechnika?

Socjotechnika
to każde działanie wpływające na inną osobę,
które ma na celu nakłonić ją do postępowania
niezgodnego z jej osobistym interesem

Christopher Hadnagy

Przestępstwa popełniane z wykorzystaniem socjotechniki nie wymagają zaawansowanej wiedzy technicznej ponieważ opierają się głównie na manipulacji i podstępie.

Cyberprzestępcy mogą atakować setki osób, wysyłając e-maile, SMS-y lub kontaktując się bezpośrednio.
Nawet jeśli tylko niewielki procent osób da się oszukać, zyski dla przestępców mogą być ogromne.

Bądź czujny, przestępcy nieustannie modyfikują scenariusze swoich działań!

Zachowaj rozwagę:

- **w każdej sytuacji, która dotyczy Twoich pieniędzy** m.in. nieoczekiwany przelew, dopłata do faktury lub przesyłki kurierskiej,
- **gdy ktoś wymaga podania przez Ciebie danych wrażliwych** (np. PESEL, data urodzenia, numery kart płatniczych itp.),
- **jeśli ktoś wymusza zalogowanie się na Twoje konto** (np. bankowe, poczty elektronicznej, w mediach społecznościowych).

Podstawowe elementy socjotechniki

Zdobywanie zaufania

Oszuści podszywają się pod instytucje publiczne, zawody zaufania społecznego (np. policjant, lekarz), członków rodziny lub znajomych. Działają tak, aby uwiarygodnić swoją historię i zdobyć Twoje zaufanie.

Manipulowanie emocjami

Najczęściej wykorzystują sytuację, gdy ich ofiara działa pod wpływem emocji. Zazwyczaj jest to poczucie zagrożenia o życie i zdrowie bliskich, obawy o utratę oszczędności. Jednak może to także być euforia czy radość np. z powodu rzekomej wygranej. Oszuści starają się wywołać silne emocje, by ograniczyć Twoje racjonalne myślenie.

Wywieranie presji czasowej

Przestępcy zmuszają do natychmiastowego działania, często używają słów takich jak „natychmiast”, „teraz”, „zaraz”. Grożą konsekwencjami, takimi jak utrata oszczędności lub możliwości pomocy bliskim. Presja ta ma na celu skłonienie do podjęcia pochopnych decyzji i uniemożliwienie konsultacji z bliskimi.

Oszustwa telefoniczne

NASK

Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- jaka jest skala problemu dotyczącego oszust telefonicznych,
- jakie są najpopularniejsze scenariusze oszustw,
- o czym należy pamiętać odbierając telefon.

Skala problemu

Nieoczekiwany telefon z banku lub policji?
Zachowaj czujność,
to może być oszustwo!

Każdego dnia wykonujemy i odbieramy wiele połączeń telefonicznych, dlatego warto zwracać uwagę na to, kto i w jaki sposób się z nami kontaktuje.

Niewykluczone, że rozmówca może próbować Cię zmanipulować lub oszukać. Oszuści są mistrzami w tworzeniu fikcyjnych historyjek, które brzmią bardzo wiarygodnie. Taka sytuacja może zdarzyć się każdemu, niezależnie od wieku.

- **Wartość strat finansowych** poniesionych w 2022 roku na skutek przestępstw telefonicznych (m.in. metoda „na wnuczka" i „na urzędnika") **to ponad 141 milionów zł**.
- Wśród ofiar tego typu oszustw **aż 3,5 tysiąca to osoby w wieku 65+***
- *Dane statystyczne z Krajowego Systemu Informacyjnego Policji (KSIP)

Pamiętaj, aby zawsze weryfikować tożsamość osoby, która się z Tobą kontaktuje.
Zakończ połączenie
i zadzwoń na znany numer
instytucji lub osoby, na którą
powołuje się rozmówca.

Policja, prokuratura, pracownicy, służb medycznych lub innych instytucji **nigdy** nie proszą o przekazanie pieniędzy!

Najpopularniejsze scenariusze oszustw

Na policjanta, prokuratora lub pracownika innej profesji o dużym zaufaniu publicznym.

Oszust podający się za policjanta może m.in. twierdzić, że prowadzi tajną akcję i prosi Cię o przekazanie pieniędzy, aby złapać przestępców na gorącym uczynku.

Na pracownika banku lub pomoc techniczną.

Oszust informuje o podejrzanych transakcjach na Twoim koncie i sugeruje, byś natychmiast utworzył „konto techniczne” i przelał na nie oszczędności, inaczej możesz stracić swoje pieniądze.

Na wypadek spowodowany przez bliską nam osobę.

Przestępcy informują Cię, że ktoś z Twoich bliskich, na przykład córka, syn lub wnuk, spowodował wypadek i pilnie potrzebuje pieniędzy na adwokata, kaucję lub zadośćuczynienie poszkodowanym.

Najpopularniejsze scenariusze oszustw

Na wnuczka lub innego członka rodziny.

Oszust może podszywać się pod wnuczka lub kogoś z rodziny, prosząc o szybkie wsparcie finansowe, na przykład na zgubiony telefon, wkład własny do kredytu mieszkaniowego lub inną atrakcyjną ofertę zakupu.

Na pracownika urzędu skarbowego lub ZUS-u.

Oszust twierdzi, że wystąpiły problemy z rozliczeniem składek i grozi wstrzymaniem świadczeń emerytalnych. Prosi o uregulowanie zaległości, aby uniknąć przerwy w ich wypłacie.

„Na każdą osobę" wzbudzającą zaufanie i przedstawiającą wiarygodną historię.

Scenariusze oszustów są nieustannie zmieniane i urozmaicane. Wykorzystują każdą sytuację, by wzbudzić zaufanie i wyłudzić pieniądze.

O czym należy pamiętać odbierając telefon?

Nie sugeruj się nazwą widoczną na ekranie telefonu,
np. banku, ZUS-u, policji
– przestępcy mogą sfałszować te informacje.

W każdej niecodziennej sytuacji zachowaj czujność i zdrowy rozsądek.

Co zrobić, gdy odbierzesz niepokojący telefon?

- **Nie podejmuj żadnych pochopnych decyzji** ani nie działaj pod presją czasu.
- Nie angażuj się w rozmowę, jeśli nie masz pewności, kto jest po drugiej stronie. **Zakończ połączenie i zweryfikuj rozmówcę** dzwoniąc na znany numer instytucji lub udając się do placówki.
- **Nigdy nie podawaj nikomu wrażliwych danych,** takich jak: PESEL, hasła logowania czy kody autoryzacyjne.
- **Nie pobieraj ani nie instaluj aplikacji lub oprogramowania** za czyjąś namową – może to umożliwić nieautoryzowany, zdalny dostęp do Twojego urządzenia.
- **Poinformuj bliskich!** Jeśli otrzymasz nietypowy telefon, skontaktuj się z zaufaną osobą, by pomogła Ci ocenić sytuację i podjąć właściwą decyzję.

Fałszywe wiadomości e-mail oraz SMS

NASK

Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- czym są fałszywe wiadomości,
- jakie są najpopularniejsze tematy fałszywych wiadomości,
- jak rozpoznać fałszywe wiadomości e-mail,
- jak rozpoznać fałszywe linki,
- co zrobić, gdy otrzymasz niepokojącą wiadomość.

Fałszywe wiadomości

Dlaczego fałszywe wiadomości są niebezpieczne?

Przestępcy, pod pretekstem fałszywej wiadomości, **próbują nakłonić Cię do kliknięcia w załączony link, który prowadzi do fałszywej strony** łudząco podobnej do oficjalnej. Może to być na przykład strona banku lub strona służąca do płacenia za zakupy.

Dane, które wprowadzasz na fałszywej stronie, trafiają do oszustów zamiast do zaufanej instytucji. W ten sposób cyberprzestępcy mogą przejąć kontrolę nad Twoim kontem lub wykorzystać Twoje dane do popełnienia innych przestępstw.

Wiadomości e-mail mogą zawierać także załączniki, w których oszuści ukrywają złośliwe oprogramowanie. Jeśli otworzysz taki załącznik, na Twoim komputerze może zostać zainstalowane złośliwe oprogramowanie, które będzie na przykład wykradać dane.

Fałszywe wiadomości

Fałszywe wiadomości dotyczą nie tylko e-maili, ale także SMS-ów lub wiadomości w aplikacjach, takich jak Messenger czy WhatsApp.

Najpopularniejsze tematy fałszywych wiadomości

Nieopłacona faktura np. za prąd, gaz i groźba odłączenia w przypadku braku płatności.

Problemy z kontem bankowym np. informacje o zablokowanym koncie lub podejrzanych aktywnościach na koncie.

Wygrane na loterii, zniżki i kupony do popularnych sklepów.

Problemy z wypłaceniem świadczeń np. emerytalnych.

Konieczność dopłacenia do przesyłki kurierskiej np. z powodu niewłaściwej wagi lub opłaty celnej.

Jak rozpoznać fałszywe wiadomości e-mail?

Umiejętność oceny, czy wiadomość jest prawdziwa pomoże Ci uniknąć ryzyka związanego z przypadkowym otwarciem niebezpiecznych załączników lub kliknięciem w podejrzane linki. Zobacz, na co zwracać uwagę.

Od: Jan Kowalski/ Specjalista ds. zabezpieczeń TWÓJ BANK <user234@email-campaign.de> 1

Do: Zofia Kowalska <kowalska.zofia@poczta.pl>

Data: 12.03.2024, 11:13

Temat: Nieautoryzowane logowanie na koncie bankowym

Drogi Kliencie,

Twoje konto wlasnie sie zalogowalo z nowego urzadzenia posiadającego zagraniczny numeru IP. Otrzymujesz te wiadomość e-mail, aby upewnić sie, ze to Ty. 2

Zaloguj się i sprawdź ostatnie logowanie 3

BANK

Dziekuje Ci,
Twoj Bank 4

Załaczniki:

Rejestr ostatnich transakcji.rar 5

https://twojbank.pl.hosting537.xyz.com/login-#5&15

Jak rozpoznać fałszywe wiadomości e-mail?

Fałszywe e-maile mogą zawierać błędy ortograficzne i stylistyczne. Jednak nie jest to regułą.

Nawet poprawny e-mail może być fałszywy, dlatego zawsze sprawdzaj poniższe elementy.

1. **Pełen adres nadawcy.** Widoczny adres to zazwyczaj nazwisko lub nazwa firmy, np. „Jan Kowalski” lub „Twój Bank”. Oszuści mogą ustawić dowolną nazwę w polu „Od”. Dlatego należy sprawdzić pełen adres e-mail i upewnić się, że część po znaku „@” nawiązuje do oficjalnej strony instytucji. Aby zobaczyć pełen adres, wystarczy, że klikniesz na pole nadawcy.

2. **Ton korespondencji.** Jeśli jest to nieoczekiwana wiadomość, która próbuje wzbudzić silne emocje np. strach przed utratą środków na koncie i zachęca do podjęcia szybkich działań (np. kliknięcia w link, pobrania załącznika lub zalogowania się na konto), zachowaj czujność, to może być próba oszustwa.

3. **Linki.** Mogą prowadzić do stron, które wyglądają niemal identycznie jak oryginalne. Oszuści wykorzystują to, aby wyłudzić Twoje dane. Jak sprawdzić, czy to prawdziwa strona? Najedź myszką na link (nie klikaj), a pełen adres pojawi się w dolnej części ekranu. Porównaj go z oficjalnym adresem strony.

4. **Szata graficzna.** Oszuści często kopiują wygląd prawdziwej korespondencji. Nie sugeruj się obecnością znanych logotypów, które mogą być użyte bezprawnie.

5. **Nieoczekiwany załącznik.** Oszuści często nadają załącznikowi nazwę, która ma skłonić Cię do jego otwarcia. Taki załącznik może zawierać szkodliwe oprogramowanie, które zainfekuje Twoje urządzenie.

Jak rozpoznać fałszywe linki?

Oszuści stosują coraz bardziej wyrafinowane metody, aby nakłonić Cię do kliknięcia w linki, które na pierwszy rzut oka mogą wydawać się zupełnie nieszkodliwe.

Gdzie możesz natrafić na podejrzane linki?

- w korespondencji e-mail,
- w wiadomościach SMS,
- we wpisach na portalach społecznościowych,
- w wiadomościach prywatnych wysłanych z przejętych kont.

Zachowaj szczególną ostrożność gdy:

otrzymasz nieoczekiwaną wiadomość wraz z linkiem, w której nadawca naciska na szybkie działanie m.in. wykonanie przelewu, podanie danych konta, zalogowanie się na portalu społecznościowym czy pobranie aplikacji,

nadawca prosi o podanie danych osobowych, haseł numerów kart płatniczych lub innych poufnych informacji,

otrzymasz wiadomość z instytucji, z którą nie byłeś związany np. od banku, w którym nigdy nie miałeś konta.

Jak rozpoznać fałszywe linki?

Zweryfikuj nazwę

Linki, które otrzymasz w korespondencji mogą wyglądać na prawdziwe, ale zawierają drobne zmiany, np. literówki lub dodatkowe znaki.

Na przykład gdy chcesz wejść na stronę **twojbank.pl**, oszuści mogą zmienić szczegół w adresie i przekierować Cię na fałszywą stronę, np. **twoj-bank.pl** lub **bank-logowanie.com**.

Oszuści mogą również używać bardzo długich nazw, aby Cię zmylić i ukryć fakt, że to zupełnie inna strona, mimo że ma taki sam początek.

Poniżej przykład jak może wyglądać próba oszustwa:

Pełen adres strony to cały ciąg znaków,
który znajduje się pomiędzy
“//” a pierwszym kolejnym “/”.

W tym przypadku jest to fałszywa strona.

Fałszywe wiadomości SMS

Zachowaj ostrożność, jeśli otrzymasz niespodziewaną wiadomość wraz z linkiem od nieznanego numeru lub firmy.

Uważaj na skrócone linki

Skrócone linki nie pokazują pełnego adresu strony. Szczególnie w wiadomościach SMS oszuści z premedytacją wykorzystują takie linki, aby przekierować Cię na fałszywe strony.

Poniżej kilka przykładów.

Co zrobić, gdy otrzymasz niepokojącą wiadomość?

Gdy otrzymasz nieoczekiwaną wiadomość, w której nadawca wywiera presję do podjęcia natychmiastowych działań, najważniejsze jest zachowanie spokoju.

Oto wskazówki, które pomogą Ci bezpiecznie i świadomie zareagować na podejrzane wiadomości.

- **Nie działaj pochopnie** i nie podejmuj decyzji pod wpływem emocji i presji czasu.
- **Zweryfikuj nadawcę,** zadzwoń na znany Ci numer instytucji, od której rzekomo przyszła wiadomość lub odwiedź jej oddział, aby potwierdzić otrzymane informacje.
- **Nie udostępniaj swoich danych** takich jak np. PESEL, data urodzenia, numery kart płatniczych, loginy i hasła do kont.
- **Nie loguj się do banku lub na inne konta** za pośrednictwem linku otrzymanego w wiadomości e-mail lub SMS.
- **Nie klikaj w linki i załączniki,** które otrzymasz w wiadomości, jeśli nie wiesz od kogo pochodzą i co się w nich znajduje.

Ważne! Samo kliknięcie w podejrzany link zazwyczaj nie jest groźne – szkody pojawiają się dopiero po podjęciu działań na fałszywej stronie.

Co zrobić, gdy otrzymasz niepokojącą wiadomość?

- **Zwracaj uwagę na wszelkie nieścisłości w komunikatach,** które wydają się podejrzane m.in. błędy językowe, nietypowe prośby.
- **Nie pobieraj i nie instaluj oprogramowania lub aplikacji,** o których mowa w wiadomości – mogą być one niebezpieczne i zainfekować Twój sprzęt.
- **Gdy otrzymasz niepokojącą wiadomość** – przekaż ją do zespołu **CERT Polska**, który ją zweryfikuje, a następnie zablokuje fałszywą stronę. W ten sposób pomagasz sobie i innym.

Deepfake i fałszywe inwestycje

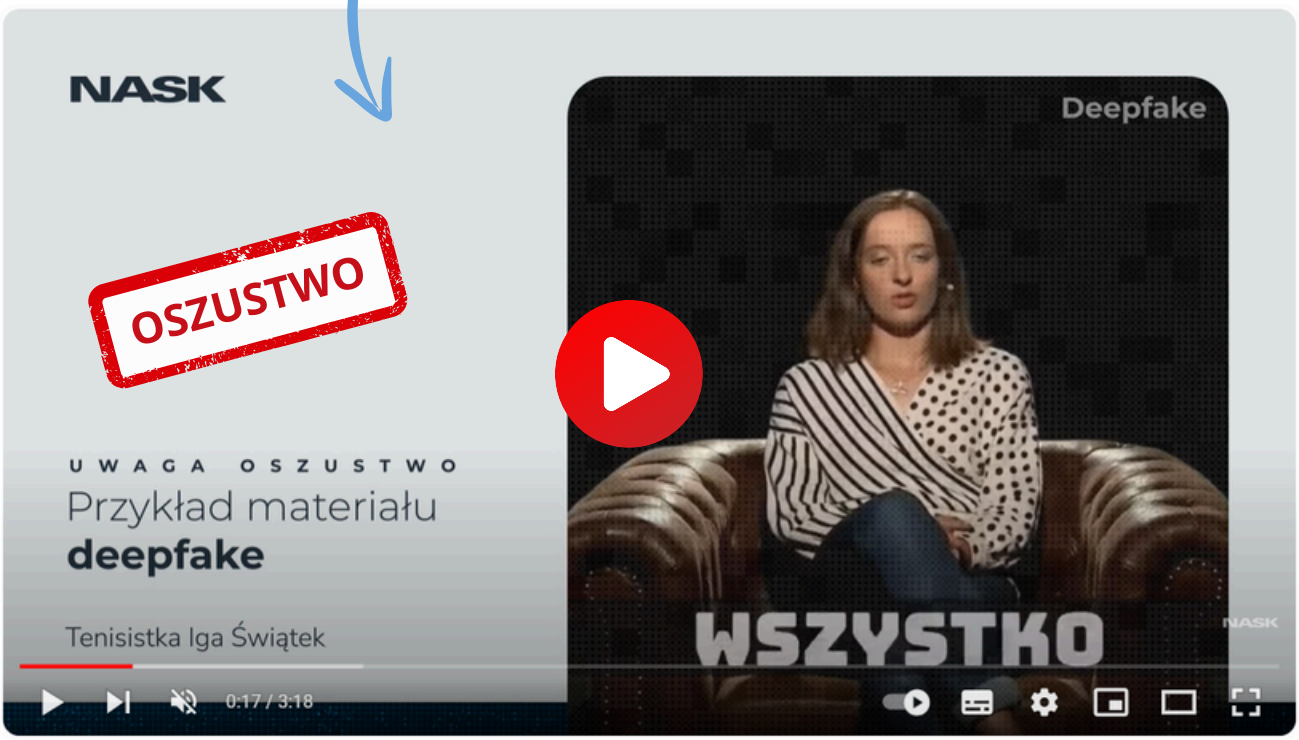
Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- czym jest deepfake,
- czym są oszustwa inwestycyjne,
- jak rozpoznać fałszywą inwestycję.

Deepfake

Deepfake to technologia, która wykorzystuje sztuczną inteligencję do tworzenia niezwykle realistycznych, ale nieprawdziwych obrazów, filmów i nagrań dźwiękowych.

Cyberprzestępcy coraz częściej używają deepfake i wizerunków znanych osób, takich jak: Andrzej Duda, Iga Świątek czy Robert Lewandowski, by wzbudzić zaufanie i nakłonić do fałszywych inwestycji.



Więcej przykładów deepfake znajdziesz na kanale YouTube NASK

Czym są oszustwa inwestycyjne?

Oszustwa inwestycyjne to działania i praktyki mające na celu wyłudzenie pieniędzy, zwłaszcza od niedoświadczonych na rynku inwestycyjnym użytkowników internetu.

Przestępcy przy użyciu metod socjotechnicznych starają się nakłonić do inwestowania np. w kryptowaluty, nieruchomości, surowce, akcje, udziały, papiery wartościowe.

Zachęta do takich inwestycji jest opatrzona wiarygodną historyjką i przedstawiana jako bezpieczna lokata, która gwarantuje wysokie zyski.
Wystarczy uzupełnić formularz, wpłacić pieniądze na wskazaną platformę lub fundusz inwestycyjny.

Pamiętaj!
Każde działanie dotyczące inwestowania wiąże się z ryzykiem.

Zanim podejmiesz jakąkolwiek decyzję, zawsze sprawdź, komu powierzasz swoje pieniądze!

Jak rozpoznać fałszywą inwestycję?

Przed podjęciem decyzji dotyczącej inwestycji, zweryfikuj bardzo dokładnie:

Wiarygodność profilu, na którym znajduje się reklama. Poniżej przykład fałszywej reklamy wraz z wyjaśnieniem, na co zwracać uwagę.

Zwróć uwagę, czy nazwa profilu nawiązuje do nazwy instytucji lub marki, którą reklamuje. W tym przypadku, mimo że profil powołuje się na autorytet rządu, jego nazwa nie jest powiązana z oficjalnym kontem rządu.

Klikając nazwę profilu, możesz sprawdzić jego historię, wcześniejsze publikacje, komentarze oraz opinie.

Gwarancja nieproporcjonalnego zysku względem inwestycji powinna budzić podejrzenia i stanowić sygnał ostrzegawczy.

Autentyczność strony, na którą nastąpiło przekierowanie. Zwróć uwagę na prawidłowy adres strony, nie sugeruj się tym, że są na niej znane logotypy – mogą być użyte bezprawnie.

Jak rozpoznać fałszywą inwestycję?

Przed podjęciem decyzji dotyczącej inwestycji, zweryfikuj bardzo dokładnie:

- **Dane rejestrowe firmy**, która ma pośredniczyć w inwestycjach. Czy na stronie są dostępne takie dane jak: adres firmy, NIP oraz dane kontaktowe tj. mail, telefon?

Ta ikona oznacza link. Kliknij, aby przejść do wskazanej strony.

- **Historię firmy.** Posiadając numer NIP możesz zweryfikować historię firmy w **Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEDIG)** lub w **Krajowym Rejestrze Sądowym (KRS)**.
- **Rejestr autoryzowanych doradców inwestycyjnych** prowadzony przez Komisję Nadzoru Finansowego. Upewnij się, że osoba, z którą rozmawiasz o inwestycjach, jest wpisana do tego rejestru. To daje pewność, że ma odpowiednie kwalifikacje i uprawnienia do udzielania porad inwestycyjnych w Polsce.
- **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.

Jeśli podejrzewasz, że padłeś ofiarą oszustwa inwestycyjnego, zbierz wszystkie dane kontaktowe oszustów (czas zdarzenia, numery telefonów, e-maile, numery rachunków, dane odbiorców, adresy portfeli kryptowalutowych) i jak najszybciej zawiadom policję lub prokuraturę oraz swój bank.

Fałszywe sklepy internetowe

Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- w jaki sposób sprawdzać sklepy internetowe,
- co zrobić, gdy dokonałeś zakupu w fałszywym sklepie.

Zanim kupisz, sprawdź!

Łatwo można wpaść w sidła cyberprzestępców, trafiając na fałszywe sklepy lub oferty kupna. Oszuści tworzą strony internetowe, które przypominają autentyczne sklepy znanych marek i oferują produkty w atrakcyjnych cenach.

Fałszywe sklepy internetowe – jak się chronić?

Zweryfikuj adres sklepu internetowego

Jeśli adres zawiera błędy, literówki lub odbiega od oficjalnej nazwy sklepu, to bardzo wyraźny sygnał ostrzegawczy.

Sprawdź dane kontaktowe i numer NIP

Brak danych kontaktowych sklepu takich jak: adres e-mail, numer telefonu, adres firmy oraz NIP może sugerować oszustwo. Gdy NIP jest widoczny, na jego podstawie sprawdź historię sprzedawcę w rejestrach takich jak: KRS lub CEIDG.

Zapoznaj się z treścią regulaminu zakupów

Zwróć uwagę, czy w regulaminie są zawarte informacje dotyczące sposobów wysyłki oraz zwrotu towaru.

Zanim kupisz, sprawdź!

Sprawdź dostępne metody płatności

W fałszywych sklepach bardzo rzadko można zapłacić za pomocą popularnych metod takich jak np. BLIK. Najczęściej nie ma także możliwości płatności przy odbiorze towaru. Podczas płatności sprawdź, czy na pewno strona, do której odsyła sklep, to prawdziwa strona Twojego banku lub serwisu płatniczego.

Przeczytaj opinie i komentarze o sklepie

Zwróć uwagę, czy wszystkie opinie nie powstały w tym samym okresie i czy na pewno dotyczą wskazanego sklepu.

Co zrobić, gdy zorientujesz się, że zrobiłeś zakupy w fałszywym sklepie?

- Bezzwłocznie **skontaktuj się ze swoim bankiem** i poinformuj o zaistniałej sytuacji.
- **Zgłoś przestępstwo w najbliższym komisariacie policji.** Im szybsza będzie Twoja reakcja, tym większa szansa na odzyskanie pieniędzy.
- Zgłoś incydent na stronie **incydent.cert.pl**. W ten sposób chronisz siebie i innych.

Oszustwa romantyczne

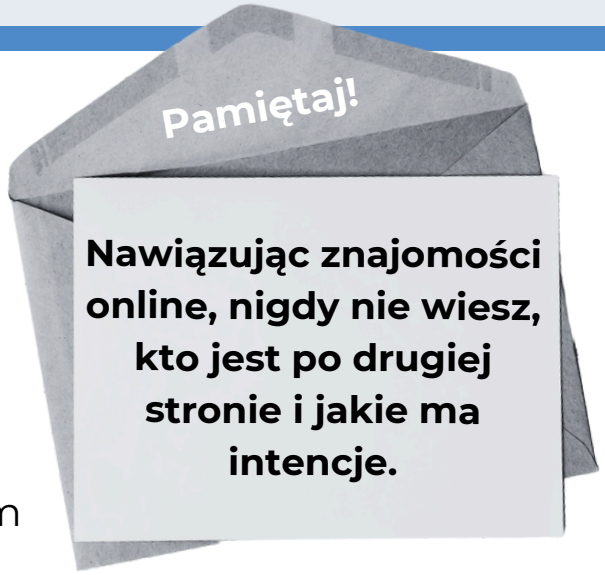
Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- jak wygląda schemat oszustw romantycznych,
- jak chronić swój portfel (i serce).

Oszustwa romantyczne

Niezależnie od wieku, każdy pragnie miłości i bliskości. Często szukamy ich w internecie, na portalach randkowych lub społecznościowych. Jednak również tam musimy zachować ostrożność.

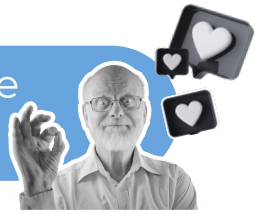
Zawsze kieruj się zdrowym rozsądkiem i zasadą ograniczonego zaufania.



Jak wygląda schemat oszustwa romantycznego?

1. Nawiązanie kontaktu – fałszywy profil lub e-mail

2. Budowanie relacji



3. Prośby o pieniądze

4. Zerwanie kontaktu

Schemat oszustwa

1 Nawiązanie kontaktu - fałszywy profil lub e-mail

Oszust tworzy fikcyjny profil na portalach randkowych, w mediach społecznościowych lub innych platformach, gdzie może spotkać osoby poszukujące „drugiej połówki".

Przykładem może być profil osoby oddanej pracy na rzecz innych, np. „amerykańskiego żołnierza", „lekarki na misji" lub innej osoby wzbudzającej zaufanie i powszechne uznanie.

Może się również zdarzyć, że oszust spróbuje nawiązać kontakt za pomocą wiadomości wysłanej bezpośrednio na Twój adres e-mail. Mógł zdobyć do Ciebie kontakt np. w wyniku wycieku danych w internecie.

2 Budowanie relacji

Oszust regularnie kontaktuje się z ofiarą, angażując ją w długie rozmowy, które mogą trwać nawet wiele miesięcy.

Stosunkowo szybko wyznaje miłość i deklaruje poważne zamiary. Często wykorzystuje techniki psychologiczne, aby wzbudzić sympatię i zaufanie, np. dzieląc się fałszywymi, ale poruszającymi historiami osobistymi.

Schemat oszustwa

3 Prośby o pieniądze

Po zdobyciu zaufania oszust zaczyna prosić o pieniądze, przedstawiając różne scenariusze, takie jak: nagła choroba, wypadek, sytuacja losowa czy problem z opłaceniem biletów, by dotrzeć na spotkanie. Tworząc zmyśloną historię, stara się wzbudzić współczucie i wywrzeć presję, aby ofiara przelała pieniądze. Gdy uda mu się to raz, kontynuuje wyłudzanie, wymyślając kolejne preteksty do przekazywania środków.

Innym przykładem jest oszustwo finansowe, w którym oszust naciska na inwestycje w kryptowaluty lub prosi o pomoc w realizacji przelewów. Fascynacja nową znajomością może prowadzić do utraty pieniędzy i nieświadomego uczestnictwa w praniu brudnych pieniędzy.

4 Zerwanie kontaktu

Gdy oszust uzna, że nie może już nic więcej wyłudzić lub rozmówca zaczyna być podejrzliwy, nagle zrywa kontakt.

Zazwyczaj znika bez śladu, usuwając swoje konta lub blokując kontakt.

Czasami oszust może oskarżać o niewdzięczność albo brak zaufania, potęgując poczucie winy i zagubienia u rozmówcy.

Jak chronić swój portfel (i serce)?

Oszustwa romantyczne to poważny problem, który może prowadzić do bolesnych konsekwencji emocjonalnych i strat finansowych dla ofiar.

Dlatego zawsze należy dokładnie weryfikować osoby poznane przez internet.

Więcej informacji na temat oszustw romantycznych znajdziesz w poradniku.

Kliknij na grafikę, aby pobrać poradnik.

Więcej informacji na stronie: **bezpiecznymiesiac.pl**

Jak się chronić?

Zanim zaufasz, sprawdź!

Poznałeś lub poznałaś kogoś interesującego w sieci? Upewnij się, że wiesz, z kim masz do czynienia.

Zweryfikuj informacje w internecie. Jeśli dana osoba ma profile w mediach społecznościowych zapoznaj się z nimi. Przeanalizuj jej zdjęcia, posty, znajomych oraz czas istnienia konta. **Jeśli nie wiesz jak to zrobić, poproś o pomoc bliską osobę.** Jeśli coś budzi Twoje wątpliwości, rozważ zakończenie znajomości.

Jak chronić swój portfel (i serce)?

Nie udostępniaj osobistych informacji

Nie podawaj osobom poznanym online danych osobowych, takich jak: numer telefonu, adres zamieszkania czy informacje o oszczędnościach.

Nie wysyłaj również swoich zdjęć ani skanów dokumentów, takich jak: dowód osobisty, paszport czy karta płatnicza, ponieważ mogą zostać wykorzystane do kradzieży tożsamości lub innych oszustw.

Chroń swoje finanse

Bądź ostrożny/ostrożna wobec próśb o przekazywanie pieniędzy, nawet jeśli chodzi o niewielkie kwoty.

Oszuści mogą używać różnych wymówek, aby zdobyć zaufanie i uzyskać dostęp do Twoich pieniędzy.

Nie ograniczaj się tylko do kontaktu telefonicznego

Jeśli osoba, z którą się komunikujesz, unika spotkań twarzą w twarz lub nie chce uczestniczyć w wideorozmowie, może to być sygnał ostrzegawczy. Takie zachowanie może wskazywać, że coś ukrywa lub nie jest osobą, za którą się podaje.

Jak chronić swój portfel (i serce)?

Weryfikuj zdjęcia, które otrzymasz online

Korzystaj z narzędzi do wyszukiwania obrazów, aby sprawdzić, czy zdjęcia, które otrzymujesz, nie są skradzione z internetu.

Zwracaj uwagę na szczegóły: mimikę twarzy, załamania światła czy nienaturalne elementy. Takie detale mogą sugerować, że zdjęcie zostało wygenerowane przez sztuczną inteligencję lub zmodyfikowane w programie do edycji zdjęć.

Jeśli nie wiesz, jak to zrobić, poproś o pomoc bliską osobę.

Porozmawiaj z bliskimi

Podziel się informacjami o nowej znajomości z przyjaciółmi lub rodziną.

Czasem druga osoba może dostrzec szczegóły, które Tobie mogły umknąć. Jej perspektywa może pomóc Ci ocenić sytuację bardziej obiektywnie i uniknąć potencjalnych zagrożeń.

Zachowaj czujność

Zwracaj uwagę, czy nie ma sprzeczności w historiach opowiadanych przez osoby poznane w sieci.

Oszuści często używają ogólników i popełniają błędy. Bądź ostrożny, jeśli ktoś szybko zasypuje Cię komplementami lub wyznaje miłość – to częsta technika manipulacji.

Cyberhigiena i ważne porady

Z TEGO ROZDZIAŁU DOWIESZ SIĘ:

- czym jest cyberhigiena,
- jak tworzyć bezpieczne hasła,
- czym jest weryfikacja dwuetapowa,
- na co jeszcze należy zwrócić uwagę – ważne porady.

Cyberhigiena

Twoja codzienna ochrona przed zagrożeniami!

Cyberhigiena to zestaw praktyk i nawyków, które pomagają chronić nasze urządzenia i dane w internecie.

To jak dbanie o higienę osobistą, np. mycie rąk, aby uniknąć chorób. Dzięki cyberhigienie możemy zapobiegać „chorobom" cyfrowym, takim jak: kradzież tożsamości, złośliwe oprogramowanie czy oszustwa internetowe.

- **Ustaw automatyczną blokadę ekranu telefonu, aby korzystanie z urządzenia było możliwe dopiero po jego odblokowaniu.** Większość urządzeń można zabezpieczyć kodem PIN, hasłem, wzorem lub biometrią, to znaczy odciskiem palca lub rozpoznawaniem twarzy.

- **Upewnij się, że Twoje urządzenia mają zainstalowane najnowsze aktualizacje systemu, programów i aplikacji.** Regularne aktualizacje chronią przed lukami w zabezpieczeniach i nowymi zagrożeniami.

- **Instaluj aplikacje wyłącznie z legalnych i zaufanych źródeł,** takich jak oficjalne sklepy z aplikacjami, ponieważ minimalizuje to ryzyko pobrania złośliwego oprogramowania.

- **Regularnie wykonuj kopie zapasowe swoich danych, zarówno na komputerze, jak i na telefonie.** W przypadku utraty danych z powodu awarii technicznej, ataku cyberprzestępców lub zgubienia urządzenia będziesz mieć możliwość ich odzyskania.

Stosuj silne hasła

W dzisiejszych czasach coraz więcej codziennych spraw załatwiamy przez internet – od kontaktów z rodziną, przez bankowość, aż po zakupy.

Dlatego tak ważne jest, aby Twoje konta były odpowiednio zabezpieczone.

Dobre hasło działa jak solidny zamek do Twojego domu – chroni przed niechcianymi gośćmi.

Im dłuższe hasło, tym jest ono trudniejsze do złamania. **Twórz hasła składające się z minimum 14 znaków**.

Aby łatwiej zapamiętać hasła, możesz tworzyć kilkuwyrazowe frazy, składające się z **co najmniej 5 słów**, np.:

Wlazl-Kostek-Na-Mostek-I-Stuka

Nie używaj dosłownego cytatu jako hasła, lecz jako inspirację do tworzenia własnych wersji.

Dodaj znaki specjalne, cyfry lub zamień niektóre słowa na inne.

Dzięki temu Twoje hasło stanie się trudniejsze do złamania!

Jak tworzyć hasła?

Unikaj haseł powiązanych z informacjami o Tobie lub Twoich bliskich jak: imię, nazwisko, data lub miejsce urodzenia, imię dziecka, wnuczka, pupila, powtórzenie frazy z loginu np.:

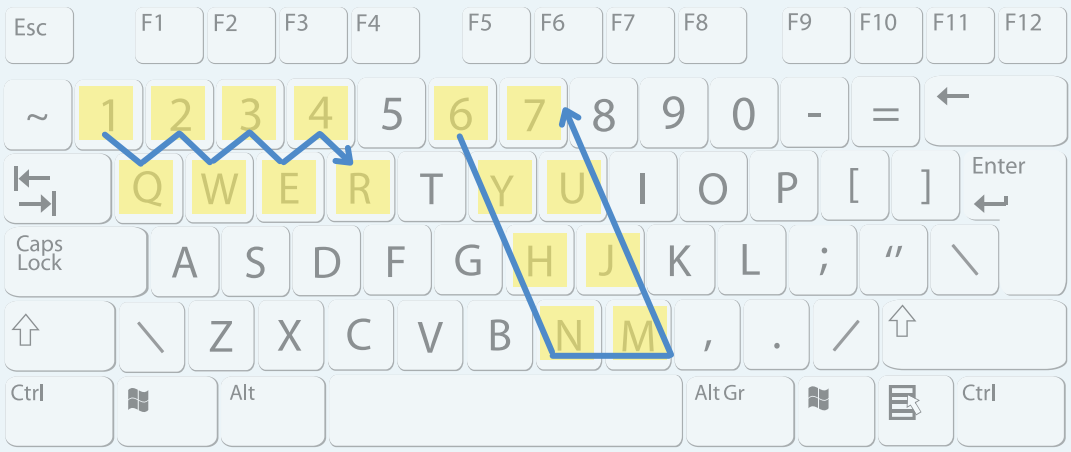
Stasiu2001
MójBurek2022

Nie twórz haseł powtarzalnych, według schematów np.:

mojehaslo1
haslogrudzien2022

Unikaj haseł “wzorów”, sekwencji z klawiatury np.:

1q2w3e4r
6yhnmju7



O czym warto pamiętać?

Jedna usługa = jedno hasło.

To zwiększa bezpieczeństwo Twoich danych. Jeśli ktoś złamie Twoje hasło lub dojdzie do jego wycieku, cyberprzestępcy mogą spróbować użyć go w innych serwisach (np. poczta e-mail, serwisy społecznościowe).

Dlatego ważne jest, aby do każdej usługi posiadać odrębne hasło.

Nie zapisuj haseł na karteczkach i nie przyklejaj ich na urządzeniu.

Unikaj przechowywania haseł w miejscach dostępnych dla innych.

Jeśli masz podejrzenie, że Twoje hasło wyciekło, **zmień je.**

Nigdy nie podawaj swoich haseł osobom trzecim.

Ostrożnie korzystaj z obcych komputerów. Unikaj logowania się na nich do ważnych usług.

Więcej informacji na temat haseł znajdziesz na stronie: **cert.pl**

Włącz weryfikację dwuetapową

Brzmi to skomplikowanie, ale w rzeczywistości jest bardzo proste. **Weryfikacja dwuetapowa to dodatkowe zabezpieczenie podczas logowania**, które chroni Twoje konta w internecie.

Jak to działa? Aby się zalogować, oprócz wpisania hasła będziesz musiał podać także dodatkowy kod. Otrzymasz go za pośrednictwem SMS-a, wiadomości e-mail lub aplikacji w telefonie. Dodatkowym zabezpieczeniem mogą być także Twoje indywidualne cechy fizyczne m.in. odcisk Twojego palca, skan twarzy lub oka czyli tzw. biometria.

1 Twoje hasło

2 Weryfikacja za pomocą kodu lub biometrii

Weryfikacja dwuetapowa jest szczególnie istotna przy logowaniu do serwisów zawierających ważne dane, m.in. poczta e-mail, konto bankowe czy media społecznościowe.

Dzięki niej zwiększasz bezpieczeństwo swoich kont!

NASK

Ważne porady!

Przestępcy będą wykorzystywać każdą okazję, by pozyskać Twoje dane, które pozwolą im np. na kradzież pieniędzy z konta, włamanie na pocztę e-mail i przejęcie korespondencji czy namawianie Twoich bliskich do szybkich przelewów na platformach społecznościowych.

Nigdy nie działaj pod presją czasu.

Uważaj na niespodziewane e-maile, SMS-y i telefony, w których oszuści mogą próbować wyłudzić Twoje dane.

Regularnie sprawdzaj historię transakcji na koncie bankowym.

Uważaj, co udostępniasz na profilach społecznościowych.
Nie udostępniaj w internecie zdjęć i relacji, na których pokazujesz swoje dokumenty.

Ważne porady!

Zastrzeż swój PESEL,
aby nikt nie mógł go użyć do zawierania umów kredytowych lub pożyczek bez Twojej zgody.
Zastrzeżenie numeru PESEL w żaden sposób nie zablokuje Ci możliwości rejestracji do lekarza, realizacji recepty czy załatwienia sprawy urzędowej.

Jak to zrobić?

Przez internet **lub** **w dowolnym urzędzie**

Co będzie potrzebne?

Potwierdzenie tożsamości za pomocą:

- profilu zaufanego,
- podpisu kwalifikowanego,
- e-dowodu,
- lub danych do logowania do bankowości elektronicznej.

Dowód osobisty

W jaki sposób zastrzec PESEL?

Zaloguj się na stronie mObywatel.gov.pl lub uruchom aplikację mObywatel na telefonie.

Zobacz filmik jak to zrobić.

Poproś o pomoc pracownika urzędu.

Skąd czerpać wiedzę?

Serdecznie zachęcamy do odwiedzenia naszej strony z bezpłatnymi materiałami kampanii **#Halo! Tu cyberbezpieczny Senior**

Kliknij na grafikę, aby przejść na stronę z materiałami.

Rekomendowane strony:

www.bezpiecznymiesiac.pl

EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA

Ogólnoeuropejska kampania, znana jako ECSM (Europejski Miesiąc Cyberbezpieczeństwa), organizowana jest przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z inicjatywy Komisji Europejskiej. W Polsce kampanię koordynuje Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy.

www.cert.pl

CERT.PL NASK

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w strukturach NASK-PIB.

NASK Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa