Projekt „Babciu, to nie twój wnuczek. Senior w sieci – bezpiecznie, świadomie, spokojnie” ma na celu podniesienie świadomości cyfrowej oraz wzmocnienie odporności psychicznej i emocjonalnej na oszustwa internetowe i telefoniczne, przede wszystkim wśród osób po 60 roku życia.

To właśnie osoby z tej grupy wiekowej są szczególnie często wybierane przez sprawców przestępstw, ponieważ:

- **oszuści postrzegają je jako bardziej podatne na presję, lęk i manipulację emocjonalną,**
- **rozwój technologiczny następuje bardzo szybko**, a osoby, które nie dorastały w erze cyfrowej, mogą nie być w pełni przygotowane na zagrożenia online,

- **działania profilaktyczne przynoszą wymierne efekty** – zwiększają czujność, poczucie kontroli i zmniejszają ryzyko utraty danych lub środków finansowych,
- **świadomość mechanizmów wykorzystywanych przez cyberprzestępców utrudnia ich skuteczne działanie** i wzmacnia bezpieczeństwo całych społeczności.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

I. Czym jest oszustwo i jak działają oszuści?

Oszustwo – zgodnie z art. 286 § 1 Kodeksu karnego – to przestępstwo polegające na doprowadzeniu innej osoby do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie jej w błąd, wyzyskanie błędu lub niezdolności do należytego pojmowania przedsiębranego działania, w celu osiągnięcia korzyści majątkowej.

Przestępstwo zagrożone jest karą pozbawienia wolności od 6 miesięcy do lat 8, a w przypadku mniejszej wagi sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Oszust **celowo manipuluje ofiarą**, aby ta zrobiła coś, czego **nie zrobiłaby nigdy, gdyby znała prawdę** – np. przekazała pieniądze, dane osobowe albo podpisała umowę.

W świetle orzecznictwa i doktryny na gruncie art. 286 Kodeksu karnego, "wprowadzenie w błąd", "wyzyskanie błędu" oraz "wyzyskanie niezdolności do należytego pojmowania przedsiębranego działania" to trzy odrębne, choć pokrewne, formy działania sprawcy oszustwa. Wszystkie prowadzą do niekorzystnego rozporządzenia mieniem przez pokrzywdzonego, ale różnią się sposobem, w jaki sprawca wpływa na jego decyzję.

1. Wprowadzenie w błąd:

- **Charakterystyka:** to aktywna działalność sprawcy, która polega na **celowym stworzeniu u pokrzywdzonego fałszywego obrazu rzeczywistości**. Sprawca aktywnie wpływa na proces poznawczy ofiary, dostarczając jej nieprawdziwych informacji lub zatajając prawdziwe.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

- **Działanie sprawcy:** sprawca wywołuje błędne przekonanie i wiarę pokrzywdzonego w nieistniejący stan faktyczny (np. wypadek wnuka). Może to być kłamstwo, zatajenie prawdy, manipulacja faktami, przedstawienie fałszywych dokumentów, podmiana prezentacji numeru telefonu (tzw. caller ID spoofing) itp.
- **Przykłady:**
  - Oszust podmienia prezentację numeru telefonu, podaje się za wnuka i opowiada zmyśloną historię o wypadku, aby wyłudzić pieniądze.
  - Sprawca tworzy fałszywą stronę internetową banku, która wygląda identycznie jak prawdziwa, aby wyłudzić dane do logowania.
  - Sprzedawca oferuje "cudowny lek", przypisując mu nieistniejące właściwości lecznicze.

2. Wyzyskanie błędu:

- **Charakterystyka:** w tym przypadku **błąd już istnieje w umyśle pokrzywdzonego**, zanim sprawca rozpocznie swoje działanie przestępcze. Sprawca nie musi aktywnie tworzyć fałszywego obrazu rzeczywistości, lecz **wykorzystuje już istniejące, niezależnie od niego powstałe, błędne przekonanie** pokrzywdzonego.
- **Działanie sprawcy:** sprawca jest bierny w sensie kreowania błędu, ale aktywny w jego wykorzystywaniu. Ma świadomość błędu pokrzywdzonego i celowo działa w taki sposób, aby błąd ten utrzymał się lub pogłębił, co doprowadzi do niekorzystnego rozporządzenia mieniem.
- **Przykład:**

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

fałszywa zbiórka charytatywna.

- **Błąd ofiary:** pokrzywdzony myśli, że przekazuje pieniądze na legalną zbiórkę charytatywną na rzecz powodzian, o której istnieniu słyszał w telewizji lub przeczytał w gazecie.

  Działanie sprawcy: oszust, wiedząc o tym, że pokrzywdzony jest w błędzie co do formy i legalności zbiórki, zbiera datki i przeznacza na własne potrzeby. Oszust w tym przypadku nie tworzył całego mechanizmu od początku, lecz wyzyskał istniejący błąd, "podszywając się" pod legalną akcję charytatywną.

3. Wyzyskanie niezdolności do należytego pojmowania przedsiębranego działania:

- **Charakterystyka:** ta forma dotyczy sytuacji, w której pokrzywdzony, ze względu na swoje cechy osobiste, jest **niezdolny do właściwej oceny sytuacji i konsekwencji swoich działań**. Chodzi tu o ogólną niemożność prawidłowego postrzegania rzeczywistości i podejmowania racjonalnych decyzji.
- **Działanie sprawcy:** polega na stałym lub przemijającym wykorzystaniu zakłócenia percepcji (świadomości) lub psychiki ofiary. Ten stan może wynikać z różnych przyczyn, takich jak:
  - **Wiek, choroba psychiczna, pozostawanie pod wpływem silnych leków, np. przeciwbólowych opiatów, brak wiedzy technicznej/specjalistycznej**
- **Przykłady:**
  - Oszust nakłania starszą osobę z zaawansowaną demencją do podpisania niekorzystnej umowy darowizny mieszkania w zamian za tzw. "dożywocie".

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

II. Najczęstsze typy oszustw

1. Oszustwo "na wnuczka"

- **Schemat:** oszust dzwoni do ofiary, podając się za krewnego (często wnuczka lub wnuczkę). Twierdzi, że znalazł się w nagłej, trudnej sytuacji i pilnie potrzebuje pieniędzy.
- **Scenariusz:** najczęściej oszust informuje o wypadku drogowym, w którym brał udział, lub o pilnej potrzebie wpłacenia kaucji, aby uniknąć aresztowania. Może też prosić o pieniądze na operację, pilne leczenie, spłatę długu czy inną nagłą potrzebę. Oszust może tłumaczyć, że sam nie może odebrać pieniędzy i poprosi o przekazanie ich zaufanej osobie, która się po nie zgłosi – np. koledze, adwokatowi, a nawet taksówkarzowi. Ważne jest, że nigdy nie pojawia się osobiście.

2. Oszustwo "na policjanta"

- **Schemat:** oszust podaje się za funkcjonariusza policji (lub innych służb – CBA, prokuratora) i informuje o prowadzonej tajnej akcji przeciwko przestępcom, np. oszustom bankowym.
- **Scenariusz: r**zekomy policjant twierdzi, że pieniądze ofiary na koncie bankowym są zagrożone lub są częścią przestępczego procederu. Aby je "zabezpieczyć" lub "pomóc w schwytaniu przestępców", nakłania ofiarę do wypłacenia pieniędzy z banku i przekazania ich "funkcjonariuszowi" lub wpłacenia na inne, "bezpieczne" konto. Może również prosić o podanie danych do logowania, kodów BLIK lub zainstalowanie oprogramowania rzekomo zabezpieczającego konto. Często przestrzega przed rozłączaniem się lub informowaniem kogokolwiek o akcji, grożąc konsekwencjami prawnymi.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

3. Oszustwo "na urzędnika"

- **Schemat:** oszust podszywa się pod pracownika instytucji publicznej, takiej jak ZUS, KRUS, Urząd Skarbowy, Urząd Miasta/Gminy czy pomocy społecznej.
- **Scenariusz:** Może informować o konieczności dopłaty do świadczeń, weryfikacji danych w związku ze zmianami przepisów, niedopłatach w rachunkach (np. za wodę, prąd), czy konieczności zapłaty rzekomej zaległości. Celem jest wyłudzenie danych osobowych, numeru konta, kodów BLIK lub nakłonienie do przelania pieniędzy na wskazane konto. Może też proponować "darmowe" usługi lub świadczenia, które wymagają weryfikacji danych.

4. Oszustwo "na bank"

- **Schemat:** Oszust podaje się za pracownika banku ofiary (konsultanta, doradcę, pracownika działu bezpieczeństwa).
- **Scenariusz:** Dzwoni z informacją o rzekomym zagrożeniu na koncie (np. próba włamania, podejrzane transakcje, zablokowanie karty, wygaśnięcie certyfikatu bezpieczeństwa). Może nakłaniać do natychmiastowego przelania pieniędzy na "bezpieczne" konto techniczne (które należy do oszusta), do zainstalowania oprogramowania do zdalnego dostępu (np. AnyDesk, TeamViewer), które umożliwi mu przejęcie kontroli nad komputerem ofiary, lub do podania danych logowania/kodów autoryzacyjnych.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

5. Oszustwo "na urząd skarbowy"

- **Schemat:** Jest to specyficzny wariant oszustwa "na urzędnika", gdzie oszust podszywa się pod pracownika Urzędu Skarbowego.
- **Scenariusz:** Najczęściej przestępca wysyła fałszywy SMS lub e-mail z informacją o rzekomej nadpłacie podatku, niedopłacie, konieczności weryfikacji danych w celu otrzymania zwrotu lub uregulowania zaległości. Wiadomość zawiera link, który prowadzi do fałszywej strony internetowej banku lub bramki płatniczej. Po zalogowaniu się na takiej stronie ofiara nieświadomie podaje swoje dane logowania do bankowości internetowej przestępcom. Może też być prośba o "pilną dopłatę" niewielkiej kwoty.

6. Fałszywe SMS-y i e-maile:

- Niedopłata za paczkę, zaległy mandat, blokada konta Netflix, zwrot podatku – zawsze wysłany jest link prowadzący do fałszywej strony płatności.

7. Media społecznościowe:

- Prośby o BLIK od znajomego wysłane z przejętego przez oszusta konta. Romantyczne oszustwa – „żołnierz z USA”. "Likwidacje" sklepu związane z "mega wyprzedażą" - sklep nigdy nie istniał itp., "promocje", które nie są promocjami.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

8. Spotkania i cudowne terapie:

- Zaproszenia na darmowe badania, pokazy garnków, terapie „lewoskrętną witaminą C” – na miejscu zazwyczaj w umowie sprzedaży ukryta jest umowa kredytowa, który senior podpisuje pod presją, lub bez czytania z uwagi na wielkość liter i brak okularów do czytania.

9. QR kody i mandaty z kodem QR za wycieraczką:

- Fałszywy mandat – „zapłać przez kod QR”. Po zeskanowaniu kodu przez ofiarę oszust uzyskuje dostęp do:
- zapisanych i przychodzących wiadomości,
- wysyłki wiadomości,
- listy kontaktów.

Informacje te można wykorzystać na wiele sposobów, oprócz pozyskania prywatnych danych przydatnych do popełniania oszustw bazujących na błędzie poznawczym ekspozycji:

- obciążenie rachunku poprzez wysyłkę wiadomości typu Premium,
- szantaże wykorzystujące informacje zawarte w wiadomościach i liście kontaktów.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

10. Na empatię, pod pozorem grożącego bankructwa, nieuleczalnej choroby własnej lub osoby najbliższej, kosztów nierefundowanego leczenia itp.:

- **Mechanizm:** nakłonienie pokrzywdzonego do udzielenia dostępu do swoich kont bankowych, profili w mediach społecznościowych, albo zaciągania pod swoim nazwiskiem pożyczek na osobę trzecią lub, co gorsze, poszukiwania kolejnych osób, które byłyby do tego skłonne.

11. Oszustwa inwestycyjne / "Na okazję życia":

- **Mechanizm:** obietnica bardzo wysokich i szybkich zysków z inwestycji, często w egzotyczne lub skomplikowane aktywa (np. kryptowaluty, egzotyczne surowce, start-upy technologiczne). Oszuści mogą pokazywać fałszywe wykresy i platformy, które pokazują "zyski", aby zachęcić do wpłacenia większych kwot.

12. Oszustwa "technicznego wsparcia" (Technical Support Scam):

- **Mechanizm:** ofiara otrzymuje telefon (lub wyskakujące okienko na komputerze) od osoby podającej się za pracownika firmy technologicznej (np. Microsoft, Apple, firmy telekomunikacyjnej), twierdzącej, że na komputerze lub telefonie wykryto wirusa lub problem techniczny. Cel to uzyskanie dostępu do komputera/telefonu ofiary i/lub wyłudzenie opłaty za "naprawę".

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

13. Oszustwa "na dopłatę do emerytury/renty" lub "na zwrot nadpłaconej kwoty":

- **Mechanizm:** przestępcy podszywają się pod pracowników ZUS, KRUS, urzędów skarbowych lub innych instytucji państwowych. Informują o rzekomej nadpłacie, dopłacie do świadczeń lub konieczności weryfikacji danych, aby otrzymać dodatkowe pieniądze.
- **Przykłady:** "otrzyma Pan/Pani dodatkową dopłatę do emerytury, proszę podać numer konta/kod SMS", "Musimy zweryfikować Pana/Pani dane, aby mógł Pan/Pani otrzymać zwrot nadpłaconego podatku". Celem jest wyłudzenie danych bankowych lub kodów do transakcji.

14. Oszustwa "na reset hasła" (phishing ukierunkowany):

- **Mechanizm:** fałszywe wiadomości e-mail lub SMS-y (wyglądające jak od banku, instytucji państwowej, portalu społecznościowego, sklepu internetowego), informujące o konieczności zresetowania hasła z powodu "wycieku danych" lub "podejrzanej aktywności". Link prowadzi do fałszywej strony, która wykrada dane logowania.
- **Przykłady:** "zauważyliśmy podejrzaną aktywność na Twoim koncie bankowym. Zresetuj hasło, klikając w link."

15. Oszustwa "na miłość" / Romansowe:

- **Mechanizm:** oszust nawiązuje romantyczną relację online (na portalach randkowych, w mediach społecznościowych), często podszywając się pod atrakcyjną osobę z zagranicy (np. żołnierza stacjonującego za granicą, inżyniera pracującego na platformie wiertniczej). Po zbudowaniu silnej więzi emocjonalnej, zaczyna prosić o pieniądze na różne "nagłe" potrzeby (np. bilet na przyjazd, leczenie, opłaty celne, uwolnienie z wojska).

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

16. Oszustwa na "darowizny" / "pomoc charytatywna":

- **Mechanizm:** wykorzystywanie nagłych tragedii, klęsk żywiołowych, chorób dzieci czy innych wzruszających historii do zbierania fałszywych darowizn. Oszuści tworzą fałszywe strony internetowe, zbiórki charytatywne lub wysyłają wzruszające maile/SMS-y.

17. Oszustwa "na listonosza" i Pocztę Polską

- w tym przypadku oszuści opracowali cały zestaw różnych oszustw, które opisuje Poczta Polska:

https://www.poczta-polska.pl/news/falszywy-pocztowiec-i-komendant-policji-poczta-polska-przestrzega-przed-oszustami/

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

OSZUSTWA TELEFONICZNE

Metoda na listonosza nr 1

Przestępca dzwoni do ofiary, podając się za listonosza Poczty Polskiej (uwaga, czasem podaje prawdziwe imię i nazwisko listonosza z danego rejonu) i pyta o prawidłowy adres doręczenia listu poleconego z banku. Podczas rozmowy oszust manipuluje rozmówcą, by uzyskać informacje o tym, w jakim banku ofiara posiada konto bankowe. Gdy przestępca ma już te informacje, następuje kolejny telefon – rzekomo z banku lub z policji. Ofiara słyszy, że wpadła przed chwilą w pułapkę przygotowaną przez byłego pracownika Poczty, albo jest informowana, że jest na podsłuchu i pod obserwacją szajki cyberprzestępców. Górę biorą emocje – zwłaszcza, gdy osoba ta słyszy, że jej pieniądze mogą być zagrożone, a nawet, że zagrożone może być jej zdrowie i życie. Przestępcy nalegają na ścisłą współpracę z „policją", a rzekomy funkcjonariusz zachęca ofiarę do udziału w policyjnej prowokacji i prosi o dokonanie wypłaty z banku, a następnie przekazanie gotówki do depozytu CBŚ, czyli np. podstawionemu wspólnikowi, który odbiera łup.

Zdarzało się również, że skrzynkami depozytowymi miały być osiedlowe śmietniki albo senior był proszony o zapakowanie pieniędzy i wyrzucenie ich przez okno w wyznaczonym czasie. Czasem oszuści próbują również wyłudzić od ofiar dane osobowe: numer PESEL, wzór podpisu oraz numer dowodu. Wszystko po to, by wziąć pożyczkę na konto ofiary.

Metoda na listonosza nr 2

Oszuści najpierw dzwonią do ofiary – najczęściej seniora – podając się za listonoszy i informują, że dzisiaj zostanie dostarczona przesyłka. Wkrótce potem dzwonią ponownie udając policjanta, który prowadzi sprawę oszustwa „na listonosza". W ten sposób zdobywają zaufanie ofiary. Następnie zadając podchwytliwe pytania lub umiejętnie kierując rozmową, zdobywają informacje o kosztownościach i pieniądzach, jakie ofiara posiada w domu. Po jakimś czasie rzekomy policjant zjawia się w domu ofiary i wchodzi twierdząc, że przyszedł zabezpieczyć zagrożoną gotówkę lub kosztowności. Po wejściu do mieszkania zastrasza ofiarę i dokonuje rabunku.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

OSZUSTWA INTERNETOWE

Oszustwo na palety

Przestępcy organizują fałszywe kampanie, nakierowane na oszukanie klientów Poczty Polskiej. Podszywając się pod Pocztę Polską, oferują zakup palet z rzekomymi przesyłkami, które nie zostały doręczone i mają zalegać w magazynach. Oferta jest zawsze bardzo atrakcyjna, a całą paletę można kupić podobno za jedyne kilka złotych. Informacja jest przekazywana poprzez media społecznościowe – zawiera krótki opis, pozytywne komentarze „kupujących" oraz zdjęcia obrazujące przesyłki paletowe z logotypem Poczty Polskiej i wyraźnie widoczną „promocyjną ceną".

Loteria z zagubioną paczką

Oszuści, podszywając się pod Pocztę, oferują za kilka złotych możliwość wzięcia udziału w loterii i wygrania „zagubionej paczki". Informacja również jest przekazywana przez media społecznościowe z opisem i zdjęciem rzekomej zagubionej paczki.

Phishing na dopłaty celne

To kampania phishingowa na dopłaty celne, w której cyberprzestępcy podszywają się pod Pocztę Polską. Maile wysyłane są z adresów podszywających się pod noreply@poczta-polska.pl, jednak należy pamiętać, że jest to oszustwo, polegające na podszyciu się pod oficjalną wiadomość od instytucji. Fałszywe korespondencja pochodzi często z adresów, gdzie „xx" może być liczbą lub zestawem liczb czy liter, a zakończenie adresu zawiera inne niż „.pl" oznaczenie, np.: @poczta-polska.xx.com, @poczta-polska.xx.org, @poczta-polska.xx.net.

Wiadomość wygląda następująco:

„Szanowny Kliencie,

Dziękujemy za wybranie Poczty Polskiej. W związku z zamówieniem Poczta Polska, będziesz musiał zapłacić dodatkowe opłaty importowe, aby otrzymać zamówienie jutro.

Cena dostawy: (0.05 €) https://..... (tu wstawiany jest link do fałszywej strony udającej stronę Poczty)

wyślemy Ci e-mail, gdy towar zostanie przekazany do dostawy, informując o zmianie statusu na wysłany".

OSZUSTWA SMS-OWE

Dopłata do paczki

Ofiara otrzymuje SMS z prośbą o dopłatę do paczki: *„Twoja paczka została wstrzymana z tytułu niedopłaty 0,50 złotych."* lub *„Twoja paczka o numerze (...) wymaga dopłaty na sumę 0,87 złotych. Brak wpłaty oznacza zwrot przesyłki do nadawcy. Prosimy uregulować należność klikając w podany link https://(...)."* A przesłany przez cyberprzestępców link prowadzi do fałszywego panelu płatności elektronicznej.

Uwaga! Poczta Polska nigdy nie prosi o uregulowanie należności w powyższy sposób. Pamiętajmy, aby nie wchodzić w przesłane linki, nie przekazywać kodów BLIK lub danych swoich kart płatniczych. Warto poświęcić trochę czasu na zweryfikowanie takiej wiadomości, aby uchronić się przed stratami – zainfekowaniem smartfona, przejęciem loginów i haseł oraz wyczyszczeniem konta bankowego.

Brak danych do przesyłki

CERT Poczta Polska informuje o nasileniu akcji phishingowych, rozsyłanych w formie wiadomości SMS, w których cyberprzestępcy, podszywając się pod Pocztę, próbują uzyskać korzyści finansowe oraz dane osobowe obywateli. Wiadomości są rozsyłane na losowe numery telefonów i nie mają nic wspólnego z rzeczywistymi przesyłkami realizowanymi przez Pocztę Polską. SMS-y z informacją o rzekomym braku możliwości dostarczenia przesyłki generowane są często z zagranicznych numerów. Wiadomości zawierają link, który przenosi ofiarę do strony wyłudzającej dane.

Błędny adres

Podszywający się pod Pocztę Polską oszuści wysyłają do ofiary SMS z informacją o braku możliwości dostawy z uwagi na błędny adres. Aby otrzymać przesyłkę, rzekomo wystarczy kliknąć w link do formularza, uzupełnić go i dokonać niewielkiej opłaty za zmianę adresu. Oczywiście strony, do których odnoszą się linki, są spreparowane, a wypełnienie formularza i dokonanie płatności może doprowadzić do utraty całej zawartości konta bankowego. Dlatego nie należy otwierać podejrzanych linków, szczególnie od nieznajomych, uważać na wszelkiego rodzaju „okazje" w sieci i weryfikować autentyczność otrzymanej wiadomości.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

18. Oszustwo "na dotację", "na dopłaty"

Te (a także inne) typy cyber-przestępstw regularnie opisują: Zaufana Trzecia Strona (https://zaufanatrzeciastrona.pl/) oraz Niebezpiecznik (https://niebezpiecznik.pl/).

- **Mechanizm:** oszust dzwoni, informując o dedykowanej dla pokrzywdzonego dotacji lub o dopłatach i oferuje konsultacje oraz pomoc w prawidłowym wypełnieniu formularzy, sugerując, że są to oficjalne działania prowadzone przez urząd, który ogłosił nabór.

  W ten sposób sprawca wyłudza adres i następnie zamiast dokumentów dotyczących dopłat lub dotacji wysyła bezwartościową paczkę za pobraniem, której koszt wynosi od 200 zł wzwyż.

19. Oszustwo "na reklamację" w banku

- **Mechanizm:** przestępca informuje o istnieniu rzekomej "luki" w systemie banku pokrzywdzonego i oferuje pomoc w próbie uzyskania bądź "odzyskania" pieniędzy od banku z tytułu owej luki. W rzeczywistości luki nie ma, a osoba składająca bezpodstawny wniosek reklamacyjny, faktycznie uczestniczy w próbie wyłudzenia i może zostać pociągnięta do odpowiedzialności karnej.
- Równolegle sprawca usiłuje przejąć konto bankowe pokrzywdzonego i zaciągnąć na jego nazwisko pożyczki.

20. Oszustwo "na szantaż"

- **Mechanizm:** sprawca wysyła mail lub SMS z informacją o włamaniu i wykradzeniu wszystkich zdjęć, filmów oraz korespondencji z komputera lub telefonu pokrzywdzonego i żąda zapłaty w ciągu krótkiego, określonego w wiadomości czasu, grożąc, że w

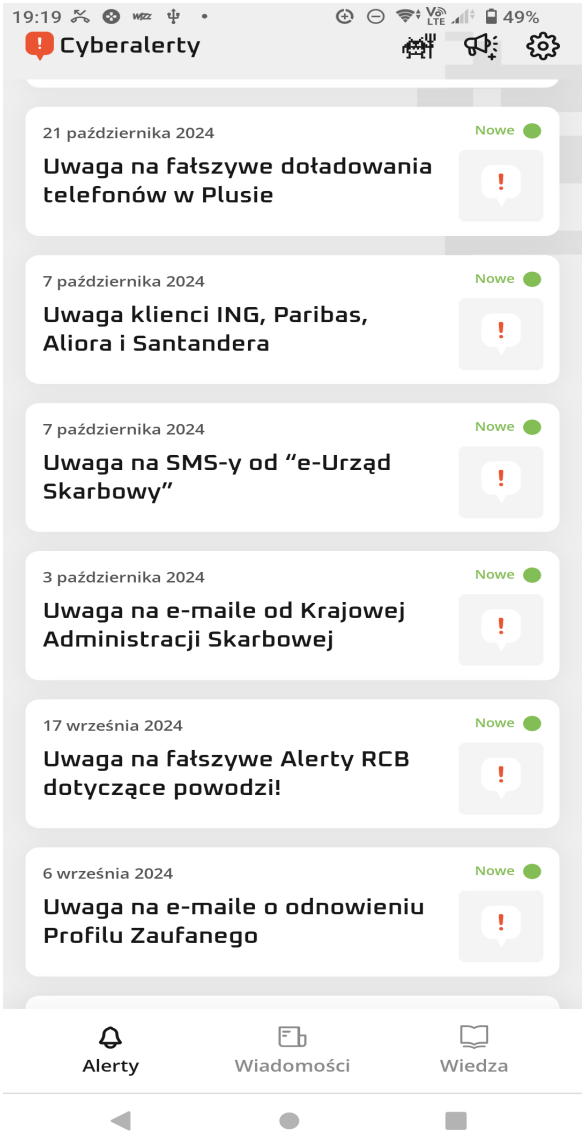
przypadku braku wpłaty ofiara straci wszystkie materiały, ewentualnie - wszystkie zostaną publicznie ujawnione i skompromitują pokrzywdzonego. Włamanie i kradzież materiałów niekoniecznie miały miejsce.

21. Oszustwo "na profil zaufany"

Mechanizm: oszuści informują o problemach z profilem zaufanym, którym zapobiec ma zalogowanie się pokrzywdzonego na profil przez podany w wiadomości link. Kliknięcie w link kieruje na stronę wyłudzającą dane do bankowości internetowej, a jeżeli logowanie jest dokonywane przez pokrzywdzonego za pośrednictwem banku i wpisze on hasła na stronie z linku - to najprawdopodobniej utraci swoje wszystkie oszczędności.

(Screen autorstwa niebezpiecznik.pl)

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

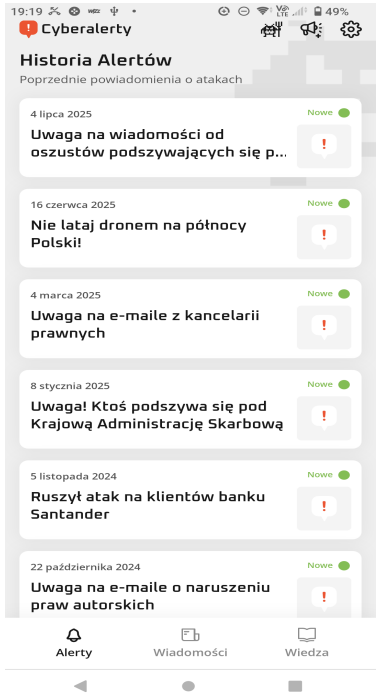


WAŻNE!

Oszustwa m.in. tzw. "pishingu" regularnie monitoruje i opisuje portal niebezpiecznik.pl:

https://niebezpiecznik.pl/post/uwaga-na-e-maile-o-wygasnieciu-profilu-zaufanego/

Portal obsługuje bezpłatną aplikację mobilną **cyber-alert**, którą warto zainstalować z oficjalnego sklepu google na swój telefon, aby być na bieżąco z najnowszymi cyber-zagrożeniami.



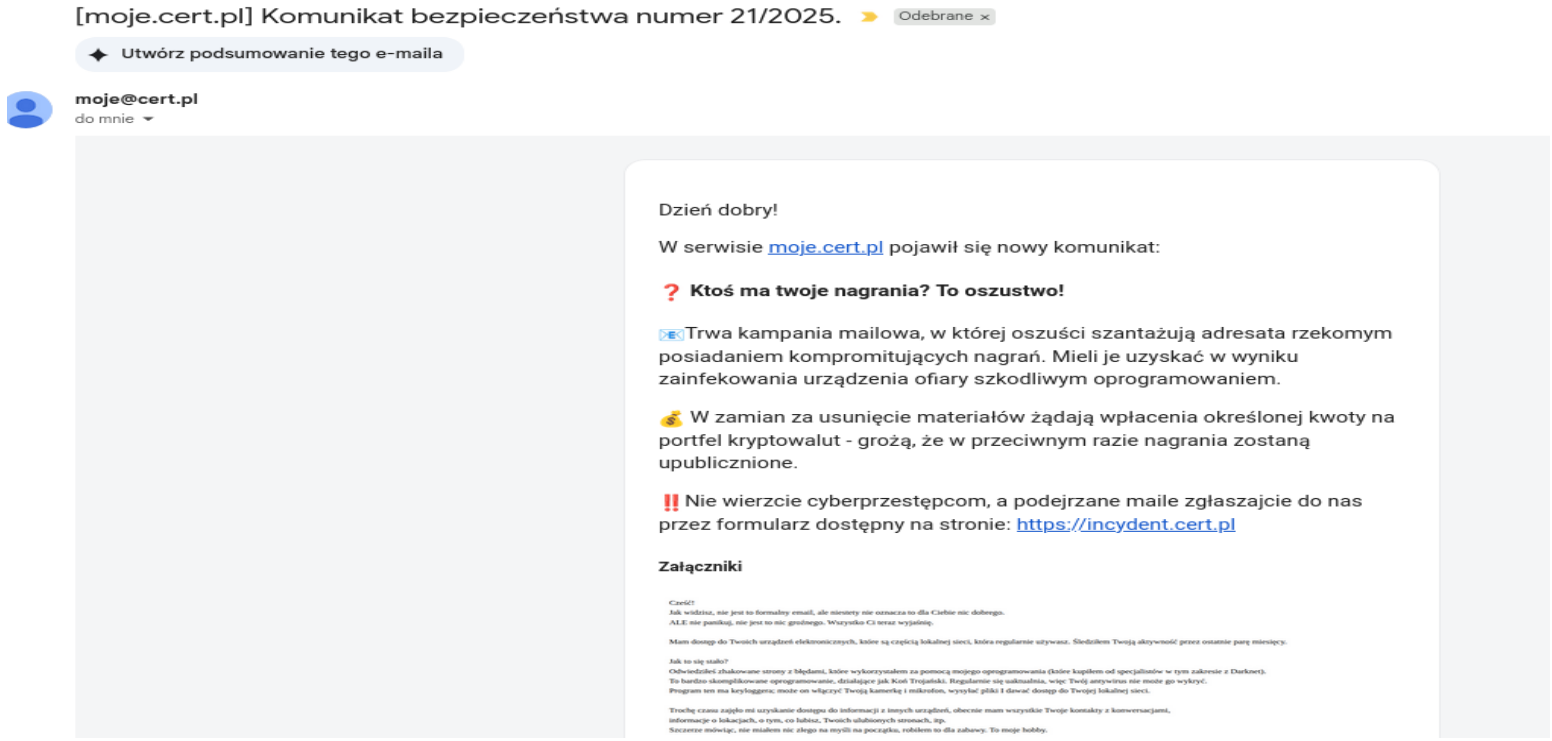
SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

WAŻNE!

Na bieżąco o najnowszych metodach cyber-oszustów informują także:

1. CERT: https://moje.cert.pl/.

Warto zalogować się na stronie i otrzymywać alerty na adres mailowy. CERT Polska (skrót od Computer Emergency Response Team Polska) to zespół ekspertów działający w strukturach NASK – Państwowego Instytutu Badawczego, m.in. reagujący na incydenty i zagrożenia cyberbezpieczeństwa.


[moje.cert.pl] Komunikat bezpieczeństwa numer 21/2025. Odebrane

Utwórz podsumowanie tego e-maila

moje@cert.pl
do mnie

Dzień dobry!

W serwisie moje.cert.pl pojawił się nowy komunikat:

❓ **Ktoś ma twoje nagrania? To oszustwo!**

📧Trwa kampania mailowa, w której oszuści szantażują adresata rzekomym posiadaniem kompromitujących nagrań. Mieli je uzyskać w wyniku zainfekowania urządzenia ofiary szkodliwym oprogramowaniem.

💰 W zamian za usunięcie materiałów żądają wpłacenia określonej kwoty na portfel kryptowalut - grożą, że w przeciwnym razie nagrania zostaną upublicznione.

‼️ Nie wierzcie cyberprzestępcom, a podejrzane maile zgłaszajcie do nas przez formularz dostępny na stronie: https://incydent.cert.pl

Załączniki

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Cześć!
Jak widzisz, nie jest to formalny email, ale niestety nie oznacza to dla Ciebie nic dobrego.
ALE nie panikuj, nie jest to nic groźnego. Wszystko Ci teraz wyjaśnię.

Mam dostęp do Twoich urządzeń elektronicznych, które są częścią lokalnej sieci, która regularnie używasz. Śledziłem Twoją aktywność przez ostatnie parę miesięcy.

Jak to się stało?
Odwiedziłeś zhakowane strony z błędami, które wykorzystałem za pomocą mojego oprogramowania (które kupiłem od specjalistów w tym zakresie z Darknet).
To bardzo skomplikowane oprogramowanie, działające jak Koń Trojański. Regularnie się uaktualnia, więc Twój antywirus nie może go wykryć.
Program ten ma keyloggera; może on włączyć Twoją kamerkę i mikrofon, wysyłać pliki I dawać dostęp do Twojej lokalnej sieci.

Trochę czasu zajęło mi uzyskanie dostępu do informacji z innych urządzeń, obecnie mam wszystkie Twoje kontakty z konwersacjami,
informacje o lokacjach, o tym, co lubisz, Twoich ulubionych stronach, itp.
Szczerze mówiąc, nie miałem nic złego na myśli na początku, robiłem to dla zabawy. To moje hobby.

Ale złapałem COVIDa i niestety straciłem swoją pracę.
Wykombinowałem więc, jak użyć "mojego hobby", by zdobyć kasę od Ciebie!
Nagrałem film z tego, jak się masturbujesz. Film ten ma oddzielny ekran, gdzie z łatwością idzie Cię rozpoznać; widać też jasno, jakiego rodzaju filmy preferujesz.
Cóż, nie jestem z tego dumny, ale potrzebuję kasy, by przetrwać.

Dobijmy targu. Zapłacisz mi tyle, ile będę potrzebował, a ja nie wyślę tego filmu do Twoich znajomych, rodziny i współpracowników.
Powinieneś zrozumieć, że to nie żart. Mogę wysłać to emailem, linkiem SMS, mediami społecznościowymi, a nawet do mediów (mam p… …wanych kont ich adminów).
Mógłbyś więc zostać "gwiazdą" Twittera, lub Instagram!

By tego uniknąć, powinieneś mi wysłać 1300 EUR w Bitcoinach na mój portfel BTC:1CbECyv… …WyAhvLLMAWcU1S6

Jeśli nie wiesz, jak używać Bitcoinów, wyszukaj w Bingu lub Google "jak mogę kupić Bitc…y", czy coś w ten d…ch.
Usunę ten film, jak tylko otrzymam swoją kasę. Usunę również złośliwe oprogramowanie z …oich urz…zeń. Nigdy w…ce… …e nie usłyszysz.
Daję Ci 2 dni, to dość jak sądzę. Zegar zacznie tykać, gdy tylko otworzysz tego maila, monit…ę to!

Jeszcze jedna sprawa:
Nie ma sensu zgłaszać to na policję, ponieważ używam TOR, więc nie ma sposobu na to, by na… …omami.
Nie odpowiadaj mi (wygenerowałem ten list na Twoim koncie i dałem prawdziwy adres człowieka, kt…y nie ma o tym zielonego pojęcia). W ten sposób nie idzie mnie namierzyć.

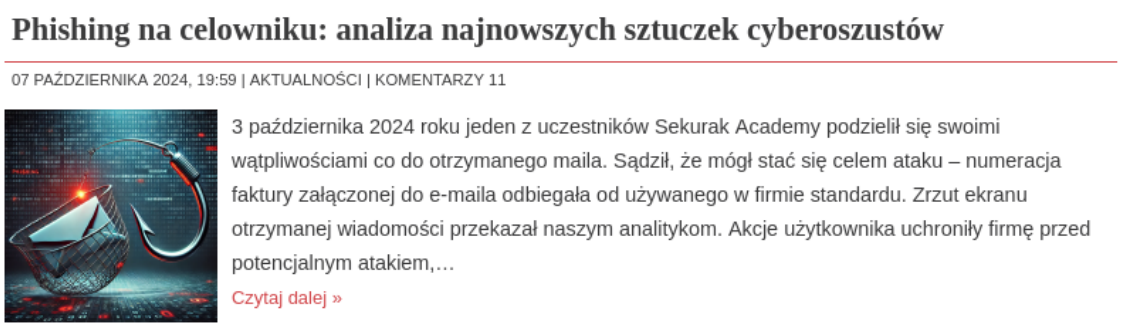
Jeśli zrobisz coś głupiego, czy niezgodnego z moimi oczekiwaniami, natychmiast udostępnię film.
Powodzenia!

OSZUSTWO

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

2. Sekurak: https://sekurak.pl/

Strona Sekuraka także oferuje newsletter, na stronie www wystarczy wpisać mail, aby otrzymywać najnowsze informacje i alerty.



Phishing na celowniku: analiza najnowszych sztuczek cyberoszustów

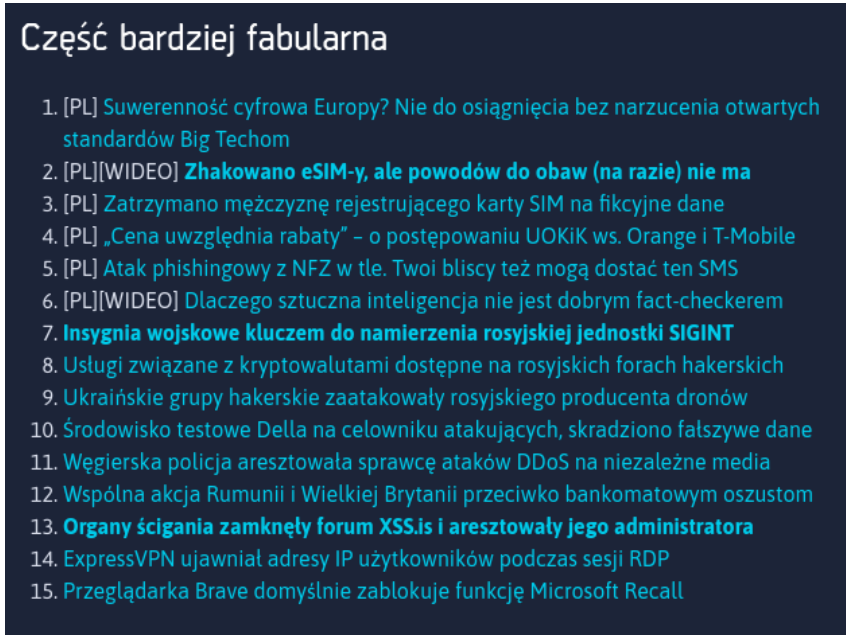
07 PAŹDZIERNIKA 2024, 19:59 | AKTUALNOŚCI | KOMENTARZY 11

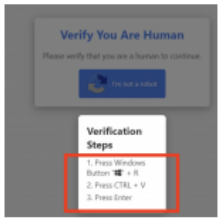
3 października 2024 roku jeden z uczestników Sekurak Academy podzielił się swoimi wątpliwościami co do otrzymanego maila. Sądził, że mógł stać się celem ataku – numeracja faktury załączonej do e-maila odbiegała od używanego w firmie standardu. Zrzut ekranu otrzymanej wiadomości przekazał naszym analitykom. Akcje użytkownika uchroniły firmę przed potencjalnym atakiem,…

Czytaj dalej »

3. Zaufana Trzecia Strona: https://zaufanatrzeciastrona.pl/

również zachęca do newslettera





Uwaga, na nową sprytną metodę phishingu, którą zaczynają stosować przestępcy. W skrócie – złośliwa CAPTCHA.

13 WRZEŚNIA 2024, 21:34 | AKTUALNOŚCI | KOMENTARZE 4

Ofiara na stronie, którą odwiedza, otrzymuje niby standardową prośbę potwierdzenia, że „jest człowiekiem" (czyli mechanizm CAPTCHA): Ale zwróć uwagę na niby niewinną instrukcję, która się pojawia przy tej okazji: 1. Naciśnij win+r2. Naciśnij ctrl+v3. Naciśnij enter Jak możesz się domyślać, najpierw złośliwa strona umieszcza coś w schowku systemowym ofiary (złośliwe…

Czytaj dalej »

Prawdopodobny phishing na adminów Mastodona za pośrednictwem Fediwersum

02 WRZEŚNIA 2024, 02:04 | W BIEGU | KOMENTARZY 10

Mastodon to oprogramowanie, które w Fediwersum miało zastąpić Twittera (obecnie X). Instancje Mastodona tworzą zdecentralizowaną federację składającą się z niezależnych instancji. Każda z instancji posiada swojego administratora, serwer, domenę i… politykę wymiany danych z innymi instancjami. W ramach pojedynczej instancji nie ma ograniczeń widoczności, jednak w Fediversum powstał specyficzny podział pomiędzy instancjami, który w uproszczeniu…

Czytaj dalej »

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

III. Jak rozpoznać próbę oszustwa?

Czerwone flagi (sygnały ostrzegawcze)

Presja czasu

„Musisz działać NATYCHMIAST!”

Prawdziwe instytucje nie każą działać w pośpiechu.

Oszust chce Cię zdezorientować i zestresować, dzięki czemu łatwiej mu będzie manipulować emocjami.

Natychmiastowe przelewy / kod BLIK / gotówka

Bank, policja, ani urząd nie prosi o przekazanie pieniędzy „do depozytu”, ani na "bezpieczne konto depozytowe".

Oszust chce zarządzać Twoimi pieniędzmi pod pozorem rzekomego zagrożenia.

Prośby o dane osobowe i logowania

Login, hasło, PESEL, PIN, CVC, kody SMS? NIE.

Prawdziwe instytucje nigdy nie proszą o takie dane przez telefon/SMS, czy e-mail.

Strony instytucji i ich numery kontaktowe oznacz jako "ulubione" lub zapisz w zakładkach na komputerze i dzwoń oraz wchodź wyłącznie przez nie, nie klikaj w linki!

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Zbyt piękne oferty

„Cudowny lek”, „złota inwestycja”, „znaleziona zagubiona paczka”?
Jeśli coś brzmi jak bajka – to zapewne nią jest.

Zastraszanie i groźby

„Zablokujemy konto!”, „Pójdzie/sz do więzienia!”
To nie są metody instytucji i urzędów – to element scenariusza oszustwa.

Nieoczekiwany kontakt

Dzwoni „wnuczek”? „ZUS”? „Listonosz z paczką”? Bank w niedzielę wieczorem?
ZAWSZE możesz się rozłączyć i sprawdzić tożsamość rozmówcy dzwoniąc pod oficjalny numer.

Błędy w wiadomości

Ortografia na poziomie dziecka? Dziwny adres mailowy z nietypową końcówką?
Instytucje dbają o profesjonalizm, szczególnie w korespondencji z klientami. Oszust dba o szybki zysk.

Znajomy z Facebooka prosi o kod BLIK?

Najpierw zadzwoń na jego numer, aby sprawdzić, czy to faktycznie on. Po pozytywnej weryfikacji - i tak nie wysyłaj kodu. Pomóc możesz także w inny sposób.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

IV. Mechanizmy psychologiczne wykorzystywane przez oszustów

Dlaczego to działa?

- Oszuści nie włamują się przez drzwi – włamują się przez nasze emocje.
- Każdy człowiek posiada automatyczne mechanizmy psychiczne, które pomagają w codziennym funkcjonowaniu i przetrwaniu w warunkach ekstremalnych – ale równocześnie mogą być wykorzystane przeciwko niemu.
- Seniorzy bywają szczególnie narażeni z uwagi na:
    - wysoki poziom zaufania i empatię,
    - wychowanie w kulturze szacunku wobec autorytetów,
    - samotność i potrzebę kontaktu.

Mechanizm 1: Presja czasu i stres

- Oszuści celowo wywołują stres i presję czasową.
- Mózg wchodzi w tryb „walki lub ucieczki” → spada zdolność logicznego myślenia.
- Objawy: przyspieszony puls, drżenie, zawężona uwaga, paraliż decyzyjny.
- Skutek: działanie automatyczne, emocjonalne, impulsywne, bezrefleksyjne.
- **Obrona**: zatrzymaj się, oddychaj, powiedz: „Oddzwonię później” i rozłącz się, zastosuj jedną z prostych technik psychologicznych obniżających poziom stresu, skonsultuj się z zaufaną osobą, zweryfikuj sytuację za pośrednictwem samodzielnie wybranych oficjalnych stron www i telefonów.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Mechanizm 2: Autorytet i zaufanie

- Oszuści podszywają się pod funkcjonariuszy, urzędników, pracowników banku.
- Wykorzystują heurystykę autorytetu – „skoro to mówi policjant, to musi być prawda”.
- Seniorzy wychowani w kulturze szacunku wobec autorytetu są szczególnie narażeni na tego typu manipulacje.
- **Obrona**: nie ufaj tytułowi, jaki sam sobie nadaje rozmówca. Zweryfikuj dane. Zadzwoń na oficjalny numer instytucji.

Mechanizm 3: Wzbudzanie emocji

- Przykłady: „Twoja córka miała wypadek”, „Tylko dziś możesz skorzystać z wyjątkowej oferty.”
- Emocje (strach, nadzieja, wzruszenie) blokują myślenie analityczne.
- Efekt amygdali: emocje dominują nad logiką.
- **Obrona**: nazwij emocję. Daj sobie czas. Sprawdź informacje, zanim zareagujesz.

Mechanizm 4: Efekt „on wie coś o mnie”

- Oszust zna szczegóły: imię syna lub wnuka, nazwisko, adres.
- To nie dowód autentyczności podawanych przez sprawcę informacji – dane często pochodzą z internetu, wycieków lub obserwacji.
- Mózg szuka potwierdzenia spójności i stosuje uproszczenia – „to pasuje, więc musi być prawdziwe”.
- **Obrona**: ustal w rodzinie hasła bezpieczeństwa, jakie podacie sobie w sytuacjach krytycznych, gdy nagle będziecie potrzebować pomocy finansowej. Nigdy nie potwierdzaj danych bez weryfikacji.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Mechanizm 5: Metoda małych kroków („efekt stopy w drzwiach” lub "plasterków salami")

- Oszust zaczyna od małych próśb o udzielenie niewinnych informacji („czy ma pani konto?”), a kończy na prośbach o dane i przelewy.
- Mechanizm psychologiczny: skoro już się na coś zgodziłem, trudniej odmówić kolejnej prośbie.
- **Obrona**: jeśli coś wydaje się zbyt szybkie, a scenariusz rozmowy przypomina efekt domino – przerwij. Masz prawo się zastanowić i odmówić.
-

Podsumowanie:

- Oszuści wykorzystują automatyczne reakcje biologiczne i emocjonalne.
- Nikt nie jest odporny – ale każdy może się nauczyć prostych technik obrony.
- Najważniejsze: nie działaj pod wpływem presji. Zatrzymaj się, oddychaj, zweryfikuj informacje.
- Pamiętaj: fakt, że ktoś zna Twoje dane lub brzmi profesjonalnie, nie znaczy, że mówi prawdę.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Proste techniki odstresowujące dla seniorów

Do wykorzystania w sytuacji presji, stresu lub emocjonalnego szoku

1. Liczenie wstecz – „5 do 0”

Metoda ta wykorzystuje procesy neuronalne w celu przerwania reakcji emocjonalnej i przywrócenia kontroli poznawczej. Działa poprzez:

Aktywację kory przedczołowej: Liczenie, zwłaszcza wstecz, wymaga zaangażowania procesów kognitywnych w korze przedczołowej, która odpowiada za planowanie, koncentrację i logiczne myślenie.

Dezaktywację ciała migdałowatego: W sytuacji silnego stresu, ciało migdałowate (amigdala) przejmuje dominującą rolę, wyzwalając emocje takie jak strach i lęk. Świadome, wymagające wysiłku umysłowego zadanie, jakim jest liczenie, przekierowuje zasoby mózgu, obniżając aktywność amigdalii i osłabiając reakcję emocjonalną.

Ćwiczenie:

1. Licz wstecz: 5… 4… 3… 2… 1… 0.
2. Licz w przód: 0… 1… 2… 3… 4… 5.
3. Powtarzaj cykl.

To proste ćwiczenie pomaga w **regulacji emocji**, obniża napięcie i przywraca zdolność do podejmowania racjonalnych decyzji.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

2. Oddychanie 4-2-6. Technika relaksacji oddechowej

Metoda ta stanowi prostą formę regulacji oddechu, aktywującą **układ nerwowy przywspółczulny**, odpowiedzialny za reakcję relaksacji. Jest to skuteczna technika obniżania poziomu stresu, która znajduje zastosowanie w sytuacjach wymagających szybkiego opanowania emocji.

Instrukcja wykonania:

1. **Wdech:** Należy wdychać powietrze nosem przez 4 sekundy.
2. **Wstrzymanie:** Zatrzymanie oddechu na 2 sekundy.
3. **Wydech:** Wydychanie powietrza ustami przez 6 sekund.
4. **Częstotliwość:** Powtórzyć ćwiczenie 5 razy.

Mechanizm działania: Po wykonaniu 5 cykli oddechowych obserwuje się obniżenie poziomu kortyzolu, co wspomaga redukcję napięcia fizjologicznego i przywraca zdolność do racjonalnego myślenia.

Dlaczego oddychanie i skupienie na tym procesie działa?
W momencie silnego stresu nasz organizm włącza tryb "walki lub ucieczki" (reakcja stresowa), za który odpowiada układ współczulny. Powolne oddychanie aktywuje układ przywspółczulny (parasympatyczny), który jest jego antagonistą. Układ ten odpowiada za stan relaksu i odpoczynku. Wyrównanie oddechu (wydłużenie wydechu w stosunku do wdechu) jest dla organizmu sygnałem, że zagrożenie minęło, a ciało może się uspokoić:

Obniżenie poziomu hormonów stresu: Aktywacja układu przywspółczulnego prowadzi do obniżenia poziomu kortyzolu i adrenaliny we krwi. Spadek stężenia tych hormonów zmniejsza fizjologiczne objawy stresu, takie jak przyspieszone bicie serca czy wysokie ciśnienie krwi.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Wzrost aktywności kory przedczołowej: Kiedy poziom hormonów stresu spada, a organizm się uspokaja, kora przedczołowa - odpowiedzialna za logiczne myślenie, planowanie i podejmowanie świadomych decyzji - może ponownie przejąć kontrolę nad działaniem mózgu. W sytuacji silnego stresu jej aktywność jest ograniczona na rzecz bardziej pierwotnych struktur mózgu, np. ciała migdałowatego (odpowiedzialnego za emocje). Właśnie z tego powodu, w silnym stresie trudniej nam logicznie myśleć.

Po takim ćwiczeniu stres **wyraźnie spada** – można je wykonać niezauważalnie dla otoczenia nawet w sklepie, autobusie, czy podczas rozmowy.

3. Technika „5-4-3-2-1” – Zakotwiczenie w rzeczywistości

Stosowana w terapii traumy i lęku – pomaga **wyjść z emocji** i wrócić do „tu i teraz”.

Ćwiczenie:

5 rzeczy, które widzę

4 dźwięki, które słyszę

3 odczucia, które odczuwam fizycznie

2 zapachy, które czuję

1 smak, który czuję

4. Napnij i rozluźnij mięśnie – technika Jacobsona

Technika tzw. progresywnej relaksacji: napinając i rozluźniając ciało, **redukujemy napięcie mięśniowe** i dzięki temu także psychiczne.

Ćwiczenie (wersja uproszczona):

1. Zaciśnij pięści na 5 sekund → rozluźnij
2. Napnij ramiona w górę → rozluźnij
3. Zaciśnij szczękę → rozluźnij
4. Naciśnij stopami w podłogę → rozluźnij

5. Hasło bezpieczeństwa – czyli „mantra opanowania”

Słowa mają moc – warto mieć gotowe **zdanie**, które powtarzamy sobie w trudnych sytuacjach.

Przykłady haseł:

„To tylko głos. Mam czas. Myślę spokojnie.”

„Mam prawo się rozłączyć.”

„Oddycham. Nic nie robię w pośpiechu.”

"Najpierw myślę, potem działam"

„Nie podejmuję decyzji pod wpływem emocji.”

"Dobre serce nie może być pułapką."

"Chcesz mi pomóc? Zrób mi przerwę!" (Hasło, które można powiedzieć w trakcie rozmowy, sygnalizując potrzebę czasu)

Powtarzanie hasła uspokaja umysł i **dodaje odwagi** w chwilach niepewności.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Mikroczynności do szybkiego uspokojenia

Dotknij zimnego metalu (np. klamki) – chłód odciąga uwagę od emocji
Weź łyk wody – sygnał dla ciała: „jesteś bezpieczny”
Stań prosto, rozluźnij ramiona – ciało wysyła sygnał do mózgu: „mam kontrolę”

V. Bezpieczne zachowania: jak nie dać się oszukać?

Zasady bezpieczeństwa w codziennym życiu

"Nie oddzwaniaj"

Nie oddzwaniaj na nieznane numery.
Samodzielnie znajdź numer banku / urzędu.
Zrób „pauzę bezpieczeństwa”: zatrzymaj się – pomyśl – zweryfikuj.
Zadzwoń na oficjalny numer i zgłoś podejrzenia.

"Nie klikaj"

Nie klikaj w linki z SMS-ów i maili, nawet jeśli wyglądają „urzędowo”!
Samodzielnie wpisz adres strony banku/urzędu lub wejdź na stronę instytucji z zakładki lub listy "ulubionych".
Sprawdzaj nadawcę, literówki, podejrzany język, adres nadawcy.

"Nie podawaj"

Nigdy nie podawaj przez telefon, SMS lub maila:
• loginu i hasła
• numeru PESEL, dowodu
• danych karty płatniczej
• kodów BLIK, PIN, haseł SMS
Nie instaluj programów typu AnyDesk, TeamViewer – dają oszustowi dostęp do Twojego komputera!

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Wsparcie rodziny i otoczenia.

Rodzina – rozmawiajcie o podejrzanych sytuacjach.
Dzwońcie do siebie, weryfikujcie.
Miej przy telefonie listę zaufanych osób.
! Wymyślcie hasło bezpieczeństwa.

Sąsiedzi – dzielcie się informacjami o próbach oszustwa.
Bank – pracownik może pomóc!
Jeśli nie wiesz co zrobić – zapytaj zaufaną osobę jak ocenia sytuację, w której się znajdujesz.

Co robić przy podejrzeniu oszustwa?

Zasada STOP:

S – Stop – zatrzymaj się. Nie klikaj, nie przelewaj pieniędzy, nie podawaj danych ani nr BLIK.

T – Tylko spokojnie – emocje są normalne, ale nie podejmuj decyzji w panice.

O – Obserwuj – co się dzieje? Kto dzwoni? Jakie informacje próbuje uzyskać?

P – Podejmij decyzję – dopiero po weryfikacji i konsultacji z zaufaną osobą.

Zasada 3Z – najprostszy sposób obrony:

Zatrzymaj się. Nie działaj pochopnie – zyskaj czas.

Zadzwoń. Sprawdź informacje – zadzwoń samodzielnie do banku, bliskiej osoby lub instytucji.

Zgłoś. Jeśli podejrzewasz oszustwo – zgłoś to policji, CERT-owi lub rzecznikowi konsumentów.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Zadaj sobie 12 pytań:

Czy znam osobę lub instytucję, z którą rozmawiam?

Czy ta osoba prosi o dane osobowe, login, hasło, BLIK, numer karty, lub pieniądze?

Czy rozmówca wywołuje we mnie silne emocje – strach, presję, poczucie winy?

Czy naciska, bym działał natychmiast, bez konsultacji?

Czy kontakt nastąpił o dziwnej porze lub nietypowym sposobem?

Czy mam możliwość samodzielnie to sprawdzić, zanim odpowiem?

Czy rozmówca daje mi czas na konsultacje z kimś zaufanym?

Czy prośba lub oferta pomocy policjanta zawiera groźby lub straszenie konsekwencjami?

Czy ktoś twierdzi, że jestem jedyną osobą, która może coś zrobić?

Czy propozycja wydaje się zbyt korzystna, by była prawdziwa?

Czy ktoś prosi mnie o przekazanie pieniędzy w nietypowy sposób – np. poprzez kuriera, paczkomat, kod BLIK lub przelew „natychmiastowy”?

Czy coś mi tu nie pasuje? Zaufaj swoim przeczuciom. Zadaj pytania. Sprawdź.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Dekalog cyberbezpieczeństwa:

1. **Zatrzymuję się i daję sobie czas na przemyślaną decyzję.**
2. **Zawsze sprawdzam, z kim rozmawiam lub kto do mnie pisze.**
3. **Nie podaję danych osobowych, haseł ani kodów BLIK.**
4. **Nie klikam w podejrzane linki ani nie skanuję nieznanych kodów QR.**
5. **Nie wpuszczam obcych bez weryfikacji dokumentów.**
6. **Nie działam w pośpiechu ani pod wpływem presji.**
7. **Konsultuję się z rodziną lub sąsiadem, gdy coś mnie niepokoi.**
8. **Nie wierzę w oferty „za darmo” i "cudowne" leki i terapie.**
9. **Zgłaszam podejrzane sytuacje odpowiednim służbom.**
10. **Pamiętam, że mogę powiedzieć: NIE – i mam do tego pełne prawo.**

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

GDZIE SZUKAĆ POMOCY?

Zgłoś każde podejrzenie oszustwa, zwłaszcza gdy doszło do wyłudzenia pieniędzy!

Policja – numer alarmowy 112

CERT Polska

Zajmuje się cyberbezpieczeństwem i analizą zagrożeń.

Strona: www.cert.pl

E-mail: cert@cert.pl

Powiatowy Rzecznik Konsumentów w Zamościu

Udziela bezpłatnych porad prawnych w sprawach konsumenckich, może wytaczać powództwa na rzecz konsumenta.

ul. Przemysłowa 4, 22-400 Zamość

tel. 84 530 09 38

e-mail: rzecznik.konsumentow@powiatzamojski.pl

Godziny przyjęć: pon.-pt. 9:00–13:00

Miejski Rzecznik Konsumentów w Zamościu

ul. Partyzantów 10, pokój nr 320, tel. 84 677 24 22

e-mail: konsument@zamosc.pl

Powiatowy Rzecznik Konsumentów w Hrubieszowie

Starostwo Powiatowe, ul. Narutowicza 34, pokój nr 25, tel. (084) 696 50 68 (nr wewn. 25)

e-mail: bmatyka@powiathrubieszow.pl

Powiatowy Rzecznik Konsumentów w Tomaszowie Lubelskim

Starostwo Powiatowe, ul. Lwowska 68, pokój 36, tel. (84) 664 12 52 wew. 36

e-mail: starostwo@powiat-tomaszowski.com.pl

Pamiętaj: Nie kontaktuj się z oszustem. Nie odpowiadaj na jego wiadomości. Przerwij kontakt. Szukaj wsparcia – nie jesteś sam.

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI - CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO
W RAMACH RZĄDOWEGO PROGRAMU FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030