Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.53.2026
Warszawa, 01 kwietnia 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 4 marca br. Posłanki na Sejm RP Pani Olgi Ewy Semeniuk-Patkowskiej w sprawie rosnącej skali oszustw internetowych skierowanych przeciwko osobom starszym (interpelacja nr 15694)

Szanowny Panie Marszałku,

na wstępie pragnę poinformować, że Ministerstwo Cyfryzacji prowadziło prace nad nowelizacją ustawy o świadczeniu usług drogą elektroniczną, mającą na celu umożliwienie stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), dalej jako „DSA". 9 stycznia br. ustawa została zawetowana przez Prezydenta RP.

Celem ustawy było zwiększenie ochrony użytkowników internetu przed nielegalnymi treściami, poprzez umożliwienie wydawania nakazów podjęcia działań przeciwko nielegalnym treściom polegających na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich. Jako nielegalne zakwalifikowano m.in. treści wypełniające znamiona z art. 286 § 1 i 2 Kodeksu karnego, który dotyczy doprowadzenia do niekorzystnego rozporządzenia mieniem przez wprowadzenie w błąd. Obejmuje on phishing, oszustwa na platformach sprzedażowych.

Polska jest jednym z ostatnich krajów w Unii Europejskiej, które jeszcze nie zaimplementowały do krajowego porządku prawnego przepisów DSA. Weto Prezydenta uniemożliwiło ten proces.

Ministerstwo Cyfryzacji przygotowało nowe projekty wdrażające DSA. Przepisy zostały ujęte w dwóch projektach, aby przyspieszyć wdrożenie. Projekty ustaw zostały wpisane do wykazu prac legislacyjnych i programowych Rady Ministrów pod numerami UC140 i UC141. W dniach 6-20 lutego br. odbył się proces ich uzgodnień i konsultacji. Projekty zostały opublikowane na stronach RCL[1].

Poniżej przedstawiam odpowiedzi na zadane przez Posłankę pytania będące we właściwości Ministra Cyfryzacji.

Ad 1) Jak zmieniała się liczba przestępstw polegających na oszustwach internetowych skierowanych przeciwko osobom powyżej 60. roku życia w latach 2020–2025?

Statystyki dotyczące przestępstw, w tym przestępstw polegających na oszustwach internetowych, znajdują się w posiadaniu właściwych organów ścigania.

CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym), prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, będący jednostką nadzorowaną przez Ministra Cyfryzacji, zbiera jedynie zgłoszenia o zagrożeniach w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa[2]. Z posiadanych danych wynika, że

[1] https://legislacja.rcl.gov.pl/projekt/12406906 oraz https://legislacja.rcl.gov.pl/projekt/12406905
[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r. poz. 20)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

liczba incydentów wciąż rośnie. W 2020 r. liczba zgłoszeń wynosiła 33 729, natomiast w 2025 r. już 272 941 (ponad 8-krotny wzrost, w ciągu 5 lat). Warto w tym miejscu podkreślić, że ww. zgłoszenia incydentów często przekazywane są przez osoby, które nie padły ofiarami przestępstw, a jedynie prawidłowo rozpoznały działania cyberprzestępców. CSIRT NASK nie zbiera informacji o wieku osób zgłaszających. Wskazuję również, że zgłoszenia można składać anonimowo. W związku z powyższym, na podstawie informacji posiadanych przez Ministerstwo Cyfryzacji, nie da się oszacować, jak zmieniała się liczba przestępstw wymierzonych w seniorów i seniorki.

Ad 2) Jakie były łączne straty finansowe poniesione przez osoby starsze w wyniku oszustw internetowych w tym okresie?

Ministerstwo Cyfryzacji nie dysponuje danymi dotyczącymi łącznych strat finansowych ofiar oszustw internetowych.

Ad 3) Jakie są najczęstsze metody oszustw internetowych stosowanych wobec osób starszych według danych Policji oraz innych instytucji państwowych?

Osoby starsze najczęściej padają ofiarą zróżnicowanych ataków socjotechnicznych, wśród których dominują oszustwa inwestycyjne obiecujące szybkie zyski, uwiarygadniane bezprawnie wykorzystywanym wizerunkiem osób publicznych, polityków i spółek Skarbu Państwa.

Równie powszechnym zagrożeniem jest ewolucja tradycyjnej metody „na wnuczka", która obecnie przybiera formę oszustwa „na zepsuty telefon" realizowanego poprzez wiadomości SMS i komunikatory internetowe, gdzie sprawcy, podszywając się pod krewnych ofiar, wywierają presję czasową w celu pilnego wyłudzenia pieniędzy. Ponadto cyberprzestępcy masowo stosują ataki phishingowe, podszywając się pod firmy kurierskie domagające się drobnych dopłat do paczek, urzędy czy banki, co prowadzi do bezpośredniej kradzieży danych logowania i informacji o kartach płatniczych.

Seniorzy są również narażeni na manipulacje ze strony fałszywych doradców bankowych czy rzekomych funkcjonariuszy policji próbujących wywołać poczucie strachu i wymusić przekazanie danych, a także na tak zwane „recovery scams", czyli wtórne oszustwa celujące w osoby, które już wcześniej straciły oszczędności, kusząc je fałszywą obietnicą odzyskania utraconych środków.

Ad 4) Czy prowadzone są analizy dotyczące wpływu rosnącej dostępności internetu i bankowości elektronicznej na skalę przestępczości skierowanej przeciwko seniorom?

Ministerstwo Cyfryzacji nie prowadzi takich badań, natomiast wraz z postępem cyfryzacji internet stał się domeną wykorzystywaną także przez oszustów.

Ministerstwo Cyfryzacji wskazuje, że zagadnienia dotyczące przetwarzania danych osobowych przez banki w Polsce, w tym danych wykorzystywanych w procesach uwierzytelniania klientów oraz przeciwdziałania nadużyciom finansowym, należą przede wszystkim do właściwości Ministra Finansów, jako organu odpowiedzialnego za kształtowanie i nadzór nad ramami prawnymi funkcjonowania sektora bankowego, zarówno w wymiarze krajowym, jak i unijnym.

W szczególności Minister Finansów pozostaje właściwym adresatem w zakresie przedstawienia szczegółowych informacji dotyczących:

- podstaw prawnych i zakresów przetwarzania danych osobowych przez banki,
- obowiązków instytucji finansowych wynikających z przepisów regulujących działalność bankową oraz nadzór finansowy,

– praktyk stosowanych przez banki w celu zapobiegania nadużyciom i wyłudzeniom danych, w tym danych klientów należących do grup szczególnie narażonych, takich jak osoby starsze.

We właściwości tego bowiem organu znajdują się sektorowe przepisy krajowe i unijne regulujące szczegółowo te kwestie.

Ad. 5) Jakie działania edukacyjne prowadzone są obecnie przez administrację rządową w zakresie bezpieczeństwa cyfrowego osób starszych?

Ministerstwo Cyfryzacji prowadzi szkolenia w ramach inwestycji C2.1.3 „E-kompetencje", finansowanej z Krajowego Planu Odbudowy, dotyczące podstawowych kompetencji cyfrowych. Szkolenia skierowane są m.in. do obywateli oraz osób wykluczonych cyfrowo, do których zaliczają się także osoby starsze.W ramach szkoleń uczestnicy zdobywają m.in. umiejętności związane z cyberbezpieczeństwem. Inwestycja obejmuje również działania na rzecz podnoszenia kompetencji cyfrowych urzędników oraz nauczycieli.

Do II kwartału 2026 r. planowane jest przeszkolenie ok. 114,3 tys. obywateli oraz 54,5 tys. osób wykluczonych cyfrowo. Szkolenia realizowane są na terenie całego kraju.

W 2024 r. rozpoczęto także realizację projektu KRC – Kluby Rozwoju Cyfrowego, finansowanego z programu FERS. Kluby te mają pełnić funkcję lokalnych centrów rozwoju kompetencji cyfrowych, w których każdy obywatel będzie mógł nieodpłatnie uzyskać wsparcie oraz poradę w zakresie korzystania z technologii cyfrowych, a także rozwijać swoje umiejętności.

W 2025 r. uruchomiono 40 pilotażowych Klubów Rozwoju Cyfrowego w całej Polsce. Pod koniec 2026 r. planowane jest rozpoczęcie fazy skalowania projektu – docelowo powstać ma 2066 klubów w całym kraju. Będą one w sposób systemowy wspierać rozwój kompetencji cyfrowych Polaków, w tym osób wykluczonych cyfrowo, m.in. osób starszych.

Ministerstwo Cyfryzacji prowadzi również szereg działań informacyjnych i edukacyjnych mających na celu podnoszenie kompetencji cyfrowych wśród seniorów co w szerszej perspektywie wpływa na bezpieczne korzystania w technologii. Do takich działań należą:

1. **Projekt pn. Szkoła międzypokoleniowa**

Projekt jest realizowany z inicjatywy Ministerstwa Cyfryzacji, we współpracy z Ministerstwem Edukacji Narodowej oraz Pełnomocnikiem Rządu do spraw Polityki Senioralnej. Operatorem projektu jest NASK – Państwowy Instytut Badawczy.

Celem działań jest integracja międzypokoleniowa oraz rozwój kompetencji cyfrowych wśród osób starszych, przy wsparciu i zaangażowaniu uczniów klas VII–VIII szkół podstawowych oraz uczniów szkół ponadpodstawowych.

W okresie realizacji pilotażu przedsięwzięcia (lata 2024-2025) zorganizowano ponad 5,5 tys. warsztatów edukacyjnych, zaangażowano 1554 szkoły z całej Polski, udział wzięło ponad 20 tysięcy uczestników, w tym seniorzy i uczniowie. Zajęcia skupiały się na praktycznym rozwijaniu umiejętności korzystania z Internetu (w tym z usług cyfrowych), obsługi urządzeń cyfrowych oraz rozpoznawania zagrożeń online. Młodzież pełniła rolę przewodników cyfrowych, dzieląc się wiedzą i wspierając seniorów w nauce, jednocześnie korzystając z możliwości wymiany międzypokoleniowych doświadczeń.

Projekt będzie kontynuowany w kolejnych latach. W tym roku nabór do programu rusza 11 marca.

2. **Projekt szkoleniowy dla seniorów w sanatoriach pn. „eFajfy"**

Głównym celem projektu jest rozwój kompetencji cyfrowych seniorów. W ramach projektu dla przebywających w sanatoriach na terenie całej Polski osób, które ukończyły 60 lat zostaną zorganizowane i przeprowadzone bezpłatne szkolenia (teoretyczne oraz praktyczne z wykorzystaniem tabletów i/lub laptopów) z zakresu bezpieczeństwa w sieci i e-usług.

Wśród przykładowych modułów merytorycznych szkoleń są: wsparcie seniorów w pierwszych krokach z technologią (w tym zakładanie konta e-mail, instalacja komunikatorów oraz swobodniejsze poruszanie się po internecie), przedstawienie korzyści płynących z korzystania z profilu zaufanego oraz e-usług i aplikacji publicznych (w tym m.in. wsparcie w założeniu profilu zaufanego, prezentacja aplikacji mObywatel oraz Internetowego Konta Pacjenta), wprowadzenie w zagadnienia związane z podstawami bezpieczeństwa w internecie, temat phishingu i metody "na wnuczka" oraz zbudowanie pewności siebie oraz poczucia komfortu i bezpieczeństwa w korzystaniu z internetu, realizując codzienne potrzeby online, jak zakupy czy rozrywka. Projekt będzie kontynuowany w kolejnych latach.

Ponadto, rządowe kampanie edukacyjne przeznaczone dla osób starszych, prowadzone przez NASK-PIB i Ministerstwo Cyfryzacji, to m.in.:

- „Seniorze – spotkajmy się w sieci!" (https://www.gov.pl/web/seniorze-spotkajmy-sie-w-sieci) – Kampania NASK, w ramach której przygotowano broszury, nagrania wideo (serial online) oraz poradniki, mające na celu oswojenie osób starszych z internetem, pokazanie jego korzyści oraz edukację w zakresie bezpieczeństwa.

Ambasadorką kampanii jest znana i lubiana – Barbara Bursztynowicz. Filmy instruktażowe z jej udziałem wprowadzają do tematyki każdego z poszczególnych zagadnień, a broszury rozwijają i uzupełniają każdy z nich. Tematy wszystkich 5 filmów instruktażowych i 5 broszur zostały dobrane tak, aby pomóc seniorowi zidentyfikować zagrożenia w sieci i sposoby ich unikania. Pierwsze trzy tematy to bezpieczne korzystanie z rozrywki i komunikacji w sieci oraz bezpieczne załatwianie różnych spraw online. Kolejne dwa dotyczą sposobów na zabezpieczenie swoich danych w sieci, a także konkretnych metod oszustów w internecie. Dzięki takiemu ujęciu, senior będzie mógł rozpoznać zagrożenie, ale też dowie się, jak poradzić sobie z nim – sam lub przy wsparciu bliskich: dzieci czy wnuków.

- „#Halo! Tu cyberbezpieczny Senior" (https://bezpiecznymiesiac.pl/baza-wiedzy/halo-tu-cyberbezpieczny-senior/)- to Inicjatywa NASK, Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) oraz Warszawskiego Instytutu Bankowości, oferująca materiały edukacyjne (poradniki, webinaria) o tym, jak nie dać się oszukać w sieci.

Kampania była realizowana poprzez webinaria, warsztaty oraz specjalne spotkania poświęcone bezpiecznemu korzystaniu z internetu i telefonu. W ramach kampanii publikowano również cykl artykułów i infografik, w których wyjaśniane są najpopularniejsze rodzaje cyberprzestępstw i skuteczne sposoby zapobiegania cyfrowym zagrożeniom, w szczególności wyłudzeniom danych (m.in. z użyciem phishingu) oraz podszywania się pod zaufane podmioty (spoofingu).

Przygotowana została specjalna ulotka zawierająca najważniejsze informacje o oszustwach telefonicznych, w tym:

a) Kiedy zachować szczególną czujność?
b) O czym warto zawsze pamiętać?
c) Co zrobić, gdy odbierze się podejrzany telefon?

- „Buduj cyfrową formę klik po kliku" (https://kompetencjecyfrowe.gov.pl/cyfrowa-forma)– najnowsza ogólnopolska kampania z 2026 r., która zaprasza każdego Polaka, niezależnie od wieku, do rozwijania cyfrowych umiejętności we własnym tempie. W ramach niej odbywają się darmowe szkolenia z obsługi internetu i cyberbezpieczeństwa. Kampania jest szeroko obecna w mediach – w największych stacjach telewizyjnych i radiowych, w tym regionalnych, a także w internecie i na kanałach własnych Ministerstwa Cyfryzacji.

Ad 6) Ilu seniorów objęto programami edukacyjnymi dotyczącymi bezpiecznego korzystania z internetu w latach 2020–2025?

Do grudnia 2025 r. w ramach inwestycji C2.1.3 „E-kompetencje" przeszkolono łącznie 59 281 osób z grupy osób wykluczonych cyfrowo oraz pozostałych obywateli.

Nie jest możliwe dokładne określenie, jaki odsetek tej grupy stanowiły osoby starsze. Jednocześnie w ramach całej inwestycji C2.1.3 do końca grudnia 2025 r. kompetencje cyfrowe nabyło lub rozwinęło 21 790 osób starszych, co stanowi 31% wszystkich uczestników szkoleń w tym okresie.

W 2025 r., w ramach pilotażowych Klubów Rozwoju Cyfrowego, wsparciem szkoleniowym objęto 1 254 osoby. Spośród nich 318 osób nabyło lub podniosło swoje kompetencje cyfrowe. Nie są dostępne dane dotyczące udziału osób starszych w tej grupie.

W ramach projektu eFajfy realizowanego w 2025 roku przeszkolono 1 015 seniorów w 76 sanatoriach.

Natomiast w trakcie pilotażu projektu pn. Szkoła Międzypokoleniowa przeszkolono 10 349 seniorów.

Ad 7) Czy prowadzone są programy wsparcia dla osób starszych w zakresie bezpiecznego korzystania z bankowości elektronicznej i usług cyfrowych?

W Polsce obowiązuje rządowy Program Rozwoju Kompetencji Cyfrowych, w ramach którego realizowany jest Priorytet II – „Zapewnienie każdemu możliwości rozwoju kompetencji cyfrowych". Priorytet ten skierowany jest m.in. do osób rozpoczynających korzystanie z technologii cyfrowych oraz osób wykluczonych cyfrowo, w tym osób starszych.

W ramach tego priorytetu realizowane były wspomniane wcześniej m.in. następujące działania:

II.2.1 – rozwój kompetencji cyfrowych osób wykluczonych, osób z niepełnosprawnościami oraz osób o niskim poziomie kompetencji cyfrowych,

II.1.5 – szkolenia dla obywateli z zakresu kompetencji cyfrowych,

II.1.1 – systemowe wsparcie edukacji cyfrowej dorosłych użytkowników ICT poprzez Kluby Rozwoju Cyfrowego.

Obecnie planowana jest rewizja Programu, w ramach której przewidziane są również nowe działania skierowane do seniorów, obejmujące rozwijanie kompetencji cyfrowych oraz umiejętności związanych z cyberbezpieczeństwem.

Jednym z planowanych działań jest „Szkoła międzypokoleniowa" (realizacja do 2030 r.), której celem jest wspieranie rozwoju kompetencji cyfrowych seniorów przez uczniów i nauczycieli szkół podstawowych i ponadpodstawowych. W ramach programu seniorzy otrzymują wsparcie w poruszaniu się po świecie cyfrowym, uczą się bezpiecznego korzystania z internetu oraz unikania zagrożeń, takich jak phishing czy oszustwa metodą „na wnuczka", a także poznają praktyczne zastosowania technologii w codziennym życiu.

Planowane jest również działanie EFAJFY (realizacja do 2030 r.), polegające na organizacji bezpłatnych szkoleń teoretycznych i praktycznych z wykorzystaniem tabletów i laptopów. Szkolenia będą dotyczyć bezpieczeństwa w sieci oraz korzystania z e-usług i będą skierowane do seniorów powyżej 60. roku życia przebywających w sanatoriach na terenie Polski.

Ministerstwo Cyfryzacji nie prowadzi działań mając bezpośredni wpływ na bezpieczeństwo seniorów w kontekście wyłudzania danych wrażliwych. Prowadzi jednak szereg działań informacyjnych i edukacyjnych mających na celu podnoszenie kompetencji cyfrowych wśród seniorów co w szerszej perspektywie wpływa na bezpieczne korzystania w technologii.

Ministerstwo Cyfryzacji realizuje systemowe podejście oparte na trzech filarach: kompetencjach, bezpieczeństwie i infrastrukturze. Działania obejmują wszystkie grupy wiekowe – od uczniów szkół podstawowych, przez nauczycieli, po seniorów. Działania kierowane do seniorów to m.in.:

- Wskazana wcześniej kampania **„Buduj cyfrową formę klik po kliku".**
- **Szkoła Międzypokoleniowa** – gdzie młodzież uczy seniorów. W okresie pilotażu przedsięwzięcia w 1554 szkołach z całej Polski przeprowadzono 5,5 tys. warsztatów dla ponad 10 tys. osób starszych (20 tys. uczestników – uczniów i seniorów). Inicjatywa ta jest realizowana we współpracy z Ministerstwem Edukacji Narodowej oraz Ministrem do spraw Polityki Senioralnej. Operatorem projektu jest NASK – PIB. W jej ramach uczniowie pod przewodnictwem nauczycieli przeprowadzają dla seniorów praktyczne warsztaty. Młodzież pełniła rolę przewodników cyfrowych, dzieląc się wiedzą i wspierając seniorów w nauce, jednocześnie korzystając z możliwości wymiany międzypokoleniowych doświadczeń.
- **Kluby Rozwoju Cyfrowego** – które działają przy istniejących instytucjach, np. bibliotekach, świetlicach, domach kultury, i oferują szkolenia oraz pomoc w korzystaniu z nowych technologii;
- **e-Fajfy** – bezpłatne, cyfrowe szkolenia (teoretyczne oraz praktyczne z wykorzystaniem tabletów i/lub laptopów) z zakresu bezpieczeństwa w sieci i e-usług dla seniorów (60+) przebywających w sanatoriach na terenie Polski. Wśród przykładowych modułów merytorycznych szkoleń są: wsparcie seniorów w pierwszych krokach z technologią (w tym zakładanie konta e-mail, instalacja komunikatorów oraz swobodniejsze poruszanie się po internecie), przedstawienie korzyści płynących z korzystania z profilu zaufanego oraz e-usług i aplikacji publicznych (w tym m.in. wsparcie w założeniu profilu zaufanego, prezentacja aplikacji mObywatel oraz Internetowego Konta Pacjenta), wprowadzenie w zagadnienia związane z podstawami bezpieczeństwa w internecie, temat phishingu i metody "na wnuczka" oraz zbudowanie pewności siebie oraz poczucia komfortu i bezpieczeństwa w korzystaniu z internetu, realizując codzienne potrzeby online, jak zakupy czy rozrywka.;
- **platformę OSE IT Szkoła** – oferującą bezpłatne kursy online z programowania, bezpieczeństwa i AI. Skorzystało z nich już ponad 338 tys. użytkowników, realizując 2,3 mln kursów;
- **projekt e-Kompetencje** – szkolenia dla nauczycieli, które do końca 2026 r. obejmą 55 000 pedagogów w całej Polsce. Ważne, aby edukować dzieci, które później przekażą wiedzę rodzicom i dziadkom;
- **Webinaria finansowe CEDUR** - CSIRT KNF organizuje w ramach Centrum Edukacji dla Uczestników Rynku (CEDUR) darmowe szkolenia dedykowane

wprost seniorom i ich opiekunom, takie jak „Bezpieczny senior – jak nie dać się oszukać w Internecie" oraz dotyczące bezpiecznej bankowości elektroniczne;

- **Kampania radiowa pn. *W cyfrowym świecie*** - W 2024 roku Ministerstwo Cyfryzacji przeprowadziło cykl 7 audycji regionalizowanych. Razem 119 audycji produkowanych regionalnie. Natomiast w 2025 roku był to cykl 8 audycji radiowych emitowanych w 17 Rozgłośniach Regionalnych Polskiego Radia, co sumarycznie dało 136 audycji produkowanych regionalnie. Kampania była skierowana do osób dorosłych, z naciskiem na ludzi w wieku 55+. Kampania miała na celu m.in. zachęcenie obywateli do ciągłego podnoszenia kompetencji cyfrowych, podnoszenie świadomości obywateli o zagrożeniach i problemach występujących w świecie cyfrowym oraz zbudowanie przekonania o konieczności świadomego i bezpiecznego korzystania z szeroko rozumianej technologii.

Ad 8) Jak wygląda współpraca administracji publicznej z bankami i operatorami telekomunikacyjnymi w zakresie przeciwdziałania oszustwom internetowym skierowanym przeciwko osobom starszym?

Współpraca administracji publicznej z bankami i operatorami telekomunikacyjnymi w zakresie ochrony obywateli, w tym szczególnie osób starszych, opiera się na rozwiązaniach prawnych, współdzieleniu technologii blokujących zagrożenia oraz na dedykowanych kampaniach edukacyjnych.

Pod pojęciem nadużycia w komunikacji elektronicznej, o którym mowa w ustawie o zwalczaniu nadużyć w komunikacji elektronicznej[3], należy rozumieć świadczenie lub korzystanie z usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi lub osiągnięcie nienależnych korzyści dla podmiotu dopuszczającego się nadużycia w komunikacji elektronicznej, innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Ustawa penalizuje zdefiniowane w niej nadużycia w komunikacji elektronicznej, którymi są m.in.: smishing, CLI spoofing i tworzenie sztucznego ruchu.

Przepisy ww. ustawy przeciwdziałają oszustwom dokonywanym na szkodę m.in. seniorów. Ograniczają liczbę fałszywych telefonów, w których oszust podszywał się pod pracownika banku. Blokują fałszywe SMS z linkami do płatności za rzekomo niezapłacony rachunek. Identyfikują i blokują fałszywe strony internetowe banków i instytucji publicznych.

Na mocy Ustawy CSIRT NASK blisko współpracuje z operatorami telefonii komórkowej.

Obywatele mogą zgłaszać podejrzane SMS-y na bezpłatny numer **8080**. Na ich podstawie analitycy tworzą wzorce złośliwych wiadomości, które w ciągu kilku minut są pobierane przez operatorów telekomunikacyjnych, mających prawny obowiązek blokowania takich SMS-ów, zanim dotrą one do potencjalnej ofiary.

Niezbędna jest ciągła kampania informacyjna o możliwości zgłaszania fałszywych wiadomości SMS do CSIRT NASK.

W 2025 r. CSIRT NASK stworzył 790 wzorców złośliwych wiadomości[4]. Na ten moment widzimy stały wzrost efektywności blokowania wiadomości. Po wprowadzeniu mechanizmu blokowania wiadomości smishingowych oszuści starają się omijać blokady

[3] ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803) (dalej: „Ustawa")
[4] https://dane.gov.pl/pl/dataset/3828/resource/1035909,statystyki-sms-ow-obsuzonych-przez-cert-polska-oraz-liczba-wytworzonych-wzorcow-faszywych-wiadomosci-sms-122025/table?page=1&per_page=20&q=&sort=

operatorów zmieniając treść wiadomości, np. poprzez dodawanie nietypowych znaków specjalnych, błędy składniowe oraz celowe literówki, co w rezultacie znacząco obniża ich wiarygodność.

Mechanizm blokowania wiadomości smishingowych należy ocenić pozytywnie, umożliwia on efektywną walkę ze smishingiem.

Ustawa umożliwia podmiotom publicznym zastrzeżenie swojego nadpisu SMS (SMS sender ID) w wykazie nazw i ich skrótów zastrzeżonych dla podmiotów publicznych jako nadpis wiadomości pochodzącej od tego podmiotu publicznego. Wykaz ten jest prowadzony przez CSIRT NASK. Zastrzeżenie nadpisu jest fakultatywne. Podmiot publiczny, który zastrzegł nadpis jest obowiązany do korzystania z usług integratorów usług SMS wpisanych do wykazu integratorów usług SMS dla podmiotów publicznych.

W wykazie nadpisów jest obecnie wpisanych ok. 332 nadpisów (stan na 13.02.2026 r.). Wydaje się, że rozwiązanie to wymaga większej promocji wśród podmiotów publicznych, szczególnie wśród jednostek samorządu terytorialnego.

CSIRT NASK prowadzi Listę Ostrzeżeń przed niebezpiecznymi stronami. Operatorzy sieci wykorzystują tę listę do automatycznego blokowania wejść na złośliwe witryny na poziomie domeny, chroniąc nieświadomych użytkowników przed wyłudzeniem danych. Zespół CSIRT KNF (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora finansowego) na bieżąco monitoruje sieć pod kątem oszustw wycelowanych w klientów banków (np. fałszywe reklamy inwestycyjne). Wykryte strony są natychmiast przekazywane do CSIRT NASK w celu ich zablokowania na Liście Ostrzeżeń.

Uruchomiona została usługa „Zastrzeż Pesel". Od 1 czerwca 2024 r. instytucje finansowe, w tym banki, mają ustawowy obowiązek weryfikacji statusu PESEL klienta przed udzieleniem kredytu czy pożyczki. Skutecznie chroni to osoby starsze przed zaciągnięciem na nie zobowiązań finansowych w wyniku kradzieży tożsamości.

Z perspektywy ochrony danych osobowych Ministerstwo Cyfryzacji wskazuje, że działalność banków podlega ogólnym zasadom przetwarzania danych określonym w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)[5], w szczególności zasadzie legalności, rzetelności i przejrzystości, zasadzie minimalizacji danych oraz zasadzie integralności i poufności. Zasady te zobowiązują wszelkich administratorów danych osobowych (nie tylko banki) do wdrażania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych, z uwzględnieniem podejścia opartego na ryzyku.

RODO nie wprowadza jednak sektorowych ani technicznych rozwiązań dedykowanych konkretnym metodom wyłudzeń danych, takim jak vishing czy spoofing. Ocena i przeciwdziałanie tego rodzaju zagrożeniom, w tym stosowanie środków technicznych i organizacyjnych w środowiskach teleinformatycznych, pozostają w kompetencjach właściwych podmiotów odpowiedzialnych za cyberbezpieczeństwo.

Ministerstwo Cyfryzacji podkreśla jednocześnie, że obowiązujące ramy prawne w zakresie ochrony danych osobowych zapewniają spójne i wystarczające podstawy do ochrony danych klientów banków, w tym osób starszych, a ewentualne działania w tym obszarze powinny koncentrować się przede wszystkim na skutecznym stosowaniu obowiązujących przepisów oraz na współpracy właściwych organów i instytucji w ramach ich kompetencji. Należy również podkreślić, że dane finansowe nie stanowią „danych

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

wrażliwych” w świetle przepisów RODO. Zgodnie z art. 9 RODO dane osobowe szczególnej kategorii („dane wrażliwe”) to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Ponadto należy zwrócić uwagę na to, że numer telefonu nie jest szyfrowany. Oszust może podszyć się pod numer telefonu innej osoby lub instytucji za pomocą internetowych bramek telefonicznych – w tym celu podstawia inny numer, wtedy ofiara widząc na ekranie telefonu znajomy numer może nieświadomie uznać, że dzwoni bliska osoba albo bank, czy inna instytucja. Przestępca wykorzystując zaufanie odbiorcy może ją nakłonić do przekazania danych osobowych, danych o koncie bankowym, haseł i doprowadzić do szkody majątkowej lub osobistej. Takie działania określa się jako CLI spoofing.

Połączenia mające charakter CLI spoofing są blokowane albo usuwana jest prezentacja numeru (CLIR). To ostatnie zachodzi w sytuacji, gdy istnieje duże prawdopodobieństwo, że połączenie ma charakter CLI spoofing, ale dane sygnalizacyjne nie dają pewności. Usunięcie prezentacji powoduje, że numer wyświetla się na ekranie telefonu jako numer zastrzeżony, co powinno wywołać wątpliwości u odbiorcy czy nie ma do czynienia z oszustwem.

We wrześniu 2024 r. przedsiębiorcy telekomunikacyjni – operatorzy sieci mobilnej wdrożyli rozwiązania tzw. Bezpiecznej Zatoki, która umożliwia identyfikację, wymianę informacji oraz blokowanie fałszywych połączeń. Szczegóły techniczne dotyczącego tego rozwiązania znajdują się w Porozumieniu operatorów sieci mobilnej z Prezesem Urzędu Komunikacji Elektronicznej[6]. Dla mniejszych przedsiębiorców telekomunikacyjnych Prezes Urzędu Komunikacji Elektronicznej wydał rekomendacje określające środki zwalczające fałszywe połączenia głosowe[7].

Na podstawie danych od przedsiębiorców telekomunikacyjnych zrzeszonych w Polskiej Izbie Informatyki i Telekomunikacji możemy wskazać, że w 2024 r. ci przedsiębiorcy telekomunikacyjni:

- blokowali około 500 tys. połączeń dziennie,
- usuwali prezentację około 700 tys. połączeń dziennie.

Dane za 2025 r. jeszcze nie są dostępne.

Rozwiązanie należy uznać za pozytywne, jednakże jego praktyka wymaga dopracowania – odbierane są pojedyncze sygnały od przedsiębiorców telekomunikacyjnych, że niektóre połączenia były blokowane niezasadnie.

Ustawa dała podstawę do funkcjonowania wykazu numerów służących wyłącznie do odbierania połączeń głosowych. Wykaz ten jest prowadzony przez Prezesa Urzędu Komunikacji Elektronicznej. Wykaz ma służyć ograniczeniu podszywania się pod numery infolinii np. banków czy urzędów – te numery nie służą do dzwonienia do klientów. Zdarzały się jednak przypadki, że oszust wykorzystywał numer infolinii banku i dzwonił do nieświadomej ofiary przedstawiając się jako pracownik banku. Przedsiębiorca telekomunikacyjny ma obowiązek automatycznie blokować numer wpisany do wykazu. Obecnie w wykazie widnieje 66 numerów. Niezbędna jest akcja promocyjna tego rozwiązania.

Ad 9) Czy rozważane jest wprowadzenie dodatkowych mechanizmów ochronnych dla osób starszych korzystających z bankowości elektronicznej i usług cyfrowych?

Ministerstwo Cyfryzacji prowadziło prace nad nowelizacją ustawy o świadczeniu usług drogą elektroniczną, mającą na celu umożliwienie stosowania przepisów rozporządzenia

[6] https://uke.gov.pl/akt/porozumienie-prezesa-uke-i-operatorow-w-sprawie-cli-spoofingu,522.html
[7] https://bip.uke.gov.pl/bezpieczenstwo/rekomendacje-prezesa-uke-dotyczace-cli-spoofing,23.html

Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), dalej jako „DSA". 9 stycznia br. ustawa została zawetowana przez Prezydenta RP.

Celem ustawy było zwiększenie ochrony użytkowników internetu przed nielegalnymi treściami, poprzez umożliwienie wydawania nakazów podjęcia działań przeciwko nielegalnym treściom polegających na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich. Jako nielegalne zakwalifikowano m.in. treści wypełniające znamiona z art. 286 § 1 i 2 Kodeksu karnego, który dotyczy doprowadzenia do niekorzystnego rozporządzenia mieniem przez wprowadzenie w błąd. Obejmuje on phishing, oszustwa na platformach sprzedażowych.

Polska jest jednym z ostatnich krajów w Unii Europejskiej, które jeszcze nie zaimplementowały do krajowego porządku prawnego przepisów DSA. Weto Prezydenta uniemożliwiło ten proces.

Ministerstwo Cyfryzacji przygotowało nowe projekty wdrażające DSA. Przepisy zostały ujęte w dwóch projektach, aby przyspieszyć wdrożenie. Projekty ustaw zostały wpisane do wykazu prac legislacyjnych i programowych Rady Ministrów pod numerami UC140 i UC141. W dniach 6-20 lutego br. odbył się proces ich uzgodnień i konsultacji. Projekty zostały opublikowane na stronach RCL[8].

Ad 10) Czy Ministerstwo planuje opracowanie kompleksowej strategii bezpieczeństwa cyfrowego osób starszych w związku ze starzeniem się społeczeństwa?

Ad 11) Jak Ministerstwo ocenia przygotowanie instytucji publicznych do przeciwdziałania rosnącej skali przestępczości internetowej skierowanej przeciwko seniorom?

Poza kontynuowaniem i rozwijaniem już rozpoczętych kampanii i inicjatyw, Ministerstwo Cyfryzacji oraz inne instytucje państwowe wdrażają szeroki pakiet systemowych projektów i inicjatyw praktycznych, które mają chronić seniorów. Zagadnienia edukacji i ochrony obywateli będą również częścią ogólnokrajowych dokumentów: przyjętej *Strategii Cyberbezpieczeństwa RP* oraz przygotowywanej *Strategii Cyfryzacji Państwa.*

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[8] https://legislacja.rcl.gov.pl/projekt/12406906 oraz https://legislacja.rcl.gov.pl/projekt/12406905