

Seniorze nie daj się oszukać!

Drodzy Seniorzy! Zachęcamy do zapoznania się z Kampanią „Stop manipulacji, nie daj się oszukać!” prowadzoną przez Stowarzyszenie MANKO, która ma na celu edukować i ostrzegać seniorów przed nieuczciwymi praktykami oszustów i przestępców.

W czasie pandemii seniorzy nie są tylko narażeni na wirusy, ale także na nieetyczne praktyki biznesowe. Od marca 2020 roku przestępcy dwoją się i troją, aby wykorzystać lęk, panikę i izolację seniorów w Polsce. Co chwilę powstają nowe techniki manipulacyjne. Niestety wyjątkowa sytuacja powoduje, że do „pomocy” seniorom włączają się również oszuści, dostrzegając szybki i łatwy zysk w obliczu wybuchu społecznej paniki. Wszechobecny lęk, szczególnie wśród osób w wieku 60+, skrzętnie wykorzystują manipulatorzy na wielu płaszczyznach. Działają w Internecie, ale też w kontakcie bezpośrednim. Do tej pory oszuści wymyślili ponad 30 różnych modyfikacji technik manipulacyjnych. Informacje na ten temat spływają do policji z całej Polski.

Wspierajmy, edukujmy, ostrzegajmy.

Oto przykładowe techniki manipulacyjne powstałe TYLKO w trakcie pandemii:

1. FAŁSZYWE SZCZEPIONKI

Mężczyzna oferował ampułki szczepionki na COVID-19 za 8 tys. zł. Oszust twierdził, że ma nieograniczony dostęp do szczepionek i posiada odpowiedni certyfikat. W trakcie spotkania oszust przekonywał, że szczepionka jest bezpieczna i wystarczy dla 4 osób.

2. OSZUSTWO NA DEZYNFEKCJĘ PRZESYŁKI

Otrzymujemy sms, telefon lub maila z prośbą o dopłatę niewielkiej kwoty w celu dezynfekcji przesyłki. Jeśli nie wpłacimy wróci ona do nadawcy. Ofiara wchodzi w link zamieszczony w wiadomości i podaje swoje dane, aby zrealizować przelew. W ten sposób wyłudzacze zdobywają dane do konta bankowego

3. OSZUSTWO NA DEZYNFEKCJĘ MIESZKANIA

Tym razem złodzieje przebrani w kombinezony, wyposażeni w rękawice i okulary ochronne pukają do drzwi i proponują dezynfekcję mieszkań. Później natomiast, po opuszczeniu mieszkań przez ich lokatorów – plądrują i kradną.

4. MASECZKA ZE SREBRA

Na rynku pojawiły się specjalne, drogie maseczki w 100% zabezpieczające przed wirusem z cząsteczkami nano-srebra. Oczywiście maseczki z cudownego materiału to oszustwo.

5. OSZUSTWO NA CHOREGO WNUCZKA

Jest to zmieniona metoda oszustwa „na wnuczka”. Oszust dzwoni z prośbą o jak najszybsze opłacenie jego testów na koronawirusa lub całego leczenia. Senior ma przekazać pieniądze „koledze wnuczka” lub wykonać przelew. Pieniądzy nigdy nie odzyska.

6. „NA NIEDOPŁATĘ ZA GAZ I PRĄD”

Oto wiadomość od naszej ambasadorki: Uwaga dostałam dziś takiego oszukańczego SMS: „PGNiG: Informujemy, że w związku z zadłużeniem na kwotę 12,45 zł na najbliższy dzień roboczy zleciliśmy odłączenie gazu. Zapłać teraz na link...” – oczywiście jest to kolejna próba wyłudzenia pieniędzy.

7. CUDOWNE LEKI NA KORONAWIRUSA

W związku z obecną sytuacją epidemiczną, wielu oszustów wykorzystuje nasz niepokój o zdrowie, oferując sprzedaż fałszywych leków lub produktów, rzekomo zapobiegających zarażeniu się koronawirusem, w niewiarygodnie wysokich cenach. Warto przed zakupem jakichkolwiek leków konsultować się z lekarzem oraz kupować wyłącznie w aptekach.

8. PREZENTACJE SPRZEDAŻOWE – GRATISY

Po odmrożeniu gospodarki znowu w najlepsze kwitnie sprzedaż drogich garnków i sprzętu AGD podczas tzw. prezentacji. Dlatego ponownie ostrzegamy przed pokazami sprzedażowymi! Seniorze, pamiętaj: nie ma NIC ZA DARMO. Żadna firma nie działa charytatywnie. Dlatego uważaj na hasła: BEZPŁATNE BADANIA, PREZENTY, GRATISY, NIEPOWTARZALNE OKAZJE. To tylko kuszące wabiki, które mają skłonić Cię do wyjścia z domu mimo epidemii i udziału w pozornie atrakcyjnym spotkaniu. W rzeczywistości chodzi o prezentację oferty handlowej i sprzedaż produktów w horrendalnych cenach.

9. FAŁSZYWE E-MAILE

Policja ostrzega przed fałszywymi wiadomościami na elektronicznej skrzynce pocztowej, które informują o wezwaniu na Policję. Pobranie oraz otwarcie załączonego pliku może spowodować, że komputer zostanie zainfekowany złośliwym oprogramowaniem. To z kolei może doprowadzić do kradzieży naszych danych osobowych lub zablokowania komputera. Następnie oszuści żądają okupu za odblokowanie go

10. „PRACOWNICY” BANKU

Przestępcy nakłaniają swoje ofiary do pobrania aplikacji, która nielegalnie pobiera ich dane. Dodatkowo, oszuści proszą o podanie danych bankowych. Konsultanci banku nigdy nie zachęcają do pobierania żadnych aplikacji do szybkiej obsługi klienta. Konsultant nigdy nie zaloguje się do systemu za Ciebie – loguj się do konta wyłącznie na stronie banku. Konsultant infolinii nigdy nie prosi o podanie poufnych danych np. numerów dokumentów, numeru karty płatniczej czy kodu CVV.

11. FAŁSZYWE ZABEZPIECZENIA FINANSOWE

W związku z rosnącą dobową liczbą osób zakażonych, oszuści oferują liczne zabezpieczenia finansowe, które przypominają ubezpieczenia. Przestępcy przekonują, że ich usługa będzie służyć nabywcom przez cały okres pandemii i zachowają oni płynność finansową w tym czasie. Te osoby są manipulowane, że wykupienie takiej usługi jest dla nich niezbędne, aby przeżyć w obecnej sytuacji.

12. ODWOŁYWANE WYDARZENIA

Oszuści podszywający się pod organizatorów wycieczek, spektakli teatralnych czy koncertów nakłaniają ludzi do odzyskania pieniędzy z powodu odwołania lub zmiany terminu zarezerwowanej przez klienta atrakcji. W takiej sytuacji najlepiej się rozłączyć i podjąć próbę kontaktu bezpośrednio z firmą, z którą zawarliśmy umowę.

13. FAŁSZYWE ZBIÓRKI

Po sieci krążą informacje zachęcające do wsparcia zbiórek pieniędzy na różne, szczytne cele. W dobie pandemii, oszuści podszywają się pod organizacje społeczne i próbują wyłudzić pieniądze na walkę z koronawirusem. Przed dokonaniem jakiegokolwiek wpłaty należy sprawdzić wiarygodność akcji i zweryfikować informacje na temat organizatora zbiórki.

14. PRZESYŁKA OLX

Oszust wysyła wiadomość do ofiary za pomocą aplikacji WhatsApp (wykorzystując numer podany w ofercie na stronie OLX). Oszust pyta czy ogłoszenie jest aktualne oraz wyraża chęć zakupu produktu za pomocą usługi „Przesyłka OLX”, a następnie wysyła sfalszowane zdjęcie ze strony OLX, gdzie wytłumaczone jest co trzeba zrobić, aby skorzystać z usługi. Oszust wysyła również fałszywy link do strony, gdzie sprzedający może odebrać pieniądze za towar. Na podanej stronie ofiara musi podać swoje dane karty bankowej, które później oszust wykorzystuje, aby ukraść pieniądze z jej konta.

15. SMS WYŚLANY Z TRYBU ALARMOWEGO SOS

Tym razem oszuści wykorzystują tryb Alarmowego SOS, który jest dostępny w praktycznie każdym smartfonie. Użytkownik smartfona może w ustawieniach dodać numery telefonicznie osób, na które przyjdzie specjalne powiadomienie SMS w sytuacji alarmowej. Oszust może wykorzystać tryb Alarmowego SOS, aby wysłać na przypadkowe numery SMS-y z linkiem do strony internetowej. Po kliknięciu w link, ofiara zostaje przekierowana na podejrzaną stronę internetową, która ma na celu wyłudzenie pieniędzy.

16. SMS OD FIRMY KURIERSKIEJ

Coraz częściej złodzieje podszywają się pod firmę kurierską i wysyłają wiadomości o podobnej treści: „Twoje zamówienie nie może zostać dostarczone! Podwód; przekroczony wymiar opakowania. Aby zrealizować zamówienie, zapłać 1,18 zł”. Oprócz tego w SMSie podany jest link, który przekierowuje do strony bankowości elektronicznej. Po wpisaniu danych wrażliwych, oszust uzyskuje dostęp do konta bankowego, skąd kradnie oszczędności ofiary.

17. FAŁSZYWE POWIADOMIENIA Z MEDIÓW SPOŁECZNOŚCIOWYCH

Oszuści często wysyłają fałszywe powiadomienia, podszywając się pod popularne sieci społecznościowe. Poruszają w nich temat nowych znajomych, ich aktywności, komentarzy czy polubień. Bardzo trudno jest odróżnić takie wiadomości od oryginalnych. Jedyna różnica jest taka, że fałszywe powiadomienie posiada specjalny odnośnik. Jeśli ofiara w niego kliknie, zostaje przekierowana na kolejną stronę, gdzie musi podać swoje dane do logowania na portal społecznościowy. Następnie takie dane są wykorzystywane przez oszusta do własnych celów.

18. FAŁSZYWE INWESTYCJE W INTERNECIE

Hasło: „Inwestycja z gwarancją szybkiego zysku, bez wychodzenia z domu” brzmi podejrzenie, jednak wciąż są ludzie, którzy wierzą w takie oferty! Firma „X” zamieszcza swoją reklamę w Internecie. Oferuje inwestycje kapitału w euro w m.in. złoto. Przedsięwzięcie najczęściej jest promowane przez znaną osobę (zdjęcie wykorzystane bez zgody tej osoby) – co wzbudza ciekawość odbiorcy. Oszust kontaktuje się z ofiarą i namawia, do zainwestowania pieniędzy, argumentując, że inwestycja jest bardzo korzystna. Po zainwestowaniu pieniędzy, ofiara nigdy nie dostaje zwrotu zainwestowanych pieniędzy, ani zysków. W innym wariantcie oszustwa, ofiara początkowo dostaje na konto niewielkie zyski, aby upewnić ją, że przedsięwzięcie jest legalne.

19. „NA KŁÓDKĘ”

Oszust montuje kłódkę na klamkach samochodów zaparkowanych np. na parkingu galerii handlowej. Oprócz kłódki oszust zostawia także list, w którym za zdjęcie kłódki żąda pieniądze (np. 400 zł). Ofiara, aby uzyskać szyfr do kłódki, musi przekazać pieniądze na podany numer poprzez Blik. Policja informuje, by nie dać się zmanipulować, a każdą próbę tego typu oszustwa należy zgłaszać.

20. „NA INKASENTA/ADMINISTRACJĘ”

W tym wypadku oszust podszywa się pod inkasenta, pracownika urzędu lub też innej instytucji. Najczęściej jednak złodzieje udają pracowników socjalnych/ZUS i odwiedzają seniorów pod pretekstem wypłaty dodatkowego świadczenia pieniężnego. Aby dostać oferowane pieniądze oszust nakłania ofiarę do wniesienia opłaty manipulacyjnej albo przekazanie pieniędzy na zakup znaczków pocztowych. W ten sposób oszust dowiaduje się, gdzie ofiara trzyma swoje oszczędności. Następnie złodziej prosi o szklanek wody, a w czasie nieobecności właściciela mieszkania okrada go.

21. „NA DOSTAWCĘ USŁUG TELEKOMUNIKACYJNYCH”

Do mieszkania ofiary przychodzi osoba podająca się za przedstawiciela firmy telekomunikacyjnej. Oszust jest bardzo wiarygodny – sprawdza dane, prosi o ostatnią fakturę za usługę i dowód osobisty. Następnie oszust stwierdza, że dotychczasowa umowa wygasa i podsuwa ofierze dokument do podpisu. Po podpisaniu okazuje się, że ofiara nieświadomie zmieniła dostawcę usług telekomunikacyjnych, a atrakcyjna oferta, którą oferował przedstawiciel okazuje się znacznie droższa od poprzedniej.

22. „NA SPRZEDAWCĘ PERFUM”

Domokrążca – osoba podająca się za sprzedawcę perfum puka do mieszkania starszej osoby. Oszust zachwala produkt, który sprzedaje i zachęca ofiarę do powąchania zapachu. Perfumy okazują się być substancją chemiczną, a po powąchaniu jej można stracić przytomność. W międzyczasie złodziej przeszukuje mieszkanie i kradnie wszystkie cenne przedmioty.

23. PILNY KONTAKT Z SANEPIDEM

Oszuści wysyłają SMSa z informacją o konieczności kontaktu z Sanepidem poprzez podany numer. Podany w wiadomości numer okazuje się numerem premium co oznacza, że takie

połączenie może kosztować aż 35 zł za 1 minutę. Sanepid nie wysyła wiadomości o takiej treści – takie SMSy najlepiej usunąć, a próbę oszustwa zgłosić na policję.

24. „NA WALKĘ Z KORONAWIRUSEM”

Oszustwo związane z walką z koronawirusem działa na podobnej zasadzie co inne SMSowe oszustwa od osób podających się za kuriera lub wierzyciela. Ofiara dostaje SMSa z informacją, że zgodnie ze specjalną ustawą dotyczącą koronawirusa jej środki znajdujące się na koncie bankowym zostają przekazane do rezerw krajowych Narodowego Banku Polskiego i aby zachować swoje pieniądze należy zalogować się na podany w wiadomości link. W efekcie oszust dostaje dostęp do konta swojej ofiary i jest w stanie ukraść znajdujące się na nim pieniądze.

25. ZDALNY PULPIT

W tego rodzaju oszustwach chodzi o to, aby zachęcić ofiarę perspektywą łatwego i szybkiego zysku i namówić ją na zainstalowanie w pełni legalnego i uczciwego programu do zdalnej obsługi komputera, bądź nakłonić do udostępnienia danych do logowania do banku. W niektórych przypadkach oszuści dzwonią do ofiary podając się za konsultantów z banku i informują o jakiś komplikacjach. Wtedy „konsultant” proponuje wsparcie ofiary poprzez usługę „zdalnego pulpitu”.

26. „NA WYPADEK”

Oszuści kontaktują się z osobami starszymi, podając się za osoby z rodziny i proszą o pomoc finansową. W trakcie rozmowy tłumaczą, że uległy wypadkowi i potrzebują pilnie dużego zastrzyku gotówki. W umiejętny sposób zyskują zaufanie seniorów i wzbudzają poczucie fałszywej solidarności. Ofiara decyduje się na przekazanie środków finansowych, a oszust nagle znika z pokaźną sumą pieniędzy.

27. „NA KARTĘ SIM”

Na początku, oszust musi przekonać operatora, że jest tym, za kogo się podaje, a więc prawowitym właścicielem danego numeru. W ten sposób wyłudza duplikat karty SIM. Oryginał przestaje działać, ofiara traci dostęp do numeru, którym zaczyna dysponować przestępca. To jednak nie wszystko. Oszust musi posiadać dostęp do konta bankowego ofiary, aby skutecznie potwierdzić operacje bankowe. Wyłudzenie najczęściej następuje poprzez wysłane e-maile phishingowe. Ofiara dostaje wiadomość o rzekomym abonamencie wykupionym na gry internetowe. Aby anulować umowę, należy wejść w przesłany link i zalogować się do banku. W ten sposób oszuści są w stanie wyciągać z kont ogromne sumy pieniędzy.

28. FAŁSZYWE SZCZEPIENIA ZA GRANICĄ

Coraz częściej oszuści proponują osobom chętnym możliwość zaszczepienia się za granicą, oczywiście za opłatą. Niestety takie oferty nie są prawdziwe, ponieważ: w wielu krajach wprowadzone są obostrzenia dotyczące przekraczania granic (zamknięcie granicy dla obcokrajowców lub kwarantanna po przybyciu) oraz szczepionki rozdzielane są według

unijnych przepisów, w związku z czym, żadne państwo nie posiada jej „nadmiaru”. Takie oferty są próbą wyłudzenia oszczędności.

29. „NA PRZYŚPIESZENIE SZCZEPIENIA ZA OPŁATĄ”

Przestępcy w wiadomości wysyłają link do fałszywej strony bankowej, skąd mogą wykraść dane osobowe, hasło, numer konta bankowego oraz wszelkie oszczędności, które się na nim znajdują. Rejestracja na szczepienie przeciwko Covid-19 jest bezpłatna!

30. „NA MOBILNY PUNKT SZCZEPIEŃ”

Polega na tym, że oszuści dzwonią do mieszkań seniorów podając się za pracowników mobilnego punktu szczepień. Pod pretekstem sprawdzenia, czy senior kwalifikuje się do szczepienia w ten sposób, oszuści wchodzą do mieszkania i je okradają. Mobilny punkt szczepień przyjeżdża tylko do tych osób, które zarejestrowały się i dostały termin na szczepienie w domu.

31. SMS ZAPRASZAJĄCY NA SZCZEPIENIE PRZECIWKO COVID-19

Coraz częściej osoby starsze otrzymują SMSy z fałszywym zaproszeniem na szczepienie przeciwko Covid-19! Może to być próba wyłudzenia pieniędzy i danych osobowych. Numerem, na który można się skontaktować w sprawie szczepienia jest numer 664 908 556. Jeśli wiadomość pochodzi z innego numeru – nie odpowiadaj ani nie podawaj swoich danych wrażliwych.

Seniorze, nie daj się oszukać!

Źródło: <https://glosseniara.pl/stop-manipulacji/>