POLICJA MAZOWIECKA

https://mazowiecka.policja.gov.pl/ra/pion-prewencji/bezpiecz/48823,Seniorze-to-apel-o-ostroznosc.html
2023-01-30, 00:22

SENIORZE - TO APEL O OSTROŻNOŚĆ!

Data publikacji 30.11.2020

Seniorzy stają się notorycznym celem przestępców, którzy wykorzystując ufność i samotność starszych osób, dokonują wyłudzeń posiadanych oszczędności, przekonują o istnieniu cudownych leków, których działanie uchroni przed chorobą i jej konsekwencjami. Niestety każdego dnia Policja otrzymuje zgłoszenia o przypadkach kradzieży i skutecznych próbach wyłudzeń środków finansowych oraz danych osobowych.

Dlaczego seniorzy są tak częstym celem ataków? Posiadać bowiem mogą określoną sumę pieniędzy w miejscu zamieszkania bądź na koncie bankowym. Z uwagi na łatwowierność lub niezbyt dobre obeznanie z nowymi technologiami, są szczególnie podatni, by stać się ofiarą podstępnych działań. Przeczytaj o najczęstszych oszustwach, na które należy zwrócić szczególną uwagę. Jak się chronić i co zrobić, jeśli staniesz się celem ataków? Podziel się tą wiedzą z bliskimi.

Oszustwa na „WNUCZKA”

Do osoby starszej dzwoni sprawca przedstawiając się najczęściej za członka rodziny, który np.: miał wypadek i potrzebuje pieniędzy na pokrycie kosztów związanych z uregulowaniem należności w zamian za „oczyszczenie z zarzutów”. Może przekonywać, że ma właśnie okazję zakupu czy inwestycji giełdowej. Może też opowiadać o chorobie osoby bliskiej i potrzebie pieniędzy na natychmiastowe leczenie i hospitalizację. Nie wierzcie, lecz sprawdźcie to zanim oddacie swoje oszczędności!

Oszustwa na „pracownika z wodociągów”

Ostrzegamy przed oszustami podszywającymi się za pracowników wodociągów i innych instytucji, z których pracownicy dokonują systematycznych pomiarów wskazań licznika. Gdy pojawi się ktoś nowy – obca osoba - zachowaj czujność. Nie wpuszczaj do mieszkania nikogo, jeśli mieszkasz samotnie.

Oszustwa na „ZUS”

Zachowaj ostrożność przy otwieraniu i odpowiadaniu na maile, które wydają się być korespondencją z ZUS. Mogą zawierać np.: informację o pilnej konieczności spłaty zaległości składkowych i konieczności wypełnienia załączonego druku. Oszuści próbują tym działaniem nakłonić beneficjentów do ujawnienia prywatnych informacji lub dokonania płatności. Dokładnie zwracaj uwagę na adres, z którego przychodzą wiadomości. W sytuacji, w której ktokolwiek z klientów ma wątpliwości co do nadawcy otrzymanej korespondencji, należy skontaktować się z najbliższą placówką ZUS-u lub Centrum Obsługi Telefonicznej pod numerem: 22 560 16 00.

Oszustwa na „cudowne leki”

Oszuści zakładają strony internetowe, aby sprzedawać fałszywe produkty obejmujące lekarstwa i środki ochronne, które są również reklamowane np.: w mediach społecznościowych. W Sieci funkcjonuje wielu fikcyjnych sprzedawców, którzy oferują towar, którego nie mają. Przyjmują zamówienia i płatności, natomiast wtedy kontakt się urywa. Nie dajcie się nabrać! Korzystajcie ze sprawdzonych źródeł zakupów internetowych. Niektórzy oszuści podszywają się pod organizacje zdrowotne i firmy, aby właśnie teraz sprzedawać cudowne leki chroniące przed zachorowaniem na COVID-19.

Oszustwa na „lekarza”

Kolejną przestrogą jest fakt, aby uważać na osoby podszywające się pod personel medyczny, które twierdzą, że leczyły

krewnego lub przyjaciela z powodu COVID-19 i żądają zapłaty za leczenie. Przestępcy informują, że członek rodziny przebywa w szpitalu chory na koronawirusa i potrzeba sfinansować zakup kosztownej szczepionki w celu ratowania życia. Uważaj na fałszywe informacje o zakażeniu krewnych czy znajomych.

Oszustwa phishingowe

To oszukańcze wiadomości e-mail, sms-y, rozmowy telefoniczne i witryny internetowe, mające na celu nakłonienie użytkowników do ujawnienia danych konta lub danych logowania.

Złośliwe oprogramowanie

Złośliwe oprogramowanie można przypadkowo pobrać pod pozorem dokumentów edukacyjnych w różnych formatach plików: pdf, mp4 i docx . Nazwy plików mogą zawierać informacje o tym, jak rzekomo uniknąć zachorowania, ale tak naprawdę zawierają wirusa, który zainfekuje komputer czy urządzenie mobilne. Jego celem jest śledzenie ofiary i gromadzenie jej prywatnych informacji.

Oszustwa na „cele charytatywne"

Niestety oszuści polują na dobrodusznych ludzi, którzy chcą pomóc innym w czasach kryzysu. Dlatego sprawdzaj organizacje przyjmujące darowizny, zanim przekażesz pieniądze.

Oszustwa na „bankowca"

W tymże przypadku osoba dzwoniąca podaje się za pracownika banku i np. przekonuje ofiarę, że stała się faktycznie ofiarą oszustwa i potrzebuje numerów karty płatniczej. Po czym z tymi danymi „rzekomy bankowiec" posiada dostęp do Twoich środków finansowych.

Po oszustwach na „wnuczka", „policjanta", „kuriera", „agenta CBŚP", „amerykańskiego żołnierza" po latach wraca **metoda na „biednego milionera",** przed którą ostrzegamy. W tym przypadku elegancko ubrani oszuści pojawiają się okolicach banków, punktów poboru opłat czy lombardów i nawiązując kontakt łamaną polszczyzną – opowiada przypadkowemu przechodniowi zmyśloną historię dotyczącą np. nagłej blokady karty kredytowej. Po czym prosi o pożyczkę, którą za chwileczkę odda… Nie potrzeba opisywać, co dzieje się później.

Jak nie stać się ofiarą???

1. **Stosuj zasadę ograniczonego zaufania.** Przed podjęciem decyzji warto skonsultować się z najbliższymi osobami.
2. **Trzymaj oszustów na dystans**. Chroń dane osobowe: nigdy nie podawaj poufnych informacji, takich jak numer PESEL, data urodzenia, numer prawa jazdy, numery kont bankowych, historia leczenia szpitalnego itp. Jeśli ktokolwiek się z Tobą kontaktuje z prośbą o weryfikację informacji powiedz, że nawiążesz kontakt z instytucją w placówce lub za pośrednictwem ich kanałów obsługi klienta (ZUS, bank, sieć telefoniczna).
3. Jeśli ktoś w rozmowie telefonicznej naciska, aby przekazać informacje lub pieniądze, jest to oszustwo i powinieneś po prostu się rozłączyć.
4. Jeśli nie wiesz, kto przysłał e-mail, nie otwieraj go. Zachowaj ostrożność przed klikaniem **hiperłącza** lub otwieraniem załączników lub wyskakujących okienek ze źródeł, których nie znasz.
5. **Nie ujawniaj swoich danych.** Nie podawaj nikomu swojego hasła, numeru konta, kodu PIN.
6. **Chroń się przed złośliwym oprogramowaniem.** Zapewnij ochronę komputera przed wirusami poprzez posiadanie aktualnego oprogramowania zabezpieczającego. Sprawdzaj wiarygodność otrzymanych plików, patrząc na ich rozszerzenia. Pliki takie jak: .pdf, .doc i .jpg są zazwyczaj bezpieczne. Uważaj na .exe, który jest rozszerzeniem pliku wykonywalnego. Zamiast klikać podejrzane linki, które oferują kuszące informacje – usuń go.
7. **Nie odbieraj** telefonu, gdy na ekranie pojawia się nieznajomy numer. Niech każdy numer, którego nie znasz, przejdzie do poczty głosowej. Jeśli przypadkowo odbierzesz jeden, nie naciskaj żadnych cyfr –tylko po prostu się rozłącz. Możesz skorzystać z funkcji blokowania takich połączeń.
8. **Bądź świadomy zagrożeń.** Bądź na bieżąco z najnowszymi metodami oszustw. Śledź informacje o oszustwach publikowane na stronie internetowej Policji. Polegaj tylko na oficjalnych źródłach informacji, aby śledzić najnowsze wydarzenia związane z pandemią.

9. **Podczas zakupów on-line upewnij się, że firma jest legalna**, upublicznia dane kontaktowe, adres i posiada pozytywne opinie klientów zanim podasz swoje imię i nazwisko, adres oraz dane karty płatniczej w celu sfinalizowania transakcji.
10. Nie wierz w tzw. **„okazje inwestycyjne”.**

Policja apeluje, pamiętaj!!!

- Przez telefon każdy może być wnuczkiem, policjantem, urzędnikiem, synem znajomego...
- Zachowaj ostrożność, gdy odbierasz telefon od osoby podającej się za krewnego lub znajomego będącego w potrzebie finansowej.
- Nigdy nie wpuszczaj do domu osób, których nie znasz i nie przekazuj im pieniędzy!
- Policja nigdy nie prosi o przekazanie oszczędności, ani nigdy nie informuje o prowadzanych tajnych akcjach przez telefon

Opr. SSz/MG Wydział Prewencji KWP zs. w Radomiu