Bitdefender

Dziadkowie na celowniku hakerów – jak zadbać o cyberbezpieczeństwo swojej rodziny?

08.09.2023

Według Internet Crime Complaint Center (IC3) FBI, oszustwa dotyczące osób starszych kosztowały Amerykanów w wieku powyżej 60 lat ponad 3,1 miliarda dolarów w 2022 r., co oznacza wzrost strat o 84% w porównaniu z 2021 r. Straty na ofiarę wynosiły średnio około 35 101 dolarów. FBI odnotowało również straty w wysokości ponad 100 00 dolarów na każde 5456 starszych obywateli, którzy padli ofiarą oszustów w zeszłym roku. Dlatego zespół Bitdefender postanowił przygotować krótki poradnik, który pozwoli Ci zadbać o cyberbezpieczeństwo swojej rodziny.

Jak zadbać o cyberbezpieczeństwo swojej rodziny – skala i skutki cyberataków

Celem większości ofiar były oszustwa związane z pomocą techniczną

(17 810 zgłoszeń), brak płatności/dostawy (7 985 zgłoszeń), naruszenia danych osobowych (7 849 zgłoszeń) oraz oszustwa związane z zaufaniem/romansem (7 166 zgłoszeń).

Jednak powyższa lista jest bardzo zapełniona różnymi innymi przestępstwami internetowymi, w tym kradzieżą tożsamości, wymuszeniami, fałszywymi możliwościami inwestycyjnymi, podszywaniem się pod rząd, oszustwami związanymi z opłatami z góry i oszustwami związanymi z kartami kredytowymi wymierzonymi w starszych obywateli.

Oprócz oczywistych, niszczycielskich skutków finansowych, ofiary często tracą ogólne poczucie dobrego samopoczucia i mogą cierpieć na problemy fizyczne i psychiczne, w tym bezsenność, depresję i stany lękowe.

Możesz pomóc swoim dziadkom nabrać większej pewności w cyberprzestrzeni i uleczyć wszelkie emocjonalne blizny, opowiadając o najnowszych oszustwach internetowych i dzieląc się wskazówkami, jak mogą chronić swoją tożsamość i pieniądze.

Najpopularniejsze metody oszustów

Ofiarą cyberprzestępców może paść każdy. Zebraliśmy kilka najpopularniejszych sygnałów ostrzegawczych, oszustw i wskazówek dotyczących bezpieczeństwa, którymi możesz podzielić się z bliskimi:

Do najczęstszych oszustw należą:

- Oszustwa związane z pomocą techniczną – oszuści udający agentów pomocy technicznej atakują starszych konsumentów za pomocą zwodniczych rozmów telefonicznych, SMS-ów, e-maili lub wyskakujących okienek online. Cyberprzestępcy często powołują się na pewne kwestie bezpieczeństwa lub problemy z urządzeniem docelowym i proszą o dane osobowe oraz pieniądze, lub przekonują Cię do zapewnienia im zdalnego dostępu do Twojego komputera.

- Oszustwa związane z romansami – celem oszustw związanych z romansami za pośrednictwem mediów społecznościowych, a nawet aplikacji randkowych są także seniorzy. Ofiary często budują emocjonalną więź z oszustem, który nie zawaha się poprosić o pomoc finansową, zawsze wymyślając wymówki, aby nie spotkać się z nimi osobiście. Kłamstwa, jakie ci oszuści romantyczni wmawiają swoim celom, mogą obejmować trudną sytuację zdrowotną, kryzys rodzinny, problem samochodowy lub prawny.

- Oszustwo na wnuczka – niektórzy cyberprzestępcy podają się za wnuka lub członka rodziny znajdującego się w tragicznej sytuacji (wypadek samochodowy lub kłopoty prawne). Oszuści wyszukują informacje na temat swoich ofiar i dzwonią do nich z prośbą o pieniądze.

- Oszustwa polegające na podszywaniu się pod rząd — hakerzy często podszywają się pod instytucje rządowe. Oszuści mogą

kontaktować się z seniorami za pośrednictwem telefonu, poczty elektronicznej lub SMS-ów i grożą swojej ofierze, że nałożą na nich karę grzywny, więzienia lub deportacji, aby przekonać je do dokonania płatności i udostępnienia wrażliwych danych.

- Loterie i oszustwa związane z rozdawaniem prezentów. E-maile, SMS-y i strony internetowe obiecujące gratisy, wspaniałe nagrody lub wygrane na loterii w zamian za dane osobowe, dane karty kredytowej oraz płatności za wysyłkę lub opłaty manipulacyjne są zawsze oszustwem.

- Oszustwa inwestycyjne – w tego rodzaju oszustwach oszuści atakują seniorów za pomocą fałszywych obietnic łatwego zarobku na inwestycjach w nieruchomości i kryptowaluty.

Sygnały ostrzegawcze

Oto sygnały ostrzegawcze świadczące o tym, że Twoi członkowie rodziny mogą być wykorzystywani finansowo:

- Na ich kontach pojawiają się podejrzane wypłaty.

- Otrzymują rachunki za usługi, których nie rozpoznają.

- Mają zablokowany dostęp do swoich kont.

- Ich aktywa są przenoszone na konta, których nie rozpoznajesz.

- Mają tajny związek online z kimś, kto przekonuje ich do ograniczenia komunikacji z przyjaciółmi i rodziną.

W jaki sposób dbać o cyberbezpieczeństwo?

Oto pomocne przypomnienie 10 wskazówek dotyczących bezpieczeństwa, którymi możesz podzielić się z członkami rodziny, aby zapewnić im bezpieczeństwo:

- Nigdy nie klikaj linków ani załączników otrzymanych od nieznanych nadawców.

- Upewnij się, że urządzenia Twoich dziadków mają aktualne aktualizacje zabezpieczeń.

- Zainstaluj system antywirusowy na urządzeniach członków swojej rodziny.

- Powiedz członkom swojej rodziny, aby nigdy nie wysyłali pieniędzy osobom podającym się za agencję rządową lub usługodawcę. Oficjalni urzędnicy rządowi nigdy nie będą prosić o płatność za pośrednictwem poczty elektronicznej, SMS-ów lub telefonu i nigdy nie grożą karą więzienia, jeśli płatność nie zostanie dokonana.

- Poproś członków rodziny, aby przestać komunikować się z podejrzanymi osobami, które proszą ich o przesłanie pieniędzy,

przekazanie aktywów, zmianę testamentu lub zainwestowanie w kryptowaluty.

- Wyjaśnij członkom rodziny, aby unikali udostępniania danych osobowych w mediach społecznościowych lub wrażliwych danych, które mogłyby zostać wykorzystane do ich oszukania. Podaj sugestie dotyczące prywatności, na przykład ustawienie konta jako prywatnego.

- Doradź im, aby używali unikalnych haseł i włączyli uwierzytelnianie dwuskładnikowe dla swoich kont.

„Jeśli nie masz pewności, czy wiadomość internetowa faktycznie pochodzi od konkretnej firmy, np. banku, rozważ zadzwonienie na jej oficjalny numer lub wizytę w lokalnym oddziale. Dzięki temu będziesz miał pewność, że członkowie Twojej rodziny nie zostaną oszukani przez cyberprzestępców podszywających się pod pracowników banków i placówek rządowych” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe.

Źródło: https://bitdefender.pl/dziadkowie-na-celowniku-hakerow-jak-zadbac-o-cyberbezpieczenstwo-swojej-rodziny/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 08.09.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.