

Ochrona osób starszych przed oszustwami

Rozmowa telefoniczna o druzgocących skutkach

Robert, 73-letni emeryt, spędził 35 lat pracując w lokalnym zakładzie produkcyjnym, oszczędzając przy tym na emeryturę i rodzinę. Wszystkie te lata ciężkiej pracy opłaciły się, ponieważ Robert miał teraz wystarczającą ilość środków na swoich kontach bankowych, oszczędnościowych i emerytalnych, aby zapewnić sobie i swojej żonie komfortowe życie.

W poniedziałkowy poranek Robert otrzymał alarmujący telefon od osoby podającej się za pracownika działu ds. oszustw w jego banku. Dzwoniący poinformował Roberta, że jego konto bankowe zostało przejęte przez cyberprzestępców, co poważnie zagraża jego oszczędnościom i emeryturze. W trybie pilnym rozmówca poinstruował Roberta, że w celu ochrony swoich oszczędności musi natychmiast przenieść środki na „bezpieczne” konta prowadzone przez bank. Oszust podał nowe dane bankowe przez telefon, zapewniając go, że jest to jedyny sposób na ochronę jego pieniędzy. Ufny i przestraszony Robert zgodził się, przelewając wszystkie swoje oszczędności na nowe konta.

Kilka dni później Robert odkrył, że został oszukany, a cała jego emerytura przepadła. To doświadczenie sprawiło, że Robert się załamał i już nie był pewny swojej przyszłości.

Dlaczego oszuści atakują osoby starsze?

Niestety, oszuści często atakują osoby starsze, wierząc że są one bardziej ufne lub mniej zaznajomione z technologią. Ponadto seniorzy są często zamożnymi celami, ponieważ być może zgromadzili przez całe swoje życie pokaźne środki finansowe. Dodatkowo osoby starsze mogą być mniej skłonne do zgłaszania oszustw z powodu wstydu, strachu przed utratą niezależności lub po prostu nie wiedząc, z kim się skontaktować. Fakt, że ci oszuści całkowicie niszczą życie innych, niewiele dla nich znaczy.

Zrozumienie strategii stosowanych przez oszustów ma zasadnicze znaczenie dla ochrony osób starszych. Obecnie oszustwa telefoniczne są jednymi z najbardziej rozpowszechnionych, często z udziałem dzwoniących podszywających się pod agencje rządowe, instytucje finansowe, firmy użyteczności publicznej, a nawet członków rodziny w trudnej sytuacji. Oszuści wywołując pośpiech lub strach, zmuszają seniorów do natychmiastowego działania bez weryfikacji informacji. Przestępcy mogą na przykład twierdzić, że rachunek za media nie został opłacony i grozi im odłączeniem usług, jeśli nie zostanie dokonana natychmiastowa płatność. Inną powszechną taktyką jest oszustwo na wnuczka, w którym przestępcy udają wnuka pilnie potrzebującego pieniędzy na kaucję, leczenie lub pomoc w podróży. Takie połączenia telefoniczne mogą być jeszcze bardziej skuteczne, jeśli oszuści wykorzystają sztuczną inteligencję do ataków polegających na klonowaniu głosu.

Phishing poprzez e-mail lub wiadomości tekstowe to kolejne powszechne metody atakowania seniorów. Na pierwszy rzut oka może się wydawać, że te wiadomości mogą pochodzić z legalnych źródeł, takich jak banki, firmy obsługujące karty kredytowe, członkowie rodziny lub znane firmy. Jednak często zawierają one alarmujące treści nakłaniające odbiorców do klikania linków, pobierania załączników lub podawania danych osobowych.

Co możemy zrobić?

Pomimo tego, że seniorzy są często celem przestępców, podlegają tym samym rodzajom cyberzagrożeń, co wszyscy inni. Edukacja na temat bezpiecznych praktyk online, takich jak rozpoznawanie oszustw, bezpieczne zarządzanie hasłami i korzystanie z zaufanych stron internetowych, może znacznie zmniejszyć ich podatność na zagrożenia. Zachęcanie do otwartych, regularnych rozmów na temat zagrożeń jest skutecznym środkiem zapobiegawczym. Rodziny powinny przypominać seniorom, że legalne organizacje nigdy nie będą żądać natychmiastowych płatności za pośrednictwem kart podarunkowych, przelewów bankowych lub przekazów pieniężnych. Powinno się doradzać seniorom, aby nigdy nie udostępniali danych osobowych, takich jak numery PESEL, danych konta bankowego lub numerów kart kredytowych, chyba że to oni zainicjowali kontakt i całkowicie ufają źródłu. Nigdy nie udzielaj zdalnego dostępu lub kontroli nad komputerem i urządzeniami mobilnymi.

Naszym celem jest sprawienie aby bezpieczeństwo było dla nich tak proste, jak to tylko możliwe. Ustawienie blokady połączeń może pomóc seniorom uniknąć niechcianych lub podejrzanych połączeń. Możesz pomóc im skonfigurować telefon tak, aby wszystkie połączenia telefoniczne, z wyjątkiem tych od rodziny, trafiały bezpośrednio na pocztę głosową. Innym pomysłem jest dodanie zakładek do najczęściej używanych stron internetowych w przeglądarce, aby wiedzieli, że uzyskują dostęp do właściwych witryn. Jeśli menedżery haseł są dla nich zbyt trudne, zasugeruj notatnik z hasłami, w którym będą zapisywać swoje hasła i przechowywać je w bezpiecznym miejscu. Rodziny mogą również okresowo przeglądać konta bankowe swoich starszych krewnych, aby szybko zidentyfikować i zająć się podejrzаныmi działaniami. Co najważniejsze, seniorzy powinni mieć pewność, że bycie celem oszustów nie jest ich winą ani powodem do wstydu.

Redaktor gościnny

Dean Parsons jest dyrektorem generalnym ICS Defense Force, głównym instruktorem SANS i pasjonatem obrony infrastruktury krytycznej. Od ponad 20 lat zajmuje się cyberbezpieczeństwem i analizą incydentów przemysłowych oraz zajmuje się tworzeniem muzyki inspirowaną latami 80. ze swoim zespołem Arcade Knights.



Źródła

Miła rozmowa i pusty portfel: Oszustwa romantyczne: <https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/>

Nie pozwól cyberprzestępcom ukraść swoich oszczędności: <https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/>

Ataki z wykorzystaniem odwzorowanego głosu: <https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/>

Polski przekład CERT Polska: Aleksandra Węgrzynowicz, Bartłomiej Wnuk

OUCH! jest publikowany przez firmę SANS Security Awareness i jest rozpowszechniany pod licencją [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszenia zawartości samego biuletynu. Zespół redaktorski: Phil Hoffman, Leslie Ridout, Princess Young.