Grają na emocjach, żeby ukraść dane osobowe

Kategoria: Styl życia
Opublikowano: piątek, 18, marzec 2022 09:59
Joanna Gryboś-Chechelska

Cyberprzestępcy w pierwszej kolejności próbują włamać się do naszych głów. Bazując na emocjach, podszywają się pod instytucje, którym ufamy lub osoby potrzebujące pomocy i wyłudzają dane osobowe. I niestety, jak pokazują statystyki nadal robią to skutecznie. Najbardziej podatne na próby oszustwa są kobiety i ludzie młodzi.

Początek 2022 roku przyniósł wiele zmian, które starają się wykorzystać cyberprzestępcy. Wprowadzenie Polskiego Ładu oraz agresja Rosji na Ukrainę. Oszuści wyłudzający dane osobowe wykorzystują nasze emocje do tego, żeby się wzbogacić.

Na cel wzięli już sobie sytuację za naszą wschodnią granicą. Jak grzyby po deszczu powstają fałszywe strony fundacji, które rzekomo organizują pomoc dla Ukrainy. Cyberprzestępcy wysyłają także maile, w których podszywają się pod ofiary rosyjskiej agresji. W emocjonalnych wiadomościach podkreślają, że zostali bez środków do życia i proszą o wsparcie finansowe.

Eksperci CERT Polska ostrzegają także przed linkami zawierającymi „szokujące nagrania" z Ukrainy. W tym wypadku przy próbie obejrzenia pojawia się panel do logowania w naszych mediach społecznościowych. Zdobyte w ten sposób dane wykorzystywane są do przejęcia konta i dalszej dystrybucji wpisów na różnych grupach na Facebooku, lub wyłudzania środków finansowych wśród naszych znajomych.

Zagrożenie jest na realne, ponieważ, jak wynika z badania przeprowadzonego przez serwis ChronPESEL.pl i Krajowy Rejestr Długów, aż 21 proc. Polaków deklaruje, że nie potrafi rozpoznać fałszywej wiadomości. Zdecydowaną pewność, co do tego ma tylko niewiele ponad 17 proc. społeczeństwa. Najwięcej problemów z rozróżnieniem prawdziwego komunikatu od próby oszustwa mają kobiety. Ponad 27 proc. z nich twierdzi, że nie potrafi tego zrobić. Podatni na wyłudzenia mogą być także młodzi ludzie. Co czwarty (24,5 proc.) deklaruje, że nie wie, kiedy w takiej sytuacji ma do czynienia z oszustem.

Ulga podatkowa za skan dowodu tożsamości

Przestępcy wykorzystują także zamieszanie towarzyszące wprowadzeniu Polskiego Ładu, największej od lat zmiany podatkowej w Polsce. Podszywając się pod przedstawicieli Ministerstwa Finansów lub urzędu skarbowego, podczas rozmowy telefonicznej informują nas o dodatkowej opłacie, która wynika z wprowadzonych zmian podatkowych. Fałszywi konsultanci zapewniają, że sprawę można załatwić bardzo szybko i wysyłają nam link do przelewu, po kliknięciu w który mogą przejąć nasze dane do logowania w bankowości mobilnej.

Ponieważ informacja o dopłacie może jeszcze wzbudzić nasze wątpliwości, oszuści wyłudzający dane osobowe dzwonią także z informacją o wysokich ulgach podatkowych, które z tytułu zmian w prawie podatkowym nam przysługują. Jedyne co musimy zrobić, to podać nasz numer PESEL, numer i serię dowodu osobistego lub wysłać skan dokumentu tożsamości. Jeśli to zrobimy konsekwencje mogą być niemniejsze niż w przypadku udostępnienia loginu i hasła do banku.

– Uzyskane w ten sposób dane posłużą potem do zaciągnięcia zobowiązań z wykorzystaniem naszej tożsamości, np. w postaci umowy kredytowej, leasingowej, drogich zakupów lub szybkiej pożyczki. I właściciel wyłudzonych w ten sposób danych osobowych dowie się o tym dopiero wówczas, gdy dostanie wezwanie do zapłaty. Dlatego warto zadbać o bezpieczeństwo swoich danych i uważać na to, kiedy i w

jakich okolicznościach je podajemy. Niebezpiecznych momentów niestety nie brakuje. Jak wynika z naszego badania, co piąty Polak znalazł się w ostatnim półroczu w sytuacji, w której został poproszony o podanie danych osobowych w postaci, np. numeru PESEL – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl, partnera Krajowego Rejestru Długów.

Oszustwa na usługę bezpieczeństwa

Cyberprzestępcy nadal chętnie podszywają się pod banki oraz instytucje finansowe. Pomimo regularnych ostrzeżeń wciąż znajdują się osoby, które dają się na to nabrać. W lutym ING Bank Śląski ostrzegał przed oszustami wysyłającymi e-maile informujące rzekomo o nowej usłudze bezpieczeństwa, którą należało aktywować. Wystarczyło kliknąć w umieszczony w wiadomości link, który przenosił na stronę banku. Ta było oczywiście oszustwo, a wpisanie swoich danych do logowania równało się z przekazaniem ich cyberprzestępcom.

Jak wynika z przeprowadzonego badania, przez ostatnie pół roku w prawie 60 proc. przypadków, w których ankietowani proszeni byli o podanie numeru PESEL, numeru i serii dowodu osobistego, kontaktował się z nimi rzekomy pracownik banku. Dodatkowo, blisko co trzecia taka rozmowa dotyczyła banku, w którym nie mamy nawet konta.

Niestety z danych NBP wynika nie tylko to, że aktywność oszustów na tym polu rośnie, ale również to, że odnoszą oni kolejne sukcesy. Z kont Polaków znikają bowiem coraz wyższe kwoty. Jak wynika z raportu, w III kwartale 2021 r. kwota pieniędzy skradzionych z kont za pomocą przelewów była aż o 80 proc. wyższa niż przed rokiem. Prawdziwe żniwo cyberprzestępcy odnotowali też, dzięki wyłudzaniu danych na temat naszych kart płatniczych. W ten sposób od lipca do września 2021 r. ukradli prawie 22 mln zł (21,8 mln zł), czyli o 69 proc. więcej niż rok temu.

– Warto pamiętać, że ani urzędnicy, ani konsultanci telefoniczni instytucji finansowych nie mogą prosić nas o podanie danych do logowania lub numeru karty płatniczej. Tak samo, nikt nie powinien wymagać od nas wysyłania skanu dokumentu tożsamości. Już samo takie zalecenie powinno wzbudzić nasze wątpliwości. Dużą uwagę powinniśmy także przykładać do sprawdzenia linków, które otrzymujemy. Tu potrzeba szczególnej ostrożności, ponieważ często adresy fałszywych witryn często różnią się w nazwie tylko jedną literką od tych, pod które się podszywają. Oszuści liczą, że tego nie zauważymy i tak się często właśnie dzieje – przypomina Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl, partnera Krajowego Rejestru Długów.

Źródło: IP