Bitdefender

Telefoniczne kampanie phishingowe – w jaki sposób się bronić?

02.02.2023

Zgodnie z raportem Better Business Bureau, hakerzy coraz częściej wykorzystują wzrost kosztów utrzymania (COLA) amerykańskiej Administracji Ubezpieczeń Społecznych. „Ze względu na inflację, płatności mogą wzrosnąć w tym roku nawet o 8,7%" – powiedział rzecznik BBB. „To znaczący wzrost – najwyższy zatwierdzony przez COLA od ponad 40 lat – i oszuści to wykorzystują".

BBB zależy na cyberbezpieczeństwie swoich klientów, dlatego stworzyli poradnik, który ma na celu szerzenie wiedzy na temat praktyk socjotechnicznych wykorzystywanych przez hakerów. Dzięki niemu użytkownicy dowiedzą się, w jaki praktyczny sposób obronić się przed próbami phishingu przez telefon, e-mail lub SMS. Niestety w Polsce ten problem jest także powszechny, dlatego w poniższym artykule przedstawimy najważniejsze zasady z poradnika BBB, dzięki którym możemy uchronić się przed kampaniami phishingowymi w naszym kraju.

W jaki sposób działają kampanie phishingowe?

Użytkownicy, którzy stali się celami kampanii phishingowych, często otrzymują niechciane telefony od przestępców, którzy chcą pozyskać dane osobowe ofiary. Aby to osiągnąć, posługują się wieloma

socjotechnikami. Na przykład podszywają się pod banki, instytucje publiczne takie, jak ZUS lub ankieterów. Podczas rozmowy pytają o numery kont, daty urodzenia, PESEL i inne dane, o które pracownicy prawdziwych firm nigdy nie proszą. Oprócz tego często szokują i szantażują rozmówców. Na przykład informacjami o tym, że w razie niepodania żądanych informacji ich konta i środki przepadną.

Innym sposobem na przeprowadzanie kampanii phishingowych jest wysyłanie wiadomości SMS oraz E-maili, w których hakerzy podszywają się pod znane firmy. Oczywistymi i głośnymi przykładami są fałszywe wiadomości SMS od rzekomych kurierów, które zawierają linki do spreparowanych stron internetowych. Pomimo tego, że takie praktyki mogą wydawać się prymitywne i niegroźne, to musimy pamiętać o skali tych przedsięwzięć, a także o tym, iż takie wiadomości trafiają również do osób, które nie mają odpowiedniej wiedzy na temat cyberzagrożeń.

„Każde oszustwo wymierzone w osoby starsze jest szczególnie ohydne, ponieważ żeruje na bezbronnych" – powiedział Matt Krueger, rzecznik prasowy BBB w stanie Nowy Jork. „Obrona przed nimi polega na tym, aby wiedzieć, czego się spodziewać i jak zareagować, jeśli staniesz się celem".

Jak nie stać się ofiarą phishingu?

Pamiętajmy o tym, że większość instytucji publicznych raczej nie kontaktuje się z petentami telefonicznie. Dlatego, jeśli otrzymasz telefon od rzekomego pracownika ZUS, który będzie chciał pozyskać od Ciebie Twoje dane osobowe, to najprawdopodobniej masz do czynienia z oszustem. Pamiętaj o tym, że korespondencje z takimi instytucjami są najczęściej prowadzone tradycyjną drogą listowną.

W poradniku BBB wzywa również odbiorców Ubezpieczeń Społecznych, aby nie ustępowali, jeśli otrzymają jakiekolwiek groźby przez e-mail, SMS lub telefon, dodając, że pracownicy takich instytucji nigdy nie grożą

zawieszeniem ich konta Ubezpieczenia Społecznego, lub aresztowaniem w przypadku nieścisłości w zeznaniach podatkowych.

„Nie poddawaj się groźbom. Hakerzy często grożą i mówią, że nie otrzymasz pieniędzy z ubezpieczenia społecznego” — powiedziała Monica Horton z BBB. „To wywołuje strach u niektórych ludzi i ma tendencję do zaciemniania ich osądu. Jednak jest to oszustwo. Więc nie ulegaj pogróżkom i rozłącz się”.

Pamiętaj także o tym, że żaden pracownik banku, czy też innych instytucji nigdy nie poprosi o podanie Twoich pełnych danych osobowych lub danych bankowych w celu potwierdzenia tożsamości osoby, z którą rozmawia. Jeśli Twój rozmówca to zrobi, natychmiast się rozłącz i zgłoś ten incydent zespołowi CERT. Aktualne dane kontaktowe możesz znaleźć na stronie: incydent.cert.pl.

„Od kilku lat obserwujemy znaczący wzrost liczby kampanii phishingowych na terenie naszego kraju. Niestety są one coraz bardziej wyrafinowane. Dlatego powinniśmy zawsze pamiętać o tym, żeby zachowywać czujność podczas rozmów z nieznanymi numerami. Warto także zabezpieczyć swoje smartfony odpowiednim oprogramowaniem antywirusowym, które automatycznie zablokuje podejrzane i niebezpieczne wiadomości. Jest to szczególnie istotne w przypadku osób starszych, ponieważ to one najczęściej stają się ofiarami cyberprzestępców” - mówi Dariusz Woźniak z firmy Marken, dystrybutora rozwiązań Bitdefender.

Źródło: https://bitdefender.pl/telefoniczne-kampanie-phishingowe-w-jaki-sposob-sie-bronic/

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

Telefoniczne kampanie phishingowe – w jaki sposób się bronić? Bitdefender

Data udostępnienia: 02.02.2023

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 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, wielkim korporacjom, jak i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz tego, że wyposażają swoje oprogramowanie w najnowsze technologie takie, jak uczenie maszynowe, heurestyka oraz EDR i XDR.