Bitdefender

Trendy tygodnia w zakresie spamu i phishingu: cyberprzestępcy wyłudzają informacje z kont QuickBooks, American Express i kont bankowych

29.11.2023

Oszuści internetowi nigdy nie odpoczywają, nieustannie atakując konsumentów za pomocą szeregu niechcianych wiadomości e-mail (spamu), których celem jest nakłonienie użytkowników do przekazania poufnych informacji, takich jak dane logowania i dane finansowe, lub pobrania złośliwego oprogramowania na ich urządzenia. Dlatego zespół Bitdefender postanowił przygotować zestawienie najgroźniejszych niebezpieczeństw związanych z phishingiem i spamem, które były popularne w zeszłym tygodniu.

Spam i phishing – groźne zjawisko w sieci

Świadomość to kluczowy element pozwalający uniknąć podstępnych zagrożeń internetowych i innych złośliwych metod stosowanych przez cyberprzestępców w celu oszukania niczego niepodejrzewających ofiar.

W tym tygodniu badacze Bitdefender Antispam Lab ostrzegają przed oszustami, których celem są konta finansowe i użytkownicy popularnej platformy księgowej QuickBooks.

E-maile phishingowe o tematyce finansowej

Według danych telemetrycznych Bitdefender Antispam cyberprzestępcy przeprowadzili kilka kampanii phishingowych, podszywając się pod popularne banki i instytucje finansowe, w tym Standard Bank, Santander Bank i American Express, w celu kradzieży danych logowania klientów.

Fałszywa korespondencja podszywająca się pod Standard Bank jest skierowana głównie do użytkowników w Republice Południowej Afryki. Oszuści informują odbiorców, że mają oczekującą płatność, która wymaga ich natychmiastowego zatwierdzenia lub uwagi.

Najważniejszym sygnałem ostrzegawczym, na który należy zwrócić uwagę, jest załącznik „.html", który według oficjalnej strony internetowej Standard Bank jest wyraźną oznaką oszustwa. Instytucja finansowa nigdy nie wysyła załączników w formacie .htm lub .html kierujących klientów do stron logowania do platformy bankowości internetowej.

Z kolei Brazylijczycy są celem fałszywej korespondencji imitującej

oficjalną korespondencję Santander Bank. Odbiorcy spamu otrzymują ostrzeżenie informujące o tym, że ich punkty lojalnościowe Santander wkrótce wygasną i są oni zachęcani do wejścia w niebezpieczny link celem ich rzekomego wykorzystania.

"Szanowny Kliencie,

Na Twojej karcie debetowej i kredytowej Santander znajduje się 160 000 wygasających punktów.

Uniknij wygaśnięcia punktów i wykorzystaj je teraz, klikając poniższy link lub przycisk:

Uwaga: Twoje punkty zostaną anulowane w ciągu 48 godzin, jeśli ich nie wykorzystasz.” – głosi treść sfałszowanej wiadomości phishingowej.

Oczywiście osoby otrzymujące taką korespondencję powinny mieć świadomość, że w każdej chwili mogą wykorzystać nagrody wynikające z karty kredytowej i że punkty premiowe nie tracą ważności w przypadku „kont o dobrej opinii”.

Cyberprzestępcy chcą również kraść dane logowania klientów American Express w USA. Oszuści stojący za tą kampanią informują odbiorców, że ich karta kredytowa została zablokowana ze względu na „ostatnio dokonany przez Ciebie nietypowy nadmierny zakup” i że muszą przejść proces weryfikacji, aby ją odblokować.

Jak chronić się przed e-mailami phishingowymi o charakterze

finansowym?

- Nie klikaj linków i załączników w niechcianych wiadomościach e-mail.

- Nie loguj się do swojej bankowości internetowej za pomocą podejrzanych linków, aby rozwiązać problemy związane z bezpieczeństwem Twoich kont lub kart płatniczych.

- Nigdy nie podawaj poufnych informacji, numerów kart kredytowych, numerów ubezpieczenia społecznego ani dokumentów tożsamości.

- Zgłaszaj i usuwaj wszelką korespondencję otrzymaną z nieznanych domen lub e-maili.

- Zaloguj się do swojego konta bankowości elektronicznej w przeglądarce lub aplikacji, aby sprawdzić powiadomienia.

- Jeśli nie masz pewności, czy wiadomość e-mail jest wiarygodna, sprawdź ją w Internecie lub natychmiast skontaktuj się z bankiem.

„Warto pamiętać także o tym, aby zawsze korzystać z urządzeń, które zostały zabezpieczone za pomocą skutecznego systemu antywirusowego wyposażonego w moduł antyphishingowy oraz bezpieczną przeglądarkę do prowadzenia operacji bankowych. Dzięki tym rozwiązaniom będziemy mogli uniknąć zdecydowanej większości

zagrożeń phishingowych” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Phisherzy chcą uzyskać dostęp do Twojego konta QuickBooks

Nowa kampania phishingowa QuickBooks krąży także w tym tygodniu w USA. Temat fałszywej wiadomości e-mail informuje odbiorcę, że otrzymał zaszyfrowaną wiadomość.

Zespół Bitdefender zaleca, aby użytkownicy QuickBooks zawsze sprawdzali ważność wiadomości e-mail Intuit przed przesłaniem jakichkolwiek informacji. Jeśli chcesz uniknąć oszustw, użyj przeglądarki, aby zalogować się na swoje konto Intuit i przejdź do sekcji Aktywność na koncie, gdzie możesz wyświetlić listę zdarzeń związanych z Twoim kontem.

Intuit podkreślił również, że nigdy nie będzie pytał klientów o dane logowania lub hasła, dane bankowe, karty kredytowe, poufne informacje o pracownikach ani nie planuje wysyłać aktualizacji oprogramowania lub pobrania w formie załącznika.

Źródło:https://bitdefender.pl/trendy-tygodnia-w-zakresie-spamu-i-phishingu/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy

Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 29.11.2023

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.