Bitdefender

Jak cyberprzestępcy wykorzystują LinkedIn, Facebook i „X”, aby Cię oszukać?

19.09.2023

Cyfrowi złoczyńcy mogą na wiele sposobów wykorzystywać platformy mediów społecznościowych, takie jak X, Facebook i LinkedIn, aby oszukać niczego niepodejrzewających użytkowników. Oszuści stosują różne schematy w celu kradzieży pieniędzy i wrażliwych danych, niezależnie od tego, czy dotyczą one rynku mediów społecznościowych, ofert pracy, reklam czy wniosków charytatywnych. Dlatego zespół Bitdefender postanowił przygotować krótki poradnik, dzięki któremu będziesz mógł skutecznie bronić się przed cyberprzestępcami na social mediach.

Jak cyberprzestępcy wykorzystują LinkedIn

Ta zorientowana na biznes platforma mediów społecznościowych nie jest obca oszustom, którzy wykorzystują ją do wykorzystywania osób

poszukujących pracy. Hakerzy bardzo często wysyłają bezpośrednie wiadomości, tworzą fałszywe oferty pracy i podszywają się pod inne osoby.

Oszuści wykorzystują profile LinkedIn, aby zwiększyć swoją wiarygodność, zamieszczając oferty na fałszywe, dobrze płatne stanowiska lub oferty pracy w domu, za które wynagrodzenie jest zbyt atrakcyjne, aby mogło być prawdziwe. Ozdabiają swoje profile fałszywymi danymi uwierzytelniającymi, stanowiskami i stopniami naukowymi, aby realizować programy kryptograficzne i szybko się wzbogacić.

Wiesz, że to oszustwo, jeśli pracodawca lub przedstawiciel HR prosi Cię o pieniądze, abyś dostał pracę!

Jak cyberprzestępcy wykorzystują Facebook (Meta)

Biorąc pod uwagę blisko 3 miliardy aktywnych użytkowników Facebooka, nie jest zaskoczeniem, że cyberprzestępcy rozpoczęli wysoce dochodową operację oszustwa na tej platformie mediów społecznościowych. Niektórzy hakerzy skupiają się na oszukiwaniu użytkowników Facebook Marketplace, przejmując konta lub tworząc fałszywe aukcje w celu promowania oszustw związanych z kryptowalutami, akcjami charytatywnymi i usługami towarzyskimi.

Wielu oszustów wykorzystuje także sfałszowane, skradzione lub sklonowane konta do tego, aby docierać do milionów obserwatorów i żerować na ich ufnej naturze w celu zarabiania nielegalnych pieniędzy.

Jak cyberprzestępcy wykorzystują X (dawniej znany jako Twitter)

Do najpowszechniejszych rodzajów oszustw na X należą praktyki związane z rzekomym rozdawaniem pieniędzy oraz cyberincydenty polegające na podwajaniu kryptowalut i phishing za pośrednictwem fałszywych kont zaprojektowanych tak, aby przypominały profile znanych osób publicznych lub firm. Celem oszustów jest kradzież danych i pieniędzy od niczego niepodejrzewających użytkowników, a także rozpowszechnianie phishingu za pośrednictwem obserwujących oraz udostępniania postów.

W jaki sposób chronić się przed oszustwami na mediach społecznościowych?

„Oszustwa w mediach społecznościowych to ciągłe wyzwanie, z którym trzeba walczyć dzięki świadomości i proaktywnym środkom, takim jak utrzymywanie dobrej higieny cybernetycznej podczas wszystkich działań w sieci oraz wykorzystywanie narzędzi, które pozwolą nam wzmocnić naszą ochronę. Do najskuteczniejszych z nich możemy zaliczyć skuteczny system antywirusowy, prywatną sieć VPN oraz menadżer haseł" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Poniżej przedstawiamy krótki poradnik przygotowany przez zespół Bitdefender:

· Uważaj na podszywanie się i przejęte konta, które mogą zostać wykorzystane do oszustw. Analizuj wszystkie przychodzące wiadomości

bezpośrednie zawierające linki lub obietnice gwarantowanych zwrotów z inwestycji i kryptowalut. Zastanów się, zanim klikniesz jakiekolwiek linki lub pobierzesz załączniki na swoje urządzenie. Mogą zawierać złośliwe oprogramowanie, które może zainfekować Twój komputer oprogramowaniem szpiegującym lub trojanami kradnącymi dane uwierzytelniające.

· Sprawdzaj wszystkie możliwości zakupów, które wydają się zbyt atrakcyjne, aby mogły być prawdziwe i nigdy nie kupuj towarów od sprzedawców, którzy akceptują wyłącznie płatności kartami upominkowymi lub przelewami bankowymi.

· Włącz 2FA lub MFA (jeśli to możliwe) na wszystkich kontach w mediach społecznościowych i skorzystaj z ustawień prywatności. Rozważ ustawienie swojego profilu na prywatny, aby chronić swoją tożsamość i uniemożliwić cyberprzestępcom zbieranie Twoich danych osobowych lub atakowanie Cię oszustwami. W ten sposób chronisz także swoich przyjaciół i członków rodziny przed osobami, które mogą próbować się pod Ciebie podszyć lub wykorzystać Twoje dane do kradzieży.

· Stosuj rozwiązanie zabezpieczające w celu ochrony przed phishingiem, fałszywymi linkami i złośliwym oprogramowaniem.

· Nigdy nie udostępniaj informacji finansowych, danych wrażliwych ani plików multimedialnych osobom poznanym w Internecie.

· Udostępniaj mniej danych o sobie. To, że jesteś w mediach społecznościowych, nie oznacza, że musisz ujawniać całe swoje życie

osobiste i dzielić się informacjami. Oszuści zazwyczaj eksplorują profil docelowy, aby zebrać informacje o Tobie i dostosować swoją taktykę, aby Cię oszukać.

Źródło: https://bitdefender.pl/jak-cyberprzestepcy-wykorzystuja-linkedin-facebook-i-x-aby-cie-oszukac/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 19.09.2023
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.