Bitdefender

5 oszustw na LinkedIn – jak ich unikać?

11.03.2024

Z ponad 1 miliardem członków w ponad 200 krajach i terytoriach na całym świecie, LinkedIn stał się niezwykle cennym narzędziem do rozwoju kariery, rekrutacji i możliwości biznesowych. Jednak jego ogromna popularność uczyniła go również atrakcyjnym celem dla cyberprzestępców chcących wykorzystać niczego niepodejrzewających użytkowników. Dlatego zespół Bitefender przygotował zestawienie pięciu najpopularniejszych oszustw na LinkedIn oraz informacje, w jaki sposób możesz ich uniknąć.

Od fałszywych ofert pracy po skomplikowane schematy phishingu – w ostatnich latach rośnie liczba oszustw na LinkedIn

Niezależnie od tego, czy aktywnie poszukujesz pracy, jesteś doświadczonym profesjonalistą, czy właścicielem firmy wykorzystującej LinkedIn do tworzenia sieci kontaktów i rozwoju, bądź świadomy oszustw internetowych, rozpoznawaj je i unikaj, aby bezpiecznie korzystać z tej platformy.

1. Oszustwa typu phishing w wiadomościach na LinkedIn

Jedną z typowych taktyk stosowanych przez cyberprzestępców w celu wykorzystania sieci zawodowej LinkedIn są oszustwa typu phishing, w ramach których przestępcy wykorzystują fałszywe profile. Phisherzy z LinkedIn często wysyłają do celów linki udające legalną witrynę lub dokument firmy, sprytnie zaprojektowane w celu kradzieży poufnych informacji lub zainstalowania złośliwego oprogramowania w przeglądarce ofiary.

Na przykład możesz otrzymać wiadomość e-mail z prośbą o zweryfikowanie konta LinkedIn. Po kliknięciu podanego linku zostaniesz przekierowany na fałszywą stronę logowania LinkedIn. Jeśli podasz swoje dane uwierzytelniające, umożliwisz oszustom dostęp do swojego konta. W związku z tym możesz zauważyć nieautoryzowane działania, takie jak podejrzane wiadomości wysyłane do Twoich kontaktów i nieautoryzowane modyfikacje profilu.

2. Fałszywe oferty rekrutacyjne

W ramach tego oszustwa cyberprzestępcy tworzą fałszywe firmy lub profile indywidualne na LinkedIn i docierają do osób ze sfabrykowanymi ofertami pracy. Aby uczynić swoje oszustwo bardziej przekonującym, często korzystają z informacji od legalnych firm i mają rozległą sieć powiązań, co utrudnia odróżnienie ich od prawdziwych rekruterów.

Po nawiązaniu kontaktu z ofiarami fałszywi rekruterzy przedstawiają im

oferty pracy i przeprowadzają je przez proces rozmowy kwalifikacyjnej, zanim zaoferują im stanowisko. Gdy dana osoba zaakceptuje tę rolę, oszuści żądają płatności lub wrażliwych informacji, takich jak dane konta bankowego i numer ubezpieczenia społecznego, twierdząc, że są one niezbędne w dalszym procesie rekrutacji.

3. Oszustwa romantyczne na LinkedIn

LinkedIn, profesjonalna platforma sieciowa, nie jest odporna na niebezpieczeństwa związane z oszustwami romantycznymi. Oszuści mogą być jeszcze bardziej skuteczni na LinkedIn, ponieważ atakują, gdy ludzie najmniej się tego spodziewają, sprawiając, że ich plany wydają się autentyczne. Cyberprzestępcy tworzą fałszywe profile, korzystając z atrakcyjnych zdjęć i sfabrykowanych osobistych historii. Losowo łączą się z ludźmi i rozpoczynają rozmowy na temat życia osobistego, a następnie próbują przenieść dyskusje na inne platformy. Gdy już zyskają zaufanie ofiary, oszuści żądają pieniędzy.

4. Oszustwa dotyczące chińskiej rzezi świń

Oszustwo polegające na rozbiorze świń to oszustwo inwestycyjne, w którym kryptowaluta jest wykorzystywana do okradania osób fizycznych. Często zaczyna się od nieznajomego, który prosi o połączenie, a następnie zdobywa zaufanie ofiary. Kiedy oszust uzna, że nadszedł właściwy moment, poleca ofierze platformę/aplikację inwestycyjną i przekonuje ją do założenia własnego portfela kryptowalutowego, a także aktywnego inwestowania. Na początku ofiary inwestują niewielką kwotę pieniędzy, za co uzyskują szybki zwrot. Gdy dana osoba jest przekonana

o legalności aplikacji, oszust namawia ją do zainwestowania większej ilości pieniędzy w drodze pożyczenia lub zaciągnięcia pożyczki, chwaląc ją i zachęcając do dalszej pracy.

Kiedy oszuści zorientują się, że ofiara wyczerpała wszystkie środki zgromadzone na inwestycji, znikają wraz z pieniędzmi.

5. Oszustwa związane z pomocą techniczną LinkedIn

Oszuści monitorują dyskusje i grupy związane z oprogramowaniem lub problemami technicznymi. Następnie podają się za legalną pomoc techniczną LinkedIn i kontaktują się z osobami, aby zaoferować rozwiązanie problemów z kontem LinkedIn. Zwykle kontaktują się za pośrednictwem poczty elektronicznej, a ich motywem jest nakłonienie ofiar do ujawnienia poufnych danych logowania lub zainstalowania złośliwego oprogramowania pod przykrywką narzędzi do rozwiązywania problemów.

Jak rozpoznać oszustwo na LinkedIn?

Oto kilka wskazówek, jak rozpoznać fałszywe profile i sygnały ostrzegawcze w aplikacji:

- Zachowaj ostrożność podczas akceptowania nowych próśb o dołączenie do sieci kontaktów. Gdy otrzymasz wiadomość z nowego połączenia, uważaj na znaki ostrzegawcze, takie jak ogólne oferty pracy, linki lub prośby o podanie danych osobowych.

- Sprawdź szczegóły. Nawet jeśli profil wygląda na prawdziwy, warto sprawdzić, czy w historii zawodowej i edukacyjnej danej osoby nie ma niespójności. Skorzystaj z linków do innych profili społecznościowych, aby zweryfikować informacje lub wyszukaj je w Google.

- Monitoruj aktywność. Oszuści rzadko wchodzą w interakcję z innymi kontami, więc jeśli profil wydaje się nieaktywny i odcięty od reszty społeczności LinkedIn, prawdopodobnie jest fałszywy.

- Jeśli oferta pracy lub możliwości wydają się zbyt piękne, aby mogły być prawdziwe, prawdopodobnie tak jest. Do wszystkich ofert pracy podchodź ostrożnie i zanim przejdziesz dalej, zapoznaj się z rekruterem.

- Używaj narzędzi do rozpoznawania phishingu, np. bezpłatnego Bitdefender Scamio.

„Podczas korzystania z LinkedIn, pamiętaj także o tym, aby zadbać o bezpieczne i unikalne hasła oraz o skuteczny system antywirus, który został wyposażony w moduł antyphishingowy. Dzięki niemu niebezpieczne linki i reklamy zostaną zablokowane” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Chociaż LinkedIn może być nieocenionym źródłem kontaktów zawodowych i rozwoju kariery, niezwykle ważne jest zachowanie czujności wobec stale ewoluujących taktyk oszustów. Możesz bezpiecznie poruszać się po platformie, zdając sobie sprawę z typowych oszustw, analizując profile i możliwości oraz zachowując ostrożność

podczas udostępniania danych osobowych lub finansowych.

Źródło: https://bitdefender.pl/5-oszustw-na-linkedin-jak-ich-unikac/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 11.03.2024
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.