Policja ostrzega przed nowym oszustwem – oferta pracy na „bookingu”

Cyberprzestępcy nieustannie próbują wyłudzać pieniądze i szukają różnych sposobów, aby nieuczciwie się wzbogacić. Jedną z najnowszych metod jest oszustwo SMS-owe zawierające fałszywe ogłoszenia o atrakcyjną pracę w branży hotelowej m.in. na Bookingu. Celem przestępców jest wyłudzenie pieniędzy, a nawet przejęcie kontroli do bankowości internetowej i „wyczyszczenie konta”. Kolejny raz apelujemy, aby nie stracić zdrowego rozsądku, nie dać się nabrać na fałszywe oferty i nie stracić pieniędzy.

Nowe oszustwo polega na rozsyłaniu wiadomości SMS-owych zawierających ofertę atrakcyjnej pracy w branży hotelowej. Cyberprzestępcy podszywają się pod markę Booking oraz różne światowe marki hotelowe. W wiadomości oferują prostą, zdalną pracę, zajmującą jedynie kilkadziesiąt minut dziennie, a przynoszącą nieproporcjonalnie wysokie zarobki. W tym celu odbiorca wiadomości ma skontaktować się z rekruterem za pośrednictwem aplikacji Whatsapp i postępować zgodnie z dalszymi instrukcjami. W rzeczywistości celem oszustów jest otrzymanie przelewu, a w dalszej kolejności uzyskanie dostępu do bankowości internetowej, co pozwoli na wyprowadzenie z konta osoby pokrzywdzonej wszystkich zgromadzonych tam pieniędzy.

Warunkiem otrzymania pracy ma być wykonanie stosownej opłaty, zwykle w kryptowalutach. Podczas „rekrutacji” możemy być również proszeni o klikanie w otrzymane linki lub instalowanie wskazanego oprogramowania. To prosta droga do przejęcia przez cyberoszustów kontroli nad naszą bankowością internetową i pozbawieniu nas wszystkich zgromadzonych na koncie środków…

Apelujemy o ostrożność i zdrowy rozsądek. Wyjątkowo atrakcyjna oferta pracy, oferowana w wiadomości SMS-owej czy mailowej, najczęściej jest oszustwem.

Jak się chronić przed fałszywymi wiadomościami?

♦ Nie otwieraj wiadomości e-mail lub wiadomości tekstowych (m.in. przez SMS, Whatsapp) od nieznanych nadawców, osób, których nie znasz.
♦ Nie klikaj w przesłane do Ciebie linki i nie otwieraj załączników, jeśli nie wiesz, co się w nich znajduje.
♦ Uważaj na żądania poufnych informacji: oszuści często proszą o podanie hasła, numery kart kredytowych czy dane bankowe. Nie podawaj takich informacji przez e-mail lub wiadomości tekstowe.
♦ Jeśli korzystasz z poczty elektronicznej, mediów społecznościowych i bankowości elektronicznej – włącz weryfikację dwuetapową na swoich kontach online.
♦ Zrób to wszędzie, gdzie jest taka możliwość. To dodatkowa warstwa bezpieczeństwa, która utrudnia dostęp oszustom.
♦ Stosuj silne, długie i bezpieczne hasła. Pamiętaj, aby Twoja hasła nie zawierały informacji o Tobie ani Twoich bliskich. Do każdej usługi internetowej stosuj inne hasło.
♦ Zachowaj ostrożność w mediach społecznościowych. Bądź rozważny podczas przyjmowania zaproszeń od nieznanych osób na platformach społecznościowych. Unikaj udostępniania poufnych informacji publicznie na swoim profilu.
♦ Regularnie aktualizuj system operacyjny, przeglądarki internetowe i oprogramowanie antywirusowe, aby być chronionym przed lukami bezpieczeństwa.
♦ Nie lekceważ komunikatów i alertów bezpieczeństwa, jakie wyświetlają się podczas korzystania z sieci.

Inf.policjaśląska