

Czym jest spoofing i jak się przed nim bronić?

27.06.2025

Spoofing to praktyka polegająca na podszywanie się pod numer telefonu poprzez fałszowanie informacji o Caller ID wyświetlanych na urządzeniu odbiorcy. Cyberprzestępcy coraz częściej wykorzystują tę metodę, aby sprawiało wrażenie, że pochodzi z zaufanego numeru, takiego jak lokalna firma, agencja rządowa, a nawet czyjś prywatny telefon. Mimo że podszywanie się pod kogoś może mieć uzasadnione zastosowanie biznesowe, stało się ono preferowanym narzędziem oszustów ze względu na łatwość użycia i skuteczność psychologiczną.

Spoofing staje się coraz bardziej uciążliwy

Dzięki technologii VoIP i aplikacjom do podszywania się, oszuści mogą podszywać się pod niemal każdy numer za pomocą zaledwie kilku kliknięć. Doprowadziło to do wzrostu liczby oszustw telefonicznych, które mają na celu wydobycie danych osobowych, danych finansowych lub bezpośrednio płatności od ofiar.

Jak działa podszywanie się pod połączenia?

Aby podrobić swój identyfikator dzwoniącego, oszuści wykorzystują technologię, która pozwala im zmieniać metadane powiązane z połączeniem telefonicznym. Częstym błędnym przekonaniem jest to, że gdy odbierasz połączenie, telefon wyświetla dane na podstawie faktycznego numeru dzwoniącego. Jednak w rzeczywistości zależy to od informacji przesyłanych przez sieć Twojego operatora.

Narzędzia do podszywania się umożliwiają personalizację lub całkowitą fabrykację tych informacji.

Podczas gdy przepisy telekomunikacyjne i protokoły uwierzytelniania zostały opracowane w celu zwalczania złośliwych praktyk, oszuści często wykorzystują międzynarodowe sieci, operatorów VoIP lub niezabezpieczone systemy, aby ominąć wykrycie. Przy minimalnej konfiguracji ktoś może podszyć się pod lokalny numer lub znaną, legalną instytucję i mogą kontaktować się z tysiącami osób na godzinę.

Rodzaje spoofingu i powiązanych ataków

Chociaż spoofing często skupia się na połączeniach głosowych, podszywanie się wpływa również na inne kanały komunikacji. Najczęstsze rodzaje podszywania się obejmują:

- Podszywanie się pod „sąsiada”: Naśladowanie lokalnego kodu kierunkowego i centrali (np. 770-555-XXX), aby wyglądał znajomo.

- Podszywanie się pod markę lub organy państwowe: Podawanie się za znaną markę, agencję rządową lub nawet osobę z Twoich kontaktów
- Podszywanie się pod SMS-y: Wysyłanie wiadomości tekstowych, które wyglądają, jakby pochodziły z zaufanych numerów lub krótkich kodów, często zawierających linki phishingowe.
- Podszywanie się pod adres e-mail i domenę: Fałszowanie pola „Od” w wiadomościach e-mail lub witrynach internetowych w celu nakłonienia użytkowników do udostępnienia danych.
- Podrabianie głosu za pomocą sztucznej inteligencji: Wykorzystuje technologię deepfake do klonowania głosów, dzięki czemu próby socjotechniczne stają się o wiele bardziej przekonujące.

Każda forma podszywania się jest tylko częścią szerszej strategii oszustwa, której celem jest zbudowanie wiarygodności i wywołanie reakcji emocjonalnych.

Typowe metody wykorzystywane przez oszustów

Techniki podszywania się są tak różnorodne, jak oszustwa, które wspierają. Znane przykłady podszywania się pod rozmowy w rzeczywistych scenariuszach obejmują:

- Podszywanie się pod urząd skarbowy: Osoba dzwoniąca podaje się za przedstawiciela US lub innego urzędu i żąda natychmiastowej zapłaty pod

groźbą podjęcia kroków prawnych.

- Oszustwo na wnuczka: Oszust podaje się za wnuka w potrzebie, często potrzebującego pieniędzy na kaucję, i podszywa się pod numer wnuczka lub numer lokalnego komisariatu policji.
- Alerty dotyczące oszustw bankowych: Podszywając się pod numer telefonu Twojego banku oszust udaje pracownika działu ds. oszustw banku, ostrzega o podejrzanym aktywności i prosi o informacje weryfikacyjne.
- Oszustwa związane z pomocą techniczną: Cyberprzestępcy podszywają się pod numer telefonu renomowanych firm technologicznych, takich jak Apple lub Microsoft, i dzwonią do swoich ofiar, twierdząc, że ich urządzenia zostały naruszone. Oszuści oferują naprawę problemu, ale żądają zdalnego dostępu, a czasem karty kredytowej jako zapłaty w zamian za swoje usługi.
- Oszustwa na dyrektorach firm: Deepfake voice i sfalszowany identyfikator rozmówcy są używane razem, aby podszywać się pod wysoko postawionych dyrektorów firm, żądając pilnych przelewów bankowych lub poufnych danych od pracowników.

To tylko kilka z najczęstszych przypadków wykorzystywanych przez oszustów. W prawdziwym życiu kreatywność i przebiegłość oszustów nie znają granic. W ten sposób sprawcy nadużywają zaufania do instytucji, znajomości, pilności i strach.

Skala problemu

Niestety oszustwa związane ze spoofingu nadal nękają obszar cyberbezpieczeństwa, stanowiąc poważne zagrożenie zarówno pod względem skali, jak i wyrafinowania. Oszustwa podszywające się pod kogoś, z których wiele zaczyna się od fałszywych połączeń, kosztowały Amerykanów prawie 3 miliardy dolarów w 2024 r., według Federalnej Komisji Handlu USA (FTC). Globalnie szacuje się, że straty z tytułu oszustw telekomunikacyjnych przekraczają 40 miliardów dolarów rocznie.

Zaawansowane podszywanie się obejmuje teraz głosy generowane przez AI i kampanie robocall, które mogą wybierać miliony numerów za pomocą dostosowanych skryptów. Te działania oszustów na skalę przemysłową nie wykazuje oznak spowolnienia, zwłaszcza że narzędzia do podszywania się stają się łatwiej dostępne, a oszustwa stają się bardziej przekonujące.

Jak się chronić przed spoofingiem?

Podczas gdy przepisy i rozwiązania technologiczne ewoluują, najskuteczniejsza obrona zaczyna się od indywidualnej świadomości i zachowywania czujności. Oto kilka praktycznych sposobów ochrony przed oszustwami typu spoofing:

- Nie ufaj bezkrytycznie identyfikatorowi dzwoniącego: Jeśli coś wydaje się podejrzanym, nawet jeśli numer wygląda znajomo, nie zakładaj, że jest prawdziwy.
- Rozłącz się i sprawdź niezależnie: Zawsze oddzwoń, używając znanego, oficjalnego numeru (ze strony internetowej, karty bankowej lub rachunku), zamiast ponownie wybierać numer przychodzący.

- Unikaj udostępniania danych osobowych lub finansowych podczas niezamawianych połączeń: Legalne organizacje rzadko, jeśli w ogóle, żądają bez ostrzeżenia poufnych informacji przez telefon.
- Zgłaszanie podejrzanych połączeń: Zgłaszaj wszystkie oszustwa do zespołu CERT Polska.
- Korzystaj z narzędzi blokujących połączenia i filtrujących spam: Większość operatorów sieci komórkowych i platform smartfonów oferuje funkcje umożliwiające redukcję spamu i identyfikację prawdopodobnych fałszywych połączeń.
- Edukuj członków rodziny (szczególnie osoby starsze): Wiele oszustw jest skierowanych do osób starszych i innych wrażliwych grup ludzi, wykorzystując manipulację emocjonalną i poczucie pilności.
- Bądź na bieżąco: Bądź świadomy najnowszych technik oszustw, zwłaszcza nowych zagrożeń, takich jak podszywanie się za pomocą głosu wygenerowanego technologią deepfake.

Czy można wykryć fałszywe połączenia?

„Podrobione połączenia można łatwo wykryć, wykonując prostą czynność. Jeśli ktoś do Ciebie zadzwoni i poprosi o Twoje dane osobowe lub dane karty kredytowej, lub poczujesz, że coś jest nie tak podczas połączenia, rozłącz się, wyszukaj numer za pomocą zaufanych źródeł (takich jak oficjalna strona internetowa lub lista kontaktów) i zadzwoń. W ten sposób możesz łatwo sprawdzić, czy dzwoniący był oszustem. Pamiętaj także o tym, aby

zabezpieczyć swoje urządzenie za pomocą skutecznego oprogramowania antywirusowego, dzięki temu uchronisz się także przed następstwami phishingu” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: <https://bitdefender.pl/czym-jest-spoofing-i-jak-sie-przed-nim-bronic/>

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

Data udostępnienia: 27.06.2025

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.