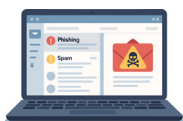


Rzeczy, które warto wiedzieć o...OSZUSTWACH INTERNETOWYCH

Internet i usługi online są wygodne i użyteczne. Jednakże zapewniają również oszustom niezliczone sposoby na oszukiwanie konsumentów. Uważaj na te metody (i podobne schematy) podczas dokonywania transakcji online.

Phishing Scams (Oszustwa phishingowe)



Phishing to nieuczciwa praktyka polegająca na wysyłaniu wiadomości e-mail lub innych komunikatów podszywających się pod renomowane firmy w celu nakłonienia ludzi do ujawnienia danych osobowych, takich jak hasła czy numery kart kredytowych.

Możesz otrzymać e-mail, który wygląda, jakby pochodził z renomowanego źródła np. z banku, firmy hipotecznej czy od wierzyciela. Oszust próbuje przekonać Cię, że na twoim koncie wystąpił problem, który wymaga natychmiastowej uwagi. Celem takiej wiadomości jest wyłudzenie danych osobowych, które następnie mogą zostać wykorzystane do kradzieży Twojej tożsamości lub środków finansowych.

Pyramid/Ponzi Schemes (Schematy piramidowe / Ponziego)



Schematy piramidowe obiecują pieniądze lub inne korzyści w zamian za rekrutowanie nowych członków do „przedsięwzięcia biznesowego”. Jeśli nowi członkowie przestają dołączać, piramida upada, a osoby na dole tracą swoją inwestycję. Takie schematy często są promowane jako gry, kluby zakupowe, firmy motywacyjne, oferty sprzedaży wysyłkowej lub organizacje inwestycyjne.

QR Code Scam (Oszustwo z kodem QR)



Oszustwa z kodami QR, znane również jako „quishing”, polegają na tym, że oszuści zachęcają ludzi do skanowania fałszywych kodów QR, które przekierowują do złośliwych stron internetowych lub aplikacji mających na celu kradzież danych lub instalację szkodliwego oprogramowania.

Package Delivery Scam (Oszustwo z dostawą paczki)



Oszust wysyła SMS-y z linkami, które rzekomo dotyczą przesyłek lub dostaw od znanych firm, takich jak Amazon czy UPS. Kliknięcie w link prowadzi na fałszywą stronę stworzoną w celu kradzieży danych osobowych lub uzyskania dostępu do konta.

Quizzes, Surveys, and Polls (Quizy, ankiety i sondaże)



Choć mogą wydawać się zabawne i nieszkodliwe, szybkie quizy, testy osobowości i inne ankiety online często zawierają pytania, które mogą prowadzić do oszustwa. Oszuści mogą wykorzystać Twoje odpowiedzi, aby spróbować zresetować Twoje konto i uzyskać dostęp do danych bankowych i innych prywatnych informacji.

Fake Gifts and Giveaways (Fałszywe prezenty i rozdania nagród)



Fałszywe konkursy i rozdania nagród często obiecują darmowe przedmioty lub atrakcyjne nagrody, jednak wymagają wcześniejszych opłat lub podania danych osobowych, aby je odebrać. Twoje dane finansowe mogą zostać przejęte, a Ty możesz stracić pieniądze lub narazić się na nieautoryzowane obciążenia Twojego konta.

Fake Job Offers (Falszywe oferty pracy)



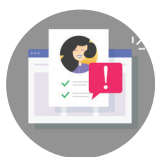
Oszust może kontaktować się z ofiarami, oferując wysokopłatną pracę z minimalnym wysiłkiem – często za pośrednictwem aplikacji do przesyłania wiadomości lub mediów społecznościowych. Często kandydat proszony jest o kliknięcie w link, który może narazić jego komputer i dane osobowe na ryzyko.

Health Care Offers (Falszywe oferty medyczne)



Konsumenci są zwabiani do zakupu sprzętu, witamin, terapii lub „cudownych leków” obiecujących lepsze zdrowie, kondycję lub wygląd. Jednak produkty i terapie mogą nie być zatwierdzone przez odpowiednie instytucje (np. FDA) lub mogą być nieskuteczne bądź szkodliwe. Niektóre zakupy mogą również nie być objęte ubezpieczeniem, mimo zapewnień sprzedawcy, co oznacza, że koszt ponosi klient.

Social Media Scams (Oszustwa w mediach społecznościowych)



Platformy społecznościowe to idealne miejsce dla różnych oszustw, które mogą obejmować fałszywe profile, reklamy, inwestycje czy zakupy online. Zachowaj ostrożność przy klikaniu linków, które mogą narażać Cię na kradzież tożsamości. Sprawdź, czy dana osoba lub firma ma inne źródło w internecie, i szukaj niezależnych opinii przed dokonaniem transakcji.

E-commerce Scams (Oszustwa w handlu elektronicznym)



Oszust może stworzyć fałszywe sklepy internetowe lub ogłoszenia na platformach, by ukraść pieniądze lub dane osobowe. Zachowaj ostrożność, zwłaszcza przy zakupach w nowych sklepach. Sprawdzaj profil sprzedawcy i historię transakcji, używaj bezpiecznych metod płatności i umawiaj się na odbiór towaru w miejscach publicznych.

WSKAZÓWKI, JAK UNIKAĆ OSZUSTW ONLINE

- Zawsze bądź czujny wobec ofert, które wydają się „zbyt dobre, by były prawdziwe”, „tajne” lub „ekskluzywne”.
- Nie podawaj danych osobowych ani finansowych w odpowiedzi na nieoczekiwane prośby. Jeśli nie masz pewności, czy prośba jest prawdziwa, skontaktuj się bezpośrednio z firmą lub instytucją, która rzekomo jes wysłała. Zawsze potwierdź jej autentyczność.
- Nie oceniaj strony po wyglądzie. To, że strona wygląda profesjonalnie, nie oznacza, że jest legalna. Przed dokonaniem transakcji sprawdź, czy firma jest wiarygodna i czy oferowane produkty są autentyczne.
- Zawsze używaj bezpiecznej przeglądarki. Upewnij się, że adres strony zaczyna się od „https://” (z ikoną kłódki w pasku adresu), zanim wpiszesz dane osobowe.
- Zawsze sprawdzaj reputację firmy. Poproś o potwierdzony adres i numer telefonu przed rozpoczęciem współpracy. Możesz też zweryfikować firmę w lokalnym biurze Better Business Bureau lub na infolinii ds. oszustw konsumenckich Prokuratora Generalnego.

INFOLINIE DS. OSZUSTW KONSUMENCKICH ATTORNEY GENERAL'S CONSUMER FRAUD HELPLINES

Chicago
1-800-386-5438

Springfield
1-800-243-0618

Carbondale
1-800-243-0607

Osoby niesłyszące lub z trudnościami w komunikacji mogą korzystać z systemu 7-1-1 (relay service).