



CONNECTICUT OCHRONA KONSUMENTÓW BIULETYN MIESIĘCZNY

Wolumen 2 / Wydanie 9 / Wrzesień 2025 r.

OSTRZEŻENIE PRZED OSZUSTWEM

Czym jest: Oszustwa z błędnymi tekstami

Jak to działa: Oszuści wysyłają Ci SMS-y, udając, że wybrali zły numer.

Zaczynają od luźnej rozmowy, aby zdobyć twoje zaufanie, a następnie próbują ukraść twoje dane osobowe lub finansowe, stosując podstęp i taktyki wywierania presji.

Jak się chronić:

Nie odpowiadaj ani nie klikaj żadnych linków od osób, których nie znasz. Bądź proaktywny, zgłaszając lub blokując numer.

Nigdy nie udostępniaj danych osobowych ani finansowych przez SMS-y, zwłaszcza jeśli nie zweryfikowałeś czyjejs tożsamości.

OSZUSTWA ZWIĄZANE Z PODSZYWANIEM SIĘ POD KOGOŚ: FAKT CZY FIKCJA?

Oszustwa polegające na wykorzystywaniu fałszywych danych stają się coraz bardziej popularne. W ostatnich miesiącach do najczęstszych oszustw zaliczają się wiadomości tekstowe informujące o niezapłaconej opłacie za przejazd lub twierdzące, że odbiorca wiadomości nie stawił się na wezwanie ławnika.

Oszuści podszywają się pod pracowników z różnych branż: agencji rządowych, wsparcia technicznego, dużych sprzedawców detalicznych i zespołów obsługi klienta. W 2024 r. straty z powodu oszustw związanych z podszywaniem się pod inne osoby w Stanach Zjednoczonych wyniosły **2,95 mld USD** [według Federal Trade Commission \(Federalnej Komisji Handlu\)](#).

Jeśli otrzymasz wiadomość twierdzącą, że pochodzi od firmy, agencji rządowej lub zespołu obsługi klienta, zadaj sobie następujące pytania:

Jeśli odpowiesz "TAK" na powyższe pytania, może to być oszustwo.

DZIAŁANIE: Czy jest wymagane natychmiastowe działanie? Czy osoba dzwoniąca żąda od Ciebie weryfikacji konta lub uregulowania salda?

PRZYCISK: Czy jest przycisk umożliwiający przejście do dodatkowej lokalizacji? Czy jest link, zdjęcie lub załącznik do pobrania?

KONSEKWENCJE: Czy wiadomość zawiera groźbę konsekwencji, jeśli działanie nie zostanie wykonane? Czy konto zostanie zablokowane? (Kara więzienia, grzywny itp.).

Ten rodzaj oszustwa nazywany jest "phishingiem" - nadawca podaje się za znaną postać lub organizację, ostrzegając odbiorcę o fałszywym problemie i żądając podjęcia pilnych działań. Zastraszają odbiorcę konsekwencjami, jeśli działanie to nie zostanie wykonane.

Oszuści stosują taktykę zastraszania, aby przekonać odbiorców do wystania pieniędzy, podania danych osobowych lub kliknięcia szkodliwego linku.

Jeśli otrzymasz taką wiadomość, zignoruj ją. Zgłoś niechcianą wiadomość i usuń ją.

Kilka dodatkowych sygnałów ostrzegawczych o oszustwach polegających na podszywaniu się:

- Natarczywa prośba o podanie danych osobowych



PROŚBA O UCZESTNICTWO

Chcesz, aby DCP (Departament Ochrony Konsumentów stanu Connecticut) przemówiło do Twojej organizacji lub pojawiło się na Twoim wydarzeniu? Skontaktuj się z Catherine Blinder pod adresem Catherine.Blinder@ct.gov, aby przesłać prośbę.

Skontaktuj się z nami

Connecticut Department of Consumer Protection

450 Columbus Boulevard,
Suite 901

Hartford, CT 06103-1840

Linia główna: (860) 713-6100
(8:30 – 16:30)

Consumer Complaint Center (Centrum skarg konsumenckich)

(860) 713-6300

Numer bezpłatny:

(800) 842-2649

8:30 – 16:30

Email: DCP.complaints@ct.gov

ODWIEDŹ NAS ONLINE
CT.GOV/DCP

- Adres nadawcy wiadomości e-mail kończy się na "@gmail.com" "@yahoo.com" lub domeną inną niż nazwa firmy.
- Występują literówki, błędy gramatyczne lub niezręczny język
- Prośba o kliknięcie linku lub pobranie załącznika w celu "wyświetlenia dodatkowych informacji lub dokumentów finansowych".
- Jeśli rozmówca podający się za "dział obsługi klienta" prosi o podanie hasła do konta lub sugeruje utworzenie nowego konta przez telefon

Jeśli otrzymasz podejrzaną wiadomość z usługi, z której regularnie korzystasz, **nie wchodź z nią w interakcję**. Aby potwierdzić, że domniemany problem jest fałszywy, należy skontaktować się bezpośrednio z firmą.

Wyszukując w wyszukiwarce "[nazwa firmy] numer obsługi klienta", możesz trafić na fałszywy numer telefonu.

Skorzystaj z numeru obsługi klienta znajdującego się na stronie internetowej firmy, w aplikacji, przesyłce pocztowej, na odwrocie karty kredytowej itp.

Oszustwa finansowe - przelej pieniądze, aby je chronić

W USA rośnie liczba oszustw polegających na podszywaniu się pod kogoś, kto chce chronić pieniądze.

Zgłoszone straty spowodowane oszustwami polegającymi na podszywaniu się pod inne osoby - poniesione przez osoby w wieku 60 lat lub starsze:

2020 55 milionów dolarów

2024 445 milionów dolarów

Dzwoni osoba podszywająca się pod bank, sprzedawcę detalicznego lub agencję rządową i powiadamia Cię o podejrzanym aktywności na Twoim koncie i o tym, że Twoje finanse są zagrożone. Osoba dzwoniąca może używać zwrotów takich jak:

"Twój dowód osobisty jest wykorzystywany w celach przestępczych"

"Twój komputer został zhakowany" "Ktoś używa Twojego konta"

Aby chronić Twoje pieniądze, zachęcają cię do przelania pieniędzy na „konto bezpieczeństwa” za pośrednictwem kryptowaluty (Apple Cash, bankomaty Bitcoin)

W niektórych raportach oszuści podawali się za przedstawicieli Federal Trade Commission (FTC), nakłaniając ludzi do przekazania kurierom stosów gotówki lub złota.

Jeśli otrzymasz podobne połączenie, rozłącz się i zgłoś incydent na stronie ReportFraud.ftc.gov

Czy czegoś nie pominęliśmy? Jest temat, na który chcesz uzyskać więcej informacji? Wyślij nam wiadomość e-mail na adres DCP.Communications@ct.gov.