



CONNECTICUT CONSUMER PROTECTION MIESIĘCZNY BIULETYN

Tom 1 / Wydanie 5 / Grudzień 2024 r.

OSTRZEŻENIE PRZED OSZUSTWEM

Co to jest: Oszustwa charytatywne

Jak to działa: W okresie świątecznym oszuści coraz częściej podszywają się pod legalne organizacje charytatywne, prosząc o datki. Oszuści ukrywają swoją tożsamość, aby wymusić na Tobie szybką darowiznę na rzecz ich oszukańczej organizacji w gotówce, za pomocą karty podarunkowej, przelewu pieniężnego lub w inny podejrzany sposób. Jak się chronić:

Zawsze sprawdzaj i potwierdzaj autentyczność prośby o wsparcie finansowe, samodzielnie wyszukując informacje na temat danej organizacji. Zapytaj dzwoniących o szczegóły rejestracji, udokumentuj każdą darowiznę i nigdy nie płać gotówką, kartą podarunkową ani przelewem pieniężnym.

Zakupy online są wygodne. Uważaj jednak na oszustów w tym sezonie świątecznym.

W grudniu sprzedaż e-commerce gwałtownie rośnie, gdy konsumenci kupują prezenty świąteczne.

Jednak w ubiegłym roku Federal Trade Commission (Federalna Komisja Handlu, FTC) odnotowała ponad 368 000 skarg dotyczących oszustw związanych z zakupami online, co stanowi drugą najczęstszą liczbę zgłoszeń dotyczących oszustw w Stanach Zjednoczonych. Jeden na czterech Amerykanów zgłosił utratę pieniędzy w wyniku oszustwa, ze średnią stratą w wysokości 500 USD.

Ponieważ cyberprzestępstwa stają się coraz bardziej wyrafinowane i trudniejsze do wykrycia, w tym okresie świątecznym ważniejsze niż kiedykolwiek jest dokonywanie rozsądnych i bezpiecznych zakupów.

Kilka wskazówek dotyczących bezpieczeństwa podczas zakupów online:

- **Sprawdź zasady zwrotów:** Zapoznaj się z polityką zwrotów lub wymiany, ponieważ główni sprzedawcy, tacy jak Amazon i Target, zaostrzają swoje zasady ze względu na rosnącą liczbę oszustw związanych ze zwrotami.
- **Nie daj się nabrać na okazje:** Mogą pojawiać się wyskakujące reklamy popularnych produktów w podejrzenie korzystnych cenach. Jeśli oferta wydaje się zbyt dobra, żeby była prawdziwa, to prawdopodobnie taka nie jest. Nie klikaj podejrzanych reklam.
- **Uważaj na nieuczciwe produkty:** Nieznane witryny będą próbowały sprzedawać podróbki produktów lub zabawek, które często są błędnie oznakowane i zawierają małe części i/lub toksyny. Rób zakupy tylko u zaufanych sprzedawców.
- **Sprawdź adres URL:** Sprawdź, czy adres strony zaczyna się od "https". Litera S oznacza, że strona jest bezpieczna.



PROŚBA O UCZESTNICTWO

Chcesz, aby DCP 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 a.m. – 4:30 p.m.)

Consumer Complaint Center

(860) 713-6300

Numer bezpłatny:

(800) 842-2649

8:30 a.m. - 4:30 p.m.

E-mail: DCP.complaints@ct.gov

ODWIEDŹ NAS ONLINE

[CT.GOV/DCP](https://www.ct.gov/dcp)

Sprawdź gramatykę na całej witrynie. Użyj [Narzędzia Google Safe Browsing](#), aby upewnić się, że witryna jest bezpieczna.

- **Przeczytaj recenzje:**
- **Użyj karty kredytowej:** Karty kredytowe oferują większą ochronę niż karty debetowe. Zgodnie z prawem federalnym możesz kwestionować nieautoryzowane obciążenia Twojej karty kredytowej. Unikaj aplikacji takich jak PayPal, Venmo i Zelle do płatności online. Używaj tej metody tylko z osobami, które znasz i którym ufasz.
- **Kupuj lokalnie:** Robiąc zakupy lokalnie, możesz uchronić się przed oszustwem internetowym.

Co zrobić, jeśli padłeś/aś ofiarą oszustwa internetowego?

1. Jak najszybciej zgłoś oszustwo do Department of Consumer Protection (DCP, Departamentu Ochrony Konsumentów), Federal Trade Commission i lokalnej policji.
2. Skontaktuj się z bankiem lub wystawcą karty kredytowej, aby zakwestionować opłaty. Mogą oni być w stanie anulować opłatę.
3. Zmień hasła do wszystkich swoich kont online.

Uważaj na smishing

Próby smishingu mają miejsce, gdy oszuści wysyłają wiadomości tekstowe, podszywając się pod firmę kurierską, aby nakłonić odbiorców do podania danych osobowych.

Oczekując na dostarczenie paczki, możesz otrzymać wiadomość tekstową, która wydaje się pochodzić od USPS lub FedEx, o treści „Twoja paczka została opóźniona; potwierdź swój kod pocztowy za pomocą linku”.

Jeśli otrzymasz podobną wiadomość, nie klikaj w link, skorzystaj z funkcji „Zgłoś spam” i zablokuj numer. Jeśli wysłałeś lub spodziewasz się paczki i nadal nie masz pewności, zadzwoń pod numer obsługi klienta firmy kurierskiej.

Pamiętaj, że będziesz otrzymywać powiadomienia tekstowe o swojej paczce tylko wtedy, gdy wyrazisz na to zgodę.

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