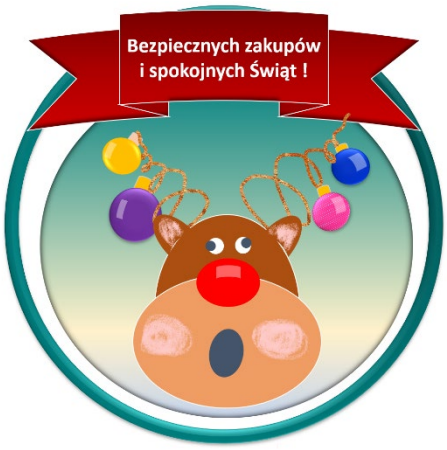
Warszawa, 30 listopada 2022 r.

Poradnik
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP, Centralnego Biura Zwalczania Cyberprzestępczości oraz Komendy Głównej Policji – bezpieczne zakupy przedświąteczne

Pada śnieg, pada śnieg dzwonią dzwonki… w telefonie, to sms przyszedł z banku o kupionym dziś zegarku…….

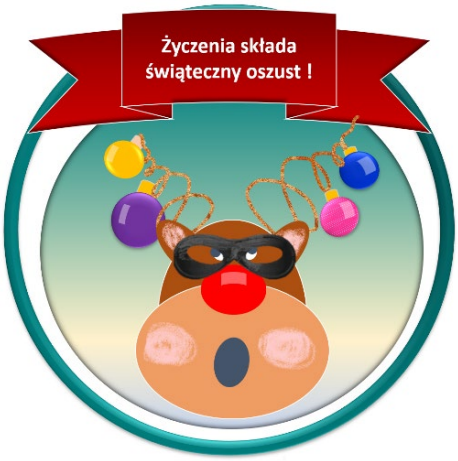
Ta historia może mieć dwa zakończenia i każde zależy TYLKO od Ciebie!!!

Aby prezenty mogły uszczęśliwić obdarowanego pamiętaj o kilku zasadach bezpiecznych zakupów:



- weryfikuj sprzedawcę/usługodawcę, czytaj negatywne komentarze i opinie;
- jeżeli wykonujesz przelew na rachunek bankowy upewnij się, czy rzeczywiście należy on do odbiorcy płatności (nr rachunku może być podmieniony przez oszusta);
- uważnie czytaj regulamin sprzedawcy – wydaje się, że jest to strata czasu, ale niezapoznanie się z nim może okazać się stratą pieniędzy;
- przekazuj tylko te dane, które są niezbędne do przeprowadzenia płatności i dostawy towaru;
- jeśli pojawił się błąd przy płatności, zwróć uwagę czy nie zostaniesz przekierowany na oszukańczą stronę, która tylko przypomina prawdziwą;
- jeśli dostaniesz komunikat o niedopłacie drobnej kwoty może być to próba oszustwa- wyłudzenie loginu i hasła do bankowości internetowej;
- wybieraj platformę e-commerce lub dostawcę usługi płatniczej, który zaoferuje Ci ochronę, w przypadku, kiedy towar lub usługa nie zostanie dostarczona lub jakość jego będzie odbiegała od zadeklarowanej w ofercie;

- nigdy nie ujawniaj informacji poufnych np.: kodów do bankowości internetowej, kodów BLIK lub kodów 3D Secure wykorzystywanych do potwierdzenia transakcji kartowych w Internecie przychodzących na telefon;
- przed zatwierdzeniem płatności zawsze uważnie czytaj treść SMS-ów jakie przychodzą na twój telefon lub komunikatów w aplikacji mobilnej banku - z ich treści może wynikać, iż akceptujesz transakcję, którą realizują oszuści;
- nie instaluj dodatkowego oprogramowania, które jest „rzekomo" wymagane z uwagi na tzw. „bezpieczeństwo płatności", lub które umożliwi udzielenie Ci zdalnego wsparcia;
- nie klikaj na linki przesłane w niespodziewanych wiadomościach e-mail lub SMS'ach.



Nieprzestrzeganie powyższych zasad może stanowić dla Ciebie zawód, rozczarowanie dla Twoich bliskich oraz straty finansowe.

NIE POZWÓL BY ŚWIĘTA ZDEZORGANIZOWAŁ CI OSZUST!

- jeśli zainstalowałeś zdalny pulpit natychmiast go odinstaluj i powiadom o tym bank;
- zgłoś reklamację w banku;
- złóż zawiadomienie na policji lub prokuraturze;
- jeżeli podejrzewasz oszustwo, w zależności od sytuacji zmień hasło do bankowości internetowej, bankowości mobilnej lub kod PIN do karty płatniczej.

Życzymy bezpiecznych zakupów i wspaniałych Świąt Bożego Narodzenia

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego

Centralne Biuro Zwalczania Cyberprzestępczości

Komenda Główna Policji

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków lub ich klientów.