

Dekalog bezpiecznych zakupów w Internecie



1. Sprawdzaj opinie o sprzedawcy.

2. Sprawdzaj dane kontaktowe sprzedawcy. Brak numeru telefonu, adresu e-mail lub adresu firmy na stronie www powinien być sygnałem ostrzegawczym.

3. Zapoznaj się z regulaminem i zasadami zwrotów. Prawo daje Ci możliwość zwrotu zakupionych towarów w 10 dni od zakupu. Upewnij się, że sprzedawca nie będzie tego utrudniał zapisami w regulaminie.

4. Uważaj na podejrzaną ofertę - przed świętami pojawiają się sklepy internetowe, które kuszą okazjnymi cenami lub zachęcają do udziału w konkursach, obiecując nagrody w postaci bonów podarunkowych. Zazwyczaj ich celem jest kradzież pieniędzy lub danych.

5. Wybieraj znane i sprawdzone sklepy oraz platformy zakupowe, które mają wdrożone procedury bezpieczeństwa oraz są wiarygodne.



6. Sprawdzaj czy strona internetowa sklepu gwarantuje bezpieczne połączenie (ma certyfikat SSL) tzn. że w przeglądarce adres witryny powinien zaczynać się od https:// i wyświetlać się znak kłódki.

7. Zakładając konto w sklepie internetowym wymyślaj długie i niepowtarzalne hasło (minimum 8 znaków, używaj duże i małe litery, znaki specjalne np. #!%, cyfry):

Unikaj haseł, które łatwo powiązać z publicznymi informacjami o Tobie (imię, nazwisko, data urodzenia)

Do każdego konta ustal inne, niepowtarzalne hasło.

Dla ułatwienia **korzystaj z managerów haseł np. KeePass XC.**

Włącz uwierzytelnienie dwuskładnikowe, tam gdzie jest to możliwe.



8. Uważaj na groźne wiadomości email i sms związane z przesyłkami.

Ataki nasilają się w świątecznym szczyście zakupowym.

Nie instaluj aplikacji z podejrzanych smsm-ów, nie loguj się do banku za pomocą przesyłanych linków.

Sprawdzaj adresata wiadomości - nie sugeruj się nazwą wyświetlaną w mailu, sprawdź z jakiej domeny wysyłana jest wiadomość informująca o przesyłce.

9. Podejrzewasz, że ktoś włamał się na twoje konto w sklepie internetowym, zmień hasło i zakończ wszystkie aktywne sesje.

10. Padłeś ofiarą oszustwa - powiadom bank - jeśli wykonałeś operację bankową za pomocą oszukanego linka lub ściągnąłeś złośliwą aplikację, natychmiast zadzwoń do banku i poinformuj o sytuacji.

przygotowane przez:

 **KOMPLUS**