KOMENDA POWIATOWA POLICJI W WODZISŁAWIU ŚLĄSKIM

https://wodzislaw-slaski.policja.gov.pl/k28/informacje/wiadomosci/187679,Nie-dajmy-sie-internetowym-oszustom.html
2021-04-19, 15:01

NIE DAJMY SIĘ INTERNETOWYM OSZUSTOM!

Data publikacji 24.11.2016

Okres zbliżających się świąt corocznie sprawia nawał „zajęć" złodziejom. Ogarniająca większość osób gorączka przygotowań do świąt powoduje, że sami często nieświadomie ułatwiamy „pracę" przestępcom. Coraz chętniej kupujemy również w Internecie. Nie ruszając się z kanapy, możemy zamówić dowolny produkt z dostawą do domu. W sieci nie istnieją kolejki czy konieczność przepychania się między sklepowymi półkami. Niestety, podobnie jak w realnym świecie, tak i w wirtualnym możemy paść ofiarą oszustów.

Internet to medium, w którym zmiany zachodzą bardzo dynamicznie a wymiana informacji, rozrywka, zakupy, bankowość dostępne są praktycznie całą dobę. Kupić można wszystko, zawrzeć umowę ubezpieczeniową, założyć konto bankowe - wszystko w Internecie bez biegania po mieście, bez stania w kolejkach, nie martwiąc się o godziny otwarcia placówek handlowych czy usługowych. Na co zwrócić uwagę wykorzystując możliwości jakie daje sieć Internet.

Poniżej przedstawione zostały reguły, których stosownie może w znacznym stopniu ograniczyć ryzyko narażenia się na działania nieuczciwych użytkowników sieci Internet.

Dokonując zakupów w sklepach internetowych pamiętajmy, że:

Warto zwrócić uwagę na regulamin danego sklepu internetowego. Zapoznajmy się w szczególności z zapisami dotyczącymi płatności, terminów dostawy, czy też możliwości zwrotu zakupionego towaru. Jeśli sklep w ogóle nie posiada takiego regulaminu, to sygnał, by zrezygnować z zakupów i poszukać innego.

Sprawdzajmy opinie o wybranym sklepie internetowym w szczególności te dotyczące przebiegu zakupów innych użytkowników oraz ewentualnych utrudnień i nieprawidłowości. W tym celu posłużyć się można popularnymi serwisami internetowymi i tematycznymi forami dyskusyjnymi.

Wiarygodność danego sklepu można także potwierdzić poprzez próbę bezpośredniego kontaktu telefonicznego czy też e-mail.

Przydatną opcją oferowana przez sklepy internetowe jest możliwość śledzenia statusu zamówienia, więc jeśli jest taka możliwość wybierajmy sklepy oferujące to udogodnienie.

Przed przesłaniem pieniędzy upewnijmy się, czy dotarło do nas potwierdzenie złożonego zamówienia np. drogą elektroniczną.

Kiedy korzystamy z aukcji internetowych:

Zawsze przed transakcją zapoznajmy się z komentarzami danego użytkownika portalu aukcyjnego oraz pamiętajmy, że sama ilość pozytywnych komentarzy nie jest jedynym wyznacznikiem uczciwości danego internauty.

Pamiętajmy również o tym, że podobnie jak w świecie rzeczywistym w internecie nie ma tzw. „okazji", nikt nam nie sprzeda samochodu czy roweru za połowę jego wartości skoro może otrzymać dużo wyższą cenę za oferowany towar. Dlatego też, nie wysyłajmy zaliczek czy przedpłat na konta osób, które takie okazje nam oferują. Zbyt niska cena też może sugerować ryzyko oszustwa.

Na fakt, iż bierzemy udział w aukcji nieuczciwego sprzedawcy, może wskazywać też sam jej opis i załączone do niej zdjęcia, jeżeli nie są one wykonane przez sprzedającego, a pochodzą np. ze strony producenta danego przedmiotu lub aukcji innego użytkownika, może to świadczyć, iż sprzedający nie jest w posiadaniu wystawianego na sprzedaż towaru.

Powinniśmy także zachować szczególną ostrożność, jeśli interesujący nas przedmiot oferowany jest na aukcji opisanej „łamaną polszczyzną" lub bez polskich znaków.

Jeśli w trakcie trwania danej aukcji pojawią się jakiekolwiek wątpliwości co do uczciwości sprzedającego zastanówmy się nad rezygnacją z udziału w tej aukcji i ewentualnym odstąpieniem od transakcji.

Wystrzegajmy się także finalizacji danej transakcji przez tzw. „zakup poza aukcją", zachęceni przez sprzedającego niższą ceną danego towaru. W przypadku oszustwa, późniejsze dochodzenie swoich roszczeń, jak i postępowanie dowodowe w takiej sytuacji jest bardziej utrudnione.

Przed dokonaniem zapłaty skontaktujmy się ze sprzedającym – im więcej informacji o sobie udostępnia (np. adres i telefon) tym mniejsze ryzyko dla nas jako kupujących.

Opcję „przedpłaty na konto" wybierajmy tylko wtedy kiedy finalizujemy transakcję u doświadczonych i pozytywnie opiniowanych sprzedawców.

Jeśli istnieje taka możliwość, wybierajmy funkcję depozytową portalu aukcyjnego i unikajmy transakcji z osobami, które nie chcą się zgodzić na taką formę płatności.

Jeżeli wybraliśmy przesyłkę za zaliczeniem pocztowym – otwórzmy paczkę przy pracowniku poczty lub kurierze, w przypadku ujawnienia oszustwa, należy spisać protokół i złożyć zawiadomienie na Policji.

Jeśli po aukcji zakończonej sprzedażą okaże się, że kupujący pochodzi z zagranicy, nie wysyłajmy towaru, dopóki pieniądze nie zostaną zaksięgowane na naszym koncie bankowym. Bardzo ostrożnie traktujmy informacje od kupującego zapewniającego nas o tym, że pieniądze zostały przelane, jednak z różnych przyczyn chwilowo wstrzymano ich zaksięgowanie, na co potwierdzeniem mają być przedstawiane przez kontrahenta, zazwyczaj spreparowane, dowody wpłat (najczęściej są to dokument w formacie *.pdf).

Nie logujmy się na swoje konto w serwisie aukcyjnym z obcego komputera (np. w kafejce internetowej, u znajomego itp.), gdyż nie mamy pewności, że na danym komputerze nie jest uruchomione oprogramowanie do pozyskiwania informacji, które to powinny być znane tylko nam lub nawet czy jest na nim zainstalowany program antywirusowy z aktualnymi bazami złośliwego oprogramowania.

Nie przekazujmy żadnych danych w odpowiedzi na zapytania od rzekomych administratorów serwisów aukcyjnego, są to preparowane przez oszustów e-maile służące przejęciu naszego konta użytkownika.

Zasady bezpiecznego korzystania z bankowości elektronicznej:

Pamiętajmy, żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.

Sprawdźmy na stronie banku jakie zabezpieczenia stosowane są w serwisie internetowym. Przy każdym logowaniu bezwzględnie stosujmy się do zasad bezpieczeństwa tam opublikowanych.

Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany. Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall.

Dokonujmy płatności internetowych tylko z wykorzystaniem „pewnych komputerów". Nie dokonujmy płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

Instalujmy na swoich komputerach tylko legalne oprogramowanie. Programy niewiadomego pochodzenia, mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

Zaleca się też, aby okresowo wykonać skanowanie komputera odpowiednim programem antywirusowym, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.

Aktualizujmy system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe. Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych.

Nie otwierajmy wiadomości i dołączonych do nich załączników nieznanego pochodzenia. Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie naszych działań.

Jeśli jednak doszło już do przestępstwa:

Należy poinformować jak najszybciej administratorów danego serwisu o zaistniałym zdarzeniu.

Powinno się zawsze zachowywać wszystkie dokumenty związane z transakcją tj. dowód przelewu na konto bankowe, korespondencję mailową, itp. jak również całą korespondencję ze sprzedawcą.

Należy zachować zapisy rozmów poprzez komunikatory internetowe, SMS-y.

Należy zgłosić się wraz z powyższymi dokumentami do najbliższej jednostki Policji.

Gdy doszło do oszustwa na aukcji internetowej, należy skompletować następujące dane: datę i numer aukcji, jej przedmiot oraz wylicytowaną kwotę, nick sprawcy oszustwa oraz jego adres e-mail, sposób kontaktu ze sprzedającym - jego e-mail, nr telefonu, adres (korespondencja e-mail powinna być zapisana w formie elektronicznej, np. w formacie *.eml), sposób dokonania zapłaty - przelew na konto bankowe, płatność za pobraniem.