



KOMPENDIUM - JAK NIE DAĆ SIĘ OSZUKAĆ W INTERNECIE

*Opracowano na podstawie artykułu
Biura do walki z Cyberprzestępczością
KGP z dnia 18.02.2021 r.*

Internet na dzień dzisiejszy to medium, w którym przeplata się świat realny z wirtualnym, życie zawodowe i prywatne... Postęp cywilizacyjny zmusza nas do pogodzenia się z „częściową wirtualizacją” naszego życia – wymiana informacji, rozrywka, zakupy, bankowość...

Praktycznie wszystkie aspekty realnego świata mają swój oddźwięk w cyberprzestrzeni. Jest szybko, tanio i 24 h na dobę. Kupić można wszystko, zawrzeć umowę ubezpieczeniową, założyć konto bankowe - wszystko w Internecie bez biegania po mieście, bez stania w kolejce, nie martwiąc się o godziny otwarcia.



- **Cyberprzestępcy w 99% przypadkach wykorzystują nieuwagę, pośpiech i naiwność ludzką, a nie zawansowane oprogramowanie czy nowe technologie!**
- **Internet tak jak każde inne miejsce nie powinien zwalniać z czujności i zachowania zdrowego rozsądku, gdyż tak jak nie uwierzymy, że w życiu realnym nikt obcy nie przekaze nam fortuny, tak samo w Internecie nie powinniśmy wierzyć w „nadzwyczajne okazje”!**



Przestrzegając kilku
podstawowych zasad
można ustrzec się
przed przykrymi
następstwami
nieuczciwej
aktywności różnych
oszustów.



PODSTAWOWE ZASADY, KTÓRE PODNOSZĄ BEZPIECZEŃSTWO W INTERNECIE:

Zakupy w sklepie internetowym:

1. Należy sprawdzić opinie o sklepie - jak przebiegały zakupy innych, czy ktoś zgłaszał jakieś nieprawidłowości (można korzystać z opinii w serwisie takich jak www.ceneo.pl lub www.opineo.pl czy sprawdzić na forach znalezionych z wykorzystaniem choćby Google).
2. Należy pamiętać, że sklep internetowy jak każda inna firma, musi posiadać numer telefonu stacjonarnego oraz adres i inne dane rejestracyjne – np. numery NIP i REGON. Powinien być też zamieszczony nr KRS (Krajowy Rejestr Sądowy), który można zweryfikować on-line, np. pod adresem www.krs-online.com.pl.



ZAKUPY W SKLEPIE INTERNETOWYM

- Należy sprawdzić poprzez kontakt telefoniczny oraz e-mail wiarygodność sklepu.
- W razie jakichkolwiek podejrzeń powinno się przynajmniej przy pierwszym zakupie sprawdzić stan przesyłki w obecności kuriera.
- Dobrze jest korzystać z ofert sklepów, które oferują możliwość śledzenia statusu zamówienia.



ZAKUPY W SKLEPIE INTERNETOWYM

- Ważną sprawą jest fakt istnienia na stronie sklepu protokołu szyfrowania danych podczas dokonywania zakupów.
- Przed przesłaniem pieniędzy należy upewnić się, czy w naszej skrzynce poczty elektronicznej pojawiło się potwierdzenie zamówienia.



ZAKUPY NA AUKCJACH INTERNETOWYCH

1. Zawsze przed transakcją należy przejrzeć opinie (komentarze) użytkownika portalu aukcyjnego, należy również pamiętać, że nie liczy się tylko duża ilość pozytywnych komentarzy, które mogą być celowo „wypracowane” poprzez zakupy przedmiotów o znikomej wartości, ale też ich statystyka – na przykład kilka ostatnio dodanych negatywnych komentarzy może świadczyć o przejęciu konta uczciwie handlującego użytkownika przez dokonującego oszustwa przestępcę.



ZAKUPY NA AUKCJACH INTERNETOWYCH

- Należy pamiętać, że nie ma „super okazji” – zbyt niska cena też może sugerować ryzyko oszustwa.
- O fakcie czy bierzemy udział w nieuczciwej aukcji, może powiedzieć opis aukcji lub załączone do niej zdjęcia. Pamiętać należy, że jeżeli zdjęcia nie są wykonane przez sprzedającego, tylko pochodzą np. ze strony producenta lub innej aukcji, może to świadczyć, iż sprzedający nie jest w posiadaniu wystawianego na sprzedaż towaru.
- Jakiegokolwiek podejrzenia, powinny skutkować odstąpieniem od transakcji.
- Przed dokonaniem zapłaty powinno się skontaktować ze sprzedawcą – im więcej informacji o sobie udostępni (np. adres i telefon) tym lepiej.



ZAKUPY NA AUKCJACH INTERNETOWYCH

- W wypadku przedpłaty na konto należy wybierać tylko doświadczonych i pozytywnie opiniowanych sprzedawców.
- Unikajmy bezwzględnie dokonywania zapłaty za zakupiony towar poprzez różne systemy płatności, które nie pozwalają w żaden sposób zidentyfikować odbiorcę naszej płatności, takich jak Western Union lub ostatnio wprowadzany system zdalnego przekazywania pieniędzy poprzez sieć bankomatów, umożliwiający dokonywanie wypłat bez konieczności posiadania karty bankomatowej, a jedynie posiadając telefon komórkowy – Hal-Cash. W celu skorzystania z usługi Hal-Cash i pobrania gotówki z bankomatu, potrzebne są wyłącznie kody, które można otrzymać np. SMS'em, bezpośrednio po zleceniu dokonany przez nadawcę. W przypadku zaistnienia oszustwa, przestępca wybiera nasze pieniądze w każdym miejscu naszego kraju, a pozostaje po nim jedynie numer telefonu komórkowego, który najczęściej jest numerem pre-paid, użytym raz do popełnienia przestępstwa.



ZAKUPY NA AUKCJACH...

- Nie należy dokonywać transakcji przez tzw. „kupowanie poza aukcją”. (Oszuści najczęściej traktują serwis aukcyjny jako sposób pozyskania ofiary. Przestępca proponuje nieświadomej zagrożenia osobie zakup po niższej cenie, ale bez pośrednictwa serwisu – choćby po to, by uniknąć opłat pobieranych przez serwis aukcyjny. Należy wziąć pod uwagę, że późniejsze dochodzenie swoich roszczeń, jak i postępowanie dowodowe jest bardzo utrudnione).
- Po zakończonej aukcji należy odczekać kilka godzin i skontaktować się samemu ze sprzedającym w celu potwierdzenia danych potrzebnych do dokonania przelewu, pamiętając że błyskawicznie otrzymany po zakończonej aukcji e-mail może być spreparowany przez oszusta.



ZAKUPY NA AUKCJACH...

- Jeśli pojawia się choć cień niepewności odnośnie sprzedającego, a istnieje taka możliwość, należy wybrać funkcję depozytową portalu, unikając transakcji z osobami, które nie chcą się zgodzić na taką formę płatności.
- Jeżeli przesyłkę przesłano za zaliczeniem pocztowym – można otworzyć paczkę przy pracowniku poczty lub kurierze i w przypadku ujawnienia oszustwa, należy spisać protokół i złożyć zawiadomienie na policji.
- Jeżeli po aukcji zakończonej sprzedażą (przeważnie niespodziewanie wysoką kwotą) okaże się, że kupujący pochodzi z zagranicy (najczęściej z Afryki), nie należy wysyłać towaru, dopóki pieniądze nie zostaną zaksięgowane na koncie, nie reagując na e-mail'e, że pieniądze zostały chwilowo wstrzymane, ale za to do informacji jest załączony spreparowany dowód wpłaty (najczęściej jest to dokument w formacie *.pdf).



BARDZO WAŻNA JEST OCHRONA SWOICH DANYCH PERSONALNYCH, BY NIE ZOSTAĆ WPLĄTANYM W PRZESTĘPCZĄ AKTYWNOŚĆ OSZUSTÓW AUKCYJNYCH!

- Nie należy logować się (podawać loginy/nick'a i hasła) z komputera obcego (np. w kafejce internetowej, u znajomego itp.), gdyż nie mamy pewności, że na danym komputerze nie jest uruchomione oprogramowanie do pozyskiwania informacji, które powinny być znane tylko nam (sniffer'y, keylogger'y) lub nawet czy jest na nim zainstalowany program antywirusowy z aktualnymi bazami złośliwego oprogramowania.
- Nie należy podawać żadnych danych w odpowiedzi na rzekome zapytania od administracji serwisu aukcyjnego, są to w 100% preparowane przez oszustów e-mail'e celem przejęcia naszego konta użytkownika.



KORZYSTANIE Z PORTALI SPOŁECZNOŚCIOWYCH

- Należy podawać jak najmniej informacji o sobie, rodzinie, bliskich, znajomych, miejscu pracy, itp.
- Nie wolno zamieszczać zdjęć, które mogą być podstawą szantażu, lub mogą pomóc w uwiarygodnieniu podszywania się.
- W przypadku, ujawnienia, iż ktoś podaje się za nas (ktoś w takim serwisie takim jak np. „Nasza Klasa” założył profil z naszymi danymi) trzeba żądać od administratora jego usunięcia.



DOKONYWANIE PŁATNOŚCI W INTERNECIE

- Przed przelaniem pieniędzy należy upewnić się, czy podane przez sklep konto rachunku bankowego nie należy do tzw. elektronicznych portmonetek, czyli kupowanych np. w urzędzie pocztowym za 5 zł. kart płatniczych wraz z numerem konta w celu późniejszego ich doładowania (karta płatnicza typu pre-paid). Sprawdzić to można wpisując nr rachunku bankowego choćby pod adresem <http://www.konto.uwaga.info/>, gdzie w przypadku karty typu pre-paid nie pojawi się żaden oddział banku, tylko centrala. Należy pamiętać, iż transakcja taka jest niebezpieczna, gdyż nr konta rachunku bankowego nie jest powiązany z żadnymi danymi personalnymi.



...PŁATNOŚCI W INTERNECIE

- Nie należy regulować płatności w Internecie tzw. „wypukłymi” kartami kredytowymi, które po dokonaniu zakupu konieczne jest podanie numeru karty oraz najczęściej specjalnego kodu zapisanego na karcie (kod ten zwany jest CVV2/CVC2, numer ten jest nadrukowany na karcie tuż obok podpisu).
- Powinno się regulować płatności w Internecie korzystając z witryn umożliwiających płatności przez centra rozliczeniowe, dzięki temu pracownicy sklepu internetowego nie otrzymują danych karty kredytowej.



...PŁATNOŚCI W INTERNECIE

- Płacąc kartą lub przelewem z elektronicznego konta bankowego należy używać wszystkich, także opcjonalnych zabezpieczeń oferowanych przez bank – np. dodatkowego kodu autoryzującego transakcję, otrzymywanego sms-em na telefon komórkowy.
- Nie wolno reagować na e-mail'e od banku z prośbą o podanie hasła jednorazowego lub zmianę hasła.
- Logując się na stronę, poprzez którą dokonuje się płatności, należy sprawdzić, czy opiera się ona na bezpiecznym połączeniu szyfrowanym oznaczonym skrótem https (w odróżnieniu od nieszyfrowanego http), jeśli tak należy sprawdzić, czy certyfikat bezpieczeństwa jest ważny klikając na symbol kłódki, który pojawi się podczas wyświetlania takiej strony w przeglądarki internetowej.



- Nie wolno reagować na e-mail'e od banku z prośbą o zalogowanie się na stronę banku przez link podany w tekście wiadomości. Strona, taka może być kopią strony banku, a klient jest proszony o podanie numeru konta, numeru identyfikacyjnego i haseł, a nawet kodów PIN do kart. Jest to typowy phishing – czyli wyłudzenie danych dotyczących kont rachunków bankowych w celu przejęcia ich zawartości.
- Na komputerze, który jest używany do transakcji internetowych, nie powinno się instalować żadnych, programów z nieznanego źródła – gry, animacje itp. mogą faktycznie służyć do monitorowania zawartości komputera.



- W trakcie logowania się do sklepu internetowego czy banku nigdy nie wolno korzystać z linków – zawsze należy wpisać adres ręcznie.
- Nie należy dokonywać płatności i logować się do serwisów z podaniem swojego hasła w punktach bezpłatnego publicznego dostępu do Internetu (tzw. hot-spotach).



NIESPODZIEWANA KORESPONDENCJA I SMS'Y

- Gdy otrzymujemy z nieznanych źródeł lub o dziwnej treści korespondencję lub sms'y, których się nie spodziewamy, może to znaczyć, że my lub ktoś kto posiadał nasze dane kontaktowe był nieostrożny i teraz ktoś inny usiłuje te dane wykorzystać w celu niezgodnym z prawem.
- Przeważnie chodzi o wyłudzenie jakiejś kwoty pieniędzy lub pozyskanie naszych danych wraz z numerem konta rachunku bankowego, czyli **phishing**.



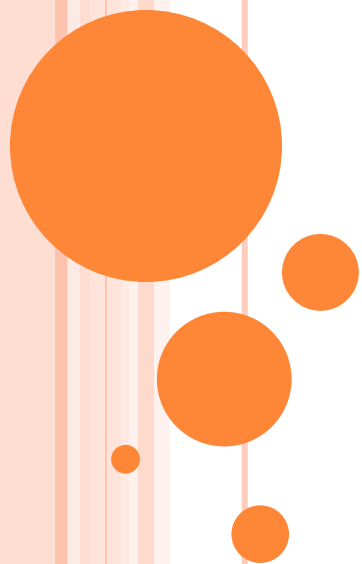
PODSTAWOWE ZASADY, O KTÓRYCH W NALEŻY PAMIĘTAĆ:

- Nikt nie daje nic za darmo! Udział w bezpłatnej loterii i szybka wygrana to absurd, gdyż funkcjonowanie darmowej loterii mija się z celem. Koszty operacyjne, które należy pokryć w celu odebrania wygranej to kwota, którą traci się na rzecz oszustów, a wygranej nigdy się nie otrzyma. Podawanie naszego numeru konta bankowego, celem przelania rzekomej wygranej, też skutkuje przekazaniem istotnych danych personalnych sprawcom tzw. **phishingu**.
- Żaden uchodźca polityczny z „Czarnego Łądu”, posiadający miliony dolarów na zamrożonym koncie bankowym, za pomoc w odzyskaniu ich nie podzieli się później tą kwotą, stracimy jedynie wyłudzone w trakcie całej operacji zwanej „oszustwem nigeryjskim”, koszty operacyjne (rzekomej opłaty dla prawników, przelewy bankowe, wytworzenia dokumentacji) kilkaset lub kilka tysięcy dolarów lub funtów.



- Otrzymując e-mail lub sms'y z informacją, że pod wskazanym adresem są kompromitujące nas materiały, a następnie żeby tam się dostać musimy wysłać sms by otrzymać kod dostępu, w 99% przypadków stracimy tylko kilkadziesiąt złotych na sms, a pod wskazanym w najlepszym wypadku nic nie będzie lub w nieco gorszym przypadku będzie złośliwe oprogramowanie, którym możemy zainfekować nasz komputer.
- Nie bierz udziału w przestępstwie zwanym „praniem pieniędzy”. Po otrzymaniu wiadomości e-mail z prośbą o pomoc w przesłaniu pieniędzy, np. od kontrahentów jakiejś firmy, którzy będą je wpłacać na udostępniony przez zwerbowaną osobę rachunek bankowy, do siedziby firmy, przeważnie za wschodnią granicę z wykorzystaniem transferu pieniężnego Western Union, po uprzednim potrąceniu np. 5% prowizji dla siebie, należy natychmiast potraktować to jako próbę zwerbowania do procederu „prania pieniędzy”.





GDY DOSZŁO DO OSZUSTWA

- Należy poinformować jak najszybciej administratorów ds. bezpieczeństwa danego serwisu.
- Powinno zawsze się 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.



MATERIAŁY EDUKACYJNE

- Program Komisji Europejskiej Safer Internet promujący bezpieczne korzystanie z nowych technologii i Internetu wśród dzieci oraz młodzieży:

www.saferinternet.pl

- Materiały, poradniki, dobre praktyki:

www.stojpomyslpolacz.pl



ZGŁOŚ INCYDENT

- www.cert.pl

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne.

- www.dyzurnet.pl

Dyzurnet.pl to zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.





NUMER ALARMOWY

112

