

KOMENDA MIEJSKA POLICJI W BIELSKU-BIAŁEJ

Źródło:

<http://bielsko.slaska.policja.gov.pl/ka2/bezpieczenstwo/dla-internautow/6382,Ciemna-strona-aukcji-internetowych-czyli-jak-nie-dac-sie-oszukac.html>

Wygenerowano: Wtorek, 27 czerwca 2017, 10:41

CIEMNA STRONA AUKCJI INTERNETOWYCH CZYLI JAK NIE DAĆ SIĘ OSZUKAĆ

Patrycja Kierzkowska

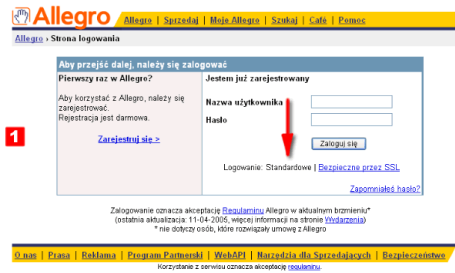
[Magazyn INTERNET](#)

Jak wszędzie, także na aukcjach zdarzają się oszustwa. Te na mniejszą skalę, o których nikt na co dzień nie mówi, i na większą - przy okazji widowiskowego zbiepania oszustów. Wbrew pozorom oszustwo Internetowe nie wiąże się z otrzymaniem czegoś zamiast towaru. Teraz na topie jest podrywanie się pod solidnych sprzedawców. Tego chyba nikt nie przewidział.

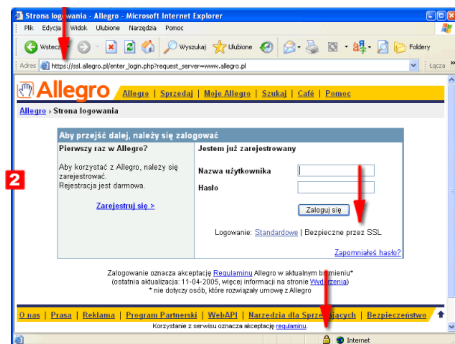
Stara szkoła licytujących mówi: "Im więcej gwiazdek, tym bezpieczniej". A jest wręcz odwrotnie. Oszukiwać najlepiej w Allegro, bo korzysta z wielu osób i jest najpopularniejszy. Poszukiwanie się pod cenowego sprzedawcę daje oszustowi gwarancję szybkiego zysku, bo korzysta z wypracowanego wizerunku innej osoby. Najprościej oszukać na... kartach pre-paid. Dlaczego? Po pierwsze są popularne i tanie, więc nie wzbudzają podejrzeń. Po drugie w większości przypadków wydrukowane kwoty nie kwalifikują się do POK-u - Programu Ochrony Kupujących (o tym wspomnę dalej). Po trzecie w momencie gdy kupujemy kod doładowujący telefon, chcemy otrzymać go jak najszybciej. Sami sprzedawcy chwalią się, że realizują transakcję w ciągu kilku godzin. Etekt? Sprzedawca akurat nie jest online, w tym czasie oszusta z konta sprzedawcy wystawia kartę na aukcji, zmienia numery kont, hasła dostępu. Chętni znajdują się szybko, kupują, płacąc od razu przelewem, a oszust znika. Cała "zabawa" trwa kilka godzin. Zanim właściciel zorientuje się i skontaktuje z pracownikami serwisu aukcyjnego, oszust już nie ma. Allegro reaguje najszybciej, powiadamia klientów, którzy dokonali zakupu, blokuje konto sprzedawcy, usuwa aukcję... i na tym kończy się ich rola. Dalej trzeba działać samemu.

Logowanie - podstawa

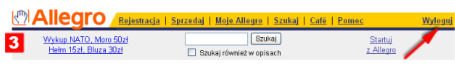
Allegro zaleca logowanie przez bezpieczne połączenie SSL, ale wchodząc na podstronę Moje Allegro (tu logujemy się) otwiera się standardowe, niebezpieczne logowanie. Spójrzmy na rys. 1.



Strona jest niebezpieczna (dowodzi tego adres w pasku przeglądarki, którego nie widać na ilustracji), natomiast w dolnej części ramki znajduje się niepokreślony napis Logowanie standardowe. Jesteśmy w niebezpiecznym logowaniu. Teraz zobaczmy rys. 2.



Adres wygląda zupełnie inaczej (https!), na dole jest niepokreślony napis Bezpieczne przez SSL, a na dolnym pasku widać żółte ikony. Po kliknięciu ikony otwory się okno z informacją o certyfikacie bezpieczeństwa - obejrzymy dokładnie. Mam nadzieję, że niedługo Allegro przestawi domyślne logowanie na SSL - taka surowość wysłałam jakiś czas temu do serwisu. Póki co należy uważać i wybierać samodzielnie SSL. O cechach dobrego hasła pisaliśmy już w M wiodukrotnie. Najważniejsze to nie używać jednego hasła do wszystkich (mail, WWW, forum dyskusyjne, sklep internetowy - niech wreszcie będzie inne!) i stosować kombinację literowych znaków i cyfr. Loginów i haseł nie należy trzymać wśród danych na dysku! Jeśli przeglądarka zapyta czy zachować hasło, kliknijmy NIE (nawet, jeśli korzystamy z komputera w domu). Gdy skończymy, nie zapominajmy wylogować się. Napis Wykopił będzie widoczny tak długo, aż się nie wylogujemy (rys. 3).



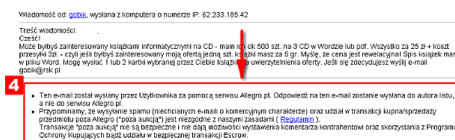
Nie polecam wykorzystywania nieznanych komputerów do jakichkolwiek działań w internecie, które będą wymagały logowania. Nie mamy żadnej pewności, że komputer na uczelni czy gdziekolwiek jest wolny od programów śledzących nasze poczynania. Pamiętajmy, że istnieją programy (keylogery), które potrafią wyprowadzić z komputera wszystko, co napiszemy na klawiaturze. Nie zapominajmy też o ochronie własnego, domowego komputera. Dobrej program antywirusowy i zagraj ongiwa to podstawa nie tylko użytkownika aukcji internetowej.

Zanim zaczniemy licytować

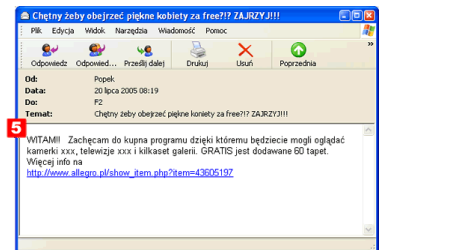
Ostrożność, podejrzliwość, ciekawość - oto cechy dobrego kupującego. Można wyróżnić dwa rodzaje oszustów: świadomy naciągacz i podszywacz. Naciągacz dość łatwo zidentyfikować. "Nabijają" sobie punkty zakupami za 1 zł, po czym sprzedają drogi sprzęt komputerowy. Drugi typ jest bardziej złożony i trudny do wykrycia, bo polega na wyłudzeniu danych w różny sposób. Może to być e-mail przypominający graficznie strony internetowe np. banków lub serwisu, z którego korzystamy (tzn. oznacza większe prawdopodobieństwo, że czytający mała z niego korzysta). W liście informują nas o tym, że musimy zweryfikować swoje dane lub ostatnią transakcję, jakiej dokonaliśmy. Po kliknięciu odzyskujemy jesteśmy przekierowani na stronę do służeńia podobną do strony prawdziwej. Podajemy swoje dane, kod, hasło, PIN... (wzrost czasu masowej kradzieży listy rzekomo pochodzącej od mBanku i Citibanku). Możemy zabezpieczyć się jak kaze nam dział pomocy Allegro, ale nie mamy pewności czy to samo zrobił sprzedawca, od którego kupujemy. Jeśli nie, istnieje duże prawdopodobieństwo, że zostaniemy oszukani, bo oszust zaloguje się na jego konto i przystąpi do działania. Nie bądźmy naiwni. Pracownicy serwisów/banków/portali NIGDY nie proszą o podawanie haseł i nie wysyłają listów z prośbą o weryfikację danych (która ma odbyć się dopiero po zalogowaniu). Nawet jeśli list wygląda wiarygodnie i pochodzi od adresata admin@kaskos.pl. Często takie przesyłki są w formie HTML-a, łatwo więc zrobić napis www.allegro.pl, który jest tylko nazwą "na wierzchu", bo "pod spodem" można wpisać zupełnie inny adres. W razie wątpliwości trzeba skontaktować się z pracownikami serwisu (dane znajdujące na oficjalnej stronie). Nawet w przypadku fałszywego alarmu zastanówmy się nad rozsądnych, myślicyjnych i podejrzliwych userów. W każdej aukcji doszukujemy się oszustwa. Czytajmy komentarze (sprawdzajmy, co kupowali i sprzedawali - to bardzo ważne), opisy, zdjęcia, próbmy o telefon stacjonarny, pytajmy o możliwość odbioru osobistego (nawet jeśli mieszkamy na Haju, a sprzedawca w Ustrzykach Bodnych). Jeśli na aukcji słuchawki kosztują 50 zł, a w sklepie identyczne są za 700 zł to zastanówmy się. Zapytajmy o dodatkowe zdjęcia przedmiotu, gwarancje, dowody zakupu (poprośmy o przesłanie skanów dokumentacji). Nawet jeśli sprzedawca twierdzi, że są nowe i zafalowane, można sądzić, że to złodziej (świadomy naciągacz), albo podszywacz (który towar zna tylko ze zdjęć w internecie).

Pozza protokołem

Chyba każdy użytkownik aukcji miał do czynienia z propozycjami kupna poza Allegro. Wygląda to tak, że jakiś user wysłał przez system Allegro wiadomość (korzysta wtedy z ogólnodostępnej opcji Zadań pytanie sprzedawcy). Każdy taki list ma odpowiednią stopkę hyba (rys. 4) informującą o niebezpieczeństwie przy dokonywaniu zakupów poza systemem Allegro.



Może też wysłać list przez program pocztowy (rys. 5). Adres ma ze strony O mnie. Wtedy już nie pojawia się ostrzeżenie przed niebezpieczeństwem. Póki biedy, jeśli jest to odsyłacz do aukcji w Allegro. Gorzej, gdy zawiera konkretną ofertę, a odbiorcą listu jest początkujący, niedoświadczony kupujący.



Stawoczo odradzam korzystanie z takich ofert, bo albo oferty są nielegalne (inaczej sprzedawca wystawiałby je na aukcji), albo to oszust i naciągacz. W przypadku oszustwa nie jesteśmy w stanie tego udowodnić sprzedawcy, nie możemy sądzić od Allegro zadośćuczynienia z POK-u i nie mamy możliwości wystawienia komentarza sprzedawcy. Wiadomości z ofertami wysyłane przez sprzedawców wyżej wymienionymi drogami należy traktować jako spam i zgłaszać administratorom serwisu aukcyjnego.

