

Musimy powiedzieć to wprost - ikona lub obrazek z kłódką na internetowej witrynie zakupowej nie stanowi żadnej gwarancji bezpieczeństwa. Choć może się to wydawać oczywiste, wymaga jednak podkreślenia, ponieważ ludzie nie podchodzą do zakupów przez internet z odpowiednią dozą ostrożności i zdrowego rozsądku. Specjaliści z AVG radzą, jak być bezpiecznym podczas zakupów online.

Internauci nadal zbyt niefrasobliwie podchodzą do zakupów za pośrednictwem internetu. Wzrost liczby osób decydujących się na tego typu transakcje nie pociąga za sobą wzrostu świadomości zagrożeń, jakie one ze sobą niosą. Przeprowadzone przez Unię Europejską badanie wykazało, że odsetek osób, które kupiły przynajmniej jeden przedmiot przez internet, zwiększył się pomiędzy 2006 a 2008 rokiem o 6 procent, osiągając wartość około 33 procent.

Fakt, że poziom wydatków na zakupy elektroniczne wzrósł w okresie recesji oznacza, że ludzie nie są obojętni na internetowe oferty i okazje. Trudno powiedzieć, czy to zapał i oczekiwanie na promocję dostępną na stronie internetowej sprawiają, że przeciętny użytkownik zapomina o podstawowych zasadach bezpieczeństwa podczas zakupów online – ale z pewnością tkwi tu pewien problem.

W supermarkecie nie wymachujesz portfelem ani torebką, prawda? Więc nie rób tego w sieci!

Rosnącej popularności zakupów przez internet towarzyszy wzrost liczby oszustw internetowych. Dane ujawnione w marcu 2010 r. przez APACS, organ zajmujący się bankowością, pokazały, że oszustwa internetowe w samej Wielkiej Brytanii wzrosły o 132 procent w porównaniu ze stratami zgłoszonymi w 2007 roku.

Kto ponosi za to odpowiedzialność i czy jest to wina jedynie konsumentów?

Jeśli nie jesteś na tyle nierozsądny, aby robić zakupy przez podejrzanie wyglądającą witrynę, to prawdopodobnie w sytuacji, gdy już postanawiasz wydać pieniądze przez internet, oczekujesz, że istnieje jakiś rodzaj ochrony konsumenta w sieci. Niepokojący wzrost liczby oszustw internetowych został przez niektóre rządy powiązany z faktem, że prawo mające służyć ochronie kupujących jest nadal za bardzo skupione na tradycyjnej formie zakupów i nie dotrzymuje kroku rzeczywistości internetowej.

„Nasz obecny system jest tak skonstruowany, aby chronić konsumenta, który idzie do centrum handlowego. Ale współczesny konsument coraz częściej kupuje towary i usługi przez strony internetowe, które mogą być obsługiwane z dowolnego miejsca na świecie, a towary wysyłane i dostarczane z zagranicy” – ostrzega brytyjski minister ds. konsumentów, Gareth Thomas. „Musimy stworzyć system, który sprawnie ochroni konsumentów przed współczesnymi oszustami i przestępcami” - dodaje.

AVG Technologies radzi, co można zrobić, żeby uchronić się przed cyberprzestępcami podczas zakupów online?

1. Przede wszystkim należy zainstalować i utrzymywać zaktualizowaną ochronę antywirusową.
2. Podnieść poziom ochrony instalując firewall i oprogramowanie antyspieszające. Prosty sposób na zagwarantowanie sobie bezpieczeństwa jest zainstalowanie podstawowych warstw zabezpieczeń.
3. Należy ponadto pamiętać, że cyberprzestępcy szukają luk w oprogramowaniu, aplikacjach internetowych lub funkcjonowaniu przeglądarek i samych systemów operacyjnych, aby zdobyć dostęp do naszych danych. Kiedy więc uruchamia się funkcja aktualizacji systemu i masz okazję zaktualizować swój komputer, skorzystaj z niej!
4. Należy upewnić się, że witryna, na której robimy zakupy jest bezpieczna - na etapie płacenia ma w adresie URL „https”. Końcówka „s” zapewnia bezpieczeństwo, a więc gdy jesteś w bezpiecznej części witryny, zobaczysz w przeglądarce także ikonę z zamkniętą kłódką – w pasku adresu lub w prawym dolnym rogu.

Ale uwaga, podczas gdy ikona kłódki rzeczywiście wskazuje na pewien poziom bezpieczeństwa, nie stanowi stuprocentowego dowodu na to, że dana strona jest bezpieczna i legalna. Według informacji podanych na brytyjskiej rządowej stronie GetSafeOnline (http://www.getsafeonline.org/nqcontent.cfm?a_id=1133) symbol kłódki dowodzi jedynie, że właściciele witryny posiadają cyfrowy certyfikat zatwierdzenia przez zaufanego dostawcę, takiego jak VeriSign lub Thawte.

4. Warto zwrócić uwagę na zielony pasek adresu pojawiający się, kiedy odwiedzasz niektóre strony. Zielony pasek oznacza, że strona, na której jesteś, ma certyfikat SSL o rozszerzonej walidacji. Zobaczysz go na takich rodzajach stron, jak sklepy internetowe lub witryny przetwarzające dane osobowe.

Aby wyświetlać zielony pasek i aktywować wyższy poziom bezpieczeństwa dostępny w niektórych przeglądarkach, właściciel witryny musi przejść audyt przeprowadzony przez Urząd Certyfikacji. Urząd ten wymaga, aby właściciel witryny uwierzytelnił własność domeny i tożsamość organizacji, z którą jest ona powiązana.

Rozszerzona walidacja jest następnie kontrolowana przez organ, który przyznał certyfikat, nie przez właściciela witryny. Zapobiega to nadużyciom i nieodpowiedniemu wykorzystywaniu zielonego paska, gdyż jest on dostarczany oddzielnie, a nie wraz z witryną, którą odwiedzasz. Krótko mówiąc, oznacza to, że ze względu na zaangażowanie tej dodatkowej strony procesu walidacji trudniej jest dokonać phishingu i oszustwa internetowego.

5. Zachowuj zdrowy rozsądek! Rzadko istnieje potrzeba robienia dużych zakupów za pośrednictwem witryn, które nie mają renomy. Odwołuj się więc do swojej rozważności i rozwiń własny zmysł osądu transakcji internetowych. Przypominamy ponownie o konieczności zachowania takiego samego zdrowego rozsądku, jak podczas zakupów w zwykłych sklepach i o odpowiednim zabezpieczeniu antywirusowym – dzięki temu będziesz o jeden duży krok do przodu.

6. W przypadku jakichkolwiek wątpliwości dotyczących danej strony, nie przeprowadzaj za jej pośrednictwem transakcji ani nie udostępniaj na niej swoich danych osobowych.

AVG