W związku z coraz częstszymi przypadkami prób oszukiwania klientów korzystających z zakupów w Internecie Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich przygotowało kilka wskazówek, które zwiększą Twoje bezpieczeństwo.

1. Przed dokonaniem zakupów warto sprawdzić:

a) komentarze innych klientów na temat danego sprzedawcy internetowego

Komentarze dotychczasowych klientów to cenne źródło informacji nt. wiarygodności sprzedawcy. W większości przypadków w sieci bez trudu można znaleźć wiele cennych informacji dotyczących poszczególnych sprzedających. Pamiętaj, że komentarzy możesz także szukać na różnego rodzaju forach internetowych.

b) czy strona sprzedawcy internetowego jest właściwie zabezpieczona

Sprawdź czy strona jest właściwie zabezpieczona (czy jest nawiązana komunikacja z użyciem szyfrowania – początek adresu winien zaczynać się od skrótu: „https"). Równie istotne jest sprawdzenie ważności certyfikatu oraz dla kogo został wydany, klikając na symbol kłódki.

c) czy sprzedawca internetowy wykorzystuje do przeprowadzenia płatności znanego operatora płatności internetowych

Profesjonalnych sprzedawców internetowych obsługują bezpieczni i uznani operatorzy płatności internetowych. Ważne jest aby klienci w trakcie dokonywania zakupów mogli zalogować się do internetowych systemów transakcyjnych banków. Firmy świadczące usługi płatnicze w Internecie także weryfikują swoich klientów.

Zachowaj szczególną ostrożność, w sytuacji kiedy sprzedawca nie korzysta z usług operatora płatności internetowych, a rachunek bankowy do płatności prześle Ci za pośrednictwem e-mail'a.

d) datę uruchomienia sklepu internetowego tj. daty zarejestrowania domeny sklepu

Często zdarza się, że przestępcy dla potrzeb przygotowywanego przestępstwa otwierają fałszywe sklepy internetowe, jednak czasami zdarza się, że jednorazowo otwierają wiele sklepów, które w późniejszym okresie są wykorzystywane do przestępstw w sytuacjach, gdy kolejne są zamykane przez organy ścigania. Datę rejestracji domeny oraz inne informacje nt. danej domeny można pozyskać np. na stronie internetowej: https://centralops.net/co/domaindossier.aspx

Warto sprawdzić te informacje decydując się na zakupy bezpośrednio w sklepach internetowych. Jeśli chcesz dokonać zakupu w niedawno otwartym sklepie, to wcale nie jest jednoznaczne, że te sklep jest otwarty w celu popełniania przestępstw. W takich sytuacjach szczególnie należy wziąć pod uwagę informacje zawarte w pozostałych punktach *Dobrych praktyk*

2. Kupuj za pośrednictwem uznanych internetowych serwisów zakupowych tzn. takich, które działają od dłuższego czasu i cieszą się dobrą opinią kupujących

Zakupy w takich serwisach nie tylko pozwalają na wybór najkorzystniejszej oferty u wielu sprzedających, ale przede wszystkim dokonując tam zakupów, masz także gwarancję bezpieczeństwa. Takie serwisy prowadzą stałą weryfikację swoich sprzedawców, rejestrują każdą zawartą za ich pośrednictwem transakcję oraz posiadają dedykowany dział wsparcia klienta. Również płatności podlegają tam specjalnej ochronie. Najlepsze z nich oferują zwrot pieniędzy w przypadku nieotrzymania przedmiotu lub kiedy otrzymany towar istotnie różni się od tego oferowanego na stronie.

3. Unikaj płacenia za towar lub usługę kartą płatniczą bezpośrednio na stronie internetowej sklepu

Zdarza się, że przestępcy chcąc wyłudzić od Ciebie dane dotyczące kart płatniczych proszą o podanie informacji o numerze karty, dacie jej ważności, imieniu i nazwisku posiadacza, kodach CVV2 lub CVC2 oraz 3d Secure. Decydując się na zapłatę kartą w sieci zawsze upewnij się, że podajesz te informacje bezpośrednio na stronie agenta rozliczeniowego.

4. Uważaj na fałszywe strony podszywające się pod agentów rozliczeniowych

Adres prawdziwej strony internetowej agenta rozliczeniowego zawsze winien kończyć się nazwą domeny tego agenta np. dotpay.pl. Przestępcy coraz częściej aby uwiarygodnić podszycie się pod oficjalnie i legalnie działającego agenta wykupują certyfikat do domeny, której nazwa może łudząco być zbieżna z nazwą jego domeny (może się różnić chociażby jednym niepozornym znakiem np. zdublowaniem jakieś litery lub rozszerzenia).

Dlatego tak ważne jest nie tylko sprawdzanie czy jest wystawiony certyfikat ale również dla kogo został wystawiony. Przestępcy nie będą mogli wykupić certyfikatu np. dla dotpay.pl, gdyż on już jest wykupiony przez tę firmę.

5. Jeśli padłeś ofiarą oszustwa:

a) złóż zawiadomienie o podejrzeniu popełnienia przestępstwa organom ścigania (Policji lub Prokuraturze)

Udaj się do najbliższej Twojemu miejscu zamieszkania jednostki Policji lub Prokuratury. Zgłaszając sprawę organom ścigania, szczegółowo opisz i udokumentuj całą sytuację. Przekaż komplet posiadanych informacji i dokumentów: adres witryny, na której dokonałeś zakupu, dane sprzedającego (również teleadresowe), numer rachunku bankowego, na który została dokonana wpłata i dokument potwierdzający dokonanie zapłaty za towar. Możesz dołączyć również wydruki treści korespondencji prowadzonej ze sprzedającym oraz wydruk strony przedmiotu czy otrzymanego od nas e-maila potwierdzającego zawarcie transakcji, gdzie widoczne będą dane sprzedającego.

b) zawiadom swój bank i poinformuj go o złożeniu zawiadomienia o popełnieniu przestępstwa

Jeśli płatność została dokonana przy użyciu kart płatniczych klienci mogą złożyć reklamacje i w ramach charge back odzyskać pieniądze. Poinformuj bank o złożeniu zawiadomienia o popełnieniu przestępstwa do organów ścigania i przekaż wszystkie niezbędne informacje.

c) ostrzeż innych potencjalnych nabywców o przestępczym charakterze działalności prowadzonej przez danego sprzedawcę internetowego.

Ostrożnie formułuj opinie i komentarze nt. danego sprzedawcy internetowego. Pamiętaj, że wszelkie nieprawdziwe i szkalujące sprzedawcę opinie i komentarze mogą być powodem wytoczenia powództwa cywilnego z tytułu zniesławienia. Dlatego skup się na faktach związanych z zakupem, w wyniku którego poniosłeś straty finansowe.

Bankowe Centrum Cyberbezpieczeństwa, Związek Banków Polskich

Materiał powstał przy udziale: banków - członków BCC ZBP, Biura dw. z Cyberprzestępczością Komendy Głównej Policji, Allegro.pl oraz Ceneo.pl