Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
oraz
Komendy Głównej Policji
z dnia 2 grudnia 2021 r.
bezpieczne zakupy przedświąteczne

Zbliżający się czas Świąt Bożego Narodzenia to nie tylko otwierany codziennie przez dzieci kalendarz adwentowy czy świąteczna kolacja z najbliższymi, to także czas przygotowań, podczas którego zakupowy szał, pośpiech i roztargnienie będą nam towarzyszyć.

Te okoliczności staną się idealne dla przestępców, którzy korzystając z naszej nieuwagi będą próbowali skusić nas na „tańsze zakupy" lub używając manipulacji pozyskają od nas dane poufne, przy użyciu których dokonają transakcji „w naszym imieniu".

Dlatego powinniśmy szczególnie uważać na:

- oszukańcze witryny sklepowe podszywające się pod legalnie działających przedsiębiorców. Rolą ich jest wyłudzenie danych uwierzytelniających, które w dalszym kroku zostaną wykorzystane do bezprawnego logowania się do bankowości internetowej lub przeprowadzenia transakcji internetowej przy użyciu kart płatniczych.
- fałszywe sklepy internetowe, które proponują atrakcyjny towar po jeszcze bardziej atrakcyjnej cenie. Oczywiście towar, którego nie posiadają i w konsekwencji relacja taka prowadzi do strat finansowych klienta.

W czasie przedświątecznych porządków typujemy rzeczy, którym za pośrednictwem portali aukcyjnych oraz ogłoszeń w serwisach społecznościowych chcemy nadać drugie życie.
Tu również może czaić się oszustwo i powinniśmy zachować czujność, by w przypływie euforii wynikającej ze sprzedaży rzeczy zalegających w szafach, nie ulec manipulacji i nie przekazać oszustom danych własnej karty płatniczej lub poufnych danych do logowania się w bankowości elektronicznej.

Zbliżający się Nowy Rok , to czas nowych wyzwań i składanych sobie obietnic, to czas w którym cześć osób podejmie decyzje o ograniczeniu wydatków i skupieniu się na oszczędzaniu i pomnażaniu pieniędzy dlatego ważne jest by zachować zdrowy rozsądek i nie ulec oszustom którzy tworzą przestępcze platformy inwestycyjne, publikują reklamy, które zachęcają do inwestycji poprzez nielegalne wykorzystanie tożsamości osoby znanych: sportowców, celebrytów, polityków, a w przypadku braku znajomości zasad inwestowania oferują swoją pomoc i doradztwo. Taka reklama to oszustwo, a zainwestowane środki nigdy nie wracają do klienta.

W okresie przedświątecznym rekomendujemy zachowanie najwyższej ostrożności oraz stosowanie kilku ważnych zasad:

- weryfikuj sprzedawcę/usługodawcę w niezależnych źródłach informacji, szczególną uwagę poświęć na analizę negatywnych opinii, gdyż te mogą być bardziej miarodajnym źródłem informacji niż pozytywne opinie na temat tego sprzedawcy/usługodawcy;
- czytaj uważnie regulamin sprzedawcy/usługodawcy oraz sprawdzaj, czy zostały podane jego dane kontaktowe, czy adres istnieje i czy jest widoczny na mapach internetowych;
- przekazuj tylko te dane, które są niezbędne do przeprowadzenia płatności i dostawy towaru lub usługi;
- obserwuj czy podczas przeprowadzania transakcji nie pojawia się błąd płatności, a w następnym kroku pojawia się inny link do jej ponowienia, który będzie linkiem do podstawionej przez oszustów strony integratora płatności służącej do wyłudzenia danych poufnych;

- wybieraj platformę e-commerce lub dostawcę usługi płatniczej, który zaoferuje Ci ochronę, w przypadku, kiedy towar lub usługa nie zostanie dostarczona lub jakość jego będzie odbiegała od zadeklarowanej w ofercie;
- nie zgadzaj się na inny kontakt do płatności niż ten oficjalny dostarczony przez integratora płatności (np. nie płać poza platformą do e-handlu przelewem na nr podany w sms lub w czacie);
- uważnie czytaj wiadomości otrzymywane z banku za pośrednictwem komunikatów sms lub aplikacji mobilnej;
- nie instaluj dodatkowego oprogramowania, które jest „rzekomo" wymagane z uwagi na tzw. „bezpieczeństwo płatności" lub które umożliwi udzielenie Ci zdalnego wsparcia;
- nie klikaj na linki przesłane w niespodziewanych wiadomościach e-mail lub SMS'ach;
- jeśli zauważysz zmiany w wyglądzie strony internetowej swojego banku lub niestandardowe zachowania wstrzymaj realizację dyspozycji i niezwłocznie skontaktuj się ze swoim bankiem za pośrednictwem infolinii;
- czytaj ostrzeżenia przekazywane przez banki, Policję i FinCERT.pl – BCC ZBP.

W przypadku podejrzenia próby popełnienia przestępstwa lub gdy przestępstwo to zostało popełnione niezwłocznie poinformuj o tym fakcie swój bank oraz złóż stosowne zawiadomienie na Policję lub do Prokuratury.

Życzymy udanych zakupów i spokojnych Świąt!

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego
Komenda Główna Policji

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków oraz ich klientów.