BEZPIECZNE ZAKUPY PRZEDŚWIĄTECZNE - PORADNIK FINCERT.PL – BANKOWEGO CENTRUM CYBERBEZPIECZEŃSTWA ZBP ORAZ KOMENDY GŁÓWNEJ POLICJI

Data publikacji 15.04.2022

Przed nami kolejne Święta i większa aktywność zakupowa, zarówno w sklepach stacjonarnych, jak i w Internecie. Coraz częściej kupujemy w Internecie nie tylko zakupy okazjonalne, ale także produkty codziennego użytku. Długa lista zakupów, pośpiech i „gorączka zakupowa” to idealne warunki dla przestępców, którzy wykorzystują naszą nieuwagę i przy użyciu różnych metod będą chcieli wyłudzić od nas pieniądze. Dlatego po raz kolejny FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP oraz Komenda Głównej Policji zwracają się do Państwa z prośbą o zapoznanie się z wybranymi praktycznymi poradami, dzięki którym zasiądziecie Państwo przy świątecznym stole z satysfakcją i radością, że nie ulegliście oszustom.

Szczególnie przestrzegamy przed:

- klikaniem w linki z wiadomościami SMS lub e-mail, które będą dotyczyły dostarczenia przesyłki kurierskiej. Ich rolą 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;
- fałszywymi sklepami internetowymi, które proponują atrakcyjny towar w konkurencyjnej cenie – proszę wierzyć, ale prawdziwe okazje trafiają się niezmiernie rzadko;
- zbiórkami związanymi z organizacją spotkań świątecznych dla uchodźców wojennych. Wszystkie tego typu kwesty powinny być dokładnie zweryfikowane przez darczyńcę przed udzieleniem wsparcia. Pamiętajmy w tym roku Prawosławne Święta Wielkanocne przypadają na 24 kwietnia, co oznacza, że będziemy dłużej narażeni na ekspozycje działań oszustów.

Jak się chronić? - należy stosować się do kilku ważnych zasad:

1. zawsze należy uważnie czytać treść SMS-ów, jakie przychodzą na telefon lub komunikatów w aplikacji mobilnej w trakcie potwierdzania chęci zapłaty za towar, lub usługę;
2. nigdy nie ujawniać kodów 3D Secure wykorzystywanych do autoryzacji transakcji kartowych w Internecie;

3. weryfikować 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;
4. czytać uważnie regulamin sprzedawcy/usługodawcy oraz sprawdzać, czy zostały podane jego dane kontaktowe, czy adres istnieje i czy jest widoczny na mapach internetowych;
5. wybieraj uznaną platformę e-commerce lub dostawcę usługi płatniczej, którzy oferują ochronę kupującego, w przypadku, kiedy towar lub usługa nie zostanie dostarczona, lub jakość jego będzie odbiegała od zadeklarowanej w ofercie.

W przypadku podejrzenia próby popełnienia przestępstwa lub gdy przestępstwo to zostało popełnione należy niezwłocznie poinformować o tym fakcie swój bank oraz złożyć stosowne zawiadomienie na Policję, lub do Prokuratury. Szybkość złożenia takiego zawiadomienia może zwiększyć szansę uratowania utraconych środków, które fizycznie mogły jeszcze nie zostać wypłacone przez oszustów.

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.