10.12.2021

Ostrzeżenie przed zagrożeniami

Szanowni Klienci,

w związku ze zbliżającym się okresem świątecznym ostrzegamy przed nasilającymi się próbami oszustw związanych z fałszywymi sklepami internetowymi, próbami oszustw polegających na podszywaniu się pod firmy kurierskie, czy też oszustw skierowanych na użytkowników (kupujących, sprzedających) serwisu internetowego OLX.

Ostrzegamy również przed działaniami przestępców podszywających się pod pracowników banków, bądź innych zaufanych instytucji, wskazujących klientom na zagrożenie ich środków finansowych ulokowanych w banku i/lub nakłaniających do instalowania na urządzeniu klienta zewnętrznych aplikacji.

Celem takich działań jest **wyłudzenie danych wrażliwych dotyczących kart płatniczych lub serwisu bankowości elektronicznej, bądź bezpośrednie wyłudzenie środków finansowych**.

Na co zwrócić szczególną uwagę?

Szczególną uwagę zwracać należy na wszelkie zdarzenia związane z:

- **niedostępnością danej metody płatności** - w fałszywym e-sklepie zazwyczaj mamy dostępną tylko jedną opcję płatności - karta płatnicza przez Internet. Sklep internetowy powinien oferować kilka metod płatności za zakupiony towar np. za pośrednictwem systemów szybkich płatności m.in. PayU, Dotpay, Przelewy24 oraz opcję płatności przy odbiorze zamówienia. Jeśli sklep, w którym zdecydowałeś się robić zakupy oferuje tylko jedną metodę płatności, lepiej zrezygnuj z robienia w nim zakupów. Jeśli jest to opcja płatności kartą - weryfikuj każdorazowo na jakiej stronie wpisujesz jej dane;

- **brakiem szyfrowanego połączenia (SSL) lub błędem certyfikatu SSL** – wszelkie komunikaty o braku szyfrowanego połączenia lub błędnego certyfikatu SSL zgłaszane w trakcie otwierania strony internetowej sklepu powinny każdorazowo wzbudzić naszą wątpliwość;

- **podejrzaną nazwa domeny** - zawsze należy zwracać uwagę na domenę widoczną w pasku adresu przeglądarki - przestępcy często tworzą nazwy sklepów, które łudząco przypominają oryginał;

- **niepoprawną polszczyzną** – często treść stron internetowych fałszywych sklepów i prezentowanych w nich ofert zawiera np. błędy składniowe wynikające z użycia przez oszusta do ich przygotowania np. translatora językowego; wszelkie tego typu symptomy powinny każdorazowo wzbudzić naszą wątpliwość;

- **wyjątkowo atrakcyjną ofertą cenową** – często oszuści podszywają się (tzw. phishing) pod istniejące, znane sklepy, przyciągając klientów mocno zaniżonymi cenami oferowanych produktów; warto zawsze porównywać ceny w kilku sklepach lub korzystać np. z internetowych porównywarek cen;

- **błędami i komunikatami wyświetlanymi na stronie np. komunikaty o niedostępności regulaminu, danych kontaktowych sklepu, itp.** – często chcąc sprawdzić wybrane dane o sklepie, np. kontakt, regulamin, formy płatności, itd. prezentowany jest np. komunikat: „trwają prace serwisowe,

spróbuj ponownie później", „strona niedostępna”, „strona w przygotowaniu”, itp.. Tego typu komunikaty powinny każdorazowo wzbudzić naszą wątpliwość.

- **podejrzanymi wiadomościami e-mail i/lub SMS podszywającymi się pod firmy kurierskie** - w treści takich wiadomości przestępcy często informują np. o konieczności dopłaty do paczki z powodu jej dezynfekcji lub o tym, że paczka jest przechowywana w magazynie, zachęcając do dokonania wpłaty pieniędzy i/lub ponownego doręczenia przesyłki (przykłady takich wiadomości poniżej). Jeśli otrzymałeś tego typu wiadomość e-mail/ SMS zawsze zweryfikuj, kto jest jej nadawcą. Pamiętaj także, że adres e-mail, który widzisz, może nie być prawdziwy – pod wyświetloną nazwą może kryć się adres skrzynki oszusta. Zanim klikniesz w jakikolwiek link w treści podejrzanej wiadomości najedź kursorem na link i co bardzo ważne **– bez klikania! w niego** – zobacz do jakiej strony prowadzi. Dokładnie przeczytaj adres strony, może się on różnić od prawdziwej strony operatora płatności tylko jednym znakiem. Nie klikaj, gdy nie rozpoznajesz adresu.

- **podejrzanymi telefonami od osób podszywających się pod pracowników banku lub innej zaufanej instytucji** - w toku rozmowy przestępcy często podają się pod pracowników banki i wykorzystują pretekst weryfikacji podejrzanego logowania, czy też transakcji i proszą o instalację oprogramowania umożliwiającego przejęcie kontroli nad urządzeniem (np. AnyDesk, TeamViewer). Często podszywają się również pod pracowników zaufanych instytucji (np. policjantów) i wykorzystując pretekst zagrożenia finansów klienta w banku, proszą o przekazanie środków na wskazane „konto techniczne” lub ich przekazanie w formie gotówkowej. Pamiętaj, aby nigdy nie podawać nadmiarowych informacji przez telefon oraz należycie chronić dane dotyczące kart płatniczych, dane logowania do bankowości elektronicznej, czy też dane dotyczące transakcji. Pamiętaj także, że przestępcy korzystając z metody tzw. spoofingu, mogą również podszywać się pod numer telefonu banku lub innej firmy/ instytucji.

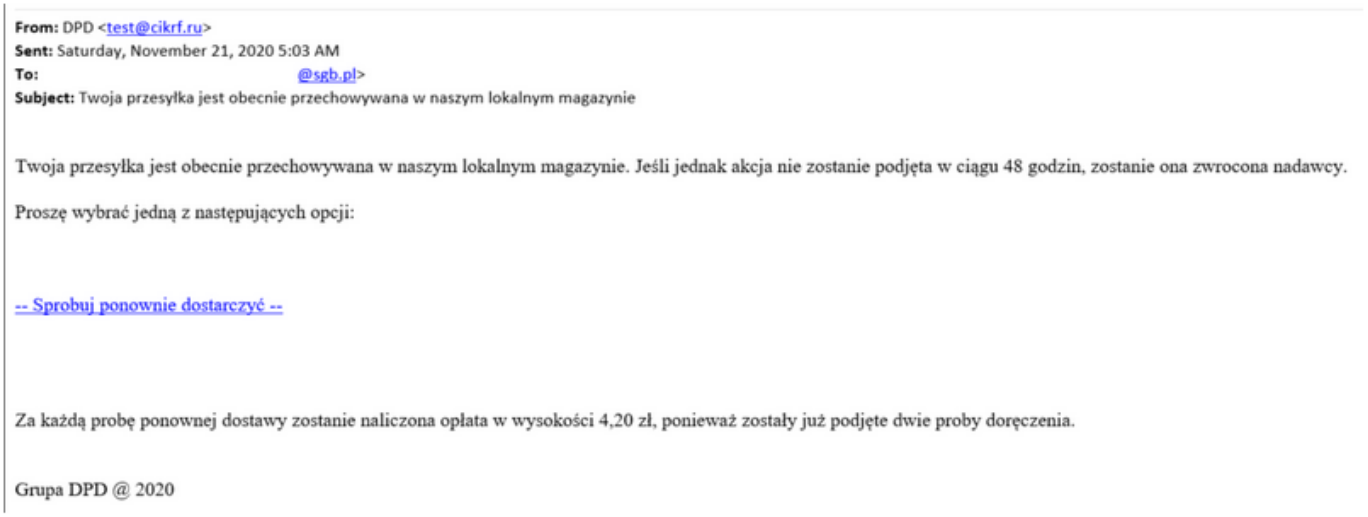
W razie jakichkolwiek wątpliwości skontaktuj się z placówką Banku obsługującą rachunek lub Infolinią SGB:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

Przypominamy:

- **w przypadku jakichkolwiek podejrzeń co do autentyczności sklepu/ oferty należy zaniechać zakupów. Zawsze przed dokonaniem zakupów warto także zweryfikować opinie innych użytkowników o sklepie i/lub osobie sprzedającej,**
- **nigdy nie klikaj w linki przesłane w podejrzanych wiadomościach e-mail/ SMS – nie otwieraj też podejrzanych załączników – zawarte w nich złośliwe oprogramowanie może spowodować zainfekowanie urządzenia i utratę danych,**
- **chroń swoje dane wrażliwe i nigdy nie podawaj nadmiarowych informacji przez telefon. W razie jakichkolwiek wątpliwości zakończ rozmowę i skontaktuj się osobiście z placówką banku lub zaufaną instytucją.**

Przykłady wiadomości (e-mail i SMS) podszywających się pod firmę kurierską:



From: DPD <test@cikrf.ru>
Sent: Saturday, November 21, 2020 5:03 AM
To: @sgb.pl>
Subject: Twoja przesyłka jest obecnie przechowywana w naszym lokalnym magazynie

Twoja przesyłka jest obecnie przechowywana w naszym lokalnym magazynie. Jeśli jednak akcja nie zostanie podjęta w ciągu 48 godzin, zostanie ona zwrocona nadawcy.

Proszę wybrać jedną z następujących opcji:

-- Sprobuj ponownie dostarczyć --

Za każdą probę ponownej dostawy zostanie naliczona opłata w wysokości 4,20 zł, ponieważ zostały już podjęte dwie proby doręczenia.

Grupa DPD @ 2020