Pomagamy chronić Państwa firmę przed nadużyciami i przestępczością finansową

HSBC bardzo poważnie podchodzi do kwestii nadużyć i innych przestępstw finansowych. Mimo, że stosujemy najlepsze na rynku systemy wykrywania nadużyć finansowych to chcemy, aby byli Państwo świadomi różnych sposobów, w jaki przestępcy mogą próbować dokonać kradzieży nie tylko Państwa pieniędzy, ale i tożsamości firmy.

Oto kilka wskazówek na temat tego, jak uchronić się przed nadużyciem finansowym lub oszustwem. Prosimy przeanalizować ten dokument wraz z naszymi Ogólnymi Warunkami.

Oszustwo metodą Business Email Compromise (BEC)
Business Email Compromise (BEC) jest wyrafinowaną metodą oszustwa wymierzoną w przedsiębiorstwa współpracujące z zagranicznymi dostawcami lub kontrahentami, które regularnie dokonują płatności na podstawie wiadomości email od właściciela firmy (Dyrektora Generalnego lub Dyrektora Finansowego) traktowanych, jako upoważnienie do dokonania takiej płatności. Osoba obsługująca płatności może nie zorientować się, że dany email nie jest autentycznym poleceniem wydanym przez szefa, ale tzw. oszustwem na prezesa.

Istnieją dwa warianty tego typu oszustwa:

- **Spoofing** – polegający na zmanipulowaniu adresu poczty elektronicznej w taki sposób, aby adres nadawcy wydawał się pochodzić od innej osoby lub z innego miejsca niż w rzeczywistości.
  - Oszuści fabrykują adres i wiadomość email rzekomego dostawcy w celu przedłożenia zmodyfikowanej faktury. To działanie nie wymaga włamywania się do systemu poczty elektronicznej dostawcy, za to faktura zostaje wysłana z adresu tak zbliżonego do adresu w domenie używanej przez dostawcę, że większość osób nie zauważy takiej różnicy — np.:
  - @CompanyABC.com zamiast @CompanyACB.com.
- **Włamanie na konto poczty elektronicznej** – czyli przejęcie konta email członka kadry kierowniczej, np. dyrektora finansowego. Oszust wysyła prośbę o płatność z przejętego konta poczty elektronicznej do innego, często niższego rangą pracownika, który traktuje taką wiadomość jak polecenie.

Do zapamiętania:

1. Należy zadbać o to, aby pracownicy wiedzieli, że należy sprawdzać adres poczty elektronicznej, z którego nadchodzi wiadomość z żądaniem zapłaty, oraz stosować odpowiednie metody weryfikacji wszelkich nowych żądań zapłaty otrzymywanych pocztą elektroniczną.

2. Należy zawsze regularnie dokonywać przeglądu sposobów weryfikacji, aby mieć pewność, że wdrożone zostały odpowiednie mechanizmy kontroli płatności, by nie paść ofiarą tego rodzaju oszustwa.

Przekierowanie płatności/oszustwa dotyczące faktur
Metoda ta polega na próbie przekonania firmy, że nastąpiła zmiana danych rachunku bankowego odbiorcy danej płatności. Oszuści podają się za stałego dostawcę przedsiębiorstwa i informują o zmianie danych rachunku bankowego.

Może to obejmować także:

- tworzenie fikcyjnej dokumentacji klientów i rachunków bankowych w celu wygenerowania fałszywych płatności.

Jak zmniejszyć ryzyko stania się ofiarą oszustwa dotyczącego faktury:

- Należy upewnić się, że pracownicy, którzy przetwarzają faktury i żądania zapłaty, są świadomi tego scenariusza oszustwa, gdy wprowadzają zmiany do ustalonych dyspozycji zapłaty.
- Należy zawsze weryfikować zmiany w uzgodnieniach finansowych z dostawcą, kontaktując się z nim bezpośrednio według danych kontaktowych zapisanych w dokumentacji.

HSBC

Phishing
Jest to sytuacja, w której pracownicy otrzymują emaile przekierowujące ich do stron internetowych, na których są proszeni o podanie poufnych danych osobowych lub finansowych. Mimo że takie emaile mogą sprawiać wrażenie pochodzących z działającej zgodnie z prawem strony internetowej, faktycznie służą one do kradzieży danych osobowych i są wykorzystywane do uzyskania dostępu do konta lub rachunku bankowego ofiary. To działanie zwane jest phishingiem. Nie wolno odpowiadać na taki email ani klikać zawartego w nim łącza, które ostrzega, że rachunek może zostać zamknięty, jeżeli nie potwierdzą Państwo swoich danych osobowych. W przypadku otrzymania takiej wiadomości należy skontaktować się z firmą nadawcy za pomocą pewnej metody — np. dzwoniąc pod uwierzytelniony numer telefonu.

Podejrzaną wiadomość email należy natychmiast skasować.

Vishing
To sytuacja, w której oszust telefonuje do przedsiębiorstwa, podając się za pracownika banku, funkcjonariusza policji, stałego dostawcę/klienta lub inną osobę godną zaufania. Taki telefon może zostać wykonany w celu nakłonienia osoby zarządzającej finansami przedsiębiorstwa do:

- wysłania pieniędzy na inny rachunek często rzekomo w celu „bezpiecznego przechowania" lub „zamrożenia" środków;
- wypłacenia gotówki i przekazania jej oszustom;
- podania osobistych danych finansowych, które można następnie wykorzystać w celu uzyskania dostępu do rachunków bankowych firmy.

Do zapamiętania:
1. Należy zachować ostrożność, odbierając nieznane połączenia telefoniczne, w szczególności jeżeli rozmówca prosi o podanie jakichkolwiek niejawnych informacji firmowych.

2. Jeżeli rozmowa wydaje się podejrzana, należy bez obaw ją zakończyć, odmawiając podania informacji.

3. Rozmowę muszą zakończyć obie jej strony, dlatego należy upewnić się, że rozmówca również się rozłączył i linia jest wolna; można wykorzystać inną linię telefoniczną w celu sprawdzenia numeru.

4. Oszuści mogą podszyć się pod inny numer telefonu (tzw. „call spoofing"), który na wyświetlaczu przypomina numer telefonu należący do banku.

5. HSBC nigdy nie dzwoni z prośbą o wygenerowanie kodu klucza bezpieczeństwa przez naciśnięcie żółtego przycisku lub podanie numeru PIN.

6. Nie należy nigdy udostępniać danych zabezpieczających firmy osobom spoza grona upoważnionego personelu. Należy chronić dane swojego konta i dane zabezpieczające.

Przestępcy mogą już mieć podstawowe informacje o firmie (np. nazwę, adres, dane konta). Nie należy zakładać, że dzwoniący jest osobą, za którą się podaje tylko dlatego, że ma te informacje lub twierdzi, że jest przedstawicielem legalnego podmiotu.

Oszustwa czekowe
Ten rodzaj oszustwa polega na modyfikacji, podrabianiu lub fałszowaniu czeków wystawionych w ciężar rachunku bankowego ofiary. Jeżeli Państwa firma lub kontrahenci korzystają z czeków, poniżej znajdą Państwo wskazówki, jak nie stać się ofiarą oszustwa czekowego i zminimalizować takie ryzyko:

- Należy sprawdzać czeki. Należy dodawać do nich dodatkowe informacje, takie jak numer referencyjny rachunku.
- Czeki należy podpisywać pełnym podpisem, a nie tylko inicjałami.
- Należy porównywać swoje odcinki wypłat na czekach z wyciągiem z rachunku. Należy jak najszybciej informować o rozbieżnościach.
- Należy przechowywać wszelkie dodatkowe książeczki czekowe w bezpiecznym miejscu.

Ochrona karty
- Nową kartę należy podpisać i aktywować niezwłocznie po jej otrzymaniu.
- Kartę można aktywować za pośrednictwem bankowości internetowej, kontaktując się z opiekunem klienta (RM) lub korzystając z bankomatu HSBC (dotyczy kart debetowych Visa, o ile nie został nadany nowy PIN).
- Jeżeli nowa karta nie dotrze na minimum tydzień przed upływem daty ważności poprzedniej karty, należy skontaktować się z opiekunem klienta (RM).

Ochrona PIN
- Nigdy nie należy zapisywać ani utrwalać w inny sposób swoich numerów PIN i innych szczegółów dotyczących bezpieczeństwa w sposób, który może być zrozumiały dla innej osoby.
- Zawiadomienie o nadanym PIN należy możliwie jak najszybciej zniszczyć.
- Należy wybrać PIN, którego nie można skojarzyć z użytkownikiem oraz który nie jest prostym ciągiem cyfr, takim jak 1234 lub 1111. Najlepiej jest wybrać losową kombinację lub sekwencję cyfr, które z jakiegoś powodu są dla Państwa istotne.

Ochrona przy bankomacie
- Na bankomacie może być zamontowane urządzenie, które umożliwia oszustowi kradzież karty lub przechwycenie informacji zapisanych na pasku magnetycznym. W przypadku zauważania czegoś niezwykłego zamontowanego na bankomacie nie należy próbować tego usunąć. Należy oddalić się od urządzenia i zatelefonować do naszego zespołu ds. zagubionych i skradzionych kart (pod numer podany w przydatnych kontaktach poniżej) lub na policję.
- Należy stawać blisko bankomatu i wpisywać PIN, zasłaniając klawiaturę drugą dłonią. Przed podjęciem próby kradzieży karty przestępcy mogą starać się obserwować osobę wpisującą PIN.
- Jeżeli bankomat nie zwróci karty, nie należy ponownie wpisywać PIN. Należy niezwłocznie zgłosić utratę karty opiekunowi klienta (RM).

Ochrona kart firmowych przy płatnościach przez telefon
- Przy dokonywaniu płatności kartą przez telefon należy mieć kartę przed sobą, ponieważ może zaistnieć konieczność podania informacji, takich jak data ważności karty, jej numer oraz trzycyfrowy kod bezpieczeństwa na pasku podpisu. Nie należy jednak NIGDY ujawniać numeru PIN przez telefon, nawet na prośbę o jego podanie.
- Należy unikać podawania informacji dotyczących karty w miejscach publicznych, gdzie mogą je usłyszeć inne osoby.
- Należy żądać potwierdzenia transakcji pocztą zwykłą lub elektroniczną.

Ochrona podczas fizycznej płatności kartą

- Podczas wprowadzania numeru PIN należy starać się zasłaniać klawiaturę ręką.
- W przypadku napotkania jakichkolwiek problemów podczas korzystania z karty należy skontaktować się z opiekunem klienta (RM).
- Karty płatnicze należy przechowywać w bezpiecznym miejscu.

Ochrona podczas płatności kartą w internecie

- Zakupów należy dokonywać wyłącznie na bezpiecznych stronach internetowych — strona żądająca wprowadzenia danych osobowych musi być oznaczona ikoną bezpieczeństwa (zamknięta kłódka) w oknie przeglądarki.
- Należy wydrukować kopię potwierdzenia zamówienia. Powinny na nim widnieć również adres pocztowy i numer telefonu.
- Przy płaceniu kartą kredytową w internecie należy zawsze korzystać z funkcji MasterCard Securecode lub Verified by Visa. Oferują one dodatkową ochronę z wykorzystanie osobistego hasła.

Ochrona haseł

- Należy stosować różne hasła dla różnych systemów.
- Nie należy ulegać pokusie używania haseł, które można łatwo odgadnąć — takich jak imiona lub daty urodzenia dzieci.
- Nigdy nie zaleźy zapisywać haseł, ale jeżeli nie ma innej alternatywy, należy zapisać je w sposób niezrozumiały dla nikogo innego.
- Zamiast wykorzystywać nazwisko panieńskie matki jako hasło kontrolne, należy rozważyć użycie np. imienia bohatera ulubionej kreskówki lub innej fikcyjnej postaci.
- Należy używać kombinacji cyfr oraz wielkich i małych liter w celu wzmocnienia hasła.

... oraz ochrona firmy i samego siebie przed kradzieżą tożsamości

Korzystając z różnych metod, przestępcy mogą uzyskać ważne dane osobowe i dane dotyczące tożsamości, takie jak numery kart kredytowych, daty ich ważności, daty urodzenia lub nazwiska panieńskie matki. Takie informacje mogą zostać wykorzystane do uzyskania dostępu do rachunków bankowych lub otwarcia nowych linii kredytowych.

Można pomóc w minimalizowaniu tego ryzyka poprzez podjęcie następujących prostych kroków:

- Należy niszczyć wszystkie otrzymane dokumenty lub pisma, które zawierają nazwę i adres firmy lub dane osobowe. Należy zrezygnować z wyciągów otrzymywanych tradycyjną pocztą, eliminując wysyłanie zbędnych dokumentów tą drogą.
- Należy skonfigurować swój bezpieczny numer telefonu, ponieważ w ten sposób możemy bezpiecznie zidentyfikować osoby kontaktujące się z nami telefonicznie.
- Nie należy podawać bezpiecznego numeru telefonu nikomu, kto się z Państwem kontaktuje. HSBC NIGDY nie prosi o podanie bezpiecznego numeru telefonu, jeżeli sam jest inicjatorem połączenia.
- W przypadku zagubienia ważnych dokumentów (np. paszportu), lub jeżeli zostały one skradzione, należy rozważyć ich niezwłoczne zastrzeżenie.

Jeżeli Państwa firma padnie ofiarą oszustwa, należy pamiętać o zgłoszeniu takiego zdarzenia do HSBC tak szybko jak to możliwe za pośrednictwem opiekuna klienta (RM).