BIZNESOWE OSZUSTWO "NA DYREKTORA"

Oszuści podszywają się pod dyrektora, żeby skłonić pracownika do zapłaty fałszywej faktury lub wykonania nieautoryzowanego przelewu z konta firmowego.

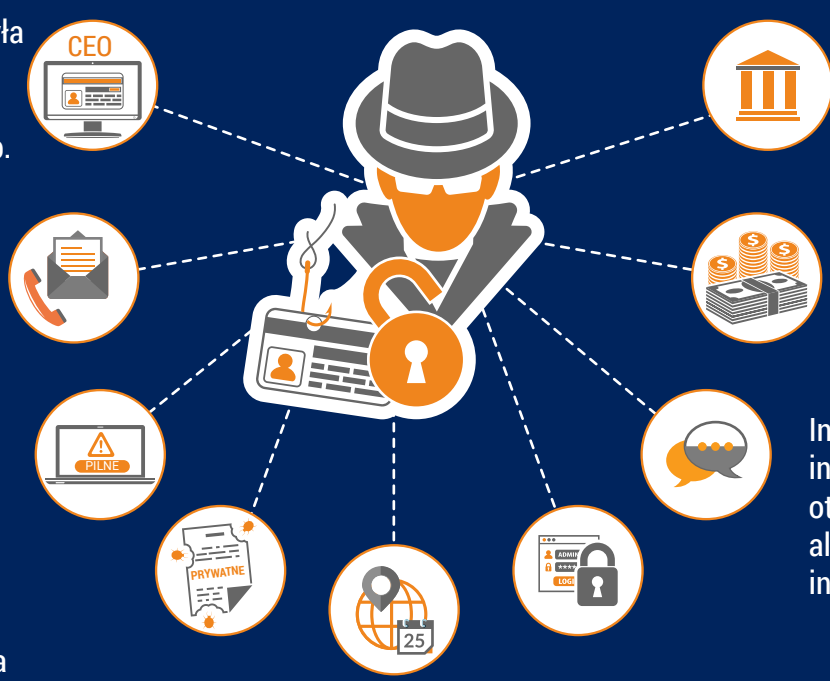
JAK TO DZIAŁA?

Oszust dzwoni lub wysyła e-mail, podszywając się pod osobę wysoko postawioną w firmie (np. dyrektora, dyrektora ds. finansów).

Jest dobrze poinformowany o strukturze organizacji.

Domaga się zlecenia natychmiastowego przelewu.

Gra na emocjach, używa zwrotów, takich jak: "poufność", "firma Ci ufa", "jestem obecnie niedostępny".



Jako argumentu używa wyjątkowej sytuacji (kontrola podatkowa, przejęcie firmy, fuzja).

Często prośba dotyczy płatności na konto w banku spoza Europy.

W efekcie pracownik przelewa pieniądze na konto oszustów.

Informuje, że dalsze instrukcje pracownik otrzyma później, mailowo albo za pośrednictwem innych osób.

Prosi, aby pracownik pominął standardowe procedury autoryzacji płatności.

JAK ROZPOZNAĆ SCAM?

- Otrzymujesz niespodziewany e-mail/telefon.
- Kontaktuje się z Tobą osoba wysoko postawiona w firmie, z którą na co dzień nie współpracujesz.
- Jesteś proszony o zachowanie całkowitej poufności.
- Wyczuwasz presję. Zadanie ma być wykonane jak najszybciej.
- Otrzymujesz niecodzienne żądanie, które jest niezgodne z procedurami wewnętrznymi.
- Słyszysz pochwały, groźby albo obietnice nagrody.

CO MOŻESZ ZROBIĆ?

JAKO FIRMA

Bądź świadomy ryzyka i **ostrzeż o nim swoich pracowników.**

Poproś, aby pracownicy traktowali **polecenia przelewów z największą ostrożnością**.

Stwórz **wewnętrzne procedury dotyczące płatności.**

Wprowadź procedury **sprawdzania płatności,** które są zlecane mailowo.

Stwórz **procedury raportowania scamów i oszustw.**

Sprawdź, czy na stronie internetowej firmy nie ma informacji, które umożliwiają poznanie struktury przedsiębiorstwa. **Uważaj co publikujesz** w mediach społecznościowych.

Zaktualizuj zabeczpieczenia techniczne.

Zawsze informuj policję o próbach oszustwa, nawet jeśli nie zostałeś ofiarą scamu.

JAKO PRACOWNIK

Stosuj się do procedur bezpieczeństwa, szczególnie tych związanych z płatnościami. **Nigdy nie ulegaj presji i nie pomijaj procedury autoryzacji.**

Uważnie **sprawdzaj adres e-mail,** szczególnie gdy wiadomość zawiera informacje poufne/zlecenie przelewu.

Gdy masz wątpliwości, **skonsultuj się z innym** pracownikiem.

Nigdy nie otwieraj podejrzanych załączników i linków otrzymanych w e-mailu. Zachowaj szczególną ostrożność, gdy sprawdzasz prywatną pocztę na firmowym komputerze.

Nie podawaj zbyt wiele informacji i zachowaj ostrożność w mediach społecznościowych.

Nie udostępniaj informacji o strukturze firmy, hierarchii, bezpieczeństwie i obowiązujących procedurach.

Jeśli otrzymasz podejrzaną wiadomość albo telefon - zawsze skontaktuj się z działem IT.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

OSZUSTWA INWESTYCYJNE

Typowe oszustwa inwestycyjne zawierają kuszącą obietnicę zysku poprzez inwestycje w akcje, obligacje, kryptowaluty, rzadkie metale, zagraniczne inwestycje gruntowe lub alternatywne źródła energii.

JAK ROZPOZNAĆ SCAM?

- Rozmówca obiecuje Ci szybkie zyski i zapewnia, że inwestycja jest bezpieczna.
- Oferta jest ograniczona czasowo.
- Wielokrotnie otrzymujesz podejrzane telefony.
- Oferta jest dostępna tylko dla Ciebie i jesteś proszony, aby nie udostępniać jej innym osobom.

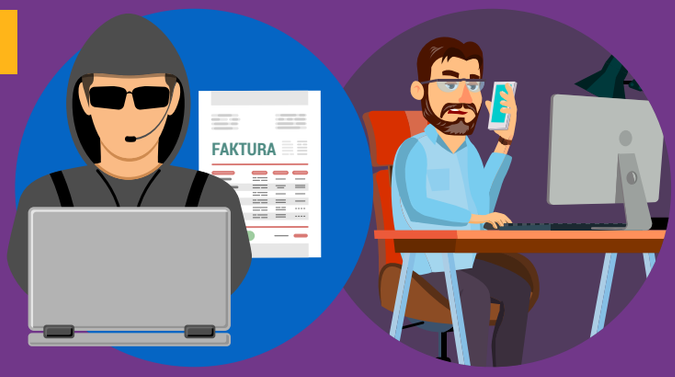
CO MOŻESZ ZROBIĆ?

- Zasięgnij **bezstronnej porady finansowej,** zanim przekażesz pieniądze na jakąkolwiek inwestycję.
- **Nie ufaj telefonom** zachęcającym do inwestycji, szczególnie gdy nie znasz rozmówcy.
- **Bądź podejrzliwy,** gdy ktoś oferuje Ci bezpieczne inwestycje lub gwarancję dużych zysków.
- **Uważaj na oszustów,** szczególnie jeśli kiedyś padłeś ofiarą scamu. Możesz być uważany za łatwy cel.
- Jeśli masz jakiekolwiek wątpliwości, **skontaktuj się z policją.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

WYŁUDZENIA "NA FAKTURĘ"



JAK TO DZIAŁA?

- Z firmą kontaktuje się osoba, która podaje się za reprezentanta dostawcy / usługodawcy / wierzyciela.
- Oszust może kontaktować się osobiście, telefonicznie, mailowo albo listownie.
- Oszust informuje o zmianie danych do płatności przyszłych faktur. Podaje namiary na nowe, kontrolowane przez siebie konto.

CO MOŻESZ ZROBIĆ?

JAKO FIRMA

Upewnij się, że **pracownicy są poinformowani o możliwości oszustwa** i będą potrafili go uniknąć.

Poinstruuj zespół odpowiedzialny za płatności, żeby zawsze **uważnie sprawdzał dane.**

Stwórz **procedurę weryfikacji danych** do płatności.

Przejrzyj stronę internetową firmy, jeśli to możliwe usuń z niej informacje o dostawcach i usługodawcach. Zwróć uwagę jakie informacje o firmie umieszczają pracownicy w mediach społecznościowych.

JAKO PRACOWNIK

Sprawdzaj żądania rzekomo pochodzące od Twoich wierzycieli, zwłaszcza jeśli poproszą Cię o zmianę danych bankowych dotyczących przyszłych faktur.

Dla płatności powyżej wyznaczonego pułapu, **utwórz procedurę potwierdzającą** prawidłowe dane do przelewu oraz odbiorcę (np. spotkanie z firmą).

Nie korzystaj z danych kontaktowych umieszczonych w podejrzanej wiadomości. Użyj namiarów wykorzystywanych we wcześniejszej korespondencji.

Po opłaceniu faktury **wyślij potwierdzenie e-mailem**. Dla bezpieczeństwa podaj nazwę banku beneficjenta i cztery ostatnie cyfry z numeru konta.

W każdej ze współpracujących firm **ustal jedną osobę kontaktową** w sprawie płatności. Domagaj się jej autoryzacji w przypadku jakichkolwiek zmian.

Ogranicz informacje, które udostępniasz o swoim pracodawcy w mediach społecznościowych.

Skontaktuj się z policją, jeżeli podejrzewasz oszustwo, nawet jeśli nie padłeś jego ofiarą.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

OSZUSTWA W SKLEPACH INTERNETOWYCH

Oferty sklepów internetowych mogą być świetną okazją nie tylko dla Ciebie, ale również dla oszustów.

CO MOŻESZ ZROBIĆ?

- **Korzystaj z krajowych sklepów internetowych,** gdy masz taką możliwość. Będziesz wiedział z kim się kontaktować, jeśli zajdzie taka potrzeba.
- **Sprawdź opinie** o sklepie, zanim cokolwiek w nim kupisz.

- **Płać kartą kredytową -** będziesz mieć większe szanse odzyskania pieniędzy.
- **Płać używając bezpiecznej usługi płatniczej -** uważaj na sklepy, które akceptują jedynie przelewy.
- Płać przez internet tylko, gdy **jesteś połączony z bezpieczną siecią** - unikaj bezpłatnego lub publicznego Wi-Fi.
- Używaj do płatności bezpiecznego urządzenia - **aktualizuj system operacyjny i oprogramowanie zabezpieczające.**
- Strzeż się reklam oferujących **cudowne produkty i podejrzane przeceny** - jeśli coś brzmi zbyt pięknie, raczej nie jest prawdziwe!
- Wyskakujące okno informuje, że wygrałeś nagrodę? **Zastanów się zanim klikniesz -** możesz wygrać wirusa.
- Jeśli nie otrzymasz produktu, skontaktuj się ze sprzedawcą. Nie odpowiada? **Zadzwoń do banku.**

Zawsze zgłaszaj policji wszelkie próby oszustwa, nawet jeśli ostatecznie nie padłeś ofiarą.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

PHISHING - WYŁUDZANIE INFORMACJI

Phishing to rozsyłanie e-maili, które oszukują odbiorców i namawiają do udostępnienia danych osobowych, finansowych lub dotyczących bezpieczeństwa.

JAK TO DZIAŁA?

Fałszywe wiadomości e-mail:

mogą wyglądać dokładnie tak, jak standardowa korespondencja z banku.

zawierają logo banku, mają układ i tekst przypominający prawdziwe e-maile.

namawiają do ściągnięcia załącznika lub kliknięcia na link zawarty w wiadomości.

używają sformułowań, które mają wywrzeć na Tobie presję i nakłonić do działania.

CO MOŻESZ ZROBIĆ?

- **Pamiętaj o aktualizacji oprogramowania,** w tym przeglądarki, programu antywirusowego i systemu operacyjnego.
- Zachowaj **szczególną czujność,** jeśli wiadomość e-mail od banku wymaga podania poufnych informacji (np. danych do logowania).
- **Przyjrzyj się dokładnie wiadomości:** porównaj adres z wcześniejszą korespondencją z bankiem. Sprawdź, czy nie ma błędów w pisowni i gramatyce.
- **Nie odpowiadaj na podejrzane wiadomości e-mail.** Prześlij je do swojego banku ręcznie wpisując adres.
- **Nie ściągaj załączników i nie klikaj w podejrzane linki.** Zamiast tego samodzielnie wpisz podany adres w wyszukiwarce.
- Jeśli masz wątpliwości, **sprawdź informację** na stronie swojego banku, lub zadzwoń na infolinię.

#CyberScams

Oszuści wykorzystują fakt, że ludzie są zajęci i nie wczytują się z uwagą w otrzymaną korespondencję.

Bądź szczególnie ostrożny, gdy korzystasz ze smartfona i tabletu. Na urządzeniach mobilnych trudniej zorientować się, że jesteś oszukiwany.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

OSZUSTWA MATRYMONIALNE

Oszuści kontaktują się z ofiarami na serwisach randkowych, a także przez media społecznościowe lub e-mail.

JAK ROZPOZNASZ SCAM?

Nieznajomy, którego dopiero poznajesz online, wyznaje że bardzo mu się podobasz i namawia do prywatnych rozmów.

Wiadomości często są niejasne i źle zredagowane.

Profil nieznajomego jest niespójny i niezgodny z tym, co do Ciebie pisze.

Nieznajomy prosi Cię o wysłanie intymnych zdjęć lub video.

Zdobywa Twoje zaufanie. Potem prosi o pieniądze, podarunki lub szczegóły Twojego konta bankowego.

Jeśli nie prześlesz pieniędzy, oszust może Cię szantażować. Jeśli prześlesz - poprosi o więcej.

JESTEŚ OFIARĄ?

Nie wstydź się!

Natychmiast zerwij wszelki kontakt. Jeśli to możliwe, zachowaj historię konwersacji.

Zawiadom policję.

Zgłoś wyłudzenie w serwisie, w którym oszust nawiązał z Tobą pierwszy kontakt.

Jeśli udostępniłeś dane konta bankowego, niezwłocznie skontaktuj się z bankiem.

CO MOŻESZ ZROBIĆ?

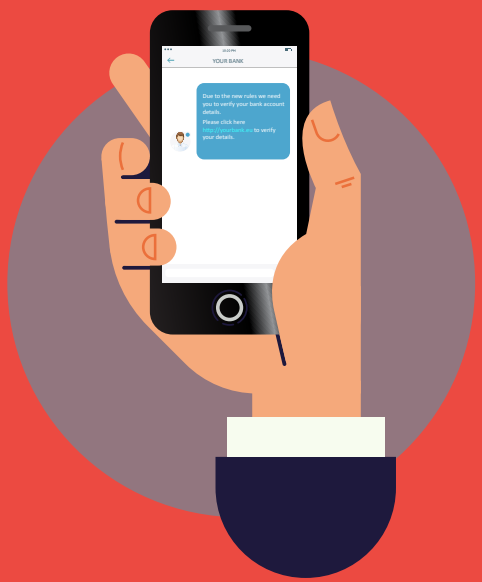
- **Uważaj** jakie informacje udostępniasz w sieciach społecznościowych i na serwisach randkowych.
- **Zachowaj czujność.** Oszuści są obecni nawet na renomowanych stronach.
- **Nie postępuj pochopnie i** zadawaj pytania, gdy masz wątpliwości.
- **Przeanalizuj zdjęcie i profil nieznajomego,** aby sprawdzić, czy nie zostały użyte w innym miejscu.
- **Bądź wyczulony** na błędy ortograficzne i gramatyczne, niekonsekwentne odpowiedzi i wymówki, takie jak niedziałająca kamera.
- **Nie udostępniaj** kompromitujących materiałów, które mogłyby zostać użyte do szantażu.
- Jeśli zgodzisz się na spotkanie, **powiedz rodzinie oraz przyjaciołom,** z kim i gdzie się umawiasz.
- **Uważaj na prośby o pieniądze.** Nigdy nie wysyłaj pieniędzy, danych karty kredytowej, haseł do konta czy kopii dokumentów.
- Unikaj wysyłania płatności z góry.
- **Nie przesyłaj pieniędzy** nieznajomym: pranie pieniędzy jest przestępstwem.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

WYŁUDZANIE INFORMACJI SMSEM

Smishing (kombinacja słów SMS i Phishing) to próba wyłudzenia informacji poufnych, firmowych lub dotyczących bezpieczeństwa za pośrednictwem SMS.



JAK TO DZIAŁA?

Otrzymujesz SMS, w którym nadawca prosi Cię o kliknięcie linku lub telefon pod wskazany numer, aby "zweryfikować", "zaktualizować" lub "ponownie aktywować" konto. Odnośniki prowadzą do fałszywej strony/telefonu oszusta, który podaje się za usługodawcę.

CO MOŻESZ ZROBIĆ?

- **Nie klikaj linków, załączników ani obrazów** otrzymywanych w SMS niewiadomego pochodzenia, bez wcześniejszego sprawdzenia nadawcy.
- **Nie spiesz się.** Sprawdź źródło wiadomości zanim udzielisz odpowiedzi.
- **Nigdy nie odpowiadaj na SMS,** który prosi o podanie Twojego numeru PIN, hasła do konta bankowego lub innych poufnych informacji.
- Jeśli podałeś swoje dane w odpowiedzi na SMS, który mógł być wyłudzeniem, **niezwłocznie skontaktuj się z bankiem.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

FAŁSZYWE STRONY INTERNETOWE

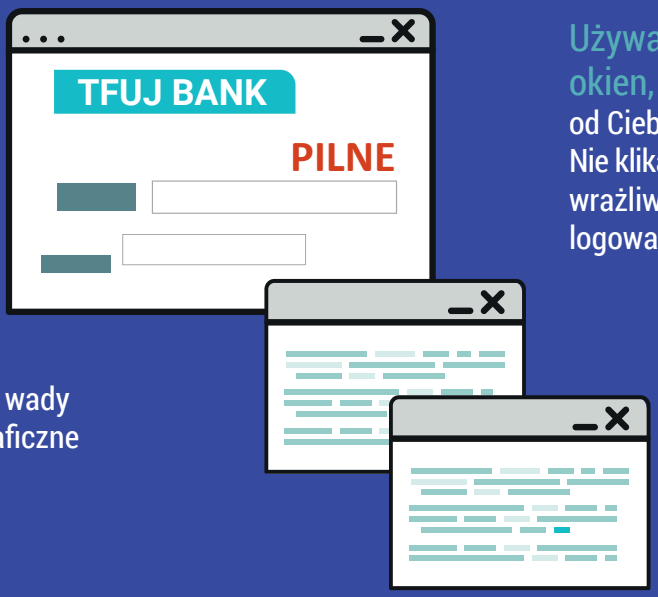
Phishing to rozsyłanie wiadomości e-mail, zawierających linki do fałszywej strony internetowej, która do złudzenia przypomina witrynę Twojego banku. Tam jesteś proszony o ujawnienie danych logowania do konta.

JAK ROZPOZNAĆ SCAM?

Fałszywe strony banków wyglądają niemal identycznie jak ich prawdziwe odpowiedniki. Takie witryny często zawierają wyskakujące okienko z prośbą o podanie danych logowania. Prawdziwe banki nie używają takich okien.

Fałszywe witryny:

Wymuszają natychmiastowe działanie: logowanie, podanie hasła. Bank nie stosuje takiego przymusu.



Używają wyskakujących okien, które próbują wyłudzić od Ciebie poufne informacje. Nie klikaj w nie, unikaj podawania wrażliwych danych i haseł logowania.

Wyglądają podejrzanie, mają wady techniczne, a także błędy ortograficzne i gramatyczne.

CO MOŻESZ ZROBIĆ?

Nigdy **nie klikaj w linki** przesyłane w mailach, które prowadzą do strony Twojego banku.

Ręcznie wpisuj adres strony banku albo korzystaj z linku zapisanego na liście ulubionych.

Używaj przeglądarki, która **blokuje wyskakujące okna.**

Ważny komunikat z banku nigdy nie jest wysyłany jedynie przez e-mail. Jeśli bank ma dla Ciebie naprawdę ważną wiadomość, zostaniesz o tym poinformowany **po zalogowaniu na swoje konto.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICJA | NASK

#CyberScams

VISHING - WYŁUDZENIE PRZEZ TELEFON

Vishing (kombinacja słów Voice - głos i Phishing) to telefoniczne wyłudzenie informacji osobistych/finansowych. Vishing może być powiązany z namową do przekazania pieniędzy.

CO MOŻESZ ZROBIĆ?

- **Bądź ostrożny,** gdy odbierasz połączenia z nieznanych numerów.
- **Poproś dzwoniącego o numer telefonu** i powiedz, że oddzwonisz.
- Sprawdź tożsamość organizacji, **wyszukaj w internecie ich numer telefonu i zadzwoń bezpośrednio.**
- **Nie sprawdzaj dzwoniącego za pomocą numeru telefonu, który Ci podał** (to może być fałszywy numer).
- **Oszuści mogą wykorzystywać informacje znalezione w internecie i mediach społecznościowych.** Nie zakładaj, że są uczciwi tylko dlatego, że dużo o Tobie wiedzą.
- **Nigdy nie udostępniaj numeru PIN do karty kredytowej i hasła do konta.** Twój bank nigdy nie zapytałby o takie informacje przez telefon.
- **Nie dokonuj przelewu na ich** prośbę. Twój bank nigdy by Cię o to nie poprosił.
- Jeśli wydaje Ci się, że odebrałeś telefon od oszusta, **powiadom swój bank.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICJA

NASK

#CyberScams