W JAKI SPOSÓB MOŻESZ ZOSTAĆ OSZUKANY?

1. Przestępcy udają, że są twoim CEO (ang. *Chief Executive Officer*) – Detektorem Generalnym.

Oszustwa typu CEO/Business Email Compromise (BEC) mają miejsce, gdy pracownik upoważniony do dokonywania płatności zostanie oszukany w celu zapłaty fałszywej faktury lub dokonania nieautoryzowanego przeniesienia środków finansowych z konta biznesowego.

Jak to działa?

Metoda opiera się na chęci pracownika do szybkiego wykonywania zadań, wymaganych przez kierownictwo wyższego szczebla. Oszuści wydają się posiadać znaczną wiedzę na temat organizacji, a przesyłane e-maile wydają się być bardzo przekonujące.

Jakie są znaki ostrzegawcze?

- Bezpośredni kontakt z przełożonym wyższego szczebla za pośrednictwem wiadomości e-mail lub poprzez połączenia telefoniczne.
- Prośba osoby kontaktującej się (przełożonego) o zachowanie całkowitej poufność.
- Nacisk i poczucie pilności.
- Niezwykłe prośby/żądanie będące w sprzeczności z procedurami wewnętrznymi.
- Zagrożenia lub niecodzienne pochlebstwa i/lub obietnice nagrody.

Co możesz zrobić?

JAKO FIRMA:

- Bądź świadomy ryzyka i upewnij się, że pracownicy są poinformowani o możliwości wystąpienia takiego typu oszustw;
- Zachęć swoich pracowników do ostrożnego podejścia w trakcie realizacji związanych z realizacją płatności;
- Wdrożyć wewnętrzne procedury dotyczące płatności;
- Wdrożyć procedurę weryfikacji legalności wniosków o płatność, które zostały otrzymane pocztą elektroniczną;
- Ustal wewnętrzne procedury raportowania dotyczące oszustw;
- Przeglądaj informacje zamieszczane na stronie internetowej swojej firmy, postara się ograniczyć ilość zamieszczanych informacji, zachowaj ostrożność w odniesieniu do zamieszczania informacji związanych z twoją firmą w mediach społecznościowych;
- Aktualizuj zabezpieczenia techniczne;
- Zawsze kontaktuj się z policją w przypadku prób oszustwa, nawet jeśli nie padłeś jej ofiarą.

JAKO PRACOWNIK:

- Ściśle stosuj się do obowiązujących procedur bezpieczeństwa dotyczące płatności i zamówień. Nie pomijaj żadnych kroków i nie poddawaj się presji;
- Zawsze dokładnie sprawdzaj adresy e-mail podczas przetwarzania poufnych informacji/ przekazów pieniężnych. Oszuści często używają kopii e-maili, w których tylko jeden element różni się od oryginału;
- Jeśli masz wątpliwości co do polecenia przelewu, skonsultuj się z kompetentnym kolegą, nawet jeśli zostałeś poproszony o zachowanie dyskrecji;
- Nigdy nie otwieraj podejrzanych linków lub załączników otrzymanych przez za pośrednictwem poczty elektronicznej. Zachowaj szczególną ostrożność podczas sprawdzania osobistych skrzynek pocztowych na komputerach firmy;
- Ogranicz informacje i zachowaj ostrożność w odniesieniu do mediów społecznościowych;
- Unikaj dzielenia się informacjami na temat hierarchii firmy, bezpieczeństwa lub procedur;
- Jeśli otrzymasz podejrzany e-mail lub telefon, zawsze informuj o tym swój dział IT.

2. Przestępcy udają, że są jednym z twoich klientów/dostawców

Jak to działa?
W firmie zjawia się osoba, która udaje, że reprezentuje dostawcę/usługodawcę/wierzyciela. Może kontaktować się telefonicznie, listownie, faksem lub pocztą elektroniczną. Oszuści żądają zmiany danych bankowych dotyczących płatności (tj. danych odbiorcy rachunku bankowego) przyszłych faktur. Nowe sugerowane konto jest całkowicie kontrolowane przez oszusta.
Co możesz zrobić?
JAKO FIRMA:
- Upewnij się, że pracownicy są o tym poinformowani i świadomi;
- Zastosuj wewnętrzne procedury dotyczące płatności;
- Poinstruuj pracowników odpowiedzialnych za za realizację płatności, aby informowali o wszelkich pojawiających się nieprawidłowościach;
- Przejrzyj informacje zamieszczone na stronie internetowej firmy, umowy zawierające dane dostawców. Poradź swoim pracownikom, aby ograniczali ilość zamieszczanych informacji o sobie na kontach w mediach społecznościowych;
- Zawsze kontaktuj się z Policją w przypadku prób oszustwa, nawet jeśli nie padłeś ofiarą tego procederu.

JAKO PRACOWNIK:
- Stosuj się ściśle do obowiązujących procedur bezpieczeństwa dotyczące płatności i zamówień. Nie pomijaj żadnych kroków i nie poddawaj się presji;
- Zawsze dokładnie sprawdzaj adresy e-mail podczas przetwarzania poufnych informacji/ przekazów pieniężnych. Oszuści często używają kopii e-maili, w których tylko jeden element różni się od oryginału;
- Jeśli masz wątpliwości co do polecenia przelewu, skonsultuj się z kompetentnym kolegą, nawet jeśli zostałeś poproszony o zachowanie dyskrecji;
- Nigdy nie otwieraj podejrzanych linków lub załączników otrzymanych przez za pośrednictwem poczty elektronicznej. Zachowaj szczególną ostrożność podczas sprawdzania osobistych skrzynek pocztowych na komputerach firmy;
- Ogranicz informacje i zachowaj ostrożność w odniesieniu do mediów społecznościowych;
- Unikaj dzielenia się informacjami na temat hierarchii firmy, bezpieczeństwa lub procedur;
- Jeśli otrzymasz podejrzany e-mail lub telefon, zawsze informuj o tym swój dział IT.

3. Przestępcy kontaktują się z tobą dzwoniąc, wysyłając wiadomości tekstowe lub e-maile
Phishing (tj. za pośrednictwem poczty e-mail), **smishing** (tj. za pośrednictwem sms) i **vishing** (tj. za pośrednictwem połączenia głosowego) są najczęstszymi atakami z wykorzystaniem socjotechniki skierowanej do klientów banków.
Wiadomości phishingowe
Wyłudzanie informacji poprzez fałszywe wiadomości e-mail, które oszukują odbiorców w celu udostępnienia ich danych osobowych, finansowych lub dotyczących bezpieczeństwa.

Jak to działa?
E-maile:
- Mogą wyglądać identycznie z rodzajem prawdziwe korespondencji wysyłanej przez banki, replikując logo banku, układ strony internetowej, bądź styl w którym pisane są prawdziwe wiadomości e-mail.
- W korespondencji używana jest stylistyka wskazująca na potrzebę bezzwłocznej reakcji z twojej strony, np.: sugerując karę, w przypadku nie udzieleniu odpowiedzi;
- Poprzez korespondencje e-mail możesz zostać poproszony o pobranie bądź otworzenie przesłanego załącznika;
Cyberprzestępcy wykorzystują fakt, iż obecnie ludzie w swoim życiu są bardzo zajęci i często nie analizują otrzymywanych wiadomości e-mail, które na tzw. „pierwszy rzut oka” wydają się być

wiarygodne. W rezultacie odbiorcy z większym prawdopodobieństwem przyjmą to, co jest w nich napisane.

Co możesz zrobić?

- Aktualizuj oprogramowanie, w tym przeglądarkę internetową, z której korzystasz, program antywirusowy oraz system operacyjny.
- Zachowaj szczególną czujność, jeśli e-mail "bankowy" wymaga od Ciebie poufnych informacji (np. twojego hasła do konta bankowego on-line). Prawdziwy bank będzie komunikować się z tobą tylko w sposób bezpieczny przez twoje internetowe konto bankowe.
- Dokładnie przyjrzyj się otrzymanej wiadomości, która została ci przesłana. Sprawdź niespójności logiczne, gramatyczne i stylistyczne, które powodują, iż jest ona całkowicie bezsensowna.
- Sprawdź niewielkie różnice wynikające z nazwy adresu nadawcy: zero może wyglądać jak "o".
- "Przesuwaj myszką" adres nadawcy i uważnie przyjrzyj się *faktycznemu* nadawcy: jeśli to możliwe, porównaj adres e-mail nadawcy z wcześniejszymi prawdziwymi wiadomościami z banku.
- Nie odpowiadaj na podejrzane wiadomości e-mail, ale prześlij je do swojego banku, wpisując adres samodzielnie.
- Nie klikaj linku ani nie pobieraj załącznika, zamiast tego wpisz adres w przeglądarce.
- Uważaj podczas korzystania z urządzenia mobilnego. Może być trudniej wykryć próbę wyłudzenia informacji z telefonu lub tabletu. Nie można "przeskoczyć myszki" na wątpliwy link, podczas gdy mniejszy ekran sprawia, że mniej prawdopodobne jest zauważenie oczywistych błędów. Jeśli jest to fałszywy e-mail, zgłoś go do swojego banku - wszystkie firmy chcą być poinformowane o tych oszustwach. W razie wątpliwości zadzwoń do swojego banku.

Bank vishing calls

Vishing (połączenie słów, głosu i phishingu) to oszustwo telefoniczne, w którym oszuści próbują nakłonić ofiarę by ujawniła osobiste, finansowe informacje celem przekazywania środków finansowych przestępcom.

Co możesz zrobić?

- Uważaj na niechciane połączenia telefoniczne.
- Zapisz numer osoby dzwoniącej i poinformuj, że oddzwonisz.
- Aby zweryfikować tożsamość osoby dzwoniącej, wyszukaj numer telefonu firmy którą reprezentuje (np. poprzez stronę internetową) i skontaktuj się z firmą bezpośrednio.
- Nie sprawdzaj osoby dzwoniącej za pomocą numeru telefonu, który został ci podany (może to być fałszywy numer telefonu).
- Oszuści mogą znaleźć podstawowe informacje o tobie lub twojej firmie on-line (np. profile w mediach społecznościowych). Nie zakładaj, że dzwoniący jest osobą godną zaufania tylko dlatego, że ma takie szczegóły.
- Nie udostępniaj numeru PIN karty kredytowej lub debetowej ani hasła do bankowości internetowej. Twój bank nigdy nie poprosi o takie dane.
- Nie przesyłaj pieniędzy na inne konto na niczyje żądanie. Twój bank nigdy nie poprosi cię o to.
- Jeśli uważasz, że to fałszywe połączenie, zgłoś to do swojego banku.

Smishing

Smishing (połączenie słów: SMS i phishing'u) to próba uzyskania przez oszustów informacji osobistych, finansowych lub dotyczących bezpieczeństwa za pomocą wiadomości tekstowej. Przestępcy działają jako wiarygodne źródło, podszywając się pod bank, wydawcę karty płatniczej lub dostawcę usług.

Jak to działa?

Przesłana do ciebie wiadomość zazwyczaj wymaga (w trybie pilnym) kliknięcia linku do strony internetowej lub zadzwonienia pod numer telefonu w celu weryfikacji, aktualizacji lub reaktywacji konta. Link do strony internetowej prowadzi do fałszywej strony internetowej i

numeru telefonu do oszusta udającego, że pochodzi z legalnej działającej firmy. Celem przestępcy jest, abyś ujawnił wszelkie informacje, które mogą pomóc oszustom w kradzieży twoich pieniędzy.

Co możesz zrobić?

- Nie klikaj linków, załączników ani obrazów otrzymywanych w niespodziewanych wiadomościach tekstowych bez wcześniejszej weryfikacji nadawcy. Możesz to zrobić, wyszukując numer on-line lub porównując go z oficjalnym numerem nadawcy/firmy, z którego pochodzi.
- Nie spiesz się. Zweryfikuj wszystkie uzyskane informacje.
- Nigdy nie odpowiadaj na wiadomości tekstowe żądające kodu PIN, hasła bankowości internetowej lub innych danych uwierzytelniających.
- Jeśli sądzisz, iż możliwe, że miałeś do czynienia z przestępstwem smishingu podając swoje wrażliwe dane, natychmiast skontaktuj się ze swoim bankiem.

4. Przestępcy tworzą sfałszowane strony bankowe

E-maile „phishingowe" zawierają zwykle linki, które prowadzą do witryny internetowej „fałszywego banku", w której wymagane jest ujawnienie informacji finansowych i osobistych.

Jakie są znaki?

Fałszywe strony internetowe banków wyglądają niemal identycznie jak ich prawdziwe odpowiedniki. Takie witryny często zawierają wyskakujące okienko z prośbą o podanie danych banku. Prawdziwe banki nie używają takich takiej formuły komunikacji.

Te witryny zazwyczaj wyświetlają:

- **Pilność realizacji**: takich wiadomości nie znajdziesz na prawdziwych stronach internetowych;
- **Mają ubogi wygląd**: zachowaj ostrożność w przypadku stron internetowych, które mają wady w swoich projektach lub błędy w pisowni i gramatyce;
- **Pop-up windows**: są one zwykle używane do zbierania poufnych informacji od ciebie. Nie klikaj ich i nie przesyłaj danych osobowych do takich okien.

Co możesz zrobić?

- Nigdy nie klikaj linków zawartych w wiadomościach e-mail prowadzących do witryny twojego banku.
- Zawsze wpisuj link ręcznie lub użyj istniejącego linku z listy "ulubionych".
- Użyj przeglądarki, która pozwala na blokowanie wyskakujących okienek.
- Jeśli coś ważnego naprawdę wymaga twojej uwagi, zostaniesz o tym powiadomiony przez twój bank, kiedy uzyskasz dostęp do swojego konta online.
- W razie wątpliwości zadzwoń do swojego banku.

5. Przestępcy udają, że interesują się romantycznym związkiem

Romansowe oszustwa zwykle mają miejsce na internetowych serwisach randkowych, ale oszuści często korzystają z mediów społecznościowych lub poczty e-mail, aby nawiązać kontakt.

Jakie są znaki?

- Ktoś, kogo niedawno poznałeś on-line, wyznaje ci silne uczucia, prosząc o prywatność na czacie.
- Przesyłane wiadomości są często słabo napisane i niejasne.
- Profil on-line osoby, z którą nawiązałeś kontakt, nie jest zgodny z tym, co pisze na swój temat..
- Przestępcy mogą również poprosić o przesłanie intymnych zdjęć lub filmów.
-Cierpliwie czekają nawet tygodniami, aby zdobyć zaufanie. Opowiadają ci skomplikowaną historię życiową prosząc o przesłanie środków finansowych na wskazane konto.
- Jeśli nie wyślesz pieniędzy, będą mogli cię szantażować. Jeśli to zrobisz, będą prosić o więcej.
- Zawsze będą mieć pretekst, aby usprawiedliwić, że ich kamera internetowa nie działa, nie może podróżować, by się z tobą spotkać i dlaczego zawsze potrzebują więcej pieniędzy.

Co możesz zrobić?

- Bądź bardzo ostrożny, ile informacji osobistych udostępniasz w sieci społecznościowej oraz na stronach randkowych.
- Zawsze rozważ ryzyko swojego postępowania. Oszuści są obecni na najbardziej renomowanych stronach w Internecie.

- Nie śpiesz się i zadawaj pytania.
- Przeanalizuj zdjęcia i profil osoby w Internecie, aby sprawdzić, czy ten sam materiał został wykorzystany w innym miejscu.
- Bądź czujny na błędy ortograficzne i gramatyczne, niekonsekwencje występujące w opowiadanych historiach i wymówki, dotyczące na przykład niedziałającej kamerki internetowej.
- Nie udostępniaj osobistych zdjęć, filmów ani żadnych kompromitujących materiałów, które oszuści mogliby później wykorzystać do szantażowania ciebie.
- Jeśli zgodzisz się spotkać osobiście, powiedz rodzinie i przyjaciołom dokąd się wybierasz.
- Uważaj na przesyłane do ciebie prośby dotyczące przesłania pieniędzy. Nigdy nie wysyłaj pieniędzy ani nie podawaj danych karty kredytowej, danych konta internetowego ani kopii ważnych dokumentów osobistych.
- Unikaj jakichkolwiek ustaleń z nieznajomym, który prosi o płatność z góry za pośrednictwem przekazu pieniężnego, przelewu bankowego, międzynarodowego transferu środków, wstępnie załadowanej karty lub kryptowalut. Rzadko zdarza się odzyskać pieniądze wysłane w ten sposób.
- Nie przelewaj środków finansowych na inną osobę: tzw. „pranie pieniędzy" jest przestępstwem.

Jeśli padłeś ofiarą romansowego oszustwa:
- Nie czuj się zawstydzony, to oszustwo zdarza się częściej, niż możesz sobie wyobrazić;
- Natychmiast przerwij kontakt;
- Jeśli to możliwe, zachowaj całą komunikację (taką jak wiadomości czatu) i wszelkie dowody, które mogłyby pomóc zidentyfikować oszusta;
- Złożyć organom ścigania, zawiadomienie o popełnieniu przestępstwa;
- Skontaktuj się z administratorem portalu, poprzez który nawiązałeś kontakt. Wskaż nazwę profilu oszusta i wszelkie inne szczegóły, które mogą pomóc;
- Jeśli podałeś dane swojego konta oszustowi, natychmiast skontaktuj się ze swoim bankiem lub instytucją finansową.

6. Przestępcy kradną dane osobowe za pośrednictwem mediów społecznościowych
Twoje dane osobowe są cenne dla przestępców. Ochrona przed oszustwami oznacza także ich bezpieczeństwo.
Jak to działa?
Nawet jeśli profile w mediach społecznościowych są skonfigurowane jako "prywatne" i odpowiednio zabezpieczone, lub jeśli jesteś ostrożny i nie udostępniasz wielu informacji w swoich profilach (zdjęcia, filmy, aktualizacje statusu itp.), Oszuści używają różnych technik, aby oszukać i mieć dostęp do twoich informacji, które następnie mogą zostać wykorzystane do kradzieży tożsamości.
Twoje dane osobowe mogą pomóc oszustom:
- dokonywać nieautoryzowanych zakupów za pomocą karty kredytowej oraz otwartych kont bankowych poprzez:
- zaciąganie pożyczek;
- sprzedawanie dane osobowe innym oszustom;
- przeprowadzania nielegalnych interesów z wykorzystaniem twoich danych osobowych.

Wiele ataków przebiega według podobnego schematu, niektóre klasyczne to:
- **Twishing** (połączenie słów Twitter i phishing) jest aktem wysyłania wiadomości do użytkownika Twittera kierującej do odwiedzenia strony internetowej. Jeśli użytkownik zaloguje się w nieuczciwej witrynie, atakujący uzyska informacje o koncie (imię i hasło).
- **„Kto obejrzał twój profil lub stronę społecznościową?"** Taka usługa poprosi cię o przyznanie jej dostępu do twojego profilu. Doprowadzi to do nieuczciwej ankiety, dzięki czemu udostępnisz swoje dane osobowe. Spamer otrzyma prowizję za każdym razem, gdy ktoś wypełni ankietę. Nigdy nie dowiesz się, kto cię szukał.

- **„Czy to ty jesteś na tym filmiku?”** Klikając na filmiki bierzesz udział się w ankiecie, na której spamera. Możesz także zainfekować swoje urządzenie złośliwym oprogramowaniem.
- **"Twoje konto zostało anulowane", "potwierdź swoje konto e-mail"**. Takie oszustwa mają na celu skłonienie użytkownika do ujawnienia swoich prywatnych informacji i danych uwierzytelniających konto.
- **Oszustwa związane z kartami upominkowymi i fałszywe oferty popularnych marek** o wysokiej wartości. Oszustwa te mają na celu skłonienie użytkownika do ujawnienia danych osobowych lub zarejestrowania się w celu skorzystania z drogich usług. Co miesiąc przyjmują nową formę i brzmią zbyt dobrze, aby mogły być prawdziwe - zamówiona usługa lub produkt nigdy nie dociera do osoby zamawiającej.
- **„Produkt cud, darmowe próby!”.** Ten schemat online wykorzystuje bezpłatne oferty Trial, fałszywych potwierdzeń i ankiety i ma na celu skłonienie użytkownika do płacenia za produkty.
- **"Zarabiaj mnóstwo pieniędzy pracujących w domu"**. Każda praca, która wymaga opłaty za rozpoczęcie, może być nieuczciwa. Reklamy te znajdują się na stronach mediów społecznościowych i kierują do oferty, która pobiera opłaty za zestaw, który pomoże ci rozpocząć zarabianie dużych pieniędzy. Możesz zostać poproszony o podanie wielu danych osobowych, m.in. kopii paszportu lub prawa jazdy. Niektóre oferty pracy mogą obejmować pokrycie nielegalnych działań procederu tzw. „prania pieniędzy”.
- **„Pomoc, mam kłopoty!”**. Przestępca udaje, że jest twoim krewnym potrzebującym pieniędzy kontaktując się z Tobą za pośrednictwem wiadomości w mediach społecznościowych.

Co możesz zrobić?
- Za każdym razem, gdy chcesz zweryfikować informacje dotyczące profilu na platformie społecznościowej, przejdź bezpośrednio do strony w sieci Internet - nie ufaj przesłanemu linkowi linkowi, za pomocą którego masz przejść do wskazanej strony.
- Bądź świadomy, ile informacji i zdjęć udostępniasz na portalach społecznościowych. Oszuści mogą je użyć, aby stworzyć fałszywą tożsamość lub sprawić, iż staniesz się ofiarą oszustwa.
- Przejrzyj swoje ustawienia prywatności i bezpieczeństwa na każdym profilu społecznościowym. Poświęć trochę czasu, aby zrozumieć, co dokładnie udostępnia twój profil publicznie.
- Sam poszukaj on-line nazwy produktu lub oferty pracy, aby zobaczyć, co na ten temat piszą inni użytkownicy Możesz połączyć je ze słowami takimi jak "recenzja", "skarga" lub "oszustwo".
- Zgłoś profile, które podejrzewasz o oszustwa na platformę społecznościowej.
- Regularnie monitoruj wyciągi z kart kredytowych i debetowych. Jeśli pobierasz opłatę za coś, czego nie zamówiłeś, skontaktuj się z bankiem i dostawcą karty.

7. Przestępcy sprawiają, że myślisz, że jesteś gotowy do przeprowadzenia mądrej inwestycji.
Typowe oszustwa inwestycyjne mogą zawierać lukratywne możliwości inwestycyjne, takie jak akcje, obligacje, kryptowaluty, rzadkie metale, inwestycje zagraniczne lub energia.

Jakie są znaki?
- Otrzymujesz wielokrotnie na swój numer telefonu niespodziewane połączenie przychodzące.
- Otrzymujesz obietnicę uzyskania szybkich zarobków, które mają „ci się zwrócić” oraz gwarancję, iż inwestycja jest całkowicie bezpieczna.
- Oferta jest dostępna tylko przez ograniczony czas.
- Oferta jest dostępna tylko dla ciebie i nie możesz się z nikim nią podzielić.

Co możesz zrobić?
- Zawsze zasięgnij porady finansowej, zanim przekażesz jakiekolwiek pieniądze lub dokonasz inwestycji.
- Bądź podejrzliwy wobec ofert obiecujących bezpieczną inwestycję, gwarantowane zwroty i duże zyski.
- Strzeż się przyszłych oszustw. Jeśli już zainwestowałeś w oszustwo, przestępcy prawdopodobnie znów będą cię atakować lub sprzedawać twoje dane innym przestępcom.

- Jeśli podejrzewasz, iż stałeś się ofiarą oszustwa skontaktuj się z Policją.

…albo prezentują si świetną ofertę on-line!
Konsumenci i firmy coraz częściej kupują i sprzedają online. Oferty internetowe są często dobrym zakupem, ale uważaj na oszustwa.

Co możesz zrobić?
- Jeśli to możliwe, korzystaj z krajowych platform sprzedaży on-line - będzie bardziej prawdopodobne, że rozwiążesz jakiekolwiek problemy.
- Zasięgnij opinii innych w Internecie, przed dokonaniem zakupów.
- Używaj kart kredytowych - masz większe szanse na odzyskanie pieniędzy.
- Płać tylko za pomocą bezpiecznej usługi płatności elektronicznej.
- Płać tylko po podłączeniu do bezpiecznego połączenia internetowego - unikaj korzystania z darmowej lub otwartej publicznej sieci Wi-Fi.
- Dokonuj płatności jedynie za pomocą bezpiecznych urządzeń.. Dbaj o aktualność systemu operacyjnego i oprogramowania zabezpieczającego.
- Wyskakującą reklamę z informacją, że wygrałeś nagrodę? Pomyśl dwa razy, możesz po prostu wgrać na urządzenie, którym się posługujesz, złośliwe oprogramowanie.
- Jeśli produkt nie dotrze, skontaktuj się ze sprzedawcą. Jeśli nie ma odpowiedzi, skontaktuj się ze swoim bankiem.
- Zawsze składaj zawiadomienia o popełnieniu przestępstwa organom ścigania.