

Poradnik



**FALSZYWA
TOŻSAMOŚĆ**

**PRAWDZIWE
RYZYKO**

Drogi Czytelniku

Na Twoje ręce przekazujemy zestaw porad opisujących, jak rozpoznać przykładowe sposoby postępowania oszustów oraz jak należy się zachować, jeżeli na takie niebezpieczne sytuacje natrafisz. W tym poradniku omówimy różne metody oszustw, które opierają się na bardzo podobnych mechanizmach polegających na grze na emocjach oraz wykorzystaniu zaufania do autorytetu. W obecnych czasach, kiedy technologia zajmuje ważne miejsce w naszym życiu, oszuści znajdują nowe sposoby, by wykorzystywać naszą ufność i „dobre serce”. Zapoznanie się z niniejszymi wskazówkami pozwoli na uniknięcie lub przynajmniej ograniczenie najbardziej istotnych dla Ciebie zagrożeń. Zachęcamy Cię do zapoznania z naszymi poradami oraz ich wspólnego przedyskutowania z osobami najbliższymi i wykorzystywania w życiu codziennym.

Śląscy Policjanci



Oszustwo na wnuczka - jest dobrze zaplanowane i może być bardzo przekonujące. Należy zachować czujność i sprawdzać wszystkie informacje przed podjęciem jakichkolwiek działań.

1. Zazwyczaj zaczyna się od telefonu od kogoś, kto podaje się za Twojego wnuka lub innego bliskiego krewnego, twierdząc, że znalazł się w nagłej potrzebie (np. spowodował wypadek, trafił do aresztu itp.) i potrzebuje pieniędzy.
2. Oszust będzie wywierał na Ciebie presję przekonując, że pomoc jest potrzebna natychmiast i szybko musisz podjąć decyzję.
3. „Wnuczek” prawdopodobnie poprosi Cię o nieinformowanie innych członków rodziny o zaistniałej sytuacji, co ma na celu uniemożliwienie weryfikacji historii.
4. Jeśli głos „wnuczka” będzie inny niż zwykle, oszust może tłumaczyć to np. przeziębieniem lub zdenerwowaniem spowodowanym wypadkiem.
5. Oszust może prosić o przekazanie gotówki przez kuriera, taksówkarza, szybki przelew bankowy, wyrzucenie gotówki przez okno lub pozostawienie jej w koszu na śmieci.

6. Oszust rozmawiając z Tobą przez telefon stacjonarny, może prosić o Twój numeru telefonu komórkowego, na który zadzwoni, aby na bieżąco słuchać, czy wykonujesz jego polecenia oraz skutecznie go zablokować przed osobami, które będą się chciały do Ciebie dodzwonić.
7. Oszust może wywierać na Tobie presję konieczności udania się do banku i wypłaty wszystkich oszczędności. Może również kazać zaciągnąć pożyczkę lub kredyt.

JAK UNIKNĄĆ OSZUSTWA ?

1. **Zawsze weryfikuj tożsamość dzwoniącego** - jeśli ktoś twierdzi, że jest Twoim krewnym w potrzebie, zadzwoń do niego bezpośrednio na znany Ci numer, aby to potwierdzić. Zadaj pytania, na które tylko prawdziwy członek rodziny zna odpowiedź.
2. **Nie podejmuj pochopnych decyzji pod wpływem silnych emocji** - oszuści liczą na Twoją szybką reakcję. Zawsze znajdź czas na przemyślenie sytuacji.
3. **Nie przekazuj pieniędzy nieznanemu** - niezależnie od tego, jak przekonująca może wydawać się historia, nigdy nie przekazuj pieniędzy osobom, których tożsamości nie możesz potwierdzić.



Oszustwo na policjanta - to typ przestępstwa, w którym sprawcy podszywają się pod funkcjonariuszy Policji, CBŚP/ABW lub innych urzędników, aby wyłudzić pieniądze lub dane osobowe. Jak możesz rozpoznać oszustwo i zapobiec staniu się jego ofiarą:

1. Rozmówca twierdzi, że jest funkcjonariuszem Policji, CBŚP/ABW lub innych służb i potrzebuje Twojej pomocy w złapaniu przestępcy, często sugerując, że Twoje pieniądze są zagrożone i musisz je „przekazać” w celu ich ochrony.
2. „Policjant” może prosić o przekazanie pieniędzy, rzekomo na kaucję za aresztowanego członka rodziny lub o podanie danych osobowych i finansowych pod pretekstem weryfikacji tożsamości oraz ochrony przed oszustwami.
3. Oszust często wywiera presję, twierdząc, że sytuacja jest pilna i wymaga natychmiastowej reakcji. Może również grozić konsekwencjami prawnymi, jeśli nie zostanie spełniona jego prośba.
4. Tak jak w oszustwie na wnuczka, sprawca może Cię prosić, abyś nie kontaktował/ła się z innymi członkami rodziny lub znajomymi, aby „nie zakłócać dochodzenia”.

JAK UNIKNAĆ OSZUSTWA ?

1. **Jeśli masz wątpliwości co do tożsamości osoby dzwoniącej** - ZAKOŃCZ ROZMOWĘ (odłóż słuchawkę) i skontaktuj się bezpośrednio z odpowiednią jednostką Policji, używając oficjalnego numeru telefonu, a nie tego podanego przez osobę dzwoniącą. Nie zgadzaj się również, aby przełączono Cię do innego „policjanta” mającego potwierdzić tożsamość tego dzwoniącego. Pamiętaj, prawdziwi funkcjonariusze nigdy nie proszą o przekazanie pieniędzy.
2. **Nie podejmuj pochopnych decyzji** - oszuści liczą na to, że szybka reakcja nie pozwoli Ci zweryfikować ich historii. Zawsze znajdź czas na przemyślenie sytuacji.
3. **Nigdy nie przekazuj pieniędzy nieznanym** - niezależnie od tego, jak przekonująca może wydawać się historia, nigdy nie przekazuj pieniędzy osobom, których tożsamości nie możesz potwierdzić.
4. **Pamiętaj, że prawdziwi funkcjonariusze** - Policji, CBŚP/ABW nigdy nie będą Cię informować o prowadzonych przez siebie akcjach oraz wymagać od Ciebie przekazania pieniędzy.



Oszustwo na pracownika banku - to metoda, w której sprawcy podszywają się pod pracowników instytucji finansowych, aby wyłudzić od ofiar pieniądze lub dane osobowe. Oto kluczowe informacje, które pomogą Ci rozpoznać tego typu oszustwo i zabezpieczyć się przed nim:

1. **Niespodziewany kontakt** - oszust kontaktuje się telefonicznie, mailowo lub poprzez wiadomości tekstowe, twierdząc, że pracuje w banku, w którym masz konto.
2. **Prośba o dane osobowe** - „pracownik banku” prosi o weryfikację danych osobowych, haseł dostępu do konta online, kodów PIN, czy innych poufnych informacji, rzekomo w celu weryfikacji tożsamości lub zabezpieczenia konta.
3. **Poczucie pilności** - oszust może twierdzić, że Twoje konto jest zagrożone, np. przez nieautoryzowane transakcje, i należy natychmiast podjąć działania, aby je zabezpieczyć.
4. **Prośba o przekazanie pieniędzy** - możesz usłyszeć, że konieczne jest przełanie środków na „bezpieczne konto – tzw. konto techniczne” w celu ochrony przed oszustwami lub do weryfikacji bezpieczeństwa transakcji.
5. **Instalacja oprogramowania** - sprawca może również prosić o zainstalowanie zdalnego oprogramowania dostępowego na Twoim komputerze lub urządzeniu

mobilnym (telefonie komórkowym, tablecie), rzekomo w celu pomocy w rozwiązaniu problemu z kontem.

JAK UNIKNĄĆ OSZUSTWA ?

1. **Nie udostępniaj poufnych danych** - prawdziwi pracownicy banku nigdy nie proszą o podawanie haseł, kodów PIN, czy innych poufnych informacji telefonicznie czy przez e-mail.
2. **Weryfikuj tożsamość dzwoniącego** - jeśli masz wątpliwości, zakończ rozmowę i skontaktuj się bezpośrednio z bankiem, używając oficjalnego numeru telefonu lub kontaktu znalezionej na oficjalnej stronie internetowej instytucji.
3. **Zastanów się przed podjęciem decyzji** - oszuści wywierają presję, aby zmusić Cię do szybkiego działania. Zawsze daj sobie czas na przemyślenie sytuacji.
4. **Nie instaluj nieznanych aplikacji** - nie zgadzaj się na instalację jakiegokolwiek oprogramowania na Twoim urządzeniu na prośbę osoby, która skontaktowała się z Tobą i twierdzi, że jest pracownikiem banku czy innej instytucji finansowej.
5. **Nie klikaj w przesłane, podejrzane linki** - oszuści mogą je wysłać w wiadomościach e-mail, SMS lub za pomocą innych komunikatorów społecznych.

Oszustwo na kod BLIK - polega na wyłudzeniu od ofiary kodu umożliwiającego nieautoryzowany dostęp do środków znajdujących się na koncie bankowym. Oto kilka wskazówek, jak rozpoznać i uniknąć takiego rodzaju oszustwa:

1. Oszust kontaktuje się z Tobą za pośrednictwem telefonu, SMS-a, aplikacji komunikacyjnych lub mediów społecznościowych, prosząc o przekazanie kodu BLIK lub innego kodu jednorazowego, często pod pretekstem pilnej potrzeby lub pomocy.
2. Możesz otrzymać informację o rzekomej wygranej w konkursie lub loterii, która wymaga podania kodu BLIK do „weryfikacji” lub odbioru nagrody.
3. Prośby o „weryfikację” tożsamości - sprawca może podawać się za pracownika banku lub innych instytucji finansowych i prosić o kod BLIK jako formę weryfikacji tożsamości lub potwierdzenia bezpieczeństwa konta.

JAK UNIKNĄĆ OSZUSTWA

1. **Nigdy nie udostępniaj kodów BLIK** - pamiętaj, że te kody służą do autoryzacji transakcji finansowych i nie powinny być nikomu udostępniane.
2. **Uważaj na prośby o BLIK** - zawsze sprawdzaj kto prosi Cię o przekazanie kodu BLIK, np. telefonując do tej osoby. Zignoruj prośby od nieznanyc osób lub niepotwierdzonych kontaktów.

3. **Weryfikuj autentyczność wiadomości** - jeśli otrzymujesz wiadomości od „banku” lub innej „oficjalnej” instytucji, zweryfikuj je, kontaktując się bezpośrednio z instytucją za pomocą oficjalnych kanałów komunikacji.
4. **Używaj kodu BLIK tylko w zaufanych źródłach** - wprowadzaj kody BLIK tylko w oficjalnych aplikacjach bankowych lub zaufanych terminalach płatniczych.





Oszustwo metodą na żołnierza - to forma oszustwa internetowego, w której sprawcy podszywają się pod żołnierzy, zazwyczaj twierdząc, że służą za granicą, aby zdobyć zaufanie i sympatię ofiar. Celują w uczucia, tworzą fałszywe relacje, a ostatecznie proszą o pieniądze, dane osobowe lub inne wsparcie finansowe. Oto jak możesz rozpoznać tego typu oszustwo:

1. **Szybka eskalacja relacji** - oszust bardzo szybko deklaruje silne uczucia lub twierdzi, że znalazł w tobie „tę jedyną” osobę, mimo bardzo krótkiego okresu komunikacji.
2. **Historie budzące współczucie** - fałszywy żołnierz może opowiadać smutne lub dramatyczne historie, takie jak bycie wdowcem, utrata bliskich, trudne warunki służby lub problemy finansowe, aby wywołać współczucie.
3. **Prośby o pieniądze** - prośby mogą dotyczyć pomocy w opłaceniu rzekomych urlopów, biletów lotniczych, opłat medycznych, prawnych lub innych „pilnych” wydatków.
4. **Unikanie spotkań na żywo** - osoba ta często znajduje wymówki, by nie spotkać się na żywo lub unikać rozmów wideo, tłumacząc to problemami technicznymi, ograniczeniami służbowymi lub tajemnicą misji.
5. **Fałszywe zdjęcia i dokumenty** - mogą używać skradzionych lub sfabrykowanych zdjęć oraz fałszywych dokumentów, aby udowodnić swoją tożsamość i historię.

JAK UNIKNĄĆ OSZUSTWA ?

1. **Zachowaj sceptycyzm** - wobec osób, które szybko deklarują uczucia lub proszą o pieniądze, szczególnie jeśli komunikujecie się tylko przez Internet.
2. **Sprawdź zdjęcia i historie** - skorzystaj z wyszukiwania obrazem w Internecie, aby sprawdzić, czy zdjęcia, którymi się dzielą, nie są powszechnie dostępne lub używane w innych kontekstach.
3. **Unikaj wysyłania pieniędzy** - nie wysyłaj pieniędzy ani nie udostępniaj danych bankowych osobom poznanym w Internecie, zwłaszcza jeśli prośby dotyczą opłacenia niezweryfikowanych transakcji czy kosztów.
4. **Zachowaj prywatność** - nie przekazuj nieznajomym w Internecie danych osobowych takich jak adres, dane bankowe czy kopie dokumentów.
5. **Poszukaj wsparcia** - jeśli masz wątpliwości co do intencji osoby, z którą się komunikujesz, porozmawiaj o tym z zaufanymi osobami.
6. **Zgłoś podejrzone kontakty** - jeśli uważasz, że padłeś ofiarą oszustwa, zgłoś to odpowiednim organom, takim jak Policja, Prokuratura lub organizacje zajmujące się walką z oszustwami internetowymi tj. CSIRT NASK

PAMIĘTAJ RÓWNIEŻ O INNYCH ZAGROŻENIACH!

Pamiętaj, że niektórzy przestępcy mogą próbować Cię oszukać przychodząc do Twojego domu. Podstawą ich działania jest podanie fałszywego celu przybycia, czy też podszywanie się za pracownika opieki społecznej, gazowni, zakładu energetycznego, wodociągów, Zakładu Ubezpieczeń Społecznych albo innej instytucji, czy nawet za krewnych lub osoby z nimi związane. Może to też być osoba, która chce Ci coś sprzedać lub prosi tylko o szklankę wody. Po uśpieniu czujności czy wykorzystaniu Twojej nieuwagi, oszuści wyłudzą pieniądze albo dokonują kradzieży cennych przedmiotów, dokumentów czy oszczędności.

W celu ochrony przed oszustwem bądź kradzieżą zachowaj szczególną ostrożność i pamiętaj o przestrzeganiu poniższych zaleceń:

1. Drzwi wejściowe zawsze zamykaj na zamki, po zmroku zasłaniaj zasłony w oknach aby strzec swojej prywatności. Teren przy domu powinien być oświetlony, a krzewy i drzewa odpowiednio przycięte tak, aby nie ograniczały widoczności.
2. Nie otwieraj drzwi bez upewnienia się kto i po co przyszedł – najlepiej sprawdź przez wizjer i zapytaj o to przez zamknięte drzwi. Osobę podającą się za przedstawiciela administracji osiedla, elektrowni, gazowni, wodociągów, ZUS, czy jakiegokolwiek urzędu, zawsze możesz sprawdzić prosząc o okazanie legitymacji służbowej, a jeżeli masz wątpliwości co do jej

autentyczności, możesz telefonicznie (bez otwierania drzwi) zweryfikować w danej instytucji czy była ona do Ciebie skierowana.

3. Pamiętaj, że pracownicy Zakładu Ubezpieczeń Społecznych nie odwiedzają swoich klientów w domach, w celu informowania ich o przysługujących świadczeniach czy usługach.
4. Jeśli musisz kogoś wpuścić do mieszkania, to nigdy nie zostawiaj tej osoby samej ani na chwilę, najlepiej, żeby wtedy w domu był jeszcze obecny ktoś z rodziny, znajomy czy sąsiad.
5. W ganku, przedpokoju czy innym miejscu, gdzie zazwyczaj witasz obce osoby nie pozostawiaj cennych rzeczy takich jak: torebka, portfel, kluczyki do samochodu, klucze do mieszkania, szaszetka z dokumentami.
6. Przechowując w domu oszczędności czy inne cenne przedmioty schowaj je w miejscu niestandardowym, znanym tylko Tobie.
7. Z uwagi na różne nieprzewidziane sytuacje, jakie mogą wydarzyć się w nocy, w pobliżu łóżka trzymaj niezbędne leki, latarkę i telefon komórkowy.

Oprócz przestrzegania powyższych zasad bardzo ważną rolę odgrywają dobre relacje międzysąsiedzkie. Dlatego nie irytuj się, kiedy sąsiad otwiera drzwi i sprawdza co się dzieje na korytarzu. Sam też zainteresuj się obcymi osobami znajdującymi się na klatce schodowej czy w pobliżu Twojej posesji, zapytaj je kogo szukają i „w czym można im pomóc”. Otoczenie wrażliwe na obecność osób obcych utrudnia działanie przestępcom.



BEZPIECZEŃSTWO W CYBERPRZESTRZENI

Każdy użytkownik Internetu, przed rozpoczęciem korzystania z jego zasobów, powinien zapoznać się z zasadami bezpieczeństwa w sieci. W trosce o swoje dane należy pamiętać o istniejących zagrożeniach, które często wiążą się z pobieraniem oprogramowania z niepewnych źródeł, odpowiadaniem na podejrzaną pocztę elektroniczną, instalowaniem niesprawdzonych aplikacji czy klikaniem w podejrzaną linki. Coraz częściej ofiarą internetowych przestępców można stać się na portalach społecznościowych czy otwierając wiadomości (e-mail, SMS) od nieznanych użytkowników.

Przeglądając strony internetowe pamiętaj, że:

1. Należy regularnie uaktualniać system i oprogramowanie, które używasz; warto zaopatrzyć swój komputer w program antywirusowy, który ostrzeże Cię przed niebezpieczeństwem.
2. Nie otwieraj linków bezpośrednio z otrzymanego e-maila, wiadomości SMS czy przesłanej przez inne komunikatory społeczne szczególnie, jeśli nie znasz nadawcy wiadomości.
3. W żadnym wypadku nie podawaj swoich danych osobowych oraz nie wypełniaj formularzy zawartych w wiadomości e-mail przesłanych z nieznanych źródeł.
4. Banki i instytucje finansowe stosują protokół **HTTPS** tam, gdzie konieczne jest zalogowanie do systemu. Adres strony WWW rozpoczyna się wtedy od „**https://**”, a nie „**http://**” (jeśli strona logowania nie zawiera w adresie nazwy **HTTPS**, zgłoś taką sytuację do banku nie kontynuując logowania).

Z uwagi na powszechny dostęp do komputera i urządzeń mobilnych uważaj na to, komu pozwalasz korzystać ze swoich profili internetowych i sprzętów. Nie zostawiaj bez kontroli telefonu bądź laptopa w miejscu, gdzie mogą mieć do nich dostęp osoby niepowołane. Nigdy nie udostępniaj swoich danych do logowania osobom trzecim. Staraj się regularnie wykonywać kopie bezpieczeństwa, a ważne pliki zapisuj na zewnętrznych nośnikach.

Stosując kilka prostych zasad możesz uniknąć stania się ofiarą internetowego przestępcy:

1. Pilnuj swoich haseł, a nowo tworzone powinny mieć odpowiednią jakość. Do podstawowych zasad tworzenia bezpiecznego hasła należy kombinacja małych i wielkich liter, cyfr i znaków specjalnych, o długości co najmniej 8 znaków.
2. Nowe hasła nie powinny wiązać się z Twoimi danymi: imieniem, nazwiskiem, ksywą. Nie powinny też zawierać nazw z bliskiego Ci otoczenia, jak miejsce pracy lub imię pupila.
3. Hasło powinno być unikalne dla każdego odwiedzanego przez Ciebie portalu, dla bezpieczeństwa, co jakiś czas, warto zmienić szyk liter i znaków.
4. Nie powinno się także zapisywać ważnych haseł do kont w plikach dostępnych na komputerze.
5. Korzystaj z menadżera haseł, aby tworzyć silniejsze hasła, których nie będzie trzeba zapamiętywać.



ZAKUPY W INTERNECIE

W celu ochrony przed cyberprzestępcami, podczas zakupów w Internecie:

1. Sprawdź cenę produktu – gdy jest zbyt niska może to sugerować towar niepełnowartościowy czy nawet podrobiony.
2. Przed zakupem zorientuj się kim jest osoba sprzedająca - mając pozytywne opinie zakup będzie pewniejszy.
3. Sprawdzaj od kiedy konto sprzedawcy widnieje w serwisie i ilu użytkowników korzystało z jego usług.
4. Za każdym razem czytaj regulamin sklepu i opis aukcji serwisu, z którego korzystasz.
5. Nie kasuj korespondencji ze sprzedającym – w przypadku oszustwa jest ona dowodem potwierdzającym zakup.

PHISHING – nie daj się złowić



Phishing - to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Cyberprzestępcy podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet naszych znajomych, starają się wyłudzić nasze dane logowania np. do kont bankowych, używanych przez nas kont społecznościowych, czy systemów biznesowych.

Przestępcy wykorzystują najczęściej sfałszowane e-maile i SMS-y. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych.

Jak radzić sobie z fałszywymi wiadomościami ?

Jeśli nie kliknąłeś w żaden link w wiadomości e-mail, to dobrze. Dopóki nie masz pewności, że nadawca jest prawdziwy, nie powinieneś klikać w żadne linki ani na nie odpowiadać.

W wiadomościach SMS lub mailach często wykorzystywane są tzw. tiny-URL, czyli skrócone adresy stron internetowych. Stąd też zalecamy zwracanie szczególnej uwagi na nazwy stron internetowych, które przesyłane są w podejrzanych mailach czy

SMS - ach np. zamiast www.allegro.pl wykorzystywany może być fałszywy adres www.allegrosklep.online itp.

Następną rzeczą jest ustalenie czy wiadomość e-mail jest autentyczna i nie jest oszustwem.

Jak rozpoznać e-mail wyłudający informacje

1. Wiadomości phishingowe są takprzygotowywane przez cyberprzestępców, aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe - często charakteryzują się niepoprawną gramatyką, interpunkcją, pisownią, czy też nie posiadają polskich znaków, np. nie używa się „ą”, „ę” itd.
2. Oceń, czy wiadomość e -mail pochodzi z firmy czy organizacji, z której została wysłana. Sprawdź użyte logotypy, stopki z danymi nadawcy itd.
3. Bądź podejrzliwy w stosunku do zwrotów typu „wyślij te dane w ciągu 24 godzin” lub „padłeś ofiarą przestępstwa, kliknij tutaj natychmiast”.
4. Twój bank lub jakakolwiek inna instytucja nigdy nie powinna prosić Cię o podanie w wiadomości e-mail danych osobowych.
5. Urzędy administracji publicznej nigdy nie proszą Cię przy pomocy SMS, czy maili o dopłatę do przesyłki, czy uregulowanie należności podatkowych.

6. Uważaj na skrócone linki, jeśli nie masz pewności, dokąd Cię poprowadzą, najedź na nie kursorem - nie klikaj! Na dole przeglądarki zostanie wyświetlony pełen adres linku.

Więcej informacji na temat bezpieczeństwa w sieci możesz znaleźć na stronach:

1. <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>.
2. <https://www.cert.pl> - gdzie można dowiedzieć się o najważniejszych cyberzagrożeniach i zgłosić różnego rodzaju niebezpieczne zdarzenia w sieci.
3. <https://dokumentyzastrzezone.pl/category/aktualnosci>
- z której możesz czerpać informacje o aktualnych zjawiskach związanych z bezpieczeństwem dokumentów – w tym bankowości internetowej.

CO ZROBIĆ, GDY ZOSTANIESZ OSZUKANY ?

1. Nie obwiniaj się. Oszuści są bardzo przekonujący i wykorzystują zaawansowane techniki manipulacji.
2. Zgłoś oszustwo w najbliższej jednostce Policji.
Twoje zgłoszenie może pomóc w ochronie innych osób.
3. Porozmawiaj o tym z rodziną i przyjaciółmi. Wspólna świadomość to najlepsza ochrona przed oszustwami.

Pamiętaj!

Twoje bezpieczeństwo jest dla nas najważniejsze. Nie wahaj się prosić o pomoc, kiedy czujesz niepewność. Razem możemy stworzyć bezpieczne środowisko dla Ciebie i Twoich bliskich.





SŁUŻBY RATOWNICZE

Jeżeli potrzebujesz pomocy służb (Policja, Straż Pożarna, Pogotowie Ratunkowe) to zadzwoń na bezpłatny numer alarmowy **112**.

Jak prawidłowo zgłaszać na numer alarmowy

Po wybraniu numeru alarmowego i zgłoszeniu się operatora postępuj zgodnie z jego zaleceniami. Spokojnie i wyraźnie powiedz

- gdzie jesteś (podaj adres) i co się stało;
- swoje imię i nazwisko;
- numer telefonu, z którego dzwonisz.

W sytuacji zgłoszenia innej interwencji niż oszustwo (np. wypadek drogowy, pożar itp.) dodatkowo podaj:

- jak wygląda sytuacja na miejscu zdarzenia;
- czy są osoby poszkodowane lub zagrożone (w miarę możliwości określ ich liczbę).

Pamiętaj!

Po przekazaniu wymienionych informacji nie rozłączaj się do czasu, kiedy wyraźnie zakomunikuje Ci to osoba przyjmująca Twoje zgłoszenie.



ZGŁOŚ PRZESTĘPSTWO

Jeśli jesteś świadkiem albo ofiarą przestępstwa, ktoś Ci coś ukradł albo Cię oszukał, zgłoś takie zdarzenie Policji lub Prokuraturze. Sprawdź, jak to zrobić.

Co musisz przygotować?

1. Dokument ze zdjęciem, który zawiera twoje dane osobowe – na przykład dowód osobisty, prawo jazdy, paszport, książeczkę wojskową.

2. W niektórych sytuacjach musisz przygotować dodatkowe dokumenty, na przykład:

- w przypadku kradzieży (np. sprzętu RTV, roweru, telefonu komórkowego) - zdjęcie, numery fabryczne itp.
- w przypadku oszustwa internetowego – zrzut ekranu

(screen shot)



prowadzonej korespondencji, otrzymanych wiadomości, itp.

Co musisz zrobić?

Opowiedz wszystko, co wiesz o przestępstwie. Policjant albo prokurator spíše protokół z Twoimi zeznaniami. Przeczytaj go uważnie i jeśli wszystko się zgadza, podpisz. Wysłuchaj jakie masz prawa i obowiązki. Gdy masz wątpliwości – porozmawiaj z policjantem albo prokuratorem.

Kiedy zgłosić?

Jak najszybciej – dzięki temu zwiększysz szansę na zatrzymanie sprawcy lub odnalezienie skradzionej rzeczy.

Gdzie zgłosić?

1. W dowolnej jednostce Policji (całodobowo).
2. W każdej siedzibie Prokuratury.

Dlaczego warto?

Dzięki temu pomożesz Policji w zatrzymaniu przestępcy i być może:

- uchronisz siebie i innych przed jego kolejnymi działaniami – na przykład przed następnym oszustwem lub kradzieżą;
- zwiększysz swoje szanse na odzyskanie rzeczy albo pieniędzy – jeśli ktoś cię okradł albo oszukał;
- zwiększysz bezpieczeństwo w swojej okolicy.



ZDALNIE – przez Internet, poprzez wysłanie wiadomości e-mail na adres danej instytucji.

Co musisz przygotować

Pisemne zawiadomienie o przestępstwie. W zawiadomieniu napisz jak najwięcej informacji na temat przestępstwa, które zgłaszasz:

- opisz dokładnie, co się stało, w jaki sposób, kiedy i gdzie,
- jeśli wiesz - napisz, kto jest sprawcą;
- podaj nazwę i adres jednostki Policji lub Prokuratury, do której wysyłasz zawiadomienie;

- podaj swoje dane kontaktowe: imię, nazwisko, telefon i adres, żeby Policja, Prokuratura lub instytucja, do której się zwracasz mogła się z Tobą skontaktować;
- podpisz się.

W niektórych sytuacjach musisz przygotować dodatkowe dokumenty, na przykład:

- w przypadku kradzieży (np. sprzętu RTV, roweru, telefonu komórkowego) - zdjęcie, numery fabryczne itp.
- w przypadku oszustwa internetowego – zrzut ekranu

(screen shot)  prowadzonej korespondencji, otrzymanych wiadomości, itp.

Co musisz zrobić?

1. Wyślij je mailem, faksem lub pocztą na adres Policji albo Prokuratury.
2. Czekaj na kontakt od osoby, która będzie zajmowała się Twoją sprawą.
3. W odpowiednim czasie zostaniesz poinformowany o wszczęciu bądź umorzeniu postępowania.

Gdzie wysyłasz dokumenty?

Powinieneś je wysłać do jednostki Policji albo Prokuratury - właściwej dla miejsca zdarzenia. Jednakże możesz je przekazać dowolnej jednostce. Jeśli nie możesz wysłać pisma,

bo np. jesteś w szpitalu, możesz poprosić kogoś o pomoc. Taka osoba może w Twoim imieniu wysłać takie zawiadomienie.

Więcej informacji znajdziesz na poniższej stronie internetowej:

<https://www.gov.pl/web/gov/zglos-przestepstwo>

Miejsce na moje notatki.



POLICJA

**Komenda Wojewódzka
Policji w Katowicach**