Informacja opracowana przez Prezesa UKE w oparciu o dane przekazane przez przedsiębiorców telekomunikacyjnych na podstawie art. 62 ust. 2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2014 r., poz. 243 ze zm., zwanej dalej „Pt").

dotycząca:

- **wskazania jakie sposoby wykorzystania usług telekomunikacyjnych są niezgodne z prawem lub stanowią rozpowszechnianie szkodliwych treści, w tym przypadki naruszenia praw autorskich i pokrewnych, oraz wskazanie konsekwencji prawnych tych czynów, a także**
- **sposobów ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych.**

Niniejsza informacja Prezesa Urzędu Komunikacji Elektronicznej stanowi wypełnienie obowiązku prawnego wskazanego w art. 62 ust. 1 pkt 3 i 4 Pt i została przygotowana w oparciu o dane przekazane przez stacjonarnych i mobilnych przedsiębiorców telekomunikacyjnych.

Warszawa, maj 2016 r.

Spis treści:

1. Niezgodne z prawem lub stanowiące rozpowszechnianie szkodliwych treści sposoby wykorzystania usług telekomunikacyjnych, w tym przypadki naruszenia praw autorskich i pokrewnych, oraz konsekwencje prawne tych czynów.

1.1. Niezgodne z prawem lub stanowiące rozpowszechnianie szkodliwych treści sposoby wykorzystania usług telekomunikacyjnych.

- działania powodujące albo mogące powodować zakłócenia pracy urządzeń aktywnych podłączonych do sieci telekomunikacyjnej lub sieci teleinformatycznej operatora oraz sieci Internet;
- kierowanie bez zgody operatora do sieci telekomunikacyjnej lub sieci innych przedsiębiorców telekomunikacyjnych za pomocą jakichkolwiek urządzeń telekomunikacyjnych przy użyciu karty SIM otrzymanej przez abonenta/użytkownika, ruchu pochodzącego z innych sieci telekomunikacyjnych;
- uzyskanie nielegalnego dostępu lub wykorzystanie usług telekomunikacyjnych lub infrastruktury telekomunikacyjnej niezgodnie z przeznaczeniem;
- wykorzystanie usług telekomunikacyjnych lub infrastruktury telekomunikacyjnej zgodnie z przeznaczeniem, ale bez zamiaru uiszczenia opłaty za usługi telekomunikacyjne;
- generowanie ruchu nie służącego bezpośredniej wymianie informacji pomiędzy użytkownikami, a mającego na celu uzyskanie jak najwyższych wskazań urządzeń rozliczających ruch międzyoperatorski;
- generowanie ruchu w celu przeciążenia elementów infrastruktury telekomunikacyjnej (tzw. Atak „Denial of Service”);
- podawanie przez abonenta/użytkownika nieprawdziwych danych lub posługiwanie się przez niego podrobionymi lub przerobionymi dokumentami przy zawieraniu lub w trakcie wykonywania umowy o świadczenie usług telekomunikacyjnych;
- wykorzystywanie hasła abonenckiego lub hasła dostępu do systemów obsługowych bez zgody uprawnionego użytkownika;
- udostępnianie usług telekomunikacyjnych operatora innym osobom w celu uzyskania korzyści majątkowych bez zgody operatora;
- używanie karty SIM, korzystając ze skradzionego telefonu lub telefonu nieposiadającego znaku zgodności z zasadniczymi wymaganiami;
- instalowanie złośliwego oprogramowania (innymi słowy instalowanie rozwiązań, aplikacji, które mogą powodować szkody na urządzeniach końcowych, niszczyć lub wykradać dane) na telefonie użytkownika, bez jego wiedzy, które mogą doprowadzić do niezamierzonych operacji, w szczególności:

a) samoczynnego restartu urządzenia końcowego (telefonu);
b) samoczynnej wysyłki danych lub komunikatów;
c) przekierowania SMS-ów bez wiedzy użytkownika;
d) przekierowań na płatne numery bez wiedzy użytkownika;
e) całkowitego lub częściowego przejęcia kontroli nad urządzeniem;

- instalowanie, bez zgody użytkownika na urządzeniu końcowym użytkownika, aplikacji niewiadomego pochodzenia, która może spowodować utratę kontroli użytkownika nad urządzeniem oraz doprowadzić do utraty poufności danych osobowych;

- podmienianie numeru nadawcy (tzw. „spoofing") - działanie polegające na fałszowaniu, podmianie numeru nadawcy tak aby zmylić odbiorcę i w konsekwencji wyłudzić dane, informacje wrażliwe, np. numer karty kredytowej, numery PIN, hasła, itp.;
- kradzież danych z urządzenia końcowego użytkownika, np. z wykorzystaniem Bluetooth;
- wysyłanie informacji handlowych, w tym innych niezamówionych informacji (SPAM-u) do innych użytkowników końcowych, bez ich zgody;
- wysyłanie wirusów do innych użytkowników końcowych;
- zwalczanie programów antywirusowych;
- blokowanie kart pamięci;
- nieuprawnione podsłuchiwanie rozmów telefonicznych bez podstawy prawnej;
- nieuprawnione lokalizowanie innych użytkowników;
- nieuprawnione dublowanie karty SIM – tzw. „klonowanie kart SIM" bez wiedzy i zgody operatora;
- wykonywanie do użytkowników jednokrotnych połączeń telefonicznych z numeru telefonicznego o formacie zgodnym z formatem standardowego numeru abonenckiego, celem skłonienia danego użytkownika do oddzwonienia i wygenerowania połączeń Premium (o podwyższonej opłacie) lub międzynarodowych o podwyższonej opłacie, lub inne działania mające na celu nakłanianie użytkowników do generowania bez ich wiedzy połączeń telefonicznych typu Premium lub międzynarodowych oraz do wysyłania SMS-ów Premium lub międzynarodowych o podwyższonej opłacie;
- wyłudzanie doładowań kont pre-paid poprzez rozsyłanie SMS-ów z prośbą o kod doładowujący przy pomocy wprowadzenia danego użytkownika końcowego w błąd co do tożsamości osoby wysyłającej prośbę;
- prowadzenie działań niezgodnych z prawem i/lub dobrymi obyczajami, w tym promowanie i/lub rozpowszechnianie nielegalnych i szkodliwych treści, w tym w Internecie, dotyczących rasizmu, faszyzmu, komunizmu, ksenofobii, szerzenia nienawiści lub nakłaniania do przemocy wobec odmiennej rasy, pochodzenia etnicznego, wyznania, płci, wieku, orientacji seksualnej itp.;
- rozpowszechnianie i/lub propagowanie pornografii, w tym:
  a) prezentowanie treści pornograficznych w taki sposób, że może to narzucić ich odbiór osobie, która sobie tego nie życzy (art. 202 § 1 ustawy z dnia 6 czerwca 1997 r. kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm., zwanej dalej: „K.k.")),
  b) prezentowanie małoletniemu poniżej lat 15 treści pornograficznych lub udostępniania mu przedmiotów mających taki charakter albo rozpowszechniania treści pornograficznych w sposób umożliwiający mu zapoznanie się z nimi (art. 202 § 2 K.k.);
  c) utrwalanie, sprowadzanie, przechowywanie i posiadanie treści pornograficznych z udziałem małoletniego poniżej 15 lat (art. 202 § 4 i 4a K.k.);
  d) produkowanie, utrwalanie, sprowadzanie czy też publiczne prezentowanie w celu rozpowszechniania treści pornograficznych z udziałem małoletniego poniżej 18 roku życia (art.202 § 3 K.k.);

e) rozpowszechnianie treści pornograficznych związanych z prezentowaniem przemocy lub posługiwaniem się zwierzęciem (art.202 § 3 K.k.);

- korzystanie z serwisu z naruszeniem prawa, praw osób trzecich (w tym praw autorskich oraz dóbr osobistych, m.in. prawa do wizerunku), dobrych obyczajów lub ustalonych zwyczajów;
- podejmowanie działań utrudniających lub uniemożliwiających funkcjonowanie serwisu lub korzystanie z niego przez abonentów/użytkowników niezgodnie z przeznaczeniem, innych działań sprzecznych z zasadami współżycia społecznego;
- niszczenie, uszkadzanie, usuwanie, dokonywanie zmian lub utrudnianie dostępu do danych informatycznych, albo ich istotne zakłócenie lub uniemożliwianie automatycznego przetwarzania, gromadzenie lub przekazywanie takich danych oraz uzyskiwanie dostępu do całości lub części systemu informatycznego lub informacji nieprzeznaczonej poprzez podłączanie się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenia;
- rozpowszechnienie treści umożliwiających uprawianie lub reklamowanie hazardu (np. zawieranie zakładów bukmacherskich i branie udziału w loteriach grach liczbowych itp.);
- podejmowanie działań (zaniechań) mających na celu dokuczanie i nękanie innych osób lub instytucji (tzw. „stalking”);
- przywłaszczanie praw autorskich, albo wprowadzanie w błąd w odniesieniu do autorstwa w całości lub części cudzego utworu i/lub artystycznego wykonania;
- rozpowszechnianie spamu, w tym niezamówionych materiałów marketingowych, promocyjnych i/lub reklamowych, manipulowanie danymi, w tym rankingami, rozpowszechnianie lub publikowanie fałszywych opinii lub ocen;
- rozpowszechnianie, bez podania nazwiska lub pseudonimu twórcy, cudzego utworu w wersji oryginalnej, albo w postaci opracowania, artystycznego wykonania, publicznego zniekształcenia takiego utworu, artystycznego wykonania fonogramu, wideogramu lub nadania oraz inne naruszenie cudzego prawa autorskiego lub prawa pokrewnego, określonego w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2006 r., Nr 90 poz. 631), zwanej dalej „PrAut”, w celu osiągnięcia korzyści majątkowej bez uprawnienia albo wbrew jego warunkom;
- rozpowszechnianie, zwielokrotnienie nabycia lub pomocy w jego zbyciu, przyjmowanie bądź pomocy w ukryciu choćby nieumyślnie cudzego utworu w wersji oryginalnej albo w postaci opracowania, artystycznego wykonania, fonogramu, wideogramu lub nadania;
- uniemożliwianie lub utrudnianie wykonywania prawa do kontroli korzystania z utworu;
- podszywanie się pod inne osoby lub podmioty;
- wykorzystywanie usług telekomunikacyjnych do popełniania przestępstw, przy czym usługa telekomunikacyjna jest tu wykorzystywana, jako kanał komunikacji z pokrzywdzonym (np. wyłudzenia środków pieniężnych metodą „na wnuczka”);
- wykorzystywanie środków masowego komunikowania się do popełniania przestępstw zniesławienia czy zniewagi.

1.2. Przykłady nadużyć telekomunikacyjnych. Oszustwa i wyłudzenia.

1) Użycie urządzeń FCT (inaczej tzw. Sim-boxing).

Nadużycie powyższe polega na wykorzystaniu różnicy pomiędzy cenami detalicznymi a stawkami za zakończenie połączenia poprzez skierowanie ruchu międzyoperatorskiego na karty SIM „udające" zwykłego abonenta/użytkownika sieci mobilnej. W tym przypadku poszkodowanym jest najczęściej operator a skutkiem ubocznym zestawienia połączenia poprzez FCT bez wiedzy abonenta/użytkownika jest zmiana numeru dzwoniącego (numeru A) oraz inne braki w funkcjonalności usługi (takie jak obniżenie jakości czy też nawet brak połączenia). Standardową procedurą operatorów telekomunikacyjnych w przypadku wykrycia zjawiska kierowania ruchu międzyoperatorskiego przez urządzenia FCT jest zawieszenie świadczenia usług telekomunikacyjnych, a następnie zerwanie umowy i w razie większych strat – dochodzenie odszkodowania na drodze sądowej. Niewykluczone jest również skierowanie zawiadomienie do prokuratury dotyczące popełnienia przestępstwa, np. fałszowania informacji dotyczącej realizacji połączeń (zmiana numeru abonenta/użytkownika dzwoniącego).

2) Prowokowanie oddzwaniania na numer o wysokiej opłacie (tzw. „Wangiri fraud").

Nadużycie to polega na oszukaniu abonenta/użytkownika, który automatycznie oddzwania na numer, który figuruje jako „nieodebrane połączenie". Numer ten najczęściej jest podobny do numeru krajowego, ale jest numerem zagranicznym o cenie za połączenie znacznie wyższej niż cena krajowa. Często wykorzystywane są podobieństwa początku numerów krajowych i międzynarodowych (np. 22 – Warszawa, +22 – kraje afrykańskie). Operatorzy w przypadku wykrycia nagłego przyrostu ruchu na dany kierunek międzynarodowy podejmują stosowne działania. Konsekwencją dla nieświadomych abonentów/użytkowników jest konieczność zapłacenia za zrealizowane połączenia.

3) Wyłudzanie kodów doładowujących poprzez SMS.

Nadużycie polegające na próbie podszycia się pod dostawcę usług i przesłanie do abonenta/użytkownika usług przedpłaconych informacji o rzekomej korzyści (podwójne doładowanie, możliwość wygrania drogiego sprzętu, etc.) w przypadku przesłania zwrotnego kodu doładowującego. Wysłany kod zostaje zużyty przez oszusta. Czyn ten może wypełniać znamiona przestępstwa oszustwa lub tzw. „kradzieży impulsów" a jego konsekwencje przewidziane są na gruncie K.k.

4) Podmiana numerów kont bankowych na fakturach.

Możliwym jest oszustwo polegające na dokonaniu kradzieży rachunku/faktury ze skrzynki abonenta/użytkownika i zmianie na tym rachunku numeru konta bankowego operatora na inne. Działanie takie nosi znamiona kilku przestępstw wskazanych w K.k. Należy więc zachować ostrożność w przypadku gdy znaleziony w skrzynce pocztowej dokument zawierający logo operatora wygląda na zmieniony czy przerobiony. Numer konta do zapłaty faktury można zawsze potwierdzić z operatorem infolinii operatora.

5) Wprowadzenie w błąd co do tożsamości podmiotu zawierającego umowę.

Nadużycie polegające na wprowadzeniu w błąd klienta co do tożsamości podmiotu, z którym klient ma zamiar zawrzeć umowę o świadczenie usług telekomunikacyjnych. Najwięcej tego typu przypadków było związanych z nieuczciwymi przedstawicielami handlowymi niewielkich spółek telekomunikacyjnych, które wykorzystywały podobieństwo nazw z dużymi, znanymi na rynku przedsiębiorcami.

6) International Revenue Share Fraud (IRSF).

Nadużycie polega na generowaniu sztucznego ruchu na zagraniczne numery premium lub o wysokim koszcie. Często dla zwiększenia zysków połączenia inicjowane są jako konferencyjne. Nadużycie polega na wykorzystywaniu rozliczeń międzyoperatorskich

i otrzymywaniu części przychodów z opłat za zakańczanie połączeń uzyskanych przez posiadacza numeru.

7) Włamania do centralek PBX (PBX Hacking).

Nadużycie polega na nieuprawnionym użyciu PBX w celu wykonywania dużych wolumenów połączeń wychodzących, w tym generowania ruchu na numery o podwyższonej opłacie. Standardową procedurą operatorów telekomunikacyjnych, w przypadku wykrycia nadużycia, jest poinformowanie właściciela centralki o identyfikacji podejrzanego ruchu. Każdy przypadek jest rozpatrywany indywidualnie.

8) SMS-y wprowadzające w błąd użytkownika (wprowadzenie w błąd w celu uzyskania korzyści).

Nadużycie polega na wprowadzeniu użytkownika w błąd, poprzez wysyłanie (najczęściej automatycznie) wiadomości, której treść sugeruje uruchomienie płatnej subskrypcji i informuje o możliwości wyłączenia usługi poprzez wysłanie zwrotnej wiadomości z określonym kodem (wysłanej na numer wysoko płatny bez podania kosztów lub przy zaniżeniu stawki za SMS zwrotny). W konsekwencji abonent/użytkownik odsyłający wiadomość, spodziewający się usunięcia subskrypcji, ponosi koszt korzystania z usług o podwyższonej płatności. Osoba pokrzywdzona może dochodzić roszczeń od właściciela serwisu premium. Konsekwencją dla nieświadomych abonentów/użytkowników jest konieczność zapłacenia za zrealizowane usługi. Abonentowi/użytkownikowi wprowadzonemu w błąd przysługuje prawo do złożenia reklamacji (wraz z podaniem odpowiednich dowodów).

9) Wprowadzanie w błąd w celu akceptacji przez abonenta/użytkownika subskrypcji MT (płatne za otrzymanie SMS/MMS).

Nadużycie podlega na tym, że osoba chcąca skorzystać z różnych serwisów w Internecie, np.: obejrzeć film, doładować telefon, wysłać e-kartkę z życzeniami, podaje swój numer telefonu w celu otrzymania kodu dla wybranej usługi, a zamiast tego otrzymuje SMS-a powiadamiającego o uruchomieniu SMS-ów wysokopłatnych przy odbiorze (nawet kilka razy w tygodniu). Ponadto ściąganie aplikacji z niezaufanego źródła, uruchamianie gier itp. również może spowodować nieświadome uruchomienie zamówienia na otrzymywanie SMS-ów MT. Sposobem ochrony jest szczegółowe zapoznawanie się z regulaminami usług oraz ich rodzajami a w przypadku braku dostępu do treści regulaminu - niekontynuowanie transakcji. Konsekwencją dla nieświadomych abonentów/użytkowników jest konieczność zapłacenia wysokiego rachunku za usługi.

10) Generowanie sztucznego ruchu telekomunikacyjnego (inaczej tzw. „ATG").

Nadużycie polega na generowaniu sztucznego ruchu, który w szczególności nie służy nadawaniu, odbiorowi lub transmisji informacji kierowanych od lub do abonenta/użytkownika, bądź którego głównym celem jest uzyskiwanie pewnej puli (liczby lub czasu trwania) połączeń telekomunikacyjnych pomiędzy siecią operatora a innymi sieciami telekomunikacyjnymi.

1.3. Przykłady naruszenia praw autorskich i pokrewnych.

Należy wskazać, że przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór). Ochrona przysługuje twórcy niezależnie od spełnienia jakichkolwiek formalności. Wszystko co oryginalne, np. tekst artykułu, projekt strony, wiadomość e-mail lub wpis na forum, zostaje automatycznie objęte ochroną prawa

autorskiego. Aby jednak ochrona taka była możliwa, stworzony utwór musi być możliwy do zidentyfikowania jako oryginalne dzieło.

Wszystkie dzieła muzyczne, artykuły, kompozycje graficzne, podobnie jak i inne dzieła artystyczne zamieszczone na stronach WWW lub pobierane za pomocą łączy internetowych, jeżeli spełniają przesłanki utworu, podlegają ochronie przewidzianej w PrAut.

Głównym celem tej dziedziny prawa jest ochrona szeroko pojętych dzieł autorów, przed ich kradzieżą i wykorzystaniem bez zezwolenia lub wbrew warunkom zezwolenia twórcy. Dla prawnoautorskiej ochrony utworu nie ma znaczenia, w jaki sposób dokonujący naruszenia wszedł w jego posiadanie lub też w jaki sposób utwór do niego dotarł. W szczególności nie ma znaczenia okoliczność, że utwór stanowiący przedmiot naruszenia dotarł do dokonującego naruszenia jako niezamawiana korespondencja przesyłana drogą elektroniczną (tzw. spam). Do wyjątków bezwzględnej ochrony autorskiej należy instytucja tzw. dozwolonego użytku (art. 25 – 35 PrAut, w tym prawo przedruku oraz prawo cytatu.

Poniżej przedstawione zostały przykładowe sposoby wykorzystania usług telekomunikacyjnych (także niekomercyjne) stanowiące przypadki naruszenia praw autorskich i pokrewnych:

1) nielegalne ściąganie (tzw. „downloading") programów z sieci do własnego urządzenia software – bez wymaganej zgody uprawnionego na korzystanie z utworów;

2) kopiowanie, dystrybuowanie lub udostępnianie zdjęć, filmów, muzyki, gier, programów, artykułów, ilustracji z gazet poza zakresem dozwolonego użytku bez wymaganej zgody uprawnionego na korzystanie z utworów;

3) udostępnianie na własnej stronie internetowej utworów, np. tekstów, artykułów, zdjęć, grafik, makiety strony, poza zakresem wynikającym z dozwolonego użytku;

4) zamieszczanie (na własnej witrynie) cudzego tekstu i podpisanie go własnym nazwiskiem;

5) zamieszczenie cudzego tekstu bez podania autora i źródła utworu;

6) rozpowszechnienie opracowań (przeróbek) cudzych utworów (tekstów) bez zezwolenia autora;

7) umieszczanie we własnych tekstach twórczych fragmentów cudzych tekstów jako własnych;

8) obchodzenie zabezpieczeń w celu możliwości korzystania z programów komputerowych (np. przez crackowanie);

9) usuwanie lub zmiana bez upoważnienia jakichkolwiek elektronicznych informacji na temat zarządzania prawami autorskimi lub prawami, a także świadomego rozpowszechniania utworów z bezprawnie usuniętymi lub zmodyfikowanymi takimi informacjami.

1.4. Konsekwencje prawne wykorzystania usług telekomunikacyjnych w sposób niezgodny z prawem lub stanowiący rozpowszechnianie szkodliwych treści.

Konsekwencje prawne wykorzystania usług telekomunikacyjnych w sposób niezgodny z prawem lub stanowiący rozpowszechnianie szkodliwych treści mogą być dwojakiego rodzaju – regulaminowe i prawne.

Zgodnie z postanowieniami regulaminów świadczenia usług telekomunikacyjnych przedsiębiorców telekomunikacyjnych w stosunku do użytkowników, którzy dopuszczają się nadużyć w stosunku do przedsiębiorców, mogą być wyciągnięte następujące konsekwencje:

- upomnienie telefoniczne lub listowne,
- czasowe zawieszenie świadczenia usług,
- wypowiedzenie umowy abonenckiej.

Należy wskazać, że konsekwencje prawne naruszeń wskazanych w rozdziałach 1.1. i 1.2., są określone w szczególności w:

- K.k.;
- PrAut;
- Ustawie z dnia 20 maja 1971 r. Kodeks wykroczeń (t.j. Dz.U. z 2015 r., poz. 1094, z późn. zm.);
- Ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2014 r., poz. 121 z późn. zm.), zwanej dalej „Kc";
- Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j Dz.U. 2013 r., poz. 1422, z późn. zm.);
- Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r.,2135);
- innych ustawach szczególnych

i mogą polegać na wymierzeniu kary pozbawiania wolności, ograniczania wolności lub grzywny oraz przepadku przedmiotów służących do popełnienia przestępstwa, szczegółowo określonych w/w aktach prawnych.

W przypadku stwierdzenia przez operatora powyższych naruszeń, na zasadach określonych w odpowiednim regulaminie świadczenia usług telekomunikacyjnych lub w innym dokumencie stanowiącym integralną cześć umowy o świadczenie usług telekomunikacyjnych, operator może być uprawniony do zablokowania możliwości inicjowania połączeń przez użytkownika podejmującego powyższe działania lub zawieszenia świadczenia na rzecz takiego użytkownika wszelkich usług; operator na zasadach określonych w odpowiednim regulaminie świadczenia usług telekomunikacyjnych lub w innym dokumencie stanowiącym integralną cześć umowy o świadczenie usług telekomunikacyjnych, może również być uprawniony do rozwiązania wiążącej go z takim użytkownikiem umowy o świadczenie usług telekomunikacyjnych z zachowaniem okresu wypowiedzenia albo bez zachowania okresu wypowiedzenia.

Niezależnie od powyższego, w przypadku, gdy dane działanie wypełnia znamiona przestępstwa, operator bądź inna osoba dotknięta naruszeniem, może złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa do odpowiednich organów ścigania.

Operator w razie poniesienia szkody w związku z opisanymi powyżej działaniami, może również skorzystać z drogi sądowej celem uzyskania odpowiedniego odszkodowania za poniesioną szkodę w postępowaniu cywilno-prawnym.

1.4.1. Konsekwencje prawne wykorzystania usług telekomunikacyjnych z naruszeniem praw autorskich i pokrewnych.

1.4.1.1. Sankcje cywilnoprawne na podstawie PrAut.

Naruszenie praw autorskich niemajątkowych (art. 78 PrAut).

Jeśli doszło do naruszenia praw niemajątkowych, twórca, może żądać:
1) zaniechania naruszenia;
2) dopełnienia przez osobę, która dopuściła się naruszenia, czynności potrzebnych do usunięcia jego skutków, w szczególności złożenia publicznego oświadczenia

o odpowiedniej treści i formie; w większości przypadków chodzi tu o przeprosiny lub publikację sprostowania na koszt pozwanego;
3) jeżeli naruszenie było zawinione (tzn. gdy osoba, która naruszyła prawo autorskie wiedziała lub z łatwością mogła się dowiedzieć o istnieniu praw twórcy), sąd może przyznać twórcy odpowiednią sumę pieniężną tytułem zadośćuczynienia za doznaną krzywdę (naprawienie szkody niemajątkowej, cierpienia, stresu lub innych negatywnych przeżyć psychicznych związanych z naruszeniem praw twórcy) lub - na żądanie twórcy - zobowiązać sprawcę, aby uiścił odpowiednią sumę pieniężną na wskazany przez twórcę cel społeczny, np. na rzecz wybranej przez powoda - twórcę fundacji czy stowarzyszenia.

Naruszenie praw autorskich majątkowych (art. 79 PrAut)

Uprawniony, którego autorskie prawa majątkowe zostały naruszone, może żądać od osoby, która naruszyła te prawa:
1) zaniechania naruszania;
2) usunięcia skutków naruszenia;
3) naprawienia wyrządzonej szkody:
   a) na zasadach ogólnych – w oparciu o przepisy Kodeksu cywilnego (uprawniony musi w takim wypadku udowodnić wysokość szkody, którą poniósł rzeczywiście, lub wysokość korzyści, które utracił na skutek naruszenia jego praw), albo
   b) poprzez zapłatę sumy pieniężnej w wysokości odpowiadającej dwukrotności stosownego wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z utworu[1];
4) wydania uzyskanych korzyści;
5) jednokrotnego albo wielokrotnego ogłoszenia w prasie oświadczenia odpowiedniej treści i w odpowiedniej formie lub podania do publicznej wiadomości części albo całości orzeczenia sądu wydanego w rozpatrywanej sprawie, w sposób i w zakresie określonym przez sąd;
6) zapłaty przez osobę, która naruszyła autorskie prawa majątkowe, odpowiedniej sumy pieniężnej, nie niższej niż dwukrotna wysokość uprawdopodobnionych korzyści odniesionych przez sprawcę z dokonanego naruszenia, na rzecz Funduszu Promocji Twórczości, gdy naruszenie jest zawinione i zostało dokonane w ramach działalności gospodarczej wykonywanej w cudzym albo we własnym imieniu, choćby na cudzy rachunek;
7) odpowiedniego rozporządzenia bezprawnie wytworzonymi przedmiotami oraz środkami i materiałami użytymi do ich wytworzenia, np. ich wycofania z obrotu, przyznania ich na poczet należnego odszkodowania lub zniszczenia.

1.4.1.2. Sankcje karne za naruszenie praw autorskich i pokrewnych.

Sankcje karne za naruszenie praw autorskich i pokrewnych zostały ujęte w następujących przepisach:

1) art. 115 PrAut

1. Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

[1] Na mocy wyroku Trybunału Konstytucyjnego z dnia 23.06.2015 r. (Dz.U. z 2015 r. poz. 932) Art. 79 ust. 1 pkt 3 lit. b ustawy o prawie autorskim i prawach pokrewnych w zakresie, w jakim uprawniony, którego autorskie prawa majątkowe zostały naruszone, może żądać od osoby, która naruszyła te prawa, naprawienia wyrządzonej szkody poprzez zapłatę sumy pieniężnej w wysokości odpowiadającej - w przypadku gdy naruszenie jest zawinione - trzykrotności stosownego wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z utworu, jest niezgodny z art. 64 ust. 1 i 2 w związku z art. 31 ust. 3 w związku z art. 2 Konstytucji Rzeczypospolitej Polskiej.

2. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.
3. Kto w celu osiągnięcia korzyści majątkowej w inny sposób niż określony w ust. 1 lub ust. 2 narusza cudze prawa autorskie lub prawa pokrewne określone w art. 16, art. 17, art. 18, art. 19 ust. 1, art. 19^1, art. 86, art. 94 ust. 4 lub art. 97, albo nie wykonuje obowiązków określonych w art. 19^3 ust. 2, art. 20 ust. 1-4, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

2) art. 116 PrAut

1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.
3. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5.
4. Jeżeli sprawca czynu określonego w ust. 1 działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3) art. 117 PrAut

1. Kto bez uprawnienia albo wbrew jego warunkom w celu rozpowszechnienia utrwala lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności do lat 3.

4) art. 118 PrAut

1. Kto w celu osiągnięcia korzyści majątkowej przedmiot będący nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnionego bez uprawnienia albo wbrew jego warunkom nabywa lub pomaga w jego zbyciu albo przedmiot ten przyjmuje lub pomaga w jego ukryciu, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od roku do lat 5.
3. Jeżeli na podstawie towarzyszących okoliczności sprawca przestępstwa określonego w ust. 1 lub 2 powinien i może przypuszczać, że przedmiot został uzyskany za pomocą czynu zabronionego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

5) art. 118 (1) PrAut

1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami lub ich komponentami, albo reklamuje je w celu

sprzedaży lub najmu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

6) art. 119 PrAut

Kto uniemożliwia lub utrudnia wykonywanie prawa do kontroli korzystania z utworu, artystycznego wykonania, fonogramu lub wideogramu albo odmawia udzielenia informacji przewidzianych w art. 47, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

1.4.1.3. Sankcje cywilnoprawne na podstawie przepisów kodeksu cywilnego.

Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać:

1) zaniechania tego działania, chyba że nie jest ono bezprawne, ciężar udowodnienia, że działanie, że działanie nie miało charakteru bezprawnego spoczywa na pozwanym, powód – twórca nie musi uzasadniać, że działanie pozwanego miało taki charakter, bowiem działa na jego rzecz domniemanie bezprawności tego działania, wyrażone w ustawie;

2) w razie dokonanego naruszenia twórca może także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie, na zasadach podobnych jak w przypadku roszczenia uregulowanego przepisami PrAut;

3) twórca może również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny, jeżeli naruszenie dóbr osobistych było skutkiem działania zawinionego, a więc podjętego mimo tego, że sprawca wiedział lub z łatwością mógł się dowiedzieć o istnieniu praw autorskich;

4) jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych, oznacza to, że w przypadku zawinionego działania sprawcy, autor uprawniony będzie do żądania zapłaty sumy pieniężnej, która pozwoli na wyrównanie strat majątkowych, jakich doznał na skutek naruszenia jego autorskich praw osobistych (mogą to być straty już poniesione, albo utracone korzyści).

2. Sposoby ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych.

Do sposobów ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych należy m.in. zaliczyć:

1) wykorzystywanie odpowiednio zabezpieczonego komputera (oprogramowanie antywirusowe, najnowsze wersje przeglądarek internetowych);

2) regularne skanowanie swojego komputera w celu wyeliminowania obecności szkodliwego oprogramowania;

3) stosowanie bezpiecznych haseł w sieci;

4) zabezpieczenie routerów i komputerów poprzez instalację zapory ogniowej (tzw. Firewall). Zapora ogniowa filtruje połączenia zarówno przychodzące, jak i wychodzące z komputera oraz blokuje potencjalnie niebezpieczne aplikacje;

5) wskazanie, że pewnych informacji nie należy podawać drogą telefoniczną, elektroniczną, w Internecie w celu zachowania prywatności, np. numeru PESEL, hasła do portali, numerów kont, PIN;

6) informacja o oszustwach sieciowych (np. phishing – abonent/użytkownik powinien unikać wchodzenia na portale bankowe, społecznościowe itd. z linków, które dostał z nieznanych źródeł);

7) ochrona przez abonenta/użytkownika karty SIM przed kradzieżą, zniszczeniem, uszkodzeniem, zagubieniem lub utratą w inny sposób oraz niezwłoczne informowanie operatora przez abonenta/użytkownika w przypadku zagubienia, kradzieży, zniszczenia, uszkodzenia lub utraty karty SIM;

8) minimalizacja ryzyka kradzieży urządzenia telekomunikacyjnego:

- zabezpieczenie dostępu do urządzenia za pomocą kodu PIN, symbolu rysowanego na ekranie, poprzez rozpoznawanie przez urządzenie swojej twarzy lub głosu, lub hasła, (patrz instrukcja obsługi urządzenia);
- zabezpieczenie dostępu do karty SIM za pomocą kodu PIN;
- sprawdzenie w instrukcji obsługi urządzenia, czy nie ma wbudowanych ono innych funkcji zabezpieczających przed nieautoryzowanym użyciem, pomagających w jego odnalezieniu lub kasujących wszystkie dane w urządzeniu w przypadku jego zagubienia lub kradzieży;
- przechowywanie w bezpiecznym miejscu numeru IMEI urządzenia. Znajduje się on na oryginalnym pudełku, na specjalnych naklejkach. Aby wyświetlić numer IMEI na ekranie urządzenia należy wpisać kod *#06# i nacisnąć przycisk dzwonienia.

9) regularne wykonywanie kopie zapasowej informacji przechowywanej w urządzeniu telekomunikacyjnym, co pozwoli uniknąć przykrych niespodzianek w przypadku jego utraty.

10) ochrona przez abonenta/użytkownika poufności i nieudostępnianie kodu PIN lub kodu PUK do karty SIM osobom trzecim oraz niezwłoczna zmiana przez abonenta/użytkownika kodu PIN w przypadku podejrzenia wejścia w jego posiadanie przez osobę trzecią;

11) blokowanie przez abonenta/użytkownika dostępu do karty SIM, aparatu telefonicznego lub innego urządzenia elektronicznego umożliwiającego za pośrednictwem karty SIM korzystanie z usług świadczonych przez operatora, w szczególności ustawienie okresu czasu, po którym automatycznie blokowany jest dostęp do aparatu telefonicznego, gdy nie jest on używany;

12) nieudostępnianie przez abonenta/użytkownika osobom trzecim dokumentów lub danych umożliwiających zawarcie w jego imieniu lub na jego rzecz umowy o świadczenie usług telekomunikacyjnych;

13) ochrona przez abonenta/użytkownika poufności i nieudostępnianie osobom trzecim dokumentów lub danych, w szczególności hasła do konta abonenckiego, wykorzystywanych do uwierzytelnienia abonenta/użytkownika przez operatora w procesie sprzedaży lub obsługi klienta oraz niezwłoczna zmiana przez abonenta/użytkownika hasła do konta abonenckiego w przypadku podejrzenia wejścia w jego posiadanie przez osobę trzecią;

14) nieudostępnianie przez abonenta/użytkownika osobom trzecim dokumentów zawierających dane o świadczonych przez operatora usługach telekomunikacyjnych, w szczególności faktur oraz szczegółowych wykazów połączeń (tzw. bilingów);

15) ochrona przez abonenta/użytkownika poufności i nieudostępnianie osobom trzecim danych, w szczególności hasła, wykorzystywanych do uwierzytelnienia dostępu abonenta/użytkownika do portalów internetowych, umożliwiającego przeglądanie poprzez dostęp elektroniczny danych dotyczących abonenta/użytkownika, usług świadczonych przez operatora na rzecz abonenta/użytkownika i składania dyspozycji oraz niezwłoczna zmiana przez abonenta/użytkownika hasła do portalów internetowych w przypadku podejrzenia wejścia w jego posiadanie przez osobę trzecią;

16) korzystanie przez abonenta/użytkownika z mechanizmów umożliwiających potwierdzanie wykonywanych operacji (tokeny, kody SMS lub hasła jednorazowe);

17) możliwość zarządzania przez abonenta/użytkownika zgodami lub sprzeciwami dotyczącymi przetwarzania jego danych, w tym danych osobowych, takich jak:

- dane, o których mowa w art. 161 ust. 3 Pt, w tym nazwisk i imion, imion rodziców, miejsca i daty urodzenia, adresu zamieszkania, numeru PESEL czy numeru dokumentu tożsamości,
- zgoda na umieszczenie danych w publicznie dostępnym spisie abonentów (książce teleadresowej), w tym na przekazywanie danych do podmiotu, o którym mowa w art. 67 Pt,
- zgoda na marketing bezpośredni z wykorzystaniem telefonu,
- zgoda na otrzymywanie informacji handlowych za pomocą środków komunikacji elektronicznej, w szczególności przy użyciu automatycznych systemów wywołujących,
- zgoda na przetwarzanie danych transmisyjnych dla celów marketingu usług telekomunikacyjnych,
- zgoda na marketing bezpośredni dotyczący innych niż Spółka (usługodawca) podmiotów, w tym za pomocą środków komunikacji elektronicznej oraz połączeń głosowych, przy użyciu telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących,
- zgoda na otrzymywanie informacji o treści proponowanych zmian warunków umowy o świadczenie usług telekomunikacyjnych na adres e-mail,
- zgoda na udostępnianie faktur VAT w formie elektronicznej,
- sprzeciw wniesiony zgodnie z art. 32 ust. 1 pkt 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), wobec przetwarzania danych osobowych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 ww. ustawy, gdy administrator danych (tj. operator) zamierza je przetwarzać w celach marketingowych lub wobec przekazywania danych osobowych innemu administratorowi danych;

18) nieoddzwanianie lub niewysyłanie komunikatów na nieznane numery;

19) niepodawanie poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowej, nieznanemu rozmówcy lub w miejscach publicznych;

20) systematyczna aktualizacja przez abonenta/użytkownika systemu operacyjnego aparatu telefonicznego lub innego urządzenia elektronicznego umożliwiającego za pośrednictwem karty SIM korzystanie z usług świadczonych przez operatora;

21) stałe kontrolowanie wszystkich nowych instalacji na urządzeniu, a w przypadku powstania jakichkolwiek wątpliwości przerwanie jej;

22) nieprzechowywanie w pamięci wewnętrznej aparatu telefonicznego lub na karcie pamięci niezabezpieczonych (niezaszyfrowanych) poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowych;

23) wyłączanie przez abonenta/użytkownika łączności bezprzewodowej Wi-Fi, Bluetooth i NFC niezwłocznie po zakończeniu korzystania z tego typu połączeń;

24) stosowanie przez abonenta/użytkownika zasad bezpiecznego korzystania z aplikacji mobilnych, w tym:

- instalowanie lub aktualizacja aplikacji mobilnych tylko z zaufanych źródeł, najlepiej producenta danej aplikacji;
- zwracanie szczególnej uwagi na wymagania instalowanego programu w zakresie dostępu do poszczególnych funkcjonalności urządzenia podczas jego instalacji;
- dokładna analiza w trakcie instalacji lub aktualizacji aplikacji mobilnych, jaki mają one uprawnienia oraz do jakich usług lub danych abonenta/użytkownika mają one dostęp,
- systematyczna aktualizacja aplikacji mobilnych poprzez instalowanie poprawek i aktualizacji systemowych;

25) zabezpieczenie urządzenia, za pomocą którego korzysta się z hot-spotu przed nieuprawnionym dostępem z zewnątrz oraz używanie oprogramowania antywirusowego;

26) przestrzegania przepisów prawa kraju na terenie, w którym korzysta się z hot-spotów, a w szczególności niewykorzystywanie hot-spotów do:

- przesyłania i udostępniania treści, które są niezgodne z prawem lub są przedmiotem ochrony własności intelektualnej, której podmiotem nie jest abonent/użytkownik,
- przesyłania i udostępniania treści mogących naruszyć czyjekolwiek dobra osobiste,
- masowego rozsyłania niezamówionych przez odbiorców treści o charakterze reklamowym (tzw. spam),
- rozpowszechniania wirusów komputerowych i innych programów mogących uszkodzić komputery innych użytkowników Internetu,
- udostępniania dostępu do Internetu innym osobom ,w szczególności używania hot-spot do budowania stałych podsieci,
- permanentnego obciążania w znacznym stopniu pasma poprzez udostępnianie serwerów WWW, IRC, NNTP itp;

27) korzystanie przez abonenta/użytkownika z aplikacji lub/i usług umożliwiających zdalne zablokowanie aparatu telefonicznego lub zdalne usuwanie danych z aparatu telefonicznego;

28) systematyczne sprawdzanie przez abonenta/użytkownika danych i aplikacji zainstalowanych w aparacie telefonicznym, czy nie zawierają one szkodliwego kodu, w szczególności wirusów;

29) usunięcie przez abonenta/użytkownika z pamięci wewnętrznej aparatu telefonicznego lub z karty pamięci poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub karty kredytowej przed sprzedażą lub przekazaniem aparatu telefonicznego do serwisu, wyrzuceniem do śmieci lub utylizacją;

30) stosowanie przez abonenta/użytkownika zasad bezpiecznego korzystania z sieci Internet, w tym:

- zainstalowanie i uruchomienie w aparacie telefonicznym programów zabezpieczających, w szczególności aplikacji antywirusowej,
- regularna i częsta aktualizacja sygnatur oprogramowania antywirusowego,
- weryfikacja, że adres wpisany do przeglądarki internetowej jest poprawny,
- korzystanie z połączeń szyfrowanych z wykorzystaniem protokołu HTTPS, w szczególności w trakcie wykonywania zakupów w sklepach internetowych lub dostępu do usług bankowości elektronicznej,
- korzystanie z połączeń szyfrowanych przy korzystaniu z komunikatorów przy wymianie poufnych i prywatnych informacji,
- wybieranie wyłącznie sprawdzonych i wiarygodnych usługodawców przy korzystaniu z poczty elektronicznej,
- nieotwieranie wiadomości pocztowych pochodzących od nieznanych nadawców,
- nieodpowiadanie na wiadomości pocztowe, w których abonent/użytkownik jest proszony o podanie lub zweryfikowanie poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowych,
- nieklikanie na linki przesłane w wiadomościach pocztowych lub na stronach WWW, które zachęcają do zmiany hasła do konta/strony/serwisu internetowego,
- nieklikanie na podejrzane linki podawane w wiadomościach pocztowych lub na stronach WWW,
- nieotwieranie, nieuruchamianie i nieinstalowanie żadnych plików lub aplikacji nieznanego pochodzenia, pobranych z niezaufanych stron WWW lub otrzymanych pocztą elektroniczną,
- nierejestrowanie się i nieujawnianie bez wyraźnej potrzeby na portalach/serwisach społecznościowych (jak np. Facebook, Twitter), forach dyskusyjnych czy blogach swoich danych osobowych ze względu na ryzyko wykorzystania tych informacji przez osoby nieupoważnione. Korzystając z serwisów wymagających rejestracji i podania danych osobowych zawsze należy zwracać uwagę na wiarygodność tych serwisów. Jeśli już podawane są dane osobowe, to wyłącznie te, które związane są ze świadczoną usługą,
- niewyłączanie w trakcie korzystania z sieci Internet programów zabezpieczających, w szczególności aplikacji antywirusowej,
- systematyczne usuwanie plików tymczasowych przeglądarki internetowej,
- wyłączenie w przeglądarce internetowej funkcji zapamiętywania haseł w formularzach,
- nieprzechowywanie haseł do kont w serwisach internetowych w łatwo dostępnych miejscach,
- nieużywanie tego samego hasła do logowania na różnych kontach/stronach/serwisach internetowych,
- nieudostępnianie osobom trzecim identyfikatora i hasła do kont/stron/serwisów internetowych,

- unikanie stron internetowych zachęcających do obejrzenia bardzo atrakcyjnych treści lub ofert,
- zachowanie szczególnej ostrożności w przypadku korzystania z sieci Internet w miejscach publicznych lub za pomocą niezabezpieczonych sieci Wi-Fi. W takim przypadku należy ograniczyć do niezbędnego minimum wykonywanie zakupów w sklepach internetowych lub korzystanie z usług bankowości elektronicznej,
- unikanie kontrahentów, którzy jako jedyną formę płatności akceptują np. Union Money Transfer lub MoneyGram, gdyż nie ma praktycznie żadnej możliwości zidentyfikowania osoby odbierającej pieniądze. Należy wybierać tych, którzy współpracują z firmami obsługującymi płatności w sieci Internet, takimi jak np.: DotPay, eCard, PayPal, Przelewy24, PayU,
- czytanie oraz korzystanie z zasad zawartych w politykach bezpieczeństwa i politykach cookies dostawców usług internetowych;

31) ignorowanie fałszywych powiadomień antywirusowych, które polega na :

- pobieraniu programów antywirusowych bezpośrednio ze stron producentów lub z dużych sprawdzonych portali,
- unikaniu instalacji dodatkowych programów antywirusowych w przypadku jednoczesnego otrzymania komunikatu o infekcji systemu;

32) utworzenie i synchronizacja kopii zapasowej danych, w ramach której należy:

- ustalić harmonogram aktualizacji kopii zapasowej – np. co miesiąc lub częściej,
- wybrać formę zapisu danych (dysk zewnętrzny, serwer),
- dokonywać regularnych aktualizacji kopii zapasowej;

33) weryfikacja certyfikatów. Sprawdzanie ważności i rzetelności certyfikatów stron internetowych (szczególnie banków) pozwala uniknąć nieprzyjemnych zdarzeń i oszustw. Należy pamiętać, że fałszywe strony internetowe bardzo często nie posiadają żadnych certyfikatów. Dlatego przed zalogowaniem do banku internetowego należy kliknąć na symbol zamkniętej kłódki na pasku przeglądarki, a następnie zweryfikować:

- czy nazwa właściciela serwera jest poprawna,
- czy certyfikat został wydany przez znane centrum,
- czy przeglądarka nie zgłasza jakichkolwiek zastrzeżeń do certyfikatu (np. utrata ważności);

34) unikanie typosquattingu. Aby uniknąć zjawiska typosquattingu (oszustwo wykorzystujące typowe błędy literowe popełniane w trakcie wpisywania adresów internetowych) szczególnie ważna jest ostrożność przy wpisywaniu adresu internetowego. Każda pomyłka w nazwie popularnych stron internetowych (portali informacyjnych, banków, wyszukiwarek) może spowodować otwarcie niechcianych stron Internetowych, a w gorszym przypadku ściągnięcia z nich szkodliwego oprogramowania;

35) Bezpieczne korzystanie z publicznych hot-spotów. W czasie korzystania z hot-spota należy:

- unikać logowania do portali społecznościowych, do kont bankowych, do skrzynki mailowej,
- korzystać z szyfrowania SSL przy konieczności wykonania powyższych operacji,

- wyłączyć udostępnianie plików podczas korzystania z publicznego punktu dostępu bezprzewodowego (udostępnianie plików można wyłączyć w menu ustawień sieciowych systemu operacyjnego),
- ograniczyć ilość poufnych danych osobistych przechowywanych w komputerach i urządzeniach przenośnych lub zabezpieczyć odpowiednie pliki hasłem;

36) Bezpieczne korzystanie ze skrzynki głosowej:

- ustawienie kodu dostępu PIN do skrzynki głosowej,
- niestosowanie kodu krótszego niż 4 cyfry,
- niestosowanie kodu łatwego do odgadnięcia, np. „0000", „1111", „1234" itp.,
- zmiana kodu dostępu co pewien czas, np. raz na miesiąc,
- zachowanie w tajemnicy swojego kodu dostępu do skrzynki głosowej,
- jeżeli kod dostępu mógł zostać przez kogoś podejrzany lub odgadnięty, należy go natychmiast zmienić;

37) Bezpieczne korzystanie z wiadomości SMS i MMS:

- nieoddzwanianie, niewysyłanie wiadomości na nieznany numer, zwłaszcza jeśli zaczyna się od innego ciągu znaków niż „+48" lub „0048",
- zapamiętanie, że istnieją serwisy o podwyższonej opłacie, w których pobierana jest opłata za wiadomości odebrane,
- zapamiętanie, że opłata za wiadomości MMS uzależniona jest od jej wielkości, a w przypadku wiadomości SMS od ilości użytych znaków i ich kodowania (np. użycie alfabetu polskiego powoduje, że wiadomość zawiera ok. dwa razy więcej znaków niż jest to wpisane w wiadomości).

Opracowanie:
Urząd Komunikacji Elektronicznej, Departament Detalicznego Rynku Telekomunikacyjnego
Zapraszamy do:
Centrum Informacji Konsumenckiej - infolinia 801 900 853, www.cik.uke.gov.pl