

# Antypiracki przewodnik dla osób prywatnych



## Czy zagrożenia związane z piractwem dotyczą także Ciebie?

Konsekwencje prawne (cywilne i karne) piractwa, czyli naruszenia praw autorskich do utworów (w tym: muzyki, filmów, oprogramowania i gier komputerowych) dotyczą nie tylko firm i nie tylko osób uprawiających ten proceder w celach zarobkowych, ale każdego z nas. To znaczy, że każda osoba fizyczna może odczuć konsekwencje prawne, finansowe i inne z powodu korzystania w pracy lub w domu z pirackich plików lub ich udostępniania w sieci.

Użytkownicy małych osiedlowych sieci są narażeni na wizytę Policji tak samo, jak abonenci dużych dostawców usług internetowych. Nie ma też znaczenia czy firma jest duża czy mała, w małej miejscowości czy w dużym mieście. Każdy kto ma w domu czy w pracy dostęp do Internetu i prowadzi nielegalne działania w Internecie musi się liczyć z przeszukaniem Policji. Nie pomoże tłumaczenie o niewiedzy lub posiadaniu nielegalnego oprogramowania czy gier tylko na użytek prywatny. W obliczu obowiązującego prawa nie ma to znaczenia.

Dopuszcza się piractwa w Internecie między innymi każdy kto:

- bezprawnie ściąga program komputerowy lub grę komputerową;
- udostępnia w jakikolwiek sposób (rozpowszechnia mailem, na stronie WWW lub przez P2P) oprogramowanie i gry komputerowe a także muzykę i filmy;
- nabywa lub sprzedaje nielegalne płyty z oprogramowaniem, gramami komputerowymi, muzyką i filmami na aukcjach internetowych lub w na stronach WWW oferujących odpłatną dostawę pirackich kopii.

Do piractwa dochodzi także wtedy kiedy z legalnej (oryginalnej) płyty z programem lub grą robimy kopię na dodatkowym komputerze a nie zezwala na to licencja lub prawo – dotyczy to także sytuacji gdy pożyczamy znajomemu tę płytę, żeby sobie skopiował i zainstalował program czy grę na swoim komputerze.

Warto także pamiętać, że ściąganie plików muzycznych i filmów w ramach sieci P2P często oznacza również ich udostępnianie – to forma piractwa muzycznego i filmowego.

Poniżej informujemy dlaczego i jak ochronić się przed zagrożeniami i konsekwencjami piractwa w życiu prywatnym i w pracy.

## **Dlaczego piractwo może być niebezpieczne dla Ciebie?**

- Ryzyko odpowiedzialności karnej z tytułu piractwa, rozumianego jako naruszenie majątkowych praw autorskich, spoczywa na każdej osobie winnej jego popełnienia.
- Sankcje karne z tytułu naruszenia majątkowych praw autorskich sięgają nawet pięciu lat pozbawienia wolności.
- W ramach odpowiedzialności karnej sprawca musi się liczyć także z obowiązkiem naprawienia szkody oraz z przypadkiem rzeczy służących do popełnienia przestępstwa (np. komputera), nawet jeśli nie stanowią własności sprawcy.
- W ramach postępowań karnych prowadzonych przeciwko osobom dopuszczającym się naruszenia praw autorskich, Policja ściga osoby bezprawnie rozpowszechniające utwory bez względu na to w jaki sposób następuje publiczne udostępnienie: mailem, na stronie internetowej czy w ramach sieci P2P.
- W wypadku oprogramowania i gier komputerowych, a także w wypadku większości sieci P2P, w których obok ściągnięcia (pobrania) plików z muzyką i z filmami dochodzi także do ich rozpowszechniania – odpowiedzialność karna obejmuje także osoby ściągające (pobierające) z Internetu nielegalne pliki.
- Policja ściga nie tylko osoby sprzedające nielegalne płyty z muzyką, filmami, oprogramowaniem lub gramami komputerowymi, ale także nabywców takich płyt – nawet jeśli nabycie nielegalnej płyty jest nieumyślne. Nie przyniesie żadnego skutku tłumaczenie, że nie znaleźliśmy zawartości płyty albo nie wiedzieliśmy, że zawartość płyty jest nielegalna, jeśli z towarzyszących okoliczności powinniśmy i mogliśmy przypuszczać, że zawarte na płycie pliki z utworami są nielegalne (tzw. paserstwo nieumyślne).
- Policja ściga nie tylko osoby czy firmy sprzedające komputery z nielegalnym oprogramowaniem, ale także nabywców sprzętu z oprogramowaniem bez licencji.
- Policja dokonując przeszukania w firmie lub w domu nie działa na zasadzie „chylbił-trafił” – zwykle trafia pod konkretny adres na podstawie nr IP komputera. Pamiętaj, że w sieci nie jesteś anonimowy.
- Odpowiedzialność cywilna (majątkowa) jest niezależna od winy. W wypadku niezawinionego naruszenia majątkowych praw autorskich do utworów (w tym: muzyka, filmy, oprogramowanie i gry komputerowe), uprawniony (twórca lub producent) może domagać się zapłaty podwójnej wysokości stosownego wynagrodzenia (opłaty licencyjnej). W razie zawinionego naruszenia – potrójnej wysokości wynagrodzenia. W wypadku profesjonalnego oprogramowania specjalistycznego (np. do obróbki graficznej, projektowania architektonicznego czy do montażu video lub tworzenia animacji) mogą to być kwoty sięgające kilkudziesięciu tysięcy złotych.
- W zakresie odpowiedzialności cywilnej, sprawca musi się liczyć także z obowiązkiem wydania uzyskanych korzyści.

- Korzystanie z nielegalnych płyt czy nielegalnych plików pobranych z Internetu wiąże się jeszcze z innym poważnym ryzykiem, tj. zainfekowaniem komputera złośliwymi dodatkami, które potencjalnie mogą umożliwić osobie z zewnątrz (intruzowi):
1. dostęp do poufnych danych, w tym np. haseł dostępu do bankowości internetowej czy do informacji stanowiących tajemnicę przedsiębiorstwa;
  2. przejęcie kontroli nad naszym komputerem i wykorzystanie go jako tzw. komputer-zombie do ataku hackerskiego;
  3. kradzież tożsamości umożliwiającej podszywanie się przestępcy pod nas w ramach działalności przestępczej.

Warto wiedzieć, że – jak wynika z przeprowadzonych badań\* - że:

- tylko 49% płyt oferowanych na aukcjach internetowych jest legalna (oryginalna);
- aż 25% stron WWW oferujących aplikacje do łamania zabezpieczeń programów komputerowych (generatory kluczy, cracki) oraz pirackie kopie oprogramowania automatycznie usiłuje instalować w komputerze użytkownika niechciane – często bardzo niebezpieczne – dodatki;
- aż 59% aplikacji służących do łamania zabezpieczeń (generatory kluczy, cracki) przesyłanych przez sieci P2P zawiera takie złośliwe dodatki.

\* badania IDC „Ryzyko związane z pozyskiwaniem i korzystaniem z pirackiego oprogramowania”, 2006

### **Jak uchronić się przed piractwem?**

- Zachowaj szczególną ostrożność w Internecie i unikaj odwiedzania witryn oferujących darmowe pobranie plików lub za zbyt „atrakcyjną” (niską) opłatą, aby była to opłata za legalny produkt.
- Nie otwieraj załączników ani linków zawartych w „podejrzanej” poczcie elektronicznej od nieznanym (25% takich stron ma złośliwe dodatki instalujące się na komputerze bez wiedzy odbiorcy\*).
- Pod żadnym pozorem nie instaluj oprogramowania z „podejrzanym” źródłem, w tym z Internetu czy z płyty kupionej na targowisku lub na aukcji internetowej oferującej nabycie oprogramowania po niskiej cenie;
- Zachowaj szczególną ostrożność na aukcjach internetowych. Zrezygnuj z zakupu oprogramowania lub gry, jeśli cena jest zbyt niska, aby była ceną za legalny produkt.
- Jeśli zdecydujesz się pobrać z Internetu darmowy program, uznając że jest to program legalny (np. freeware, wersja trialowa), zwróć uwagę na treść licencji i warunki korzystania z takiego oprogramowania. Może okazać się, że z programu można korzystać jedynie w celach prywatnych (niekomercyjnych) a nie w ramach działalności zawodowej lub gospodarczej.
- Jeżeli zorientujesz się, że w komputerze masz zainstalowany program do pobierania i udostępniania plików w sieci P2P upewnij się, że pliki, które pobierasz lub udostępniasz mogą

być przedmiotem takiego obrotu. Jeżeli nie, usuń takie pliki, a być może również aplikację P2P. Możesz w tym celu skorzystać z bezpłatnego programu Digital File Check, który jest prostym narzędziem służącym do odnalezienia i odinstalowania lub zablokowania programów P2P, wykorzystywanych do nielegalnego udostępniania plików multimedialnych chronionych prawem ([http://www.ifpi.org/content/section\\_resources/digital-file-check.html](http://www.ifpi.org/content/section_resources/digital-file-check.html)).

- Rozsądnie kupuj komputer. Niektórzy sprzedawcy w celu uatrakcyjnienia zakupu sprzedają komputer z zainstalowanym nielegalnym oprogramowaniem. Zawsze oczekuj legalnych wersji z dokumentacją i oryginalnym nośnikami. Żądaj wyszczególnienia oprogramowania na fakturze.
- Ponadto w celu zmniejszenia ryzyka zagrożenia bezpieczeństwa swojego komputera i zawartych w nim danych:
  1. Regularnie dokonuj aktualizacji oprogramowania, w tym systemu operacyjnego.
  2. Zainstaluj firewall i oprogramowanie antywirusowe.
  3. Regularnie zmieniaj hasła dostępu do komputera, poczty i bankowości internetowej – np. raz w miesiącu.

\* badania IDC „Ryzyko związane z pozyskiwaniem i korzystaniem z pirackiego oprogramowania”, 2006