Zagrożenia związane z umieszczaniem i pobieranie treści z internetu

Witam! Ta prezentacja służy temu, aby uświadomić co tak naprawdę może się stać w internecie

Pobieranie filmów, muzyki, treści i zdjęć

Prawa autorskie do utworów intelektualnych i ich ochrona prawa

Prawo autorskie (ang. *copyright*, symbol: ©) – pojęcie prawnicze oznaczające ogół praw przysługujących autorowi utworu albo zespół norm prawnych wchodzących w skład prawa własności intelektualnej, upoważniających autora do decydowania o użytkowaniu dzieła i czerpaniu z niego korzyści finansowej.

Pamiętaj: Wykorzystując materiały pobrane z internetu podaj źródło !!!

Źródło www.Wikipedia.org

Kiedy pobieranie plików jest nielegalne

Z prawnego punktu widzenia ściąganie muzyki lub filmów itd. jest legalne do momentu, gdy z plików tych jedynie korzystamy, nie popełniamy przestępstwa, nawet gdyby znalazły się w sieci nielegalnie. Gdybyśmy jednak chcieli udostępnić je innym (albo poprzez umieszczenie w serwisie internetowym, albo też z własnego dysku za pomocą programów typu peer to peer), narażamy się na zarzut rozpowszechniania bez zgody uprawnionego (twórcy lub wydawcy).

Z etycznego punktu widzenia powinniśmy rozpatrywać każde pobranie utworu bez uzyskania zgody jego twórcy lub prawowitego właściciela jako formę kradzieży!

Źródło www.Prawo.rp.pl

Konsekwencje prawne piractwa

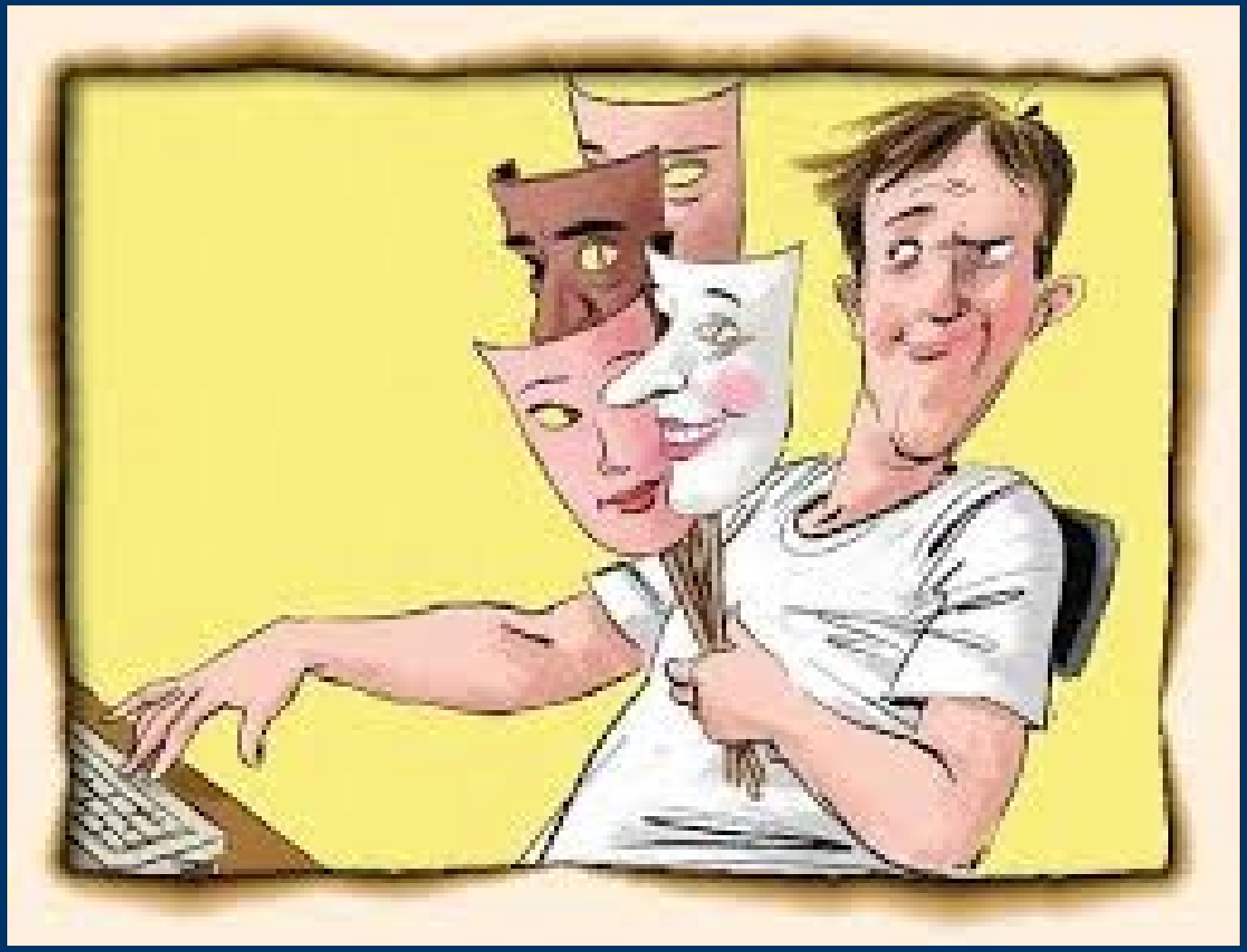
Co grozi za posiadanie nielegalnych kopii? Jej pobranie jest traktowane jako kradzież. Na podstawie art. 278 kodeksu karnego (Dz.U. z 1997 r. nr 88, poz. 553 z późn. zm.) uzyskanie bez zgody osoby uprawnionej cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej podlega karze od trzech miesięcy do nawet pięciu lat więzienia.
Także przepisy dotyczące paserstwa stosuje się odpowiednio do programów komputerowych. Mianowicie już za samo przyjęcie programu, o którym można przypuszczać, że jest piracki, grożą grzywna, ograniczenie wolności i dwa lata więzienia.

Podsumowując... Jeśli nie jesteśmy pewni pochodzenia utworu, gry czy zdjęcia nie ściągajmy go bo możemy popaść w konflikt z prawem i narazić na konsekwencje nie tylko samych siebie ale także naszych opiekunów !!!

Jak zabezpieczyć swoje utwory przed nielegalnym rozpowszechnianiem

- **Aby zabezpieczyć swoje utwory (które sami zrobiliśmy) należy oznaczyć je znakiem © „Copyright”**

Umieszczanie w sieci danych swoich i osób trzecich



Co to są dane osobowe

Dane osobowe – termin prawny, który w prawie polskim został zdefiniowany w ustawie z dnia 29 sierpnia 1997 roku o ochronie *danych osobowych*. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
Szczególną kategorią *danych osobowych* są dane wrażliwe, których przetwarzanie jest poddane szczególnemu trybowi. Istnieje generalny zakaz przetwarzania danych wrażliwych z wyjątkiem sytuacji, gdy zezwalają na to przepisy prawa.
Nad kontrolą i ochroną prawną czuwa Generalny Inspektor Ochrony Danych Osobowych.

Źródło www.Wikipedia.org

Ochrona danych osobowych w prawie i w praktyce

Ochrona danych osobowych – regulacje prawne dotyczące tworzenia i posługiwania się zbiorami danych osobowych, a także pojedynczymi danymi, mające na celu administracyjno-prawną ochronę prawa do prywatności.

W praktyce dane osobowe mogą być gromadzone i przetwarzane tylko kiedy zostaną spełnione następujące warunki :

- Istnieje uzasadniony powód przetwarzania (np.. relacje biznesowe)
- Osoba udzieli dobrowolnej zgody na przetwarzanie swoich danych podmiotowi przetwarzającemu
- Przetwarzane będą tylko dane niezbędne do wypełnienia celu przetwarzania i tylko w takim zakresie na jaki została udzielona zgoda
- Osoba będzie mieć pełny wgląd w dane i możliwość ich poprawy lub zmiany

Zagrożenia związane z umieszczaniem danych osobowych w sieci

Systemy teleinformatyczne obecnie wspomagają działania niemal we wszystkich dziedzinach życia. Są wykorzystywane w każdej nowoczesnej instytucji, zarówno dużym przedsiębiorstwie, jak i w małej firmie, urzędzie, szkole czy szpitalu. Decydują obecnie o poziomie rozwoju gospodarki państwa, jakości działania jego struktury organizacyjno-administracyjnej, szeroko rozumianym bezpieczeństwie, jak również poziomie życia obywateli. Rozwój sieci telekomunikacyjnych i usług sieciowych, który nastąpił w ostatnich latach, spowodował, że zarówno duże organizacje, jak i małe podmioty, w tym osoby fizyczne, w coraz większym stopniu są uzależnione od sprawności i bezpieczeństwa użytkowanych systemów teleinformatycznych. Są one pomocne do wyszukiwania różnorodnych informacji, robienia zakupów czy przekazywania bankowi dyspozycji w zakresie wykonania określonych operacji.

Zagrożenia związane z umieszczaniem danych osobowych w sieci cd.

Jak wynika z wielu badań, z usług oferowanych przez systemy teleinformatyczne korzystałoby jeszcze więcej osób, gdyby nie obawa przed cyber przestępczością, której celem jest pozyskanie poufnych informacji, kradzież środków pieniężnych z banków, dorobku intelektualnego lub rozprowadzanie prawnie zakazanych informacji i materiałów.
Obawy te są w pełni uzasadnione. Nasilenie działań przestępczych skierowanych na kradzież i nielegalne wykorzystanie informacji w sieciach telekomunikacyjnych systematycznie wzrasta, tak jak wzrasta liczba dostępnych usług i wielkość zgromadzonych w sieci zasobów informacyjnych.
Najpoważniejsze z zagrożeń to ataki hakerów – programistów posiadających szeroką wiedzę informatyczną, którzy wykorzystują luki w oprogramowaniu i bezpieczeństwie systemów informatycznych, oraz ataki przestępców komputerowych, zwanych również crakerami, którzy do celów przestępczych wykorzystują wiedzę i/lub procedury opublikowane przez hakerów oraz nieświadomość i naiwność użytkowników

Portale społecznościowe- jeszcze zabawa czy już równoległy świat?

Źródło : Google grafika

Dlaczego używanie portali może być niebezpieczne

Strony internetowe, takie jak portale społecznościowe , na których większość z nas posiada własne konto to całkiem sympatyczna możliwość kontaktowania się z dawnymi znajomymi, dająca szansę na dowiedzenie się, co słychać u tych, którzy wyprowadzili się z naszego miasta, których nie widujemy na co dzień. Patrząc z innej perspektywy, serwisy te stają się trochę niebezpieczne. Nie dość, że na portalach często udostępniamy pełny pakiet informacji o sobie, swoim życiu, miejscu zamieszkania, to jeszcze wywlekamy najintymniejsze szczegóły naszego życia. Opisujemy dokładnie, w jakim stanie byliśmy po sobotniej imprezie, gdzie zrobiliśmy zakupy oraz co zjedliśmy na śniadanie.

Trudno nie zauważyć, że powoli przesuwa się **granica prywatności** obowiązująca na portalach społecznościowych. Udostępniamy znajomym z portalu intymne przemyślenia, wywlekamy na „światło dzienne" swoje frustracje, obawy oraz pragnienia. Już nie siedzimy z przyjacielem przy kubku dobrej kawy, opowiadając mu po cichu jak bardzo samotni się czujemy, a wrzucamy na „tablicę" post, mówiąc o swoim nieszczęściu nie jednej, bardzo bliskiej nam osobie, a tym, których mamy wśród internetowych znajomych (lub nawet wszystkim – gdy nie zablokujemy widoczności naszego profilu przed obcymi).

Źródło www.Giodo.org

Czego nie powinniśmy umieszczać na portalach społecznościowych ?

- Na portale społecznościowe nie powinniśmy wrzucać :
  - danych np. swojego imienia i nazwiska , zdjęcia dowodu osobistego czy numeru karty kredytowej
  - daty urodzenia
  - Zdjęć, które mogą służyć innym do identyfikacji naszego miejsca zamieszkania, nawyków i zachowań czy statusu materialnego
  - Treści obrażających inne osoby
  - Itd..
-

Kto jest odpowiedzialny za treści umieszczone na portalach

Prowadzenie strony internetowej przez przedsiębiorcę jest związane z ponoszeniem odpowiedzialności za treści zamieszczane w takim serwisie. Nie w każdym jednak przypadku administrator serwisu internetowego będzie odpowiadał za treści w nim publikowane. Przepisy prawa polskiego – art. 14 ustawy o świadczeniu usług drogą elektroniczną – wyłączają odpowiedzialność za dane przechowywane w zasobach systemu teleinformatycznego w przypadku, gdy administrator strony nie wie o bezprawnym charakterze danych lub związanej z nimi działalności. Jednak gdyby administrator otrzymał urzędowe zawiadomienie lub uzyskał wiarygodną wiadomość o bezprawnym charakterze danych lub związanej z nimi działalności, powinien niezwłocznie uniemożliwić dostęp do tych danych albo wykazać gotowość do usunięcia kontrowersyjnych treści.

Podsumowując: jeśli umieszczamy na portalu jakiekolwiek dane , które są nielegalne lub w jakikolwiek sposób niezgodne z prawem czy obowiązującymi regulaminami portalu, na którym zostały umieszczone narażamy się na KONSEKWENCJE !!!

Kto może mieć dostęp do naszych danych i jak je chronić

Zgodnie z treścią art. 101 Konwencji Wykonawczej do Układu z Schengen, dostęp do danych wprowadzonych do Systemu Informacyjnego Schengen oraz prawo ich bezpośredniego przeglądania zastrzeżone są wyłącznie dla organów odpowiedzialnych za kontrole graniczne oraz inne kontrole policyjne i celne prowadzone w ramach danego kraju, jak również koordynację takich kontroli. Wskazać jednak należy, że prawo bezpośredniego dostępu do danych przetwarzanych w Systemie Informacyjnym Schengen przyznane zostało również krajowym organom sądowym, w tym odpowiedzialnym za oskarżanie z postępowaniu karnym oraz przesłuchania na etapie przed sporządzeniem aktu oskarżenia, w zakresie dotyczącym wykonywania ich zadań.

W praktyce dostęp d o naszych danych mają często ludzie, którzy dostępu mieć nie powinni !!! Zanim umieścimy w internecie jakiekolwiek dane pomyślmy czy chcielibyśmy aby stały się publicznie dostępne.

PAMIĘTAJ: W momencie kiedy coś trafi do internetu zostanie tam już prawdopodobnie na zawsze i nigdy nie wiesz kto to kiedyś zobaczy !!!

Najważniejsze zasady naszej ochrony w internecie

- Anonimowość
- Ograniczone zaufanie
- Unikanie niebezpieczeństw
- Aktualne oprogramowanie antywirusowe
- ROZSĄDEK!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

- DZIĘKUJE ZA UWAGĘ!!!!!!!