Cyfrowy ślad

”

SZKOLNA GAZETKA ZZSP
IM. JANA PAWŁA II

Chrońmy swoje dane

W dzisiejszym świecie nikt z nas nie wyobraża sobie życia bez Internetu. Sprawdzanie poczty e-mail, robienie zakupów on-line, spotykanie się ze znajomymi na różnego rodzaju portalach społecznościowych czy chociażby nauka przez Internet stały się codziennością.
Ale czy przebywając w rzeczywistości internetowej jesteśmy tak do końca bezpieczni? Wielu z nas nie zdaje sobie nawet sprawy z niebezpieczeństw, które czyhają na nas w sieci.

Jednym z nich jest niewątpliwie kradzież danych osobowych i utrata tożsamości. Poprzez kradzież danych personalnych rozumiemy uzyskanie przez osobę niepowołaną pewnych informacji tj.: imię i nazwisko, data urodzenia, adres zamieszkania, numer telefonu, PESEL, numer konta bankowego, numer karty kredytowej, NIP, loginy i hasła. Informacje te mogą zostać potem wykorzystane przez oszusta w celu podszycia się pod nas (tzw. Kradzież tożsamości). Kradzież danych osobowych i utrata tożsamości mogą skutkować przede wszystkim stratami finansowymi. Oszuści będą mogli na nasze konto zaciągać kredyty, wynajmować mieszkania, podpisywać umowy z sieciami komórkowymi, robić zakupy, podrabiać dowody osobiste i prawo jazdy oraz karty kredytowe. Ponadto umożliwi im to obraźliwie wypowiadanie się w naszym imieniu na różnego rodzaju forach internetowych i portalach społecznościowych co może skutkować sankcjami karnymi jak np. pozwaniem do sądu ludzi nie mających z tym nic wspólnego.

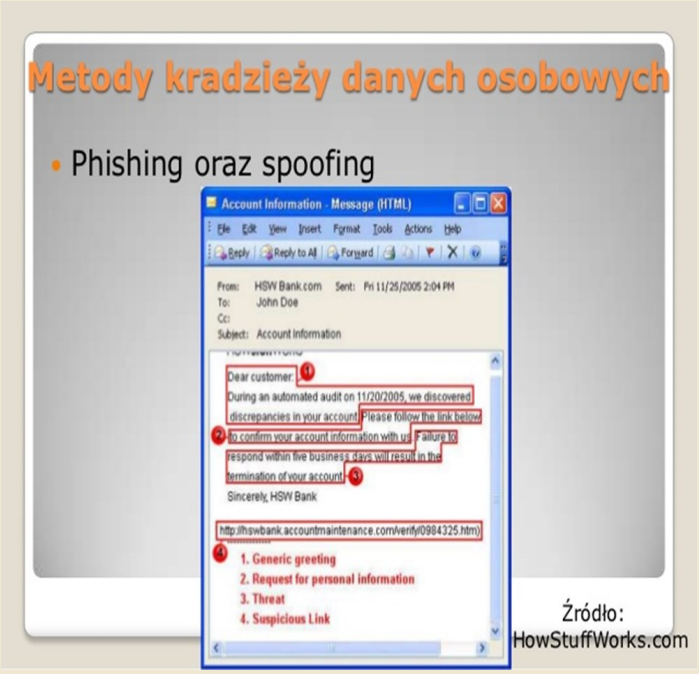
Według badań przeprowadzonych w 2012 r. w 9 krajach Europy (w tym w Polsce) okazuje się, że aż 17% dorosłych Polaków zostało okradzionych z tożsamości, a 46% z tej grupy ze środków znajdujących się na rachunkach bankowych.

JAK WYKRAŚĆ DANE?

Jedną z metod używanych do kradzieży danych personalnych jest *phishing*. Pojęcie to możemy zdefiniować jako próby wyłudzenia od kogoś poufnych danych, np. szczegółów karty kredytowej czy rachunku bankowego. Termin ten powstał w latach 90 w środowisku hakerów, którzy próbowali wykraść hasła do kont w serwisie AOL. Podawali się za pracowników tej firmy i wysyłali e-maile z prośbą o podanie hasła w celu rzekomej weryfikacji konta.
Phisher działa poprzez wysyłanie dużej ilości e-maili zamieszczając w nich prośbę do odwiedzenia przez użytkownika i zalogowania się przez niego na stronie do złudzenia przypominającej prawdziwą witrynę (np. banku czy platformy aukcyjnej). W treści maila phisher najczęściej umieszcza prośbę o **uzupełnienie danych osobowych ofiary**
i ostrzeżenie, że jeśli tego nie zrobi to jej konto zostanie zawieszone.

Cyfrowy ślad

Phishing jest bardzo często utożsamiany ze *spoofingiem* czyli podawaniem się za kogoś innego lub maskowaniem rzeczywistego nadawcy korespondencji w celu zdobycia czyjegoś zaufania i wyłudzenia danych personalnych.
Innym sposobem pozyskiwania informacji są *keyloggery* umożliwiające sprawdzenie, jakie klawisze klawiatury zostały naciśnięte przez użytkownika podczas logowania, bądź umieszczanie niebezpiecznych kodów w plikach graficznych. Jednym z takich urządzeń jest *SpyLogger* za pomocą, którego możemy kontrolować co robią np. nasze dzieci i bliscy w Internecie.



Dmuchaj na zimne:

1) Używaj programów antywirusowych
2) Stosuj zaporę sieciową firewall
3) Korzystaj ze skanerów on-line
4) Nie zamieszczaj w sieci zbyt wielu informacji na temat swojej osoby ani zdjęć świadczących o Twoim stanie majątkowym
5) Sceptycznie traktuj korespondencję e-mail od nieznanych nadawców
6) Układaj mocne hasła, w miarę możliwości co jakiś czas je zmieniając

Dmuchaj na zimne:

7) Podczas logowania się do witryn, np. banków sprawdzaj czy w pasku adresu widnieje znak zamkniętej kłódki
8) Co pewien czas sprawdzaj wszystkie operacje dokonywane na koncie
9) Pamiętaj, aby zawsze wylogowywać się z sesji
10) W miarę możliwości nie gromadź żadnych ważnych danych na podpiętym do sieci komputerze
11) Nie udostępniaj swojego komputera nieuprawnionym użytkownikom

Posiadając cudze dane osobowe można narazić kogoś na:

Straty finansowe	Straty moralne
zaciągnąć kredyt na nazwisko ofiary	obraźliwie wypowiadać się w imieniu ofiary na forach internetowych czy też portalach społecznościowych. Może to doprowadzić do ukarania poszkodowanej osoby sankcjami karnymi.
wynająć mieszkanie pod jej nazwiskiem	
podpisać umowę z różnorodnymi firmami	
dokonać zakupów w sklepach Internetowych	
podrobić dokumenty typu: dowód osobisty, prawo jazdy czy karty kredytowe	

17% dorosłych Polaków padło ofiarą kradzieży danych osobowych

w tym

46% z nich w wyniku kradzieży straciło środki z rachunku bankowego

http://www.militaryteenonline.com/page/warning-identity-thieves

Nieskradzione.pl

Jak informuje Policja, skala kradzieży tożsamości – czyli posiadania przez niepowołane osoby naszych danych osobowych – rośnie w zastraszającym tempie. Już w 2014 roku Policja stwierdziła ponad 14 tysięcy przypadków posługiwania się dokumentem innej osoby oraz ponad 30 tysięcy przestępstw związanych z podrabianiem dokumentów. Oszustwa dokonywane dzięki skradzionej tożsamości przybierają najróżniejsze formy.

Kilka miesięcy po fakcie możemy np. dowiedzieć się, że ktoś wynajął mieszkanie na nasze skradzione dane, wyrobił sobie kartę kredytową, sprzedaje fikcyjne przedmioty na portalach aukcyjnych lub wypożyczył auto i już go nie oddał. Sytuacja przyjmuje wyjątkowo nieprzyjemny obrót, kiedy do drzwi puka komornik albo listonosz z listem poleconym wzywającym do zapłaty zadłużenia, którego nie zaciągnęliśmy. Ale istnieją scenariusze znacznie bardziej ponure – w pewnych sytuacjach dochodzi nawet do aresztowań za przestępstwa, które ktoś popełnił na nasze konto.

W odpowiedzi na rosnącą skalę zagrożeń, Biuro Informacji Kredytowej wraz Komendą Główną Policji rozpoczynają ogólnopolską akcję edukacyjną – Nieskradzione.pl. Celem akcji jest uświadomienie wszystkim Polakom, że wystarczy przestrzegać kilku prostych zasad, aby uniknąć bardzo nieprzyjemnych konsekwencji kradzieży tożsamości. Przede wszystkim pamiętajmy, aby nie udostępniać danych osobowych niepowołanym osobom i starannie niszczyć wszystkie dokumenty, na których te dane widnieją.

Nie zgadzajmy się również na spisywanie danych z naszego dowodu oraz zostawianie dokumentu w tzw. depozycie – np. wypożyczając sprzęt sportowy. Zabezpieczmy się też na wypadek kradzieży czy zgubienia dokumentu – wystarczy założyć on line bezpłatne konto w BIK, a w sytuacji utraty dokumentu jednym kliknięciem zgłosimy dowód do systemu DZ prowadzonego przez Związek Banków Polskich. W kilka minut dowód zostanie wyłączony z obiegu, a informacja dotrze do wszystkich banków w Polsce, Poczty oraz operatorów telefonii komórkowej. W ten sposób nikt nie będzie mógł już posługiwać się naszą tożsamością. Więcej informacji oraz porad m.in. przedstawicieli Komendy Głównej Policji na nieskradzione.pl.

Jak wynika z danych Policji, w 2014 roku przestępcy posługujący się skradzioną tożsamością próbowali wyłudzić kredyty na łączną kwotę 400 milionów zł. Spłata cudzego kredytu to najczęstszy problem ofiar cyberprzestępców. Jak zatem chronić się przed kradzieżą danych osobowych?
Wystarczy, że złodziej uzyska dane z naszego dowodu, a będzie mógł zaciągnąć nawet sporą pożyczkę w banku, przez Internet lub w firmie udzielającej chwilówek. Niektórzy przestępcy zmieniają adres do korespondencji więc o zadłużeniu możemy dowiedzieć się dopiero gdy otrzymamy wezwanie do zapłaty lub telefon z firmy windykacyjnej. Jak zatem chronić się przed kradzieżą danych osobowych?

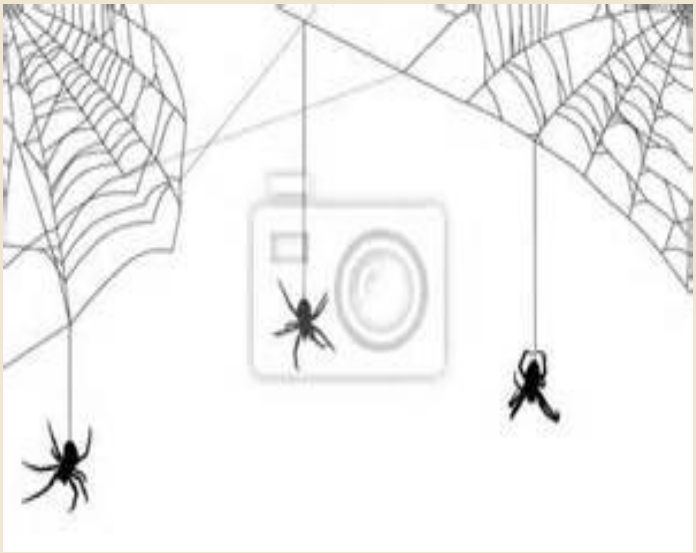
Po pierwsze – nie zostawiajmy naszych dokumentów w rękach osób niepowołanych, np. w zastaw, gdy chcemy wypożyczyć sprzęt sportowy. Żadna instytucja nie może żądać od nas zostawienia dowodu osobistego i jest to zakaz usankcjonowany prawnie.

Po drugie – nie podawajmy naszych danych osobowych nieznajomym osobom w trakcie rozmów telefonicznych.

Po trzecie – nie otwierajmy e-maili podejrzanych lub nieznanego pochodzenia. Prowadzą one do fałszywych stron czy platform aukcyjnych, które zawierają wezwanie do pilnego uzupełnienia danych osobowych, pod pretekstem zawieszenia konta.

I po czwarte - zabezpieczmy się na wypadek kradzieży czy zgubienia dokumentu. Wystarczy założyć online bezpłatne konto w BIK, a w sytuacji utraty dokumentu jednym kliknięciem zgłosimy dowód do systemu DZ prowadzonego przez Związek Banków Polskich. W kilka minut dowód zostanie wyłączony z obiegu, a informacja dotrze do wszystkich banków w Polsce, poczty oraz operatorów telefonii komórkowej i nikt nie będzie mógł już posłużyć się naszą tożsamością.

Natomiast jeśli dopiero po jakimś czasie zorientujemy się, że mogliśmy paść ofiarą kradzieży tożsamości – aktywujmy alerty BIK chroniące przed wyłudzeniem kredytu. BIK wyśle powiadomienie na telefon komórkowy lub e-mail za każdym razem, gdy pojawi się zapytanie z banku lub SKOK-u o naszą historię kredytową. Jeśli nie składaliśmy żadnych wniosków kredytowych, nic nie kupujemy na raty ani nie poręczaliśmy kredytu, to pojawienie się alertu może oznaczać, że ktoś zgłosił się do banku i próbuje wziąć kredyt na nasze nazwisko.



Zalety i wady portali społecznościowych

Serwisy społecznościowe stały się bardzo popularne w ciągu ostatnich lat. Korzysta z nich mnóstwo osób mających dostęp do Internetu, niezależnie od wieku, wykształcenia, płci czy koloru skóry. Pozwalają odświeżyć stare znajomości, nawiązać nowe, podzielić się z innymi ludźmi swoimi zainteresowaniami oraz znaleźć ludzi podobnych do nas. Niewątpliwie mają swoje dobre strony ale i niosą ze sobą pewne zagrożenia. O wadach i zaletach serwisów społecznościowych będzie traktował ten wpis.

Zalety

Serwisy społecznościowe umożliwiają użytkownikom w łatwy sposób utrzymać ze sobą kontakt niezależnie od dzielącej ich odległości. Oczywiście można utrzymywać kontakt za pomocą standardowych sposobów jak listy, telefony czy e-mail, jednakże serwisy społecznościowe przez swoją dostępność, łatwość w użyciu i bezpłatność są atrakcyjnym sposobem komunikacji dla ludzi żyjących szybko, korzystających często z urządzeń z dostępem do Internetu. Dzięki serwisom społecznościowym ułatwione jest odnowienie kontaktów z dawno niewidzianymi znajomymi oraz nawiązywanie nowych.

Serwisy społecznościowe wykorzystać można także do uzyskiwania natychmiastowej opinii na prawie każdy temat albo do zadawania pytań i otrzymywania na nie szybkich odpowiedzi. Użytkownicy mogą zakładać ankiety na dowolny temat, w których inni mogą wziąć udział.

Ilu jest ludzi, to tyle może być przekonań czy poglądów na daną sprawę. Ludzie korzystający z serwisów społecznościowych wystawieni są na kontakt z różnorodnymi punktami widzenia. Ta różnorodność pomóc może w byciu bardziej tolerancyjnym na przekonania innych ludzi i w rozpatrywaniu problemów pod różnymi kątami.

Wiele firm dzięki posiadanym profilom na portalach społecznościowych promuje swoją markę. Firmy mogą informować o aktualnych ofertach i promocjach. Użytkownikom umożliwia się identyfikowanie z daną marką. Firmy korzystają z serwisów społecznościowych aby zyskać na wiarygodności, polepszyć relacje z pracownikami, zbudować forum komunikacyjne z klientami i w większości przypadków zwiększyć sprzedaż.

Wady

Kradzież czyjejś tożsamości jest łatwiejsza niż można by sobie to wyobrażać. Z kradzieżą tożsamości mamy do czynienia wtedy gdy osoba nieuprawniona wejdzie w posiadanie czyichś danych osobowych i wykorzysta je podszywając się pod daną osobę, najczęściej szkodząc. Dzięki serwisom społecznościowym kradzież tożsamości staje się łatwiejsza. Ludzie nie panują nad informacjami, którymi dzielą się przez Internet i nie zdają sobie sprawy, że Google niczego nie zapomina. W sieci można znaleźć imiona i nazwiska, daty urodzin, dane członków rodziny, historię zatrudnienia i edukacji a czasem nawet więcej informacji na temat wielu osób. Jakie mogą być konsekwencje kradzieży tożsamości? Osoba posiadająca dostęp do czyichś danych może założyć fałszywy profil tej osoby na jednym z wielu serwisów społecznościowych i dzięki niemu publikować obraźliwe treści w imieniu osoby poszkodowanej. Zaciągane mogą być też zobowiązania finansowe (np. zakupy, pożyczki) w imieniu osoby, której dane osobowe zostały zdobyte. Istnieją także strony w Internecie, które wyglądają dokładnie jak popularne serwisy społecznościowe. Celem ich istnienia jest wykradzenie danych używanych do uwierzytelniania się w serwisie. Gdy już ktoś zdobędzie czyjeś hasło może go użyć do zlikwidowania profilu tej osoby, bądź do wysyłania z niego wiadomości zawierających spam lub wirusy.

Kolejną wadą serwisów społecznościowych jest to, że każdą informację zamieszczoną przez użytkowników można wykorzystać przeciwko nim. Wielu ludzi zamieszcza na swoich profilach zdjęcia z zakrapianych imprez, na których przykładowo jeden z uczestników usnął a inny pomalował mu twarz mazakiem. Są osoby, które w swoich profilach jawnie przyznają się do łamania prawa, przykładowo do przekraczania prędkości prowadząc samochód czy do palenia marihuany. Osoby przeprowadzające rekrutację kandydatów do pracy mogą wyszukać na serwisach społecznościowych niewygodne informacje na temat kandydata, które mogą zadecydować o przyjęciu bądź odrzuceniu kandydata. Także korzystanie z serwisów społecznościowych w czasie pracy, które jest łatwe do wykrycia, czy publikowanie treści źle widzianych przez pracodawcę, może kosztować utratą pracy.

Co w przypadku informowania znajomych o aktualnym miejscu przebywania lub planowanych wycieczkach? „Jutro wieczorem jedziemy z całą rodziną w góry". Czy opublikowanie takiej informacji może przynieść jakąś szkodę? Na pierwszy rzut oka wszystko jest w porządku. Jednakże w połączeniu z łatwym do znalezienia w sieci adresem zamieszkania jest to informacja dla złodzieja, kiedy może opróżnić czyjś dom.

Kolejnym problemem są dzieci. Dzieci nie powinny korzystać z Internetu bez pewnej formy nadzoru ze strony rodziców. Rodzice powinni monitorować jakie informacje zamieszcza dziecko na swoim profilu na portalu społecznościowym i czy nie zamieszcza ich za dużo, np. swojego adresu domowego lub numeru telefonu. Dzieci mogą nie być świadome tego, że osoby z którymi rozmawiają online mogą kłamać na temat tego kim są i mogą je skrzywdzić. Osoby takie mogą wyglądać na przyjaciół i powoli zdobywać informacje na temat dziecka. Profile takich osób wyglądają jak profile innych dzieci włączając fałszywe zdjęcia znalezione gdzieś w Internecie.

Ostatnią z wymienianych wad jest konsumpcja czasu przez korzystanie z serwisów społecznościowych, które tego czasu potrafią pochłaniać mnóstwo. Czasu mamy zawsze tyle samo warto więc rozważnie korzystać z serwisów społecznościowych aby nie stracić go zbyt wiele.

Minimalizacja zagrożenia

Dużo zostało napisane o zagrożeniach ze strony serwisów społecznościowych. Jak się przed nimi bronić?

Warto ocenić zawartość swojego profilu, zastanowić się nad jak się czujemy z tym co oglądają na naszym profilu nasi pracownicy czy pracodawca, rodzice albo dziadkowie.

Nie zamieszczać prywatnych informacji takich jak numery telefonów, adres domowy, rozkład zajęć w szkole, itp. Nie publikować niczego, co może być zawstydzające przykładowo na rozmowie kwalifikacyjnej.

Kolejnym krokiem jest dostosowanie ustawień prywatności w serwisie społecznościowym aby nasze prywatne dane nie były widoczne publicznie.

Jak chronić swoje dane?

W województwie łódzkim w 2014 roku stwierdzono 1527 przypadków sfałszowania dokumentów, w 2015 - 1698. Nadal zdarzały się sytuacje posługiwania się dokumentem innej osoby co także stanowi przestępstwo. W 2014 roku na terenie woj. łódzkiego było 1455 takich sytuacji, natomiast w 2015 - 1202. Dane pozyskane z naszego dowodu osobistego przestępcy wykorzystują np. do zaciągnięcia kredytu, zakupów na raty, czy popełnienia na nasze konto czynu zabronionego. Niestety nie wszyscy zdają sobie sprawę z negatywnych konsekwencji braku dbałości o zabezpieczenie swych dokumentów, a akcja Nieskradzione.pl ma tą sytuację zmienić.
Wystarczy bowiem przestrzegać kilku prostych zasad, aby uniknąć bardzo nieprzyjemnych konsekwencji kradzieży tożsamości. "Kradzież danych mi nie grozi, zawsze pilnuję swoich dokumentów" - tak myśli niestety duża grupa osób. Jesteś wśród nich? Jeśli tak, to musisz wiedzieć, że do kradzieży tożsamości złodzieje nie zawsze potrzebują Twoich dokumentów - dowodu, paszportu czy prawa jazdy. Wystarczą im dane, jakie sam w chwili nieuwagi niefrasobliwie dostarczysz.

Jak zatem ochronić się przed kradzieżą danych osobowych?

1. Nie podawaj swoich danych w trakcie rozmów telefonicznych nieznajomym osobom

Czym są dane osobowe? Takie dane to m.in. imię, nazwisko, data urodzenia, adres, numer konta bankowego, informacje o wykształceniu, doświadczeniu zawodowym, numer telefonu, adres e-mail. Obecnie, w niektórych sytuacjach, jako dane osobowe traktowane są również pliki cookies, numer IMEI, nick, login itp.

2. Bardzo dokładnie niszcz stare dokumenty i korespondencję, których chcesz się pozbyć - to fantastyczne źródło wiedzy na Twój temat.

I wbrew temu, co możesz myśleć, nie ma pewności, że kiedy trafią do śmieci, nikt ich nie przeczyta. A kiedy trafią w ręce osób niepowołanych, możesz w dość krótkim czasie odczuć to dość boleśnie, poprzez konieczność spłacania kredytu wyłudzonego na Twoje nazwisko.Choć tak naprawdę konsekwencji kradzieży danych może być więcej.

3. Nie zostawiaj swoich dokumentów w rękach osób niepowołanych

Np. nie udostępniaj dowodu osobistego w zastaw, gdy chcesz wypożyczyć kajak lub rower. Nigdy nie wiesz, co stanie się z nim podczas Twojej nieobecności i w czyje ręce trafią Twoje dane, gdy stracisz dowód z zasięgu wzroku. Może trafić w ręce oszustów, złodziei tożsamości.

Żadna instytucja lub placówka nie może żądać od Ciebie zostawienia dowodu osobistego w zamian za wypożyczenie sprzętu. I jest to zakaz usankcjonowany prawnie, za złamanie którego grozi nawet kara pozbawienia wolności.

4. Nigdy nie otwieraj e-maili podejrzanych lub nieznanego pochodzenia

Często spotykaną praktyką, jaką stosują oszuści, jest wysyłanie wiadomości, które zawierają niebezpieczne linki. Prowadzą one do fałszywych stron znanych banków, platform aukcyjnych itp. Znajdziesz na nich ponaglającą informację wzywającą do uzupełnienia w dość krótkim czasie swoich danych osobowych, pod pretekstem zawieszenia konta.
To standardowy przykład próby oszustwa. Pamiętaj, że banki, instytucje finansowe ani żadne inne uczciwe instytucje nie stosują tego typu praktyk! Nigdy więc się do nich nie stosuj i ignoruj tego typu maile!

5. Nie daj się złodziejom

Złodzieje, którzy mają Twoje dane osobowe, mogą nie tylko utworzyć fałszywe konto na portalu społecznościowym, ale również zwrócić się do banku po pożyczkę. Gdy ta zostanie im przyznana, mogą podpisać umowę kredytową. Dlatego też, co jeszcze raz podkreślamy, warto zawsze być czujnym i ostrożnym, a z drugiej strony wzmocnić ochronę, korzystając z Alertów BIK. Dzięki nim zostaniesz zaalarmowany, kiedy ktoś będzie próbował wyłudzić kredyt, poszywając się pod Ciebie.

Prawo do prywatności

Prawo do ochrony prywatności – jedno z podstawowych praw człowieka – ma kilka aspektów. Jednym z nich jest ochrona danych osobowych. Koncepcja ta narodziła się w Europie w latach 70. XX w., kiedy zaczęto rozwijać nowe możliwości automatycznego przetwarzania informacji. W polskim prawie ochrona danych osobowych pojawiła się dopiero po transformacji ustrojowej. Konstytucja RP z 1997 r. gwarantuje prawo do prywatności i autonomii informacyjnej. Ukonkretnia je ustawa o ochronie danych osobowych (z tego samego roku) oparta na rozwiązaniach przyjętych w Unii Europejskiej. Na jej podstawie utworzono instytucję Generalnego Inspektora Ochrony Danych Osobowych (GIODO), który rozpatruje skargi obywateli, opiniuje akty prawne, sygnalizuje potrzebę zmian prawa i prowadzi akcje edukacyjne dotyczące ochrony danych osobowych. GIODO jest powoływany przez Sejm za zgodą Senatu na 4-letnią kadencję.

Zgodnie z obowiązującym prawem dane osobowe to wszelkie informacje dotyczące konkretnej osoby – zidentyfikowanej (np. takiej, którą znamy bezpośrednio) lub możliwej do zidentyfikowania (czyli takiej, którą można wskazać na podstawie posiadanych informacji, choćby numeru identyfikacyjnego, wyglądu lub jakiejkolwiek kombinacji cech, np. ruda dziewczynka, która ma zielony plecak i chodzi do konkretnej szkoły i klasy). Nie mamy do czynienia z danymi osobowymi wówczas, gdy informacja dotyczy instytucji (np. firmy), grupy osób, osoby zmarłej lub fikcyjnej (np. postaci literackiej). Daną osobową może być każda informacja, nie tylko imię i nazwisko, ależ też np. kolor oczu określonej osoby; choroba, na która cierpi; informacja, jakie strony internetowe odwiedza czy jakie ma oceny z chemii. To, czy jakaś informacja jest daną osobową, zależy od kontekstu. Tablice rejestracyjne dla policji są daną osobową, bo policja bez trudu może w bazie danych zweryfikować, kto jest właścicielem samochodu, ale dla innego kierowcy, który nie ma takiej możliwości – już nie.

Według ustawy o ochronie danych osobowych „przetwarzanie danych" to wszystkie działania dotyczące danych osobowych: zbieranie, przechowywanie, udostępnianie, a nawet ich usuwanie. Podmiot, który decyduje o tym, że dane są przetwarzane i w jaki sposób się to odbywa, jest nazywany administratorem danych. On ponosi odpowiedzialność za to, by przetwarzanie danych odbywało się zgodnie z prawem i było odpowiednio zabezpieczone.

Dane osobowe podlegają ochronie, co oznacza, że podmioty, które chcą je przetwarzać (i firmy, i publiczne instytucje), powinny spełnić określone warunki. Szczególnie chronione są tzw. dane wrażliwe, czyli dane dotyczące m.in. pochodzenia, poglądów politycznych, wyznania, stanu zdrowia czy karalności. Nikt – ani pracownik firmy, ani urzędnik państwowy, ani policjant – nie może przetwarzać naszych danych bez podstawy prawnej. Ustawa wskazuje konkretne sytuacje, w których jest to uprawnione. Najczęściej wykorzystywane to:

- zgoda osoby, której dane dotyczą (musi być dobrowolna; w drobnych, codziennych sprawach mogą ją wyrażać osoby powyżej 13 roku życia; w innych przypadkach — tylko osoby dorosłe);
- przepis prawa (np. szkoła ma prawo przetwarzać dane uczniów w celach związanych z kształceniem);
- fakt, że dane są niezbędne do wykonania umowy (np. adres wysyłki w przypadku zakupów w sklepie internetowym).

Zgoda na przetwarzanie danych osobowych powinna dotyczyć konkretnego administratora danych i konkretnego celu. Żeby przetwarzać dane w innym celu, trzeba uzyskać osobną zgodę. Na przykład, jeśli wyrazisz zgodę na przetwarzanie swoich danych w ramach udziału w konkretnym konkursie – organizator nie ma prawa wykorzystać informacji ze zgłoszenia w kolejnej edycji. Nie może też przekazać danych innemu podmiotowi, który np. chciałby wysyłać katalogi reklamowe (chyba że wyrazisz zgodę również na to).

Każdej osobie, której dane są przetwarzane, przysługują w związku z tym konkretne uprawnienia:

- prawo do informacji o tym, skąd dany podmiot pozyskał dane i w jakim celu je przetwarza, np. jeśli dzwoni do Ciebie telemarketer, możesz oczekiwać informacji, skąd ma Twój numer telefonu, jaki podmiot i w jakim celu go wykorzystuje;
- prawo do wycofania zgody, jeśli po pewnym czasie zmieniłeś/-aś zdanie, np. jeśli podałeś/-aś swój adres e-mail organizacji, ale nie chcesz już otrzymywać jej newslettera, możesz napisać do niej, by zaprzestała przetwarzać Twoje dane;
- prawo do uzupełnienia, uaktualnienia i sprostowania danych – jeśli Twoje dane się zmieniły lub są niezgodne z prawdą, możesz je zaktualizować;
- jeśli ktoś legalnie przetwarza Twoje dane, ale nie odbywa się to na podstawie żadnej z trzech podstaw prawnych wskazanych wyżej (a np. na podstawie usprawiedliwionego interesu administratora), możesz zgłosić sprzeciw i żądać zaprzestania przetwarzania danych.

Każdy może mieć wpływ na to, jakie informacje o nim są ujawniane i wykorzystywane. Podpowiadamy, na co warto zwrócić uwagę:

Zanim skorzystasz z usługi, która wymaga podania Twoich danych, zapoznaj się z jej regulaminem, żeby dowiedzieć się, jak te informacje zostaną wykorzystane.

- Nie zawsze warto wyrażać zgodę na przetwarzanie danych osobowych – nie musisz zgadzać się na wszystko, co ktoś Ci sugeruje.
- Żeby skorzystać z wybranej usługi, musisz co prawda zaakceptować, że do jej realizacji niektóre dane będą niezbędne (np. adres e-mail, jeśli zamawiasz coś przez Internet), ale nie musisz zgadzać się na wysyłanie ofert reklamowych czy przekazywanie danych innym firmom.
- Jeśli ktoś żąda od Ciebie zbyt szerokiego zakresu danych i chce je wykorzystywać do niejasnych celów, najlepiej zrezygnuj z danej usługi. Jeśli korzystając z jakiejś usługi, nie musisz zakładać konta lub podawać swoich danych, nie rób tego.

W praktyce nasze dane są przetwarzane na każdym kroku i przez rozmaite podmioty. Obowiązujące prawo nie nadąża za zmianami, jaki w ostatnich latach dokonały się w technologii i biznesie. Szczególnie za nowymi modelami generowania zysku opartymi na przetwarzaniu danych na masową skalę i integrowaniu informacji z różnych źródeł. Dlatego nie w każdej sytuacji prawo skutecznie chroni dane osobowe. Co więcej, wiele podmiotów celowo bądź z niewiedzy nie przestrzega prawa. Co zrobić, jeśli ktoś przetwarza dane, chociaż nie ma do tego prawa (np. zalewa odbiorców niechcianymi ofertami handlowymi mimo sprzeciwu lub bez zgody przekazuje dane innym podmiotom)? Jest kilka możliwości:

- Jeśli Twoje prawa zostały naruszone, warto złożyć skargę do GIODO (jak to zrobić, dowiesz się ze strony giodo.gov.pl).
-

Jeśli naruszenie ochrony danych spowodowało szkodę materialną lub krzywdę, można żądać odszkodowania lub zadośćuczynienia w sądzie cywilnym.

- Jeśli sprawa jest poważna, należy powiadomić policję.

Warto pamiętać, że wymogi wskazane w ustawie o ochronie danych osobowych nie dotyczą wszystkich sytuacji. Ustawa nie dotyczy np. osób prywatnych, które gromadzą informacje w celach osobistych lub domowych (np. nie trzeba spełniać jej wymogów, żeby zapisywać kontakty do przyjaciół i rodziny w telefonie).

Drugi ważny wyjątek dotyczy zagranicznych firm, które mają bazy danych ulokowane poza Polską. Wiele popularnych usług internetowych świadczą firmy z siedzibą w Stanach Zjednoczonych, które gromadzą dane na serwerach poza Europą. Dlatego ani polskie, ani europejskie prawo ich nie obowiązuje, a dane polskiego użytkownika amerykańskiej usługi – portalu społecznościowego (np. Facebook) czy poczty e-mail (np. Gmail) – nie są dostatecznie chronione. Systemowym rozwiązaniem tego problemu ma być nowe unijne rozporządzenie dotyczące ochrony danych, które ma objąć także firmy spoza Unii Europejskiej, jeśli świadczą usługi na unijnym rynku. Tymczasem austriacki aktywista Max Schrems (akcja Europe vs Facebook) na drodze sądowej próbuje zmusić tę amerykańską firmę do szanowania europejskiego prawa i odnosi na tym polu znaczące sukcesy.

Słowniczek pojęć:

Autonomia informacyjna – ważny aspekt prywatności, prawo do samodzielnego decydowania o ujawnianiu informacji na swój temat oraz do kontrolowania informacji dotyczących własnej osoby, którymi dysponują inni.

Dane osobowe – wszelkie informacje dotyczące konkretnej osoby fizycznej – zidentyfikowanej (np. takiej, którą znamy bezpośrednio) lub możliwej do zidentyfikowania (czyli takiej, którą można wskazać na podstawie posiadanych informacji). Nie mamy do czynienia z danymi osobowymi wówczas, gdy informacja dotyczy instytucji (np. firmy), grupy osób, osoby fikcyjnej (np. postaci literackiej) czy takiej, której nie jesteśmy w stanie rozpoznać. Dane osobowe podlegają ochronie i nie mogą być zbierane bez odpowiedniej podstawy prawnej (np. zgody osoby, której dotyczą).

Odszkodowanie – rekompensata za wyrządzoną szkodę majątkową. Może dotyczyć szkody na mieniu (zniszczony przedmiot, utracony przewidywany zysk związany z jego wykorzystaniem) lub szkody na osobie (np. uszkodzenie ciała, rozstrój zdrowia). Odszkodowanie otrzymuje poszkodowany od tego, kto szkodę wyrządził lub ponosi za nią odpowiedzialność (np. rodzic ponosi odpowiedzialność za szkodę wyrządzoną przez dziecko). Rekompensata może przybrać formę pieniężną lub polegać na przywróceniu stanu istniejącego przed wyrządzeniem szkody.

Prywatność – sfera życia człowieka, w którą nie należy wkraczać bez pozwolenia. Ma ona swój aspekt cielesny, terytorialny, informacyjny i komunikacyjny. Prywatność jest chroniona przez prawo (m.in. przez Konstytucję RP i akty prawa międzynarodowego). Ograniczenie prawa do prywatności możliwe jest tylko w określonych sytuacjach (na przykład ze względu na bezpieczeństwo publiczne czy ochronę zdrowia).

Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza gdy odbywa się w systemach informatycznych.

Zadośćuczynienie – pieniężna rekompensata za niemajątkową krzywdę odczuwaną jako cierpienie fizyczne lub psychiczne. Zadośćuczynienie otrzymuje osoba poszkodowana od tego, kto wyrządził szkodę lub

Dane osobowe wrażliwe - dane osobowe, które podlegają szczególnej ochronie. Należą do nich informacje o rasie, pochodzeniu etnicznym, poglądach politycznych, przekonaniach religijnych, stanie zdrowia, przynależności partyjnej, związkowej lub wyznaniowej, kodzie genetycznym, nałogach, życiu seksualnym, skazaniach i orzeczeniach dotyczących mandatów i kar.

Administrator danych osobowych - jednostka (osoba, podmiot gospodarczny, instytucja, itp.) decydująca i podejmująca działania związane z przetwarzaniem danych osobowych. Nałożony jest na nią obowiązek informacyjny (konieczność podania danych teleadresowych). Zobowiązana jest do staranności w przetwarzaniu danych w celu ochrony interesów osób, których dane posiada, oraz do aktualizowania danych i zaprzestania przetwarzania danych na żądanie.

Zagrożenia

- Szkodliwe treści
- Niebezpieczne kontakty
- Cyberprzemoc
- Cyberprzestępstwa
- Uzależnienie

http://www.chip.pl/news/bezpieczenstwo/technologie-bezpieczenstwa/2012/02/polak-w-internecie-mniej-swiadomy-zagrozen-od-przecietnego-europejczyka

Cyberprzemoc

- Wyzywanie
- Nękanie
- Poniżanie
- Ośmieszanie
- Kradzież tożsamości

http://www.swiat-prezentacji.pl/prezentacja,cyberprzemoc,406

Cyberprzestępstwa

- Nielegalne kopiowanie i rozpowszechnianie plików i programów komputerowych
- Włamania do systemów komputerowych

Uzależnienie

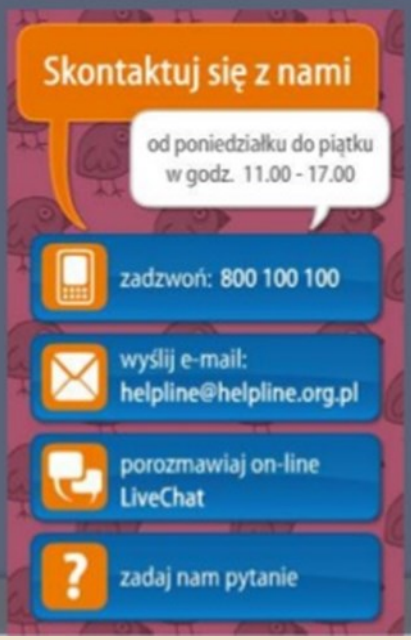
- Skutki:
  - nieprzystosowanie społeczne
  - wyalienowanie
  - problemy w szkole
  - problemy zdrowotne

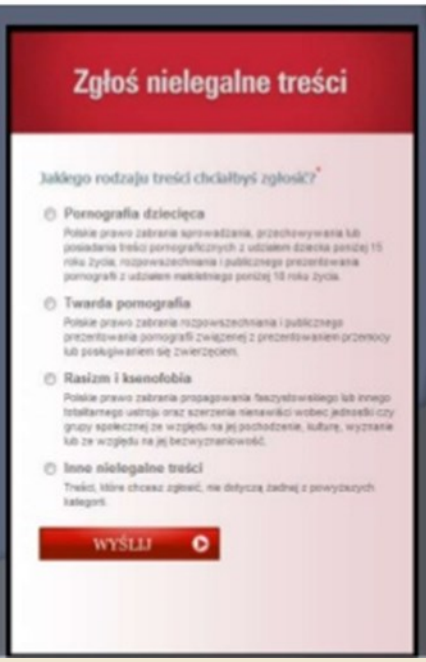
http://www.megapedia.pl/uzaleznienie-od-internetu.html

Zgłaszaj wszystkie zauważone próby dokonania cyberprzestępstwa !

800 100 100
helpline.org.pl

dyżurnet.pl





Wydawca: Koło Historyczne ZZSP im. Jana Pawła II

ZZSP im. Jana Pawła II

Adres: Plac Kilińskiego 8,

95-100 Zgierz , tel. 42 719 08 66

E –mail: zzspzgierz@op.pl

www.zzsp.miasto.zgierz.pl