Jak chronić swoje dane osobowe?

Dane osobowe, są cennym „towarem” rynkowym wykorzystywanym w celach marketingowych i sprzedażowych.

Zdarza się jednak, że w przypadku utraty danych osobowych, kiedy to danymi posługuje się osoba do tego nieuprawniona, dane te użyte są w celach przestępczych, takich jak np. wyłudzanie pożyczek czy kredytów.

Przestępcy wykorzystują skomplikowane techniki informatyczne lub środki socjotechniczne, by wejść w posiadanie informacji o Tobie, w tym o Twoich danych osobowych.

Bywa i tak, że wyrażasz zbyt wiele zgód i dzielisz się bezrefleksyjnie danymi. I o ile nie jesteś w stanie w 100 proc. ich ochronić, to możesz zrobić sporo, by ograniczyć ryzyko ich wykorzystania nie tylko w celach przestępczych, ale przede wszystkim dla ochrony swojej prywatności.

1. **Uważaj na to co i komu udostępnisz o sobie w Internecie**

   W XXI w., w szczególności media społecznościowe mogą być kopalnią wiedzy o Tobie, o Twoim stanie majątkowym, miejscu pracy, wydarzeniach z Twojego codziennego życia. Zdarza się, że nadmiernie dzielisz się informacjami na swój temat. Przez to Internet jest źródłem wiedzy także o Twoich poglądach, zachowaniach konsumenckich, zainteresowaniach. Dane te są cenne nie tylko dla działów marketingu różnych firm, po to by na Twoich zachowaniach w sieci oprzeć kierowaną ofertę, ale niekiedy i dla przestępców. Szczególnie gdy profil, który Ciebie dotyczy jest w pełni publiczny, możesz być narażony na użycie Twoich danych bez Twojej wiedzy i przyzwolenia niezgodnie z celami, dla których dane udostępniłeś.

2. **Nie zostawiaj dokumentów w zastaw**

   Podczas urlopu, wykonując różnego rodzaju aktywności, wypożyczając sprzęt, np. kajaki, łódki, czy narty albo łyżwy, nie oddawaj w zastaw dowodu osobistego, paszportu, prawa jazdy, legitymacji szkolnej lub studenckiej. Warto pamiętać, że zgodnie z prawem zatrzymywanie dowodu osobistego bez podstawy prawnej jest karane, natomiast nie wszystkie dane osobowe zawarte we wskazanych dokumentach są niezbędne dla realizacji celu wypożyczenia sprzętu. Utrata kontroli nad dowodem osobistym naraża Cię na posłużenie się tym dokumentem bez Twojej wiedzy i woli, co z kolei stwarza niebezpieczeństwo kradzieży tożsamości. Osoby dysponujące kompletem informacji o Tobie, czy kopią Twojego dokumentu tożsamości, mogą podszyć się pod Ciebie i np. dokonywać na Twoją szkodę różnych transakcji, takich jak chociażby zaciągnięcie kredytu w banku czy wypożyczenie drogiego sprzętu i niezwrócenie go (np. samochodu). Nieodpowiedzialne zachowanie, o którym mowa – utrata kontroli nad identyfikującym Cię dokumentem, zwłaszcza potwierdzającym Twoją tożsamość – naraża Cię na wykorzystanie Twojego wizerunku oraz innych danych osobowych w celu wyrządzenia Ci szkody majątkowej lub osobistej. Osoby, które przejmą taki dokument mogą, korzystając z Twojej tożsamości, zawrzeć w Twoim imieniu różnego rodzaju umowy, np. z zakresu usług telekomunikacyjnych, z dalszymi tego faktu obciążającymi Ciebie konsekwencjami.

Co do zasady nie powinieneś się godzić na kopiowanie Twojego dokumentu tożsamości. Tylko w niektórych sytuacjach jest to wyjątkowo dopuszczalne, gdy pozwalają na to przepisy. Gdy administrator domaga się kopii np. Twojego dowodu osobistego, poproś, aby wskazał Ci podstawę prawną, która nakłada na niego obowiązek takiego działania.

3. **Nie podawaj danych przez telefon**

   Unikaj przekazywania danych telefonicznie – szczególnie, gdy to nie Ty inicjujesz rozmowę, ale ktoś dzwoni do Ciebie. Udostępnianie danych na odległość obarczone jest ryzykiem, brakiem pewności co do tego komu faktycznie dane są przekazane. Nie daj się zaskoczyć, sprowokować do udostępniania danych wbrew Twojej woli, dla nieznanych, niewyjaśnionych przez rozmówcę celów. Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

4. **Uważaj na różne formularze, poprzez które udostępniasz dane**

   Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Zastanów się czy faktycznie chcesz założyć kartę lojalnościową w sklepie, by mieć rabaty lub dodatkowe promocje. W takich sytuacjach podajesz sklepom imię, nazwisko, adres zamieszkania, datę urodzenia, adres e-mail, numer telefonu, a w zamian otrzymujesz promocje, bony rabatowe, dodatkowe upominki przy zakupach. Ale czy rzeczywiście warto?

   Należy pamiętać, że administrator musi spełnić wobec Ciebie obowiązek informacyjny, czyli przekazać Ci niezbędne informacje na swój temat, podając m.in. swoją tożsamość, dane kontaktowe oraz dane kontaktowe swojego inspektora danych osobowych (o ile go wyznaczył), a także cel i podstawę prawną przetwarzania danych.

   Nie podawaj wszelkich danych, które pozwalają na pełną identyfikację, jeżeli w danej sytuacji nie jest to konieczne, danych nadmiarowych. Jeśli musisz skorzystać z danej usługi, to podaj tylko dane niezbędne do jej wykonania – dobrze przemyśl przekazanie tych, których przekazanie oznaczone jest jako opcjonalne.

   Zanim zaznaczysz wszystkie zgody, upewnij się czego dotyczą. Zwróć uwagę czy w formularzu zgody nie są zaznaczone domyślnie. Zgodnie z prawem nie powinno tak być. Dokładnie też czytaj, czego dotyczą klauzule zgód. W przypadku wątpliwości, zadawaj pytania administratorom. Powinni Cię poinformować o okresie przez jaki dane będą przetwarzane oraz o przysługujących Ci prawach, w tym dostępu do danych, ich sprostowania, usunięcia czy wniesienia sprzeciwu wobec przetwarzania, a także, czy Twoje dane będą komuś innemu (innym odbiorcom) przekazywane.

   Pamiętaj, że wyrabiając kartę lojalnościową często udzielasz zgód na wykorzystywanie danych w celach marketingowych nie tylko administratora, ale i jego partnerów biznesowych. O ile możesz, zweryfikuj, kim oni są, jakie to są firmy. Zgody na marketing „cudzy” powinny być nieobowiązkowe, powinna być Ci pozostawiona możliwość wyboru co do tego, czy taką zgodę wyrazisz.

Administrator powinien Ci zapewnić, by możliwość wycofania zgody była równie łatwa, jak jej udzielenie oraz powinieneś być poinformowany o prawie do cofnięcia zgody nim ją wyrazisz.

5. **Nie wyrzucaj danych na śmietnik, dopóki ich nie zniszczysz**

   Wszelkie dokumenty z Twoimi danymi, to kolejne źródło wiedzy o Tobie, zwłaszcza gdy zawierają one wiele różnych informacji umożliwiających wyciągania wniosków na Twój temat, np. ustalenie tego, gdzie pracujesz, ile zarabiasz, kiedy nie ma Ciebie w domu, ile masz dzieci, jak drogie robisz zakupy. Dlatego też - zanim wyrzucisz dokumenty do kosza – należy je zniszczyć (np. faktury, rachunki), zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach, w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.

6. **Usuwaj trwale dane z nośników**

   Ogrom danych o Tobie może znajdować się na Twoich starych dyskach twardych, kartach pamięci, pendrive'ach czy innych nośnikach. Zwróć uwagę, że coraz więcej informacji na Twój temat jest zapisanych w komputerach, smartfonach, aparatach fotograficznych czy tabletach. Zanim się pozbędziesz takich urządzeń lub nośników, trwale usuń z nich dane. Jednak zwykłe ich skasowanie nie będzie wystarczające, gdyż wiele danych da się odzyskać. Dlatego zanim wyrzucisz nośnik albo go sprzedasz, usuń z niego dane, korzystając przy tym z odpowiedniego do tego oprogramowania. Warto też przywrócić ustawienia fabryczne urządzenia, aby nie było w nim zapamiętanych loginów i haseł do różnych usług i aplikacji, z jakich korzystałeś, a zwłaszcza z takich, z których nadal korzystasz.

7. **Używaj programów chroniących komputer**

   Używaj oprogramowania chroniącego komputer i urządzenia mobilne przed niepożądanymi działaniami z zewnątrz, np. złośliwego oprogramowania. Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall.

8. **Bądź czujny w sieci**

   Nie odpowiadaj na maile od osób, których nie znasz np. tzw. spamerów, zwłaszcza gdy domagają się podania jakichś informacji o tobie czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika, sugerują zmianę identyfikatora i hasła. Zachowaj ostrożność także przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet. Zwracaj uwagę czy aby na pewno logujesz się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL (widoczny w pasku adresu przeglądarki). Weryfikuj sklepy, w których chcesz coś kupić: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego. Jeśli masz wątpliwości co do bezpieczeństwa Twoich danych zastanów się czy koniecznie musisz dokonać zakupów u tego sprzedawcy. Weryfikuj regulaminy i polityki prywatności – unikaj sprzedawców nieprzedstawiających takich dokumentów czy też prezentujących w nich postanowienia zbyt ogólne, niejasno czy nieprecyzyjnie brzmiące, sformułowane niepoprawnie gramatycznie czy językowo, może to

bowiem oznaczać, że są to podmioty niepodlegające polskiemu czy europejskiemu prawu.

9. **Zmieniaj hasła**

   Zazwyczaj to głównie pracodawcy wymagają od pracowników zmiany haseł co pewien czas, by chronić nie tylko dane osobowe, ale i tajemnice firm. Taką zasadę warto też wdrożyć w życiu prywatnym i okresowo zmieniać hasła dostępu do swojego komputera, do poczty elektronicznej, systemów bankowości elektronicznej, ale nawet sklepów internetowych, w których -masz konto użytkownika. Staraj się przy tym korzystać z różnych haseł. Dobrze jest, aby nie miały one nic wspólnego z Twoimi życiem osobistym, miejscem zamieszkania, Twoim imieniem i nazwiskiem, datą urodzin, imionami Twoich bliskich czy Twoich zwierząt itp., tj. informacjami, które łatwo można skojarzyć z Tobą obserwując Twoje zachowania w sieci, czy połączyć z innymi informacjami o Tobie.

2019-10-10 

- Urząd Ochrony Danych Osobowych
- ul. Stawki 2, 00-193 Warszawa