

# Bezpieczeństwo w cyfrowym świecie



**D**ane osobowe to towar poszukiwany m.in. dla w celów przestępczych (fikcyjne umowy, wydłużanie pieniędzy) lecz nie tylko. Tworzone są pełne profile osób (imię, nazwisko, adres zamieszkania, PESEL, NIP, adres e-mail, adres IP, wersje oprogramowania) ułatwiające oszustwo. Podszycie się pod inną osobę (np. użycie cudzego pseudonimu na forum czy blogu, utworzenie w serwisie społecznościowym konta z kompromitującymi danymi, albo wykonanie w cudzym imieniu operacji bankowej) powoduje straty trudne do oszacowania, często gorsze niż utrata karty kredytowej czy dowodu osobistego, które można zastąpić. Dzieje się tak, mimo sankcji prawnych za posługiwanie się cudzymi danymi osobowymi.

■ Ramy prawne ochrony danych osobowych to w szczególności Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 r. nr 101 poz. 926, z późn. zm.) i Rozporządzenie MSWiA z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

■ Rozwiązania prawne i administracyjne będą skuteczne, gdy towarzyszyć im będzie odpowiedzialność i świadomość użytkowników Internetu. Większość internautów przeświadczona jest o anonimowości w sieci. Nic bardziej mylnego. Cyfrowe ślady aktywności w Internecie pozostawiane są świadomie (fora, blogi, portale społecznościowe, serwisy, e-maile, komunikatory) lub nieświadomie (IP komputera, data, czas i rodzaj połączenia, informacje o wersji oprogramowania w komputerze, preferencjach użytkownika, ruchu sieciowym zbieranym przez szkodliwe oprogramowanie typu spyware, adware itp.). Ślady zostają też w komputerze: pliki tymczasowe i historia przeglądanych stron internetowych, pliki cookie, pozwalające śledzić użytkownika.

■ Ślady w sieci można ograniczyć dbając o prywatność. Najważniejsze są rozważa i umiar w informowaniu o sobie, swoich bliskich i znajomych, unikanie zamieszczania zdjęć świadczących o stanie majątkowym. Bardzo istotny dla bezpieczeństwa naszych kont w systemach jest proces logowania (uwierzytelnienia). Używane hasła należy konstruować z co najmniej ośmiu małych i dużych liter oraz znaków specjalnych, przechowywać je w bezpiecznym miejscu. Nie ujawnić hasła nikomu, okresowo

je zmieniać i różnicować - nie stosować jednego do wszystkich serwisów. Należy też dbać o usuwanie danych osobowych w sposób uniemożliwiający ich odtworzenie, nie wyrzucać na śmietnik dokumentów i nośników informatycznych bez uprzedniego ich zanonimizowania. Nie należy we mailu podawać w jawnej postaci danych osobowych, odpowiadać na spam i e-maile proszące o potwierdzenie danych, otwierać wiadomości pochodzących od nieznanych nadawców. Aby zminimalizować wysyłane i pozostawiane na urządzeniach dane należy używać trybu prywatnego przeglądarki, odwiedzać tylko serwisy zaufane i świadomie zezwalać im na użycie plików ciasteczek, usuwać ciasteczka i historię gromadzoną przez przeglądarki internetowe. Gdy jest to konieczne, używać serwisów anonimizujących. Ważna jest rozważa przy wypełnianiu i podpisywaniu ankiet, formularzy czy umów. Przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet warto ręcznie wpisywać adres banku lub sklepu internetowego (nie klikać linków), aby uniknąć przekierowania do fałszywych stron internetowych. Autentyczność witryny sprawdzić należy zwracając uwagę czy połączenie z serwerem jest nawiązane kanałem zaszyfrowanym - adres strony zaczyna się na

„https://” zamiast „http://” oraz czy widnieje „zielony” znaczek dostawcy certyfikatu witryny internetowej (w przeglądarce informacja ta znajduje się po lewej stronie wpisanego adresu strony). Podczas połączenia, np. z serwisem bankowym, nie należy uruchamiać w przeglądarce dodatkowych zakładek i otwierać nowych okien. Wybierając najkorzystniejszą ofertę trzeba kierować się nie tylko jej atrakcyjnością, lecz także bezpieczeństwem transakcji, **zapoznać się z regulaminem i polityką ochrony danych oferenta e-commerce**. Powinno się zrezygnować z zakupów z użyciem przypadkowego sprzętu (np. kafejki internetowej). Zaleca się korzystanie wyłącznie z legalnego i uaktualnionego oprogramowania (antywirusy, zapory, IDS/IDP, itp.). Warto znać zagadnienia opisane na platformie edukacyjnej eduGODO oraz na forach i w serwisach poświęconych bezpieczeństwu w Internecie.

■ W przypadku kradzieży danych powinniśmy niezwłocznie zgłosić administratorowi ten fakt, w miarę możliwości usunąć przyczynę (np. wirus z komputera, zaktualizować programy), jak najszybciej zmienić hasło i login.

■ Ponadto można podjąć działania o charakterze prawnym. Każdy może żądać od administratora udostępnienia informacji o treści własnych

danych osobowych, ich źródle i dacie rozpoczęcia przetwarzania danych, zakresie udostępniania. Można też wnieść sprzeciw wobec dalszego przetwarzania naszych danych i administrator powinien usunąć je niezwłocznie. Każdy kto ma wiedzę o naruszeniu przepisów ustawy o ochronie danych osobowych w odniesieniu do jego danych, może złożyć skargę do Generalnego Inspektora Ochrony Danych Osobowych (GODO). W przypadku potwierdzenia zasadności skargi, decyzja administracyjna GODO nakazuje doprowadzenie do stanu zgodnego z prawem. GODO może też skorzystać z uprawnień ustawowych, tj. skierować do zaskarżonego podmiotu wystąpienie w sprawie udoskonalenia ochrony danych, żądać wszczęcia postępowania dyscyplinarnego wobec winnych uchybień, a w uzasadnionych przypadkach skierować do organów ścigania zawiadomienie o podejrzeniu popełnienia przestępstwa. Dodatkowe informacje znajdziesz na stronie [godo.gov.pl](http://godo.gov.pl)



**Tomasz Soczyński**  
Z-ca Dyrektora  
Departamentu  
Informatyki  
Biuro Generalnego  
Inspektora  
Ochrony Danych  
Osobowych