Warto wiedzieć

Kradzież tożsamości – uważaj na swoje dane osobowe!

Tożsamość każdego z nas określana jest przez unikalne cechy, oraz dane osobowe, które umożliwiają naszą identyfikację i pozwalają na odróżnienie od innych osób. Dotyczą one m.in. takich danych, jak: imię, nazwisko, adres zamieszkania, numer PESEL, numer dokumentu tożsamości, a także innych specyficznych cech charakteryzujących naszą fizyczność, umysłowość, czy kulturowość.
O kradzieży tożsamości mówimy w przypadku, gdy osoba niepowołana, niezgodnie z prawem (najczęściej w sposób podstępny), wejdzie w posiadanie naszych danych osobowych. Dane mogą zostać pozyskane m.in. poprzez włamanie do naszego osobistego komputera, a także za pomocą przesłanych drogą elektroniczną wirusów czy programów szpiegujących. Do większości przypadków kradzieży danych dochodzi przez nieostrożność ich właściciela, jak również niewłaściwe ich zabezpieczanie.

Jeśli dojdzie do kradzieży tożsamości, jesteśmy narażeni m.in. na:
- założenie fałszywego profilu czy konta internetowego;
- umieszczanie w sieci obraźliwych komentarzy, opinii na nasz temat, bądź w naszym imieniu;
- próby szantażu i wyłudzania pieniędzy;
- posługiwanie się naszym dokumentem tożsamości w celach niezgodnych z prawem, np. zawarcia umowy czy zaciągnięcia zobowiązania finansowego w naszym imieniu.

Dlatego warto wiedzieć, że…
- nie udostępniaj zbyt wielu informacji o sobie (w tym np. o swoim statusie majątkowym) w internecie, oraz nie podawaj swoich danych osobom, których nie znasz;
- nie udostępniaj swoich danych osobowych w miejscach publicznych. Staraj się np. w zatłoczonym autobusie nie udostępniać danych podczas rozmowy telefonicznej;
- nie korzystaj z publicznych sieci Wi-Fi. Jeśli jednak, nie masz innej możliwości, użyj wirtualnej sieci prywatnej (VPN), aby ukryć swoje działania online, i nie narazić na utratę cennych informacji o sobie;
- nie udostępniaj zdjęć karty płatniczej ani dokumentów tożsamości w internecie;
- nie zostawiaj dokumentów (legitymacja, dowód, paszport) w zastaw i nie zezwalaj na ich kopiowanie;
- używaj programów antywirusowych i oprogramowania pochodzącego z autoryzowanych źródeł. Pamiętaj o ich aktualizacji;
- sprawdzaj ustawienia prywatności online, oraz ustawienia urządzenia z którego korzystasz (usługi lokalizacji, udostępnianie zdjęć, kontaktów, kalendarzy, mikrofonu itp.);
- nie otwieraj e-maili od nieznanych nadawców, a także od znajomych, jeśli budzą Twoje podejrzenia. Pozwoli to uniknąć ataków phishingowych, których celem jest m.in. wyłudzenie dodatkowych danych lub uzyskanie dostępu do internetowych systemów usług, z których korzystasz;
- używaj zróżnicowanych haseł dostępu i regularnie je zmieniaj. Nie zezwalaj również, na zapamiętywanie haseł w przeglądarce urządzenia z którego korzystasz, oraz nie podawaj ich osobom trzecim. Warto korzystać ze stron i serwisów używających kilkustopniowego procesu uwierzytelniania (np. przy pomocy jednorazowych kodów, przesyłanych SMS-em);
- usuwaj dane trwale z nośników;
- zachowaj ostrożność przy wypełnianiu formularzy lub ankiet, upewniając się, że instytucja, która gromadzi Twoje dane, udostępniła szczegółowe informacje o sobie oraz sposobie i celu, w jakim chce uzyskać Twoje dane;
- starannie niszcz dokumenty zawierające Twoje dane osobowe. Nie wyrzucaj na śmietnik rzeczy zawierających dane, które pozwoliłyby na Twoją pełną identyfikację.

Jeśli podejrzewasz lub wiesz, że Twoja tożsamość została skradziona:
- poinformuj o tym fakcie rodziców, nauczycieli, opiekunów;
- zmień natychmiast hasła dostępu do witryn. Jeśli nie możesz się zalogować, przejdź do działu pomocy technicznej strony, w celu uzyskania pomocy;
- pamiętaj, że każdorazowo należy zgłosić policji kradzież dokumentów zawierających dane osobowe.