Ochrona danych osobowych podczas korzystania z nowych technologii

Szanowni Państwo,

nasz Urząd jak i Urząd Ochrony Danych Osobowych zachęca do bezpiecznego korzystania z zasobów internetowych.

Poniżej kilka najważniejszych kwestii związanych z ochroną danych osobowych podczas korzystania z nowych technologii, o których pamiętajmy w codziennej pracy jak i w życiu prywatnym.

Zadbaj o zróżnicowane i silne hasła logowania

Hasło powinno być trudne do odgadnięcia i zawierać duże/małe litery, cyfry oraz znaki specjalne- – hasła z większą liczbą znaków są mniej podatne na złamanie w krótkim czasie. Nie zaleca się zapamiętywania haseł w pamięci przeglądarki lub w aplikacji na urządzeniu. Nie należy także używać tej samej nazwy użytkownika w połączeniu z identycznym hasłem we wszystkich aplikacjach, z których korzystasz;

Dopasuj ustawienia prywatności konta w mediach społecznościowych

Ustaw je tak, aby dostęp do informacji, danych osobowych, zdjęć, komentarzy na profilu w mediach społecznościowych miały jedynie zaufane osoby, będące w gronie Twoich znajomych. Rozważ także, czy Twój profil powinien być widoczny dla zewnętrznych wyszukiwarek;

Uważaj, jakimi informacjami, ale też zdjęciami lub filmami, dzielisz się z innymi

Opublikowane przez Ciebie dane mogą zostać wykorzystane wbrew Twoim intencjom. Przykładowo, Twoje zdjęcia mogą być wystawione na ocenę innych osób, a ewentualna ich reakcja i komentarze mogą okazać się raniące, dokuczliwe, a nawet wulgarne. Pamiętaj, że osoba której zdjęcia zamieszczasz powinna być co najmniej poinformowana o tym fakcie. Uszanuj brak zgody innych osób na rozpowszechnianie informacji o nich. Raz opublikowana informacja, treść bądź fotografia może pozostać w cyberprzestrzeni już na zawsze, a konsekwencje złych wyborów ciągnąć się latami;

Nie ujawniaj zbyt wielu informacji o sobie

Media społecznościowe nie są odpowiednimi miejscami do dzielenia się danymi/informacjami takimi, jak adres zamieszkania, numer telefonu czy miejsce pracy. Uważaj na zamieszczenie zdjęć lub nagrań pozwalających osobie nieznajomej zlokalizować miejsce Twojego pobytu. Ponadto nie zamieszczaj zdjęć np. dowodu tożsamości, karty płatniczej, druków zawierających dane osobowe, kart pokładowych czy prawa jazdy. Należy mieć świadomość, że dane osobowe lub dane kontaktowe mogą pozyskać przestępcy, którzy zechcą wykorzystać je przeciwko Tobie lub Twoim najbliższym;

Uważaj na zaproszenia od nieznanych użytkowników

Bądź ostrożny i nie akceptuj automatycznie zaproszeń do grona znajomych lub obserwowania od obcych osób. Osoba podająca się za określoną osobę, może okazać się w rzeczywistości zupełnie kimś innym, dlatego należy być ostrożnym przy zawieraniu nowych znajomości w sieci. Pamiętaj też, że ktoś obcy może się podszyć także za Twojego bliskiego, przejmując wcześniej jego tożsamość w sieci;

Uważaj na tzw. phishing

Jest to jedno z najbardziej niebezpiecznych działań zmierzających do kradzieży loginów i haseł, które dotyczy również portali społecznościowych. Hakerzy rozsyłają odsyłacze do fałszywych serwisów społecznościowych, do złudzenia przypominających te, z których korzystasz na co dzień. Po kliknięciu w taki link i wprowadzeniu danych do logowania cyberprzestępcy mogą uzyskać dostęp do Twoich danych;

Uważaj na szkodliwe oprogramowanie, które może być przesyłane za pomocą komunikatorów

Zachowaj czujność, zanim otworzysz otrzymany link, upewniając się, że pochodzi z zaufanego źródła. Hakerzy, wykorzystując nieuwagę użytkownika, rozsyłają linki do zainfekowanych stron lub dodają złośliwe rozszerzenia do przeglądarek, dzięki czemu mogą przejąć kontrolę nad kontem użytkownika;

Uważaj na publiczne lub niezabezpieczone połączenia internetowe

Nie loguj się do serwisów społecznościowych podczas korzystania z otwartych sieci, ponieważ może to grozić udostępnieniem Twoich danych cyberprzestępcom.

Źródło: https://uodo.gov.pl/pl/138/2634