Bezpieczne media społecznościowe

Media społecznościowe stają się coraz bardziej popularne i istotne w naszym życiu. Pozwalają na łatwe utrzymanie kontaktu z rodziną, znajomymi oraz dzielenie się ważnymi chwilami z naszego życia. Niestety, korzystanie z mediów społecznościowych niesie ze sobą również pewne ryzyka.

Jakich danych nie powinniśmy udostępniać w mediach społecznościowych?

Przede wszystkim unikajmy publikowania swoich danych osobowych: pełnego imienia i nazwiska, adresu zamieszkania, numeru telefonu, daty urodzenia oraz numeru PESEL. Takie informacje mogą być wykorzystane do kradzieży tożsamości.

Kradzież tożsamości może przybrać różne formy i prowadzić do negatywnych konsekwencji. Aby zminimalizować ryzyko kradzieży tożsamości, ważne jest, aby chronić swoje dane osobowe. Zwracajmy uwagę nie tylko na informacje, jakie o sobie zamieszczamy, ale również na zdjęcia jakie „wrzucamy" do Internetu, najczęściej za pośrednictwem mediów społecznościowych.

Jakich zdjęć nie powinniśmy zamieszczać w internecie?

Po pierwsze, jeśli chcemy chronić naszą tożsamość nie powinniśmy udostępniać zdjęć z widocznymi dokumentami tożsamości. Dowód osobisty, paszport czy prawo jazdy „powinny zostać w portfelu", ponieważ zawierają one poufne dane. Po drugie nie należy publikować zdjęć z widocznymi danymi kart kredytowych, wyciągami bankowymi, dowodami rejestracyjnymi samochodu, które mogą zostać wykorzystane do oszustw.

Uważajmy na publikowanie zdjęć z precyzyjną informacją o lokalizacji domu, miejsca pracy czy szkoły naszych dzieci. Jeśli udostępnimy w internecie zdjęcie na tle swojego domu, z widocznym jego numerem, to już zdradzamy nasz adres. Czy chcemy, aby wszyscy wiedzieli gdzie mieszkamy? Nie umieszczajmy zdjęć z wakacji czy weekendowych wyjazdów, które sygnalizują naszą nieobecność w domu i tym samym zachęcają potencjalnych złodziei.

Zachowując ostrożność przy publikacji zdjęć, minimalizujemy ryzyko wystawienia się na potencjalne zagrożenia związane z cyberbezpieczeństwem. Zadbajmy o ustawienia prywatności swojego konta na mediach społecznościowych, aby ograniczyć dostęp do zdjęć i informacji.

Internet nie zapomina, a raz opublikowane informacje trudno jest usunąć. Zanim coś opublikujemy, zastanów się, czy rzeczywiście chcemy, aby te dane były dostępne publicznie.

Hasła i dane do logowania

Media społecznościowe są również bardzo często wykorzystywane do wyłudzanie od nas haseł. Ujawnienie hasła do logowania może nastąpić na różne sposoby, często wynikające z nieostrożności lub braku świadomości użytkowników.

Jedną z metod na wyłudzenie od nas danych do logowania jest phishing. Oszuści tworzą wiadomości lub strony internetowe, które wyglądają jak oficjalne witryny znanych firm czy usług. Ofiary są przekierowywane na te fałszywe strony, gdzie podają swoje dane logowania, włączając w to hasła, które następnie trafiają w ręce przestępców.

Oszuści mogą również podszyć się pod naszych znajomych w mediach społecznościowych, następnie wysyłać wiadomości, w których proszą o szybkie przekazanie pieniędzy. Informacje w internecie, które tak naprawdę sami zamieściliśmy, pomagają przestępcom zdobyć nasze zaufanie.

Na portalach społecznościowych pojawiają się także fałszywe aplikacje, gry czy quizy, które często proszą o dostęp do naszego profilu, co może prowadzić do ujawnienia haseł lub innych wrażliwych danych. Oszuści mogą też spróbować złamać nasze hasło metodą siłową, korzystając z narzędzi, które generują wiele kombinacji hasła w krótkim czasie. Im słabsze hasło, tym łatwiej jest je złamać.

Aby zabezpieczyć się przed wyłudzaniem oraz złamaniem haseł, również za pośrednictwem mediów społecznościowych, powinnyśmy:

- stworzyć hasło odpowiednio długie. Hasło powinno składać się z co najmniej 12 znaków. Im dłuższe hasło, tym trudniejsze do złamania.
- używać silnych haseł, które są trudne do odgadnięcia. Łączmy duże i małe litery, cyfry oraz znaki specjalne.
- używać haseł różnych do różnych kont. W ten sposób, jeśli jedno konto zostanie złamane, inne pozostaną bezpieczne.
- chronić swoje hasła. Nie udostępniajmy ich nikomu, nawet znajomym czy rodzinie.
- Włączyć dwuetapowe uwierzytelnianie (2FA) tam, gdzie jest to możliwe. Dzięki temu, nawet jeśli oszuści zdobędą Twoje hasło, nadal nie będą mogli uzyskać dostępu do Twojego konta.

Weryfikujmy autentyczność stron, na których wpisujemy swoje dane logowania. Pamiętajmy, że https:// czy „zielona kłódka" nie oznaczają, że jesteśmy na właściwej stronie internetowej. Korzystajmy z mediów społecznościowych, ponieważ dają nam wiele możliwości. Pamiętajmy jednak, że bezpieczeństwo naszych danych zależy gównie od nas samych.

***

Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

BANKOWCY DLA EDUKACJI
program sektorowy