Już 123 miliony Europejczyków posiada konto na Facebooku - na całym świecie korzysta z niego ponad 350 mln osób. Wzrasta popularność serwisu, a tym samym ilość ataków na jego użytkowników. Oto kilka porad, które pozwolą uniknąć nieprzyjemnych niespodzianek.

Na fali rosnącej popularności Facebooka wielu jego użytkowników zapomina o podstawowych zasadach bezpieczeństwa, którymi powinni się kierować podczas korzystania z jego licznych funkcji. Specjaliści ds. bezpieczeństwa przygotowali listę 10 wskazówek, dzięki którym każdy, nawet najmniej doświadczony użytkownik będzie mógł czuć się bezpieczny podczas korzystania z portalu Facebook.

1. Zastanów się kogo dodajesz do znajomych

"Zastanów się dwa razy kogo tak naprawdę dodajesz do znajomych"

Jak największa liczba znajomych nie jest najważniejsza. Akceptując zaproszenie pamiętaj, że twój nowy znajomy uzyska dostęp do dużej ilości informacji na twój temat. Dotyczy to postów na tablicy, zdjęć, wiadomości oraz wszystkich informacji osobistych, które o sobie publikujesz. Znajomych możesz usunąć w każdej chwili – może właśnie nadszedł moment, aby odświeżyć swoją listę i zastanowić się nad tym, kto powinien mieć dostęp do informacji na twój temat.

2. Sprawdź swoje ustawienia

Niedawno Facebook zmienił ustawienia prywatności tak, że wszystkie informacje domyślnie ustawione są, jako dostępne publicznie. Warto poświęcić zatem chwilę na przejrzenie ustawień i wprowadzenie koniecznych zmian – możliwe, że dzielisz się większą ilością informacji na swój temat, niż miałeś/miałaś zamiar. Tylko od ciebie zależy jak wykorzystasz te ustawienia – warto na nie zerknąć i stworzyć profil, który naprawdę będzie ci odpowiadał.

3. Zastanów się po co jesteś na Facebooku

Zadaj sobie pytanie, po co ci twój profil. Wykorzystujesz go do publikowania zdjęć, utrzymywania kontaktu ze znajomymi, a może do dzielenia się linkami i informacjami na temat twojego aktualnego zajęcia? Czasem lepiej jest ograniczyć ilość informacji, które udostępniasz na profilu – dotyczy to również logowania się do aplikacji, które pobierają wiele informacji o tobie. W każdej chwili możesz przekonfigurować ustawienia profilu tak, by odpowiadał twoim aktualnym potrzebom.

4. Postępuj rozsądnie ze swoim hasłem

Staraj się nie korzystać z jednego hasła do wszystkich swoich kont – wiele osób to robi, a cyberprzestępcy doskonale zdają sobie z tego sprawę. Warto również zastanowić się nad tym, jakie pytania bezpieczeństwa ustawiasz – dobrze, jeżeli jesteś jedyną osobą, która może znać na nie odpowiedź.

"Czasem lepiej jest ograniczyć ilość informacji, które udostępniasz na profilu"

5. Uważaj skąd się logujesz

Sprawdź, czy komputer, przy pomocy którego logujesz się do profilu nie przechowuje informacji na temat twojego adresu e-mail i hasła. Wydaje się to proste, jednak często łatwo przez pomyłkę wybrać opcję „zapamiętaj hasło”. Upewnij się, że twoja przeglądarka ma ustawione właściwe opcje prywatności.

6. Uważaj, co publikujesz

Przed publikacją danej informacji zastanów się czy na pewno chcesz, by każdy mógł się z nią zapoznać. W momencie publikacji każdy, kto zobaczy tę informację może ją skopiować i opublikować dalej, lub też na jej podstawie podjąć pewne działania. Czy na pewno chcesz, aby wszyscy wiedzieli np. to, że w przyszłym tygodniu wyjeżdżasz, sugerując, że twój dom pozostanie niestrzeżony?

7. Uważaj na ataki phishingowe

W zeszłym roku miało miejsce wiele przypadków prób wyciągnięcia od użytkowników portali społecznościowych ich loginów i haseł. Cyberprzestępcy, podając się np. za przedstawicieli Facebook’a, wysyłali fałszywe e-maile nakłaniające internautów do wpisywania swoich danych dostępowych. Nigdy nie klikaj żadnych linków w e-mailach proszących o zresetowanie twojego hasła. Zawsze kieruj się bezpośrednio na witrynę Facebook – jeżeli wystąpił problem, obsługa poinformuje cię o tym na stronie internetowej.

8. Podejmuj niezwłoczne działania

Jeżeli twoi znajomi zaczną dostawać od ciebie spam lub zaczną pojawiać się aktualizacje statusu, nie będące twoim dziełem, może to oznaczać, że na twoje konto ktoś się włamał. Jeśli masz takie podejrzenia, niezwłocznie zmień hasło dostępu. Jeżeli nie możesz zalogować się na swoje konto, kliknij łącze Centrum pomocy znajdujące się u dołu każdej strony Facebooka, a następnie wybierz opcję Bezpieczeństwo, aby powiadomić przedstawicieli portalu o problemach z kontem.

9. Chroń swój telefon komórkowy

Uważaj na to, kto może mieć dostęp do twojego telefonu komórkowego. Wiele telefonów wyposażonych jest w aplikacje umożliwiające łączenie się z portalami społecznościowymi takimi jak Facebook. Jeżeli wykorzystujesz tego typu aplikacje pamiętaj o tym, aby wylogować się z nich po zakończeniu korzystania.

10. Monitoruj podejrzaną aktywność

Zwracaj uwagę na podejrzaną aktywność na twojej Tablicy, w Aktualnościach oraz w Skrzynce Odbiorczej Facebooka. Nigdy nie klikaj podejrzanych łączy. Często wyglądają one zachęcająco, np. „Hej, odwiedź moją stronę żeby zobaczyć moje zdjęcia z charytatywnego rajdu rowerowego”. Zanim klikniesz przyjrzyj się im bliżej! Czy strona wygląda na prawdziwą? Jeżeli masz jakiekolwiek wątpliwości – nie klikaj.

Tak jak i w przypadku innych aktywności w Internecie, najlepszym doradcą w kwestiach bezpieczeństwa jest zdrowy rozsądek połączony z odrobiną nieufności.

**Zabronione jest korzystanie z Facebooka przez osoby poniżej 13. roku życia. / wypis z regulaminu Facebooka/**

Rejestracja i bezpieczeństwo konta

Użytkownicy serwisu Facebook podają swoje prawdziwe imiona i nazwiska oraz dane. Potrzebujemy pomocy użytkowników, aby utrzymać ten stan rzeczy. Poniżej zawarto przyjęte przez użytkownika zobowiązania względem serwisu Facebook, które dotyczą rejestracji oraz troski o bezpieczeństwo konta:

Zabronione jest podawanie fałszywych danych osobowych na Facebooku i tworzenie konta dla innej osoby bez jej pozwolenia.

Użytkownik może utworzyć tylko jedno konto osobiste.

W przypadku zablokowania konta użytkownik nie ma prawa utworzyć kolejnego bez naszego zezwolenia.

Zabronione jest wykorzystywanie osobistej osi czasu głównie do celów komercyjnych. Do takich zastosowań są przeznaczone strony na Facebooku.

**Zabronione jest korzystanie z Facebooka przez osoby poniżej 13. roku życia.**

Zabronione jest korzystanie z Facebooka przez osoby skazane za przestępstwa seksualne.

Użytkownik jest zobowiązany dbać o rzetelność i aktualność swoich danych.

Zabronione jest udostępnianie swojego hasła (lub poufnego klucza w przypadku twórców aplikacji), zezwalanie innym na uzyskanie dostępu do własnego konta oraz wykonywanie innych czynności, które mogą spowodować spadek poziomu bezpieczeństwa konta.

Zabronione jest przekazywanie swojego konta (a także administrowanej przez siebie strony lub aplikacji) innej osobie bez wcześniejszego uzyskania naszego zezwolenia w formie pisemnej.

W przypadku wybrania przez użytkownika nazwy użytkownika lub podobnego identyfikatora dla konta lub strony rezerwujemy sobie prawo do usunięcia lub odebrania go w razie potrzeby (np. jeżeli właściciel znaku towarowego złoży skargę na nazwę użytkownika niezwiązaną z jego faktycznym imieniem/nazwiskiem).

Netykieta

10 przykazań użytkownika komputera

1. Nie będziesz używał komputera aby szkodzić innym.

2. Nie zakłócaj pracy na komputerach innym.

3. Nie zaglądaj bez pozwolenia do cudzych plików.

4. Nie będziesz używał komputera aby kraść.

5. Nie będziesz używał komputera do dawania fałszywego

świadectwa.

6. Nie będziesz używał ani kopiował programów, za które nie

zapłaciłeś.

7. Nie będziesz używał zasobów cudzych komputerów bez zezwolenia (autoryzacji).

8. Nie będziesz przywłaszczał sobie wysiłku intelektualnego innych.

9. Będziesz myślał o społecznych konsekwencjach programu, który piszesz.

10. Będziesz używał komputera z rozwaga i ostrożnością.

**In­ternet - cza­sem naj­lep­szy przy­jaciel,**

**cza­sem naj­gor­szy wróg!**