Ponad połowa dzieci i młodzieży w wieku 8-16 lat ma swoje profile na Facebooku. To wciąż najpopularniejsze medium społecznościowe wśród najmłodszych użytkowników Internetu. Zgodnie z zasadami Facebooka konto może utworzyć tylko osoba, która ukończyła co najmniej 13 lat Utworzenie konta z fałszywymi danymi stanowi naruszenie regulaminu. Dotyczy to także kont zarejestrowanych w imieniu osób, które nie ukończyły 13 lat.

Eksperci zwracają uwagę, że Facebook nie jest portalem przyjaznym dzieciom. Młode, nieświadome osoby nie zdają sobie sprawy z zagrożeń wynikających z udostępniania nieznajomym ogromnej ilości informacji na temat swojego prywatnego życia oraz że są narażone na nieodpowiednie treści, np. nawołujące do przemocy lub o charakterze seksualnym.

Problemem Facebooka jest brak filtrów ograniczających wiadomości nieodpowiednie dla młodych osób. Warto również pamiętać, że nieznani nam „znajomi" mogą mieć ogromny wpływ na to, jakie informacje docierają do dziecka. Oczywiście możemy blokować użytkowników i aplikacje, które prezentują treści nieodpowiednie dla naszych dzieci – jednak dopiero po fakcie, gdy zorientujemy, że stanowią zagrożenie.

Eksperci zalecają rodzicom, aby zakładali swoim dzieciom konto na Facebooku jak najpóźniej. Kiedy jednak już to nastąpi, warto przestrzegać poniższych rad.

- Co jakiś czas przejrzyj profil dziecka, sprawdzając, czy nie ujawnia na nim poufnych informacji, takich jak adres domowy, nazwa szkoły, numer telefonu, zbyt osobiste zdjęcia lub filmy.
- Porozmawiaj z dzieckiem o nowych znajomych pojawiających się na jego liście kontaktów, szczególnie gdy ich nie znasz. Postaraj się wyjaśnić dziecku, dlaczego rozmowa o jego nowych znajomych jest ważna.
- Sprawdź, jakie aplikacje i gry Twoje dziecko zainstalowało oraz zorientuj się, jakiego rodzaju informacje one gromadzą.
- Porozmawiaj z dzieckiem na temat ustawień prywatności i upewnij się, że treści, które ujawnia, trafiają tylko do grona jego znajomych, nie stają się publiczne.
- Pokaż dziecku, jak zablokować niechciane kontakty. Wyjaśnij, jak zgłosić moderatorowi niestosowne i obraźliwe posty.
- Pokaż dziecku, jak przeglądać zdjęcia, na których zostało oznaczone oraz gdzie w ustawieniach można tę funkcję całkowicie zablokować.
- Porozmawiaj z dzieckiem o cyberprzemocy, jak ją rozpoznawać i jak jej unikać.
- Naucz dziecko rozpoznawać fałszywe wiadomości i oferty, tworzone w celu generowania kliknięć oraz profile przeznaczone do zbierania lajków.
- Używaj oprogramowania do monitorowania aktywności Twojego dziecka w mediach społecznościowych.

10 wskazówek, dzięki którym każdy, nawet najmniej doświadczony użytkownik będzie mógł czuć się bezpieczniej podczas korzystania z portalu Facebook.

1. Zastanów się kogo 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.

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.

Zgodnie z regulaminem Facebooka użytkownik nie może wykorzystywać jego produktów do wykonywania czynności ani udostępniania treści, które: naruszają prawa innej osoby, w tym jej prawa własności intelektualnej.
Facebook może usunąć lub zablokować treści, które naruszają powyższe postanowienie.