Korzystanie z aplikacji mobilnych, a bezpieczeństwo najmłodszych użytkowników

Większość z nas korzysta z aplikacji mobilnych na co dzień. Ułatwiają życie, służą do kontaktu z najbliższymi, dostarczają rozrywki. Popularność urządzeń z interfejsem dotykowym sprawia, że aplikacje mobilne stają się coraz prostsze w obsłudze. Interfejs wielu z nich pozwala na intuicyjną nawigację najmłodszym użytkownikom – nawet tym, którzy nie potrafią jeszcze czytać i pisać. Technologie, które zachęcają atrakcyjnymi kolorami, dźwiękami stały się popularne wśród dzieci i nastolatków, którzy poświęcają im coraz więcej czasu. Aplikacje najczęściej dostarczają rozrywki w postaci gier, zabaw edukacyjnych lub są mobilnymi wersjami serwisów (np. społecznościowych), często też funkcje te przenikają się.

Wiele z treści nielegalnych lub szkodliwych zgłaszanych przez użytkowników internetu do zespołu Dyżurnet.pl znajduje się w popularnych aplikacjach. Dlatego ważne, aby każdy użytkownik miał świadomość możliwych zagrożeń. Niestety mało osób wie, jakie niebezpieczeństwa mogą płynąć z nieodpowiedzialnego korzystania z aplikacji mobilnych oraz z korzystania z aplikacji nieodpowiednich dla wieku odbiorcy.

Dzieci zachęcone popularnością aplikacji wśród rówieśników lub dostępnością do treści kreowanych przez influencerów, atrakcyjnością produktu czy kierowane ciekawością niechętnie przyjmują nakładane ograniczenia wiekowe i zawyżają wiek, zakładając profile i omijając zabezpieczenia. Niestety mała świadomość opiekunów na temat zagrożeń oraz tego, w jaki sposób prawidłowo konfigurować urządzenia i profile, aby ograniczyć kontakt z nieodpowiednimi treściami lub innymi użytkownikami, wpływa na to, że dzieci i młodzież korzystają z aplikacji przeznaczonych dla starszych grup wiekowych z biernym przyzwoleniem rodziców.

Wiele z popularnych aplikacji dostarcza użytkownikom dużej dawki rozrywki oraz możliwości poznania osób o podobnych zainteresowaniach, a czasami po prostu służy do przyjemnego spędzenia czasu. Poza pozytywnymi i wartościowymi materiałami, jakie możemy znaleźć w każdej z nich, możemy trafić również na nieodpowiednie materiały. Jest to ryzyko, jakie pociąga za sobą każda platforma dająca możliwość tworzenia contentu użytkownikom. Dlatego tak ważne jest, żebyśmy byli świadomi zagrożeń oraz konsekwencji naszych zachowań online.

Na co może narazić najmłodszego użytkownika korzystanie z nieodpowiednich aplikacji?

- kontakt z nieodpowiednimi – szkodliwymi i nielegalnymi treściami,
- kontakt z niebezpiecznymi osobami,
- dystrybucja materiałów przedstawiających dziecko w nieodpowiednim kontekście,
- ujawnienie i wyciek prywatnych informacji,
- utrwalanie niebezpiecznych zachowań i nawyków,
- nadużycia finansowe,
- zagrożenia związane z cyberbezpieczeństwem.

Dofinansowane przez Unię Europejską

dyżurnet.pl NASK

saferinternet.pl

Jak chronić młode osoby?

Młody użytkownik aplikacji posiadający dobry kontakt z bliskimi dorosłymi jest mniej narażony na negatywne konsekwencje trudnych sytuacji w sieci czy nawiązanie zastępczej relacji z nieznajomym poznanym w internecie. Wielu sieciowym zagrożeniom można starać się zapobiegać przy wykorzystaniu nowoczesnych narzędzi technologicznych, chociaż nie zawsze są one w pełni skuteczne i nie należy opierać działań zapobiegawczych tylko na nich. Pamiętajmy o zachowaniu szczególnej ostrożności przy publikowaniu prywatnych treści o nas - nie każde wydarzenie z życia musi być pokazywane online lub prezentowane w czasie rzeczywistym. Szczególna ostrożność powinna być zachowana, jeśli aplikacja umożliwia kontakt z nieznajomymi użytkownikami.

Na co warto zwrócić uwagę:

- jakie korzyści przyniesie korzystanie z aplikacji,
- w jaki sposób aplikacja jest prezentowana w sklepie oraz czy prezentowane informacje są pełne i odpowiednie,
- czy jest możliwe wyłączenie powiadomień i innych informacji wyświetlanych podczas gdy nie używamy aplikacji,
- czy możliwy jest kontakt z nieznajomym – każdego, nie tylko młodego użytkownika, może narażać to na niebezpieczeństwo, ponieważ zachowanie innych użytkowników bywa nieprzewidywalne,
- w jaki sposób weryfikowana jest tożsamość użytkowników zakładających konta – jeśli dane są jedynie deklaratywne, może to prowadzić do kontaktu użytkownika z osobami, które nie są tymi, za kogo się podają,
- kto ma dostęp do udostępnianych materiałów – nigdy nie można mieć pewności, jak zostaną wykorzystane przez innych materiały opublikowane w serwisie. Wrzucając materiał do sieci, użytkownik traci nad nim kontrolę,
- kto ma dostęp do informacji (i jakich informacji) o użytkowniku – dostęp do zbyt wielu informacji ułatwia użycie ich w sposób niewłaściwy, zagrażający prywatności,
- jakiego typu materiały zawiera aplikacja – te, które opierają się na materiałach tworzonych i udostępnianych przez użytkowników zawsze stwarzają zagrożenie, że znajdą się tam treści niewłaściwe lub prezentujące zachowania szkodliwe. W grach warto zwrócić uwagę na to, czy np. jest dostępny czat między użytkownikami i jaka panuje kultura wypowiedzi lub czy po wpisaniu kodu są dostępne treści erotyczne,
- czy każdy może publikować materiały dostępne dla innych użytkowników i czy przechodzą one weryfikację – ważne jest również to, czy każdy użytkownik może udostępniać wytworzony przez siebie materiał, ponieważ może to generować ryzyko kontaktu z treściami szkodliwym lub niewłaściwymi dla młodszych użytkowników, które niekoniecznie muszą być nielegalne (np. patostreamy , wulgarne zachowania i wypowiedzi, przemoc, nadużywanie alkoholu),
- jakie dostępy uzyskuje aplikacja/gra i czy są one uzasadnione – niektóre aplikacje i gry proszą o nadanie dostępu do funkcji naszego urządzenia, który jest nieuzasadniony. Mogą być to dostępy do aparatu, multimediów, geolokalizacji, kamery itp.,

Dofinansowane przez Unię Europejską

dyżurnet.pl NASK

saferinternet.pl

- jakie informacje o użytkowniku gromadzi gra/aplikacja – najczęściej opis informacji gromadzonych przez grę/aplikację znajdziemy w Polityce Prywatności; warto mieć świadomość, czy poprzez aplikację przekazywane są informacje o wyszukiwaniach w internecie, otoczeniu, lokalizacji użytkownika,
- w jaki sposób zabezpieczone są płatności – jakie są zabezpieczenia w przypadku dokonywanych płatności, aby uniknąć tych niechcianych i nie narażać się na straty finansowe,
- czy jest możliwość zgłoszenia niewłaściwych treści/zachowań – jeśli aplikacja lub gra umożliwia kontakt użytkowników ze sobą lub zezwala na udostępnianie treści przez użytkowników, zawsze powinna znajdować się w niej opcja zgłoszenia niewłaściwych zachowań czy materiałów,
- czy gra lub aplikacja zawiera linki pozwalające na jej opuszczenie – np. reklamy dostępne na platformie mogą przekierowywać do treści szkodliwych dostępnych poza aplikacją/grą (np. reklamy gier 18+ zamieszczane w grach dla młodych użytkowników),
- czy wiek użytkownika jest w jakiś sposób weryfikowany – warto sprawdzić, czy aplikacja poza zapisem w Polityce prywatności/Regulaminie prosi o wpisanie daty urodzenia,
- czy w aplikacji występują filtry/opcje upiększenia – może to być szkodliwe, ponieważ zakrzywia obraz rzeczywistości. W serwisie postrzegamy wszystko jako piękne i idealne, a jest to zasługą zastosowania odpowiednich filtrów. Kontakt z takimi materiałami może prowadzić do obniżenia samooceny i pewności siebie.

Zawsze warto zapoznać się z Regulaminem i Polityką Prywatności przed instalacją gry lub aplikacji, ponieważ to właśnie tam znajduje się większość odpowiedzi na pytania dotyczące poziomu bezpieczeństwa aplikacji. Jeśli gra lub aplikacja jest np. dozwolona od 13. roku życia, nie należy instalować jej młodszemu dziecku, ponieważ oznacza to, że prawdopodobnie zawiera ona treści nieodpowiednie dla użytkownika poniżej 13 r. ż. PEGI i zapisy w regulaminach są tworzone z myślą o bezpieczeństwie użytkownika, więc nie należy ich bagatelizować.

Dofinansowane przez Unię Europejską

dyżurnet.pl NASK

saferinternet.pl