NASK dyżurnet.pl

APLIKACJE MOBILNE
– CZY NASZE DZIECI SĄ BEZPIECZNE

Wydawca

NASK Państwowy Instytut Badawczy

ul. Kolska 12

01-045 Warszawa

e-mail: info@nask.pl, info@dyzurnet.pl

Tekst: Martyna Różycka, Oliwia Chojnacka, Katarzyna Trojanowska

Korekta: Anna Maria Hernik-Solarska

Opracowanie graficzne: Julia Zdancewicz

Szanowni Państwo,

Zespół Dyżurnet.pl powstał w 2005 roku w NASK i od 2018 roku realizuje zadania CSIRT NASK zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa. Państwowy Instytut Badawczy NASK od lat podejmuje szereg inicjatyw na rzecz budowania bezpiecznego internetu. W związku z obserwowanym na przestrzeni lat dynamicznym rozwojem technologicznym, a co za tym idzie również rozwojem aplikacji mobilnych, postanowiliśmy przyjrzeć się bliżej kilku z nich, tym najbardziej popularnym. Każdy z nas, a zwłaszcza młodzi użytkownicy, wiąże swoje codzienne aktywności z aplikacjami służącymi do różnych celów — rozrywki, edukacji, wyrażania siebie, kontaktu ze znajomymi itp. Zdarza się, że obok wartościowych i rozwijających treści, możemy natknąć się na materiały w jakiś sposób szkodliwe lub niewłaściwe, a czasami nielegalne. Ważnym aspektem bezpiecznego korzystania z aplikacji jest świadomość możliwych zagrożeń, którą chcemy zwiększać poprzez przekazanie informacji zawartych w poniższym raporcie.

Szczególne wyrazy uznania i podziękowania za inspirujące spotkania oraz rozmowy dotyczące bezpieczeństwa aplikacji kierujemy do ekspertów, kolegów i koleżanek z NASKu, którzy podzielili się z nami swoją wiedzą z wielu poziomów.

Zapraszamy do lektury!

Zespół Dyżurnet.pl

Spis treści

Wstęp

Jednym z głównych znaków czasów współczesnego świata jest wirtualizacja otaczającej nas rzeczywistości, która przyspieszyła wraz z rozwojem internetu i przerodziła się w „wyścig zbrojeń" projektów i firm tworzących multimedialną płaszczyznę XXI wieku. Rozwój tego trendu wspieranego przez nasilające się zjawisko konwergencji medialnej[1] oraz miniaturyzację technologii cyfrowych, doprowadził do powstania aplikacji mobilnych, których ogólnym celem jest umożliwienie ludziom dostępu do rozrywki oraz globalnej interakcji społecznej, przy równoczesnym dążeniu, by mogli oni korzystać z tych możliwości niezależnie od miejsca i czasu.

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, którzy nawet nie potrafią 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 (edutainment) lub są mobilnymi wersjami serwisów (np. społecznościowych), często też pozwalają na przenikanie się funkcji.

Dlatego korzystanie z aplikacji i ich funkcjonalności umożliwia zaspokajanie potrzeb na różnych poziomach, takich jak potrzeba przynależności, potrzeba kontaktu z innymi czy potrzeba ekspresji. Pod tym względem najmłodsi nie różnią się od dorosłych i dlatego chętnie sięgają po produkty, które zaspokajają ich potrzeby. Dodatkowo dzieci zachęcone popularnością aplikacji, atrakcyjnością produktu czy kierowane ciekawością niechętnie przyjmują nakładane ograniczenia wiekowe i zawyżają wiek zakładając profile i omijając zabezpieczenia. Niestety mała świadomość opiekunów na temat tego w jaki sposób prawidłowo konfigurować urządzania 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, na podstawowych ustawieniach, czyli takich, które nie chronią młodszych użytkowników przed niewłaściwymi dla nich treściami.

Korzystanie z nieodpowiednich aplikacji może narazić najmłodszego użytkownika na zderzenie się z zagrożeniami takimi jak:

- kontakt z nieodpowiednimi – szkodliwymi i nielegalnymi treściami
- kontakt z niebezpiecznymi osobami
- dystrybucje materiałów przedstawiających dziecko w nieodpowiednim świetle
- ujawnienie i wyciek prywatnych informacji
- utrwalanie niebezpiecznych zachowań i nawyków
- nadużycia finansowe
- zagrożenia związane z cyberbepieczeństwem

1 Henry Jenkins, 2007, Kultura konwergencji. Zderzenie starych i nowych mediów, Wydaw. Akad. i Profesjonalne, Warszawa
2 Raport z badań „Nastolatki 3.0", Warszawa

Wybór aplikacji, z której może korzystać dziecko nie jest łatwy dla jego opiekunów. Atrakcyjny interfejs, popularność wśród rówieśników, brak czasu i niskie kompetencje cyfrowe rodziców – to sytuacje, które sprawiają, że aplikacja przed instalacją właściwie nie przechodzi żadnej oceny ze strony rodziców. Często też w przypadku młodszych dzieci, a bardzo często wśród nastolatków, zdarza się, że dziecko samo je instaluje bez wiedzy i zgody rodzica. Badania pokazują, że ponad 65% dzieci nie ma ustalonych przez rodziców/opiekunów zasad korzystania z internetu dotyczących czasu spędzanego w sieci czy treści oglądanych w internecie[2].

Sytuacja ta stawia trudne wyzwania dotyczące konieczności nabycia przez rodziców, opiekunów i edukatorów odpowiedniej wiedzy i świadomości, na temat zagrożeń w „sieci" oraz podjęcia odpowiedzialności za bezpieczeństwo dzieci i młodzieży w tym wymiarze. Z drugiej strony konieczne jest również wzięcie odpowiedzialności za bezpieczeństwo dzieci i nastolatków przez twórców aplikacji oraz producentów urządzeń końcowych.

Działanie na rzecz bezpieczeństwa w internecie oraz technologiach powinno stanowić współdziałanie:

- dzieci i młodzieży — którzy mają prawo do zaspokajania swoich potrzeb oraz ich wyrażania; wymagają wsparcia w przypadku wystąpienia nadużyć; mogą być łącznikiem pomiędzy młodszymi grupami odbiorców oraz pozostałymi grupami;
- opiekunów – którzy najlepiej rozumieją potrzeby swoich dzieci; reagują na bieżąco na niepokojące sytuacje; działają w imieniu dziecka i na rzecz ochrony jego praw;
- edukatorów i badaczy – którzy rozumiejąc aktualną sytuację, zauważając oraz analizując trendy i zjawiska; przeciwdziałając zagrożeniom mogą wskazywać pojawienie się nowych zagrożeń oraz przygotowują rekomendacje;
- przedstawicieli branży technologicznej – którzy rozumiejąc i kształtując rozwój technologiczny, stawiają bezpieczeństwo użytkowników na pierwszym miejscu oraz wdrażają środki zapobiegawcze nadużyciom oraz mechanizmy ograniczające ich wpływ; monitorują bieżącą sytuację wdrażając koniecznie zmiany;
- instytucje regulujące – opracowują odpowiednie regulacje oraz monitorują ich zastosowanie; stoją na straży ochrony praw dzieci i ich opiekunów.

Jakie są cele tego raportu?

Podstawowym celem raportu jest wskazanie ogólnych potencjalnych zagrożeń oraz zasad bezpieczeństwa korzystania z aplikacji mobilnych przez dzieci i młodzież.

Drugim ważnym celem było stworzenie rekomendacji dla opiekunów, na co powinni zwracać szczególną uwagę, podczas sprawdzania, czy dana aplikacja jest dostosowana do wieku ich podopiecznych. By to osiągnąć twórcy raportu postanowili przebadać i przeanalizować szereg aplikacji z różnych perspektyw (o czym więcej informacji znajduje się rozdziale poświęconym metodyce badania).

Trzecim celem było stworzenie rekomendacji dla twórców aplikacji wskazującej na co powinni zwrócić szczególną uwagę dostosowując aplikację do wieku jej użytkowników oraz w jaki sposób powinni ostrzegać, jeśli aplikacja nie jest przeznaczona dla użytkowników poniżej jakiegoś wieku.

Do kogo skierowany jest ten raport?

Raport, z jednej strony skierowany jest do rodziców, edukatorów i opiekunów dzieci i nastolatków, z drugiej strony również do twórców aplikacji mobilnych, dla których może być bazą do tworzenia w przyszłości aplikacji bezpiecznych już na poziomie projektowania. Raport ma również na celu rozpoczęcie szerszej dyskusji na temat bezpieczeństwa aplikacji mobilnych przeznaczonych dla dzieci i młodzieży.

Metodyka badania

Wybór aplikacji do badania

Wybór aplikacji do badania był podyktowany popularnością aplikacji wśród dzieci i młodzieży w oparciu o dostępne dane z platformy Google Play oraz wybór ekspertów Dyżurnet.pl, którzy uznali konieczność przeglądu niektórych z aplikacji, dostępnych w sklepie Google Play, ze względu na ich wzrastającą popularność.

Kryterium popularności jest szczególnie ważne ze względu na to, że najmłodsi użytkownicy chętnie korzystają z produktów, które są przeznaczone dla starszych grup wiekowych, a nie tylko aplikacji skierowanych do dzieci lub młodzieży. Dlatego też badanie objęło nie tylko takie aplikacje, które są tworzone z myślą o najmłodszych i znajdują się w odpowiednich kategoriach w sklepach z aplikacjami, ale takie, z których faktycznie dzieci korzystają.

Wiek odbiorcy aplikacji

W badaniu zachowano podział wiekowy proponowany przez PEGI[3] — 3, 7, 12, 16 i 18 ze względu na utrwalony już model i powielony przez platformę Google Play. Oznaczenia PEGI mają na celu skategoryzowanie grupy wiekowej dla jakiej produkt jest przeznaczony oraz wskazania, jakie treści mogą się w nim znajdować (przemoc, wulgarny język, używki itp.). Stosowanie kategorii „dla dzieci" (osoby poniżej 18 roku życia) jest też zbyt ogólne i nieodpowiednie, ponieważ aplikacja bezpieczna dla odbiorcy od wieku 16 lat nie jest automatycznie bezpieczna dla młodszych dzieci.

3 https://pegi.info/pl

Należy zaznaczyć, że przy pobieraniu aplikacji (w Google Play) nie zawsze jest zamieszczona informacja dla jakiej grupy wiekowej jest ona skierowana. Jeśli nie podano kategorii wiekowej w sklepie to należy jej szukać w polityce prywatności aplikacji lub regulaminie – dokumenty są zazwyczaj dostępne bez konieczności pobierania aplikacji.

Producenci aplikacji, podobnie jak i innych produktów przeznaczonych dla dzieci, dają jedynie wskazówkę opiekunom, uśredniając gotowość odbiorców w danym wieku. Natomiast do opiekunów należy ostateczny wybór korzystania z serwisu lub usługi. Dobre rozeznanie w cechach produktu, które skłoniły producenta do wyboru kategorii wiekowej powinny być jasne dla wszystkich konsumentów na każdym etapie korzystania z produktu.

Sposób badania

Aplikacje były badane empirycznie, gdzie szczególną uwagę zwrócono na wrażenia użytkownika oraz łatwość dostępu do informacji. Sprawdzeniu podlegały wszelkie dokumenty zawarte w aplikacji mówiące o skali dostępów jakie uzyskuje oraz kwestii dotyczących materiałów w niej zawartych, takich jak zasady społeczności. Każdorazowo aplikacje były sprawdzane ręcznie w celu jak najwierniejszego oddania sposobu użytkowania aplikacji przez użytkownika.

Badania przeprowadzono według z góry ustalonego przez testera schematu. Badanie podzielono na fazy.

01

Faza I
Pierwszym krokiem było przeprowadzenie rozpoznania budowy systemu. W ramach tej fazy zidentyfikowano i opisano przeznaczenie szczegółowych funkcjonalności aplikacji mobilnych dostępnych z poziomu interfejsu użytkownika oraz opisano metadane aplikacji.

02

Faza II
Drugim krokiem badania była analiza pliku AndroidManifest.xml oraz analiza kodu źródłowego aplikacji. W ten sposób zweryfikowano zakres i zasadność uprawnień przyznawanych aplikacji. Uprawnienia zostały opisane i każdemu z nich przypisano poziom ochrony, który mógł przyjąć jedną z dwóch wartości – normalny, niebezpieczny.

03

Faza III
Kolejnym krokiem była ocena poziomu kontroli ustawień i prywatności jakie zapewnia aplikacja. Jako, że oprogramowanie badane było pod kątem użytkowania przez osobę nieletnią wzięto pod uwagę szereg scenariuszy jak, np.: czy aplikacja wymaga podania wieku użytkownika (jeżeli tak, czy możliwe jest korzystanie przez osoby poniżej 13 roku życia), jakie dane na temat użytkownika są zbierane, czy dane są powszechnie dostępne, czy można ograniczyć kontakt użytkownika z innymi (np. dorosłymi) użytkownikami, czy istnieje możliwość kontroli nad zebranymi danymi – usunięcia/edycji.

Obszary bezpieczeństwa

W badaniu zostało wyłonionych kilka **Obszarów Bezpieczeństwa** zwracając tym samym uwagę na wiele aspektów, które powinny być brane pod uwagę przy ocenie aplikacji i wyborze konsumenta.

Pierwszy obszar, który został poddany badaniu ma na celu sprawdzenie, jakie **informacje o aplikacji są dostępne w sklepie** Google Play. Bardzo ważna jest prawidłowość i kompletność podanych informacji, ponieważ pozwala to na dokonanie właściwego wyboru.

nieodpowiednia prezentacja aplikacji

Nieprawdziwe informacje prezentujące aplikację w sklepie wprowadzają w błąd użytkowników. Odpowiednia klasyfikacja oraz identyfikacja wizualna pozwala na ograniczenie widoczności produktów przeznaczonych dla innych kategorii wiekowych niż ta, do której należy użytkownik.

Odpowiednia prezentacja pozwala na prawidłowe zapoznanie się z aplikacją bez potrzeby instalacji.

brak kontaktu z developerem

Utrudniony kontakt z developerem może wskazywać na nieodpowiedzialnego producenta, dla którego nie mają znaczenia negatywne doświadczenia klientów.

Drugi z aspektów, który został wzięty pod uwagę w badaniu, **dotyczy treści** znajdujących się w aplikacji. Znaczna część badania jest spójna z klasyfikacją PEGI, która nakazuje, aby była dostępna informacja o treściach, takich jak używki, seks, przemoc. Należy jednak zwrócić uwagę, że klasyfikacja PEGI pierwotnie opracowana dla gier, nie zawsze będzie wygodna i odpowiednia do stosowania dla innych typów aplikacji. Szczególną uwagę należy zwrócić, czy produkt pozwala na kontakt z innymi użytkownikami oraz na rodzaj treści, które taki przekaz może zawierać.

Szkodliwe filtry dostępne w aplikacjach

Szczególną uwagę należy zwrócić na dostępność w aplikacjach społecznościowych filtrów upiększających i sposób ich oznaczenia. Niektóre aplikacje już zdecydowały się na wprowadzenie oznaczeń na materiałach, które zostały edytowane przez użycie dostępnych w aplikacji filtrów. Szkodliwość stosowania filtrów upiększających opiera się głównie na przedstawieniu jako prawdziwy wyidealizowanego świata, życia oraz wyglądu co może mieć wpływ

na pogorszenie samooceny wśród osób, szczególnie młodych, korzystających z aplikacji — nadmierne przywiązanie do wizerunku, fizyczności, uzależnienie wiary w siebie i poczucia wartości od opinii innych oraz uzależnienia behawioralne mogą mieć negatywny wpływ na młodą osobę. Najczęściej jednak nie są stosowane żadne oznaczenia mówiące o tym czy i jaki filtr został zastosowany przy obróbce materiału.

treści tworzone przez użytkownika – nieweryfikowane przed publikacją; linki pozwalające na wyjście z aplikacji; aplikacja może wpływać na postrzeganie siebie (filtry, upiększenia); możliwy kontakt z nieznajomymi.

hiperłącza przenoszące poza aplikację

Szczególnie młodsi użytkownicy aplikacji powinni być chronieni przed przypadkowym wyjściem z aplikacji, co może wpłynąć na kontakt z nieodpowiednimi treściami, dokonywaniem zakupów, a nawet przypadkową zmianą ustawień na urządzeniu.

Kolejnym obszarem badanym był **Obszar interfejsu** — najtrudniejszy poziom do oceny przez dorosłego badacza należy bowiem ocenić jak z produktu korzystają młodsi użytkownicy. Dokładniejsze poznanie tego poziomu wymaga pogłębionych badań z odpowiednią grupą odbiorców, podczas których będzie można ocenić intuicyjność dla danej grupy wiekowej. Mając na uwadze konieczność oceny obszaru interfejsu, zespół kierował się głównie wytycznymi opracowanymi przez innych badaczy i dostępnych w literaturze przedmiotu (Sonia Livingstone i inni[4] ; Elizabeth McClure i in.[5]).

Obszar zachowań jest jednym z najważniejszych aspektów badania. Zachowania, których aplikacja uczy lub utrwala, mogą być szczególnie szkodliwe dla młodego odbiorcy. Korzystanie z niej może wpłynąć na to, jak użytkownik postrzega siebie, na jego poczucie własnej wartości czy krytyczne myślenie.

Innym aspektem, który został wzięty pod uwagę w badaniu jest wspieranie zachowań i nawyków hazardowych jako bezdyskusyjnie nieodpowiednich dla najmłodszych. Ważnym elementem obszaru zachowań było zbadanie czy aplikacja wspiera uzależnienie od samego produktu, które może być niebezpieczne i szkoldliwe dla użytkownika. Oceniono czy aplikacja żąda, aby użytkownik w określonym czasie musiał z niej skorzystać nie pozostawiając wyboru co do tej kwestii jej użytkownikowi.

Żądanie wykonania odpowiedniej czynności wymaga, aby dziecko dostosowało do aplikacji rytm swojego dnia bazując na możliwości poczucia straty poprzez niewykonanie konkretnego działania i utratę, np. punktów. W ten sposób wzmacniane jest wyrobienie nawyku częstego korzystania z aplikacji, które jest narzucone przez twórców, a nie regulowana przez samego użytkownika oraz przywiązanie do aplikacji. Długotrwałe budowanie postaci czy świata ma oczywiście również pozytywne aspekty, jednak nie powinno się to odbywać na zasadzie przymusu.

4 Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G. and Ólafsson, K. (2014). Net Children Go Mobile: The UK Report. London: London School of Economics and Political Science.

5 McClure, E., Vaala, S., Spiewak Toub, T., (2017) A Quick Report Discovering kids' apps Do family strategies vary by income? The Joan Ganz Cooney Center

rytm korzystania wyznaczony przez aplikację

Narzucenie rytmu korzystania – pora dnia, liczba logowań w ciągu dnia, powiadomienia, brak zastopowania, brak możliwości przewidzenia długości używania — wzmacniają uzależnienia oraz brak kontroli nad używaniem produktu.

Kolejnym niezwykle ważnym elementem są **powiadomienia**, które pojawiają się, gdy użytkownik nie korzysta z aplikacji. Aplikacja powiadamia użytkownika, gdy z niej nie korzysta o nowych funkcjonalnościach, zadaniach do wykonania lub informacjach od innych użytkowników. **Każdy produkt powinien mieć możliwość wyłączenia powiadomień, ponieważ w momencie pojawienia się ich, wymuszają one interakcję ze strony użytkownika, rozpraszają go i „odwołują" od wykonywanej czynności. Ciągłe otrzymywanie powiadomień może mieć destrukcyjny charakter (wzmacniać poczucie FOMO), rozpraszać.**

Szczególnie niebezpieczna dla użytkownika może być możliwość kontaktu z nieznajomym. Każda z usług, która umożliwia kontakt z osobami nieznajomymi, powinna być szczególnie uważnie sprawdzona przez opiekunów. Kontakt może przybierać różne formy:

- od najmniej inwazyjnego – np. pokazującego ranking graczy;
- po kontakt pośredni – gdzie widać aktywności innych, ale nie ma możliwości bezpośredniego kontaktu lub może się on odbyć przy zaistnieniu konkretnych okoliczności;
- aż do pełnego kontaktu z innymi, którzy mogą przesyłać tekst, zdjęcia, filmy, naklejki itp. lub nawiązywać kontakt głosowy.

Należy podkreślić, że każda „widoczność" innych użytkowników może prowadzić do zagrożeń – użytkownicy mogą np. używać wulgarnych i nieodpowiednich dla młodszych osób nazw postaci lub swojego profilu.

Inną kategorię stanowią aplikacje, które umożliwiają bezpośrednią komunikację między użytkownikami. Tutaj też można wyodrębnić kilka ich rodzajów – posiadające „książkę telefoniczną" lub krąg „znajomych" – te umożliwiają kontakt pod warunkiem, że inny użytkownik został już zaakceptowany. W ten sposób najczęściej pozostaje ślad konwersacji. Ustawienia prywatności, którym rodzice powinni poświęcić specjalną uwagę, muszą być łatwo dostępne i zrozumiałe. W tym miejscu kluczową rolę stanowi rola platform i developerów, aby ustawienia były czytelne dla dzieci i nastolatków, ale również konta młodych użytkowników miały domyślnie przypisane najwyższe formy ochrony prywatności.

Zagrożenie może stanowić również łączenie informacji z różnych platform. **Każde połączenie różnych tożsamości w internecie pokazuje nowe obszary informacji o dziecku, co ułatwiać może osobom o złych zamiarach lepsze poznanie potencjalnej ofiary.** Zakładając, że niebezpieczna osoba pozna profil ofiary na portalach społecznościowych, identyfikując zainteresowania i hobby, rytm dnia czy sposób funkcjonowania w grupie jest w stanie wykorzystać te informacje w sposób zagrażający dziecku.

łączenie tożsamości pomiędzy platformami

Wpływa na ujawnianie większej ilości informacji o użytkowniku; pozwala na transfer kanału komunikacji między użytkownikami

Obszar e-commerce

nieodpowiedni marketing

Młodzi użytkownicy są również konsumentami i adresatami kampanii marketingowych, chociaż nie rozumieją charakteru reklamy i nie potrafią go odróżnić od przekazu neutralnego.

Część aplikacji (aplikacje produktowe) powstały w celu podtrzymywania relacji pomiędzy użytkownikiem a produktem, którego jest nośnikiem. Niestety, niektórzy użytkownicy ze względu na zbyt małą świadomość mechanizmów marketingowych mogą nie rozpoznać przekazu reklamowego od innego, np. informacyjnego. Użytkownicy chętnie oglądają przyciągające wzrok reklamy video, ale nie zawsze rozumieją wpływ reklamy na dokonywanie wyborów konsumenckich.

Obszar prywatności i poziom ustawień

Wszystkie usługi udostępniane na telefonie powinny zwracać szczególną uwagę na **zagadnienia związane z prywatnością**. Jest to wyjątkowo ważne w przypadku urządzeń, z których korzysta jedna osoba i ma je przez większość czasu przy sobie. Zbierane dane mogą powiedzieć bardzo dużo o ich właścicielu, gdzie przebywa, jak często, jakie są jego różne preferencje, w jaki sposób korzysta z urządzenia. **Dlatego priorytetem powinna być prywatność rozumiana na dwóch poziomach: jakich informacji wymaga aplikacja do poprawnego działania oraz jakie informacje zbiera czy przetwarza w tle i czy jest to zgodne z podanymi oficjalnie informacjami.**

ujawnianie prywatnych informacji

Funkcjonalności, które w atrakcyjny sposób zachęcają użytkownika do udostępnienia prywatnych informacji takich jak numer telefonu czy geolokalizacja mogą prowadzić do naruszeń, a nawet niebezpieczeństwa w świecie rzeczywistym.

Zachęcanie do upubliczniania informacji wrażliwych takich jak geolokalizacja lub nawet „zameldowania" w popularnych miejscach, nie powinno być dostępne w aplikacjach przeznaczonych dla młodszych grup wiekowych, a nawet młodzieży.

Często aplikacje społecznościowe pozwalają na informowanie innych użytkowników o posiadaniu profilu już na poziomie książki kontaktów w telefonie. Jest to wygodne rozwiązanie pod warunkiem, że numer telefonu dziecka nie zostanie przekazany w niepowołane ręce. Pedofile oraz inne osoby o niebezpiecznych intencjach komunikują się ze swoimi ofiarami za pomocą różnych platform, wybierając szczególnie te, które pozwalają na utajoną komunikację, która nie jest zapisywana i zachowywana.

Niezwykle ważne jest dbanie o prywatność i możliwości korzystania z usług jakie zapewnia serwis. Balans pomiędzy łatwością znalezienia znajomych, a dbaniem o prywatność użytkowników, szczególnie tych młodszych, powinien być przechylony w stronę dbania o bezpieczeństwo. To, co powinno zwrócić szczególną uwagę użytkownika decydującego się na korzystanie z aplikacji to również możliwość zgłaszania nadużyć i przekazania informacji do moderacji. Szczególny nacisk powinien być położony na intuicyjność i szybkość procesu oraz responsywność ze strony administratora.

Przy różnego rodzaju nadużyciach bardzo ważne są funkcje, które z łatwością pozwalają na zapisanie i zarchiwizowanie komunikacji, zgłoszenia do platformy lub przekazania powiadomienia do rodziców.

Duża ilość gromadzonych przez aplikacje danych może stwarzać ryzyko wycieku danych wrażliwych użytkownika. Kolejny problem może stanowić weryfikacja wieku użytkownika, która w większości przypadków ogranicza się do pytania o datę urodzenia – co w opinii zespołu badawczego jest mało wiarygodnym sposobem zapobiegania korzystania z aplikacji przez osoby poniżej dozwolonego wieku.

Na podstawie przeprowadzonych badań stwierdzono, że aplikacje zbierają ogromną ilość danych na temat użytkownika. Do opisu zgromadzonych informacji sklasyfikowano je w czterech grupach:

- **Grupa I – Dane profilowe**

Dane na temat użytkownika, takie jak imię, nazwisko, płeć, data urodzenia, wiek, numer telefonu komórkowego, adres email, dane na temat pracy, skończonej szkoły, lokalizacja.

- **Grupa II – Aktywność użytkownika**

Wszelkie działania podejmowane w aplikacji. W przypadku grupy Social Media są to publikowane posty, prywatne wiadomości (nawet te skasowane), polubione, zapisane, skomentowane oraz udostępnione materiały, lista znajomych (jak również lista zablokowanych użytkowników, lista wysłanych zaproszeń do znajomych, lista otrzymanych zaproszeń), historia wyszukiwania, opublikowane multimedia (zdjęcia, filmy, nagrania), zapisane mutlimedia.

- **Grupa III – Dane techniczne**

Dane na temat urządzenia, bądź technicznych aspektów korzystania z aplikacji. Są to miedzy innymi: adres IP, ID telefonu, User-Agent, historia logowania, informacje na temat rejestracji. Dla przykładu przedstawiono dane wyjęte z jednego z plików JSON na temat aktywności użytkownika (przykład 1) oraz rejestracji użytkownika (przykład 2).

```
{
„cookie_name”: „**********Csc”,
„ip_address”: „xxxx:yyy:zzzz:aaaa:bbbb:cccc:1111:2222”,
„language_code”: „pl”,
„timestamp”: „2020-06-22T09:56:48+00:00”,
„user_agent”: „Appname xxx.x.x.xx.xxx Android (26/8.0.0; 640dpi; 1440x2768; samsung; SM-G960F; starlte; samsungexynos9810; pl_PL; 221134032)”,
„device_id”: „android-abcde”
},
```


Przykład 1


```
{
 „registration_username”: „Kamil Kowalski „,
 „ip_address”: „12.23.34.243”,
 „registration_time”: „2017-09-30T16:02:37+00:00”,
 „registration_email”: „”,
 „registration_phone_number”: „+48 999999999”,
 „device_name”: „alex”
 }
```


Przykład 2

- **Grupa IV – Ustawienia aplikacji**

Czyli preferencje jakie posiada użytkownik w związku z ustawieniami korzystania z programów. Chodzi tu przede wszystkim o język, ustawienia bezpieczeństwa oraz powiadomienia.

Obszar interakcji i pomocy

Podczas badania zwrócono również uwagę na pomoc i instrukcje, jakie są dostępne w aplikacji.

Bardzo ważną funkcją, szczególnie w przypadku młodszych użytkowników, jest utrudnienie możliwości opuszczenia usługi lub przynajmniej sygnalizowanie i konieczność potwierdzenia wyboru. Powinno to ograniczyć przypadkowe wyjście z aplikacji, w wielu sytuacjach jest to konieczna funkcja, która pozwala na bezpieczne korzystanie z urządzenia osoby dorosłej.

Dużym ułatwieniem może być kontrola czasu korzystania z aplikacji, która powinna być stosowana przez opiekunów podczas korzystania z aplikacji oraz urządzenia przez dziecko.

Wszystkie aplikacje, w których jest możliwość interakcji z innymi użytkownikami, powinny mieć opcje łatwego zgłoszenia i zablokowania użytkownika. Jest to konieczne w przypadku różnego rodzaju nadużyć (cyberprzemoc, uwodzenie dziecka, itp.). Inną konieczną funkcją jest możliwość zachowania rozmowy, która może być przydatna w prowadzonych postępowaniach.

brak reakcji ze strony platformy

Często jedynym miejscem, gdzie użytkownik zwraca się po pomoc w przypadku naruszenia jest bezpośrednio dział bezpieczeństwa serwisu. Brak reakcji ze strony platformy prowadzi do dalszego rozpowszechniania nieodpowiednich treści lub zachowań, wzrastającego poczucia winy u ofiary, wzmocnienia poczucia bezkarności u sprawcy.

Aplikacje

Z przeprowadzonych badań wynika, że aplikacje posiadają dostęp do:

3 na 7 aplikacji

elementy usuwane/przeniesione do archiwum

4 na 7 aplikacji

lista wysłanych/otrzymanych zaproszeń, Grupy wydarzenia

5 na 7 aplikacji

imię, nazwisko, numer telefonu, kontakty w telefonie, płeć, publikowane treści, prywatne wiadomości, skasowane wiadomości, polubione treści, zapisane treści, skomentowane treści, lista znajomych, historia zakupów oraz dane na ich temat, jak numery i inne dane kart kredytowych lub debetowych, dane kont, informacje rozliczeniowe, kontaktowe i wysyłkowe, historia wyszukiwarki

6 na 7 aplikacji

data urodzenia, strefa czasowa, lista zablokowanych użytkowników, informacje na temat połączenia internetowego, z jakich innych aplikacji korzysta użytkownik

7 na 7 aplikacji

wiek, adres email, lokalizacja, adres IP, ID telefonu, Model urządzenia, nazwa urządzenia

Badanie aplikacji mobilnych, które składało się z przeglądu 7 z nich pozwala na wyciągnięcie wniosku, że część aplikacji nie jest przygotowana do tego, aby korzystali z nich najmłodsi. Wiele produktów nie chroni w wystarczający sposób prywatności użytkownika na różnych poziomach – poprzez zachęcanie do prezentowania jak największej ilości danych, wymuszanie dostępu do danych gromadzonych przez urządzenie, jak również transferowanie danych między serwisami oraz przekazywanie danych w tle.

Prezentowane informacje w postaci regulaminów i zawiłych procedur, które potrafią zmieniać się kilka razy w ciągu miesiąca nie zachęcają użytkownika do korzystania z plików pomocy, weryfikacji zapisów regulaminów oraz odwoływania się w przypadku błędnych decyzji podjętych przez moderację. Proces zgłaszania treści również w wielu przypadkach pozostaje zbyt skomplikowany lub czasochłonny, formularze zgłaszania bywają ukryte głęboko w aplikacji.

Nadmierne przywiązanie do wizerunku, fizyczności, uzależnienie wiary w siebie i poczucia wartości od opinii innych oraz uzależnienia behawioralne mogą zniekształcić i wypaczyć proces dorastania. Aplikacje mobilne, które służą głównie rozrywce ich użytkowników stają się niestety miejscem powstawania i utrwalania zagrożeń, takich jak cyberprzemoc czy uzależnienia behawioralne.

Monetyzacja użytkowników, która jest celem większości produktów, powinna być balansowana przez inne cele. Jeśli branża technologiczna nie jest w stanie wprowadzić balansu pomiędzy innymi wartościami (jak prywatność użytkowników czy well-being) regulatorzy oraz odbiorcy powinni narzucać i wymuszać taką potrzebę.

Duża ilość gromadzonych przez aplikacje danych może stwarzać ryzyko wycieku danych wrażliwych użytkownika. Kolejny problem może stanowić weryfikacja wieku użytkownika, którą w większości przypadków ogranicza się do pytania o datę urodzenia – co w opinii zespołu badawczego jest mało wiarygodnym sposobem zapobiegania korzystania z aplikacji osobom poniżej dozwolonego wieku.

Zgodnie z wymaganiami Unii Europejskiej właściciele usług mają obowiązek udostępnić użytkownikom informacje na temat gromadzonych przez serwisy społecznościowe danych.

Przebadane aplikacje teoretycznie nie posiadają uprawnień przekraczających ich przeznaczenia. Każde z nich jest wymagane przez konkretną funkcjonalność aplikacji potrzebną do jej „prawidłowego" działania. Podczas badań zwrócono szczególną uwagę na uprawnienia o wyższym ryzyku, czyli takie, które dawałyby żądającej aplikacji dostęp do prywatnych danych użytkownika.

Najczęściej występującymi z ww kategorii były uprawnienia:

- dotyczące dostępu do kamery,
- dotyczące nagrywania dźwięków audio,
- umożliwiające dostęp do kontaktów w telefonie,
- umożliwiające dostęp do dokładnej lokalizacji dostarczanej na podstawie danych GPS,
- umożliwiające zapisywanie danych na zewnętrznej karcie pamięci podłączonej do urządzenia.

Rekomendacje do aplikacji społecznościowych i gier

Dzieci od najmłodszych lat używają różnego typu urządzeń elektronicznych, jest to dla nich element codzienności. Każdy z przebadanych serwisów 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 na każdym z nich, możemy trafić również na materiały w jakiś sposób niewłaściwe lub nieodpowiednie. 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.

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, że 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 innego użytkownika jest nieprzewidywalne.
- 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 wielu informacji o użytkowniku 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 (np. postać będzie biegać nago), czy zawiera dużo przemocy, agresji, wulgarności
- 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.,
- jakie informacje o użytkowniku gromadzi gra/aplikacja – najczęściej opis informacji gromadzonych przez grę/aplikację znajdziemy w Polityce Prywatności, warto mieć świadomość czy 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 w grze występują zachowania niewłaściwe – warto sprawdzić czy, np. użytkownicy wobec siebie nie są agresywni lub wulgarni, czy gra nie zawiera przemocy, a jeśli tak to w jakim stopniu
- czy gra lub aplikacja zawiera linki pozwalające na jej opuszczenie – linki zamieszone np. w reklamie dostępnej 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/ upiększenia – może to być szkodliwe, ponieważ zakrzywia obraz rzeczywistości. W serwisie widzimy wszystko piękne i idealne, a jest to zasługą zastosowania odpowiednich filtrów. Kontakt z takimi materiałami może być szkodliwy dla użytkowników, ponieważ prowadzi 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 powyżej, np. 13 roku życia, nie należy instalować jej młodszemu dziecku, ponieważ oznacza to, że prawdopodobnie zawiera ona treści nieodpowiednie dla użytkownika poniżej 13 rż. PEGI i zapisy w regulaminach są tworzone z myślą o bezpieczeństwie użytkownika, więc nie należy ich bagatelizować.

Wyzwania

Badanie pozwoliło na uchwycenie wycinkowego obrazu dzisiejszej rzeczywistości aplikacji mobilnych. Dało możliwość nakreślenia obszarów, które powinny być objęte dalszymi analizami, dając tym samym pełniejszy obraz.

Podstawowym celem raportu było wskazanie ogólnych potencjalnych zagrożeń oraz zasad bezpieczeństwa korzystania z aplikacji mobilnych przez dzieci i młodzież.

Jak pokazało badanie, wiele produktów, tego dość młodego rynku nie chroni w wystarczający sposób prywatności młodych użytkowników, co implikuje wiele zagrożeń. Główną zasadą bezpieczeństwa pozostaje zatem kontrola rodzicielska. W obecnych czasach zmian cyfrowych jest ona trudna do realizacji. Jej najsłabsze punkty, to nieznajomość zagrożeń przez osoby dorosłe, powodująca zbyt pobieżne podejście do tematu prywatności osób nieletnich lub też, z kolei za mocna ingerencja w ich prywatność.

Drugim ważnym celem było stworzenie rekomendacji dla opiekunów, na co powinni zwracać szczególną uwagę, podczas sprawdzania, czy dana aplikacja jest dostosowana do wieku ich podopiecznych.

W raporcie tym znalazł się szereg uwag wskazujących owe rekomendacje. Jednakże jest to temat do dalszych badań, gdyż jest on bardzo rozległy i powinien być „krok po kroku" wyjaśniany. Trzeba również zaznaczyć, że rekomendacje dla opiekunów osób nieletnich, podobnie jak i dla developerów oprogramowania, żeby były prawdziwie skuteczne, muszą zawierać perspektywę nie tylko ekspertów, co zostało przedstawione w tym raporcie, ale również osób niepełnoletnich. Uchwycenie tej perspektywy jest jednym z największych wyzwań, stojącym przed przyszłymi badaniami.

NASK – Państwowy Instytut Badawczy

ul. Kolska 12
01-045 Warszawa

Recepcja

+48 22 380 82 00
+48 22 380 82 01

Sekretariat

+48 22 380 82 04
+48 22 380 82 01

nask@nask.pl