NASK dyżurnet.pl

MOBILE APPLICATIONS
- ARE OUR CHILDREN SAFE

Publisher

NASK National Research Institute

Kolska 12

01-045 Warsaw

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

Text: Martyna Różycka, Oliwia Chojnacka, Katarzyna Trojanowska

Correction: Anna Maria Hernik-Solarska

Graphic design: Julia Zdancewicz

Ladies and Gentlemen,

The Dyżurnet.pl team was established in 2005 at NASK and, since 2018, has been carrying out the tasks of NASK's CSIRT following the National Cyber Security System Act. The NASK National Research Institute has been undertaking several initiatives to build a safe Internet for years. Because of the rapid technological development observed over the years and the development of mobile applications, we decided to take a closer look at a few of them, the most popular ones. The daily activity of each of us, especially the young users, revolves around apps for various purposes - entertainment, education, self-expression, contact with friends, etc. Sometimes, alongside valuable and developing content, we may come across material that is in some way harmful or inappropriate and sometimes illegal. The awareness of possible risks is central aspect of safe application use. Our goal is to increase it by providing the information gathered in this report.

Our special appreciation and thanks for the inspiring meetings and talks on application security go to the experts and colleagues from NASK, who shared their knowledge with us from many levels.

Enjoy the read!

Dyżurnet.pl team

Contents

Introduction

One of the main signs of the times in the modern world is the virtualisation of the reality around us, which has accelerated with the development of the Internet and has turned into an "arms race" of projects and companies creating the multimedia plane of the 21st century. The development of this trend, supported by the increasing phenomenon of media convergence[1] and the miniaturisation of digital technologies, has led to the emergence of mobile applications with the overall aim of enabling people to access entertainment and global social interaction while aiming for people to be able to take advantage of these opportunities regardless of place or time.

The popularity of touch-enabled devices is making mobile applications increasingly easy to use. The interface of many of them allows intuitive navigation for the youngest users who can't even read and write. Technologies enticing with attractive colours and sounds have become popular among children and teenagers, who devote more and more time to them. Apps often provide entertainment in games, edutainment or mobile versions of services (e.g., social networking) and often enable cross-platform functions.

Therefore, the use of the apps and their functionality enables the fulfilment of needs on different levels, such as the need to belong, contact with others or the need for expression. In this respect, the youngest are no different from adults, so they are eager to use products that cater to their needs. In addition, children encouraged by the app's popularity, the attractiveness of the product or driven by curiosity are reluctant to accept the imposed age restrictions and inflate their age by setting up profiles and bypassing safeguards. Unfortunately, limited awareness among caregivers on how to properly configure devices and profiles to limit contact with inappropriate content or other users allows children and teenagers to use apps designed for older age groups with passive parental consent on basic settings, i.e. settings that do not protect younger users from inappropriate content for them.

Using inappropriate apps can expose the youngest users to encounter dangers such as:

- contact with inappropriate, harmful and illegal content
- contact with dangerous persons
- distribution of materials depicting the child in an inappropriate light
- disclosure and leakage of private information
- perpetuation of hazardous behaviours and habits
- fraud
- cybersecurity risks

1 Henry Jenkins, 2007, Convergence Culture. Clash of old and new media, Academic and Professional Publishing House, Warsaw
2 Nastolatki 3.0 research report, Warsaw

Choosing an app a child can use is not an easy task for the caregivers. Attractive interface, popularity among peers, lack of time and low digital competence of parents contribute to the app being installed virtually without parents' prior evaluation. It is also common for younger children and teenagers to install them independently without the parent's knowledge or consent. Studies show that over 65% of children do not have Internet use rules set by their parents/guardians regarding time spent online or content viewed online[2].

This situation poses complex challenges regarding the need for parents, caregivers and educators to acquire adequate knowledge and awareness about the dangers of the "net" and to take responsibility for the safety of children and young people in this dimension. On the other hand, it is also necessary for app developers and end device manufacturers to take responsibility for the safety of children and teenagers.

Assuring Internet and technology security should be a collaborative effort of:

- children and adolescents - who have the right to have their needs met and expressed; require support when abuse occurs; they can be a link between younger consumers and other groups;
- caregivers - who best understand the needs of their children; respond in real-time to troubling situations; and act on behalf of the child and to protect their rights;
- educators and researchers - who understand the current situation, notice and analyse trends and phenomena; counter threats and can point out the emergence of new threats and prepare recommendations;
- representatives of the technology industry - who, through understanding and shaping technological developments put user security first and implement abuse prevention measures and mechanisms to limit their impact; they also monitor the current situation implement necessary changes;
- regulatory institutions - who develop relevant regulations and monitor their application; uphold the protection of the rights of children and their caregivers.

What are the goals of this report?

The report's primary purpose is to identify general potential risks and safety rules for using mobile applications by children and young people.

A second important goal was to create recommendations for caregivers on what they should pay special attention to when checking whether an app is age-appropriate for their charges. To achieve this, the report's creators decided to study and analyse several applications from different perspectives (for more information see the section on the study's methodology).

The third goal was to create a recommendation for app developers indicating what they should pay special attention to when adapting an app to the age of its users and how they should warn if the app is not intended for users under a certain age.

Who is this report for?

The report, on the one hand, is intended for parents, educators and caregivers of children and teenagers. But, on the other hand, also mobile application developers for whom it can be a basis for future development of applications that are safe already at the design level. The report also aims to start a broader discussion on the safety of mobile apps for children and teens.

Survey methodology

Choosing an application for the study

The selection of apps for the study was dictated by the popularity of apps among children and young people based on available data from the Google Play platform and the choice of Dyżurnet.pl experts, who recognised the need to review some of the apps available in the Google Play store due to their growing popularity.

The popularity criterion is fundamental given that the youngest users are eager to use products designed for older age groups rather than just apps aimed at children or teenagers. Therefore, the study included not only those apps that are created with the youngest in mind and are in the relevant categories in the app stores, but those that children actually use.

Age of the application user

The study retained the age breakdown proposed by PEGI3 - 3, 7, 12, 16 and 18 due to the already established model and replicated by the Google Play platform. PEGI designations are intended to categorise the age group for which a product is intended and to indicate what content may be present (violence, foul language, stimulants, etc.). The use of the "for children" category (users under 18) is also too general and inadequate, as an app that is safe for an audience of 16 or older is not automatically safe for younger children.

It should be noted that when downloading an app (on Google Play), the age group it is aimed at is not always provided. If no age category is given in the store, look for it in the app's privacy policy or terms and conditions - the documents are usually available without downloading the app.

Manufacturers of apps, like other children's products, only give a hint to caregivers, averaging the audience's readiness at a given age. On the other hand, it is up to caregivers to make the final choice of using the service. A good understanding of the product features that led the manufacturer to choose an age category should be clear to all consumers at every stage of product use.

Method of study

The applications were studied empirically, where special attention was paid to user experience and ease of access to information. We checked all documents in the app regarding the scale of access it receives and issues regarding the materials in it, such as community rules. Each time, the apps were checked manually in order to reflect the user's use of the app as closely as possible.

The tests were conducted according to the tester's predetermined scheme. Testing was divided into phases.

01

Phase I
The first step was to conduct a survey of the system's construction. As part of this phase, the purpose of the detailed mobile application functionalities accessible from the user interface was identified and described, and the application metadata was described.

02

Phase II
The second step of the study was to analyse the AndroidManifest.xml file and the application's source code. This verified the scope and legitimacy of the permissions granted to the applications. Permissions were described, and each was assigned a level of protection, which could take one of two values - regular and dangerous.

03

Phase III
The next step was to evaluate the level of control over settings and privacy of the app. As the software was studied in the scope of use by a minor, several factors were considered, such as: does the application require the user's age (if so, is it possible for people under 13 to use it), what data is collected about the user, is the data publicly available, can the user's contact with other (e.g., adult) users be limited, and is it possible to control the collected data - deleting/editing.

Security areas

In the study, several **Security Areas** were selected, thus drawing attention to many aspects that should be considered when evaluating applications and consumer choice.

The first area examined was the **information about the app available** in the Google Play store. The correctness and completeness of the information provided are fundamental, as they allow you to make the right choice.

inadequate presentation of the application

False information presenting the app in the store misleads users. Appropriate classification and visual identification make it possible to limit the visibility of products intended for other age categories than the one to which the user belongs.

Proper presentation allows the user to explore the application without installing it.

no contact with the developer

Difficult contact with the developer may indicate an irresponsible entity for whom negative customer experiences do not matter.

The second aspect that was taken into consideration **concerns the content** found in the app. Much of the study is consistent with the PEGI classification, which dictates that information about content such as stimulants, sex, and violence must be available. However, it should be noted that the PEGI classification originally developed for games will not always be convenient or appropriate for other types of applications. Particular attention should be paid to whether the product allows contact with other users and the type of content that such a message may contain.

Harmful filters available in applications

The presence of beautification filters in social media applications and how they are marked should also be closely examined. Some apps have already decided to introduce markings on materials that have been edited by using filters available in the app. The harm of using beauty filters is mainly based on the presentation of an idealised world, life and appearance as reality, which can have a negative impact on the deterioration of self-esteem among people, especially young people, who use the

app — excessive attachment to image, physicality, the dependence of self-confidence and self-esteem on the opinions of others and behavioural addictions can hurt a young person. Most often, however, no markings are used to tell whether or what kind of filter was used to process the material.

user-generated content - not verified before publication; links to exit the app; the app can influence self-perception (filters, beautification); possible contact with strangers.

hyperlinks that lead outside the application

Younger app users should be protected from accidentally exiting the app, which can affect exposure to inappropriate content, making purchases, or even accidentally changing settings on the device.

The next element tested was the **Interface** - the most challenging level for an adult researcher to evaluate. It is necessary to assess how younger users interact with the product. A more accurate understanding of this level requires in-depth research with a relevant audience, during which intuitiveness can be assessed for a given age group. Given the need to assess the interface area, the team mainly followed guidelines developed by other researchers and available in the literature (Sonia Livingstone et al.[4]; Elizabeth McClure et al.[5]).

The area of behaviour is one of the most critical aspects of the study. The behaviours that the app teaches or perpetuates can be particularly harmful to the young viewer. Using it can affect the user's self-perception, self-esteem, and critical thinking.

Another aspect that was taken into account in the study is the promotion of gambling habits and risky behaviour as indisputably inappropriate for the youngest consumers. An important part of the behavioural area was investigating whether the app supports addiction to the product, which can be dangerous and harmful to the user. It was evaluated whether the application demands that the user has to use it at a particular time without leaving them a choice.

The demand for an appropriate activity requires the child to adjust the rhythm of their day to the application based on the possibility of feeling a loss by not performing a given action and losing, for example, points. This reinforces the formation of a habit of frequent app use, which is imposed by the developers rather than user-regulated, thus contributing to forming an attachment to the app. Long-term process of building a character or a world also has positive aspects, of course, but it should not be done on a forced basis.

the rhythm of use set by the application

The imposition of a use rhythm - time of day, number of logins per day, notifications, no pausing, no predictable length of use - reinforces addictions and lack of control over product use.

Another vital element is the **notifications** appearing when the user is not using the app. The application notifies the user when they are not using it about new features, tasks to be performed or information from other users. **Every product should provide the possibility to turn off notifications because when they appear, they force interaction on the user's part and distract them from their current activity. A continous stream of notifications can be disruptive (reinforcing feelings of FOMO) and distracting.**

The possibility of contact with strangers can be particularly dangerous for the user. Any service that allows contact with strangers should be checked especially carefully by caregivers. The contact can take many forms:

- ranging from the least intrusive - such as showing player rankings;
- through indirect contact - where you can see the activities of others, but there is no possibility of direct contact or it can take place under specific circumstances;
- up to full contact with others, who can send text, photos, videos, stickers, etc., or make voice contact.

It should be noted that any "visibility" of other users can lead to risks - users may, for example, use vulgar names of characters or their profiles that are inappropriate for younger people.

Another category is applications that allow direct communication between users. Here, too, several types of them can be distinguished - having a "phone book" or a circle of "friends" - these allow contact provided that another user has already been accepted. This is usually how conversation can be traced. Privacy settings, which parents should pay special attention to, must be easily accessible and understandable. This is where the role of platforms and developers is crucial, so that settings are clear to children and teens, but also young users' accounts have the highest forms of privacy protection assigned by default.

Combining information from different platforms can also be a threat. **Each combination of different identities on the Internet shows new areas of information about the child, making it easier for people with bad intentions to get to know a potential victim better.** Assuming that a dangerous person will know the victim's profile on social networks, identifying interests and hobbies, the rhythm of the day or how he functions in a group, they can use this information in a way that threatens the child.

linking identities between platforms

Causes disclosure of more user information; allows users to switch between communication channels.

E-commerce area

inadequate marketing

Young users are also consumers and addressees of marketing campaigns. However, they do not understand the nature of advertising and cannot distinguish it from a neutral message.

Some of the applications (product applications) were created to sustain the relationship between the user and the product it carries. Unfortunately, due to insufficient awareness of marketing mechanisms, some users may not recognise an advertising message from an informational one. Users enjoy watching eye-catching video ads, but they don't always understand the impact of advertising on making consumer choices.

Privacy area and setting level

All services made available on the phone should pay special **attention to privacy issues**. This is especially important for devices that a single person uses and carries with them most of the time. The data collected can tell a great deal about their owner, where they stay, how often, their various preferences, and how they use the device. **Therefore, priority should be given to privacy understood twofold: what information the application requires to function correctly, what information it collects or processes in the background, and whether this is consistent with the publicly available information.**

disclosure of private information

Functions that, with their attractive form, encourage the user to share private information such as phone number or geolocation can lead to violations and even danger in the real world.

Encouraging sensitive information such as geolocation or even "checking in" at popular locations to be made public should not be available on apps aimed at younger age groups or even teenagers.

Social media applications often allow you to inform other users that you already have a profile at the level of your phone's contact book. This is a convenient solution, provided the child's phone number is not passed into the wrong hands. Paedophiles and others with dangerous intentions communicate with their victims through various platforms, choosing especially those that allow for latent communication that is not recorded and retained.

It is imperative to be able to use the service while also maintaining privacy. The balance between making it easy to find friends and taking care of the user's privacy, especially younger ones, should be tilted toward security. The ability to report abuse and forward the information to moderation should also be a decision-making factor for the user in considering the app. Particular emphasis should be placed on the intuitiveness and speed of the process and responsiveness on the administrator's part.

With various types of abuse, functions that easily allow you to save and archive communications, report to the platform or forward a notification to parents are very important.

The large amount of data collected by applications can pose a risk of leaking sensitive user data. Another problem may be the verification of a user's age, which in most cases is limited to asking for the date of birth - which, in the research team's opinion, is an unreliable way to prevent people under the permitted age from using the app.

Based on the research, it was found that apps collect a massive amount of data about the user. The collected information was classified into four groups:

- Group I - Profile data

Data about the user, such as name, surname, gender, date of birth, age, cell phone number, email address, data about work, finished school, and location.

- Group II - User activity

Any action taken in the application. In the case of the Social Media group, these include published posts, private messages (even deleted ones), liked, saved, commented and shared content, friends list (as well as blocked users list, list of sent friend invitations, list of received invitations), search history, published media (photos, videos, recordings), saved multimedia.

- Group III - Technical data

Data on the device or technical aspects of using the application. These include IP address, phone ID, User-Agent, login history, registration information, among others. For example, data extracted from one of the JSON files on user activity (example 1) and user registration (example 2) are shown.

```
{
„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”
},
```


Example 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”
 }
```


Example 2:

- **Group IV - Application Settings**

That is the user's preferences concerning the settings for using the programs. This is mainly about language, security settings and notifications.

The area of interaction and assistance

In the survey, we also paid attention to the help and instructions available on the app.

Leaving the service should be made difficult, or the user should be notified and asked to confirm their choice. This is critical, especially for younger users. This should reduce accidental exit from the app, a necessary feature in many situations that allows an adult to use the device safely.

It can be a great help to control the time of use of the app, which caregivers should use when the child is using the app and the device.

All apps with an opportunity to interact with other users should have options to easily report and block the user. This is necessary in the case of various types of abuse (cyberbullying, child grooming, etc.). Another necessary feature is the ability to preserve the conversation, which can be helpful in ongoing investigations.

no response from the platform

Often the only place a user turns to for help in a breach is straight to the site's security department. The platform's failure to respond leads to further dissemination of inappropriate content or behaviour, increasing guilt in the victim and reinforcing the perpetrator's sense of impunity.

Applications

The survey shows that the applications have access to:

3 out of 7 applications

removed/archived items

4 out of 7 applications

list of sent/received invitations, Event Groups

5 out of 7 applications

first name, last name, phone number, phone contacts, gender, published content, private messages, deleted messages, liked content, saved content, commented content, friends list, purchase history and data about them, such as credit or debit card numbers and other data, account data, billing, contact and shipping information, search history

6 out of 7 applications

date of birth, time zone, list of blocked users, internet connection information, what other applications the user uses

7 out of 7 applications

age, email address, location, IP address, phone ID, device model, device name

The study of mobile apps consisted of a review of 7 of them. Based upon its findings, we conclude that some apps are not tailored for the youngest users. Many products do not sufficiently protect user privacy on various levels - by encouraging the presentation of as much data as possible, forcing access to data collected by the device, transferring data between services and transferring data in the background.

The information presented in the form of regulations and complicated procedures, which can change several times a month, does not encourage the user to use the help files, verify the provisions of the regulations and appeal in case of erroneous decisions made by the moderation. The content submission process also remains overly complicated or time-consuming in many cases, with submission forms sometimes hidden deep within the application.

Excessive attachment to image and physicality, the dependence of self-confidence and self-esteem on the opinions of others, and behavioural addictions can distort and disturb the process of growing up. Mobile apps, which mainly serve to entertain their users, are unfortunately becoming a place where threats such as cyberbullying and behavioural addictions are created and perpetuated.

User monetisation, which is the focus of most products, should be balanced by other goals. If the technology industry can't strike a balance between other values (like user privacy or well-being), regulators and consumers should enforce the need.

The large amount of data collected by applications can pose a risk of leaking sensitive user data. Another problem may be the verification of a user's age, which in most cases is limited to asking for the date of birth - which the research team believes is an unreliable way to prevent people under the permitted age from using the app.

Under European Union requirements, service owners are required to provide users with information about the data collected by social networks.

The researched applications theoretically do not have powers beyond their intended use. Each is required by the application's specific functionality needed for its "proper" operation. During the research, special attention was paid to higher-risk permissions, which would give the requesting application access to the user's private data.

The most common of the aforementioned categories included permissions for:

- camera access,
- audio recording,
- access to contacts on the phone,
- access to the exact location provided based on GPS data,
- saving data on an external memory card connected to the device.

Recommendations for social applications and games

Children use various types of electronic devices from an early age. Therefore for them, it is part of everyday life. Each of the sites surveyed provides users with a hefty dose of entertainment and opportunities to meet people with similar interests and sometimes simply serves as an enjoyable way to pass the time. In addition to the positive and valuable material we may find on each of them, we may also come across material that is somehow inappropriate or inadequate. This is the risk that any platform that allows users the opportunity to create content has to consider. That's why it's so important for us to be aware of the risks and consequences of our online behaviour.

A young app user who has good contact with close adults is less likely to suffer the negative consequences of difficult situations online or to establish a surrogate relationship with a stranger met online. It is possible to prevent multiple network threats using modern technological tools. However, they are not always fully effective, and prevention efforts should not be based on them alone. Remember that not every life event needs to be shown online or in real-time.

Particular caution should be exercised if the application allows contact with unfamiliar users.

What to focus on:

- what benefits will come from using the app,
- how the application is presented in the store and whether the information presented is complete and adequate,
- whether it is possible to disable notifications and other information displayed while not using the app,
- whether contact with strangers is possible - anyone, not just an underage user, can be put at risk because the behaviour of another user is unpredictable.
- who has access to the shared materials - you can never be sure how the materials published on the site will be used by others. By uploading any material to the web, the user loses control over the following:
- who has access to information (and what information) about them - access to a lot of information about them makes it easy to use it in inappropriate, privacy-threatening ways,
- what type of materials the application contains - those that rely on user-generated and shared materials always run the risk of offering inappropriate content or presenting harmful behaviour. In games, it is worth paying attention to whether it is possible to chat with users and what the culture of speech is, whether erotic content is available after entering the code (for example, the character will run around naked) and whether it contains a lot of violence, aggression and foul language
- whether anyone can publish material available to other users and whether it passes verification - it is also important whether any user can share material they have produced, as this can generate the risk of exposure to harmful or inappropriate content for younger users, which may not necessarily be illegal (e.g., pathostreams, vulgar behaviour and speech, violence, alcohol abuse),
- what permissions are granted to the app/game and whether they are legitimate - some apps and games ask to give unjustified access to the device's functions. These can include access to the camera, multimedia, geolocation, etc.,
- what information the game/app collects about the user. Most often, a description of the data collected by the game/app can be found in the Privacy Policy. It is worth being aware of whether information about internet searches, the environment, and the user's location is transmitted,

- how payments are secured - what safeguards are in place for payments made to avoid unwanted ones and not expose yourself to financial loss,
- whether there is an option to report inappropriate content/behaviour - if an app or game allows users to interact with each other or allows users to share content, there should always be an option to report inappropriate behaviour or materials,
- whether inappropriate behaviour occurs in the game - it is worth checking whether, for example, users are not aggressive or vulgar towards each other, whether the game does not contain violence, and if so, to what extent,
- whether a game or app contains links leading out - links embedded in, for example, an ad available on the platform may redirect to harmful content available outside the app/game (e.g., ads for 18+ games posted in games for young users),
- whether the user's age is verified in some way - it's worth checking if the app, in addition to the provision in the Privacy Policy/Regulations, asks you to enter your date of birth,
- whether there are filters/beautifiers in the app - this can be harmful because they distort reality. Everything looks beautiful and perfect on the screen. This is achieved using appropriate filters. Contact with such materials can harm users leading to lower self-esteem and self-confidence.

It's always a good idea to read the Terms of Service and Privacy Policy before installing a game or app, as this is where most of the answers to questions about the app's security level are found. If a game or app is above the age of 13, do not install it for a younger child, as this means it probably contains inappropriate content for a user under 13. PEGI and the provisions in the regulations are created with user safety in mind, so they should not be ignored.

Challenges

The study captured a slice of today's mobile app reality. They provide an opportunity to outline areas that should be covered by further analysis, thus offering a more complete picture, which is helpful in the decision process.

The report's primary goal was to identify general potential risks and safety rules for using mobile applications by children and adolescents.

As the study showed, many products of this fairly young market do not sufficiently protect the privacy of young users, which implies multiple risks. Parental control remains the leading, most effective security principle. However, it is challenging to implement in these times of digital change. Its weakest points are adults' lack of risk-awareness, resulting in too cursory an approach to the subject of minors' privacy, or to the contrary - too strong an intrusion into their privacy.

A second important goal was to create recommendations for caregivers on what they should pay special attention to when checking whether an app is age-appropriate for their charges.

The report included several comments indicating these recommendations. However, this is a topic for further research, as it is extensive and should be explored step by step. It should also be noted that recommendations for caregivers of minors, like those for software developers, to be truly effective, must include the perspective not only of experts, as outlined in this report, but also of minors. Capturing this perspective is one of the biggest challenges facing future research.

NASK – National Research Institute
Kolska 12
01-045 Warsaw

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

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

nask@nask.pl