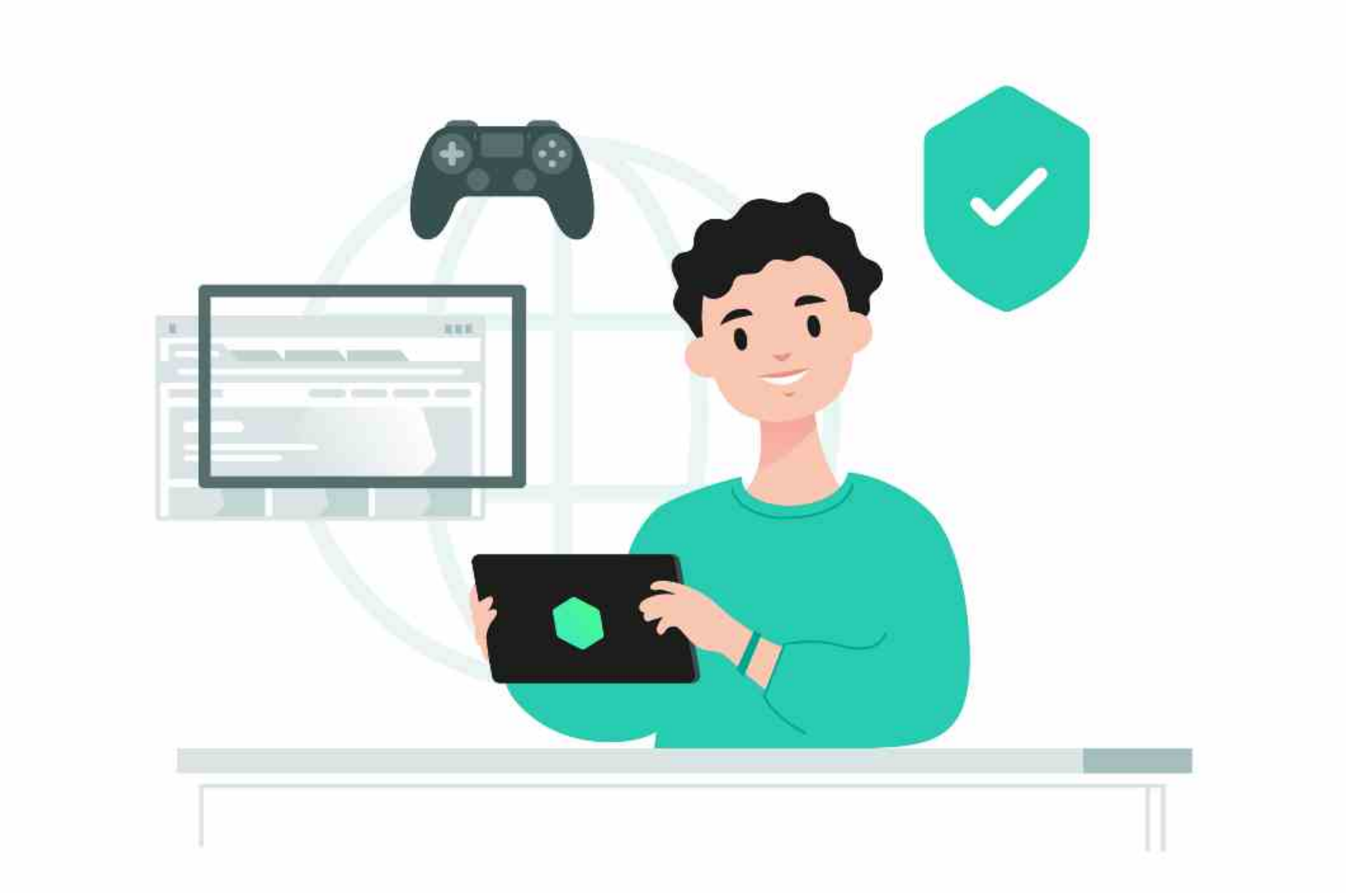
Threats behind the screen: how cybercriminals target young gamers

This report delves into the cyberthreat landscape that has targeted kids playing video games from H2 2023 to H1 2024, highlighting the related dangers and providing insights on how to protect this vulnerable group.



The end of summer signals a shift for young gamers, as the familiar rhythm of school days resumes, following a holiday season filled with free time for hobbies such as gaming, socializing, and exploring the online world. The increased online activity makes young gamers frequent targets of cyberattacks, scams, and other online threats. In this report, we analyze the shifts in the cyberthreat landscape targeting young gamers from H2 2023 through H1 2024. Besides raising awareness about the modern threats of the gaming world, the report provides insights on how to protect kids against those risks as they navigate the digital world.

Methodology

To gain insights into the current gaming threat landscape for young players, Kaspersky experts searched the most popular children's game titles as keywords. Using this process, they have determined the scale of distribution of malicious files and potentially unwanted software related to these games, as well as the number of users attacked with the use of these files. For these purposes, researchers analyzed threat statistics from Kaspersky Security Network (KSN), using anonymized data about malicious and potentially unwanted applications files from July 1, 2023, to June 30, 2024. Our experts examined phishing pages, using various children's game titles as a lure, to discover numerous scams targeting young gamers.

The list of video games was compiled based on several public rankings of the most popular children's games:

1	Minecraft
3	Roblox
4	Fortnite
5	Apex Legend
6	Brawl Stars
7	Five Nights at Freddy's
8	Toca Life World
9	Overwatch 2

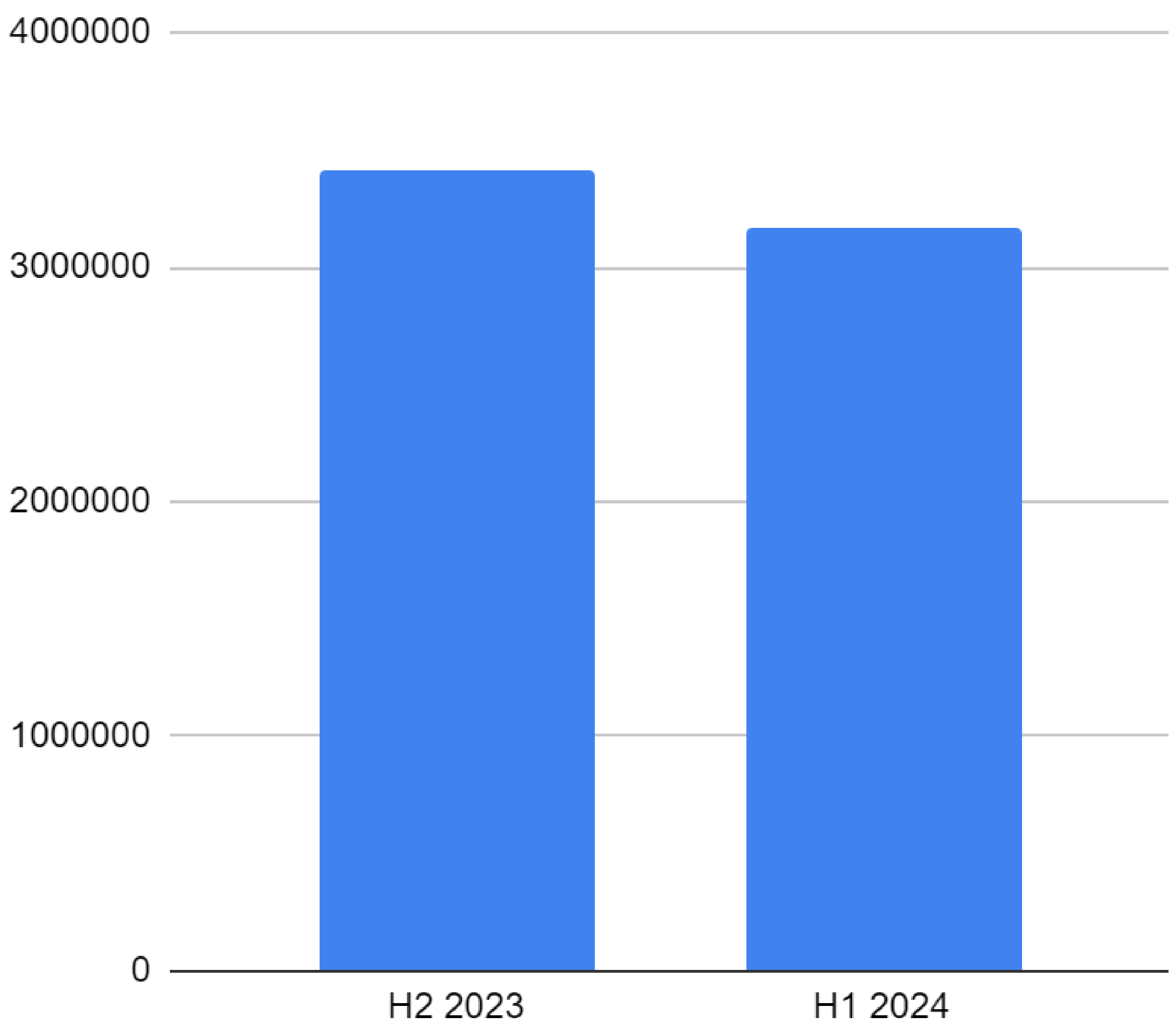
10	Among Us
11	Poppy Playtime
12	Valorant
13	Mario Kart
14	The Legend of Zelda
15	Pokémon GO
16	Angry Birds
17	Splatoon
18	Subway Surfers

Key findings

- *Kaspersky security solutions detected more than 6.6 million attempted attacks capitalizing on video games popular among young gamers from July 1, 2023, to June 30, 2024.*
- *The number of targeted users surged by 30 percent in H1 2024 compared to H2 2023.*
- *The most exploited children's games remained Minecraft, Roblox, and Among Us.*
- *The main type of threats spread under the guise of video games popular among kids remain downloaders and adware.*

Analysis of attack attempts and targeted users

During the period from H2 2023 to H1 2024, Kaspersky solutions detected a total of 6.6 million attack attempts, in which malicious actors tried to lure young gamers into their traps by mentioning popular video games.

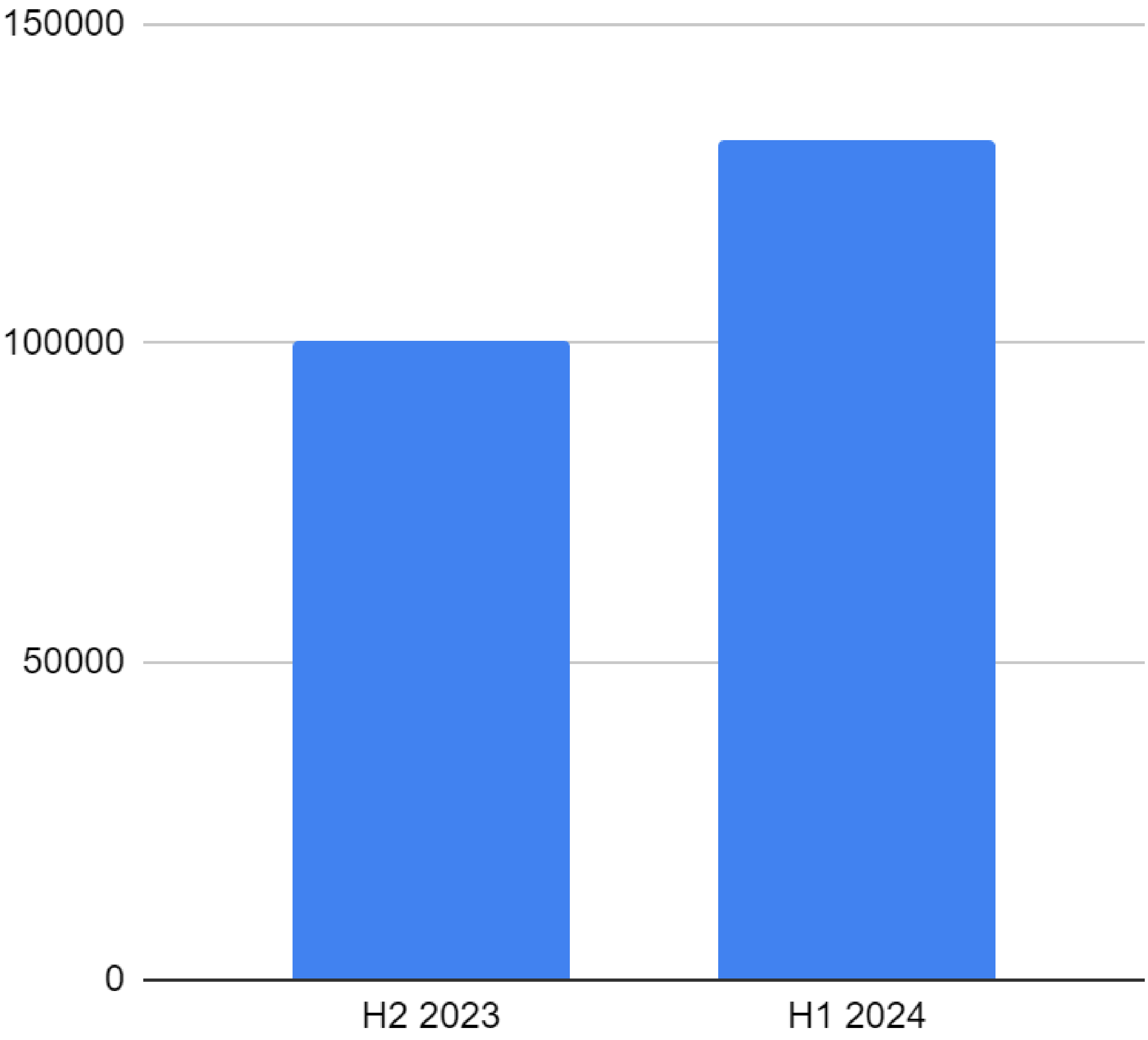


Attempts to download malicious or unwanted files disguised as games for children H2 2023 — H1 2024

In the first half of 2024, Kaspersky security solutions detected 3.16 million attempted attacks, which constitutes a decrease of seven percent compared to 3.4 million cases detected in H2 2023.

This decline might be explained by a heightened interest in gaming in the second half of 2023, due to events such as the release of the “Five Nights at Freddy’s” movie and other updates.

It is noteworthy that the decline in the number of attack attempts in H1 2024, was accompanied by an increase in the number of attacked users: the number of affected users increased by more than 30% in H1 2024, reaching 132,000. In H2 2023, the figure stood at 100,000 users. Overall, throughout the reported period, 207,000 users tried to download malicious or potentially unwanted applications under the guise of children's popular games.



Users attempting to download malicious or unwanted files disguised as games for children H2 2023 — H1 2024

We believe that the growing trends can be explained by general cyberthreat landscape development trends that we have been observing recently, namely:

Attacks are more sophisticated

We see that cybercriminals have become increasingly adept at understanding the current trends and interests in the gaming industry, using this knowledge to craft more cunning and less obvious schemes. Instead of broad, general attacks, they are capitalizing on areas of high interest, making their tactics more effective. This could lead to fewer overall attacks but a higher number of users being affected.

Use of automated tools

Cybercriminals are increasingly using artificial intelligence (AI) to automate and personalize phishing attacks. These AI-driven campaigns may craft convincing messages that are more likely to deceive young gamers. At the same time, new advanced phishing kits — pre-made templates of phishing pages — created with automated tools consistently appear on the dark web, allowing attackers to deploy highly effective phishing sites that mimic popular gaming platforms. The use of such automated tools may also lead to higher success rates in compromising users.

The most exploited children’s games by number of attempted attacks

Below are the Top 10 children’s games that became the most popular among cybercriminals during the period from H2 2023 to H1 2024.

Title of the game	The number of attack attempts
Minecraft	3,094,057
Roblox	1,649,745
Among Us	945,571
Brawl Stars	309,554
Five Nights at Freddy’s	219,033
Fortnite	165,859

Angry Birds	66,754
The Legend of Zelda	33,774
Toca Life World	28,360
Valorant	28,119
Mario Kart	14,682
Subway Surfers	14,254
Overwatch 2	9,076
Animal Crossing	8,262
Apex Legend	8,133

Minecraft

Out of the 18 games we chose for this research, Minecraft still remains the most popular among cybercriminals. The primary reason is a range of Minecraft features that allow gamers to use cheats and mods to enhance and personalize their digital experience. In particular, cybercriminals tend to disguise malware under the guise of Minecraft's mods and cheats, having launched 3 million attempts on over 120,000 users throughout the reported period.

Roblox

Second place went to the popular Roblox game, with more than 28 million daily active users under the age of 13. Throughout the period reported, cybercriminals attempted 1.6 million attacks, affecting more than 45,000 users.

Among Us

Although Among Us experienced a surge in popularity during the pandemic, and young players' interest in the game hasn't faded — which means it's also attracting the attention of cybercriminals. One of the reasons for such popularity among cybercriminals, along with the sheer number of players, is that the game relies heavily on online chat and communication between users, creating opportunities for social engineering attacks. Cybercriminals can potentially exploit this by sending malicious links or files through these communication channels.

Among Us was used as a disguise in 945,000 attempted attacks on more than 18,000 young gamers from H2 2023 to H1 2024.

TOP 10 cyberthreats using popular games as a lure throughout H2 2023 — H1 2024

During the reported period, cybercriminals used a variety of cyberthreats disguised as popular children's games.

TOP 10 cyberthreats	Attack attempts
Downloader	6,089,127
Adware	283,928
Trojan	91,027
RiskTool	49,053
WebToolbar	20,966
DangerousObject	19,314
Trojan-PSW	6,715
Trojan-SMS	6,643
Trojan-Dropper	5,420
Trojan-Spy	4,991

As can be seen from the statistics, the most popular type of cyberthreat targeting users under the guise of video game-related content remains downloaders. This trend has been relevant for several years across a wide variety of games for both children and adults. While this type of software is not malicious in itself, downloaders are often used to load other threats onto devices. Another common software, spread as kids' games, is adware, which displays unwanted (and sometimes irritating) pop-up ads that can appear on a user's computer or mobile device.

Furthermore, cybercriminals also used various types of trojans. A Trojan inherently, ranked third in the top above, is a type of malicious software that disguises itself as legitimate software to trick users into installing it on their computers. Once installed, Trojans can perform a range of malicious activities without the user's consent or knowledge. Throughout the reporting period, young gamers faced various members of the Trojan family, namely:

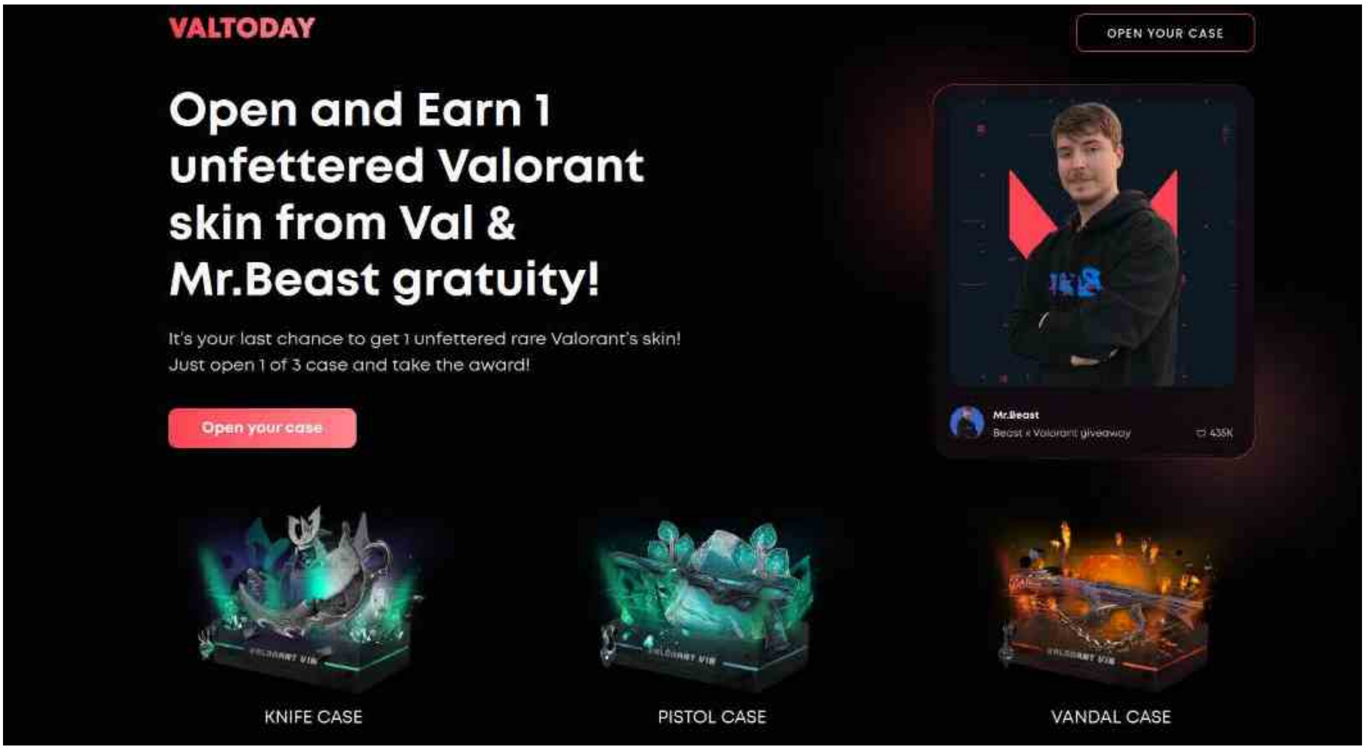
- Trojan-SMS, sending messages to premium-rate numbers from an infected mobile device without the user's knowledge;
- Trojan-Spy, capturing keystrokes, screenshots, and other data such as login credentials;
- Trojan-PSW, specifically designed to steal passwords from the infected system;
- Trojan-Dropper that "drops" (installs) other malicious programs on the gadget.

Hidden hazards: scams on kids' popular games

One of the most common scams in gaming is the offer to receive new skins for your character — essentially clothing or armor that enhances the hero's skills. Some skins are common, while others are extremely rare and, therefore, more desirable.

One of the most common scams in gaming is the offer to receive new skins for your character — essentially clothing or armor— that enhances the hero's skills. Some skins are common, while others are extremely rare and, therefore, more

desirable. Kaspersky experts have found an example of a scam that uses both the name of popular game Valorant and that of world-famous Mr. Beast. The choice of the cybercriminals was not accidental: Mr. Beast is one of the most influential YouTubers in the world, with more than 306 million subscribers across his channels, including millions of children. By selecting this blogger and using his photo, the scammers aimed to capture children's attention and hook them into their fraudulent scheme.

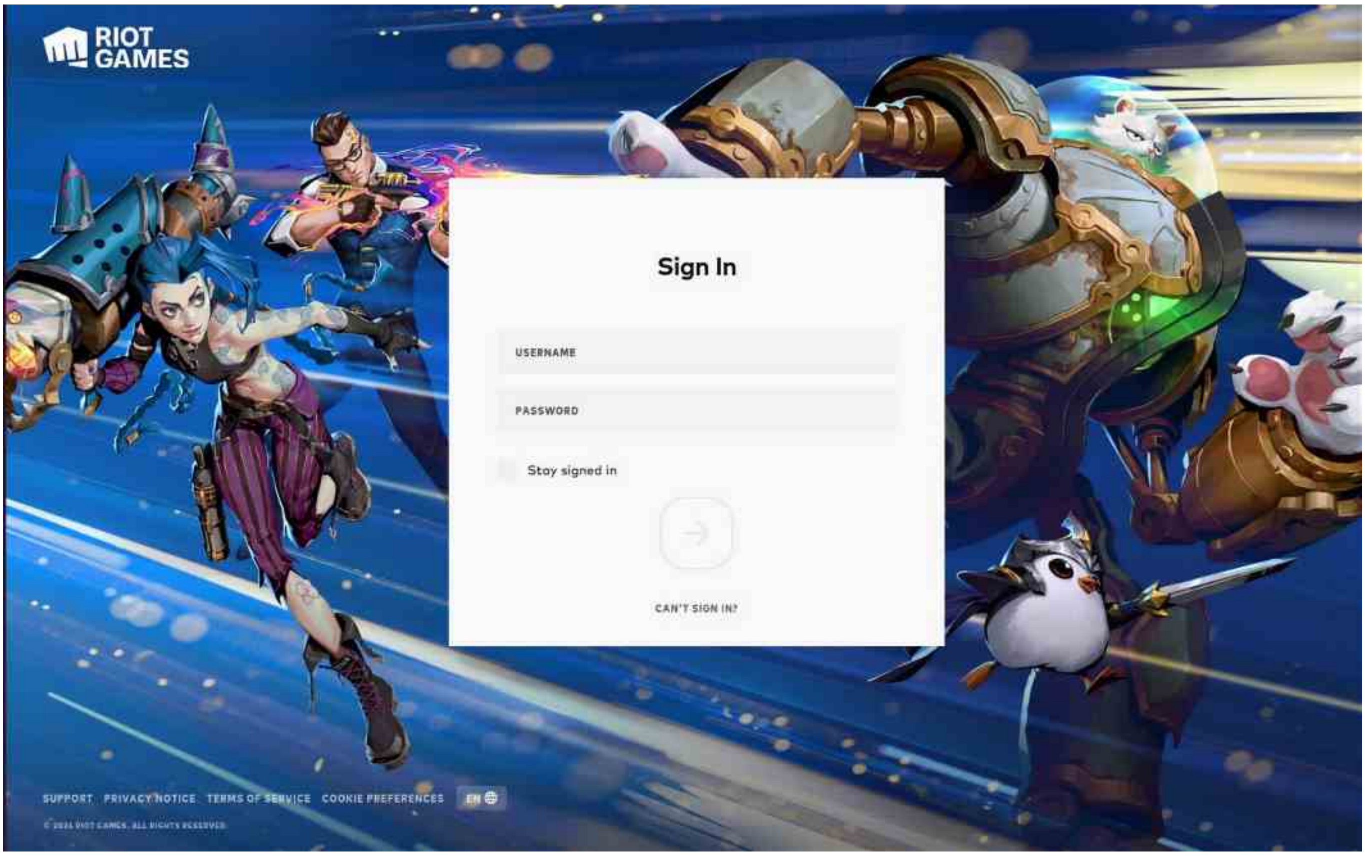


Open and Earn 1 unfettered Valorant skin from Val & Mr.Beast gratuity!

It's your last chance to get 1 unfettered rare Valorant's skin! Just open 1 of 3 case and take the award!

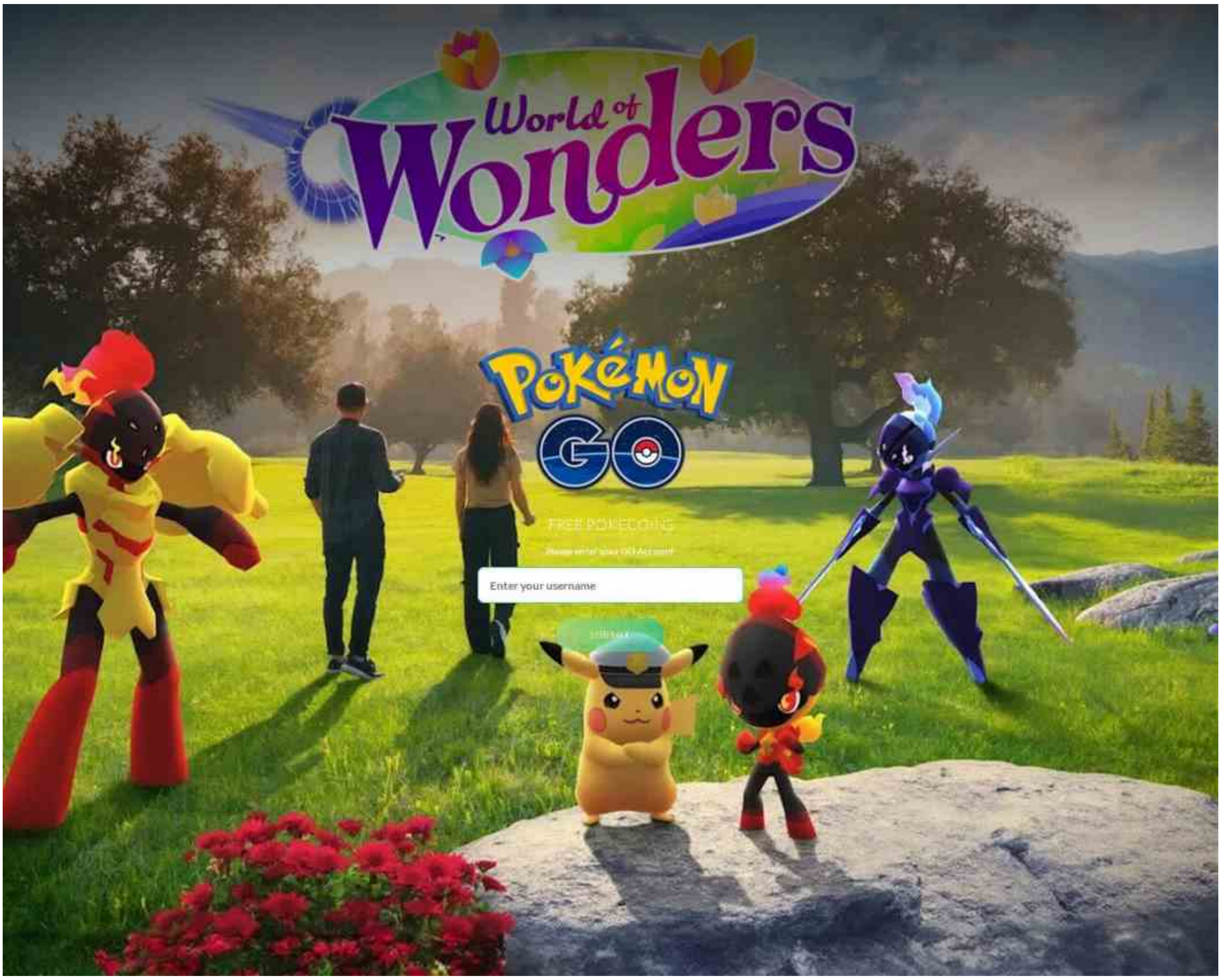
The image of Mr. Beast is used as a lure to make kids to follow the fraudulent scheme

To receive the desired Mr. Beast skin, young users are asked to enter their login and password for their gaming account. However, instead of receiving any gift, their gaming account is stolen by the scammers.



Users are asked to enter the credentials of their Valorant account

In addition to skins, a popular trap is the offer of receiving in-game currency. For example, in one of the discovered scams exploiting the Pokémon GO brand, users are asked to enter the username for their gaming account. Next, they're asked to take a survey to prove they're not a bot. Once the survey is complete, they are redirected to a fake website, usually one promising free prizes or giveaways. This is where the real scam kicks in. The scammers aren't actually after personal data like credit card details; they're using the guise of gaming to lure users into another scam, such as fake downloads, prize claims, or other deceptive offers. The whole process is a clever way to redirect users to a different, more dangerous scam under the pretense of a legitimate verification step.



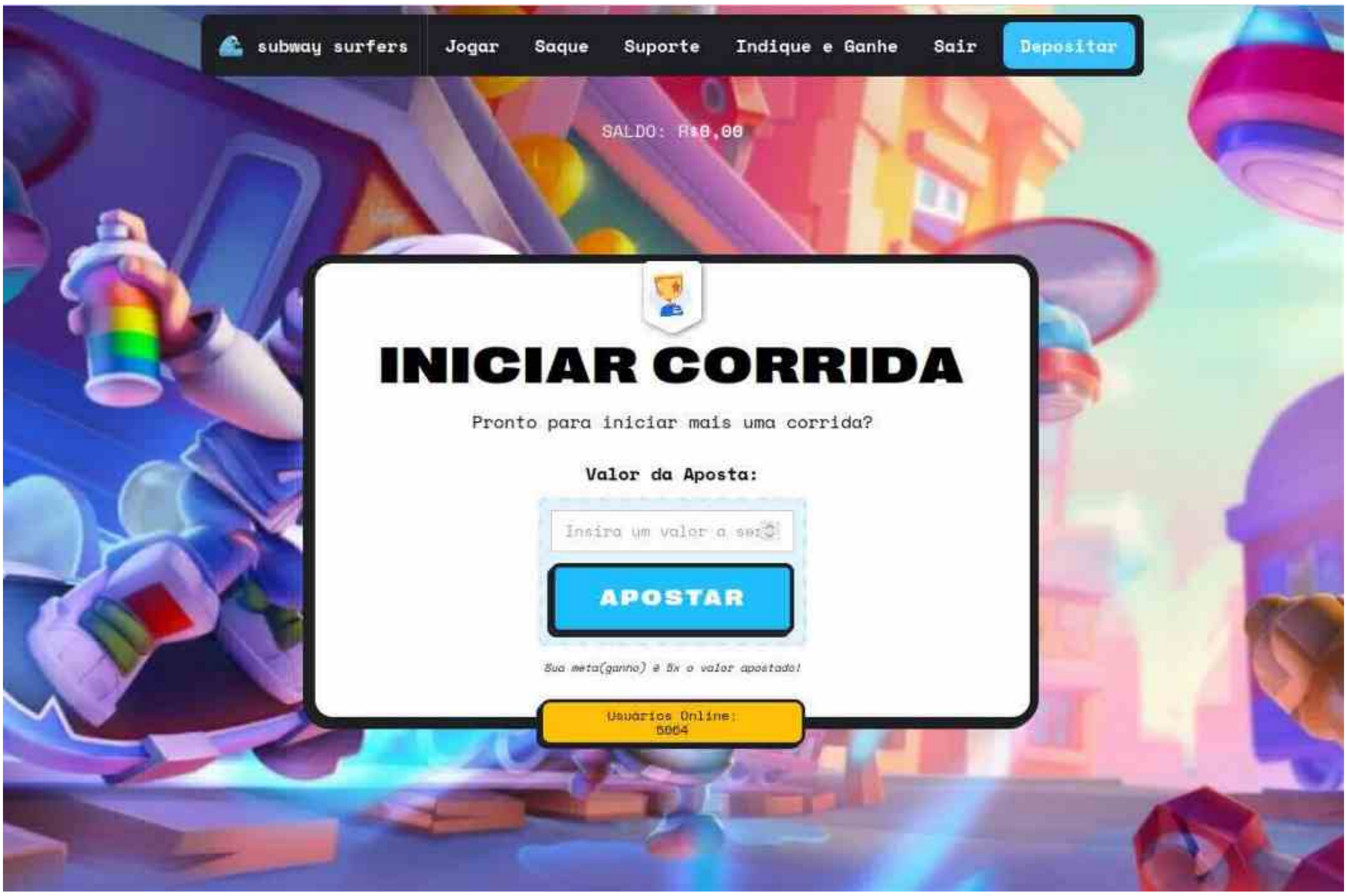
FREE POKECOINS

Please enter your GO Account

Enter your username

Scam exploiting the brand of Pokémon GO

At the same time, scammers also try to lure young users with the promise of getting a new iPhone or even money. In Brazil specifically, we encountered a similar scenario on a phishing page exploiting the brand of the popular mobile game Subway Surfers. This website is a fake version of the game, presented in a web format. You have to register and make a deposit to start playing the game and increase the amount five-fold.



SALDO: R$0,00

INICIAR CORRIDA

Pronto para iniciar mais uma corrida?

Valor da Aposta:

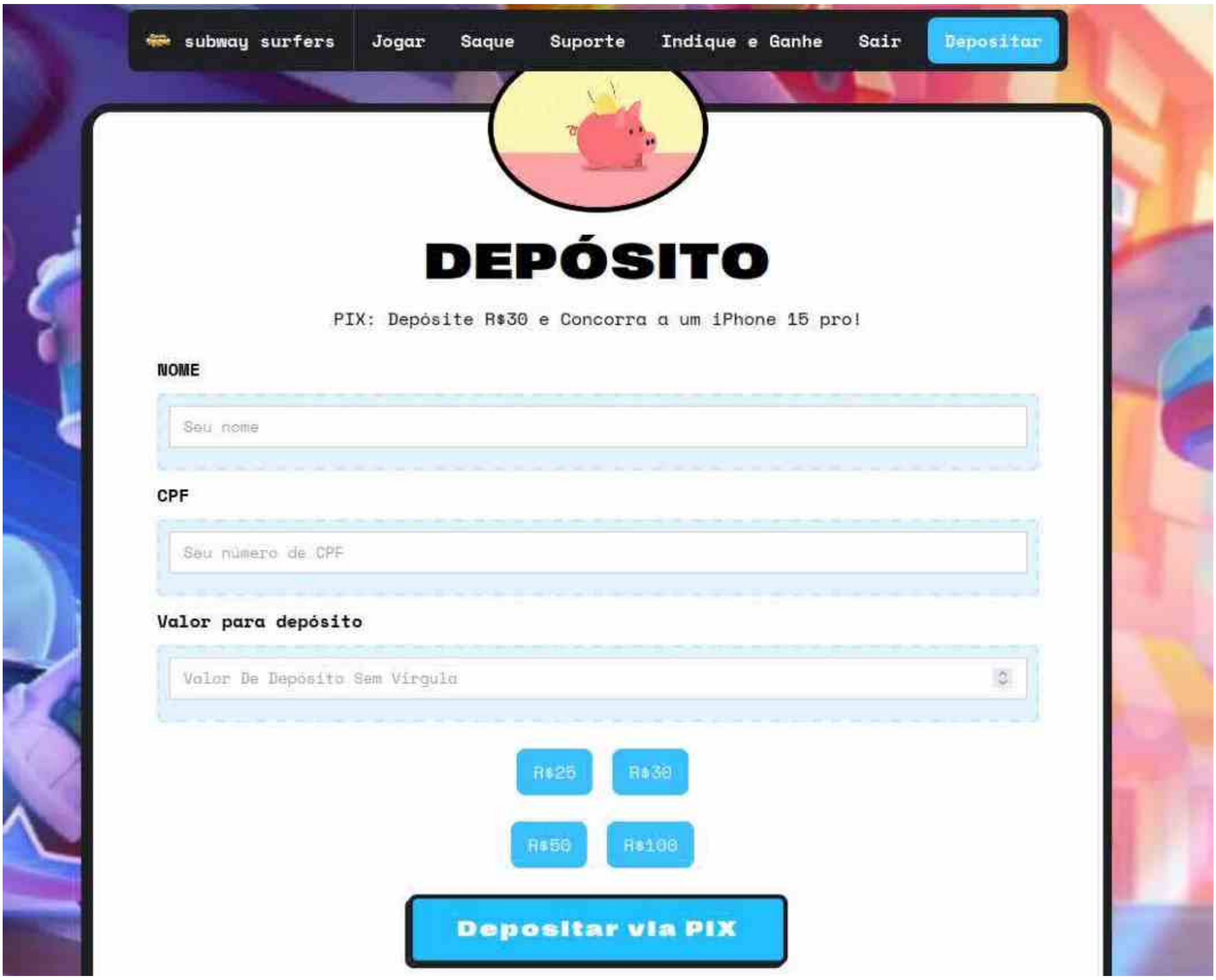
Insira um valor a ser

Sua meta(ganho) é 5x o valor apostado!

Usuários Online:
5064

The phishing page in Portuguese asking young users to make a deposit

However, in order to make a deposit, the user is asked to specify not only their name, but also Cadastro de Pessoas Físicas (CPF) — the Tax ID issued when you register with the Brazilian Revenue. The CPF is crucial for various activities in Brazil, including opening a bank account, signing contracts, and engaging in financial transactions. If someone obtains another person's CPF information fraudulently, they could potentially misuse it for identity theft or financial fraud.



DEPÓSITO

PIX: Depósite R$30 e Concorra a um iPhone 15 pro!

NOME

Seu nome

CPF

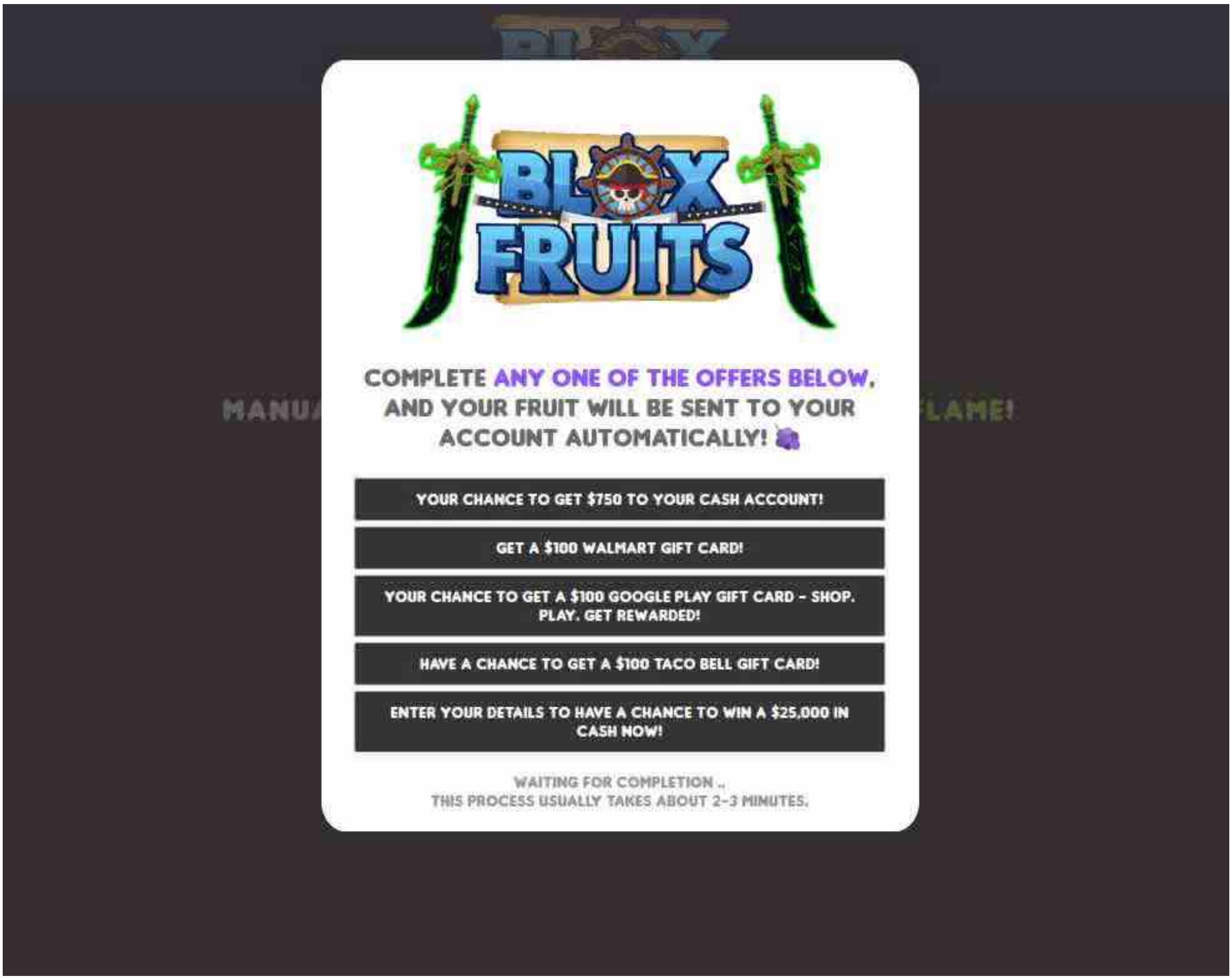
Seu número de CPF

Valor para depósito

Valor De Depósito Sem Vírgula

Users are asked to enter their Cadastro de Pessoas Físicas – one of the most sensitive pieces of personal information in Brazil

We encountered a similar scenario on phishing pages related to Roblox. In this case, users were offered a chance to receive a US$100 Gift Card for Walmart hypermarkets, $100 for the fast-food restaurant Taco Bell, or even $25,000 in cash — if they entered their payment details. However, young players would not receive any real prizes. The danger here is that as in many countries, legislation does not allow children to have their own bank accounts. As a result, children might try to use their parents' credit card information, potentially leading to the loss of money from the family account.



COMPLETE ANY ONE OF THE OFFERS BELOW, AND YOUR FRUIT WILL BE SENT TO YOUR ACCOUNT AUTOMATICALLY! 🍇

YOUR CHANCE TO GET $750 TO YOUR CASH ACCOUNT!

GET A $100 WALMART GIFT CARD!

YOUR CHANCE TO GET A $100 GOOGLE PLAY GIFT CARD - SHOP. PLAY. GET REWARDED!

HAVE A CHANCE TO GET A $100 TACO BELL GIFT CARD!

ENTER YOUR DETAILS TO HAVE A CHANCE TO WIN A $25,000 IN CASH NOW!

WAITING FOR COMPLETION ..
THIS PROCESS USUALLY TAKES ABOUT 2-3 MINUTES.

Users are offered a variety of fake prizes under the guise of one of the Roblox’ games

Conclusion and recommendations

The digital landscape for young gamers is a complex and ever-evolving one. This report sheds light on the cyberthreats that have targeted young users during H2 2023 — H1 2024. Our research indicates that attacks on children are becoming a more common vector for cybercriminals: meaning that vigilance, education, and proactive measures are critical. Children may often be unaware of the basics of cybersecurity and easily fall into attackers’ traps, for example, when trying to download a free version of a popular game. This is why cyber hygiene education is a “must-have” when building children’s safety in the online environment. By fostering critical thinking, responsible online behavior, and a strong understanding of the risks, we can create a safer and more positive online experience for this generation of digital natives.

To keep your kids safe online, Kaspersky recommends users take the following steps:

- By staying informed about the latest threats and actively monitoring their children's online activities, parents can create a safer online environment for their kids.
- It's crucial for parents to have open communication with their children about the potential risks they may encounter online and to enforce strict guidelines to ensure their safety.
- Help your child choose a unique password and aim to change it periodically.
- Set clear ground rules about what they can and can't do online and explain why you have put them in place. You need to review these as your child gets older.
- With dedicated apps for digital parenting such as Kaspersky Safe Kids, parents can effectively safeguard their children across both online and offline spaces. These apps help adults ensure a safe and positive digital experience for little ones by establishing healthy habits, protecting them from inappropriate content, balancing screen time and monitoring children's physical location.
- To help parents introduce their children to cybersecurity, Kaspersky experts have developed the Kaspersky Cybersecurity Alphabet. In this book, your kids will get to know new technologies, learn the main cyber hygiene rules, find out how to avoid online threats, and recognize fraudsters' tricks. You can download the pdf of the book for free.
- To secure your child from downloading any malicious files during their gaming experience, we advise them to install a trusted security solution on their device. It works smoothly with Steam and other gaming services.