Ebook

Arkose Labs

Creating the Next Generation of Fraud Defenders

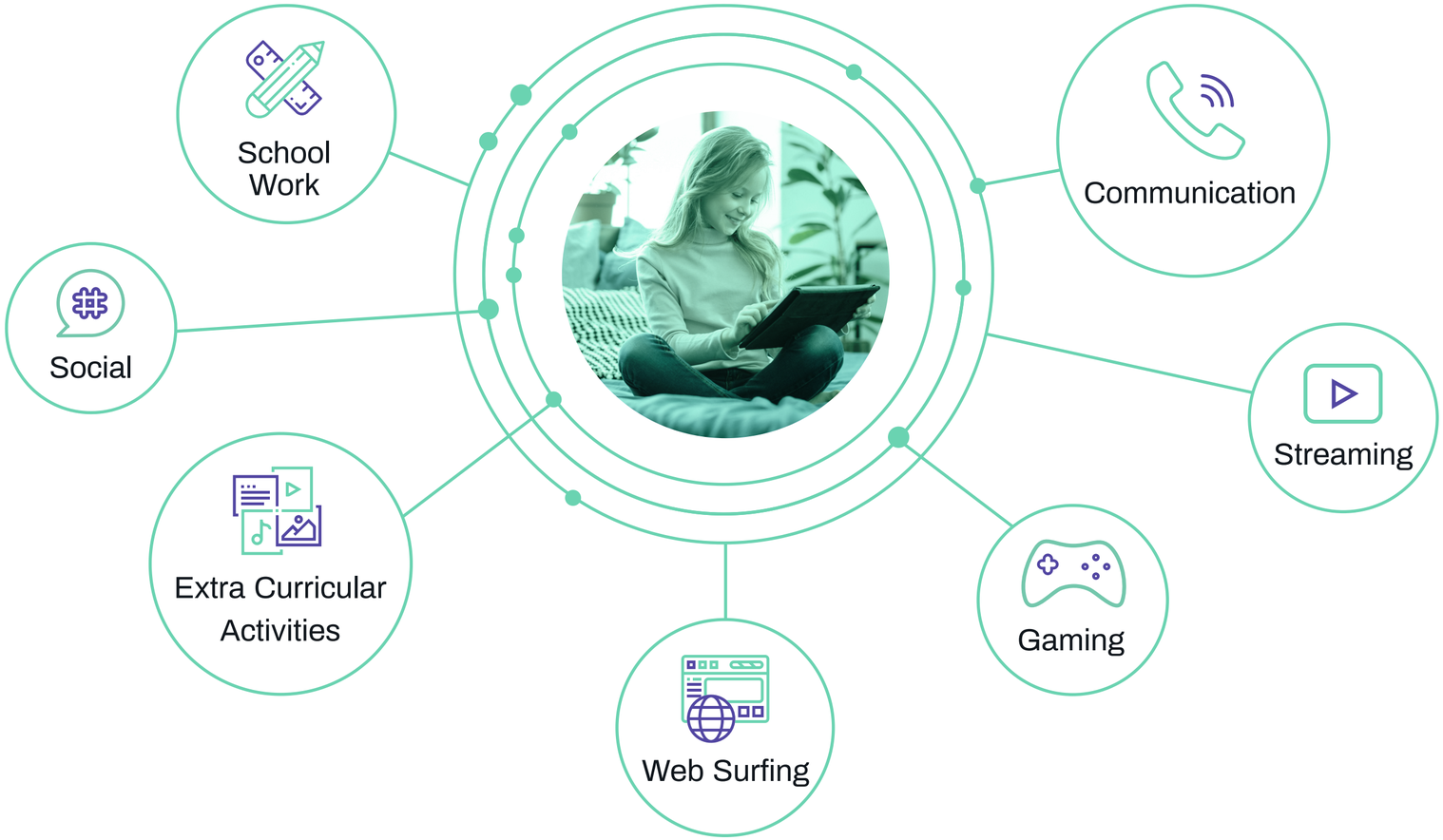
How to get kids cyber-savvy and make a safer internet for all

Digital Transformation and its Effect on Children

As digital transformation continues apace, many everyday activities have moved online - especially for children.

According to UNICEF over 175,000 new children go online everyday—that's one new child every half second. The internet is a treasure trove of information and can provide a wealth of knowledge. However, there's also inappropriate content in equal proportion. Then there are cyber criminals looking to lure innocent children into sharing private information, sexual abuse and a host of other criminal activities.

As more and more children get online, their vulnerability to the risks associated with cyber exposure also increases. To protect our children from online abuse, it is important to instill good digital habits in them.



COVID-19: A Digital Gamechanger

At the same time, the COVID-19 pandemic has had a big impact on the digital ecosystem. Much of what was formerly done face-to-face is now done in the virtual realm.

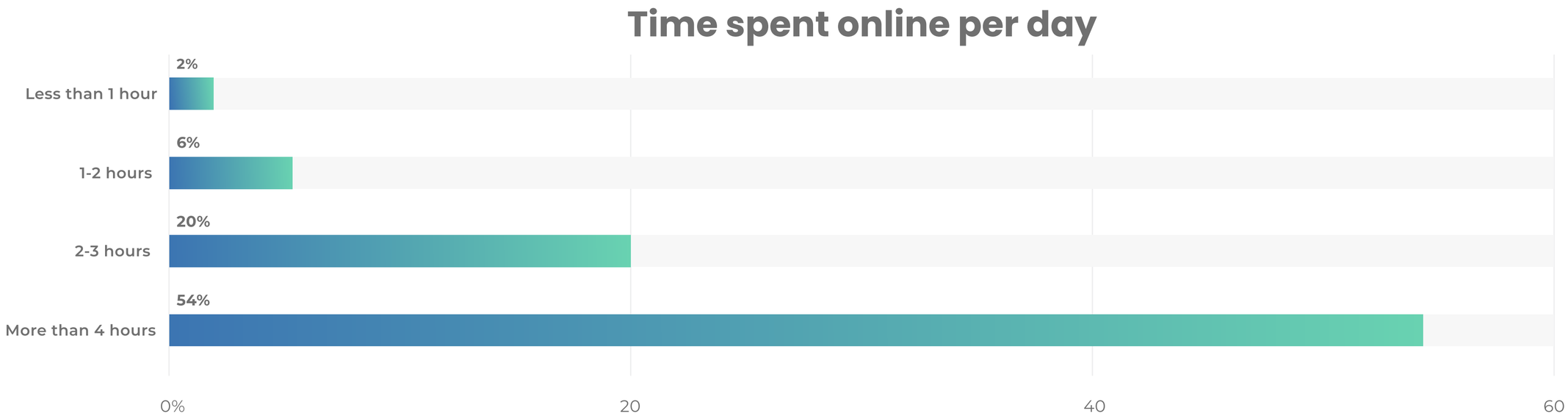
This new reality has benefited some industries and hurt others. Travel sites, for example, have seen far less traffic. But companies in areas such as social media, online gaming or video-sharing have exploded. Incidentally, these are also among the most popular digital destinations for children. That means children are on digital platforms that suddenly have an increased amount of traffic — as well as fraudsters.

To see how kids view online fraud, Arkose Labs commissioned a study of more than 80 children aged 6-16 across 3 continents. Unsurprisingly, this generation of youngsters is digital native. More than 54% of children spend four hours or more every day. 20% spend between two and three hours a day, 6% spend one to two hours, while only 2% spend less than an hour. There's an understandable spike in the daily time spent online due to COVID19. 95% children reported spending even more time online due to online classes and other activities.

Lockdowns Accelerate Digital Adoption

The lockdowns across countries have forced closure of schools, daycare and other institutions. All teaching activity is now being done through digital means, either using video conferencing tools or videos that teachers create and upload to an online central repository. Furthermore, social interactions are also happening more frequently online. These can take the form of the “virtual playdates” that have become commonplace during lockdowns, or increased time on various digital platforms.

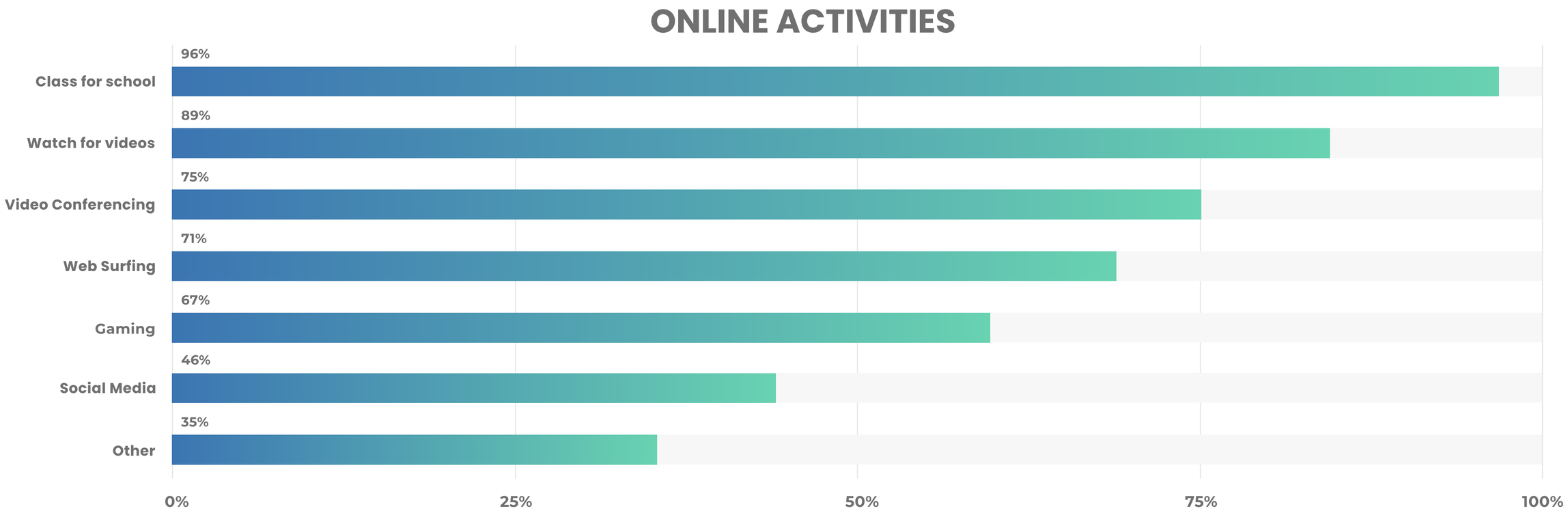
It’s a parenting trope in the modern, digital age: parking your kid in front of the screen so you can get some work done, or even enjoy a glass of wine. But the dangers of the online world are just as prevalent — if not more so — than those encountered in the real world. That’s why it’s crucial for children to have a baseline understanding of cybercrime and online fraud.



Popular Digital Destinations

It's still a bit hard to believe, but virtually all of life's activities have migrated online, at least for the time being. This not only includes school, but things like music lessons, athletic instruction and coaching, activities like ballet and karate, and much more.

When asked what activities kids were doing the most online, it was a bit surprising that playing video games came in fifth, with 67% reporting that as the top online activity. While gaming is still a popular pastime for kids, things like school classes, surfing the web and video chatting with friends were even more popular. This highlights the importance of protecting all digital platforms and making them safe for children.

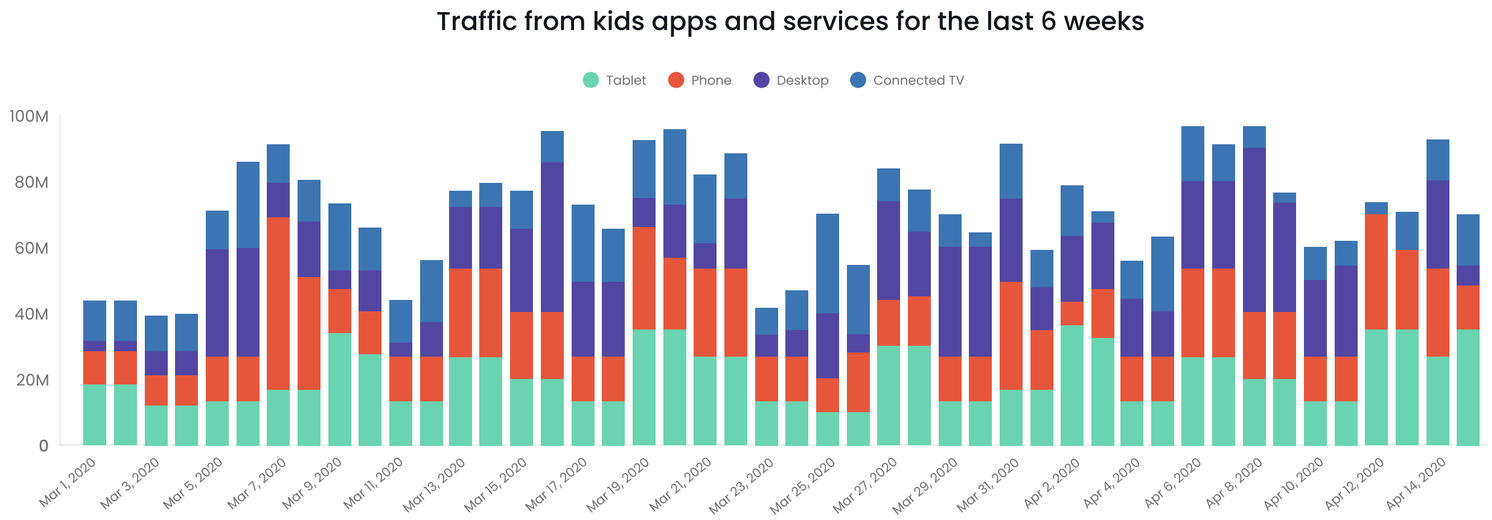


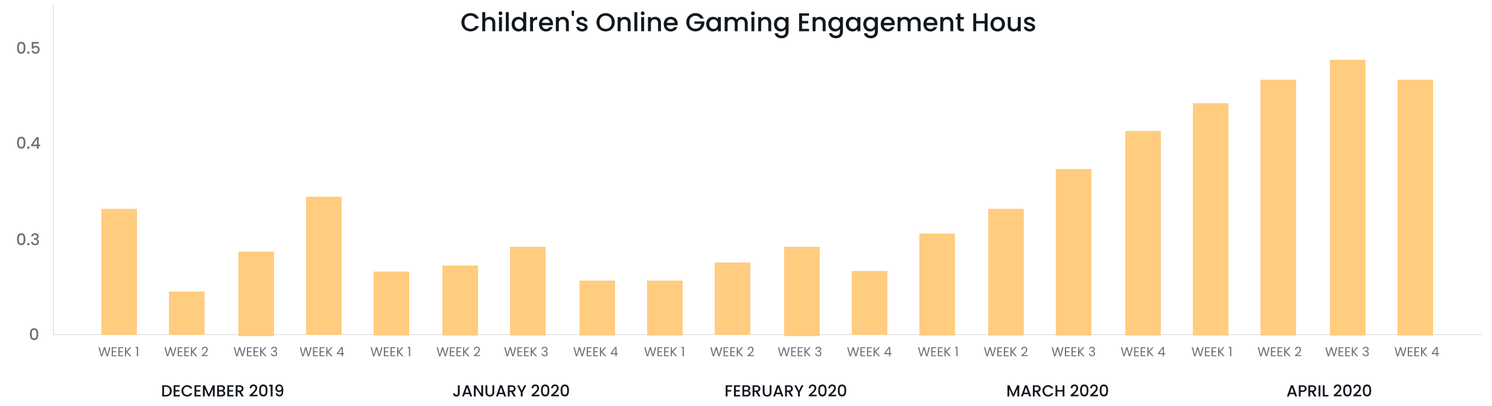
More Time Home, More Time Online

Covid-19 has led to a 50% increase in screen-time for kids. Although a proportion of this is for education, figures released from various companies show that much of this increase is being spent in games. Two-thirds of all US kids between 9 and 12 are now playing Roblox.

All of a sudden, kids have become a much larger consumer segment than prior to the pandemic-related lockdowns.

In terms of their presence and participation, kids have now become an audience that no digital service provider can ignore.





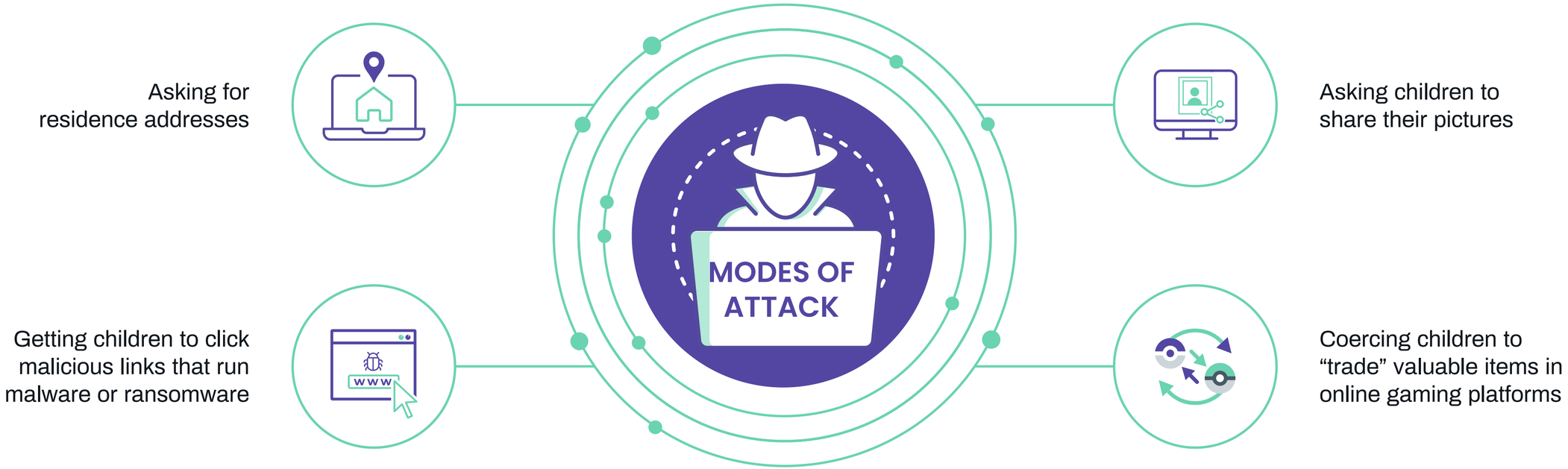
1 PWC Digital Media Report 2019

2 The Common Sense Consensus: Media Use by Kids Age Zero to Eight, 2017

Cybercriminals Target Kids for Profit

The threats that children face in the online world are for real. These can have serious consequences and even scar the personalities of the affected children for the rest of their lives. These can include bullying, sexual abuse, exposure to inappropriate content, social engineering, ransomware, malicious links, and addiction.

As education has moved online, cyber criminals have also found a new attack vector in eBooks. They lace these documents with malware and circulate them on the internet for free download. When children download these ebooks, the malware either locks the device or steals data from the device.



Children's Awareness of Online Security

Although children are aware of some the scams and criminal activity plaguing the internet, they often don't know the true depth and breadth of fraud online.

Personal Data:

Many know that sharing personal information, especially information related to payments (94%) and social security numbers (93%) on the internet can be dangerous. 44% of the children polled affirmed that they were careful when sharing any information online. However, sharing log-in credentials among friends for thing like streaming services was still commonplace.

Online Fraud:

When asked specifically about what online fraud is, children were clear that it involved stealing personal details for impersonation and financial scams. Children know that cyber criminals try to steal passwords or trick them into paying money.

Identity Theft

Children are aware of what identity theft means. They explained it as cyber criminals stealing user information to pretend to be someone in order to get money.

Have They Been Hacked?

We were not expecting children to report incidents of hacking. However, children today are aware and 7% admitted to getting hacked. As expected, though, the majority of children (81%) said they were not hacked, while 12% weren't sure.

What do children say constitutes online fraud?

People who claim to be legal and take your details

Faking something

People tricking you into buying stuff but scamming you instead

Stealing and using your money

Stealing passwords and money online

Taking someone else's password and use it to get access to their account

Someone tricks you into paying them

Someone pretending to be someone else

Cheating someone online by stealing their money, passwords or personal information

Doing illegal things online such as online theft

It means that a person has someone else's personal information which they are using to their benefit online

Protecting The Ecosystem

Fraudsters are looking for the quickest way to make a buck, and will attack targets that require the least amount of effort. Unfortunately, this often means children. In this way fraudsters follow the old adage, “taking candy from a baby” quite literally.

However, parental control can play a key role in protecting children from the dangers that the internet poses. However, as more parents are working remotely and spending the day online themselves, it can be hard to be vigilant about this.

Therefore, it’s imperative for parents to let their children know that nothing is private on the internet. Even something seemingly innocuous, like sharing a photo, can have disastrous consequences down the line, since online activities are permanent and can never be erased.

Parents must also emphasize that children must not purchase anything online without their presence. Discourage children from opening emails that seem suspicious and teach them about some telltale signs. All of this counseling and awareness can help children be mindful of the potential dangers in the online world and prepare them better for a safer digital life.

Our Collective Responsibility

UNICEF believes that in addition to parents and other caregivers, businesses can play a massive role in protecting children in the digital world. This is very important from a moral sense as well as a business sense.

Increased losses due to chargebacks in cases where children were the victims of fraud are one result of a failure to have the property security in place. Furthermore, parents of children who are the victims of fraud on a website or digital platform will likely blame the company for not having the proper protocols in place. This could result in losing a loyal customer, or even negative brand awareness if the parents uses social media to air their grivances.

Ultimately, Businesses are responsible for protecting users and need to be aware of the dangers to all their customers, especially the most vulnerable ones, such as children and the elderly.

Businesses Stepping Up

For their part, businesses are coming forward to shoulder the responsibility of making the internet safer for children. From creating tools to awareness campaigns, there's a lot of ways businesses are helping make the cyber world safe for children.

01 Many gaming and streaming services have parental controls that restrict what children can play or view, or even how much time they can spend on the platform.

02 Video-sharing services have created content and UI that is child-friendly, as well as dedicated controls to prevent children from straying into adult content.

03 Cyber security companies regularly release software and tools to help fight rising cyber threats. They also release patches and updates to plug-in vulnerabilities and keep the software up-to-date.

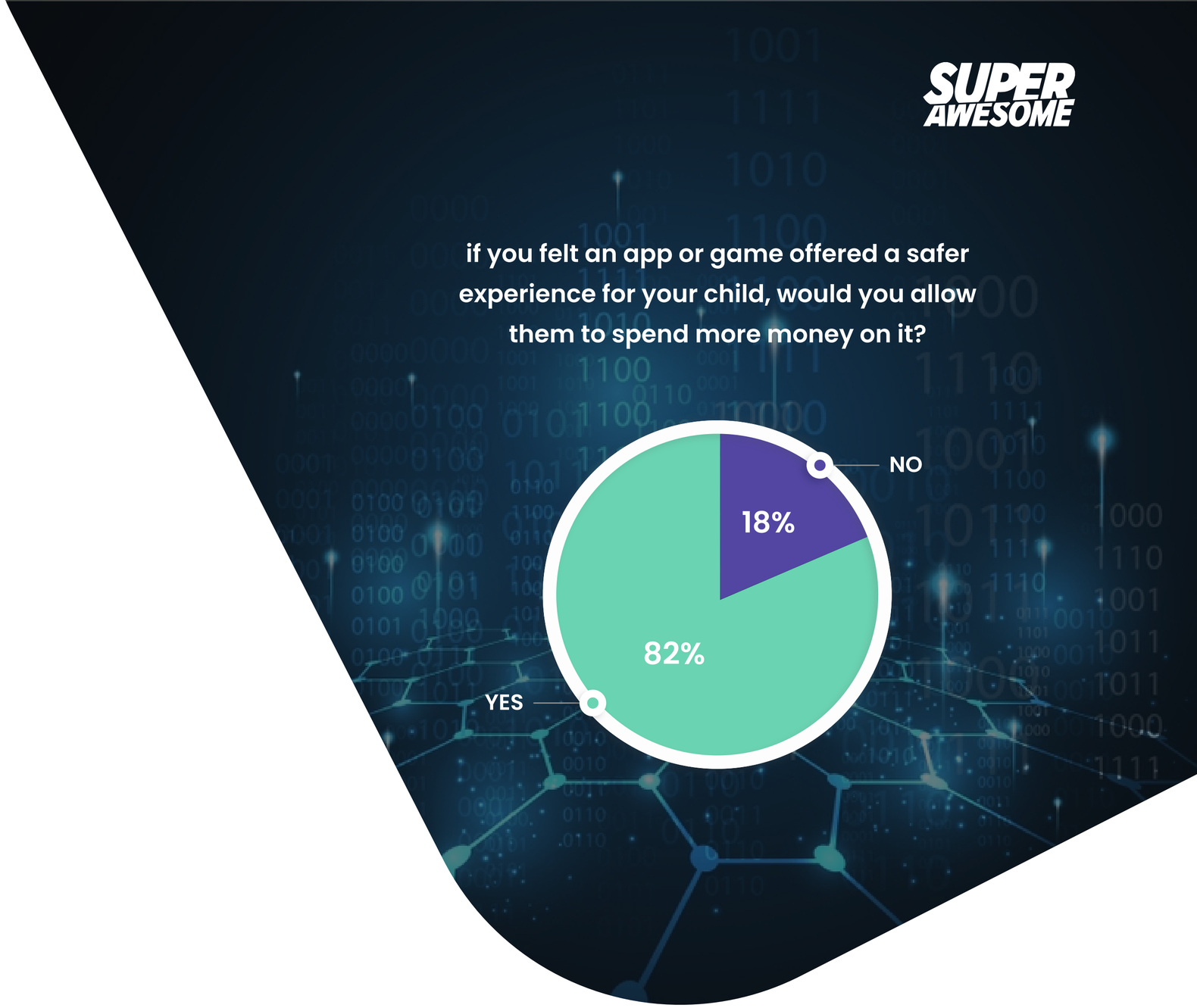
Companies such as SuperAwesome work with businesses in the video game industry and help provide them with solutions to raise digital awareness and engage in appropriate content for the under-16 demographic. They are helping digital businesses safely and effectively engage with young adults and children.

Good Security Means Loyal Customers

A separate study conducted by SuperAwesome found that parents want the digital services that their kids engage with to have the proper controls in place. The idea that parents are unaware of (or apathetic to) the content their kids consume online is simply not true.

According to a SuperAwesome survey of parents, 96% said they would like to see more parental controls in the games and services their kids uses. Meanwhile, 72% said they have recommended a game or digital service to another parents because they felt it offered a safe online experience.

Creating a safer platform for kids will ultimately lead to more engaged and loyal customers, and improve the bottom line for businesses.



Arkose Labs Helps Businesses Protect Kids

It is laudable that these and many other businesses have taken measures to protect children. Arkose Labs plays a vital role in these efforts, as we work with many of the most popular digital platforms to keep them safe from fraud and abuse. The Arkose Labs platform is the industry leader in detecting and stopping automated new account creation, which is often used to then launch spam and phishing messages. Using a variety of data points and device heuristics analyzed in real time, we are also able to accurately detect malicious human traffic, and feed them increasingly complex authentication challenges, to the point where they give up and attack another site.

Case Study:

Business Problem : Arkose Labs worked with a popular streaming media site that has a particularly younger demographic among its user base. This site had an issue with bots being deployed to create new accounts en masse, which then were used to disrupt streaming videos, as well as disseminate spam and malicious content.

Solution : After deploying the Arkose Labs platform, this bot activity was completely stopped, making for a safer environment for all users. Spam against good users was eliminated, and overall a better customer experience was created.

Children are the Future

Children are growing up in an age where digital is the norm. They spend considerable amounts of time in online activities such as online classes, games, videos, and social media. The ongoing coronavirus pandemic has resulted in a spike in the time spent online, largely due to the online schooling that most children around the globe are attending.

An increased exposure to the digital world means a heightened risk to cyber threats. The online experience of the children can have a profound effect on their personalities. It is therefore necessary for everyone—parents, teachers, schools, society, governments, and businesses—to come together and make the online experience for children safe.

Arkose Labs reaffirms its support to all activities that aim to make the digital world safe for our children. To get your copy of the report, please click here.

About Arkose Labs

ABOUT THE STUDY

The global study entitled ‘From the Mouths of Babes’ was conducted across North America, Asia, and Europe. The respondents were categorised into three categories according to their age. These included children aged 6-8 years, 9-11 years, and 12-16 years.

ABOUT ARKOSE LABS

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU