Arkose Labs

Ebook

Navigating Internet Safety When Screen Time Becomes Full Time

A Guide for Parents and Digital Businesses

Prioritizing Security in the New Digital World

It's been a year since the world changed drastically and our lives moved online almost overnight. Everything from work to play became digital. For young people, their lives were especially upended. Between the advent of home learning — with many under increasing pressure to progress academically in a drastically new environment — to virtual social gatherings and spending more time in digital worlds for entertainment, much of their life was spent virtually. To find out how kids and their parents are coping with this increased digital usage, Arkose Labs polled more than 180 parents and children on their screen time habits over the last year.

There is a concept known as the Stockdale Paradox, which broadly speaking has to do with balancing optimism and pessimism appropriately. While it is often used in relation to crisis management, it can also apply to how younger digital natives navigate the online world. On one hand, they are tech-savvy and often can operate in a digital environment with more ease than their parents, many of whom did not access the internet until they were teenagers. At the same time, however, this native familiarity with the online world can also desensitize kids to recognizing possible scams, fraud and other hazards.

Despite the digital divide, one interesting trend both parents and their children agree upon is that kids are spending too much time in front of screens. While it is probably not surprising that nearly 90% of parents were concerned about their children's screen time, more than half of the kids we polled said they were spending too much time online.

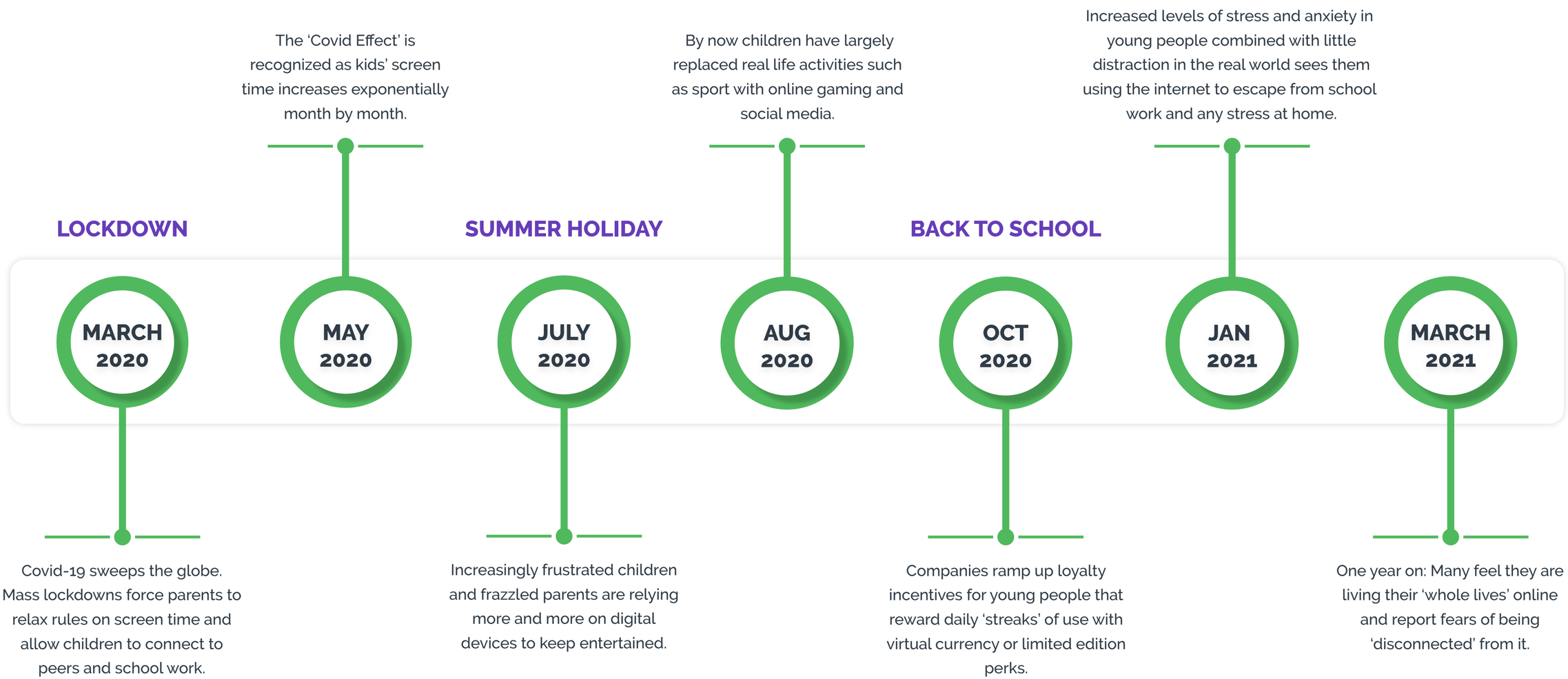
With children — along with most everyone else — online more than ever before, it is critical that businesses ensure their digital platforms are safe and secure for all users. The tide of fraud is ever-rising, and we must all work together to create a safer internet and protect the most vulnerable users.

Kevin Gosschalk

Founder and CEO

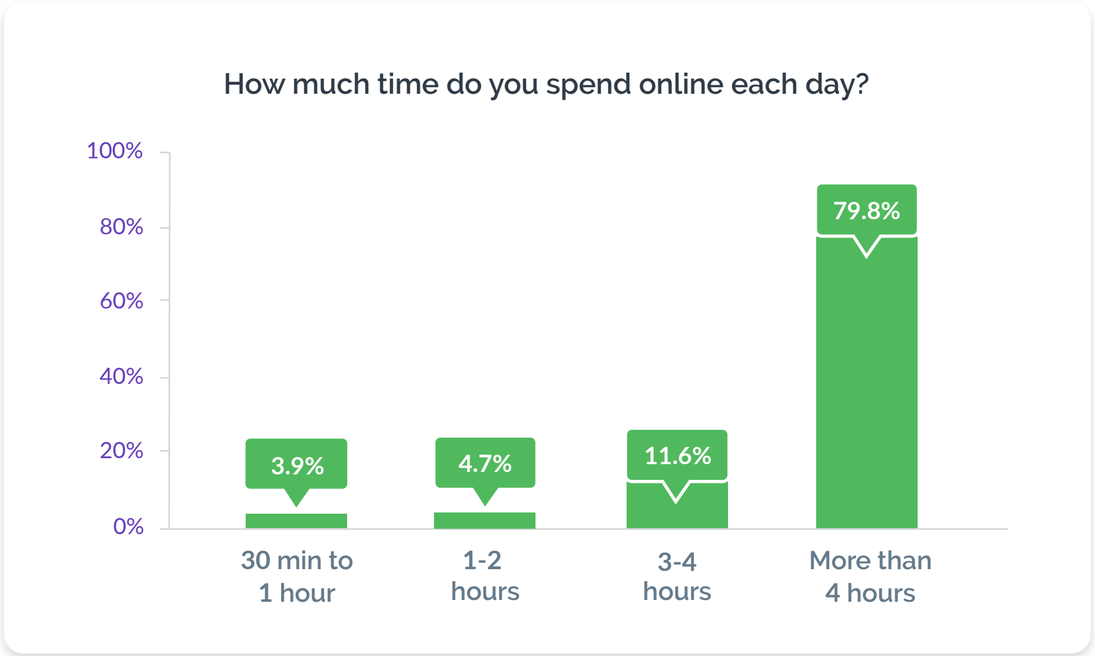
Despite the digital divide, one interesting trend both parents and their children agree upon is that kids are spending too much time in front of screens.

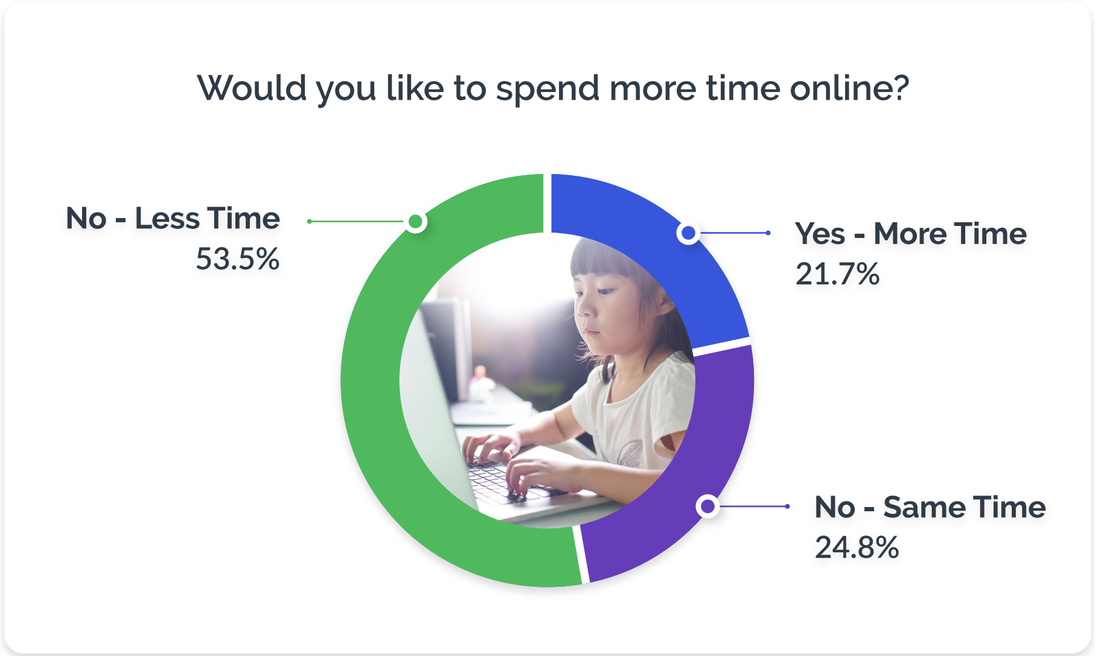
A Timeline of Our New Digital World



Shocking Reversal: Kids Want Less Screen Time

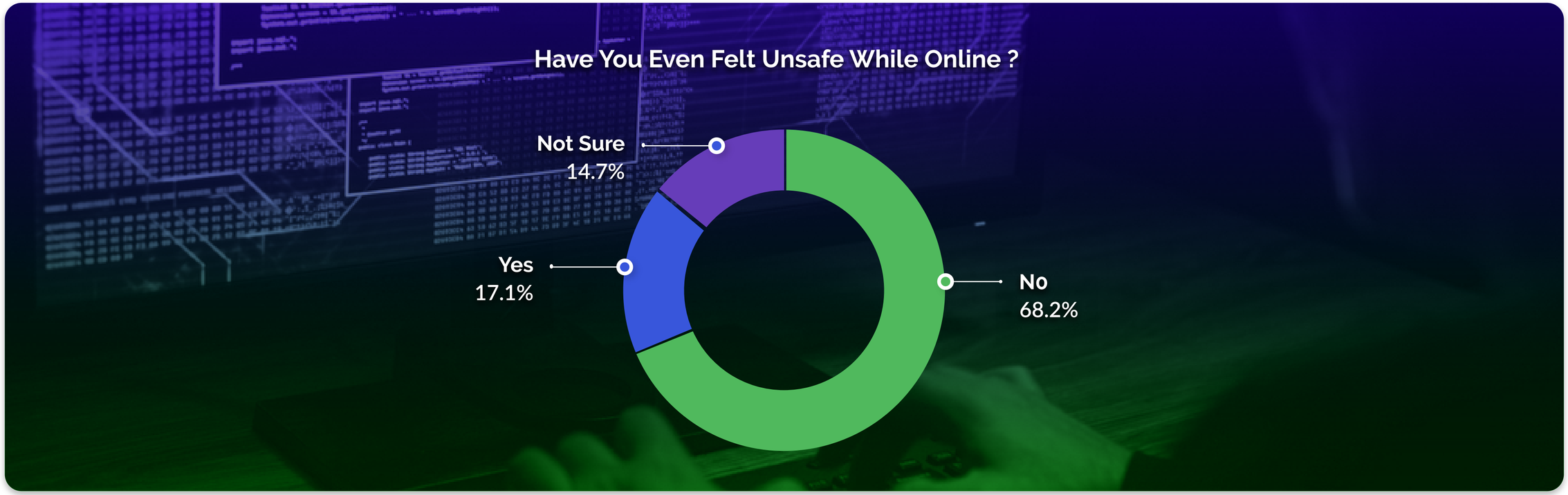
There is a strong consensus that too much time is being spent online, with 53.5% of young people concerned about their own screen time, and 89% of adults concerned about their kids' screen time. It's perhaps surprising that more than half of the children surveyed were concerned about screen time; this is a stark reversal from previous years, where kids had to be practically dragged away from their digital devices. However, with the vast majority of children spending well more than 4 hours per day online, managing screen time levels will become increasingly difficult for both parents and kids.





Lulled Into a False Sense of Security?

This generation of young people are digital natives, which can be both good and bad. Compared to their parents, most of whom first used the internet as teenagers, they are digitally savvy, but at the same time there can be an artificial sense of safety online that comes with such familiarity. 68% of young people surveyed said they had never felt unsafe online; however it's important to note that they aren't always able to recognize such instances. Young people are spending more time than ever unsupervised online, making them extremely vulnerable to scams and other fraud. Abuse is widespread and wide ranging, including bullying, sexual abuse, exposure to inappropriate content, social engineering, ransomware and malicious links. With more activities being done online than ever before, it provides fraudsters and other bad actors with more channels through which to attack.



A New, Wider Digital Attack Surface

School

Globally there are 1.2 billion children learning online, causing a huge spike in traffic to digital education platforms. Remote learning presents new attack vectors, for example fraudsters infecting free eBooks with malware. There were also major security issues in the early days of the pandemic where weak security protocols enabled some students to hacks classmates' accounts and pose as each other.*

Virtual Parties

Among the biggest winners of the last year have been video conferencing platforms which provide much needed connection for young people in isolation. They have been vital in connecting people socially around the globe, but they also can be used for malice. Parents and guardians should be aware of things like 'Zoom bombing' where attackers hijack meetings, sharing offensive or even criminal content.

Gaming

Gaming platforms have seen unprecedented levels of traffic across the board over the past year. This has produced ample opportunities for fraudsters to target young players who possess valuable accounts. Furthermore, there is a rise in young people themselves playing the role of fraudster, looking to steal in-game currency and items and create fake new accounts for bonus abuse.

Social Media

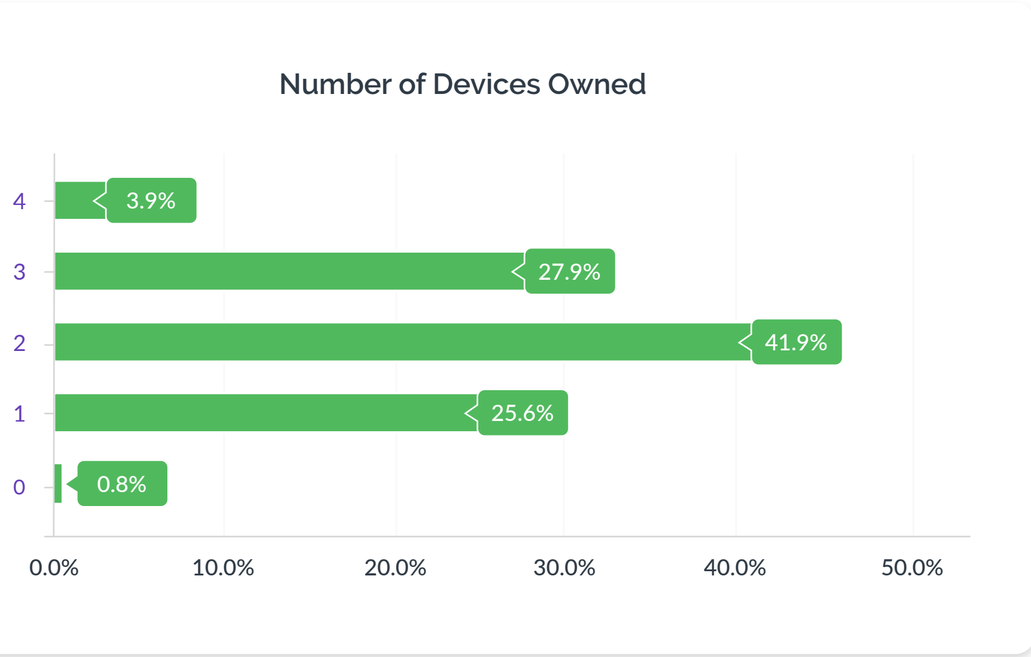
90% of American teens use social media platforms.* These are providing lifelines to young people who are increasingly feeling isolated by the pandemic. However, these platforms are also targeted by predators, for example in 2020, 20% of teens using the internet had received unwanted sexual solicitation online.**

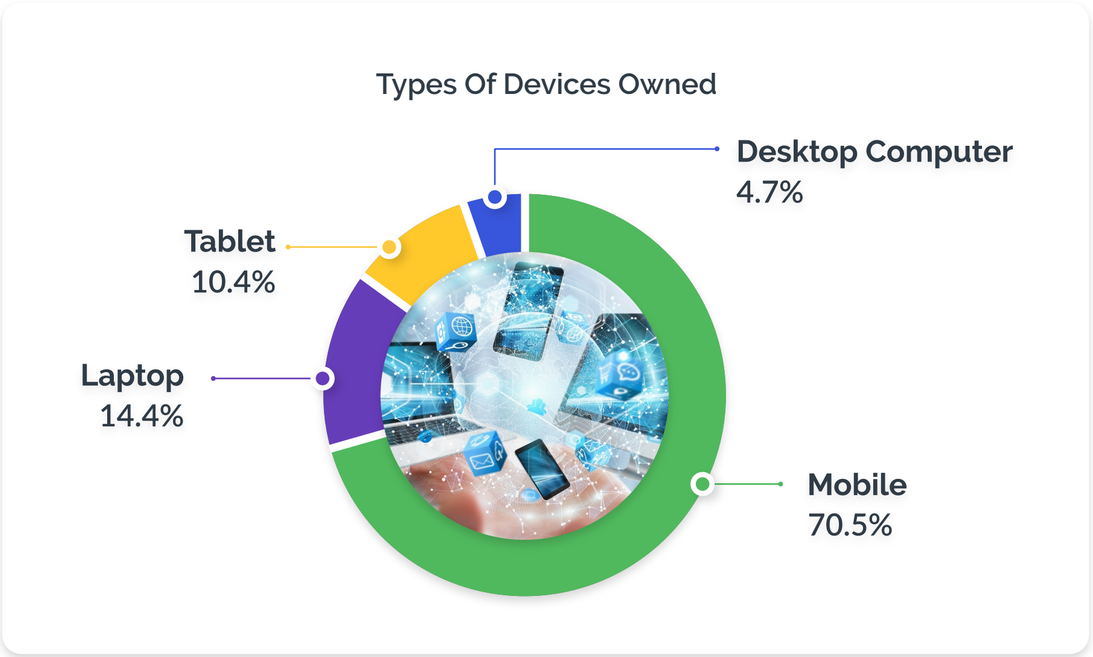
http://actforyouth.net/adolescence/demographics/internet.cfm

**http://www.unh.edu/ccrc/pdf/victimization_online_survey.pdf*

Many Ways to Connect, Many Avenues for Fraud

Most consumers -- and especially teenagers and younger children -- connect to the internet using a variety of platforms. While this means many more ways for businesses to connect with their customers, they also must keep these channels secure from inventive fraudsters. That's why it is critically important to protect every customer touchpoint. This is especially true for younger consumers, who are more likely to regularly use multiple devices. Nearly three-quarters of children surveyed by Arkose Labs own two or more connected devices.





Reports From the Digital Playground

Here are some examples of what our poll respondents reported as potentially suspicious behavior encountered online.

"I was playing a game on a website and random popups came up and I felt unsecure"

"I don't like when people I don't know send DMs"

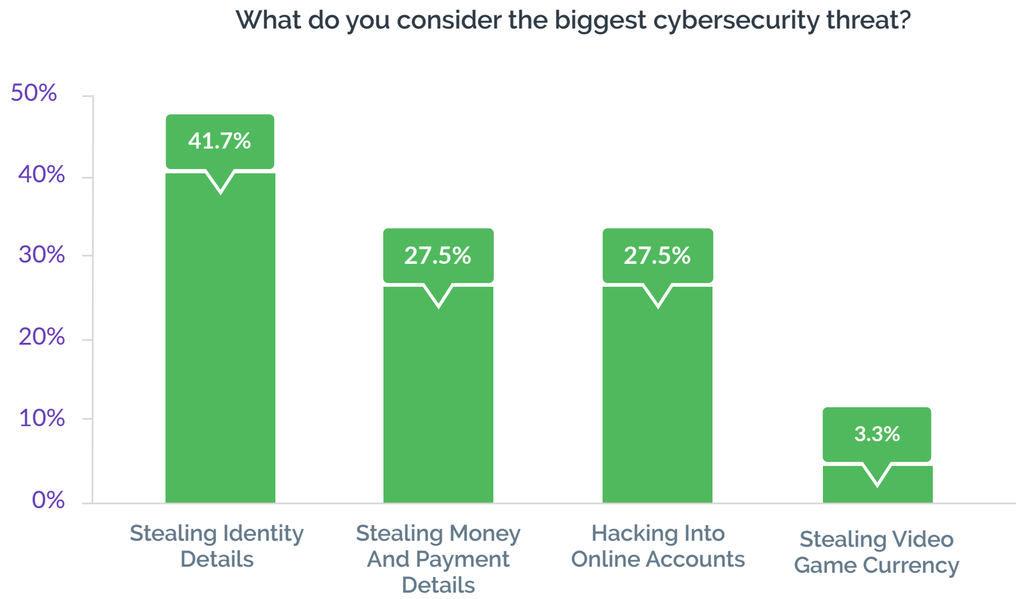
"A friend ran a public Instagram fan page and someone with a scary profile (that was known to send DM's getting people to do scary things) commented on her post and she blocked them"

"There was a website saying that a virus was in the phone but I didn't click on the link"

"I was playing an online game and there was a stranger that kept swearing at me, but I reported the person and they were then blocked."

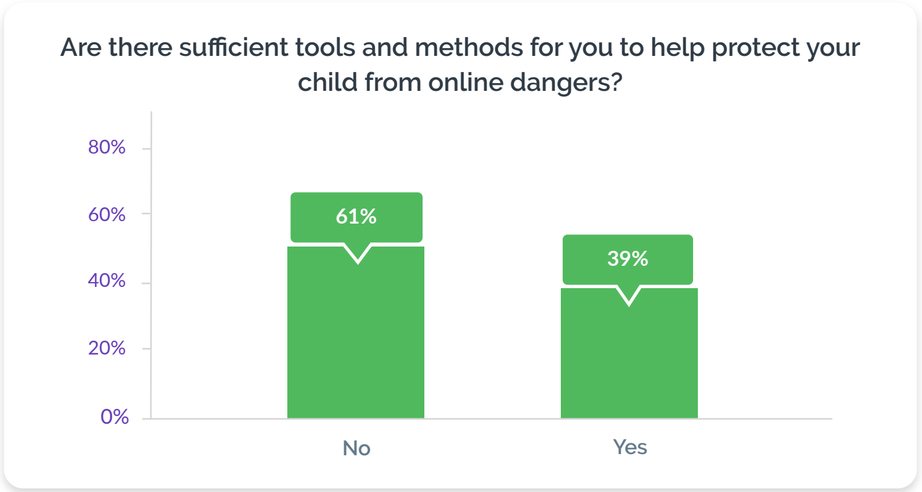
"Somebody was asking for my phone number, but I just wrote 1234567 and left."

"Not clicking random links. Strong passwords."



Businesses Must Gain the Trust of Mom and Dad

Historically, parents have a reputation of not always being fully aware as to what their children get up to online, however a 2020 study by SuperAwesome showed that during the pandemic 84% of parents have been checking their children's devices at least on a weekly basis. Parents still control the majority of youth spending on apps and sites. They will remove apps they don't trust, and on the flip side will be quick to recommend content that they do. They should be viewed as major stakeholders in the future of digital development for kids. With 61% feeling unsatisfied by current tools available to protect their children, there is a strong incentive for businesses to invest in ensuring their platforms are secure for young users.



Digital Safety: Actionable Advice for Parents

With busy lives themselves, parents can be hard pressed to always monitor what their child is doing online. Here then are some tips parents can use for instilling a sense of digital vigilance in their children.

- Talk to your children regularly about their lives online. Be open, and interested, and make sure they understand that nothing is private online.
- Teach them to understand and recognize potential threats. Stress that even seemingly friendly requests can have consequences down the line - online activities are permanent and cannot be erased.
- Help your children manage their risk: make sure they know not to purchase anything without your supervision, and not to open emails from strangers, or anything that seems suspicious.
- Keep your security software up to date. Also, don't use the same password across accounts and use robust parental controls.

Conclusion: Creating a Safer Internet

Covid-19 has forced digital acceleration to warp speed, with businesses and individuals alike scrambling to catch up. For young people, everything they know about internet safety is being tested all the time. Though they are light years ahead of their parents at equivalent ages, we need to remember that their understanding of risk doesn't always match their digital know-how.

While businesses are adapting to this, no amount of work in-house will be enough without a coordinated effort across industries. Fraudsters constantly share information, and businesses should too - collaboration is key in the fight for online security, and benefits everyone.

Young people are a fast growing customer base, and their spending power is often controlled by parents and guardians who repeatedly ask for better security measures. Parents' security concerns have massively increased over the past year, with nearly 80% citing digital safety for their children as a growing concern. Businesses should take note, and focus on security solutions that are user-friendly and adaptive to the customer demographic. By protecting young people, they will also improve customer loyalty, and ultimately, the bottom line. It will also help create a safer internet for all, both now and into the future.

About Arkose Labs

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
arkoselabs.com

Offices

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

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo