Gazal Shekhawat Didem Özkul February 10th, 2025

The many faces of online scams – four key deceptions targeted at children

When many people think about online scams, they think about financial scams targeted at older people, or at adults in general. However, children are also the targets of deceptive behaviour online. Here, Gazal Shekhawat and Didem Özkul of the Digital Futures for Children centre review the evidence around some of the ways that children might be manipulated or deceived in the online world.

This Safer Internet Day, we at the Digital Futures for Children centre are exploring some of the biggest threats to children's safety, well-being and rights in the digital world. We approach the theme "Too good to be true" by exploring the multitude of ways children are manipulated and deceived online. From deceptive design tactics that nudge kids into making unintended choices to the growing risks of AI-driven manipulation, technology-facilitated sexual exploitation, and gaming-related risks, the online landscape is full of complex challenges. This blog brings together key research insights from resources from our publicly available research database to highlight these pressing issues and what they mean for children, parents, and policymakers.

1. Deceptive design

Deceptive design refers to any features of digital products that manipulate users into choosing options that go against their "*best interests*". While also commonly called manipulative design or "dark patterns" the field is moving past the use of racialised language to more accurately describe the phenomena used by businesses to increase profits or retention.

- **Deceptive design features are common**: A 2022 US study by Radesky et al finds that four out of five apps used by young children (aged 3-5) contain manipulative design features. This includes blockades that hinder app navigation through pop-ups, encouraging parasocial interaction or lures

to increase the time and money spent on the platform, as well as advertising manipulations. The authors also find that some not-for-profit apps have more ethical designs.

- **Children disapprove of deceptive design but struggle to identify it**: Schäfer et al.'s recent study (2024) investigates German children's awareness of deceptive design features. It reveals that children are less approving of deceptive design features while rating fairer interfaces better. Most participants are also adept at identifying "fishy" practices but may struggle when encountering several at once, for example in rapid gameplays. According to the study, the four types of deceptions that children may encounter are "bad defaults", "emotional and sensory manipulation", "confirmshaming", and "trick questions".

2. Technology-facilitated sexual exploitation and abuse

Technology-facilitated child sexual exploitation and abuse encompasses any criminal activity involving the use of technology to sexually abuse or exploit children. This includes the production, distribution, and possession of child sexual abuse material (CSAM), as well as online grooming and enticement of children for sexual purposes.

- **It's a growing problem**: Maxwell (2022) highlights the ever-increasing proliferation and threat of CSAM due to the influx of digital technologies, particularly in relation to the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC). Maxwell calls for a move away from criminalisation and towards child-centred prevention to mitigate children's vulnerability to online risks. He also suggests that digital literacy can empower children and build resistance against online harms, as advocated by the Convention on the Rights of the Child (CRC).

- **Children need support to understand and disclose these experiences**: A Disrupting Harm project report on Conversations with Young Survivors about Online Child Sexual Exploitation and Abuse examines the experiences of 33 young survivors of online child sexual exploitation and abuse (OCSEA) from Kenya, South Africa, Namibia, Malaysia and Cambodia. Following the 'survivor conversations' approach, which ensures that young people are active participants in the research, the report highlights key moments leading to disclosure or discovery. The key messages from young people are: "Help me understand myself", "Online sexual exploitation does not take place in isolation", "Help me understand the Internet's rules", "Be available to talk about my online world", "Help when things go wrong", "Trust me", "Respect my privacy", "Understand my social life and needs", "Make clear where I can get help", "Do not judge me", and "Be there when I am ready to talk".

3. AI related manipulation

AI related manipulation refers to the misuse of artificial intelligence to deceive, exploit, or harm children. These methods have become increasingly sophisticated and difficult to detect, thereby elevating the risks for children online. Examples of AI related manipulation include AI-generated content, personalised manipulation, and amplified sextortion.

- **AI tools need child-centred design and enhance, not replace human support**: Kurian (2024) suggests that child-centred design for AI can protect children from potential risks of harm, especially concerning the "empathy gap" in Large Language Models (LLMs). She emphasises the need for responsible AI design, continuous monitoring, and child-centred safeguards to ensure that AI tools complement human guidance rather than replace it, thereby protecting children's rights and supporting their overall development.

- **Using emotional AI in education has clear disadvantages**: McStay (2020) examines the drawbacks of using AI to analyse students' facial expressions in the classroom. The paper raises serious concerns about this technology's use in education including the potential inaccuracies and biases based on flawed data, commercial exploitation of children, exploitation of children's emotions captured as data, violation of children's right to privacy, and psychological implications of being always tracked in the classroom.

4. Gaming related risks

Online games offer many benefits to children like problem-solving skills and opportunities for play but also pose potential risks. These may include addictive designs, pathways to gambling and the use of loot boxes by companies to drive up profits.

- **Vulnerable children face higher risks**: Richard and King conducted a meta-analysis of 44 studies showcasing the prevalence of online gambling among adolescents. They find that elongated use of video games, along with casino websites and loot boxes are correlated with engagement in "problematic gambling behaviour". Boys are more likely to engage in this behaviour than girls. Particularly, teens battling depression, behavioural disorders or lacking impulse control are more at risk of developing gambling problems.

- **"Luck-based" features like loot boxes are more harmful**: While loot boxes resemble other "microtransactions" present in games (such as the purchase of extra lives, coins, or performance boosters), they present more challenges. The rewards from loot boxes are unknown to users and randomised, meaning that children may need to buy several before getting their desired result. Brooks and Clark's longitudinal study across the USA, UK and Canada also shows that using loot boxes can increase the likelihood of gambling activity. This correlation was not found with microtransactions at large, highlighting the riskiness of "luck-based" transactions that gamers are

encouraged to select. While the study was conducted with younger adults (18-26), its findings speak to the need to regulate loot box design in kids' gaming apps.

As digital technologies evolve, so do the risks children face online. From deceptive design to AI-driven manipulation, technology-facilitated exploitation, and gaming-related harms, these challenges demand urgent attention. Research offers critical insights, but real change requires action—from policymakers enforcing stronger protections to platforms prioritising child-centered design. On this Safer Internet Day, let's commit to building a safer digital world where children's rights, safety, and wellbeing come first.

The author would like to thank Saumyadeep Mandal and Zichen Hu for their contribution to the database, Dr Ivelise Fortim for her inputs on gaming related harms, and Dr Didem Özkul for her contribution to this post.

This post gives the views of the author and not the position of the Media@LSE blog, nor of the London School of Economics and Political Science.

Featured images: Photo by Kelly Sikkema on Unsplash

About the author

Gazal Shekhawat

Gazal Shekhawat is a Research Associate at the Digital Futures for Children centre where she contributes to emerging research projects, administration, and communications. She is also a PhD researcher at LSE, where she studies how media and communications shape the everyday lives of women in India's Hindi heartland. Capturing their experiences at different stages of life and vocation, she seeks to understand how women navigate the push and shove of culture in the age of social media platforms. Before starting her PhD, she was a Research Fellow at Microsoft Research Lab, India where she worked on civic participation and misinformation on social media platforms.

Didem Özkul

Dr Didem Özkul is a Research Consultant at the DFC centre. Didem is interested in the social uses and societal implications of emerging digital technologies. Her recent research focuses

on AI and human agency, and the social uses and implications of human-machine communication.

Posted In: Internet safety