|  |  |
| --- | --- |
|  | **Document CWG-COP-21/INF/12** |
| **18 September 2024** |
| **English only** |
|  |  |
| Contribution by Kaspersky |
| MULTISTAKEHOLDER COOPERATION ON PROTECTING CHILDREN AGAINST DOXING |
| **Purpose**Multistakeholder cooperation on protecting children against doxing**Action required**This report is transmitted to the Council Working Group on child online protection **for information**. |

As a global cybersecurity leader, Kaspersky strongly believes that creating a safe online environment for children is a top priority that will shape our future, helping them thrive both in the digital world and in real life. The company is addressing this challenge both independently and in partnership with relevant government authorities, international organizations, non-governmental organizations (NGOs) and other stakeholders.

We would particularly like to underscore the concerning, steady rise of doxing, an activity that involves the gathering and dissemination of private data, typically with malicious intent, which could lead to the victim being blackmailed or facing retaliation.

According to a recent Kaspersky survey conducted in five countries in the Middle East, Türkiye, and Africa, 9 per cent of children have had damaging information and photos of themselves posted on social media. Another one of our company’s studies, conducted among more than 9 000 respondents from over 10 countries in Europe, Latin America, and the USA, revealed that an increasing number of individuals —including younger adolescents aged 16 to 18 years old— are sharing intimate images without considering the long-term consequences. Meanwhile, almost half (46 per cent) of respondents globally have either faced (7 per cent) or know someone who has encountered intimate image abuse.

Being particularly susceptible to emotional turmoil, children could struggle with the lasting effects of such harassment. Notably, victims often experience significant emotional and psychological distress, including anxiety and depression. The betrayal of trust can lead to enduring issues with suspicion and difficulties in maintaining healthy social interactions, self-esteem, intimacy, and personal safety. An additional problem is the digital footprint: children often don’t realize that the items they post online can remain accessible indefinitely.

To address this challenge, Kaspersky advocates for a concerted effort involving all stakeholders, including governments, international organizations, NGOs, and the corporate sector. This comprehensive approach should target a variety of audiences —children, parents, and educators— and focus on preventing and responding to the malicious use of personal information posted online, as well as analyzing children’s behavior on the internet.

The private sector can play a crucial role in addressing the issue of doxing and intimate image abuse by prioritizing education and conducting awareness campaigns. It is critical to implement comprehensive programs that teach children and their parents about digital literacy, consent, and the importance of privacy. This should include fostering open dialogue, allowing children to feel safe when discussing their online experiences and concerns.

To launch initiatives aimed at enhancing children’s protection online, Kaspersky is joining forces with its partners among government entities and international organizations worldwide. One vivid example of this collaboration is a recent joint program with the United Nations Children's Fund (UNICEF) and the Ministry of Digital Development of Kazakhstan, aimed at ensuring children’s safety in the online environment. Within these concerted efforts, the parties launched a series of free master classes for parents in different Kazakh cities and designed a bilingual brochure in both Russian and Kazakh, as well as a video about the importance of children’s digital literacy.

In conclusion, doxing and intimate image abuse pose significant risks that can have lasting effects on a child's safety and well-being. By educating children about online privacy, implementing preventative measures, and encouraging open communication, the multistakeholder community can help protect them from this growing threat. Ensuring a cybersecure future is impossible without mitigating future cyberthreats to our children as much as possible. As these challenges are constantly evolving, the same must be true for the way we protect the younger generation on the Internet, with the ultimate goal of staying one step ahead of malicious actors.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_