Policy recommendations

Technology fraud and online exploitation

The opportunity

Cloud computing is revolutionizing how people work, learn, interact, and play. Education is just one example as a new generation of cloud-based services connects students to an entire world of information and resources, while providing teachers with new ways to teach.

Social networks are another example, as people of all ages use a vast array of online services to form communities and connect with friends and colleagues. In addition, cloud services have become important vehicles through which people and governments advance fundamental values including freedom of expression, civic engagement, privacy, and free access to information.

The challenge

At the same time, online services have given rise to new risks and new potential for harm, especially for vulnerable populations such as children and the elderly. Predators use cloud-based services to create and distribute images of child sexual abuse and to solicit minors for sexual exploitation.

Scammers trick people into believing that they have nonexistent malware or viruses on their computer and into paying for unnecessary tech support services. Unfortunately, the methods that criminals deploy are becoming more sophisticated and harder to detect.

Policy recommendations

The unique challenges of protecting children, the elderly, and other vulnerable populations require a coordinated and comprehensive response. In many cases, existing laws need

to be updated to address current technologies and threats, balanced against the need to protect freedom of expression, individual privacy, and vibrant innovation. These updated legal frameworks should promote industry best practices and the development of technology tools that consumers can use to help protect themselves. Some of these areas include:

Strengthen and enforce laws to deter creation of online exploitation and fraud. Many existing laws that are intended to fight fraud and the exploitation of minors were not written to address online crimes and, as a result, are not vigorously enforced. According to the International Centre for Missing and Exploited Children, 35 countries still do not have legislation that deals specifically with child sexual abuse images. Of the 79 countries that do, 26 do not address computer-based offenses. In addition, many laws criminalizing the creation and distribution of images of child sexual abuse fail to cover the online world and are ill-suited to the new tactics of tech-savvy child predators. As governments update their laws to tackle these new threats, they should work closely with child rights, advocacy, and support groups, as well as technology suppliers—all of which play a role in protecting children and families in the digital age.

Support public-private partnerships. Public-private partnerships are essential to address the increasing variety and complexity of online threats. Governments, technology companies, and online service providers should work together to develop and share technology tools and expertise, conduct awareness campaigns, and educate the public about online risks. To address child protection, governments should consider joining the WePROTECT Global Alliance to End Child Sexual Exploitation Online, a coalition that includes 70 countries along with technology companies and civil society organizations dedicated to eradicating child sexual exploitation and abuse online.

Promote international cooperation. Increasingly, online crimes involve perpetrators in one country and victims in another, which can hamper effective prosecution. New international agreements and modernized mutual legal assistance treaties are needed to strengthen cross-border cooperation, information-sharing, and enforcement.

Promote consumer education. Many online crimes can be avoided if people are better informed about how to identify threats and protect themselves. According to a Microsoft-supported survey, one in five customers have experienced a fraudulent interaction online. Millennials are particularly vulnerable to fraudulent email and intrusive pop-up advertisements. Governments should focus on consumer online safety education to help people identify threats and protect themselves, with a special emphasis on schools so that young people learn to defend against online predators and enter adulthood with strong online safety habits. Governments should also consider joining and promoting awareness campaigns such as "STOP. THINK. CONNECT."—a global public-private partnership that offers basic guidance to citizens about safe online habits and practices.

Support industry self-regulation. Even as governments work to address the risks associated with online services, they can promote an environment of technological innovation and industry self-regulation that provides the flexibility to respond to the rapidly changing nature of online threats, which can be difficult to achieve solely through legislation. Governments and industry should work together to establish safety principles and service providers should be given the opportunity—and the responsibility—to determine the means of implementation.

Evidence and further reading:

WePROTECT Global Alliance to End Child Sexual Exploitation Online: http://www.weprotect.org/

STOP. THINK. CONNECT.: https://www.stopthinkconnect.org/

For links to these and other resources, please visit:
http://www.microsoft.com/cloudforgood