1. How do you define a culture of cybersecurity?

Security is a concept tied to rules running and involving real world, brought out from prepared and specialized personnel, even belonging to the police or other military strengths, in order to achieve the standards of safety and reaching the highest performance of social order, with the aim to establish discipline, rationality and coherence among stakeholder interests. It can be articled in different grades of warning, from the low level to the higher warning point, corresponding with a state of emergency.

The concept of the "cyber" redirect the concept of virtual world security, but even through this new settlement we do find applicable the rules of security above mentioned, with the only exception that the vulnerability assets must be strictly checked and the warning rise suddenly to the highest level due to an easiest way for anyone to be hidden behind false accounts, pictures or false statements. Certain sites could even lead directly to scam sites in order to steal personal informations and this corresponds to an higher amount of danger that the user may encounter. One of the duty of postal and communication investigators is to inspect upon social meeting sites, dark sites and financial sites in order to prevent any potential and possible cybercrime .

2. What are typical values and norms that are important to you or your constituents?

In order to ensure that all the devices work on a regular basis it is convenient to check them regularly with specific antivirus, antispyware and antimalware software. One of the rule that is necessary to follow strictly is avoiding to leave personal password or bank codes memorized in common and public devices, otherwise that could bring directly to a violation of privacy .

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.

School represents since ever the mediator between the society and the learning community and it aims to build children personalities and their behavioral assets as well. During latest 10 years learning communities knew a more massive employment of New Technologies and devices, apps, teaching and learning education platforms are nowadays considered integrated to the schooling process. Words as implementation, app, platform, cybernetics that once were used for science fiction are today used in the common language and this involves a modernization of the teaching methods, in order to let them being attractive and motivating towards the students.

School is the favorite place where security is focused on, above all because being the students until 18 minors law imposes strict rules regarding surveillance upon them. So periodically school organize meeting with communication police's forces to enhance knowledge of recent laws and to report recent cybercrimes in order to let people being aware of all the danger to which they are exposed at.

4. are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?

I follow simple rules as avoiding to open any mail from unknown sender, and above all any kind of attachment the email could be a good starting point . I always inform there are dark sites which children must avoid to visit, and surely families have to be aware of all the accounts their children dispose and of all the sites they visit, and I try to let families know what kind of risks their children are exposed to.

5. **Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?**

Students often take video during lessons and even all the sanctions they have been given**,** they continue to make video for uploading them on the net. Notwithstanding all the recommendations each teacher suggested, they aren't able to get rid of that bad habit.

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

Implementing cybersecurity norms is something related with specific technical competencies but lot of tips come from ordinary usage and above all from advices given from children.

I have personally experienced several attacks directed from unknown cyber pirates to my bank account online.. I've even received false phone calls to my personal cell phone that advised me to change the password of my bank account online and to communicate this to the operator who was talking to me.
I have promptly informed internet Police department which advised me upon the best practices to utilize in order to discourage, prevent and contrast those kinds of circumstances.

Furthermore, a dear friend of mine was contacted from a man who pretended to be an American business man working in Turkish. After a couple of months it run out that he was a fake, that false man used the image of the present Bulgar minister of culture and tried to steal money to my friend because he mocked to have been taken from some thieve who stole all the money he has to give to his workers. I started to have some suspect upon his real intention and asked to my friend I could have done some search upon google image. In this way it came out he was a fake, that photos belonged to the minister of culture in Bulgaria, and this discovery surprised a lot my friend and me.

7. Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

The chief of the school is the headmaster who cooperated with his deputy and an Administrative Director. Together they take decisions in order to establish rules and fix principles to protect children and prevent any kind of illegal act who may compromise the school's reputation but above all the safety and the integrity of students and of their families.

The headmaster is responsible of digital services of the school, and he provides to settle securities measures within each building of the school for which he had delegated a trustee teacher. In Italy a recent law of 2017, n 71, and the related guidelines soon after edited, proposes all the safety measure to prevent cyber bullying episodes, by individuating an admonition responsible in case of cyber bullying events, and suggests several opportunities even in cooperation with cybercrime police, for educative campaigns of information, contrasting and prevention of cyber violence. The recommended subjects are: preferences about social, in order to prevent any kind of pedophile attempt to corrupt the minor, monitoring the habit of minors in order either to prevent bullying towards a single or a group either to let Police intervene upon any kind of cyber attack, consciousness about the newest types of violence .

CRISTINA CUOMO SEPTEMBER 14TH 2018