Resolution GA/3/1.1

Social, Humanitarian, and Cultural Second Committee

Co-sponsors: Kingdom of Bhutan, Bosnia and Herzegovina, republic of Cameroon, Union of the Comoros, Republic of Cyprus, Dominican Republic, Federal Democratic Republic of Ethiopia, Federal Republic of Germany, Republic of Italy, Japan, State of Kuwait, Republic of Liberia, Republic of Lithuania, United Mexican States, Kingdom of Morocco, Kingdom of the Netherlands, Republic of Nicaragua, Republic of Paraguay, Kingdom of Saudi Arabia, republic of Senegal, Republic of Serbia, Republic of Korea, United Arab emirates, United Kingdom of Great Britain and Northern Ireland, Bolivarian Republic of Venezuela, Republic of Zimbabwe

Topic: Countering the use of information and communications technologies for criminal purposes

Alarmed by the dangers of online harassment,

Deeply concerned by the fact that we cannot identify the people who commit cyberbullying,

Fully aware that financial losses is a big part of cybercrime,

Realizing that insecure websites are causing major loss because of cybercrime,

Deeply concerned about the number of scams that are successful,

Concerned that people are stressed due to the loss of personal information because of scams,

Alarmed by the cybercrimes happening each year,

Deeply concerned by multiple identities online,

Fully aware of the predators in the digital world, Realizing the presence of insecure websites that steals information,

Having heard of the fake websites that exist,

Cyberbullying and Online Harassment

1. Recommends creating a cybercrime hotline;
2. Further invites member states in a better cyber secure place to help fund better security system;
3. Introduces the idea of member states signing a treaty to further protect citizens from cybercrime;
4. Encourages countries with a better security system to share the knowledge about their cyber safety;

Financial Cybercrime and Insecure Websites

5. Calls upon all member states to enhance their firewalls;
6. Further invites member states to filter insecure websites to prevent further cybercrime;
7. Requests all technology companies to create an alert that shows when a website is insecure;
8. Calls for member states to educate their people about cybercrime for further prevention;
9. Encourages countries to collaborate with other member states to create strict international laws to combat financial cybercrime;
10. Further invites cybersecurity organizations to set focus on cyberattacks that relate to financial theft;

Online Scams

11. Emphasizes that people should be informed on how to identify scams;
12. Inform children at schools on how to identity scams;
13. Emphasizes having more complex passwords;
14. Encourages countries to donate money for VPN funding;
15. Calls upon countries to encrypt the passwords file/websites to enhance security;

16. Urges government to educate its citizens on phishing messages/emails;
17. Advises the creation of an agency to ensure that websites are not scamming their users;
18. Requests that member states inform each other about scams;

Personal Information and Identity Theft

19. Advises countries to educate their citizens about identifying theft and predators;
20. Calls for governments to have databases that validate identities;
21. Considers providing more kinds of alerts about whether the websites are secure and sort them;
22. Strongly advises a better system to flag suspicious accounts;
23. Welcomes the usage of strong, complex passwords and enable 2-factor authorization;
24. Further recommends that guilty individuals be found and banned from technology for a period of time depending on the charges.