|  |  |
| --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2009-2012 | **Joint Coordination Activity on Accessibility and human Factors (JCA-AHF)** |
|  | **Doc. 133** |
| **English only****Original: English** |
| **Source:** | JCA-AHF Convener |
| **Title:** | Overview of cybercrime targeting persons with disabilities (document submitted by Mali to Question 22/1 - Securing information and communication networks: best practices for developing a culture of cybersecurity, Second Meeting of ITU-D Study Group 1 Geneva, 5-9 September 2011)  |

This document is submitted for information.

|  |  |
| --- | --- |
| TelecommunicationDevelopment SectorStudy Groups |  |
| Second Meeting of ITU-D Study Group 1 |  |
| Geneva, 5-9 September 2011 |  |
|  |  |
|  | Document 1/69-E |
| 2 July 2011 |
| Original: French |
|  | For action |
| Question 22-1/1: Securing information and communication networks: best practices for developing a culture of cybersecurity |
| SOURCE: | Mali |
| TITLE: | Overview of cybercrime targeting persons with disabilities |
| Action required: | Application of the proposals |

Abstract

Access to and the constant evolution of new information technologies have paved the way for massive expansion of the web. This has improved our lives, but has also prompted an exponential rise in cybercrime. However, we note that some members of the population (e.g. senior citizens and persons with disabilities) are the most vulnerable. A series of proposals are put forward to protect this segment of society.

Introduction

As entire aspects of our lives (medical or banking data), our production methods (corporate IT or industrial equipment) and our defence increasingly depend on information systems, cybersecurity becomes a vital necessity.

Actions to combat the digital divide have enabled widespread access to new technologies, which, while improving lives, has also made swindles and fraud in general an everyday issue. However, it should be noted that some segments of society are much more vulnerable to these threats, namely:

* children
* persons with disabilities
* senior citizens
* Focal Point: Name/organization/entity: Mr Abdoulaye Dembele, Mali Telecommunication Company
* Phone number: +223 6 670 2312
* Email: dembelea@yahoo.fr
* women.

What kind of threats do these vulnerable segments of society face? Developing countries typically constitute a very fertile ground for bourgeoning cybercrime.

What measures must we take to protect these people?

**Cybercrime targeting vulnerable segments of society**

**Cybercrime and culture**

A people's culture is a feature for their identity and cohesion. It is undeniable that the developing countries are enduring rather than participating in the march of globalization. Their cultures are being reshaped under the noses of the government and population, powerless to do anything about it. The effects, particularly evident on the population, are compounded by the extraordinary technological progress in mass electronic communication, which is invading the airwaves, a collective asset, without effective control or supervision by government authorities.

**Cybercrime and e-commerce**

Whatever one's difficulties, whatever one's disability, everyone must be able to access e-commerce just like the average person. What are the dangers that may face a paralysed person wishing to shop over the Internet, or a sight-impaired person wishing to conduct a banking transaction at an ATM?

**Cybercrime and fraud ("swindles")**

The rapid evolution and changing nature of information technologies, coupled with the rapid expansion of the web over the last 10 years, plus the exponential growth in the speed of data exchanges, have considerably raised the hopes of organizations/associations of paralysed or sight-impaired/blind people. However, the fact that e-services are available to everyone has made cybercrime a prolific problem, insofar as it allows people with malicious intent to commit offences at the expense of associations of persons with disabilities.

**Proposed measures**

* Legislation: We believe that the every country must take all possible action to adopt suitable cybercrime legislation. We must never cease impressing upon governments that combating cybercrime is a matter of survival for the nation.
* Training: Training takes place at two levels. First, at the "macro" level: training and exchanges of experiences for legal staff, in order to equip them with the required competencies in relation to cybercrime. Secondly, at the "micro" level: creating a network of trainers and focal points to educate and raise awareness among associations or organizations of persons with disabilities on the use of new technologies, while drawing their attention to the dangers and threats it entails.
* Agencies: Governments must encourage the creation and implementation of agencies, organizations or entities that will combat this scourge and effectively manage incidents. Developing country governments have so many priorities that only such agencies/organizations will be able to combat cybercrime effectively. However, governments must allocate the necessary financial and structural means to these agencies/organizations.
* Subregional integration: The world is a "global village", and so no country can effectively fight against cybercrime on its own. A cybercrime can be committed even when the criminals and the targeted victims are not in the same place. It is essential that nations develop a well-coordinated system of collaboration. However, regional differences in law may constitute an obstacle in combating cybercrime: content deemed illegal in one country may be legally displayed on a server in another. Most mutual legal assistance is based on the principle of dual criminality, such that investigations focus on acts that are criminalized in all the countries affected, and problems arise when laws diverge. Accordingly, subregional organizations like the Economic Community of West African States (ECOWAS) or the West African Economic and Monetary Union (WAEMU) need to harmonize legislation in force and/or new legislation.
* Cybersecurity technologies: A vast awareness campaign needs to be conducted to make sure all large centres using the Internet (e.g. cybercafés), companies or enterprises and Internet service providers have reliable security infrastructures.

Access to and the constant evolution of new information technologies have paved the way for massive expansion of the web. This has improved our lives, but has also prompted an exponential rise in cybercrime. However, we note that some members of the population (e.g. senior citizens and persons with disabilities) are the most vulnerable. A series of proposals are put forward to protect this segment of society.

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