|  |  |
| --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2009-2012 | **Joint Coordination Activity on Accessibility and human Factors (JCA-AHF)** |
|  | **Doc. 142** |
| **English only****Original: English** |
| **Source:** | JCA-AHF Convener |
| **Title:** | Overview of cybercrime targeting persons with disabilities and other vulnerable persons (document submitted by Viable, France Q.20/1 and Q22/1, 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 1/75-E |
| 5 July 2011 |
| Original: French |
|  | For action |
| Question 20-1/1: Access to telecommunication services and information and communication technologies (ICTs) by persons with disabilities |
| Question 22-1/1: Securing information and communication networks: best practices for developing a culture of cybersecurity |
| SOURCE: | Viable France, France |
| TITLE: | Overview of cybercrime targeting persons with disabilities and other vulnerable persons |
|  |  |
| Action required: | The meeting is requested to take note of this document and to bear it in mind when elaborating the guidelines |

Abstract

Use of the Internet has enabled widespread access to new technologies which, while improving lives, has also made swindles and fraud in general an everyday issue. It is, moreover, to be noted that some segments of society are much more vulnerable to these threats, namely:

* children
* persons with disabilities
* senior citizens
* women.

Focal Point: Name/organization/entity: Mr Michel René Lemaitre, Viable France, France

Phone number: +33 6 68 54 93 67

Email: michel.lemaitre@ties.itu.int

1 Introduction

Use of the Internet has enabled widespread access to new technologies which, while improving lives, has also made swindles and fraud in general an everyday issue. It is, moreover, to be noted that some segments of society are much more vulnerable to these threats, namely:

* children
* persons with disabilities
* senior citizens
* women.

**2 European Union standpoint**

In response to the development of cybercrime in recent years, the European Commission has, in close cooperation with the Member States and other EU institutions, elaborated a policy on the fight against cybercrime. The communication from the Commission entitled "Towards a general policy on the fight against cyber crime", issued in 2007, sets out the main pillars of the EU's policy: increased cooperation on law enforcement, public-private partnership and international cooperation.

In 2010, the Commission put forward a proposed directive on attacks against information systems in response to the growing number of large-scale cyberattacks directed not only against companies but also, and increasingly, against governments, an example of this being the 2007 cyberattacks against Estonia. The key novelty of the proposal lies in the criminalization of the use, production and sale of tools (known for the most part as "botnets") for mounting attacks against information systems. The proposal is currently being debated in the European Parliament and Parliament of the Council.

In addition to the criminal aspects of cyberattacks, the corresponding security aspects are being addressed under the Commission’s initiative on Critical Information Infrastructure Protection (CIIP). In March 2009, the Commission published a communication on CIIP entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". The participation of ENISA (European Network and Information Security Agency) is intended to support the exchange of best practices among Member States.

The Commission has also stepped up dialogue with the private sector, which controls a major part of the information infrastructures and whose involvement in the fight against cybercrime is crucial. Recommendations dealing with operational cooperation between police authorities and private operators were approved by the Justice and Home Affairs Council under the French presidency of the EU in November 2008, and were supplemented by other conclusions of the Council under the Spanish presidency in April 2010.

The Commission is also in the process of establishing a European platform on cybercrime/research training in partnership with the Member States, Europol, CEPOL, universities and the private sector.

The following link is to the European Commission’s web page concerning the fight against cybercrime (in English only): <http://ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm>.

**3 Standpoint of UNAPEI, the French association for persons with disabilities**

Family members and professional carers must devote time to passing on recommendations to persons with disabilities regarding Internet usage, such as:

− Don’t give out personal contact details

− Don’t post any photos

− Don’t arrange to meet with anyone encountered on the Internet without discussing the matter with a close individual (e.g. a parent, professional carer, etc.)

− Use a pseudonym

− Don’t trust anyone you don’t know

− Don’t use the webcam with someone you don’t know

− Don’t say anything insulting, hurtful or racist

− If a website makes you feel uncomfortable, leave it immediately

− Be on your guard if money is mentioned.

In this regard, two key questions arise:

− What kinds of threat do these vulnerable segments of society face?

− What measures must we take to protect these people?

**4 Threats**

⦁ Cybercrime and culture

A people's culture is a feature of 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 paralyzed 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 ten years, plus the exponential growth in the speed of data exchanges, have considerably raised the hopes of organizations/associations of paralyzed 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.

**5 Proposed measures**

⦁ Legislation

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 experience 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 to will 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", which means that 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 adopt 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.

Finally and above all, every effort has to be made to make cybercriminals “visible” in order to dissuade them. Cybercriminals are by nature cowardly and do not want to be exposed.

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