Lesson 1.5 – Cybercrime Basics

|  |  |  |
| --- | --- | --- |
| Lesson 1.5 Cybercrime Basics | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * PowerPoint presentation * Projector and display screen * Internet access (if available) * Whiteboard * Whiteboard pens (at least 2 each of blue, black, red and green) * 2 Flipcharts with adequate paper * Student notepaper and pens. * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily | | |
| **Session Aim:**  This session provides the delegates with an introduction to the information society & cybercrime, and identifies international organisations and their efforts to tackle this modern type of criminality.  Tit also serves to provide basic definitions of cybercrime, consider the CoE Budapest Convention and define contemporary forms of cybercrime. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Identify different types of cybercrime and their impact * List the threats, trends and tools of cybercrime and responses to the phenomenon. * Explain the concepts of cybercrime that are considered types of crime under most legislation and international standards * Analyse the needs and the advantages of the harmonisation between national legislation and the international instruments, in particular the Budapest Convention | | |
| **Trainer Guidance**  This session is intended to provide trainers with a framework for developing training material to be delivered as part of a wider programme. It cannot be comprehensive as technology changes so rapidly that any detailed technical specifications would be out of date almost as soon as the document is published. Ensuring that Judges and prosecutors have sufficient understanding of technical issues as they relate to matters before them is essential to the fair running of any judicial system. This session provides an overview of the relevant aspects of cybercrime and its relevance to the criminal justice system. A PowerPoint presentation is provided as a resource for trainers to use if considered appropriate.  This session provides information about technology and terminology that will be encountered by Judges and prosecutors during their work and which is used by criminals to commit crime and law enforcement to detect it. The Powerpoint presentation seeks to aid in presenting the technologies to the delegates. However, it should only serve as a template and needs to be adopted by the trainer to fit the target audience, the schedule and the information relevant to his/her country. The trainer should look to use practical and real world examples and demonstrations to emphasise the learning and should add their own experiences and knowledge to the presentation with their own case studies where appropriate.  The time allocated to this session is 90 minutes, so it will be necessary for the trainer to adapt the materials to meet the needs of each audience and these may be different, for example depending on the legal system in the country or countries where the training is taking place. As mentioned, this material provides a framework upon which the trainer should prepare their material to be delivered, in accordance with the lesson objectives.  The times listed below are indicative of the amount of time to be allocated to each section of the lesson. Of necessity, this will mean that some parts will be dealt with across more than one of the three allocated sessions.   * Introduction and opening (Agenda and Session objectives) (5 Minutes) * Part 1 - The ‘Information Society’ (10 minutes) * Part 2 - What is Cybercrime? (10 minutes) * Part 3 - Budapest Convention (10 minutes) * Part 4 - International organisations for Cybercrime (10 minutes) * Part 5 - Cybercrimes & case studies (40 minutes) * Summary (5 minutes)   The slide pack for this presentation is extensive – and there is guidance in the Lesson Content section below about what is essential and which could be removed/hidden if necessary | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 4  Mandatory | The opening slides are the introduction to the session and include the Agenda and the session objectives. The trainer should ensure that these are amended where it has been decided to exclude sets of slides or subject areas. These slides set the scene of where the presentation is going.  Some of the content of the introduction to technology section has been brought into this section. | |
| 5 to 16  Important | This section seeks to introduced the delegates to the Information Society – and why this has spurned the phenomenon of Cybercrime.  Trainers may choose to describe this in their own way but this set of slides with builds will provide an overview of the background and the issues. | |
| 17 to 23  Mandatory | These slides deal with introducing the concept of Cybercrime – and trying to describe, in the absence of a formal definition, what it is.  Trainers can get the delegates to form their own opinions on the subject – allowing them to express themselves – but bringing the collective views back to slide 24 where there is an overarching ‘description’. | |
| 24 to 33  Mandatory | This section talks about the Budapest Convention and gives a background to it and its existence. With this being dissected later in the short course, this is very much an introduction. | |
| 34 to 51  Important | This section tries to identify he relevant organisations that are involved in the investigation of Cybercrime activities on an international basis.  Again, the trainer can allow the delegates the opportunity to list them and perhaps, with time permitting, describe any interaction they have had with these. | |
| 52 to 98  Mandatory | This section allows the trainer to work through many of the Cybercrimes and describe them – allowing time to discuss the issues and logistics in uncovering and investigating them.  The early part of the session is description – whilst the end of the session are slides on the trends that are being seen – and the sort of crimes the judges and prosecutors may have before them.  The trainer can use their own examples of encountering these crime types if necessary introducing their own case studies where appropriate. | |
| 99 to 100  Mandatory | The final section provides the opportunity for the trainer to reflect on what has been taught in the lesson and ensure that the objectives have been met. It also provides the delegates with the same opportunity and to raise any issues that may require clarification. | |
| **Practical Exercises**  No practical exercises are envisaged for this particular session as there is no guarantee that the level of technology and Internet access to deliver such exercises will be available at all venues.  Trainers may in the future seek to supplement to learning by adding exercises, where the training is delivered in an environment where the facilities are suitable. | | |
| **Assessment/Knowledge Check**  No specific knowledge check in addition to that listed above is currently envisaged for this course. No official assessment has been requested. | | |