**Lesson Plan**

Lesson 1.1.2 (Introduction to Cybercrime - Threats, Trends and Challenges)

|  |  |  |
| --- | --- | --- |
| Lesson 1.1.2 (Introduction to Cybercrime) | | Duration: 120 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The overall purpose of this session is to provide to the delegates an introduction to the information society and cybercrime, international organisations and their efforts to tackle this modern shape of criminality, basic definitions of the cybercrime, Council of Europe (CoE) Budapest Convention and existing 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 has been prepared to provide delegates with a comprehensive understanding of the place of the cybercrime and cyber criminality in the first quarter of 21st Century. This session has been divided into seven parts. First part of the presentation will describe the new realities of the information society and will refer to the emerging illegal activities on the networks. Second part will recover some of the historic approaches to cybercrime, by some international organisations. Third part will try to arrive to the reality covered by the eventual concept of cybercrime. Fourth part will explain what the Budapest Convention on Cybercrime is and will underline the importance of this single binding international instrument in fighting cybercrime. Fifth part will refer to some of the more important illegal activities online, nowadays. Sixth part will briefly touch upon major vectors of contemporary and emerging trends of the cybercrime. Part Seven will recover the major topics of all the presentation. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 19 | These slides intend to provide the delegates with an understanding of the contemporary aspects of the information society and meaning and implications of the. Also, explanation of the global phenomenon of the Internet and its good new forms of human organisation and interaction by using new technologies at our disposal aspects is very much relevant, what should be introduction to the first forms of the cybercrime as such.  Global aspect and internationalisation of the crimes perpetrated on all levels of computer networks in the world is nowadays astonishing, what opens new questions about possibilities at disposal to the legal enforcement agencies, prosecution and judiciary to tackle the problem with efficiency.  Modern challenges, cybercrime phenomenon’s and digital and cyber environment should be presented to the delegates in the manner which will provide them basic understanding and impressions about how much present and evolving this criminality is.  Also, issues related to the protection of critical infrastructures from cyber-attacks, cyber security and cyber warfare are making this comprehension even more complex. | |
| 20 to 32 | These slides are covering outsets of the terms which are used in the terminology of the contemporary cybercrime. The terms “computer crime”, “high-tech crime”, “IT crime” and “cybercrime” are often intermingled and create confusion and misunderstanding. Technology can be used (abused) in number of the ways, which must be gradually explained through the slides. All aspects are important and existing in cybercrime cases through-out the world of today.  Also, trainer should explain broader and narrow sense of the cybercrime and compare it with traditional forms of the criminality and to put it in the perspective of the real life circumstances and consequences. | |
| 33 to 37 | These slides are giving the introductory scope to the most important international treaty regarding cybercrime today, which is Council of Europe Cybercrime Convention (ETS 185), commonly known as “Budapest Convention”. | |
| 38 to 58 | These slides introduce the delegates to some international initiatives and mechanisms for combating cybercrime, from most global to the local level, including various organisations, agencies and treaties that can enable and facilitate effective reaction of the domestic and international LEA, Prosecution and Judiciary. The trainer should explain these different international responses to cybercrime. The slides cover United Nations, G8, EU, OSCE, Council of Europe and regional and local level organisations, treaties and documents, and their responses to the cybercrime, each of which should be introduced to the delegates. | |
| 59 to 85 | These slides are providing comprehensive basic presentation and insight in majority of the illegal activities and cybercrime tools of today. Phishing, spam and spamming, malware in broader and narrow sense, computer viruses, computer worms, spyware, ransomware, computer Trojans, botnets, DarkNet, and TOR, are just some of the examples, but very important ones.  Trainer should especially concentrate on contemporary and locally important forms of these activities by engaging more closely with the delegates and gathering necessary knowledge to understand with this regards which forms are most troublesome for the audience. | |
| 86-95 | These slides are providing brief and basic introduction to the current trends in the perpetration of the criminal acts. Mobile platforms, banking malware, ransomware and business e-mail compromise, hactivism and abuse of the social networks, IPR infringements, advanced persistent threats and its forms, mobile transactions and cryptocurrencies, Internet of Things and its aspects, all of these forms and trends of cyber criminality are very much present today and inflicting outstandingly large damages to the World.  Presenter should interact with delegates during this portion of the presentation and find out what contemporary forms are present on the local level. | |
| 96-98 | Summary. What is cybercrime and why worry about it.  Threats, trends and tools of cybercrime and responses to the phenomenon.  Realities covered under the expression *cybercrime* and concepts that are considered types of crime under most legislation and on international standards.  Need and advantage of the harmonisation between national legislation and the international instruments, in particular the Convention of Budapest. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |