**Plano de aula**

Aula 1.1.2 (Introdução ao cibercrime - Ameaças, tendências e desafios)

|  |  |  |
| --- | --- | --- |
| Aula 1.1.2 (Cooperação internacional) | | Duração: 120 minutos |
| **Materiais necessários:**   * PC/computador portátil com versões de software compatíveis com os materiais preparados * Projetor e ecrã de exibição. * Acesso à Internet (se disponível). * Bloco de notas de estudante e canetas. | | |
| **Objetivo da sessão:**  O objetivo geral desta sessão é fornecer aos delegados uma introdução à sociedade das informações e ao cibercrime, organizações internacionais e seus esforços para combater esta forma moderna de criminalidade, definições básicas do cibercrime, Convenção de Budapeste do CoE e formas contemporâneas existentes de cibercrime. | | |
| **Objetivos:**  No final da sessão, os estudantes serão capazes de:   * **Identificar diferentes tipos** de cibercrime e o seu impacto. * **Enumerar ameaças, tendências e ferramentas** de cibercrime e respostas ao fenómeno. * **Explicar os conceitos** de cibercrime que são considerados tipos de crime na maioria da legislação e normas internacionais padrão. * **Analisar as necessidades e as vantagens da harmonização** entre a legislação nacional e os instrumentos internacionais, em particular a Convenção de Budapeste | | |
| **Guia de formação**  Esta sessão foi preparada para fornecer delegados com uma compreensão abrangente do local do cibercrime e cibercriminalidade no primeiro quarto do século 21. Esta sessão foi dividida em sete partes. A primeira parte da apresentação irá descrever as novas realidades da sociedade de informação e irá referir as atividades ilegais emergentes nas redes. A segunda parte irá recuperar algumas das abordagens históricas sobre o cibercrime, por algumas organizações internacionais. A terceira parte irá tentar chegar à realidade abrangida pelo eventual conceito do cibercrime. A quarta parte irá explicar o que a Convenção de Budapeste sobre Cibercrime é e irá destacar a importância deste simples instrumento internacional de vinculação ao combate ao cibercrime. A quinta parte irá referir algumas das atividades ilegais online mais importantes nos dias de hoje. A sexta parte irá abordar brevemente os principais vetores das tendências contemporâneas e emergentes do cibercrime. A sétima parte irá recuperar os principais tópicos de toda a apresentação. | | |
| **Conteúdo da aula** | | |
| **Número dos slides** | **Conteúdo** | |
| 1 a 3 | Os primeiros slides expõem a estrutura e objetivos desta sessão. Os delegados devem ter a oportunidade de fazer quaisquer perguntas preliminares que possam ter relativamente à estrutura e objetivos da sessão. | |
| 4 a 19 | Estes slides destinam-se a fornecer aos delegados uma compreensão dos aspetos contemporâneos da sociedade das informações e o significado e implicações. Além disso, uma explicação do fenómeno global da Internet e as suas boas novas formas de organização e interação humana através da utilização de novas tecnologias ao nosso dispor, aspetos muito mais relevantes, qual deve ser a introdução às primeiras formas de cibercrime, como tal.  Aspeto global e internacionalização dos crimes cometidos em todos os níveis de redes de computadores a nível mundial nos dias de hoje é fascinante, o que abre novas questões sobre possibilidades à disposição das agências policiais, acusação e judicial para enfrentar o problema com eficiência.  Desafios modernos, o fenómeno do cibercrime e o ambiente digital e online devem ser apresentados aos delegados na forma que irá fornecer-lhes uma compressão e impressões básicas sobre o quão presente e envolvente a criminalidade é.  Além disso, questões relacionadas com a proteção de infraestruturas críticas de ataques cibernéticos, cibersegurança e guerra cibernética estão a tornar esta compreensão ainda mais complexa. | |
| 20 a 32 | Estes slides abrangem desde do início dos termos que são utilizados na terminologia do cibercrime contemporâneo. Os termos "crime informático", "crime de alta tecnologia", "crime de TI" e "cibercrime" são normalmente misturados e criam confusão e mal entendidos. A tecnologia pode ser utilizada (abusada) de várias formas, que devem ser explicadas gradualmente através dos slides. Todos os aspetos são importantes e existentes nos casos de cibercrime através do mundo de hoje.  Além disso, o formador deve explicar amplamente e resumir o significado do cibercrime e compará-lo com as formas tradicionais de criminalidade e colocá-lo em perspetiva com as circunstâncias e consequências da vida real. | |
| 33 a 37 | Estes slides fornecem o âmbito introdutório para o tratado internacional mais importante relativamente ao cibercrime dos dias de hoje, que é a Convenção do Concelho Europeu sobre Cibercrime (ETS 185), normalmente conhecida como "Convenção de Budapeste". | |
| 38 a 58 | Estes slides apresentam os delegados a algumas iniciativas e mecanismos internacionais de combate ao cibercrime, do nível mais global ao mais local, incluindo várias organizações, agências e tratados que podem permitir e facilitar a reação efetiva de LEA nacional e internacional, processual e judicial. O formador deve explicar estas diferentes respostas internacionais ao cibercrime. Os slides abrangem as Nações Unidas, G8, UE, OSCE, Concelho Europeu e organizações a nível regional e local, tratados e documentos e as respetivas respostas ao cibercrime, cada um será apresentado aos delegados. | |
| 59 a 85 | Estes slides fornecem uma apresentação básica e visão compreensiva sobre a maioria das atividades ilegais e ferramentas de combate ao cibercrime de hoje. Phishing, spam e spamming, malware no sentido mais abrangente e restrito, vírus informáticos, worms informáticos, spyware, ransomware, Trojans informáticos, botnets, DarkNet e TOR são apenas alguns dos exemplos, mas talvez os mais importantes.  O formador deve especialmente concentrar-se nas formas contemporâneas e importantes localmente destas atividades envolvendo mais restritamente com os delegados e reunir o conhecimento necessários para compreensão relativamente a quais formas são mais problemáticas para a audiência. | |
| 86-95 | Estes slides fornecem uma breve e básica introdução às tendências atuais na preparação dos atos criminosos. As plataformas móveis, malware bancário, ransomware e comprometimento de e-mails comerciais, hacktivismo e abuso das redes sociais, violação de DPI, ameaças persistentes avançadas e as suas formas, transações móveis e criptomoedas, a Internet das Coisas e os seus aspetos, todas essas formas e tendências de cibercrime estão muito presentes atualmente e a infligir danos muito grandes no mundo.  O formador deve interagir com os delegados durante essa parte da apresentação e descobrir quais são as formas contemporâneas que estão presentes a nível local. | |
| 96-98 | Resumo. O que é cibercrime e qual é o motivo de preocupação?  Ameaças, tendências e ferramentas de cibercrime e respostas ao fenómeno.  Realidades abrangidas pela expressão *cibercrime* e conceitos que são considerados tipos de crime na maioria das legislações e nos padrões internacionais.  Necessidades e vantagens da harmonização entre a legislação nacional e os instrumentos internacionais, em particular a Convenção de Budapeste. | |
| **Exercícios práticos**  Não são previstos exercícios práticos para esta aula. | | |
| **Avaliação de conhecimentos**  Não foi apresentada uma avaliação formal para esta sessão. O formador é encorajado a verificar o conhecimento e compreensão ao fazer perguntas importantes ao longo da sessão. | | |