Premessa

Quando parliamo di cybercrime, o crimine informatico, a cosa ci riferiamo esattamente?

Cosi come accade per il crimine tradizionale, quello informatico può assumere varie forme e può essere perpetrato sempre e ovunque.

Nel trattato del Consiglio d'Europa sulla criminalità informatica si utilizza il termine "cybercrime" per definire reati che vanno dai crimini contro i dati riservati, alla violazione di contenuti e del diritto d'autore. Tuttavia, altri suggeriscono una definizione più ampia che comprende attività criminose come la frode, l'accesso non autorizzato, la pedopornografia e il "cyberstalking" o pedinamento informatico.

Il manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico (The United Nations Manual on the Prevention and Control of Computer Related Crime) nella definizione di crimine informatico include frode, contraffazione e accesso non autorizzato.

Come si evince da queste definizioni, il crimine informatico si riferisce a una gamma molto ampia di attacchi. Per questo, è ormai di fondamentale importanza comprendere le differenze tra i vari tipi di cybercrime, perché ciascuno necessita di un approccio diverso al fine di migliorare la sicurezza del computer.

Destinatari

Il corso online EIPASS Informatica giuridica è rivolto a tutti coloro i quali vogliano approfondire i diritti, i danni, le normative e i reati connessi all'utilizzo delle nuove tecnologie, in particolare in materia di privacy e trattamento dei dati, di commercio elettronico e di cybercrimes.

Disclaimer

Certipass ha predisposto questo documento per l'approfondimento delle materie relative alla Cultura Digitale e al migliore utilizzo del personal computer, in base agli standard e ai riferimenti Comunitari vigenti in materia; data la complessità e la vastità dell'argomento, peraltro, come editore, Certipass non fornisce garanzie riguardo la completezza delle informazioni contenute; non potrà, inoltre, essere considerata responsabile per eventuali errori, omissioni, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione ed eventualmente utilizzate anche da terzi.

Certipass si riserva di effettuare ogni modifica o correzione che a propria discrezione riterrà sia necessaria, in qualsiasi momento e senza dovere nessuna notifica.

L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del sito dedicate al Programma.

Cybercrimes: Criminologia e reati informatici

Internet offre a tutti nuove possibilità, abbattendo le distanze, permettendo l'informazione gratuita e favorendo la condivisione. L'altra faccia della medaglia è però rappresentata dai rischi legati a un uso improprio di questo strumento.

Tra i reati informatici che più spesso si nominano vi sono virus e malware, furto di identità, cyberstalking e pedofilia, reati le cui dinamiche sono difficilmente riconoscibili. Difatti, tanti utenti del web non sanno riconoscere episodi criminali né possono da questi difendersi.

Attraverso il corso Cybercrimes: criminologia e reati informatici si forniscono competenze basilari in materia di diritto penale, si presentano i reati in internet, approfondendo gli aspetti più significativi dal punto di vista criminologico. Obiettivo centrale è di ridimensionare il profilo del Cybercriminale, il suo modus operandi, la firma, la vittimologia e i fattori di rischio. I reati informatici previsti dall'ordinamento italiano sono diversi e per questo è fondamentale per adulti e ragazzi conoscerli, affinché l'ambiente del web non diventi un posto ad alto rischio di criminalità.

	Ambiti di intervento		Testing di competenza
1.	Introduzione alla criminologia	1.1	Evoluzione storica
		1.2	Criminologie, criminalistica e investigazione criminale
		1.3	Studio del fenomeno criminale
		1.4	Autori del crimine e criminal profiling
		1.5	Vittimologie
		1.6	Crime mapping
2.	Cybercrimes e aspetti criminologici	2.1	Autori e cybercrime: criminal profiling
		2.2	Le vittime
		2.3	Computer forensics
3.	Alcune fattispecie delittuose	3.1	Cyberstalking
		3.2	Cyberbullismo
		3.3	Cyberpedofilia
		3.4	Cyberterrorismo
4.	Lineamenti di diritto penale	4.1	I principi del diritto penale
		4.2	Il reato
		4.3	Il tentativo
		4.4	Le circostanze del reato
		4.5	Il concorso di reati
		4.6	Il concorso di persone nel reato
		4.7	La punibilità, la pena e le misure di sicurezza
5.	I reati informatici	5.1	Legislazione Nazionale e Influenza del Diritto Comunitario
		5.2	La Legge n. 547 del 1993
		5.3	La legislazione europea
		5.4	I reati informatici
6.	I reati a mezzo internet	6.1	Ingiuria e diffamazione (artt. 594, 595 c.p.)
		6.2	Sostituzione di persona (art. 494 c.p.)
		6.3	Molestia o disturbo alle persone (art. 660 c.p.)
		6.4	Atti persecutori (art. 612-bi c.p.) e cyberstalking
		6.5	Cyberbullismo
		6.6	Pedopornografia (artt. 600-ter, 600-quater, 600- quater.1 c.p.)
		6.7	Estorsione
		6.8	Art. 167 cod. privacy
		6.9	Cyberterrorismo