CORSO COMPUTER CRIMES

CATEGORIA: Privacy

PROGRAMMA

Cyber crime – Cyber Security: scenari attuali e futuri dei fenomeni

- Come è cambiato il mondo del Cyber crime negli ultimi anni
- ENISA: panoramica delle principali minacce informatiche europee delineate dal Threat landscape Report del 2020
- Il rapporto CLUSIT 2020
- Il Deep web, il Dark web

L'impatto economico del Cyber Crime per le Aziende: in cosa consiste e quanto costa effettivamente?

Definizione di Cyber Crime e analisi giuridica delle norme penali in materia:

- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)
- Possesso e diffusione abusiva di codici di accesso (art. 615 quater c.p.)
- Diffusione di programmi finalizzati a danneggiare un sistema informatico (art. 615 quinquies c.p.)
- Frode informatica (art. 640 ter c.p.)
- Il fenomeno del DeepFake

- Risposte efficaci agli attacchi: quali strategie devono adottare le Aziende per evitare di incorrere nella responsabilità ex D. Lgs. 231/01?

Case study: i Cyber crime ai tempi del Covid-19 (la vulnerabilità delle Aziende italiane)

Le interrelazioni tra Cyber security e trattamento dei dati personali

- Tutela dei dati personali online e diritti su internet
- I Big data tra concorrenza e privacy

L'impatto del Computer Crimes sulla proprietà intellettuale e industriale

- Illeciti e violazioni in tema di diritto d'autore: violazioni di copyright o di marchi registrati
- tutela dei software
- cybersquatting

Case study