



UNIVERSITÀ DEGLI STUDI DI PALERMO

DIPARTIMENTO	Scienze Politiche e delle Relazioni Internazionali		
ANNO ACCADEMICO OFFERTA	2020/2021		
ANNO ACCADEMICO EROGAZIONE	2021/2022		
CORSO DILAUREA MAGISTRALE	SCIENZE DELLE AMMINISTRAZIONI E DELLE ORGANIZZAZIONI COMPLESSE		
INSEGNAMENTO	PRIVACY AND CYBER CRIMES		
TIPO DI ATTIVITA'	B		
AMBITO	50524-statistico-quantitativo		
CODICE INSEGNAMENTO	21301		
SETTORI SCIENTIFICO-DISCIPLINARI	ING-INF/05		
DOCENTE RESPONSABILE	AGATE VINCENZO	Ricercatore a tempo determinato	Univ. di PALERMO
ALTRI DOCENTI			
CFU	8		
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	144		
NUMERO DI ORE RISERVATE ALLA DIDATTICA ASSISTITA	56		
PROPEDEUTICITA'			
MUTUAZIONI			
ANNO DI CORSO	2		
PERIODO DELLE LEZIONI	1° semestre		
MODALITA' DI FREQUENZA	Facoltativa		
TIPO DI VALUTAZIONE	Voto in trentesimi		
ORARIO DI RICEVIMENTO DEGLI STUDENTI	AGATE VINCENZO Martedì 15:00 17:00 Ricevimento in modalita telematica		

DOCENTE: Prof. VINCENZO AGATE

PREREQUISITI	Nessuno
RISULTATI DI APPRENDIMENTO ATTESI	Conoscenza e capacita' di comprensione (knowledge and understanding): Lo studente, al termine del corso, avra' acquisito conoscenze e metodologie per affrontare problematiche legate alla protezione della privacy e ai cyber crimes che possono essere sferrati tramite le moderne tecnologie di elaborazione delle informazioni. Conoscenza e capacita' di comprensione applicate (applying knowledge and understanding): Lo studente avra' acquisito conoscenze e metodologie per analizzare le caratteristiche dei diversi cyber crimini. Autonomia di giudizio (making judgements): Lo studente avra' acquisito una metodologia di analisi dei diversi crimini informatici, in termini di gravita' del crimine, di norme disattese e degli impatti socio-economici. Abilita' comunicative (communication skills): Lo studente sara' in grado di discutere con competenza e proprieta' di linguaggio problematiche legate alla protezione della privacy e all'analisi dei crimini informatici. Capacita' di apprendere (learning skills): Lo studente sara' in grado di affrontare con autonomia l'analisi di qualsiasi scenario di crimine informatico.
VALUTAZIONE DELL'APPRENDIMENTO	Le conoscenze e le competenze acquisite dallo studente saranno verificate attraverso un colloquio orale, volto ad accertare il possesso delle competenze e delle conoscenze disciplinari previste dal corso; la valutazione viene espressa in trentesimi. Durante il colloquio saranno proposte domande di diverso e crescente livello di complessita' al fine di valutare il raggiungimento degli obiettivi formativi e le abilita' comunicative dello studente. Infine, allo scopo di valutare l'autonomia di giudizio, sara' richiesto di analizzare le caratteristiche di specifici scenari applicativi e di proporre le soluzioni piu' adeguate ai problemi individuati. La valutazione finale terra' conto sia del punteggio della prova scritta (50%) che di quello delle prove orali (50%). Eccellente 30-30 e lode. Durante entrambe le prove lo studente dovra' dimostrare padronanza completa degli argomenti del corso. Durante il colloquio orale l'allievo dovra' dimostrare la maturita' di saper collegare i diversi aspetti trattati e la capacita' di saper generalizzare. Dovra' mostrare autonomia nella soluzione dei quesiti e la capacita' di individuare le informazioni necessarie per la soluzione degli stessi. Molto buono 27-29 Buona padronanza degli argomenti, lo studente e' in grado di applicare le conoscenze per risolvere i problemi proposti. Buono 24-26 buona conoscenza dei principali, discreta padronanza e proprieta' di linguaggio, con capacita' di applicare autonomamente le conoscenze alla soluzione dei problemi proposti. Discreto 21-23 Piu' che sufficiente padronanza degli argomenti principali dell'insegnamento, limitata capacita' di applicare autonomamente le conoscenze acquisite. Sufficiente 18-20 conoscenza di base degli argomenti principali dell'insegnamento e del linguaggio tecnico. Insufficiente non possiede una conoscenza accettabile dei contenuti degli argomenti trattati nell'insegnamento.
OBIETTIVI FORMATIVI	La transizione epocale della societa' moderna verso le Tecnologie delle Informazioni e delle Telecomunicazioni, che con i loro nuovi ed indispensabili servizi costituiscono il cosiddetto Cyber-Space, ha determinato una rigida dipendenza dalle infrastrutture digitali. Una tale condizione espone la nostra societa' a nuovi rischi; di conseguenza enormi ed imprevedibili minacce devono essere fronteggiate ogni giorno. Crimini informatici contro la proprieta' e le persone, attacchi informatici ad apparati dello stato, cyber terrorismo, spionaggio on-line, rappresentano oggi le minacce che per la natura del mezzo su cui vengono perpetrate sono transnazionali e non riconducibili a classiche entita' nemiche. I criminali informatici attaccano aziende private (grandi multinazionali e piccole medie imprese) e pubbliche amministrazioni prendendo di mira i loro servizi vitali, quali reti di vendita e di approvvigionamento o infrastrutture pubbliche critiche (trasporti, rifornimento idrico, ospedali). Le contromisure adottate dalla societa' civile e dai governi si scontrano con la completa anarchia e liberta' della Internet originaria, con controlli sempre piu' intrusivi che possono violare la privacy degli utenti. Obiettivo del corso e' fornire agli studenti una ampia disamina delle minacce informatiche, offrendo al contempo una breve introduzione all'attuale governo di Internet, una panoramica sugli strumenti per fronteggiare la criminalita' informatica, e una analisi sulle problematiche relative alla privacy.

ORGANIZZAZIONE DELLA DIDATTICA	Lezioni frontali.
TESTI CONSIGLIATI	Jonathan Clough, Principles of Cybercrime, Cambridge University Press

PROGRAMMA

ORE	Lezioni
6	Introduzione ai sistemi informatici e alle tecniche per la loro protezione.
4	Crimini Cibernetici: concetti ed evoluzione
26	Tipologie di crimini informatici Furto della proprieta' intellettuale, Furto di altre informazioni proprietarie (dati finanziari personali, ecc.), Attacchi di DOS, Virus, worms e altri codici malevoli, spyware, Frodi, Furto di identita, Generazione illegale di messaggi di posta elettronica, Phishing, Accesso ed uso non autorizzato dei sistemi e delle reti, Sabotaggio, Estorsioni, alterazione di siti web, macchine zombie, crimini legati al sesso: pedopornografia, diffusione non autorizzata di materiale privato
2	Cyber-Terrorismo e Guerra cibernetica
2	Lotta al cybercrime
2	Liberta' individuali ed interessi di sicurezza nazionale
2	Difesa personale attiva in ambito digitale
2	Legislazione sui crimini informatici
2	Proprieta' Intellettuale
2	Privacy
4	Regolamento UE 2016/679 GDPR (General Data Protection Regulation)
2	Aspetti Etici