



ORDINE DEGLI AVVOCATI  
DEL  
CANTONE TICINO

## MARATONA DEL DIRITTO

Centro Studi Bancari, Vezia

Data: 18 novembre 2017

Cyber criminalità

# Cyber criminalità, evoluzione e modus operandi, come pensa un hacker

Relatore: Dr.Ing. Alessandro Trivilini

La cyber criminalità è senza dubbio un contesto tra i più resilienti e complessi da gestire, ma pone al centro del dibattito molti interrogativi sulla difficoltà di avvalersi di competenze tecniche sempre più complesse e interdisciplinari adeguate per fronteggiare un mercato che vede il crimine informatico come un vero e proprio business.

Gli approcci di repressioni finalizzati all'uso di sola tecnologia di analisi non è più sufficiente per intraprendere un'adeguata e proporzionata strategia investigativa. E lo strumento della rogatoria internazionale per la richiesta di informazioni e dati che risiedono in altri Paesi non sempre porta ai frutti sperati, nei tempi sperati e nelle modalità sperate, complicando ulteriormente in sede penale la comprensione del cyber crimine avvenuto e la sua oggettiva e completa descrizione in fase difensiva.

Ecco perché conoscere da vicino il pensiero che contraddistingue un hacker, è senza dubbio di grande utilità, non solo per definire in azienda opportune strategie di sicurezza ma anche per limitare i danni che sempre più spesso fanno leva sull'anello debole della catena: il fattore umano.

Scoprire come un hacker concepisce una truffa informatica è il miglior modo per intraprendere un'adeguata preparazione alla strategia cyber. Questo vale per gli addetti alla gestione della sicurezza in azienda, agli amministratori delegati chiamati a investire grosse somme di denaro per salvaguardare il proprio business, ma anche per le autorità giudiziarie chiamate a comprendere un'infrastruttura informatica complessa, distribuita e in forte mutamento.

Pensare come un hacker diventa quindi una necessità e un modus operandi preventivo necessario per ridurre rischi, costi e tempi di intervento, soprattutto citando Kaspersky, che nei mesi scorsi in merito all'evoluzione del crimine informatici e alla possibilità di essere colpiti ha detto: **«prima o poi è diventato ora»**.

### Short Bio



ORDINE DEGLI AVVOCATI  
DEL  
CANTONE TICINO

Dr. Alessandro Trivilini, dal 2011 è responsabile del Laboratorio di informatica forense del Dipartimento tecnologie innovative della SUPSI ([www.supsi.ch/forense](http://www.supsi.ch/forense)), nato in collaborazione con il Dipartimento delle Istituzioni, la Polizia e la Magistratura del Cantone Ticino. In SUPSI è anche docente di ingegneria del software, informatica forense e information security. Autore di libri e pubblicazioni scientifiche sul tema della sicurezza informatica, ha lavorato nella Silicon Valley in California in qualità di ingegnere informatico presso Invision Technologies Inc., azienda leader nella produzione di scanner a raggi-X usati negli aeroporti per il ritrovamento di bombe ed esplosivi. Ha un Bachelor of Science in ingegneria informatica, un Master in tecnologie della comunicazione, e un dottorato di ricerca conferito con lode dal Politecnico di Milano nel campo dell'intelligenza artificiale, con applicazione nel contesto forense. Partecipa come Chairman e public speaker a conferenze e congressi nazionali e internazionali su aspetti di cyber security, digital forensics e cyber intelligence. È membro del comitato scientifico internazionale dell'IMA World Maintenance Forum per temi di cyber security. A gennaio del 2017 è stato nominato dalla Segreteria di Stato Svizzera per la formazione, la ricerca e l'innovazione (SEFRI) quale rappresentante della Svizzera in seno al comitato di gestione dell'azione COST "Multi-modal imaging of forensic science evidence - tools for forensic science", del programma intergovernativo di cooperazione europea nella ricerca scientifica e tecnologica.

**Maggiori informazioni:**

[www.trivilini.info](http://www.trivilini.info)