

L'UNICO SEMINARIO A 360°
IDEATO SU MISURA PER
IT MANAGER E FRAUD MANAGER!



Prevenire, gestire e limitare i danni di

*SPECIALI SESSIONI
INTERATTIVE!*

FRODI e ATTACCHI INFORMATICI

STRATEGIE DI DIFESA

LE VITTIME E I DANNI

GESTIONE DEI RISCHI

ASPETTI LEGALI E
INVESTIGAZIONE

UN SEMINARIO COMPLETO E APPROFONDITO SU:

- Quali sono le principali frodi esterne e chi sono i possibili aggressori
- Come proteggersi dal rischio frode
- Come organizzare la Corporate Security Aziendale Antifrode
- Quali sono le metodologie e le tecniche più recenti per prevenire, rilevare e gestire le minacce di intrusione al sistema informativo aziendale
- Come proteggersi dal furto d'identità e dal falso documentale
- Come garantire la sicurezza nei pagamenti elettronici con gli strumenti più innovativi
- Come tutelarsi legalmente e limitare il danno d'immagine e le conseguenze per l'organizzazione in caso di frode

CON LA PARTECIPAZIONE DI:

- Osservatorio Internazionale Cards
- UCAMP - Ufficio Centrale Antifrode dei Mezzi di Pagamento
- Osservatorio Nazionale Permanente sulla Sicurezza
- Centro Studi Anticontraffazione

28 - 29 Gennaio 2009

1° Edizione

28 - 29 Aprile 2009

2° Edizione

Milano - Capitol World Class Hotel

Ai partecipanti è rilasciato un
Attestato di Partecipazione.

 **IDC**
Analyze the Future

PLUS

- + Il seminario è arricchito da numerosi esempi e casi pratici
- + E' prevista una sessione speciale di domande e risposte
- + I partecipanti sono coinvolti in prima persona per condividere esperienze e trovare le soluzioni ai problemi

Il seminario si apre con la condivisione degli obiettivi tra i partecipanti, per profilare il seminario sulle esigenze comuni del gruppo di lavoro.

PERCHÈ PARTECIPARE

In Italia un'azienda su 5 ha subito una frode informatica, con un danno che incide del 3% sul fatturato.

E' quello che è emerso da un sondaggio effettuato nel 2008 da InfoFinax che rileva anche la necessità di diffondere a tutti i livelli "una cultura della prevenzione" del rischio frodi.

D'altra parte la legge impone sempre più alle organizzazioni di adeguarsi alle nuove norme di protezione dei dati e di tutela delle transazioni, inasprendo parallelamente le pene per i trasgressori.

Impostare un valido ed efficace sistema di prevenzione e controllo delle frodi e delle intrusioni, possedere una chiara visione delle normative italiane e internazionali in materia di sicurezza e instaurare un efficace rapporto con l'autorità giudiziaria sono le nuove sfide con cui le aziende si devono confrontare oggi per dare fiducia e garanzie alla clientela.

Questo seminario IDC consente al partecipante di acquisire conoscenze concrete per individuare, prevenire e controllare le insidie più comuni e quelle di ultima generazione, di conoscere le nuove tecniche utilizzate dagli hackers più abili e di avvalersi degli strumenti e dei metodi più innovativi per limitare il danno alla propria organizzazione e gestire l'investigazione in modo efficiente e proattivo.

Il corso è arricchito da esercitazioni pratiche in cui sono coinvolti i partecipanti.

CHI NON PUÒ MANCARE

Questo corso è studiato per Banche e Istituti Finanziari, GDO & Retail e Pubblica Amministrazione, in particolare è rivolto a:

- Risk Manager/Fraud Manager
- IT Security Manager/CSO
- Direttori di Amministrazione e Finanza
- Titolari di Agenzie Investigative Private

RELATORI

Il Seminario è a cura di:

Stefano Izzi, *Docente di Corporate Security*

Con la partecipazione di:

Giovanni Pollastrini, *Direzione frodi carte di Pagamento, UCAMP*

Maurizio Pimpinella, *Presidente dell'Osservatorio Internazionale Cards*

Emilio Lucchetta, *Esperto di Investigazione Forense*

Massimo Cotrozzi, *Partner, Sertytude Italia*

Daniela Mainini, *Presidente, Centro Studi Anticontraffazione*

Guido Verdi, *Osservatorio Nazionale Permanente sulla Sicurezza*

Giuseppe Provera, *General Manager, Convey*

PROGRAMMA DEL SEMINARIO

28 GENNAIO

MATTINA

Cosa s'intende per frodi e quali tipologie di frodi esistono

- ☐ Che cosa sono le frodi esterne
 - ▶ Chi sono gli aggressori e chi sono le vittime
 - ▶ Quali strumenti e tecniche di aggressione si utilizzano più frequentemente in Azienda
 - ▶ Quali e quanti sono i possibili danni di una frode
- ☐ Le frodi a danno di carte di pagamento e nel credito al consumo
 - ▶ Quali sono i sistemi di pagamento più in uso
 - ▶ Conoscere le frodi nelle transazioni con: *Carta di credito, Bancomat, Carte revolving e Carte prepagate, Pagamenti a distanza*
 - ▶ Individuare i principali metodi fraudolenti:
 - Che cos'è il *Phishing* e come funziona
 - L'utilizzo dello *Skimming* e del *Pharming* nel furto dei dati
 - Le insidie via telefono o VoIP: il *Vishing*
 - ▶ *L'Automated Teller Machine*: cos'è e come funziona
 - ▶ I terminali *POS (Point of Sale)* e le possibili frodi a loro danno
 - ▶ Quali contromisure è necessario adottare a livello strategico e operativo per combattere le frodi
 - ▶ Come coinvolgere i punti vendita nel processo di prevenzione

a cura di Stefano Izzi, *Docente di Corporate Security*

L'esperienza dell'Osservatorio Internazionale Cards nella lotta alle frodi - Relazioni ed assistenza ai consumatori e finalità dell'Osservatorio

- ☐ Le frodi in ambito e-commerce
 - ▶ Come funziona e quali sono le peculiarità della frode in ambiente *card not present*
 - ▶ L'intercettazione delle coordinate di pagamento durante le transazioni online: lo *Sniffing*
 - ▶ Come identificare gli ordini fraudolenti o modificati effettuati via internet
 - ▶ Quali sono le verifiche anti-frode da eseguire prima e durante le transazioni di pagamento
 - ▶ Chi sono gli hackers del futuro, quali nuovi strumenti utilizzano e come è possibile prevenirli

a cura di Maurizio Pimpinella, *Presidente dell'Osservatorio Internazionale Cards*

Sessione interattiva di domande e risposte

POMERIGGIO

L'esperienza diretta dell'UCAMP Ufficio Centrale Antifrode dei Mezzi di Pagamento

- ☐ Il Progetto SIPAF (Sistema Integrato di Prevenzione Amministrativa Antifrode) dell'UCAMP del Ministero del Tesoro
- ☐ Finalità e supporto della collaborazione Pubblico/Privato

a cura di Giovanni Pollastrini, *Direzione frodi carte di Pagamento, UCAMP*

Il furto e la frode di identità

- ☐ Definire il furto d'identità
- ☐ Quali sono le diverse tipologie dell'Identity Theft:
 - Financial Identity Theft, Criminal Identity Theft, Identity Cloning*
- ☐ Cosa si intende per frode d'identità
- ☐ Le tecniche di acquisizione dei dati: il *Trashing* e lo *Spoofing*
- ☐ Che cos'è il falso documentale
- ☐ Cenni sul controllo documentale
- ☐ Individuare le vulnerabilità dei principali documenti digitali
- ☐ Qual è il ruolo delle Autorità di Certificazione

Conoscere i metodi tecnologici di difesa antifrode:

- ☐ L'*Intrusion detection system*
- ☐ I servizi di *Firewall Management*
- ☐ Il *Content Filtering Management: antispymware e antiphishing*
- ☐ Conoscere i metodi di Autenticazione più diffusi:
 - Login e PIN*, firma digitale, identificazione tramite tecnologie biometriche

PER ISCRIZIONI E INFO:

☎ 0228457354 - ☎ 0228457313

✉ infoevents@idc.com - 🌐 www.idc.com/italy

Responsabile del Progetto: Nicoletta Puglisi



- Sistemi di criptazione antifrode
Che cos'è la crittografia e come funziona;
Quali tipologie di crittografia esistono e come scegliere le più sicure
- Il programma *Pretty Good Privacy (PGP)*
- La scelta della gestione della sicurezza tra *out-sourcing* e *in-sourcing*: vantaggi e svantaggi
- Gestire la sicurezza in ambito *Wireless*: quali sono i rischi di aggressione e come proteggere i dati e criptare il trasferimento nel mondo wireless
- I protocolli sicuri per la mobilità
- Come proteggere le chiamate vocali contro le intercettazioni in ambito VoIP

a cura di *Guido Verdi, Esperto di sicurezza Informatica dell'Osservatorio Nazionale Permanente sulla Sicurezza*

29 GENNAIO

MATTINA

Come prevenire le intrusioni a fini illeciti e il furto dei dati

- Il paradigma di *Confidenzialità, Integrità e Disponibilità*
- Come identificare i possibili aggressori e le minacce della rete
- Come far transitare dati privati in reti pubbliche in sicurezza: *Secure Virtual Private Network (VPN)*
- Cosa sono e quali sono i protocolli di sicurezza più usati
- *L'Intrusion Prevention System*
- Quali sono gli step da fare in caso di attacco: *Incident Management*

Come proteggersi dal rischio frodi

- Profilare le analogie e le differenze del rischio frode a danno dei diversi settori: bancario e finanziario, della GDO & Retail, della PA
- In che modo misurare e valutare il rischio di frode: il processo e le metodologie di analisi del rischio
- Il ruolo della formazione di dipendenti e collaboratori
- Come compilare un report di valutazione del rischio di frode

Come impostare una efficace attività antifrode in Azienda

a cura di *Massimo Cotrozzi, Sertytude Italia*

Come favorire il lavoro delle forze dell'ordine e degli uffici legali nella fase investigativa

- Identificare la dinamica dell'attacco e l'analisi delle cause, raccolta delle prove, perizie

a cura di *Emilio Lucchetta, Esperto di Investigazione Forense*

Sessione interattiva di domande e risposte

POMERIGGIO

Come tutelarsi legalmente e limitare il danno avvenuto

- Qual è il quadro Legislativo Italiano e la normativa internazionale in fatto di frodi informatiche
- Qual è il ruolo delle certificazioni ISO
- Qual è il valore legale delle transazioni e dei documenti digitali
- Quali sono i ruoli e le responsabilità della *Funzione Sicurezza* quando avviene una frode
- Come si distribuisce il rischio frode tra azienda e utente
- Come limitare il danno d'immagine e le conseguenze per l'organizzazione

a cura di *Daniela Mainini, Presidente, Centro Studi Anticontraffazione*

Conoscere e confrontare gli strumenti di analisi per svolgere attività antifrodi in azienda

- Analizzare le caratteristiche e le peculiarità dei diversi strumenti di analisi antifrode
- Come integrare questi strumenti nei sistemi già esistenti
- Quali sono i costi e il ROI
- Quali sono i vantaggi e gli svantaggi di tali strumenti

a cura di *Giuseppe Provera, General Manager, Convey*

Analisi ed Intelligence Antifrode

a cura di *Stefano Izzi, Docente di Corporate Security*

Ciascuna giornata di seminario si conclude con la
SESSIONE INTERATTIVA
"I partecipanti diventano i protagonisti": spazio aperto per domande e risposte, condivisione di idee ed esperienze

5 MOTIVI in più PER NON PERDERE QUESTO APPUNTAMENTO

Confrontarsi con le esperienze di altri Manager che come lei devono trovare le soluzioni più all'avanguardia per combattere le frodi

Avere gli strumenti per conoscere meglio le minacce e trovare le soluzioni per prevenire le mosse degli hacker più intraprendenti

Avere a disposizione per due intere giornate consulenti esperti per dissipare i dubbi

Avere una visione completa e approfondita degli argomenti trattati

Diventare protagonisti del dibattito nelle speciali sessioni di domande e risposte



Specialisti IDC intervengono ad ogni incontro per dare un breve e significativo sguardo al futuro nel mercato di riferimento

A questo Seminario partecipa:

Ezio Viola, Group Vice President and General Manager, EMEA Vertical Markets & Insights, IDC

IDC è leader mondiale nell'ambito della ricerca di mercato, dei servizi di consulenza e degli eventi nei settori dell'information technology e delle telecomunicazioni. IDC aiuta i professionisti IT, i dirigenti aziendali e la community degli investitori a prendere decisioni sugli acquisti e sulla strategia di business nell'area tecnologica sulla base di elementi concreti e di fatto. Oltre 775 analisti IDC in 50 paesi forniscono regionale e locale la propria esperienza sulle tendenze e del mercato. Per oltre 40 anni, IDC ha fornito analisi strategiche per aiutare i propri clienti a raggiungere i loro principali obiettivi di business. IDC è una società del gruppo IDG, realtà leader mondiale nel settore dell'editoria, della ricerca e degli eventi in ambito tecnologico. Si possono avere maggiori informazioni su IDC visitando il sito <http://www.idc.com>.



MODULO DI ISCRIZIONE

L'iscrizione si intende perfezionata al momento del ricevimento, da parte di IDC Italia, della presente scheda - da inviarsi via fax allo 02 28457 313 - debitamente compilata in tutte le sue parti e sottoscritta per accettazione. Allegare copia del bonifico bancario e/o ricevuta di pagamento effettuato con carta di credito.

SEMINARIO: Prevenire, gestire e limitare i danni di FRODI e ATTACCHI INFORMATICI

- 28 - 29 Gennaio 2009
 28 - 29 Aprile 2009

Quota d'iscrizione per partecipante + IVA:

- € 1.350,00 + IVA
 SCONTO di € 200,00 per iscrizioni entro un mese dalla data dell'evento

SCONTO 10% per ISCRIZIONI MULTIPLE

Applicabile per 3 o più iscritti della stessa Azienda

Gli sconti non sono cumulabili

La quota d'iscrizione comprende la documentazione didattica, la colazione e i coffee break. Per circostanze imprevedibili, IDC Italia si riserva la facoltà di modificare senza preavviso il programma e le modalità didattiche, e/o cambiare i relatori e i docenti.

TUTELA dei DATI PERSONALI - INFORMATIVA

Informativa ai sensi dell'art. 13 d.lgs 196/2003: i dati personali raccolti con questo modulo sono trattati per la registrazione all'iniziativa, per elaborazioni di tipo statistico, e per l'invio, se lo desidera, di informazioni commerciali su prodotti e servizi di IDC Italia e degli Sponsor, con modalità anche automatizzate, strettamente necessarie a tali scopi. Il conferimento dei dati è facoltativo ma serve per l'esecuzione del servizio. In relazione ai dati il Partecipante ha il diritto di opporsi al trattamento sopra previsto. Titolare e responsabile del trattamento è IDC Italia, V.le Monza 14 - 20127 Milano nei cui confronti il partecipante potrà esercitare i diritti di cui al D. Lgs. 196/03 (accesso, correzione, cancellazione, opposizione al trattamento, indicazione delle finalità del trattamento). La comunicazione potrà pervenire a: infoevents@idc.com - tel. +39 02 28457 333 - fax +39 02 28457.313



CODICE: **WEB**

MODALITÀ DI ISCRIZIONE

TELEFONO: +39 02 28457 354
FAX: +39 02 28457.313
E-MAIL: infoevents@idc.com
POSTA: IDC Italy - V.le Monza 14 - 20127 Milano
WEBSITE: www.idc.com/italy

SEDE del SEMINARIO

Milano - Capitol World Class Hotel
Via Cimarosa 6, Milano - Tel. 02 43859.1

L'Hotel riserva ai partecipanti particolari tariffe per il pernottamento.
IDC Italia si riserva il diritto di modificare la sede dell'evento.
IDC Italia si riserva altresì il diritto di cancellare il seminario programmato, dandone comunicazione scritta ai partecipanti, 5 giorni lavorativi prima dell'inizio del seminario. In tal caso, suo unico obbligo è provvedere al rimborso dell'importo ricevuto senza ulteriori oneri.

DATI del PARTECIPANTE

NOME _____ COGNOME _____ FUNZIONE _____

TELEFONO _____ FAX _____ E-MAIL _____

DESIDERA RICEVERE INFORMAZIONI SU ALTRE INIZIATIVE IDC Sì: Via email Via Fax NO

DATI dell'AZIENDA

RAGIONE SOCIALE _____ INDIRIZZO _____

CITTÀ _____ PROV. _____ CODICE POSTALE _____

INTESTATARIO FATTURA _____

PARTITA IVA o CODICE FISCALE _____ N° RIFERIMENTO PER FATTURAZIONE _____

TIMBRO _____ FIRMA _____

MODALITÀ di PAGAMENTO

La quota d'iscrizione deve essere versata all'atto dell'iscrizione effettuando il pagamento tramite:

- Bonifico bancario intestato: IDC Italia s.r.l. c/c nr. 000000000130 c/o CREDITO ARTIGIANO AGENZIA N.21, VIALE MONZA, 14 - 20127 MILANO
CIN: B - ABI: 03512 - CAB: 01626 - IBAN: IT26B035120162600000000130 - CHECK DIGIT: 26 - CODICE PAESE: IT - BIC SWIFT: ARTI IT M2
- Carta di Credito

Intestata a _____ Numero Carta _____ Scadenza (mese/anno) _____

Visa MasterCard CartaSi American Express Diners

Firma _____

IDC Italia si riserva la valutazione di ammettere al seminario solo gli iscritti in regola con il pagamento della quota di partecipazione

RECESSO/MODALITÀ di DISDETTA

E' possibile rinunciare all'iscrizione entro e non oltre il 12° giorno lavorativo precedente la data d'inizio del seminario dandone comunicazione scritta. In questo caso sarà restituita l'intera quota versata. Qualora la comunicazione della volontà di recesso avvenga dopo tale termine oppure avvenga di fatto per la mancata presenza al seminario, sarà comunque dovuto l'intero importo.

Saremo comunque lieti di accettare un suo collega in sostituzione alla sua partecipazione, purché il nominativo venga comunicato in forma scritta almeno un giorno prima dalla data del seminario.