MARCO STRANO

INTERNATIONAL CRIME ANALYSIS ASSOCIATION

www.criminologia.org

Duke UNIVERSITY

Laboratory for Intelligent Systems (LISC)

CRIMINAL PROFILING LAB

North Carolina - USA

Il Prof. Marco Strano: curriculum

- **Marco Strano**, Psicologo e Criminologo è il Presidente dell'ICAA (International Crime Analysis Association) ed è considerato uno dei maggiori esperti del mondo di Psicologia investigativa e criminal profiling. E' Professore a contratto dell'Insegnamento di Psicologia Investigativa e Criminal Profiling dell'Università degli Studi di Palermo. Svolge inoltre attività di ricerca e insegnamento universitario presso la Duke University (North Carolina - USA) e in Italia presso l'Istituto di Psichiatria e Psicologia dell'Università Cattolica del Sacro Cuore di Roma, presso l'Università degli Studi di Urbino., presso l'Università LUMSA di Roma. Insegna presso corsi di perfezionamento e master di numerose Università italiane. Collabora con la rete televisiva canale 5, con l'emittente televisiva Teleroma56, con il Quotidiano "Il Messaggero", con il mensile ICT security e con altri organi di stampa. Collabora come Presidente dell'ICAA con l'Unità di Scienze comportamentali (*Behavioral Science Unit*) dell'Accademia FBI di Quantico con cui sta sviluppando insieme alla Duke University un progetto di ricerca sul criminal profiling (NNPCP research project)

ON-LINE FRAUD RISK PERCEPTION RESEARCH PROJECT

PROGETTO PHISHING

CYBERCRIME RESEARCH and ANALYSIS LABORATORY

AISIC - ANSSAIF - ICAA

BANCHE COINVOLTE NEL PROGETTO

- BANCA NAZIONALE DEL LAVORO
- MONTE DEI PASCHI DI SIENA
- BANCA SELLA
- SAN PAOLO – IMI
- ARTIGIANCASSA
- BANCA INTESA
- CAPITALIA
- UNICREDIT

PSICO-CRIMINOLOGIA DELLE MINACCE EMAIL

DIFESE

STIMOLAZIONE

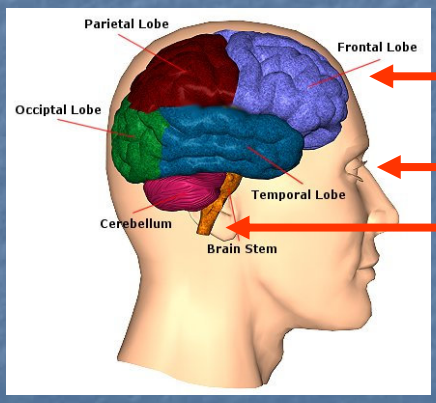
INFORMAZIONI - BENI

CRIMINAL

VICTIM OF CRIME

BIDIRECTIONAL EMAIL THREATS

PSICOFISIOLOGIA DELLA TRUFFA: IL RICONOSCIMENTO DEL PERICOLO



VALUTAZIONI LOGICHE

PERCEZIONE VISIVA, UDITIVA, TATTILE E OLFATTIVA

INTUIZIONE

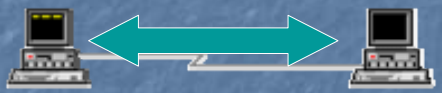
VICTIM OF CRIME

TECNOMEDIAZIONE E INTERNET FRAUD

UN SOGGETTO SI DIFENDE DALLE TRUFFE OFF-LINE FORMANDOSI UN'IMPRESSIONE DI AFFIDABILITA' DELLO SCENARIO E DELL'INTERLOCUTORE SU BASE VISIVA, UDITIVA E INTUITIVA (SISTEMA LIMBICO)



LA TECNOMEDIAZIONE RIDUCE LA PERCEZIONE DEL RISCHIO


GLI INTERROGATIVI PER LA PREVENZIONE PSICOLOGICA DEL PHISHING

PERCHE' ALCUNI RISPONDONO?

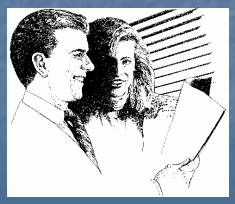
PERCHE' MOLTI NON RISPONDONO?

COSA PERCEPISCONO E PENSANO QUELLI CHE NON RISPONDONO?

E' POSSIBILE FORNIRE A QUELLI CHE RISPONDONO GLI STESSI STRUMENTI COGNITIVI DI QUELLI CHE NON RISPONDONO ?

Progetto phishing

- Lo studio si prefigge di analizzare il fattore umano nell'ambito della dinamica delle più diffuse frodi on-line, in particolare rispetto al fenomeno emergente del "*phishing*".



Progetto phishing

- In particolare vengono prese in considerazione le reazioni emotive e comportamentali e la valutazione del rischio da parte degli utenti di internet.

Progetto phishing

- La finalità dello studio è centrata sulla prevenzione del fenomeno attraverso la progettazione di percorsi di sensibilizzazione mirata.

QUESTIONARIO OFRPQ

- (A) Questionario strutturato O.F.R.P.Q. (On-line Fraud Risk Perception Questionnaire) ICAA da somministrare ad un campione *random* di 5000 utenti di internet.

QUESTIONARIO OFRPQ

Lo strumento intende misurare l'incidenza generale del fenomeno in una specifica popolazione, le sue tipologie e la reazione psicologica del soggetto ricevente.

- Il questionario OFRPQ è assolutamente anonimo, è composto da circa 15 items e da una sezione contenente le informazioni biografiche dell'utente.
- Il tempo di compilazione è di circa 10 minuti.

INTERVISTA SEMISTRUTTURATA

(B) Intervista semistrutturata ICAA da somministrare ad un campione di 100 utenti di internet che usufruiscono assiduamente dei servizi di banca on-line e altre attività economiche mediate dalla rete e che negli ultimi mesi hanno ricevuto email di phishing.

I soggetti utilizzabili vengono estrapolati da quelli a cui viene somministrato il questionario O.F.R.P.Q..

INTERVISTA SEMISTRUTTURATA

Lo strumento intende approfondire gli atteggiamenti e le reazioni di soggetti che hanno subito un tentativo di frode (*phishing*).

L'intervista ha un tempo di somministrazione di circa 45 minuti e deve essere condotta da psicologi-criminologi qualificati ed appositamente addestrati attraverso un breve corso di formazione (di circa 3 ore).

STUDIO DELLE EMAIL-PHISHING

- (C) Analisi psico-criminologica degli strumenti del *phishing* usati dai criminali.
- Attraverso un'analisi linguistica, grafica e contenutistica verrà delineato il livello di sofisticazione della frode e eventuali modifiche diacroniche dei messaggi, cercando di individuare quelli maggiormente efficaci rispetto al campione di utenti considerato.
- Tale fase prevede una valutazione comparata di un campione di email inviate negli ultimi mesi agli utenti italiani.

OBBIETTIVI DELLA RICERCA

1. AREA DI STUDIO: incidenza del fenomeno
2. AREA DI STUDIO: modus operandi
3. AREA DI STUDIO: reazioni della vittima

1° OBBIETTIVO: CREARE UNO STRUMENTO DI PREVENZIONE HUMAN FACTOR

2° OBBIETTIVO: SVILUPPARE LE TECNICHE INVESTIGATIVE

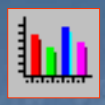
3° OBBIETTIVO: MIGLIORARE LE TECNOLOGIE DI PREVENZIONE

Tempistica della ricerca

- Elaborazione e pre-testing degli strumenti: entro fine dicembre 2005 (completata)
- Somministrazione questionari e interviste semistrutturate: entro fine aprile 2006:
- analisi dei dati, report finale, convegno di studi e presentazione dei dati alla stampa: entro il 20 maggio 2006

INSIDE ATTACK
ICAA RESEARCH PROJECT

CRIMINAL PROFILING
INSIDER SU BASE STATISTICA



INSODDISFAZIONE SUL PROPRIO LAVORO

VENDETTA

PAGA INADEGUATA

DIFFICOLTA' FINANZIARIE PERSONALI

DISTURBI PSICHIATRICI E ABUSO DI SOSTANZE

ELEMENTI TROPPO DIFFUSI PER COSTITUIRE UN VALIDO INDICATORE DI RISCHIO

HIGH PROFILE INSIDE :
TECNICHE INFORMATICHE DI ATTACCO

INSIDER

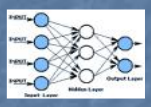
SOCIAL ENGINEERING

- **PRIVILEGE ESCALATION**
- **SNIFFING**
- **SPOOFING**
- **LEAST PRIVILEGE LACK EXPLOIT**
- **PASSWORD CRACKING**
- **BACK DOOR/TROJAN HORSE**
- **DENIAL OF SERVICE**
- **VIRUS**
- **TUNNELING**
- **DUPSTER DIVING**
- **HACKER TOOLKIT**
- **EXPLOIT APPLICATIVO**

INSIDE ATTACK DATABASE

Duke UNIVERSITY

DESCRIZIONE ATTACCO



NNPCP

HIGH PROFILE

LOW PROFILE

UNAWARE

COMPETENZA INFORMATICA

COLLOCAZIONE GERARCHICA

MOTIVAZIONE

CARATTERISTICHE BIOGRAFICHE

NEURAL NETWORK FOR PSYCHOLOGICAL CRIMINAL PROFILING

COMPUTER CRIME RISK PERCEPTION

ICAA RESEARCH PROJECT

L'importanza del "fattore umano" nell'ambito della sicurezza informatica

- Ogni sofisticato sistema di sicurezza fisico e logico può essere vanificato da utilizzatori non addestrati o poco convinti della sua necessità….

CONCEZIONE AVANZATA DEL FATTORE UMANO

PSYCHOLOGICAL RISK ASSESSMENT

FATTORE UMANO → ANALISI PSICOLOGICA SISTEMA/UTENTI → MISURAZIONE PERCEZIONE DEL RISCHIO

↓

FORMAZIONE SENSIBILIZZAZIONE FOCUS GROUP → INCREMENTO DELLA MOTIVAZIONE AL RISPETTO PROCEDURE

PSYCHOLOGICAL TRAINING

Strumenti dell'ICAA sugli aspetti psicologici della sicurezza informatica

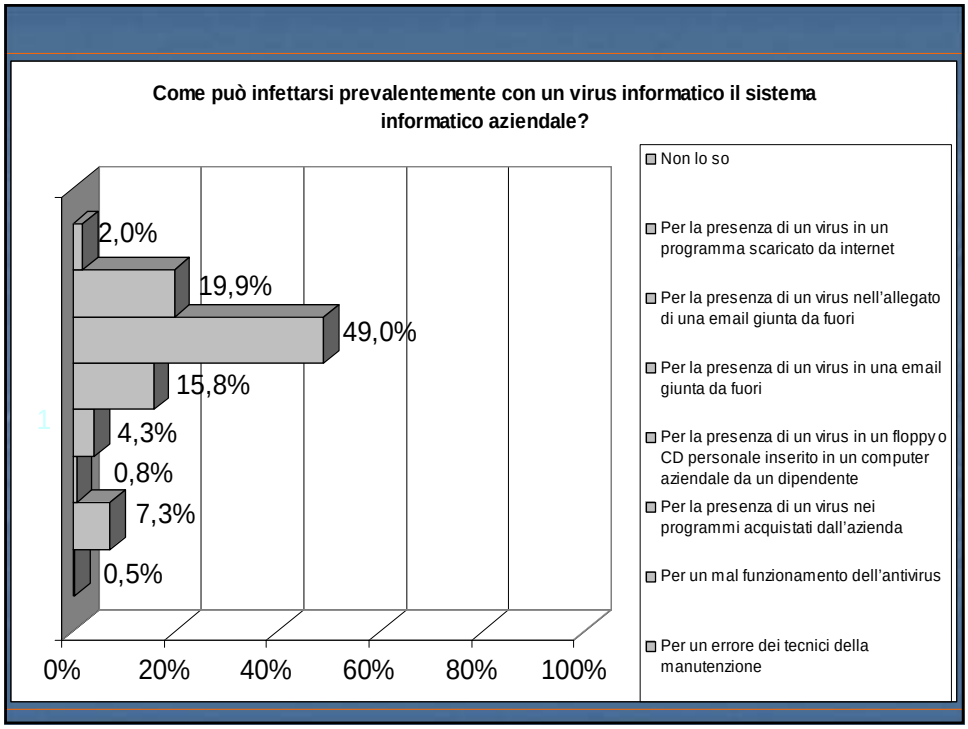
SECURITY ASSESSMENT

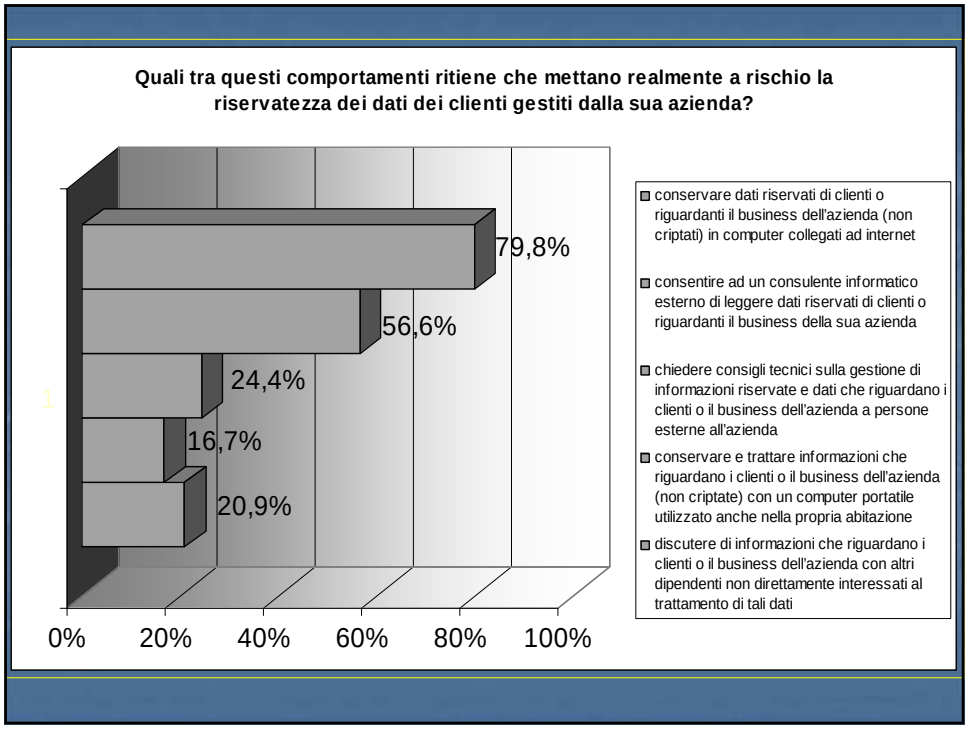
PSYCHOLOGICAL RISK ASSESSMENT (ICAA)

- **ICT security Top-management interwiew**
- **Workplace Computer Crime Analysis Grid (W.C.A.G.)**
- **Computer crime Risk Perception Questionnaire (C.R.P.Q)**
- **Workplace Computer Crime Psychology Questionnaire (W.C.P.Q.)**
- B.I.P.Q. (Biometrics Impact Perception Questionnaire)

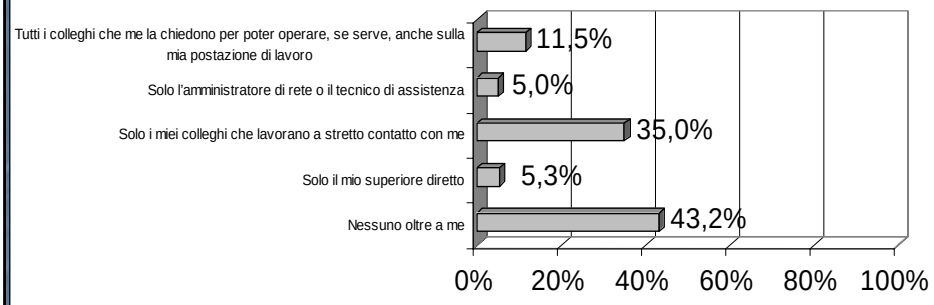
CRPQ

Computer crime Risk Perception Questionnaire

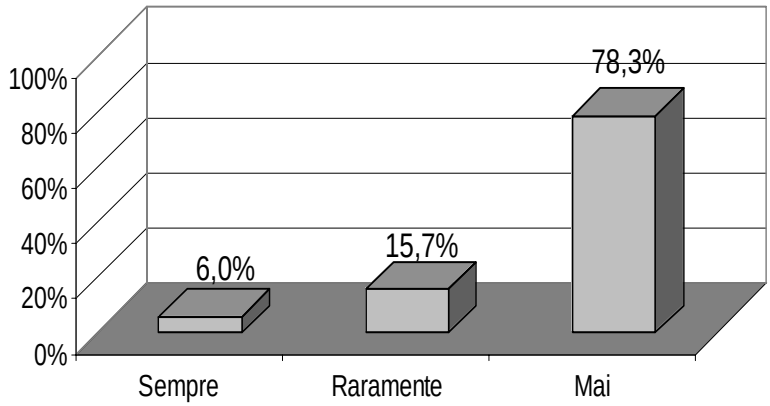

Come può infettarsi prevalentemente con un virus informatico il sistema informatico aziendale?
2,0%
19,9%
49,0%
15,8%
4,3%
0,8%
7,3%
0,5%
0%
20%
40%
60%
80%
100%
Non lo so
Per la presenza di un virus in un programma scaricato da internet
Per la presenza di un virus nell'allegato di una email giunta da fuori
Per la presenza di un virus in una email giunta da fuori
Per la presenza di un virus in un floppy o CD personale inserito in un computer aziendale da un dipendente
Per la presenza di un virus nei programmi acquistati dall'azienda
Per un mal funzionamento dell'antivirus
Per un errore dei tecnici della manutenzione


Quali tra questi comportamenti ritiene che mettano realmente a rischio la riservatezza dei dati dei clienti gestiti dalla sua azienda?
79,8%
56,6%
24,4%
16,7%
20,9%
0%
20%
40%
60%
80%
100%
conservare dati riservati di clienti o riguardanti il business dell'azienda (non criptati) in computer collegati ad internet
consentire ad un consulente informatico esterno di leggere dati riservati di clienti o riguardanti il business della sua azienda
chiedere consigli tecnici sulla gestione di informazioni riservate e dati che riguardano i clienti o il business dell'azienda a persone esterne all'azienda
conservare e trattare informazioni che riguardano i clienti o il business dell'azienda (non criptate) con un computer portatile utilizzato anche nella propria abitazione
discutere di informazioni che riguardano i clienti o il business dell'azienda con altri dipendenti non direttamente interessati al trattamento di tali dati

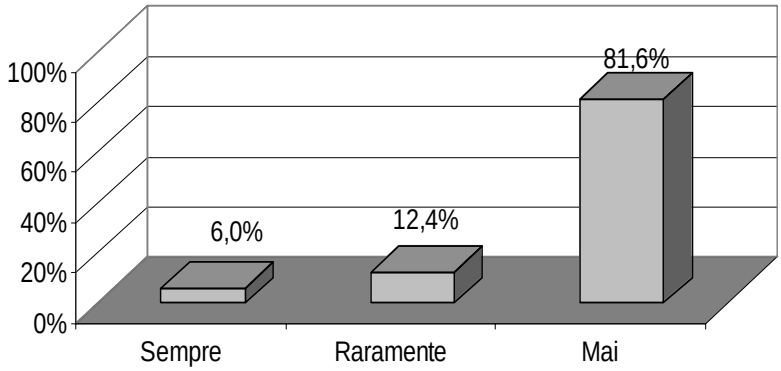
Quante persone conoscono la sua password?



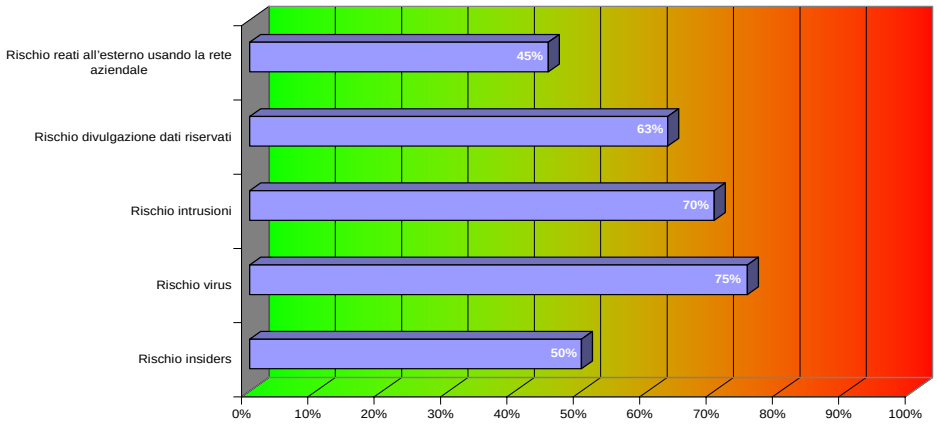
Le capita di connettersi ad Internet con modem e contemporaneamente alla LAN aziendale?



Le capita di disattivare per brevi periodi l'antivirus per velocizzare il PC durante alcune operazioni specifiche?



L'andamento delle aree critiche CRPQ nel campione analizzato



HUMAN FACTOR E CERTIFICAZIONE DI SICUREZZA ICT

CERTIFICAZIONE DI SICUREZZA ICAA HF- ICT/2006

OPERATORE ICT – SINGOLO PROFESSIONISTA

RESPONSABILE SICUREZZA ICT (TRAINER)

AZIENDA - ORGANIZZAZIONE

Disponibile su richiesta
www.criminologia.org