ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Come formarli (e perché)

Il punto di partenza

Le modalità della formazione

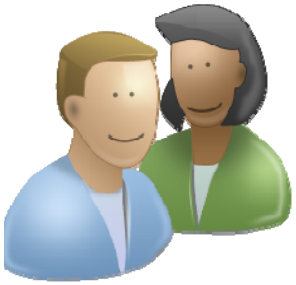
Gli argomenti da toccare

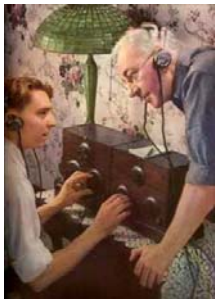
Cosa serve

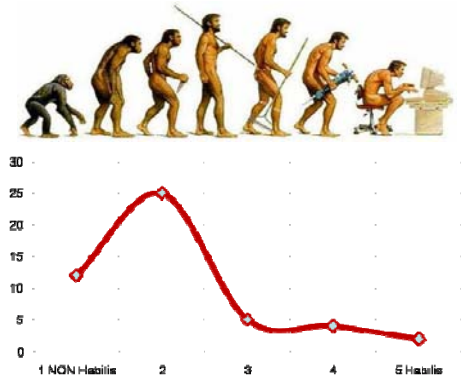
PDCA

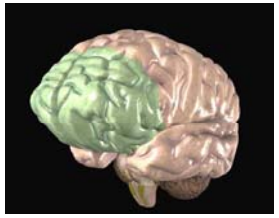
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

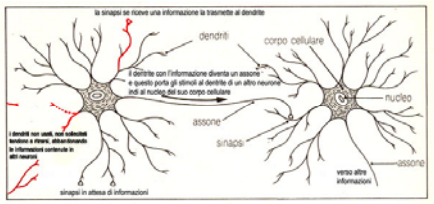
Riassumendo

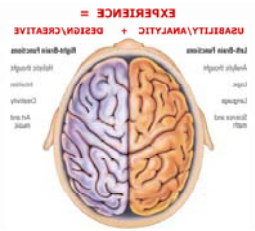


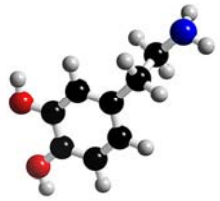












distorsione informativa
pre-decisionale

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Come formarli (e perché)

Il punto di partenza

Le modalità della formazione

Gli argomenti da toccare

Cosa serve

PDCA

Il punto di partenza:

Il progetto formativo

- L’utente
- Competenze da trasmettere
- Le modalità

Come formarli (e perché)

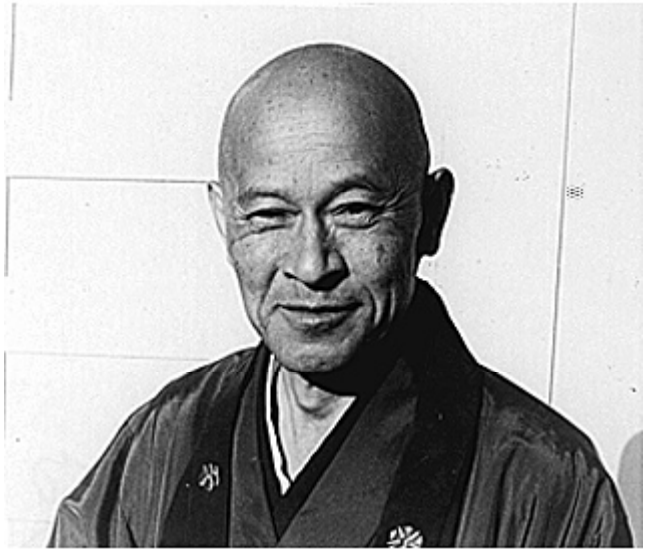
Il punto di partenza:

l'Utente

- Utentepitecus NON habilis
- Sceglie in base alle emozioni
- Non avvezzo alla formazione tecnica

"Il vero segreto dell'apprendimento è avere sempre una mente da principiante perché nella mente di un principiante ci sono molte possibilità, nella mente di un esperto, poche“

Shunryu Suzuki
Maestro Zen e scrittore



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Come formarli (e perché)

Gli argomenti da toccare

- Normativa
- Obiettivi aziendali
- Metodi di controllo
- Chi è pericoloso ?
- I perché
- I luoghi comuni
- Attacchi tecnologici
- Difese tecnologiche
- Attacchi non tecnologici (SE)
- Difese non tecnologiche
- Risorse aziendali
- Riferimenti

Come formarli (e perché)

Le modalità della formazione

Fruibilità

- Logos
- Semplicità
- Esempi pratici
- Immagini e Filmati
- Interesse personale
- E - learning (?)

Interattività

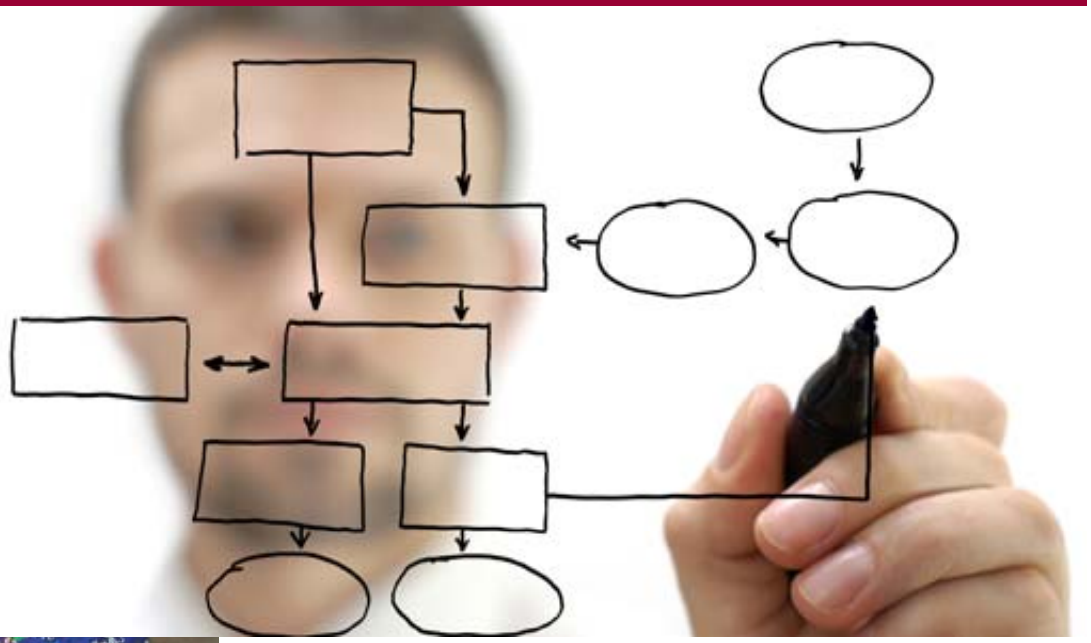
- Esercitazioni
- Case scenarios
- Q & A

L'APPRENDIMENTO

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Apprendimento semantico

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter



Apprendimento esperienziale

Apprendimento esperienziale

2001: a space odissey

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Apprendimento esperienziale

L’attimo fuggente

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

REPETITA IUVA[N]T

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Repetita iuva[n]t

Minuti

Ore

Settimane

Mesi

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

e-learning

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

E-learning

Possibile ma… non è la stessa cosa !

Ottimo per:
- **Introduzioni**
- **Refresh**
- **Approfondimenti**
- **Test**
- **Forum**

Iscrivereste vostro figlio ad un corso di…


…nuoto on-line ?

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

IL PATTO

“Ciao, mi chiamo Carlo…”

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

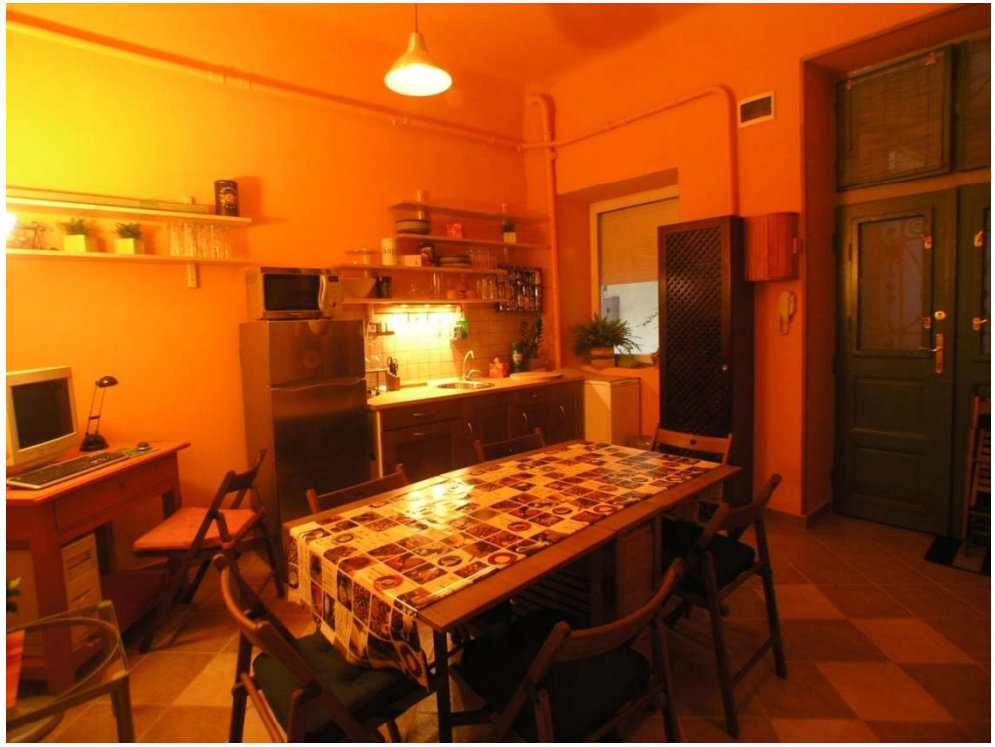
PERSONAL USE

OF THE TRAINING

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Personal use

"Che bisogno ha una persona di tenersi un computer in casa?"



Kenneth Olsen,
fondatore della Digital Equipment,
alla convention della World Future Society 1977

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Personal use

“Internet... ben presto esploderà in modo spettacolare, come una supernova, e nel 1996 collasserà catastroficamente. “

Robert Metcalfe,
fondatore della 3Com,
inventore dello standard Ethernet, 1992

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

L'ATTENZIONE

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

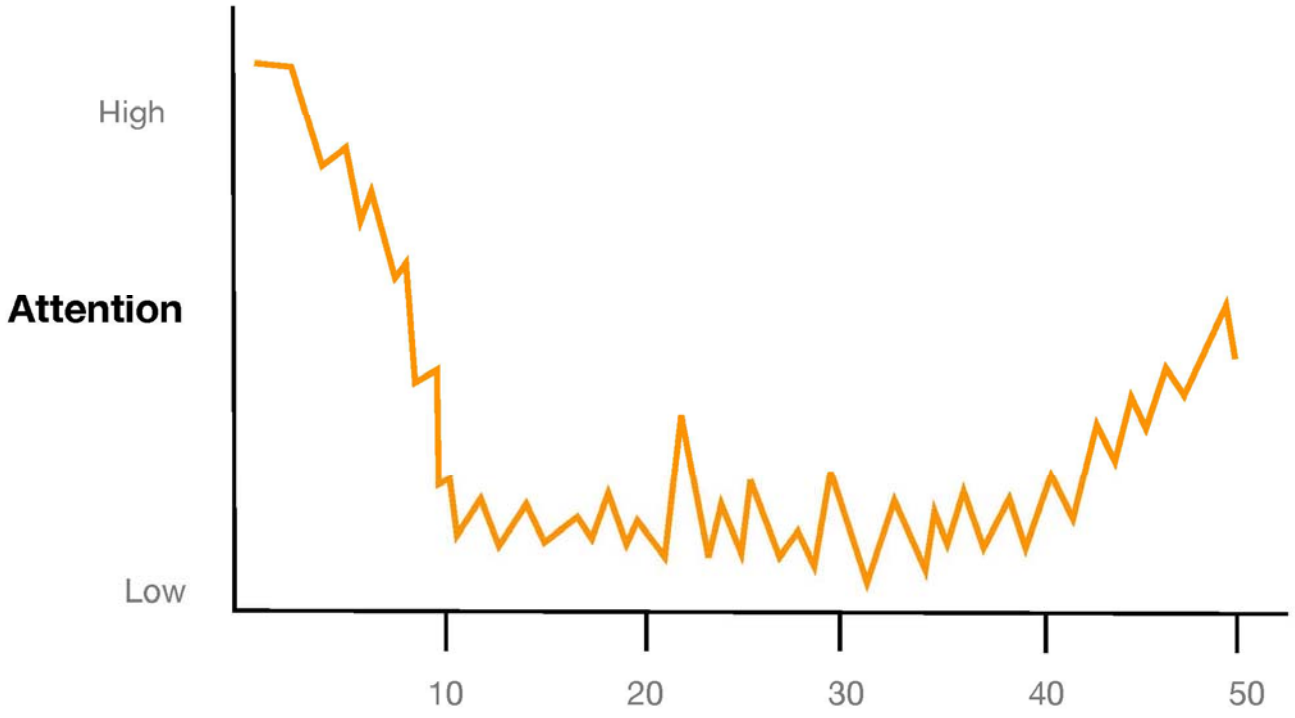
L'attenzione degli utenti è un bene prezioso, proteggiamolo !!!

Le modalità della formazione

La capacità di concentrazione è una cosa che non esiste.
Esiste solo la qualità di ciò che si percepisce.
La gente presta un'attenzione infinita, se si diverte.

Jerry Seinfeld

The 10-minute rule



Source: www.brainrules.net/attention

Come formarli (e perché)

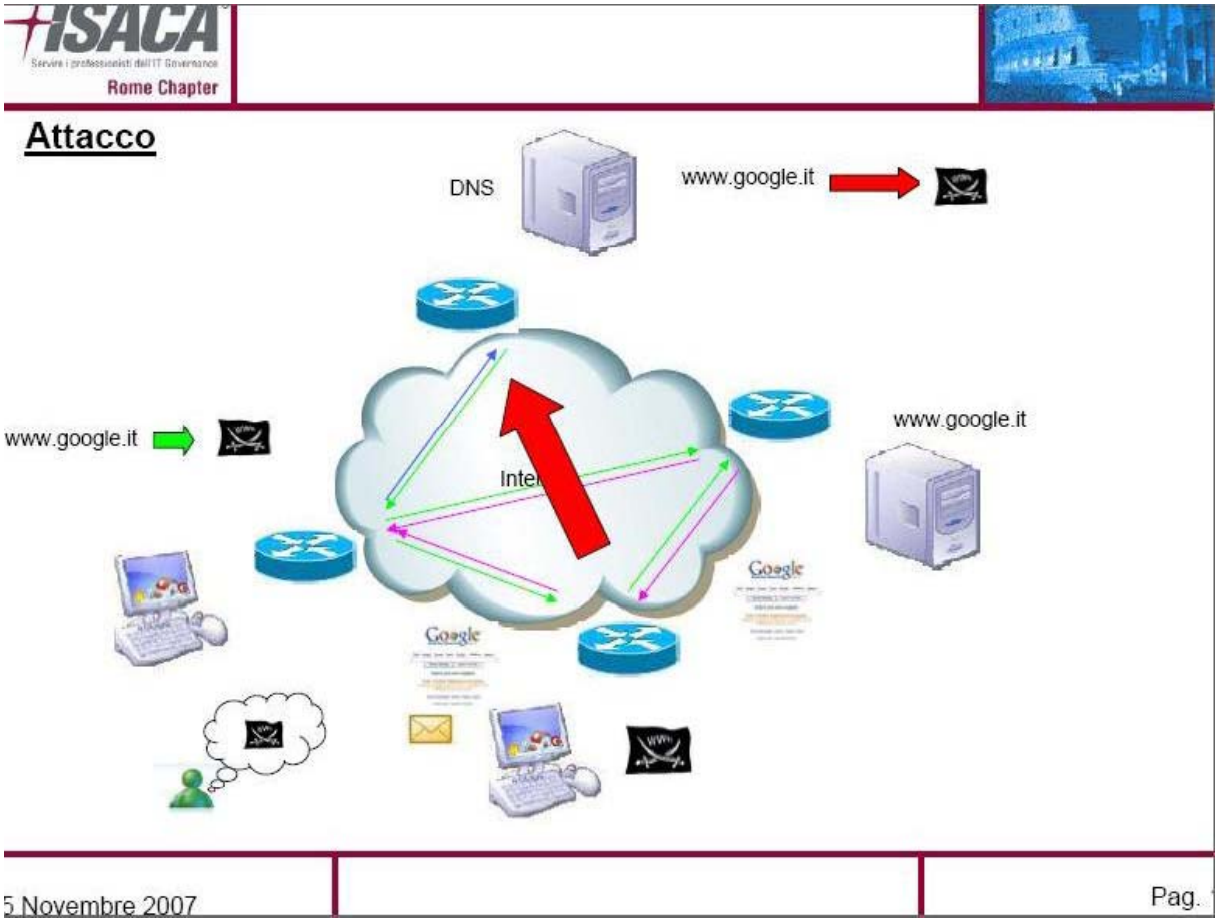
- Informazioni tecniche [fruibili]
- Filmati
- Immagini
- Esempi pratici

…

EMOZIONI !!!

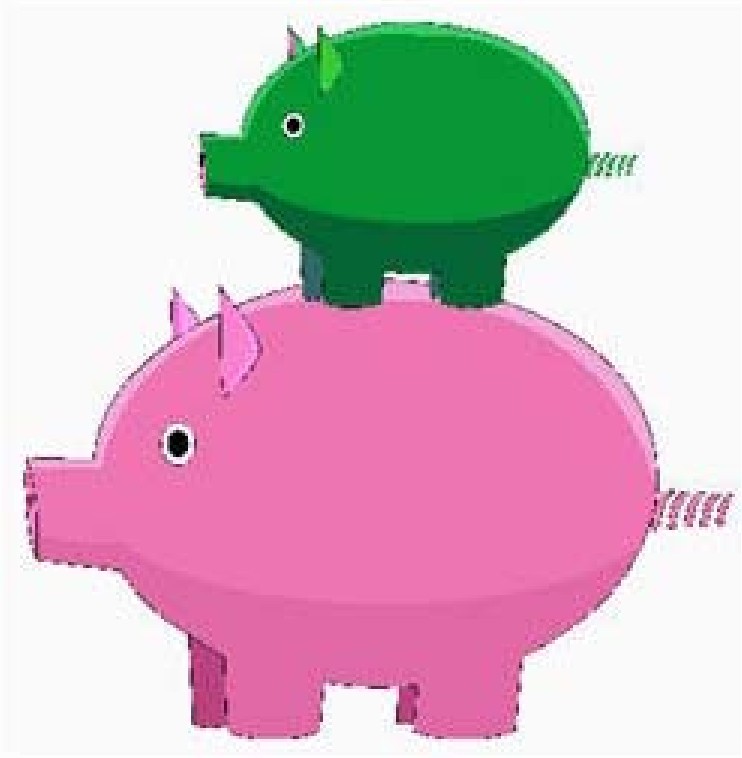
ESEMPI

Esempi


ISACA
Rome Chapter
Attacco
DNS
www.google.it
www.google.it
www.google.it
Google
Google
5 Novembre 2007
Pag.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Piggy Backing



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Piggy Backing

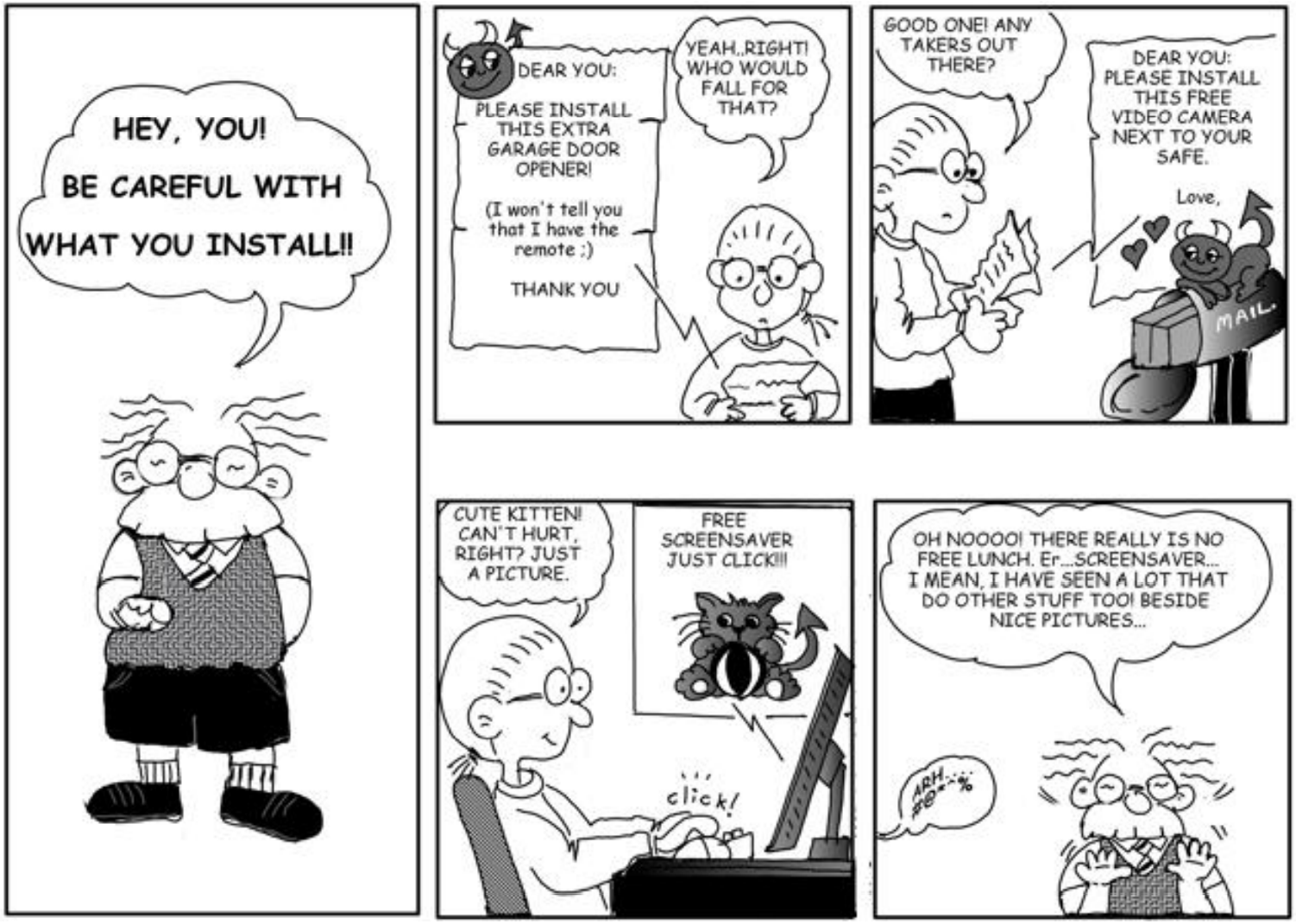
- 1. Following an authorized person into a restricted access area.
- 2. Electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions.

Fonte: ISACA Glossary of Terms
1 June 2008

L’ottavo nano

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Unauthorized downloads



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Disaster recovery

- DILBERT

Password rules

- DILBERT

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Shoulder surfing

Spam

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Lo Spamming e Wikipedia

- Lo ***spamming*** (detto anche **fare spam** o **spammare**) è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Lo Spamming e Wikipedia

Origine del termine [modifica]

Il termine trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam …Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con "spam" ("uova e spam, uova pancetta e spam, salsicce e spam" e così via) si contrappone alla riluttanza del cliente per questo alimento, il tutto in un crescendo di un coro inneggiante allo "spam" da parte di alcuni Vichinghi seduti nel locale.[

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Le Porte TCP

Le **porte note** (traduzione dell'inglese *known ports*) sono le porte TCP e UDP nell'intervallo 0-1023 e sono assegnate a specifici servizi dalla IANA. …I numeri delle porte registrate sono quelli nell'intervallo 1024-49151. I numeri di porta dell'intervallo 49152-65535 appartengono a porte private o dinamiche e non sono utilizzati da un'applicazione in particolare.

Fonte: Wikipedia

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Firewall medievale

"…Una prima definizione chiusa di firewall è la seguente:

Apparato di rete hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa. …"

Fonte: Wikipedia

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Antivirus medievale

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

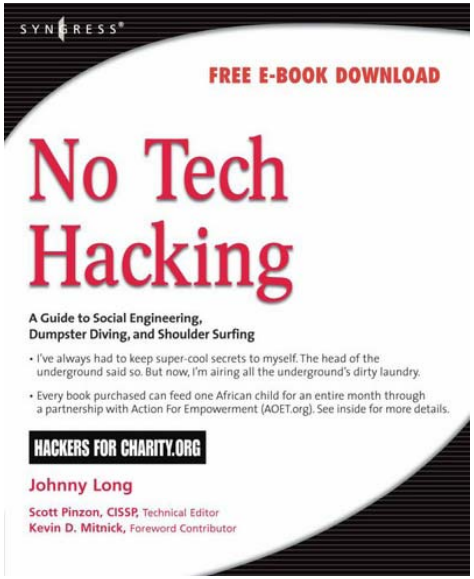
Helpdesk medievale

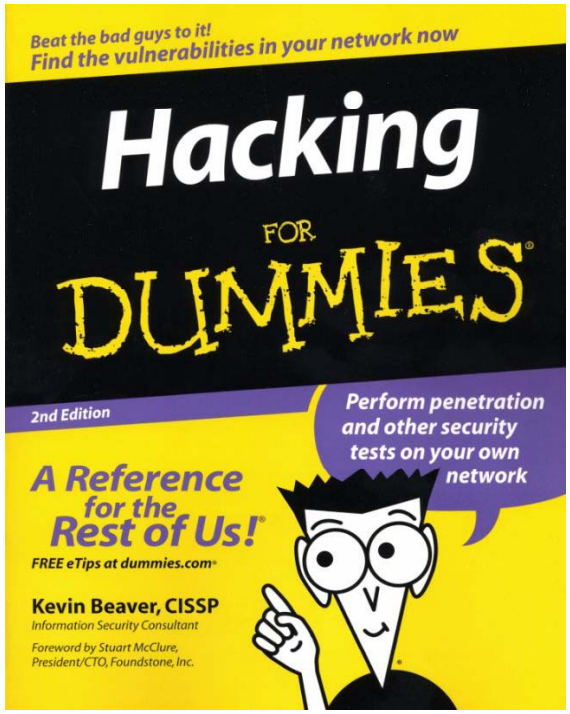
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

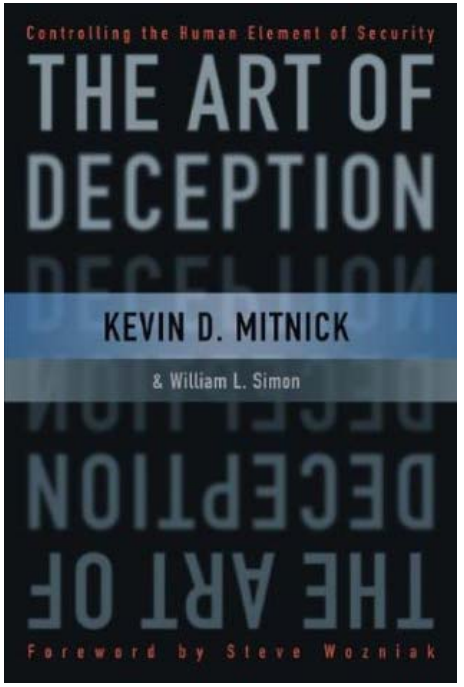
Sensibilizzazione

www.cybertipline.com

Procedura
Cifratura
Ethical Hacking
Phone freaks
Social Engineering
Steganografia
Trojans
Key Loggers
…


SYNGRESS
FREE E-BOOK DOWNLOAD
No Tech Hacking
A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing
• I've always had to keep super-cool secrets to myself. The head of the underground said so. But now, I'm airing all the underground's dirty laundry.
• Every book purchased can feed one African child for an entire month through a partnership with Action For Empowerment (AOET.org). See inside for more details.
HACKERS FOR CHARITY.ORG
Johnny Long
Scott Pinzon, CISSP, Technical Editor
Kevin D. Mitnick, Foreword Contributor


Beat the bad guys to it!
Find the vulnerabilities in your network now
Hacking
FOR
DUMMIES
2nd Edition
A Reference for the Rest of Us!
FREE eTips at dummies.com
Perform penetration and other security tests on your own network
Kevin Beaver, CISSP
Information Security Consultant
Foreword by Stuart McClure, President/CTO, Foundstone, Inc.


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

I TEMPLATE

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Strumenti: Termografie

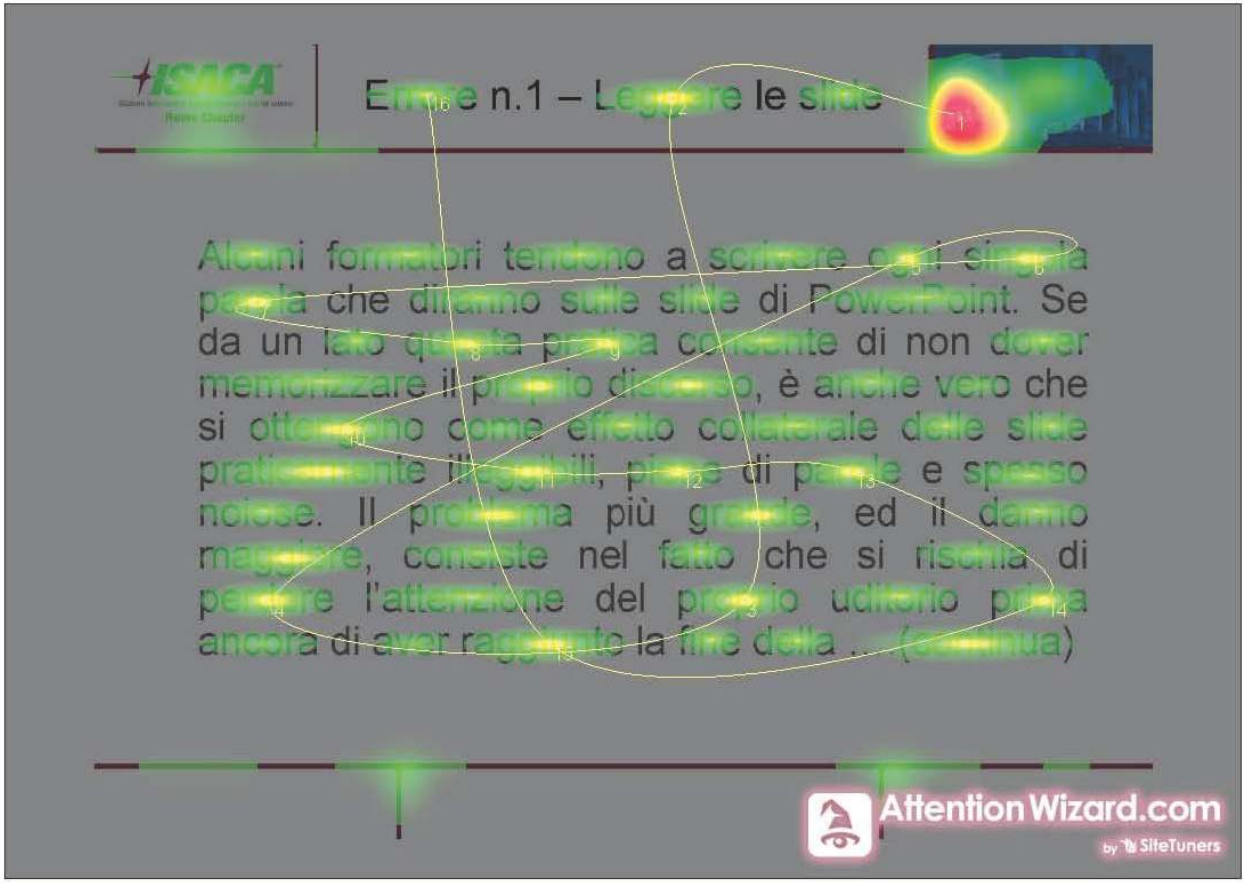
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Errore n.1 – Leggere le slide

Alcuni formatori tendono a scrivere ogni singola parola che diranno sulle slide di PowerPoint. Se da un lato questa pratica consente di non dover memorizzare il proprio discorso, è anche vero che si ottengono come effetto collaterale delle slide praticamente illeggibili, piene di parole e spesso noiose. Il problema più grande, ed il danno maggiore, consiste nel fatto che si rischia di perdere l'attenzione del proprio uditorio prima ancora di aver raggiunto la fine della ….(continua)

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Strumenti: Termografie



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

GLI ORARI


10-20 %


10-20 %


15:00

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

CONTENT MODE

FAC[T]S & FIGURES

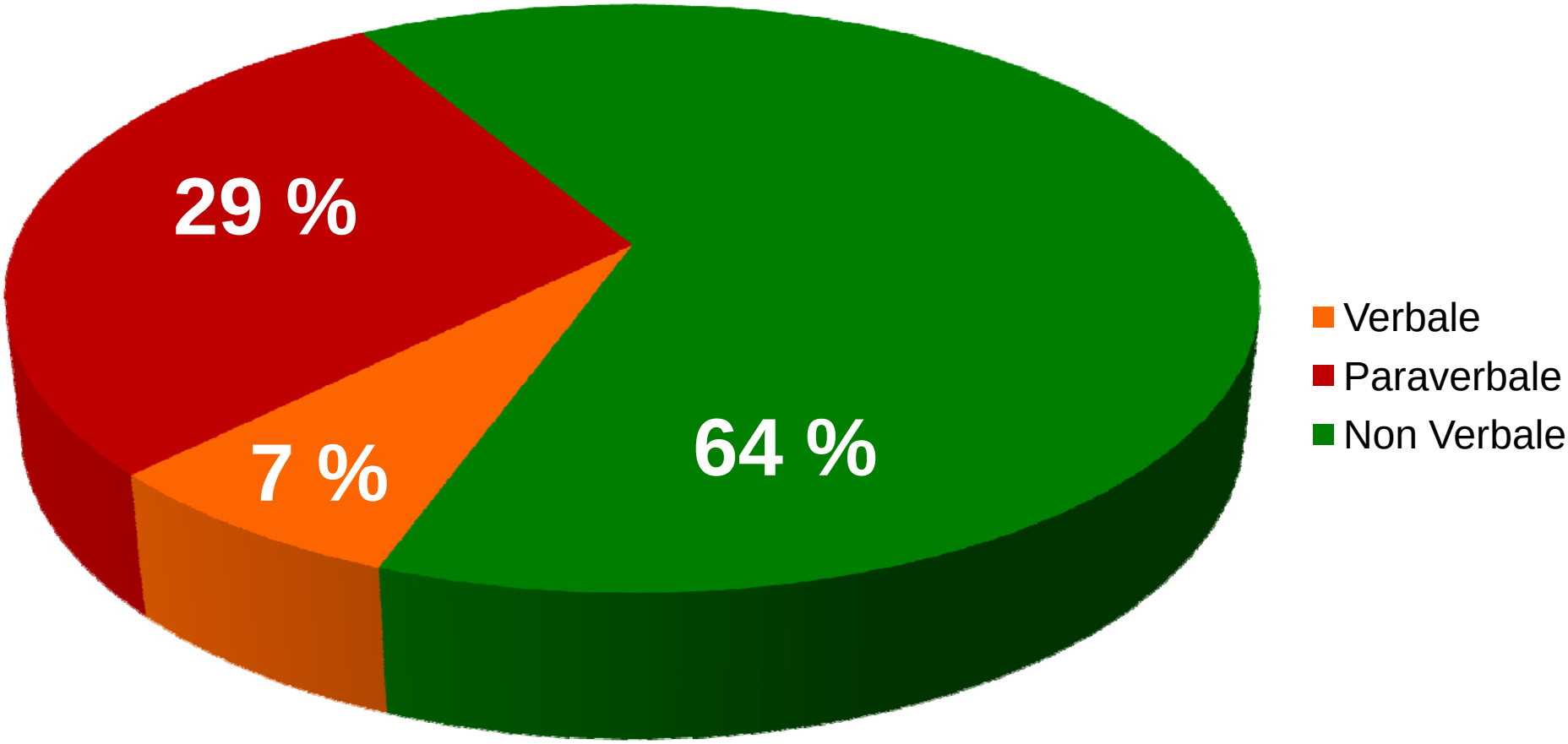
Perché le immagini ?

Circa 1/3 della corteccia cerebrale è dedicata alla interpretazione delle immagini

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

L'approccio visivo

Canali della comunicazione



Dopo 3 giorni…

10%

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Dopo 3 giorni…

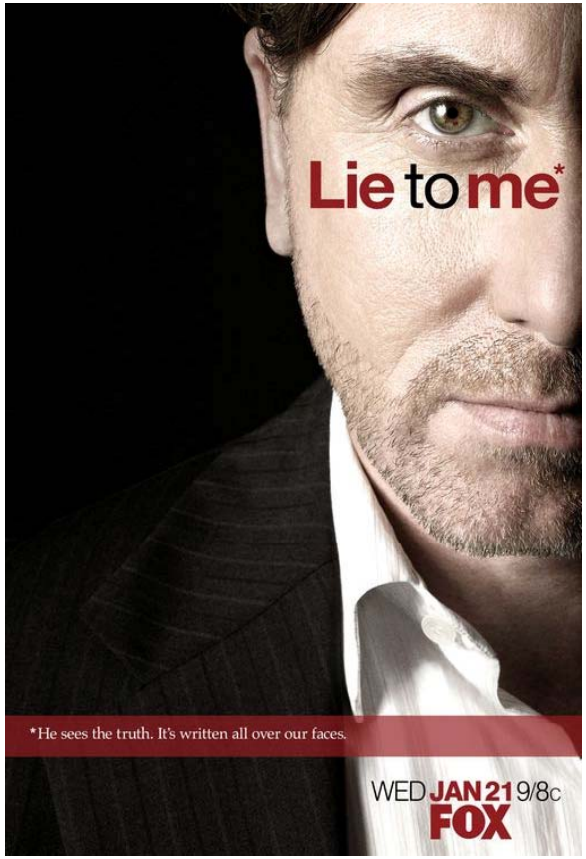
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Dopo 3 giorni…

65%

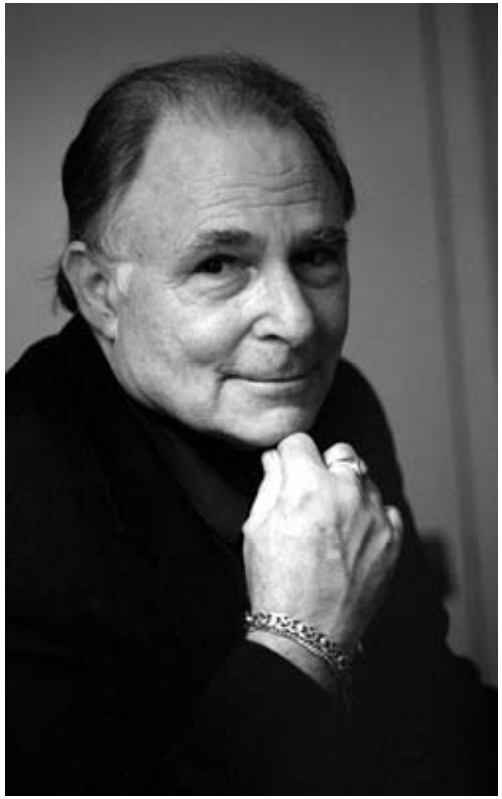
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Perché le immagini ?



FACS

Facial
Action
Coding
System



Paul Ekman

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Perché le immagini ?

Il 64% della comunicazione
avviene in forma non verbale

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Perché le immagini ?

Il 64% della comunicazione
avviene in forma non verbale



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Perché le immagini ?

Perché le immagini ?

Le domande fondamentali

Riuscirò a mangiarlo ?

Riuscirà a mangiarmi ?

Mi ci posso accoppiare?

Si accoppierà con me?

L'ho già visto ? [ho un ricordo in merito?]

Perché le immagini ?

Le domande fondamentali

Se lo faccio ne avrò un danno ?

Mi conviene farlo ora oppure in seguito?

L’ho già visto ? [ho un ricordo in merito?]

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Non dobbiamo cercare di trasformarli in…

… specialisti della sicurezza…

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

…ma dobbiamo portarli a fare (e farsi)…

… le domande appropriate…

…per trovare (o farsi dare)..

…le risposte giuste

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Come formarli (e perché)

Cosa serve

Competenze tecniche

Capacità relazionali

Immaginazione

Curiosità

Voglia di divertirsi

(e di mettersi

in discussione)

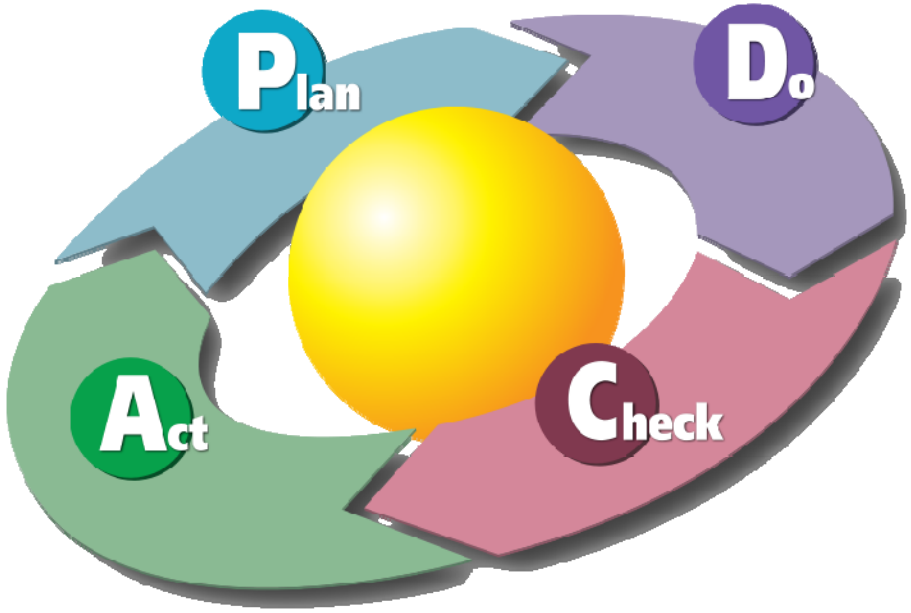
Budget

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

PDCA

Assessment
Contenuti
Modalità della comunicazione
Tempi
Logistica
Budget

Realizzazione



Attuazione dei correttivi

Feedback
Test pre-fine sessione
Test periodici

Misuriamo i risultati

Misurazione diretta

- Modulo di feedback
  - Gradimento del corso
  - Mood
- Apprendimento (test)
- Q&A sessions
- KPI interni

Misuriamo i risultati

Misurazione indiretta

- KPI esterni
  - HD calls
  - andamento utilizzo risorse
- richieste di iscrizione (al corso)
- commenti con colleghi

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

‘Venderlo’ in azienda

Costo o investimento ?

- R.O.I .

Strategia di presentazione

- a chi ? M.A.N.

Modalità di erogazione

- classi eterogenee ?
- durata ?
- in azienda ?
- …

‘Venderlo’ in azienda

Costo o investimento ?

‘Venderlo’ in azienda

R.O.I.

$$ROI = \frac{Risultato\ operativo}{Capitale\ investito}$$

dove per Risultato Operativo si intende il risultato economico della sola Gestione Caratteristica, mentre per Capitale Investito si intende il totale degli impieghi caratteristici, ossia l'Attivo Totale Netto meno gli Investimenti Extracaratteristici (investimenti non direttamente afferenti all'attività aziendale, ad esempio immobili civili)

Fonte: Wikipedia

‘Venderlo’ in azienda

R.O.I.

Costi

- Progettazione
- Infrastruttura
- Erogazione
- …

Ricavi

- Conformità

  [Esiti Audit]

- Ottimizzazione risorse

  [KPI sicurezza]

  [KPI risorse]

  [Chiamate SD]

  [Produttività]

  …

Strategia di presentazione: a chi ?

M A N

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

‘Venderlo’ in azienda

Modalità di erogazione

classi eterogenee ?

durata ?

in azienda o fuori ?

quante persone per classe ?

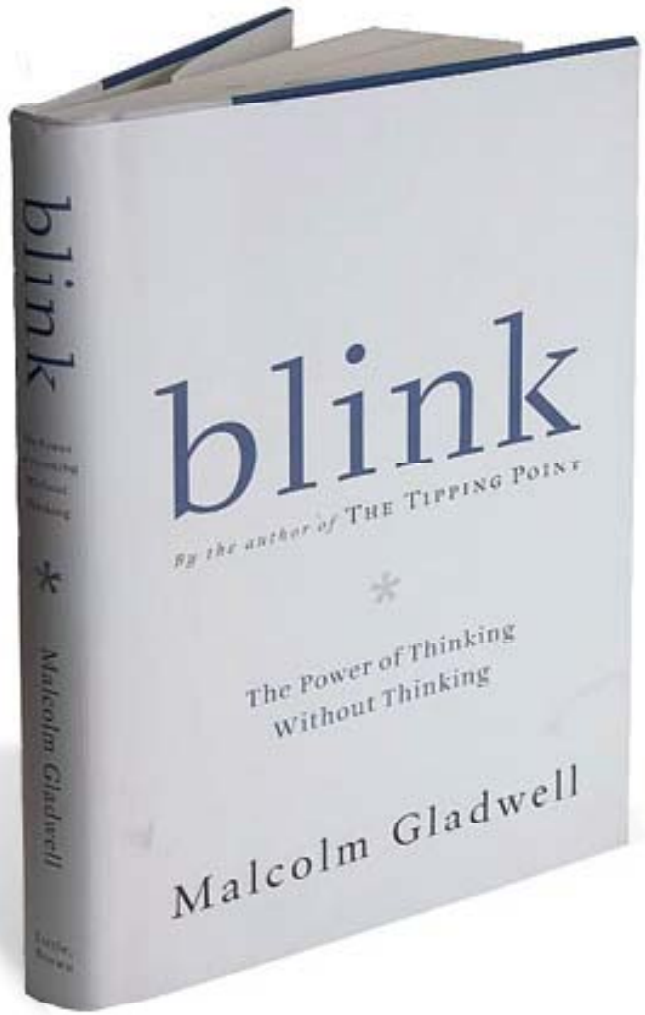
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Per approfondire

TED Ideas worth spreading

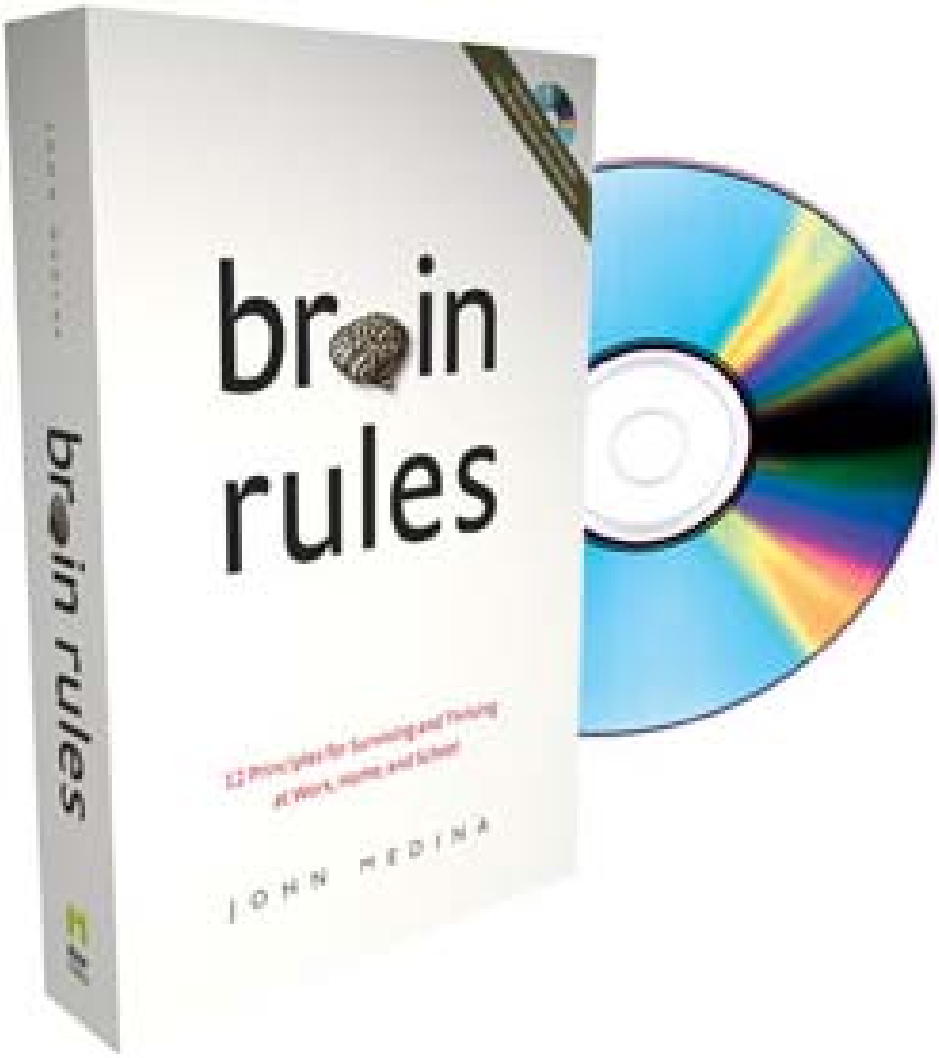
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Per approfondire



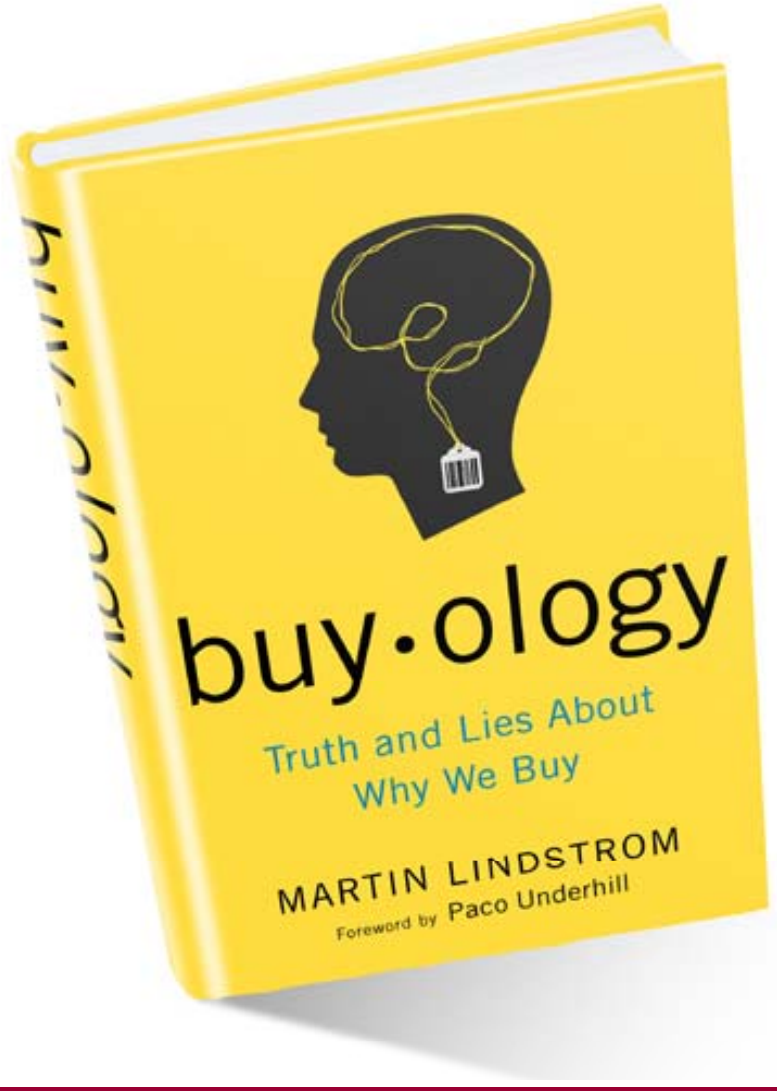
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Per approfondire



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Per approfondire



UN CASO REALE

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

L’azienda

- Filiale italiana di società biomedicale americana
- Quotata al NYSE
- HQ + 12 sedi periferiche
- 120 dipendenti + 240 collaboratori esterni
- Fatturato 130 M€ ca.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Il progetto

- Analisi congiunta del fabbisogno
- Personalizzazione
- Erogazione di base
- Format
- Consulenza media
- Formazione ai formatori
- Consulenza per l’integrazione e-learning

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Il progetto – opzioni aggiuntive

- Dispense
- Test periodici
- Assessment periodico
- Pillole trimestrali
- Gioco a premi
- ….

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Erogazione

- doppia/tripla modalità
  - middle management
  - utenti
  - top management

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Budget

- 40% HR
- 40% Quality & Compliance
- 20% IT

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Target formativi

- Formazione ex. D.Lgs.231/01
- Formazione ex D.Lgs.196/03
- Ottimizzazione utilizzo risorse IT
- Diminuzione esposizione al rischio

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Erogazione

- aule da 20 discenti max.
  - 114 discenti
  - test ingresso
  - test uscita
- versione mid : 2 giorni
- versione users: 1 giorno
- versione Top : ½ giornata
- attestato di partecipazione

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Argomenti trattati

- Normative (SOX,196/03,231/01,C.P.,…)
- Auditing e Controllo
- Sicurezza delle informazioni
  - Storia
  - Attacchi tecnologici
  - Difese tecnologiche
  - Attacchi non tecnologici
  - Difese non tecnologiche
  - Esercitazioni pratiche
- Utilizzo risorse tecnologiche aziendali

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

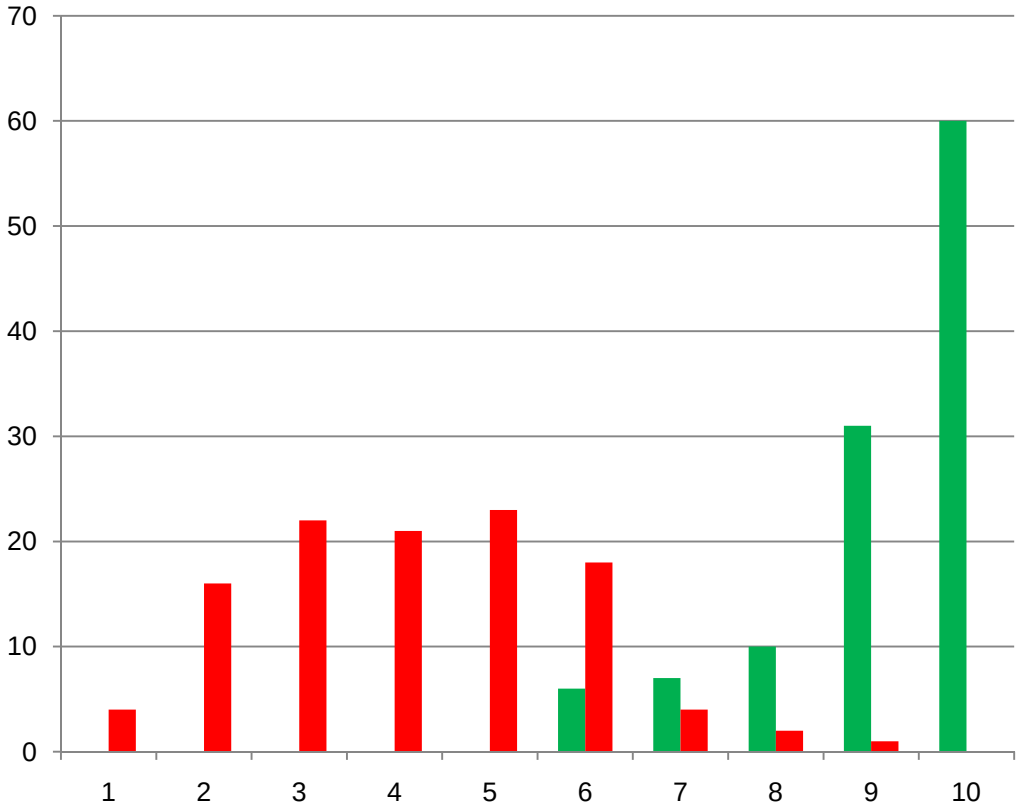
Contenuti **L.Lassig**

Ns. esempio	**Oggi**	**11/03/10**
Durata(m) :480	**210**	**36:49**
Slide/Vis. : 82	217	350
Immagini : 45		101
Animazioni : 32		42
Filmati : 5		10
Grafici : 8		1
Parole : 2000 ca.		830

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Misurazione



test ingresso : 4,05/10

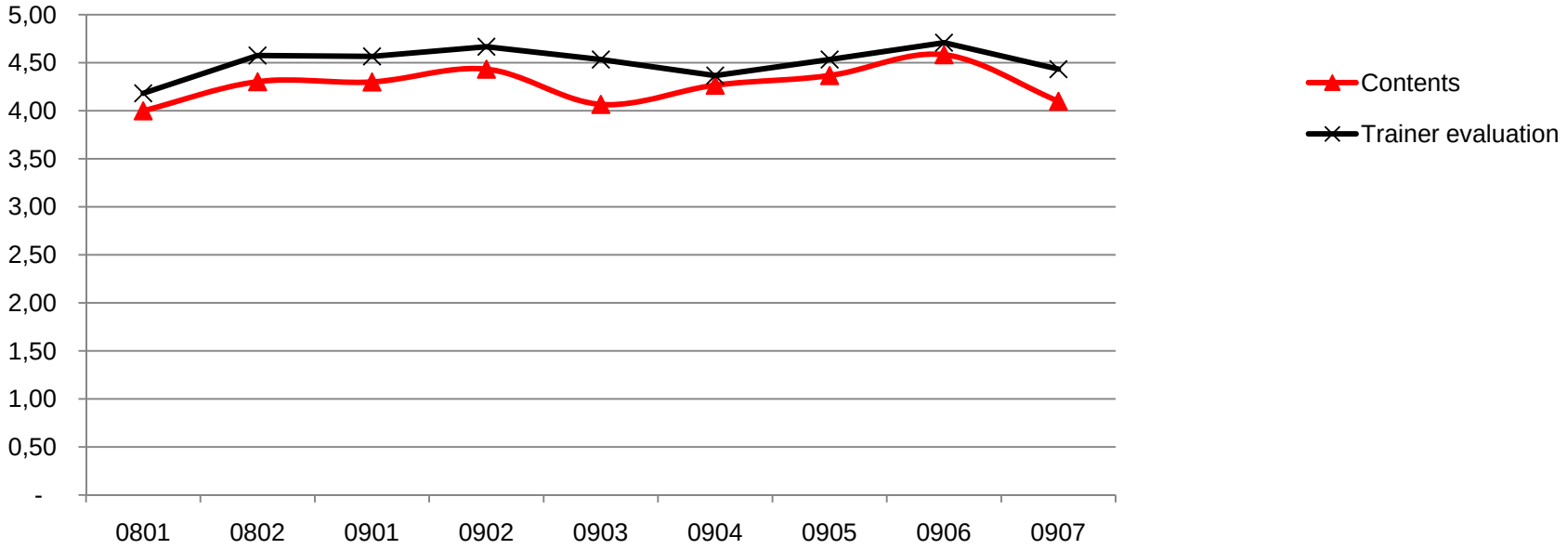
test uscita : 9,07/10

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Misurazione

- valutazione del corso : 4,32/5
- valutazione delle metodologie: 4,34/5
- valutazione del formatore : 4,59/5



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Alcuni commenti

Ora ho capito!! Grazie??

Grazie, adesso vivo preoccupata !!!

Si, poteva (doveva) fare prima !!

Ottimo in tutto!

Sono estremamente contento di aver partecipato a questo corso.

Ma…allora con questi PC ci possiamo solo lavorare !?! ☹

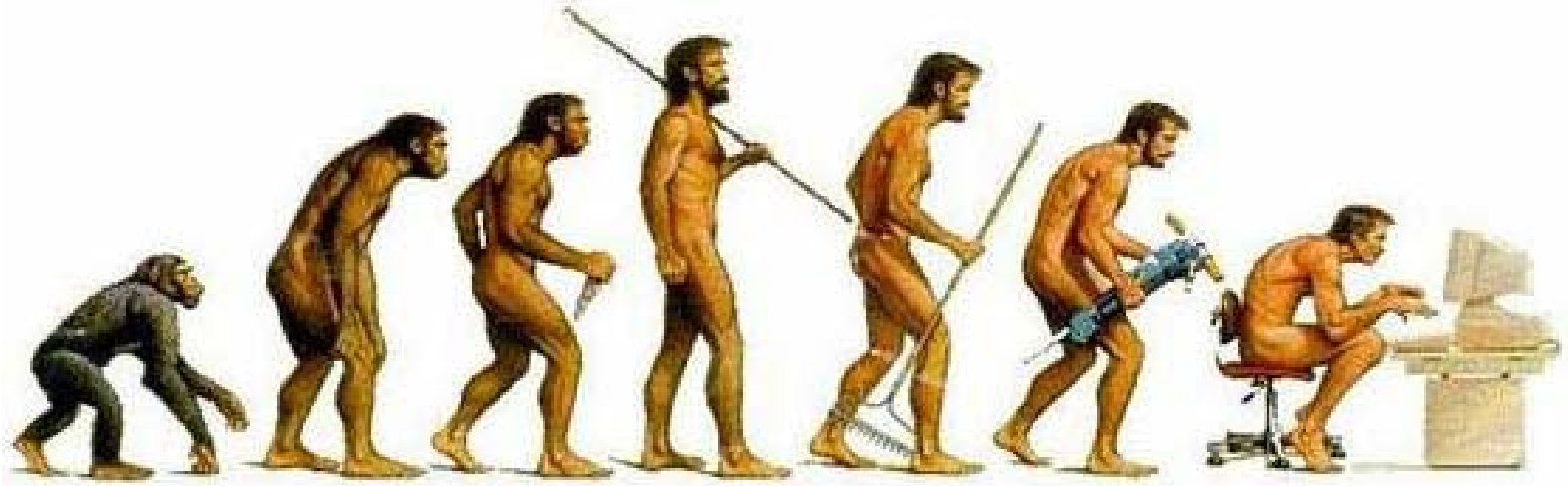
E' il più bel corso mai organizzato da questa azienda

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Evoluzione

- Completamento del programma (2010)
- Refresh e aggiornamenti annuali
- Pillole email (trimestrali)
- Inserimento nella formazione obbligatoria aziendale
- Riproduzione in EMEA



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Un caso reale

Risultati

- Personale formato su SOX
- Personale formato su rischi IT

…per questi motivi ma…

- Personale formato su 231/01 e 196/03

…pagato anche con questi soldi (budget)…

- Diminuzione delle chiamate al SD del 28%
- Riduzione consumo di banda del 60 %

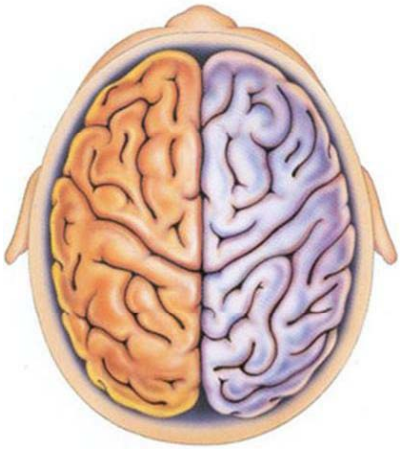
…e ha prodotto questo ROI !!

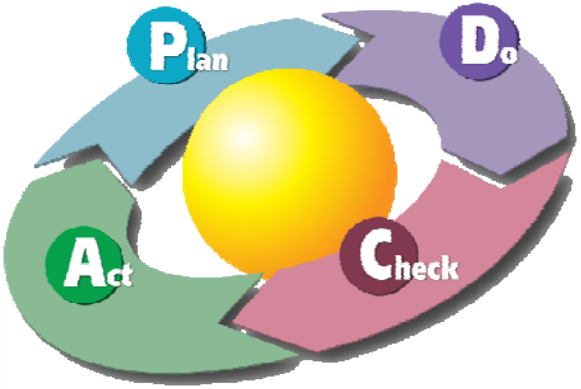
- Cambiamento percezione IT dept

Questo progetto è stato realizzato…

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Concludendo

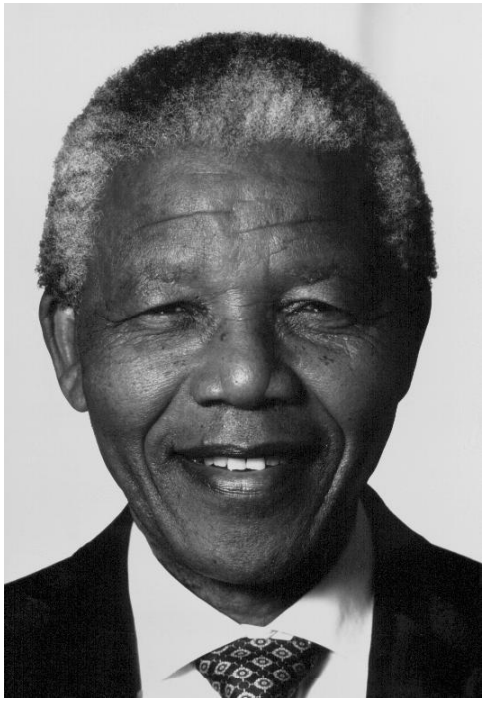




"L'istruzione e la formazione sono le armi più potenti che si possono utilizzare per cambiare il mondo“

Nelson Mandela

(Premio Nobel per la pace)



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Q & A

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Carlo Rossi

Mob.+39.392.976.7699

Fax. +39.06.6227.5039

Skype: crlrss

carlo.rossi@crconsultingnet.it

carlo.rossi@5i.co.uk

c.rossi@isacaroma.it

carlorossi@nasaga.org

crconsultingnet.typepad.com

www.crconsultingnet.it

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Sitografia

- www.crconsultingnet.it
- crconsultingnet.typepad.com
- www.rankopedia.org
- ocw.mit.edu
- www.technicallyfunny.com
- www.ted.com
- www.youtube.com
  - Neurons-How they work-Human Brain
  - The Frinky Science of Human Mind
  - Risk: The Neural Basis of Decision Making
  - How it feels to have a stroke
- http://www.mindbodypsychotherapy.net/mbconnection.htm

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Bibliografia

The Back of the Napkin – *Dan Roam*

The art of intrusion – *Kevin D. Mitnick*

The art of deception – *Kevin D. Mitnick*

Blink - *Malcolm Gladwell*

Buy-ology – *Martin Lindstrom*

Security Metrics – *Andrew Jaquith*

The Human side of managing technological innovation – *Ralph Katz*

Your brain is [almost] perfect – *Read montague*

Hackers handbook 3.0 – *Dr.K*