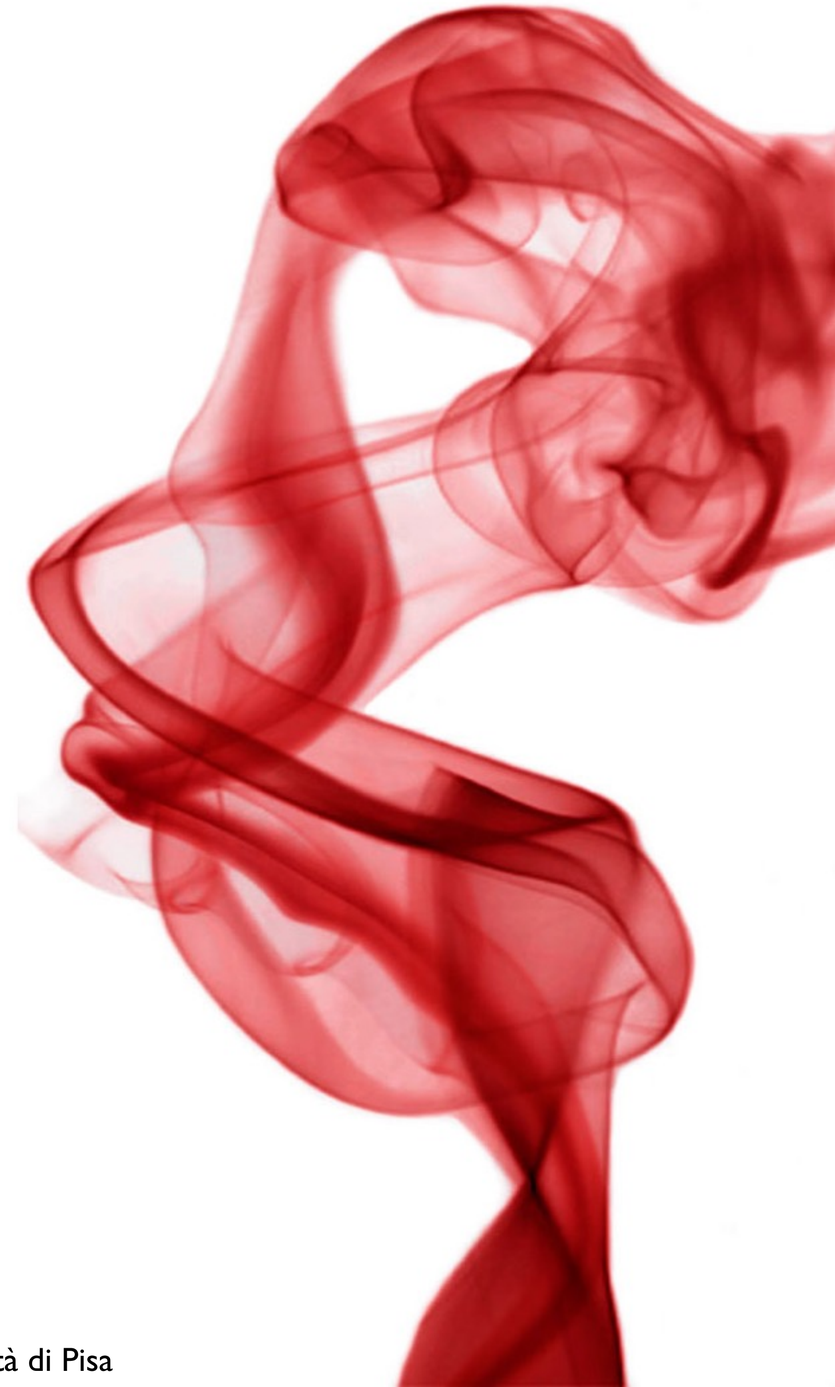
Giuseppe Augiero - E-Privacy XIX (2016)

PRIVACY E CAPTATORI: ERRORI E ORRORI TRA SILENZI E SEZIONI UNITE.



CHI SONO...

- Esperto di sicurezza informatica.
- Membro attivo della comunità Open Source.
- Relatore a numerosi convegni e seminari del mondo dell'ICT.
- Entusiasta della Computer Forensic.

GIUSEPPE AUGIERO

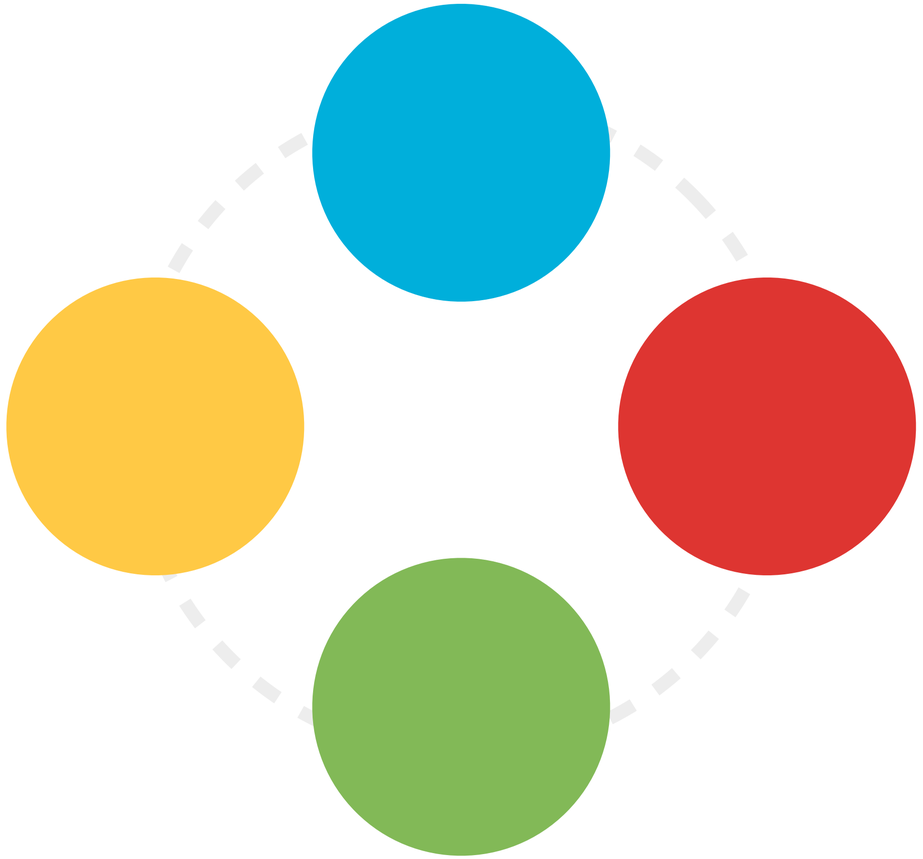
"I miei speech creano dipendenza."

PRIVACY

PRIVACY

DEFINIZIONE

"The right of individuals **to be left alone** and to be protected against physical or psychological invasion or the misuse of their property.
It includes freedom from intrusion or invasion into one's private affairs, the right **to maintain control over certain personal information**, and the freedom to act without outside interference." (1997)

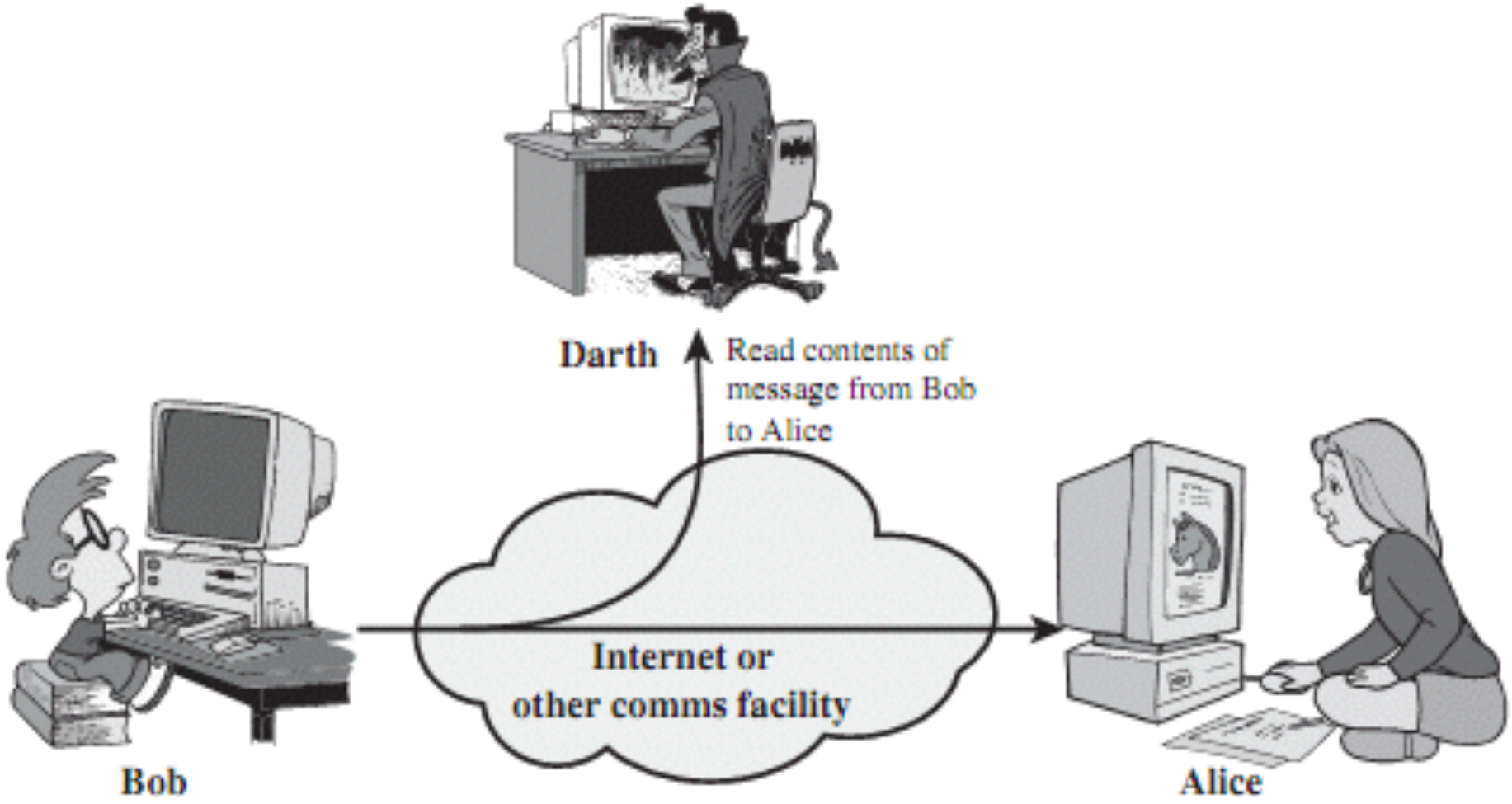


PRIVACY

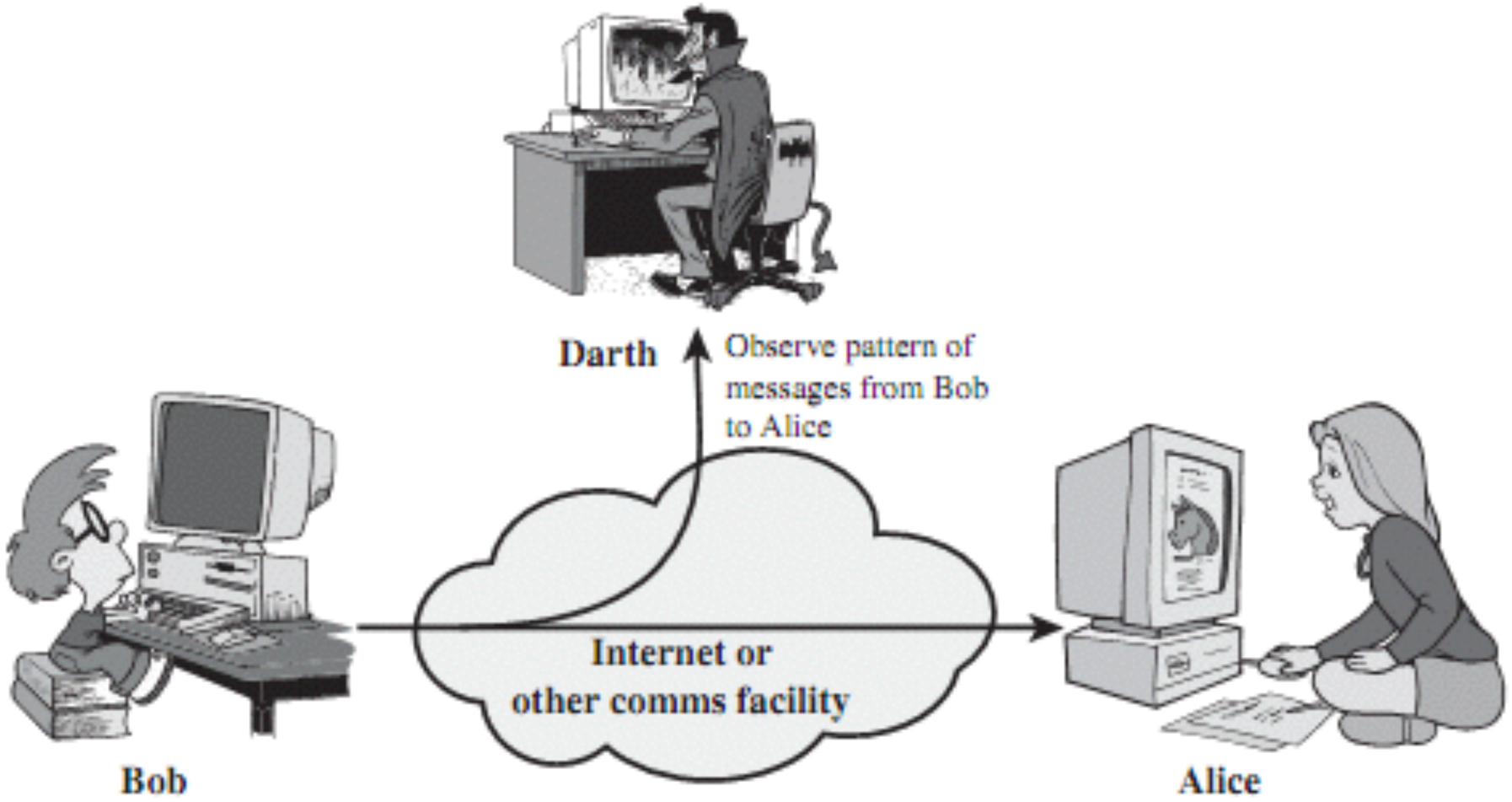
EVOLUZIONE O REGRESSIONE?

- La **tecnologia**, se usata male, non è amica della **privacy**.
- Un numero elevato di **protocolli** che usiamo non nascono con l'intento di "**offrire sicurezza**".
- Il nostro **io digitale** va tutelato.

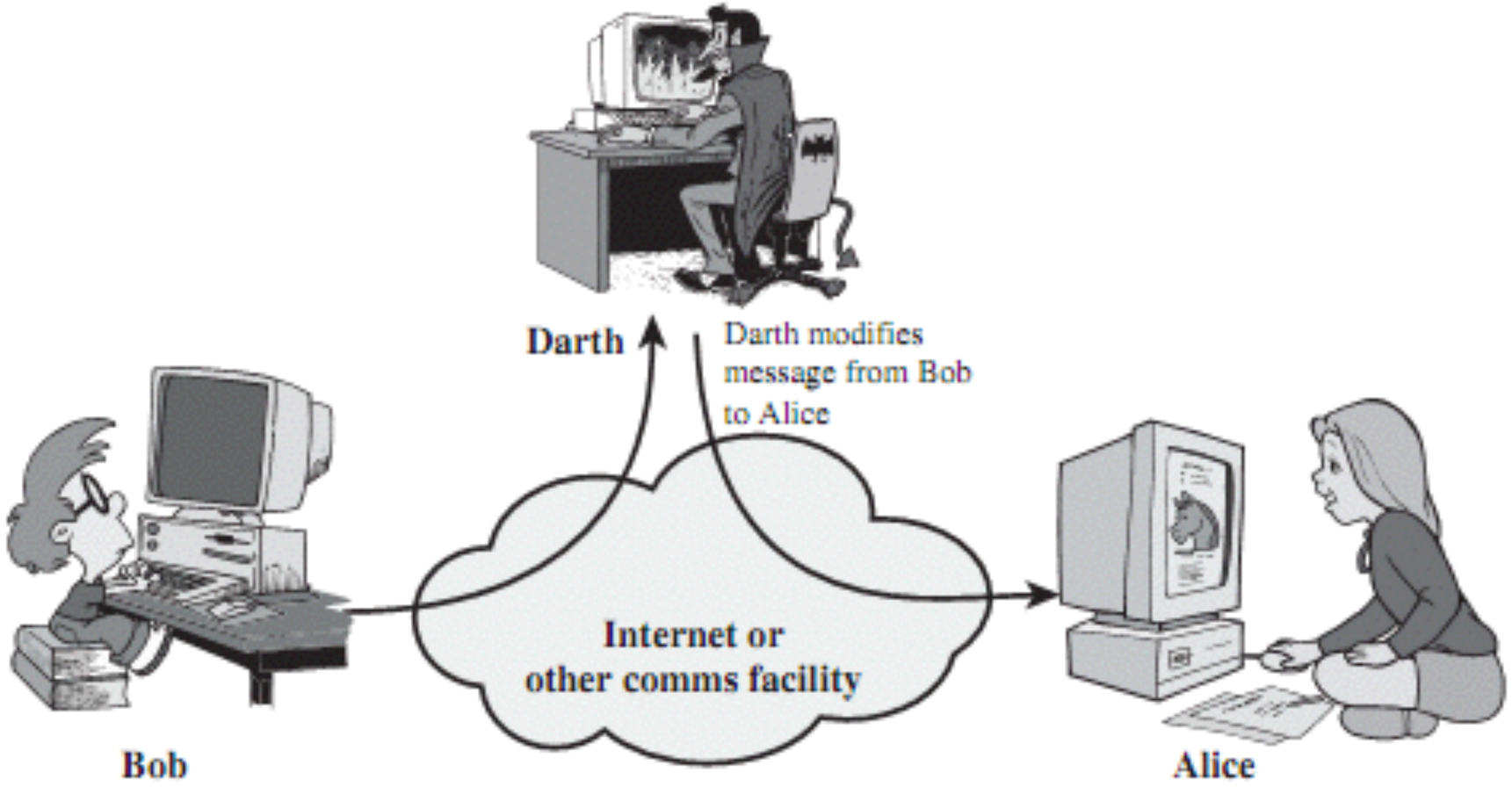
INTERCETTAZIONE DEL TRAFFICO



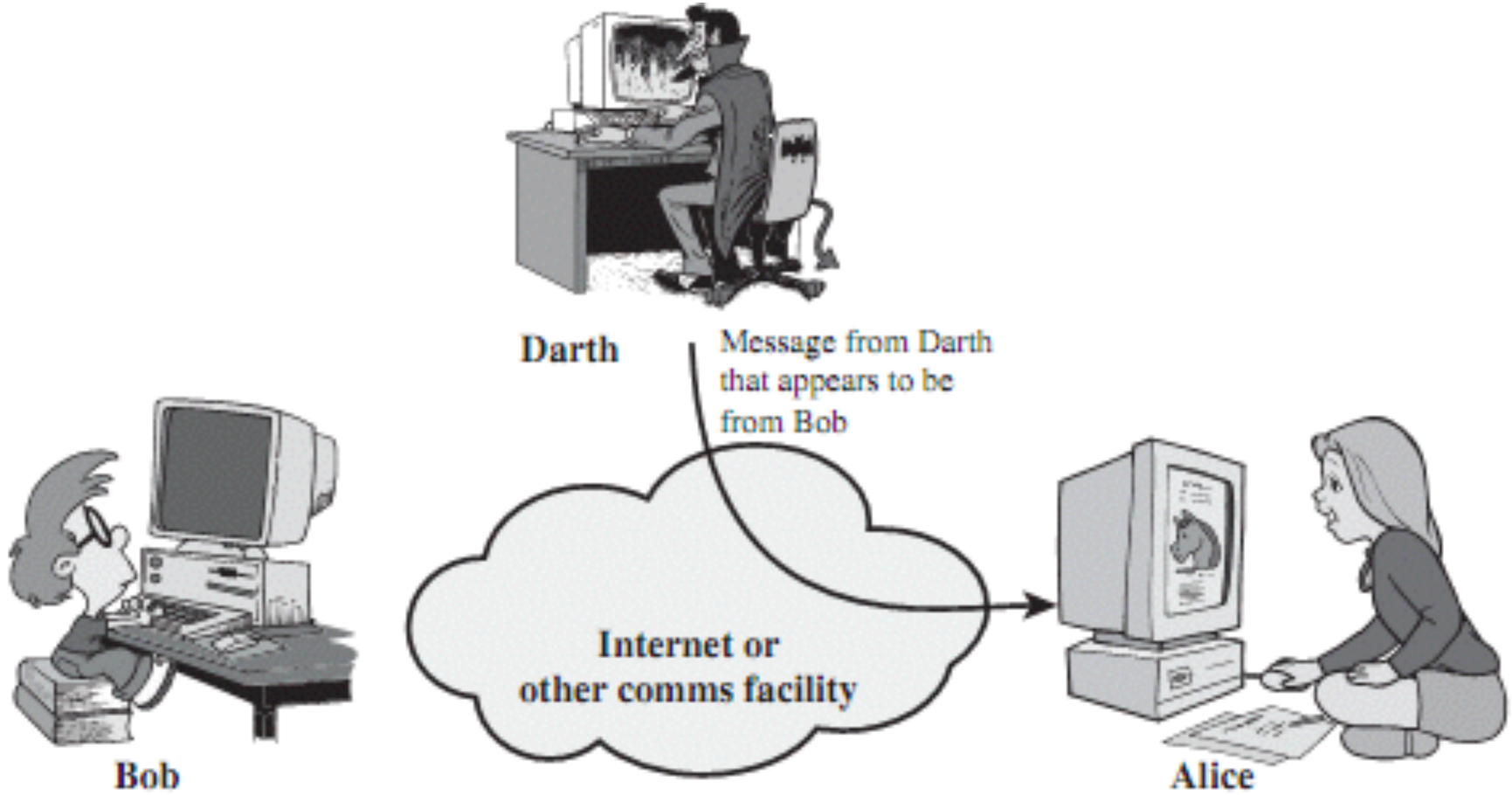
ANALISI DEL TRAFFICO



MAN IN THE MIDDLE



SPOOFING


Darth
Message from Darth
that appears to be
from Bob
Internet or
other comms facility
Bob
Alice

COME EVITARE?

PRINCIPI DI BASE DI SECURITY

- Confidenzialità.
- Integrità.
- Autenticazione.
- Non ripudio.

COME EVITARE? (II)

CONSAPEVOLEZZA

- Maggiore consapevolezza.
- Farsi consigliare dalle persone giuste.
- Comprendere il valore dei propri dati.

CAPTATORI INFORMATICI

BUONI O CATTIVI?

LE 2 FACCE DELLA STESSA MEDAGLIA

- Garantendo privacy e anonimato diventa più difficile qualsiasi operazione di investigazione.

- Analizzare il traffico cifrato di un indagato potrebbe essere una operazione molto complessa (ma non impossibile).

CAPTATORI (I)

IL SOFTWARE

- Attraverso un captatore informatico è possibile "intercettare" il traffico direttamente alla fonte prima che esso venga cifrato o protetto.
- **E' un applicativo software che viene introdotto, in maniera nascosta, in un sistema informatico.**

CAPTATORI (II)

COMPONENTI

- Due sono i componenti principali:
  - Elemento che permette l'intrusione e l'installazione del software residenze sul dispositivo informatico.
  - Captatore vero e proprio.

- **Veri gioielli tecnologici.**

CAPTATORI (III)

CHI LI PRODUCE

- Possiamo pensare che il "prodotto finale" sia il risultato di più mani e di più aziende.
- Lo Zero Day viene quasi sempre acquistato da una azienda esterna.
- L'azienda produttrice non conosce il target.

CAPTATORI (IV)

CHI LI USA (O NE ABUSA)?

- Intelligence.
- Forze di polizia.
- Agenzie investigative.

- Anche i “cattivi” hanno iniziato a usare dei particolari captatori.

- Qualcosa si inizia a trovare in vendita sul deep web.

CAPTATORI (V)

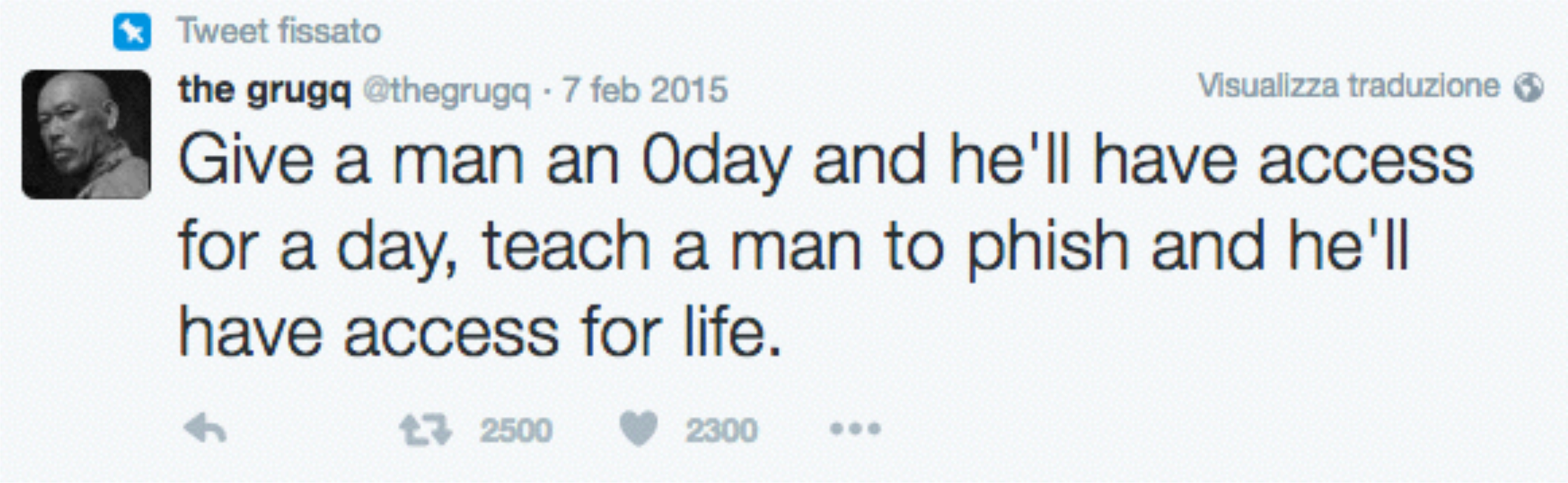
COME DIFENDERCI

- Utilizzare soluzioni sicure e aggiornate.
- Diversificare.
- Non installare di tutto e di più.
- Dati riservati offline.
- No Cloud.
- No Iot.
- Avere senso critico.
- Consapevolezza.

SIAMO AL SICURO?

PHISHING

IL SAGGIO DICE:



AEROPORTI

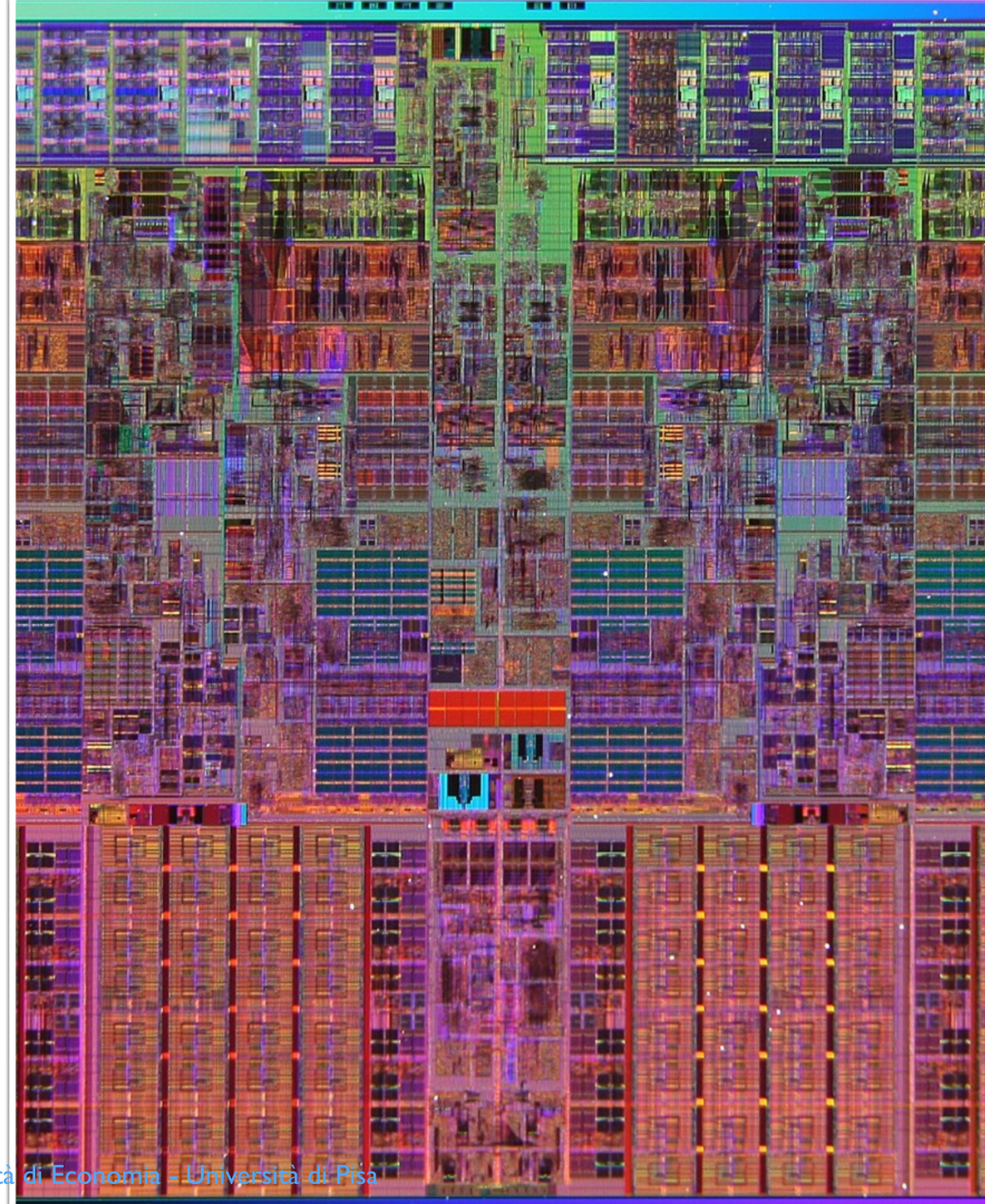
RICARICHE USB

- Quando collegate il vostro telefono a una stazione di ricarica usb, esso invia il “proprio nome”, il modello e il numero di serie.
- E’possibile compromettere il cellulare.
- E’ possibile sottrarre dati.

PROCESSORI INTEL

RING -3

- Intel Management Engine (ME) è un sottosistema composto da uno speciale microprocessore ARC a 32 bit che è fisicamente ubicato all'interno del chipset.
- Il firmware in esecuzione sul ME implementa un sistema denominato Active Management Technology.
- E' del tutto trasparente al sistema operativo e non è disattivabile.

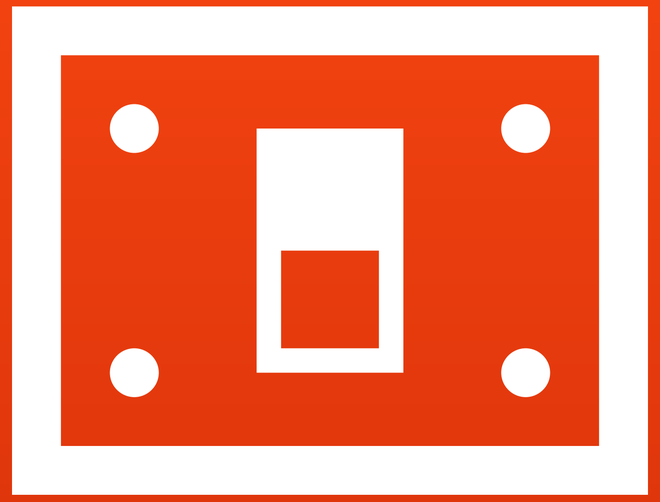


CREDENZIALI

MAI FIDARSI

- Nelle ultime settimane abbiamo potuto assistere a due grandi furti di credenziali:
  - LinkedIn.
  - TeamViewer.

- **Mai usare la stessa password.**

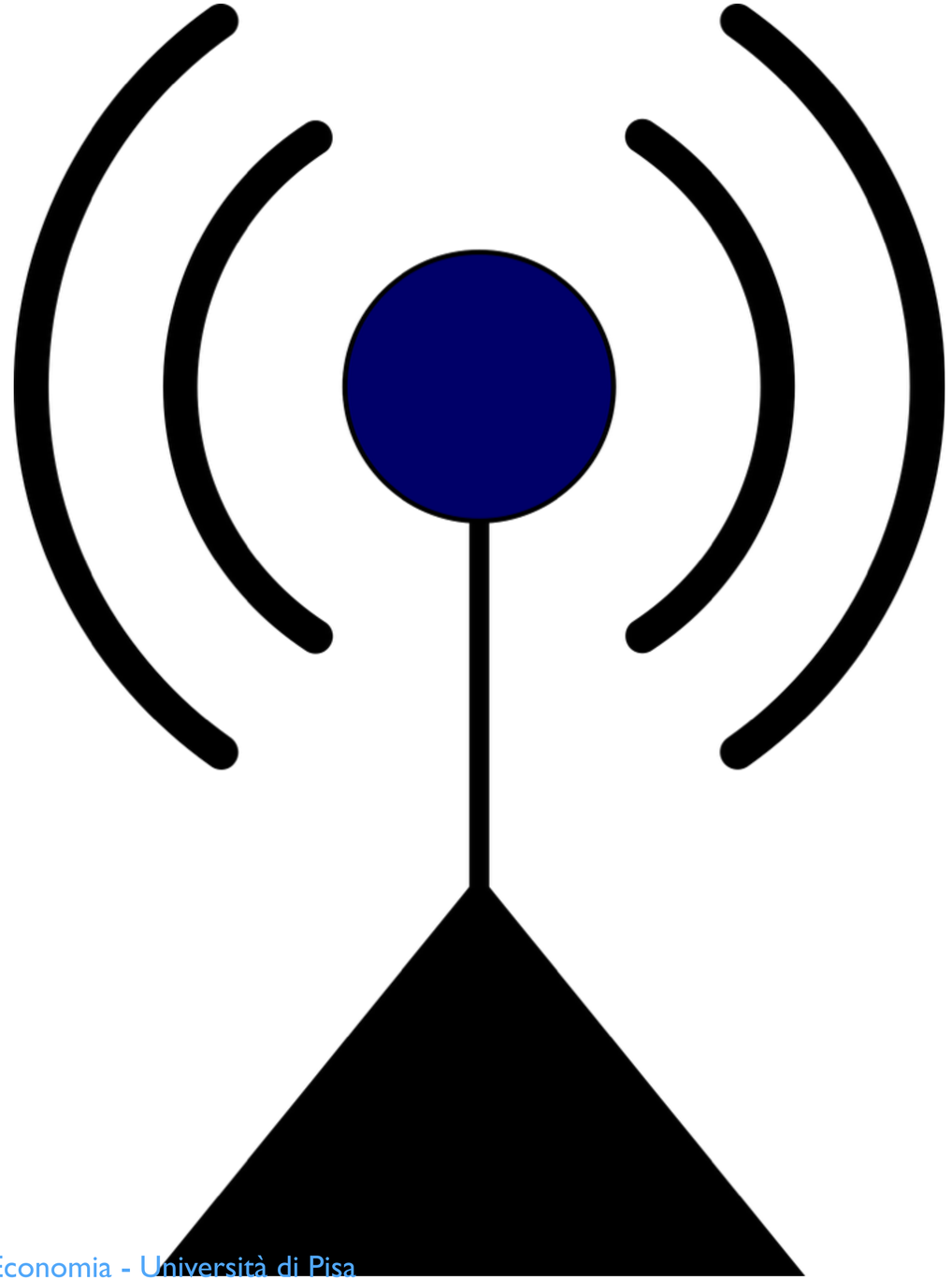


L’ESPERIMENTO

ACCESS POINT

ROGUE AP

- E’ stato accesso un access point che non richiedeva credenziali per l’accesso alla rete.
- Il sistema ha lavorato utilizzando una batteria.
- E’ possibile usare un semplice pc e utilizzare dei wizard automatici.



LAYOUT

NO ACCESSO A INTERNET

NO CREDENZIALI

NO CATTURA TRAFFICO

NO SALVATAGGIO DATI

NO MANOMISSIONE

NO SPOOFING

CAPABILITIES

TRAFFICO DI RETE

Possibilità, da parte di un utente malintenzionato, di catturare e analizzare il traffico di rete.

CREDENZIALI

Possibilità, da parte di un utente malintenzionato, di sottratte credenziali di accesso.

MANOMISSIONE

Possibilità, da parte di un utente malintenzionato, di modificare il traffico in uscita.

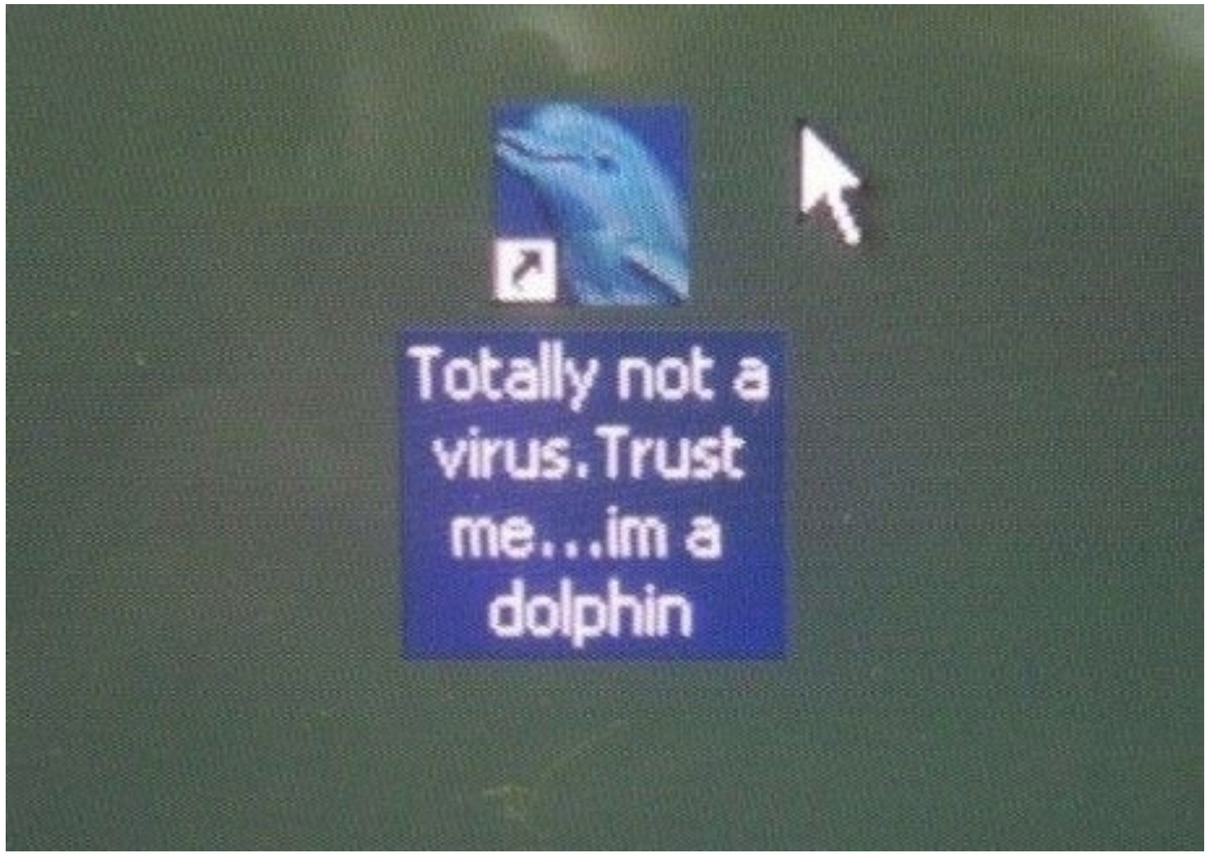
CAPTATORE

Possibilità (molto complessa), da parte di un utente malintenzionato, di infilare nel dispositivo dell'utente un captatore.

Esperimento da non ripetere!

IN CONCLUSIONE

TRUST



TUTTO RUOTA INTORNO

AL CONCETTO DI

FIDUCIA

CYBER WARFARE

PRIVACY

OCCORRE ESSERE PROATTIVI

- Non basta una legge o l'acquisto di un firewall o un ids per sentirsi al sicuro e per aver garantita la propria privacy.

TECNOLOGIA

- Non esiste una tecnologia buona o cattiva.
- Dipende dal contesto e dall'uso.

IT SECURITY

- Familiarizzare con la sicurezza informatica permette di riconoscere meglio le minacce.

VALORE DEI DATI

- **Garantire la privacy è un diritto fondamentale.**

GRAZIE !!!

CONTATTI:

EMAIL: TALK AT AUGIERO DOT IT

TWITTER: @GIUSEPPEAUGIERO

WWW.AUGIERO.IT

Giuseppe Augiero - E-Privacy XIX (2016)

PRIVACY E CAPTATORI: ERRORI E ORRORI TRA SILENZI E SEZIONI UNITE.