Sicurezza informatica e responsabilità sociale, l'importanza della consapevolezza

Andrea Zwirner


andrea@linkspirit.it


@AndreaZwirner

Chi sono

- Mi interesso di sicurezza informatica dallo scorso millennio
  - “Connettere” significava “intrecciare”
  - Hacker non aveva ancora alcun significato

- Ho fondato Linkspirit, azienda che si occupa di
  - Consulenza nella progettazione sicura di software e sistemi
  - Verifiche di sicurezza su software e sistemi
  - Formazione in materia di sicurezza informatica

Cosa faccio

- Partecipo a diversi progetti liberi legati la divulgazione della cultura sulla sicurezza informatica

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

www.isecom.org

Hacker Highschool
SECURITY AWARENESS FOR TEENS

www.hackerhighschool.org

Progetto scuole

www.progettoscuole.it

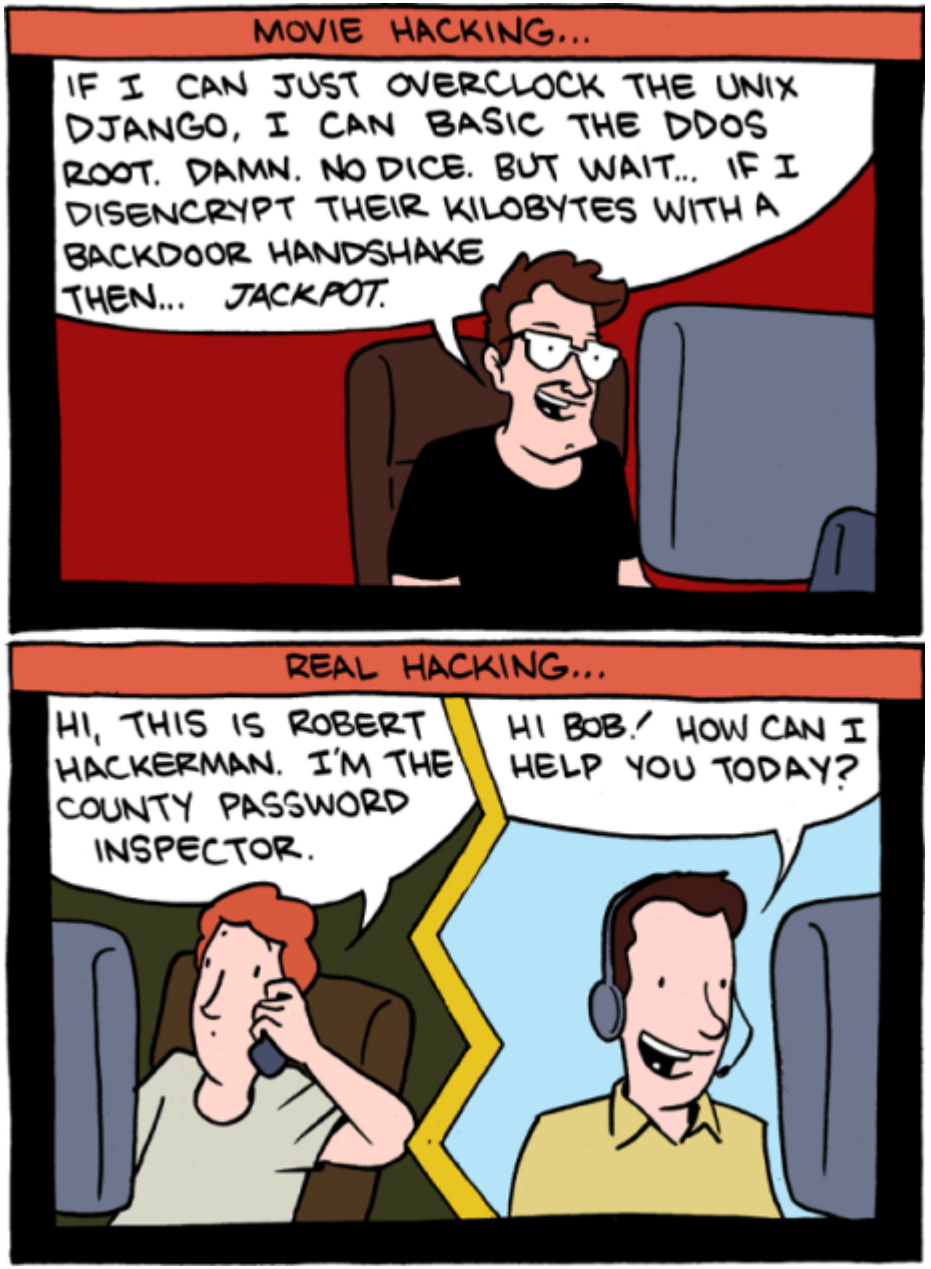
Il problema non è tecnologico, ma culturale.

Cos'è la sicurezza applicativa

- Comprende alcune questioni tecnologiche

- Consapevolezza di analisti, sviluppatori, tester, **utenti finali**
  - Sviluppo dell'architettura (secure by design)
  - Ciclo di sviluppo del software
  - Scrittura del codice
  - Controlli di sicurezza comuni nelle fasi di test / review
  - **Utilizzo consapevole da parte degli utenti finali**

Qual è l'idea da cui dobbiamo liberarci

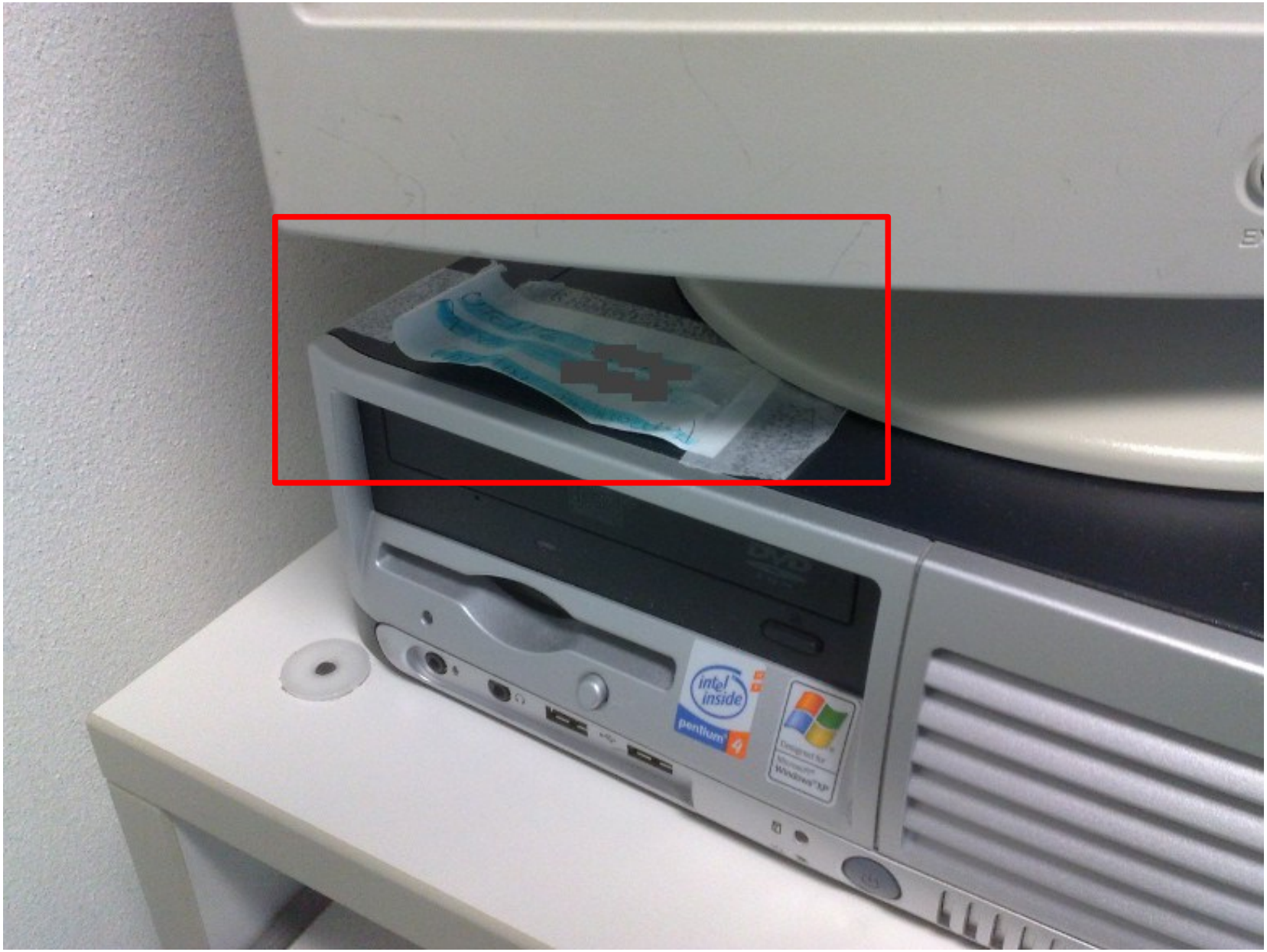


In realtà le cose vanno così

In realtà le cose vanno così

In realtà le cose vanno così

In realtà le cose vanno così



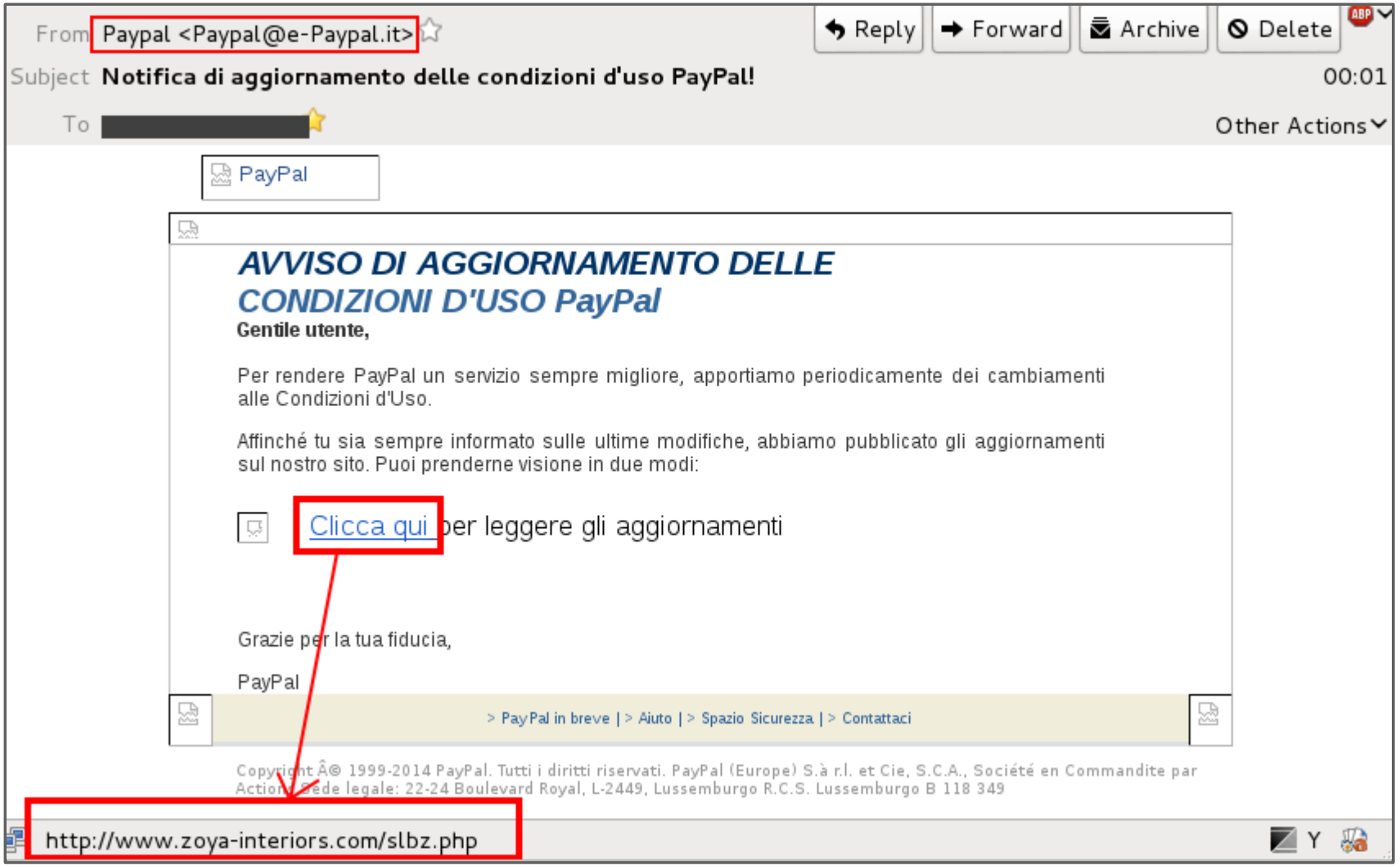
Il problema della sicurezza è culturale

- Possiamo immaginare la sicurezza come una catena composta da anelli tecnologici ed umani
- Portare a buon fine un attacco informatico significa riuscire a rompere questa catena
- Una catena è resistente quanto il suo anello più debole
- L'anello più debole della catena è la componente umana

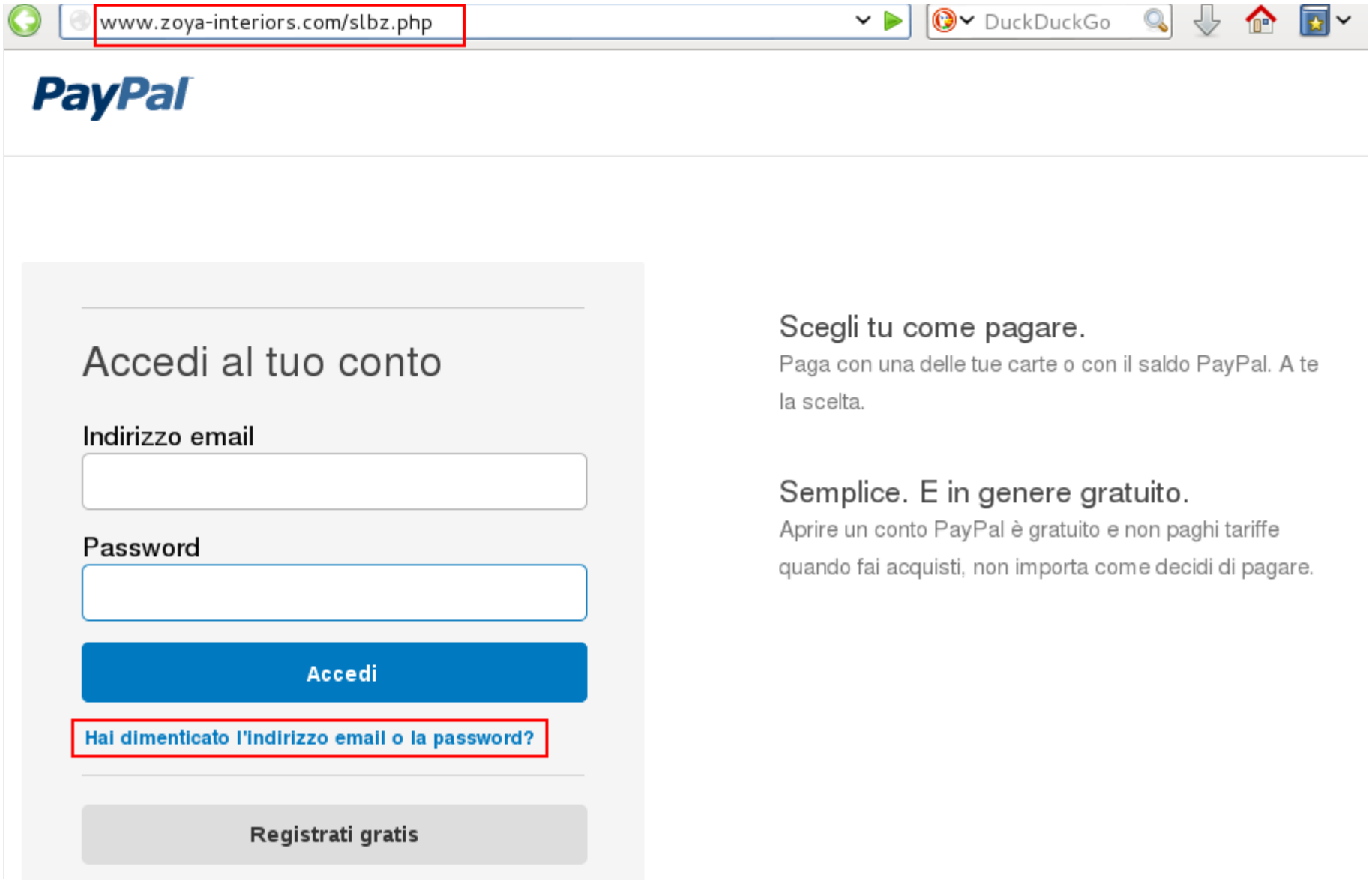
Un esempio concerto: il phishing

- Viene attuato mediante messaggi privati
- Ha il fine di far decidere all'utente di compiere un'azione
  - visitare una pagina web all'utente per e portarlo ad inserire le proprie credenziali, rubandogliele
  - eseguire un software malevolo per prendendone il controllo della sua postazione
- Il messaggio può provenire da persone (o aziende) conosciute, facendo leva sulla fiducia che l'utente ripone in queste ultime
- Fa leva sulla curiosità dell'utente

Un esempio di phishing



Un esempio di phishing



Riepilogando

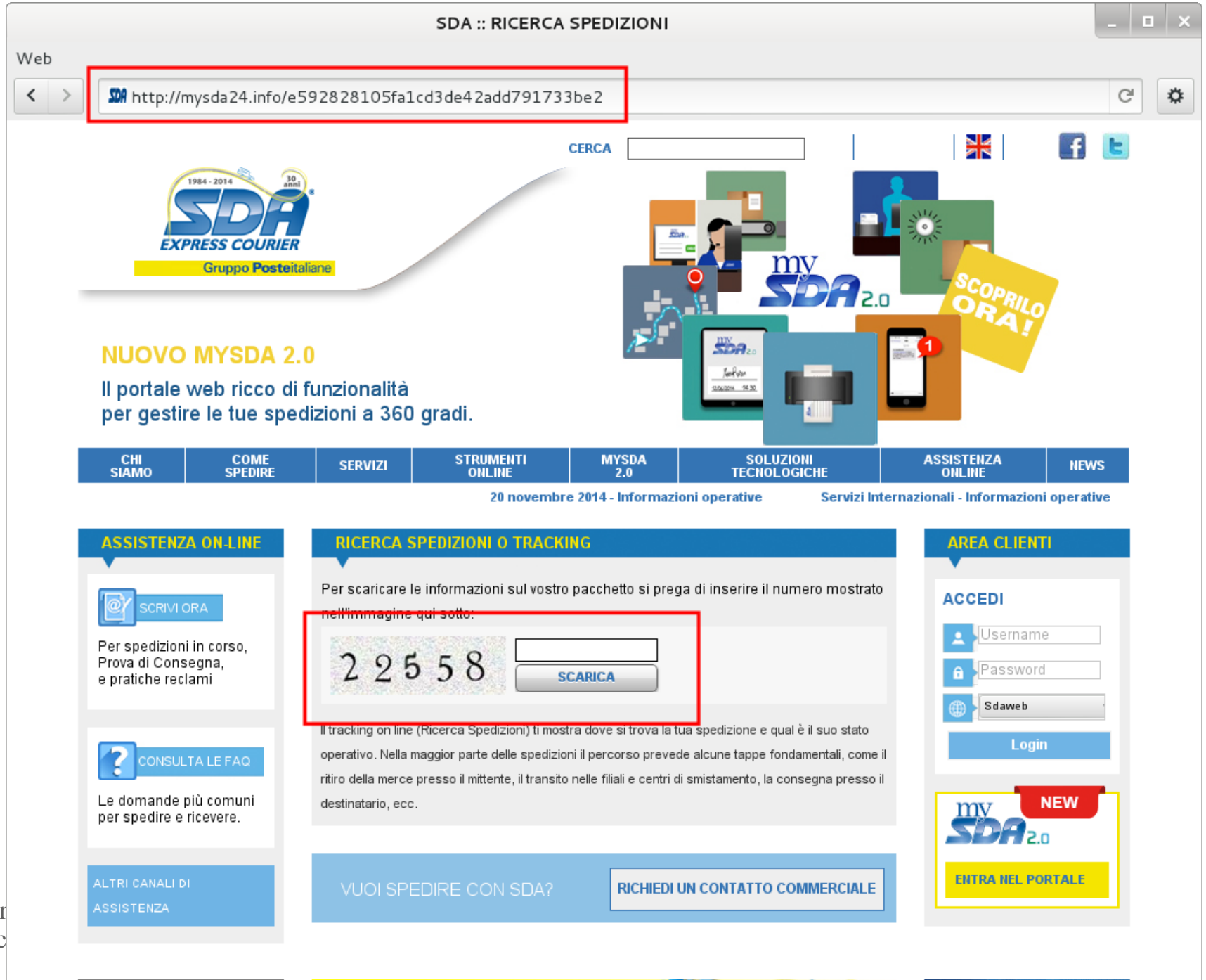
- L'utente è convogliato verso un sito che sembra quello di PayPal
- L'utente inserisce le proprie credenziali in tutta tranquillità
- Le credenziali vengono salvate, quindi l'utente ignaro dell'accaduto viene rediretto sul sito reale
- La maggior parte delle volte, l'utente non si accorge di nulla!
- L'attacco fa leva sulla mal riposta fiducia

Il caso phishing SDA

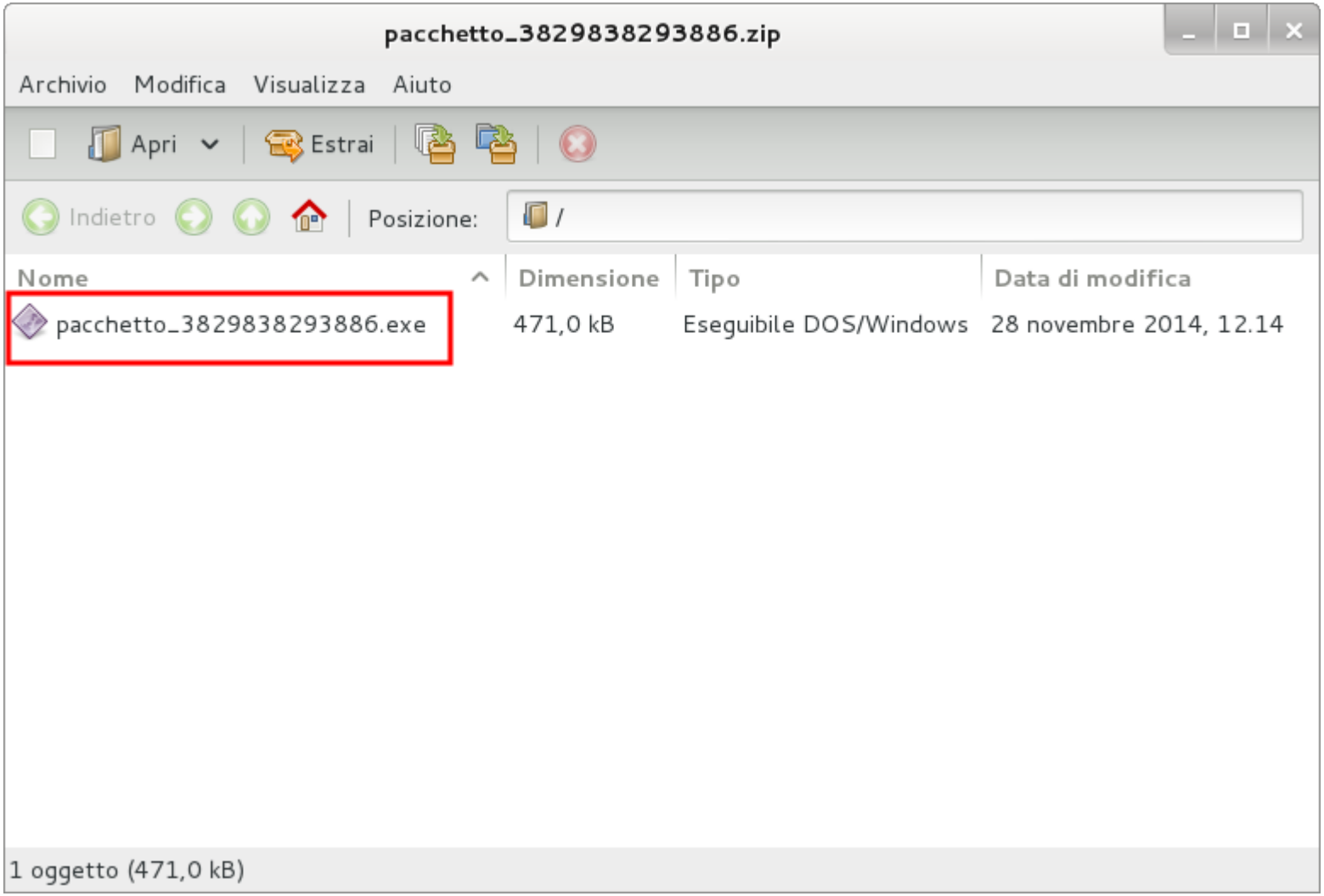
- Arriva una mail dal corriere SDA che avverte di un pacco in fermo deposito

- rimanda al sito mysda24.info per il download dei moduli per il ritiro

Il caso phishing SDA



Il caso phishing SDA

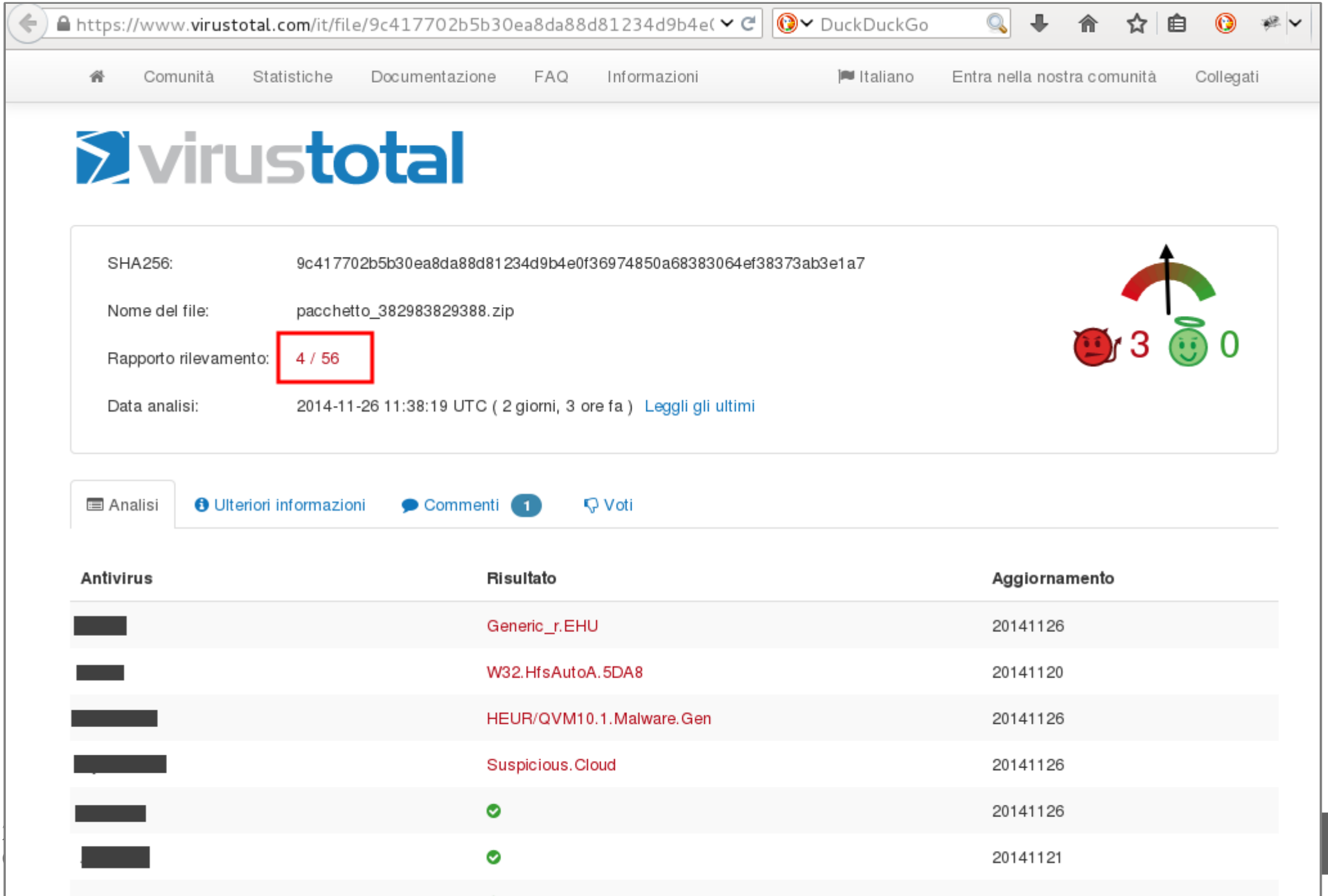


Salvagente tecnologico

- E se l'utente ha un buon antivirus installato, aggiornato e perfettamente funzionante?

Il problema non è tecnologico, ma culturale.

E se c'è un antivirus?



Gli antivirus non funzionano?

- Il modello di funzionamento degli antivirus oggi è obsoleto!

- La velocità di propagazione è troppo alta per permettere agli antivirus di essere efficaci!

Antivirus is dead!

L'effetto degli attacchi di phishing

- Primo esempio
  - Furto di credenziali d'accesso, non a scopo collezionistico

- Secondo esempio
  - Controllo totale della postazione attaccata
    - Farvi transitare operazioni illecite
    - Usarla come base per sferrare altri attacchi informatici (verso l'interno o verso l'esterno)
    - Rubare dati aziendali
    - Rubare dati personali ed identità

Cosa fare con un identità rubata?

- Riciclare denaro sporco mediante il gioco on-line
  - Bastano due codici fiscali: uno perde l'altro vince!
  - Ma chi perde, i soldi dove li ha presi?

- Effettuare furti, ricatti, estorsioni,
  - ai danni dell'utente
  - ai danni di terzi

- La vittima spesso si trova imputata di reati compiuti a suo nome!

Furto di identità

Il problema è culturale

- Perché gli attacchi visti vanno a buon fine?
- Perché gli utenti ripongono la loro fiducia nell'attaccante?
  - Perché si trovano in un luogo familiare e confortevole
  - Perché non conoscono i rischi cui sono esposti
  - Perché non sanno quanto sia facile portare a termine un attacco verso di loro e quanto gravi possano essere gli impatti

La responsabilità sociale

- L'interconnessione globale facilita
  - l'informazione
  - le comunicazioni private e d'impresa
  - la proliferazione di software malevolo

La responsabilità sociale

- Ogni volta che mi metto a rischio su Internet, metto a rischio tutte le persone che mi sono vicine
- Come posso evitare di mettermi a rischio se non sono consapevole di quali siano i rischi?
- La consapevolezza dei rischi di Internet è una questione di responsabilità sociale

Il rischio per le PMI

- Tutti gli impiegati hanno accesso ad un computer
- Tutti i computer sono collegati ad Internet
- Tutti gli impiegati rivestono tutte le mansioni (o quasi)

Il rischio per le PMI

- Nessun impiegato ha una preparazione adeguata ad affrontare le tematiche di sicurezza

- Cosa succede se
  - Serve un “programmino” per...
  - Si trova una chiavetta USB nel parcheggio?
  - In casella c'è un avviso di “pacco in fermo deposito”?
  - Arriva via email una “fattura da pagare”?
  - …

Il rischio per le PMI

- Le PMI costituiscono la maggior parte dell'economia e delle industrie europee e contribuiscono fino all'80% all'occupazione di alcuni settori industriali.

- La consapevolezza dei rischi Internet da parte degli utenti finali diventa una questione fondamentale per proteggerle

Il rischio per le PMI

- Le PMI costituiscono la maggior parte dell'economia e delle industrie europee e contribuiscono fino all'80% all'occupazione di alcuni settori industriali.

- La consapevolezza dei rischi Internet da parte degli utenti finali diventa una questione fondamentale per proteggerle

- Spesso le grandi imprese ereditano molte delle problematiche delle PMI...

La strategia europea

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE OF THE
EUROPEAN UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

Consapevolezza

Se non si coinvolgono gli utenti, ogni sforzo è vano

"*Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.*"

Cybersecurity Strategy of the European Union

Commissione europea, febbraio 2013

La strategia italiana

Consapevolezza

"[…] *al fine di rafforzare le capacità nazionali di prevenzione, reazione e ripristino* […] *individua come nodi primari* […]:

p*romozione e diffusione della cultura della sicurezza cibernetica sia tra i cittadini che all'interno delle istituzioni [...] al fine di accrescere il livello di consapevolezza e di conoscenza della minaccia e dei relativi rischi*"

Quadro strategico nazionale per la sicurezza dello spazio cibernetico

Presidenza del Consiglio dei Ministri, dicembre 2013

Quindi, cosa dobbiamo fare?

- Il problema è … ?

Quindi, cosa dobbiamo fare?

- Il problema è **culturale** !
- Dobbiamo attivarci per arricchire la nostra base culturale
- E' essenziale che la consapevolezza dei rischi di Internet diventi parte della nostra cultura, sia personale che d'impresa

Quindi, cosa dobbiamo fare?

- Come?

Grazie per l'attenzione.

Sicurezza informatica e responsabilità sociale, l'importanza della consapevolezza

Andrea Zwirner

andrea@linkspirit.it

@AndreaZwirner