Corso di Sicurezza – A.A. 2006/07

Attacchi login spoofing, phishing, sniffing, keyloggers

Giovanni Lughi
261607

17/05/2007

Spoofing (ingannare)

- Insieme di tecniche atte a mascherare una persona o un programma con finalità illegittime.
- Alcune tecniche di spoofing:
  - Man-in-the-middle attack
  - Mail Spoofing
  - URL Spoofing (vedi Phishing)
  - Ip Spoofing
  - ARP Spoofing
  - Login Spoofing
- Per la maggior parte queste tecniche sono valide perchè a vari livelli della rete manca l'autenticazione!

Mail Spoofing

Due diverse tipologie:

- Mascheramento E-mail (vedi Phishing)
- Mascheramento Allegato:
  - Cambiando il nome dell'allegato si può convincere il bersaglio ad aprirlo e l'allegato in genere contiene un virus
  - foto1.exe => foto1.jpg (funziona solo su vecchi OS)
  - foto1.exe => foto1.jpg.exe (può funzionare se la vittima ha disabilitato la visione delle estensioni)
  - L'icona di un file può essere cambiata!
  - Soluzione: non aprire allegati sospetti o provenienti da sconosciuti!

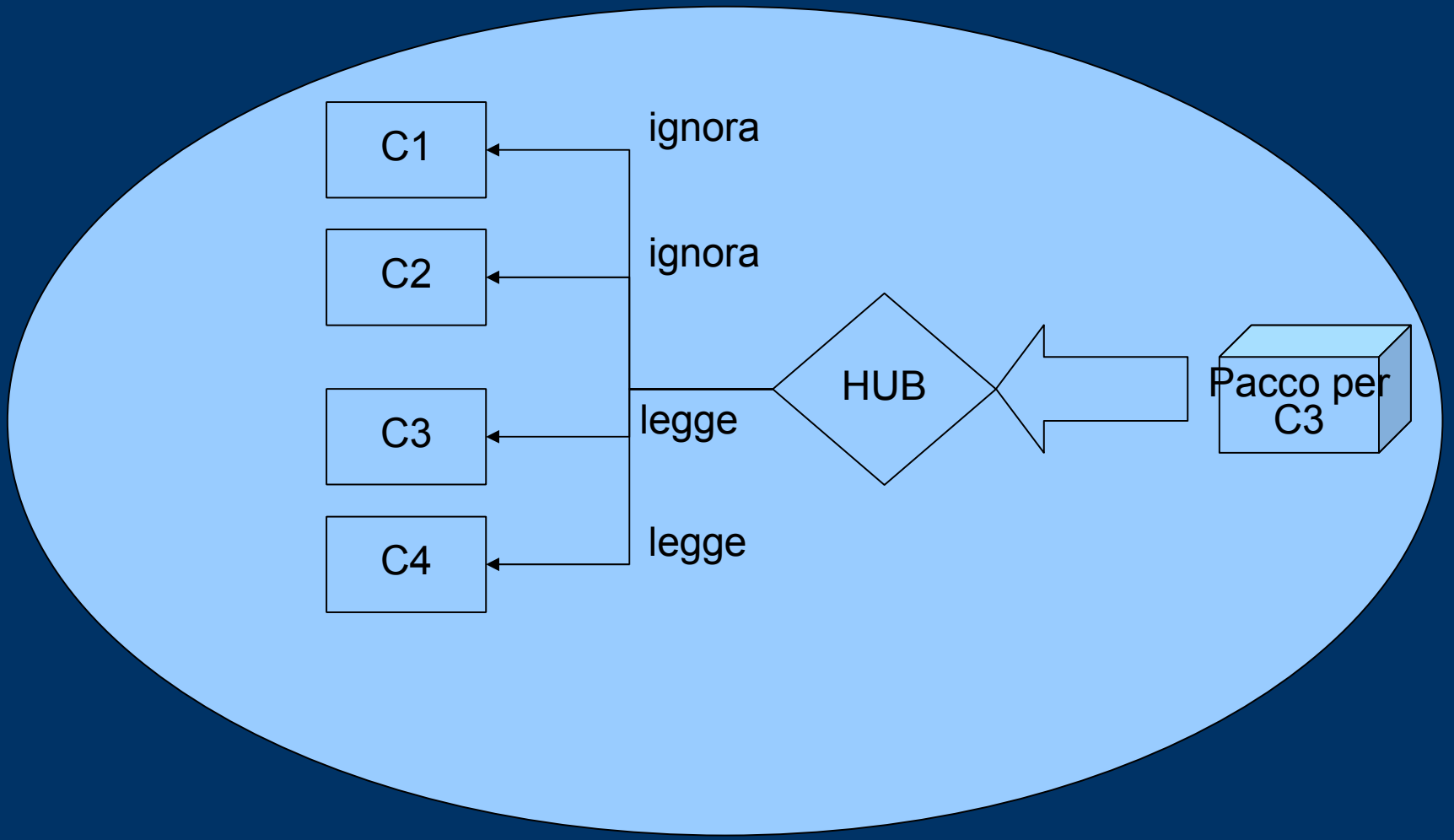
IP Spoofing

- È il più classico degli attacchi di spoofing.
- Consiste nell'inviare un pacchetto di cui si è cambiato l'IP del mittente.
- È possibile perchè nella trasmissione dei pacchetti ha importanza solo il destinatario e il mittente non è controllato.
- È facilitato dal fatto che esistano socket in cui l'IP del mittente non è letto in automatico ma può essere settato dal programmatore.
- Viene utilizzato principalmente per attacchi DoS o per guadagnare privilegi in alcune LAN.
- Soluzione: IPSec

ARP Spoofing - 1

- ARP (Address Resolution Protocol) : protocollo per il riconoscimento e diffusione dei MAC nella LAN.
- Attacco all'interno di una rete LAN.
- Usato per il MITM Attack all'interno della LAN.
- ARP non è dotato di un meccanismo di autenticazione.
- LAN con HUB:
  - L'HUB invia i pacchetti a tutta la LAN e non solo ai destinatari
  - È possibile settare una scheda ethernet in modo promiscuo e leggere tutti i pacchetti in arrivo
  - Poco attuale, gli HUB sono ormai poco usati

ARP Spoofing - 2

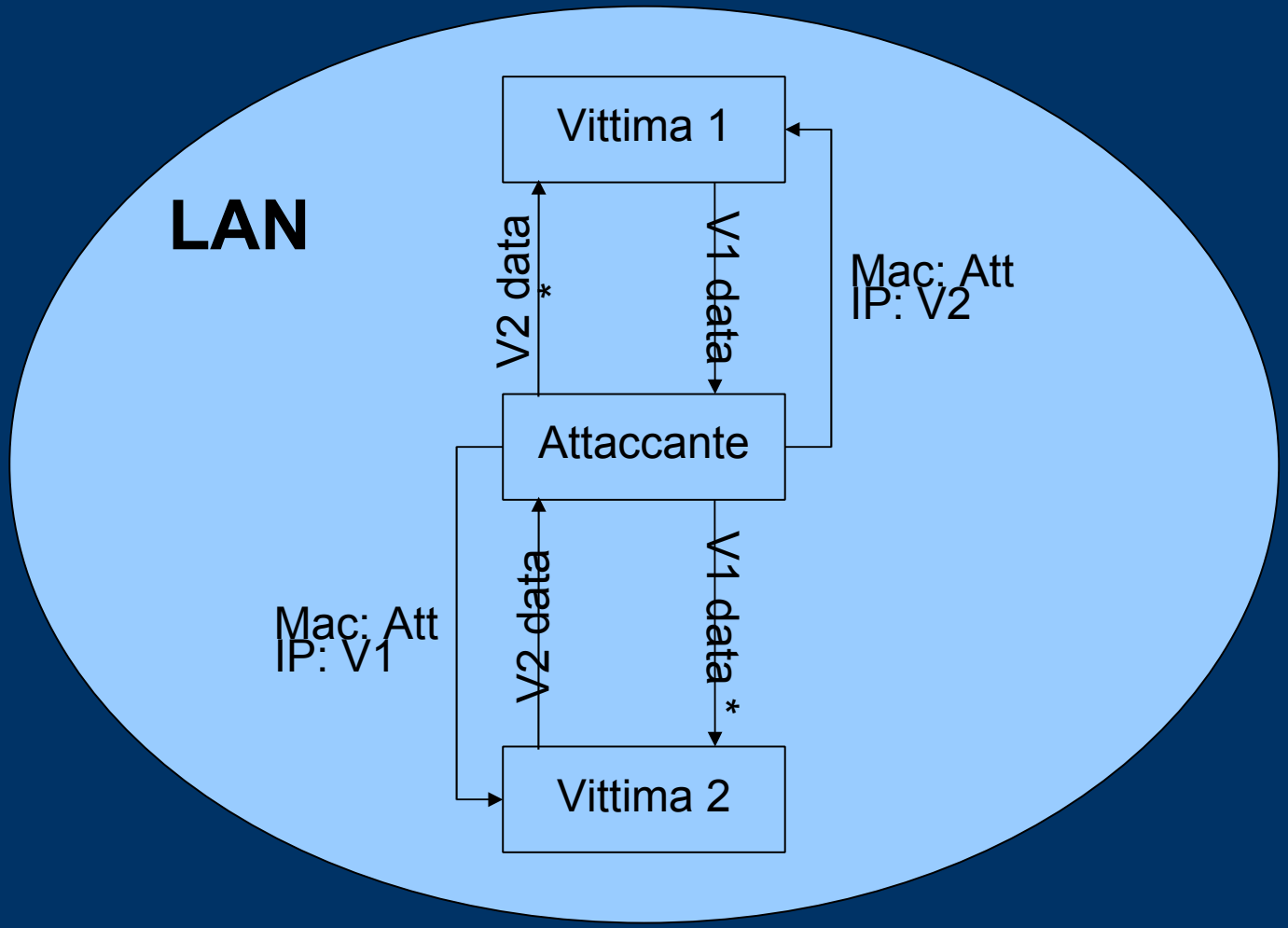


ARP Spoofing - 3

- LAN con SWITCH (ARP poisoning):
  - Lo switch invia i pacchetti solo ai destinatari quindi la tecnica precedente è inutilizzabile.
  - Le ARP cache di ogni host in rete contengono gli indirizzi IP degli altri host ed i relativi MAC
  - Ogni host fornisce il proprio IP e MAC
  - L'attacco consiste nel fornire il proprio MAC associato all'IP di una vittima, in questo modo l'IP viene riconosciuto come giusto ma i pacchetti arrivano alla nostra scheda di rete.
  - Soluzioni: IEEE 802.1x (EAP, ecc.), SARP, port security sugli switch (1 solo Mac per porta), software di analisi delle attività di rete.

ARP Spoofing - 4

- È un Man-In-The-Middle Attack!



Sniffing – 1

- Sniffing (annusare, fiutare): intercettazione dei pacchetti che transitano su una rete, può essere:
  - Legittimo = per risolvere problemi di comunicazione sulla rete o individuare tentativi di intrusione
  - Illegittimo = intercettazione di informazioni
- Se i pacchetti intercettati non sono criptati il loro contenuto sarà chiaramente leggibile, altrimenti si dovrà procedere ad un tentativo di decriptatura.
- Come per l'ARP Spoofing si hanno notevoli differenze a seconda che si operi su una Lan con con hub o switch:
  - Sniffing su hub lan = Spoofing su hub lan
  - Sniffing su switch lan = per poter intercettare i pacchetti si può operare in due modi, un'attacco MITM (come per lo spoofing) o un MAC Flooding.

MAC Flooding

- Uno Switch ha una Mac Table (Mac = Media Access Control) in cui memorizza tutti i Mac di cui è a conoscenza e le relative porte.
- Se la Mac Table è piena si procede eliminando l'indirizzo più vecchio.
- Se arriva un nuovo pacchetto per un Mac eliminato lo switch va in *fail open*, ovvero fa broadcast del pacchetto.
- Il Mac Flooding consiste nell'inviare numerosi pacchetti creati apposta, in modo da riempire la Mac Table di indirizzi falsi, così i pacchetti veri saranno inviati a tutti.
- Soluzioni: "port security" - "packet filtering" - ecc. (a seconda del produttore prende nomi diversi), queste tecniche filtrano i pacchetti secondo diversi criteri (in genere indirizzo e porta di sorgente e destinazione).

Sniffing - 2

- Lo sniffing può avvenire anche su reti più estese delle LAN.
- In questo caso si porta sempre un Man In The Middle Attack inviando false corrispondenze fra domini e Ip sfruttando la mancanza di autenticazione del sistema Dns.

- Soluzioni: cifratura (confidenzialità), software che rilevano gli sniffer su una rete (locale).

Login Spoofing

- Tecniche di spoofing usate per rubare login e password degli utenti di un sistema.
- All'utente viene presentata una finestra per l'inserimento di login e password del tutto identica a quella originale ma che in realtà memorizza i dati e li invia all'attaccante.
- Si differenzia dall'Url Spoofing in quanto lavora in locale e non su pagine web.
- Presuppone che l'attaccante sia già entrato in possesso (in modo lecito o meno) di molti poteri sulla macchina "trappola".
- Soluzione: diversi OS richiedono un Secure Attention Key, ovvero la pressione di una combinazione di tasti, prima dell'immissione di login e password (es. Ctrl-Alt-Canc).

Phishing – 1

- Attività illegale che sfrutta la Social Engineering per ottenere informazioni riservate (es. password, pin, codici carte credito).
- Phishing deriva da "fishing", inteso come il pescare dati degli utenti, o il prende all'amo gli utenti stessi.
- Tecniche di phishing e spoofing spesso corrispondono.

- Mail Phishing risolvibile con la Firma Digitale!

Phishing - 2

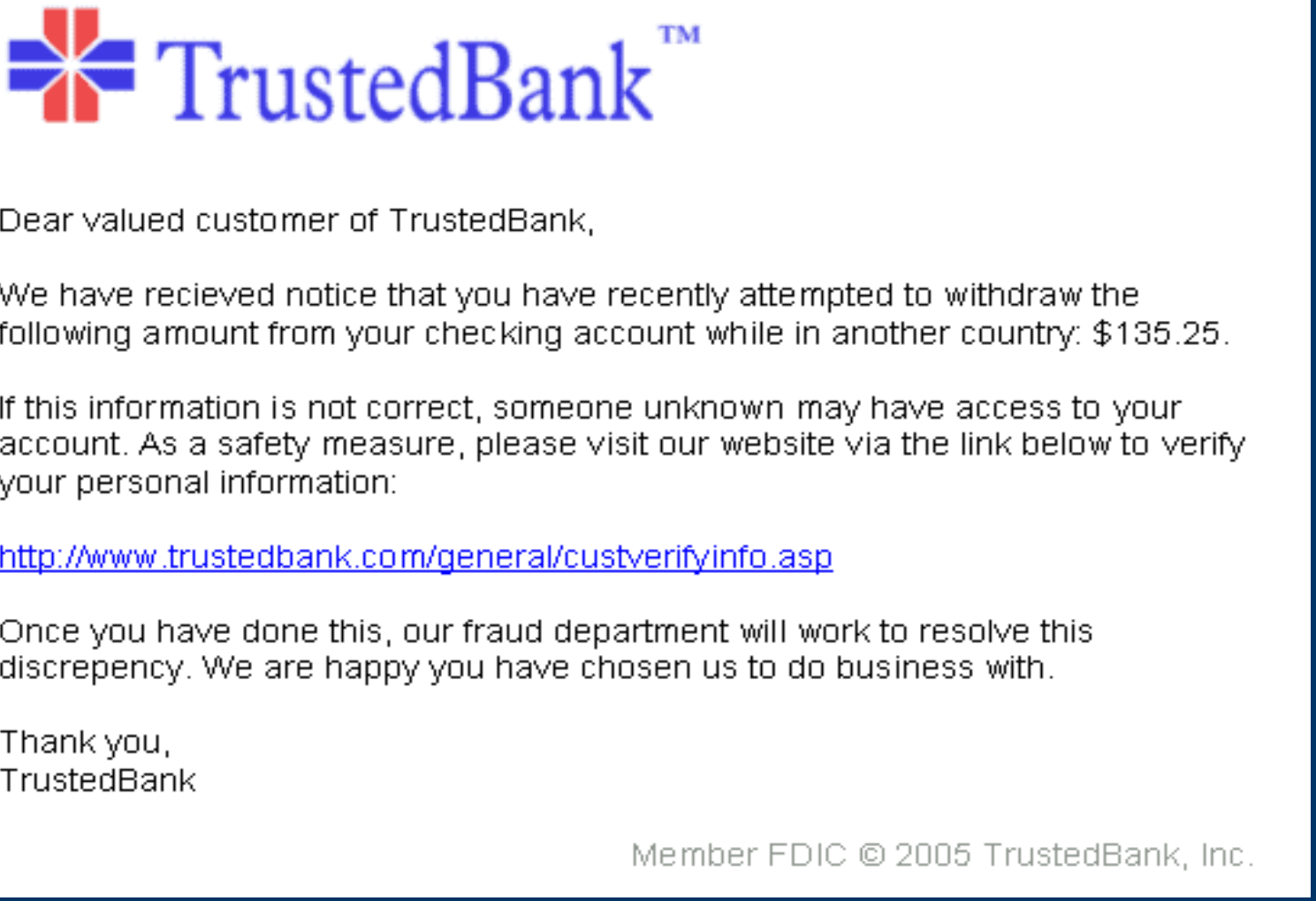
- Il phisher (chi esegue l'attacco) invia una mail alla vittima in cui finge di essere un'ente noto (es. banca, provider, eBay).
- In questa mail vengono illustrati particolari problemi (es. Scadenza account) e viene richiesto alla vittima di accedere al sito del servizio per risolvere i suddetti problemi.
- La mail contiene un link ad una pagina web falsa identica a quella originale, ma che in realtà serve solo a rubare i dati della vittima.
- Mail e pagina web saranno nella grafica e nei contenuti il più simile possibile a quelle originali per essere più credibili.
- Gli eventuali link della pagina fasulla porteranno al sito originale per non destare sospetti.

Phishing - 3

- Fondamentale è la credibilità dell'indirizzo e-mail mittente e del link presente nella mail.
- I link seguenti sembrano uguali ma portano a siti differenti:
  - www.csr.unibo.it
  - www.csr.unibo.it

- E per l'indirizzo e-mail del mittente? È quasi altrettanto facile!
- Quindi basta replicare fedelmente la grafica di mail e sito e il gioco è fatto.

Mail Fake



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

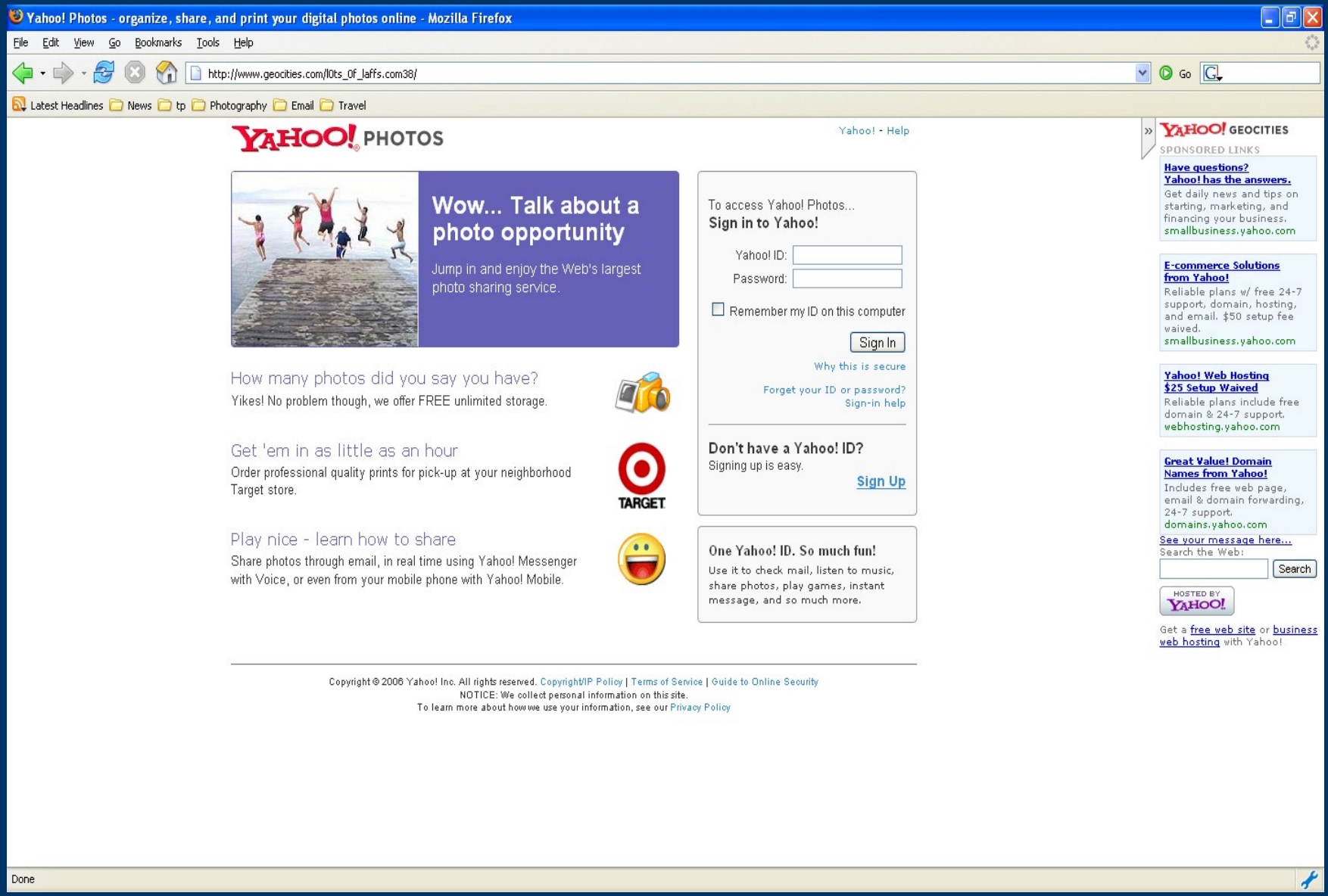
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

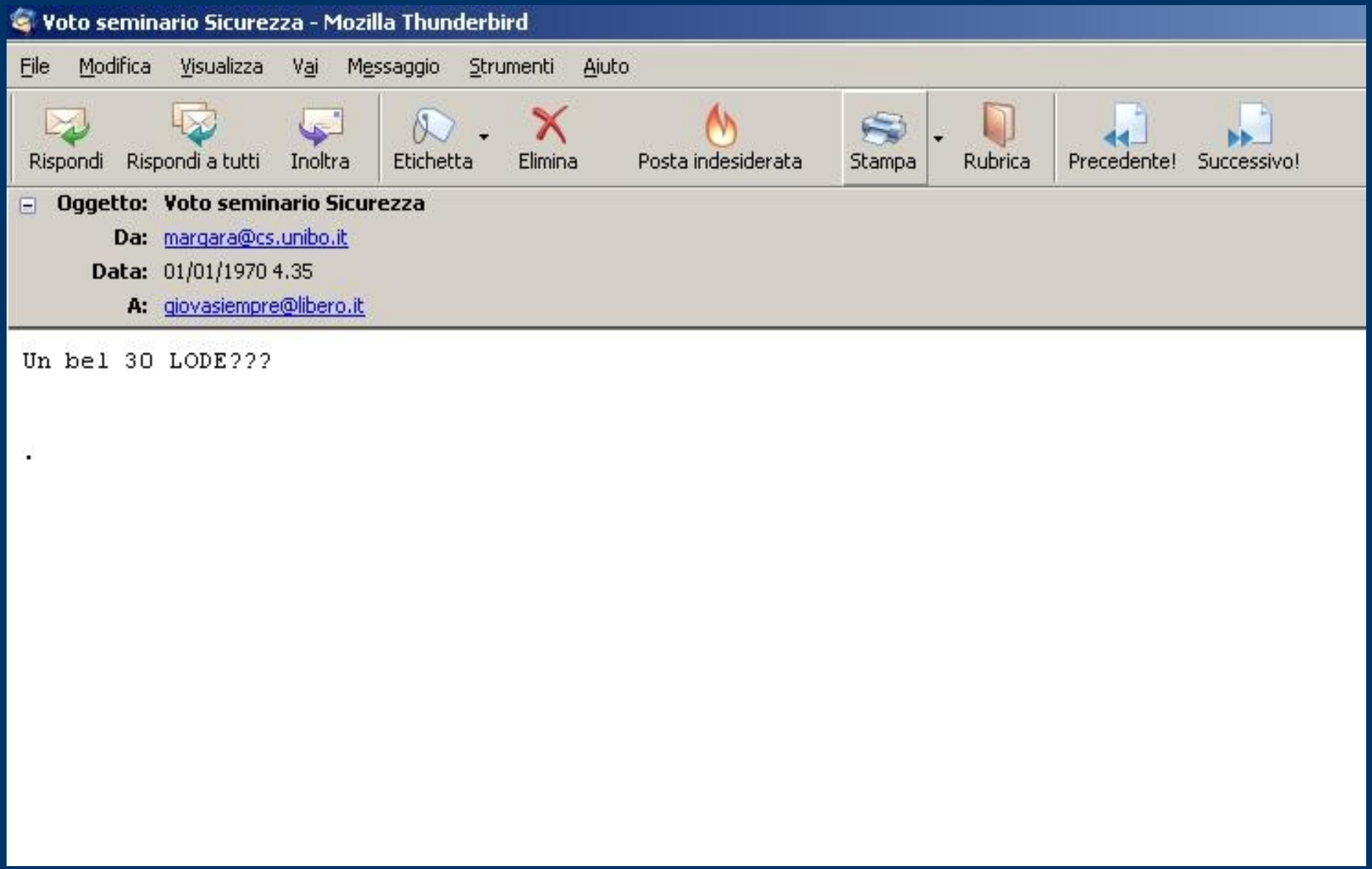
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Site Fake


Yahoo! Photos - organize, share, and print your digital photos online - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.geocities.com/l0ts_0f_laffs.com38/
Go
Latest Headlines News tp Photography Email Travel
YAHOO! PHOTOS
Yahoo! - Help
Wow... Talk about a photo opportunity
Jump in and enjoy the Web's largest photo sharing service.
How many photos did you say you have?
Yikes! No problem though, we offer FREE unlimited storage.
Get 'em in as little as an hour
Order professional quality prints for pick-up at your neighborhood Target store.
TARGET
Play nice - learn how to share
Share photos through email, in real time using Yahoo! Messenger with Voice, or even from your mobile phone with Yahoo! Mobile.
To access Yahoo! Photos...
Sign in to Yahoo!
Yahoo! ID:
Password:
Remember my ID on this computer
Sign In
Why this is secure
Forget your ID or password?
Sign-in help
Don't have a Yahoo! ID?
Signing up is easy.
Sign Up
One Yahoo! ID. So much fun!
Use it to check mail, listen to music, share photos, play games, instant message, and so much more.
YAHOO! GEOCITIES
SPONSORED LINKS
Have questions? Yahoo! has the answers.
Get daily news and tips on starting, marketing, and financing your business.
smallbusiness.yahoo.com
E-commerce Solutions from Yahoo!
Reliable plans w/ free 24-7 support, domain, hosting, and email. $50 setup fee waived.
smallbusiness.yahoo.com
Yahoo! Web Hosting $25 Setup Waived
Reliable plans include free domain & 24-7 support.
webhosting.yahoo.com
Great Value! Domain Names from Yahoo!
Includes free web page, email & domain forwarding, 24-7 support.
domains.yahoo.com
See your message here...
Search the Web:
Search
HOSTED BY YAHOO!
Get a free web site or business web hosting with Yahoo!
Copyright © 2006 Yahoo! Inc. All rights reserved. Copyright/IP Policy | Terms of Service | Guide to Online Security
NOTICE: We collect personal information on this site.
To learn more about how we use your information, see our Privacy Policy
Done

Address Mail Fake

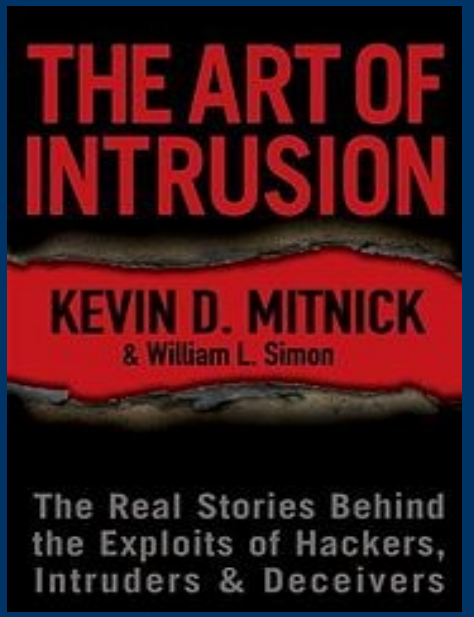


Social Engineering – 1

- Social Engineering (Ingegneria Sociale) è lo studio del comportamento di una persona al fine di sottrarle informazioni.
- Il phishing e ogni tecnica che cerca di ingannare gli utenti fa parte della Social Engineering.
- L'evoluzione dell'informatica ha reso l'Uomo l'anello debole della catena "sicurezza": è più facile scoprire una password con l'inganno che con tecniche informatiche!
- Similmente al "Metodo del tubo di gomma" queste tecniche sono spesso molto più efficienti di quelle di crack informatiche.
- Il metodo del tubo di gomma dice che, se esiste una persona a conoscenza di una chiave segreta, battendo con un tubo vigorosamente e ripetutamentela pianta dei suoi piedi, prima o poi rivelerà l'informazione.

Social Engineering - 2

- Il Social Engineering non si limita quindi a strumenti informatici, anzi invita all'uso della fantasia per capire il modo migliore di rubare informazioni ad una vittima in particolare.
- Telefonare, rovistare nella spazzatura, spacciarsi per altre persone, conoscere di persona la vittima...
- Es: il cracker si spaccia per un tecnico aziendale e chiede telefonicamente a un impiegato di dargli login e password.
- "L'Arte dell'Inganno" - Kevin Mitnick



Keylogger - 1

- Strumento in grado di intercettare tutto quello che viene digitato sulla tastiera.
- Possono essere:
  - Hardware: collegati fisicamente alla tastiera, difficili da inserire, difficili da individuare, molto efficienti, usati nello spionaggio.
  - Software: applicazioni che girano in background sul computer infettato registrando tutti i tasti premuti, in genere prevedono un modo per inviare quanto intercettato ad un computer remoto, disponibili a tutti.
- I Keylogger software sono usati molto spesso in rete per spiare qualcuno o per rubare informazioni sensibili (password, carte credito, ecc.).
- Nel 2002 l'Fbi grazie a un keylogger ha incastrato il boss mafioso Nicky Scarfo Jr.

Keylogger - 2

- Per infettare un computer con un keylogger si possono usare diversi mezzi: allegato e-mail, virus, trojan horse...
- Creare un keylogger è molto semplice, è difficile far si che le informazioni intercettate siano trasmesse al creatore senza rivelarne l'identità.
- Inviare dati via mail o a un determinato indirizzo Ip rischia di esporre l'attaccante, ciò nonostante questi rimangono i principali metodi per recuperare le intercettazioni (insieme a Telnet, Irc, ecc.).
- Nel 1997 proposto un modo abbastanza sicuro di trasmettere le intercettazioni dei keylogger:
  - I dati da trasmettere vengono cifrati con la chiave pubblica dell'autore del keylogger (otteniamo quindi un ciphertext)
  - Il ciphertext viene inviato moltissime persone (ip o mail)
  - Tra tutti i riceventi solo l'autore avrà la chiave privata necessaria a decifrare il ciphertext.

Keylogger - 3

I Keylogger si possono suddividere in base alla difficoltà nel rilevarli ed eliminarli:

1) il kl si inserisce nel kernel dell'OS stesso, è praticamente introvabile, molto potente ma anche difficile da realizzare
2) il kl sfrutta gli hook alle Api dell'OS
3) il kl utilizza direttamente alcune Api (GetAsyncKeyState, ecc.), facile da realizzare e da scoprire, causa un notevole incremento nell'uso di CPU e quindi può essere scoperto facilmente, ogni tanto alcune key non vengono intercettate

- Soluzioni:
  - Controllare quali applicazioni sono in corso
  - Anti-Spyware: limitati però alla loro *know-list*
  - Firewall: può impedire al keylogger di inviare dati
  - Completamento automatico o "Copia e Incolla"
  - Web-based keyboards: tastiere a video in cui si scrive con il mouse

Bibliografia

- www.wikipedia.org
- *Real World ARP Spoofing* - Raul Siles, 2003
- http://ettercap.sourceforge.net
- *Sniffer - Basics and Detection* – Sumit Dhar
- www.anti-phishing.it
- www.google.com/safebrowsing/report_phish/
- http://keylogger.org
- http://anti-keylogger.org