

The background features a series of concentric circles and arrows. On the left, there are three circular icons, each containing an arrow pointing in a different direction (up-left, up, and up-right). On the right, there is a large, prominent arrow pointing towards the right edge of the frame. The overall design is minimalist and technical, using a grayscale color palette.

COMPUTER SECURITY

Marco Schiaffino

www.securityinfo.it



PROBLEM EXISTS BETWEEN KEYBOARD AND CHAIR

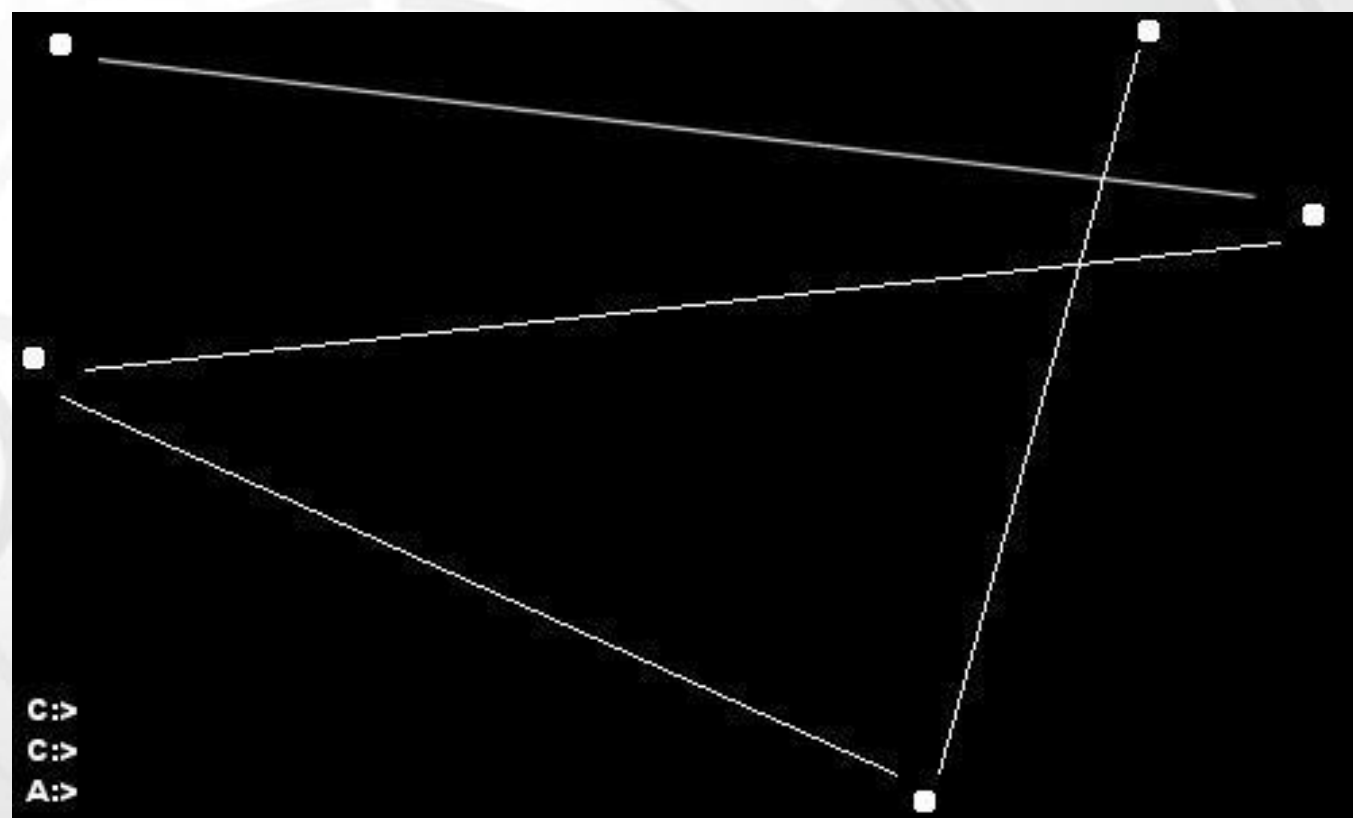


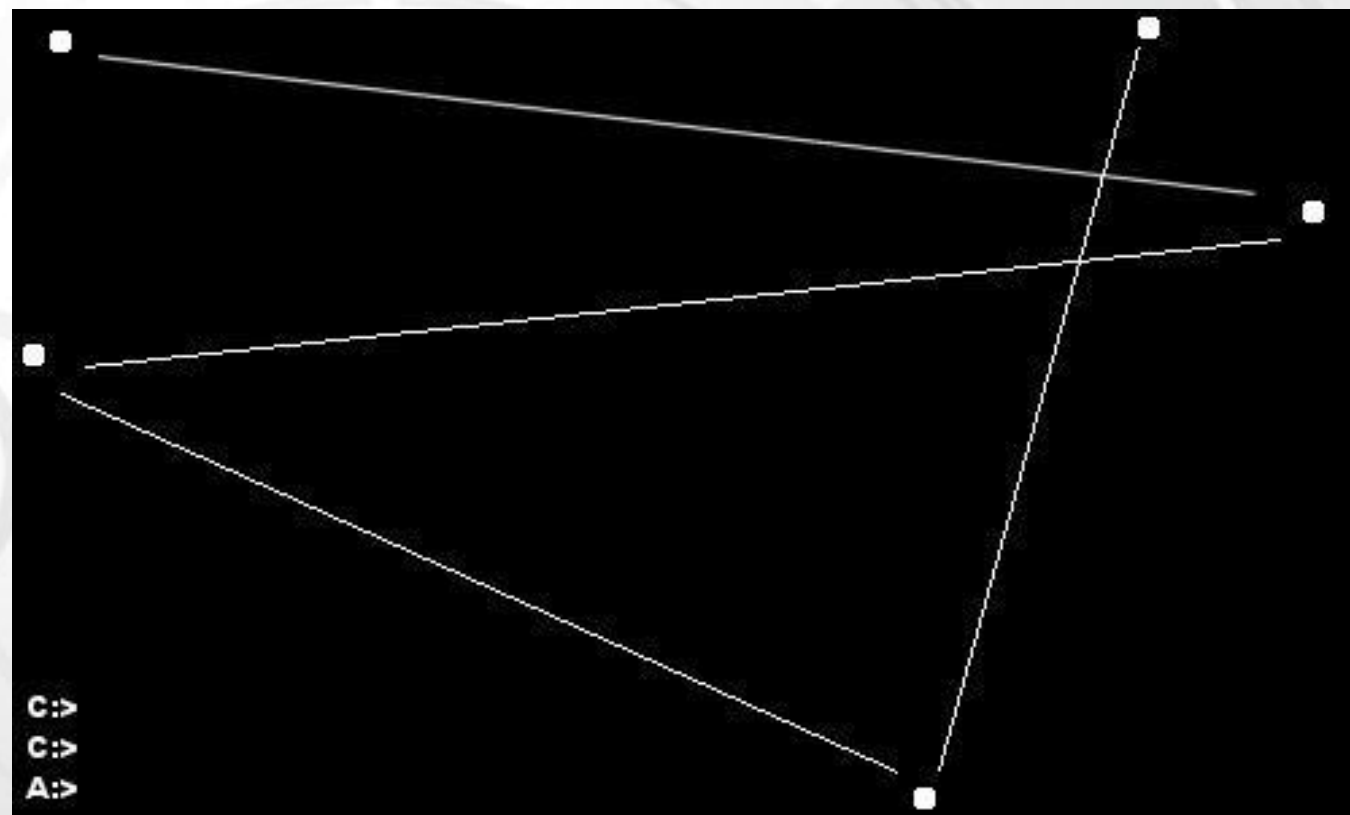
CONOSCI IL TUO NEMICO

The background features a light gray maze with several circular nodes. Inside some of these nodes are arrows pointing in different directions (up, down, left, right). A large, prominent white arrow points from the right side of the frame towards the center, passing behind the main text.

LEGGENDA METROPOLITANA #1

**‘IL MIO COMPUTER FUNZIONA BENE,
QUINDI NON HO NESSUN MALWARE’**





1988



RAT

REMOTE ACCESS TOOL

Consentono
di controllare
il computer
a distanza

Sono invisibili
e non rallentano il
sistema

Consentono
di accedere ai dati
memorizzati
sul computer




Programmatore

Pirata informatico

Organizzazione
criminale

Cliente finale

SERVIZI DISPONIBILI



- Attacchi DDoS contro siti Web	20€
- Invio di spam	40€
- Raccolta dei dati di carte di credito	50€
- Furto di email e account social	100€
- Furto di documenti	500€
- Discredito di un concorrente	variabile
- Crypto-Jacking	variabile

CONOSCI IL TUO NEMICO

- Professionisti del crimine informatico
- Utilizzano strumenti sofisticati
- Sono interessati a guadagnare denaro utilizzando il nostro computer
- Lavorano sul lungo periodo





RANSOMWARE



Polizia di Stato

Polizia postale e delle comunicazioni

**Centro Nazionale Anticrimine Informatico
per la Protezione delle Infrastrutture Critiche**



C.N.A.I.P.I.C

Attenzione!!!

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violazione delle leggi della Repubblica Italiana!

È stata fissata una seguente violazione: Dal tuo indirizzo IP "79.10.107.129" era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.

Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.

Il bloccaggio di computer serve per troncato l'attività illegale dalla parte tua.

I tuoi dati:

IP: 79.10.107.129
Posizione: Italy

Per togliere il bloccaggio devi pagare una multa di 100 euro. Hai due seguenti varianti di pagamento:

1) Effettuare il pagamento tramite l'Ukash.

Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net.

2) Effettuare il pagamento tramite il Paysafecard:

Per questo inserisci per favore il numero ricevuto (nel caso di necessità insieme con la password) nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net.

Ukash Dove passo trovare Ukash?

Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale **Epay, Epipoli**.

 Recati presso il punto vendita dotato di terminale **Epay, Epipoli** a te più vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovrà stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.

 **epay** - Voucher Ukash sono disponibili da migliaia di negozi con un terminal epay. **Epipoli** - Voucher Ukash sono disponibili da migliaia di negozi con un terminal Epipoli.

paysafecard Dove passo trovare Paysafecard?

paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisal e Penny.

RANSOMWARE

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

1. Type the address <http://torproject.org> in your Internet browser. It opens the Tor site.
2. Press 'Download Tor', then press 'DOWNLOAD Tor Browser Bundle', install and run it.
3. Now you have Tor Browser. In the Tor Browser open the <http://www.torproject.org>.onion
Note that this server is available via Tor Browser only
4. Write in the following public key in the input form on server. Avoid missprints.

1990-1991	1991-1992	1992-1993	1993-1994	1994-1995	1995-1996	1996-1997	1997-1998
1998-1999	1999-2000	2000-2001	2001-2002	2002-2003	2003-2004	2004-2005	2005-2006
2006-2007	2007-2008	2008-2009	2009-2010	2010-2011	2011-2012	2012-2013	2013-2014

- 5. Follow the instructions on the server.**

RANSOMWARE

RANSOMWARE

- Non pagare
- Non spegnere il computer
- Contattare la società antivirus





GLI STRUMENTI DI DIFESA

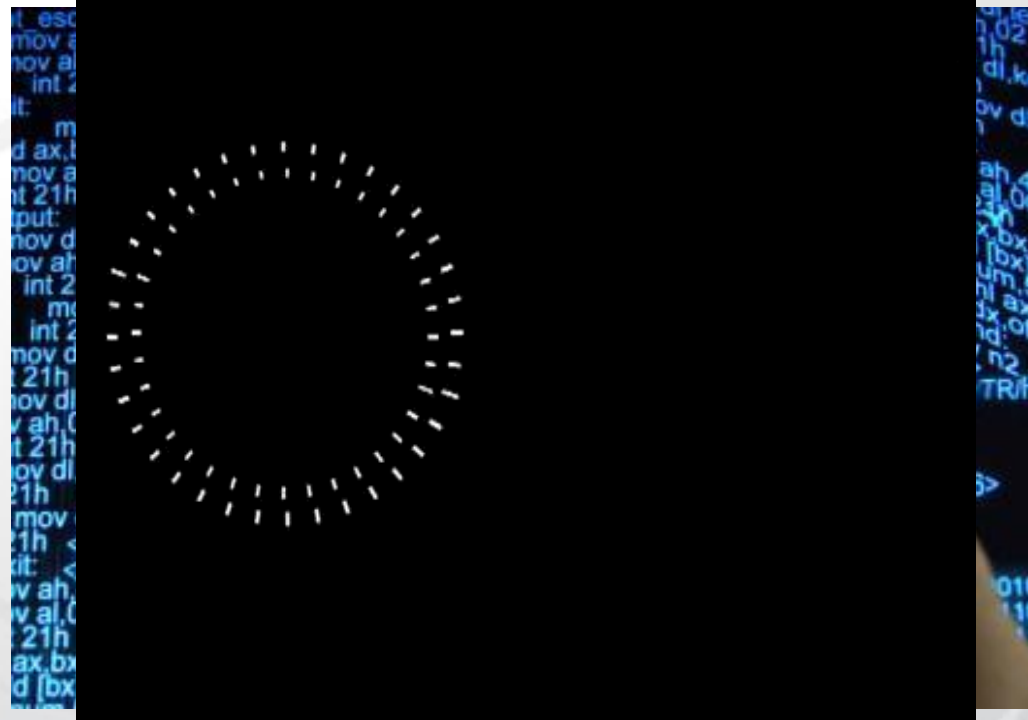
SOFTWARE DI PROTEZIONE

Firewall

Antivirus

Crittografia

COME FUNZIONA L'ANTIVIRUS



The background features a complex, light gray maze pattern. Several circular nodes within the maze contain arrows pointing in various directions (up, down, left, right, and diagonally). A large, prominent white arrow points from the right side of the frame towards the center, passing behind the main text.

LEGGENDA METROPOLITANA #2

**‘I PRODUTTORI DI ANTIVIRUS
CREANO I MALWARE PER VENDERE
DI PIÙ I LORO PRODOTTI’**

UNA CORSA CONTRO IL TEMPO

Società di sicurezza

Sviluppatore software

Aggiornamento

Vulnerabilità

Utente

Pirata informatico

Malware

BLASTER (2003)



**KEEP
CALM
AND
UPDATE
SYSTEM**



LEGGENDA METROPOLITANA #3

**‘USO UN MAC, QUINDI NON
HO BISOGNO DELL’ANTIVIRUS’**

GLI STRUMENTI DI DIFESA

- Non esistono SO al riparo dai malware
- Antivirus e firewall sempre attivi
- Antivirus sempre aggiornato
- Programmi e SO sempre aggiornato
- Il fattore tempo è determinante





FEDERICO



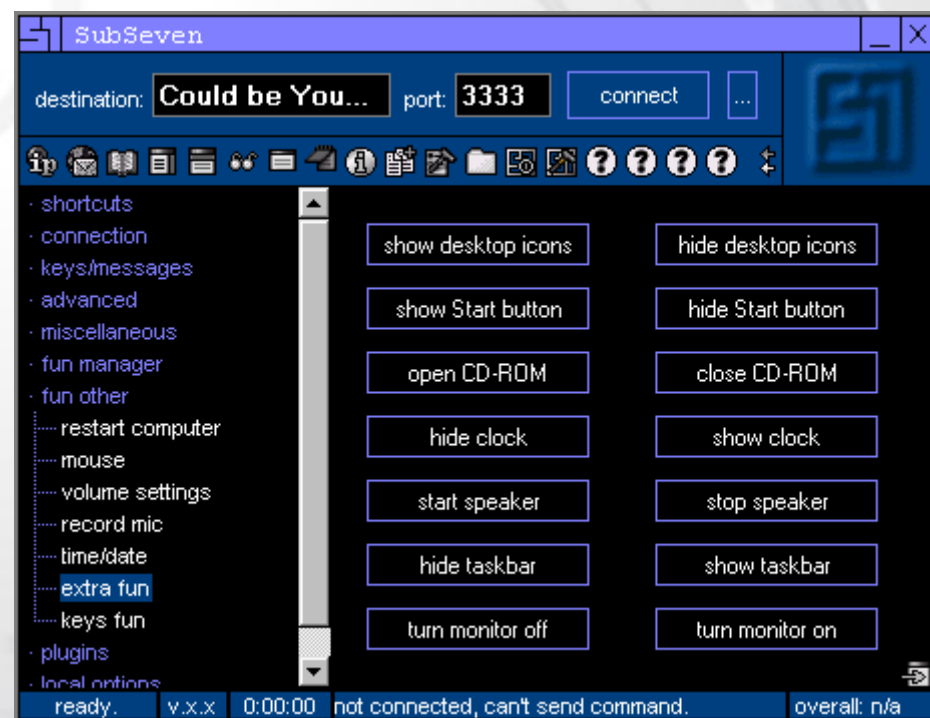
NICOLETTA

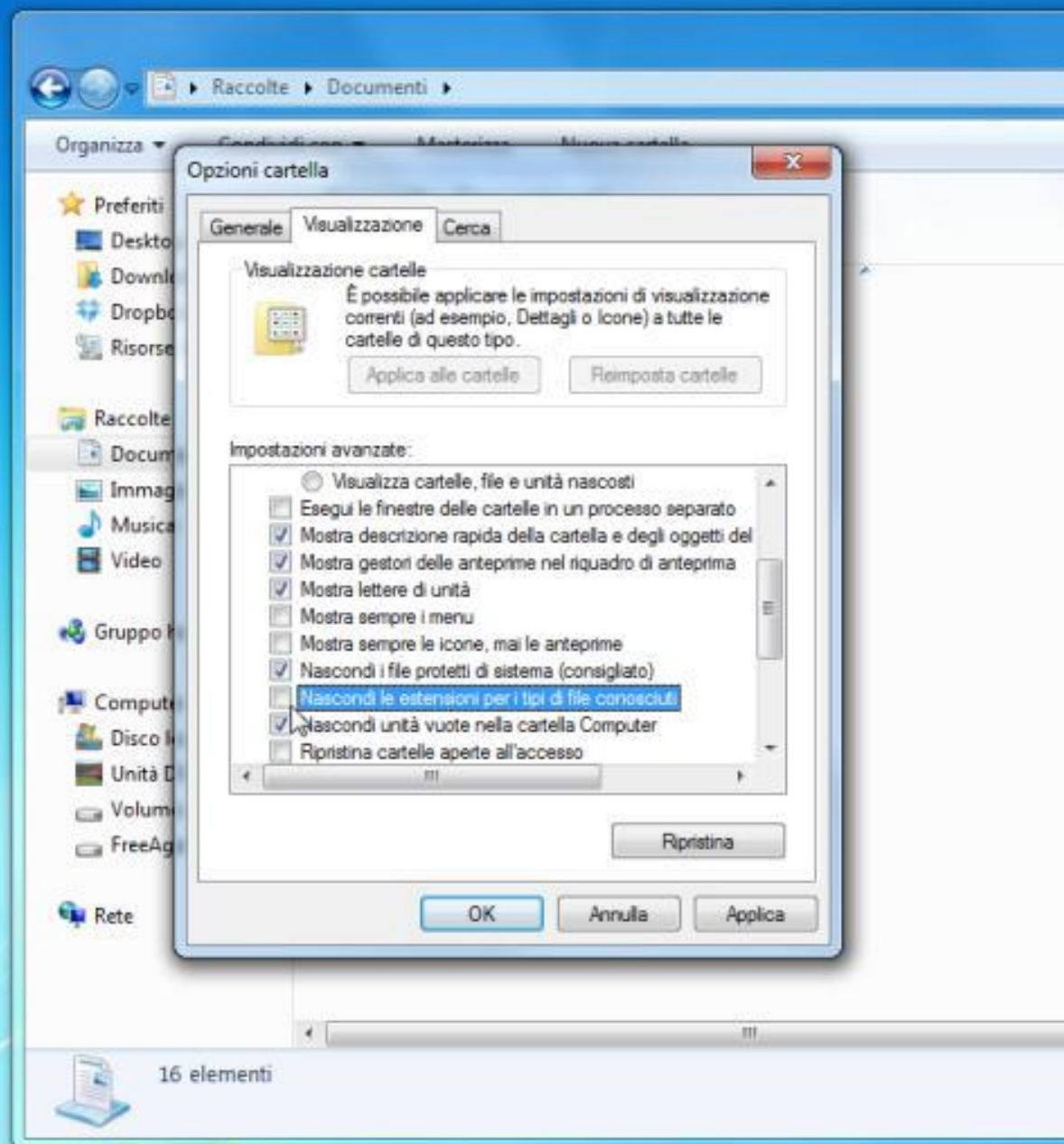


CHRISTIAN



LEA







CONOSCI (MEGLIO) IL TUO NEMICO



PHISHING



Protezione anti-frode 3D Secure 785306240 - Messaggio (HTML)

FILE MESSAGGIO GpgOL

Ignora Elimina Posta indesid. Rispondi Rispondi a tutti Inoltra Sposta in: ? Al responsabile Messaggio di p... Regole OneNote Azioni Segna come da leggere Categorizza Traduci Zoom


Elimina Rispondi Azioni rapide Sposta Categorie Modifica Zoom


lunedì 18/11/2013 12:27

CartaSi_Informa@cartasi.it <postmaster@archyvusistemas.it>

Protezione anti-frode 3D Secure 785306240

A ☐

 Fare clic qui per scaricare le immagini. Per motivi di privacy, il download automatico di alcune immagini del messaggio non è stato eseguito.



Per poter procedere con modifica della password del sistema anti-frode 3D

Se ne copia il codice di conferma nell'apposito spazio sul Portale Titolare:

Clicca Qui: <http://www.cartasi.it/gtwpages/common/index.jsp?id=gutTnPKdDl>

Per eventuali problemi o, se non avessi chiesto tu la modifica, contatta

il Servizio Clienti CartaSi.

I migliori saluti.

Servizio Clienti CartaSi



PREMIO MENSILE



dal 01/07/10 al 31/05/11
rinnova la tua postepay Visa
e vinci **fantastici premi**



+



+



Concorso "Riparty con Postepay"

Promozioni *postepay*

Dal 1° luglio 2010 al 31 maggio 2011 rinnova la tua Postepay, attivala e utilizzala subito* e parteciperai al concorso!

Gentile Cliente,

Perché sei stato un cliente fedele e hai usato la tua carta postepay nell'ultimo mese, hai vinto all'estrazione mensile una ricarica di **200 €** alla tua carta PostePay!

Cosa devi fare per ottenere il premio? - Molto semplice!

Accedi al nostro sito web dedicato alle carte PostePay e richiedi il tuo premio!

In palio per te ogni mese un fantastico premio!

Scrigno Elation long week end tra arte e sapori per due persone + Fotocamera Digitale Samsung WP 10

E se fai almeno 3 pagamenti sul circuito Visa durante il periodo del concorso, potrai partecipare all'estrazione finale e vincere una Vespa 125 GTS Giallo Lime.

**Partecipano alle estrazioni mensili i titolari che avranno rinnovato la carta e avranno effettuato almeno una transazione Visa nello stesso mese di attivazione della nuova carta. Sono escluse le transazioni effettuate sul circuito Postamat (es. ricarica carta, pagamenti bollettini o altri acquisti sul sito www.poste.it o presso gli uffici postali)*
Montepremi complessivo indicativo di € 11.449,00.

**La ricarica sarà eseguita nelle prossime 24 ore dopo la richiesta.*

Accedi al sito di postepay :



Estrazione di gennaio 2011

Ref. Id. HK-9395-3575-3105-0029
Firma Digitale Poste Italiane.

PHISHING

- Diffidare sempre di offerte e regali
- Nessuna banca chiede username e password via email
- Controllare il collegamento
- Usare sempre l'indirizzo o i preferiti





SPEAR PHISHING

Linked 

twitter 

facebook®

Pinterest

SOCIAL ENGINEERING

SPEAR PHISHING IN TRE MOSSE

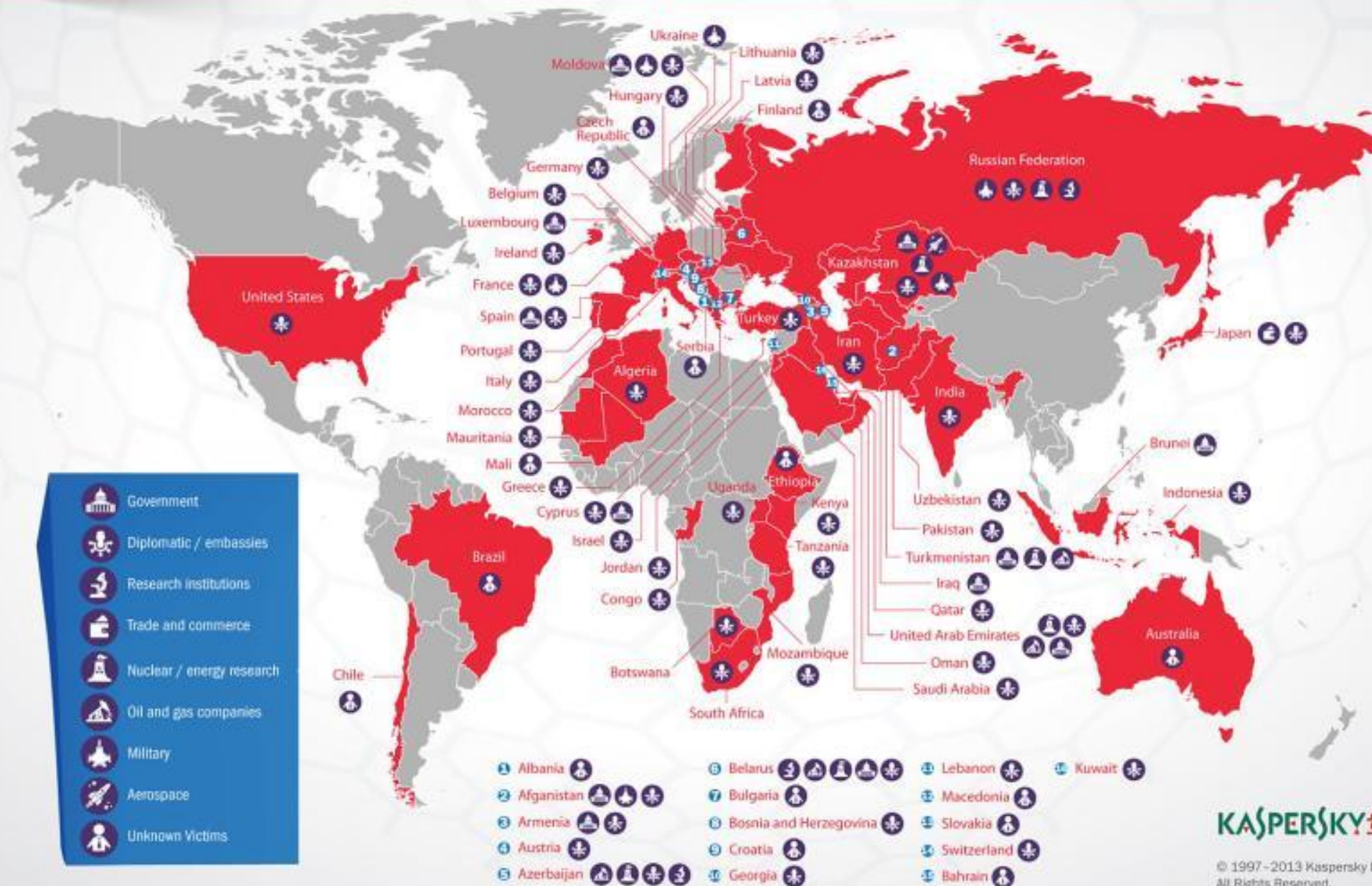
Studio della vittima

Esca

Attacco

Operation "Red October"

Victims of advanced cyber-espionage network



SPEAR PHISHING

- Software e sistema sempre aggiornati
- Impostare la privacy nei social network
- Verificare identità e credibilità
- Incrociare le dita





SPIONAGGIO DI STATO



Registrazione metadati
telefonate

Marina
(conservazione dati)

Boundless Informant
(mappatura dati)

Xkeyscore
(ricerca database)

Prism
(intercettazioni web)

Blarney
(intercettazioni dati
telefonici)

Bullrun
(violazione crittografia)

IL CASO STUXNET (2010)





INTERNET SERVICES



TM

INTERNET SERVICES

INTERNET SERVICES

- Controllare che cosa si memorizza
- Utilizzare sistemi di verifica complessi per l'accesso all'account
- Non utilizzare mai Wi-Fi aperte





LA PAROLA GIUSTA

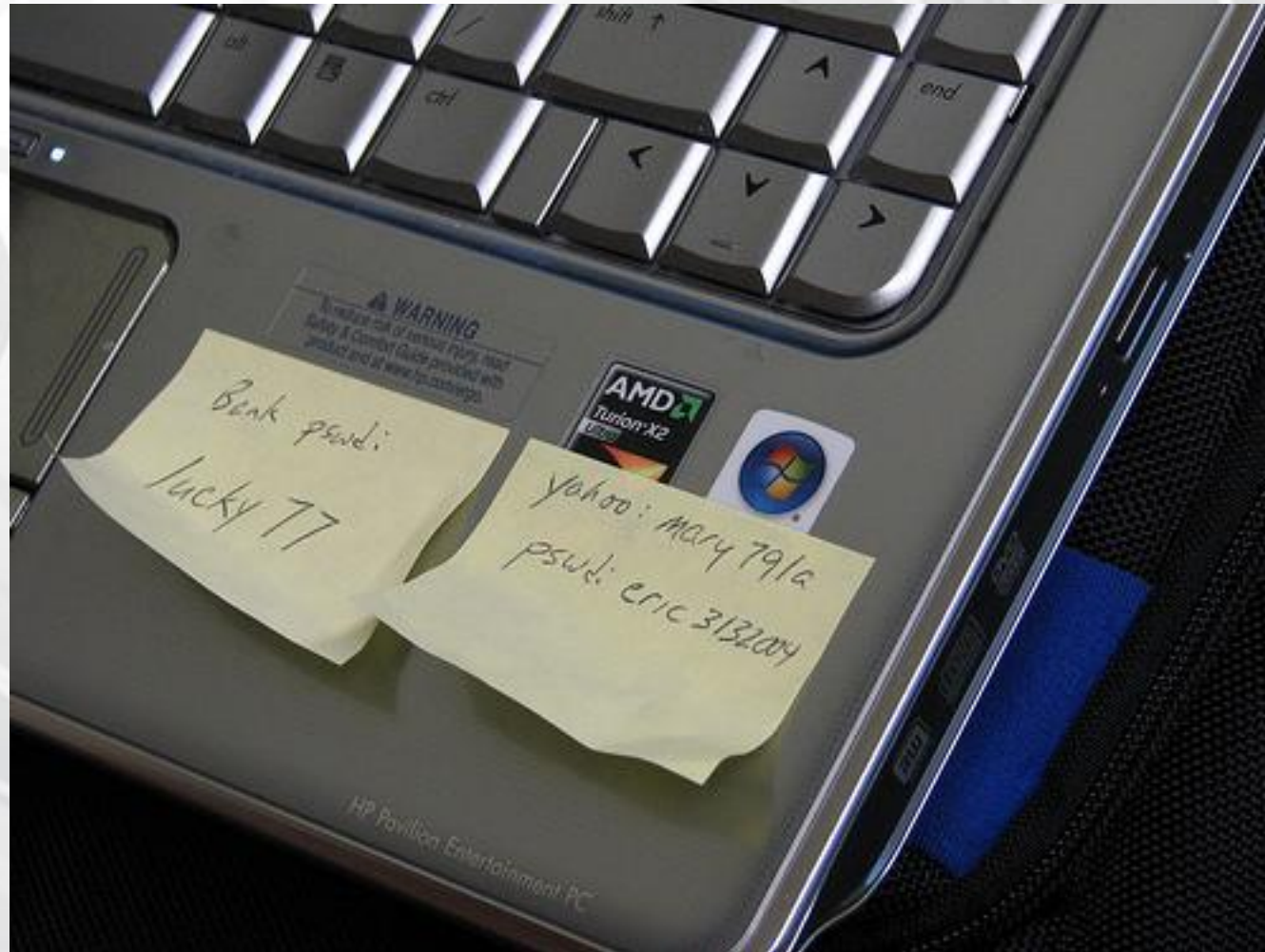
TECNICHE PER VIOLARE LE PASSWORD

Brute Forcing

Social Engineering

Dizionari

LA SINDROME DEL KAMIKAZE



LA PAROLA GIUSTA

- Password «robuste» (8 caratteri o più)
- Non usare sempre la stessa
- Meglio non scriverla su carta
- Mai darla a qualcun altro
- Usare software per la gestione
- Cambiarla periodicamente



That's all folks!

