ASSOCIAZIONE
NUOVA CIVILTÀ
DELLE MACCHINE

Forlì, 14 Marzo 2015

# Il crimine informatico: dalla criminalità organizzata al cyberbullismo

ulrico.bardari@poliziadistato.it
ulrico.bardari@unibo.it

ASSOCIAZIONE
NUOVA CIVILTÀ
DELLE MACCHINE

Forlì, 14 Marzo 2015


# Il crimine informatico: dalla criminalità organizzata al cyberbullismo

ulrico.bardari@poliziadistato.it
ulrico.bardari@unibo.it

# Attenzione

# INTERNET

Internet è uno straordinario mezzo di comunicazione che ci permette di ricevere informazioni da tutto il mondo, comunicare in tempo reale con persone distanti migliaia di chilometri ed altri innumerevoli vantaggi!

# Quali sono i principali rischi

Per il computer

Per i dati personali

Per la propria persona

# *Alcune leggi*

- Legge 547/1993 - Computer Crime
- Legge 48/2008 – Recepimento Convenzione di Budapest
- D.Lgs. 196/2003 - Misure minime di sicurezza.
- Illecito utilizzo di Carte di pagamento : Art. 55 n. 9 D.lgs. 21 novembre 2007, n. 231 (norma già esistente art. 12 D.l. 3 maggio 1991 n. 143)

# Legge 547/93

- 615 TER - Accesso abusivo ad un sistema informatico o telematico;

- 615 QUATER - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

- 615 QUINQUIES - Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;

- 617 QUATER - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;

- 617 QUINQUIES - Installazione di apparecchiature atte a intercettare, impedire od interrompere comunicazioni informatiche o telematiche;

- 617 SEXIES - Falsificazione, aiterazione o soppressione del contenuto di comunicazioni informatiche o telematiche;

- 640 TER - Frode informatica.

# *Legge 48/2008*
# *(Ratifica Convenzione di Budapest)*

- 1) La eliminazione della diversità nella definizione di "**documento informatico**" tra il diritto civile e il diritto penale;
- 2) L'introduzione del delitto di false dichiarazioni al Certificatore (art. 495-bis c.p.);
- 3) La profonda modifica dell'art. 615 - quinquies (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) in tema di virus e malware, con l'estensione delle condotte non solo al software, ma anche alle altre "apparecchiature e dispositivi", utilizzati allo scopo di danneggiare illecitamente un sistema informatico o telematico;
- 4) La rivisitazione del danneggiamento di dati, programmi, e dei sistemi informatici, anche di pubblica utilità, con l'introduzione della punibilità a querela del danneggiamento di dati "privati";
- 5) L'introduzione di una nuova fattispecie di frode informatica, commessa dal soggetto che presta servizi di certificazione di firma elettronica;
- 6) L'estensione ai reati "informatici" della responsabilità amministrativa degli enti, di cui al D.lgs 231/01;
- 7) La profonda modifica delle procedure di acquisizione dell'evidenza informatica, mediante l'imposizione dell'adozione di misure **tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**, e in altri casi l'adozione di procedure che assicurino la conformità dei dati acquisiti a quelli originali e la loro immodificabilità;
- 8) L'introduzione della **proceduta di "congelamento" dei dati per ragioni urgenti**, sottoposta a convalida da parte del Pubblico Ministero;
- 9) **L'affidamento delle indagini in tema di reati informatici e di pedo-pornografia agli uffici del pubblico ministero presso il tribunale del capoluogo del distretto di corte d'appello**.

# Pedofilia on line

PEDOFILIA ON LINE

Legge 3 agosto 1998, n. 269

**Casi di imputazione Artt. 600 ter e quater C.P.**

*PEDOFILIA ON-LINE*

Quando parliamo di pedofilia on-line ci riferiamo al comportamento di adulti pedofili che utilizzano la rete internet per incontrare altri pedofili (chat, forum, social networks), per alimentare le loro fantasie sessuali deviate, per contrattare e scambiare materiale fotografico o video pedopornografici e per ottenere contatti o incontri con i bambini che sono sulla rete.

# *PEDOFILIA ON-LINE*

Quando parliamo di pedofilia on-line ci riferiamo al comportamento di adulti pedofili che utilizzano la rete internet per incontrare altri pedofili (chat, forum, social network), per alimentare le loro fantasie sessuali deviate, per rintracciare e scambiare materiale fotografico o video pedopornografici e per ottenere contatti o incontri con i bambini che sono sulla rete.

# *PEDOFILIA ON LINE*

## *Legge 3 agosto 1998, n. 269*

## Casi di imputazione Artt. 600 ter e quater C.P.

- Realizzare, produrre
- Commerciare

→ **6-12 anni**

- Distribuire (materiale)
- Diffondere, divulgare (materiale o notizie finalizzate adescamento)
- Pubblicizzare (materiale o notizie finalizzate adescamento)

→ **1-5 anni**

- Cedere anche a titolo gratuito

→ **Fino a 3 anni**

- Detenere (consapevolmente)
- Procurarsi (consapevolmente)

→ **Fino a 3 anni**

# PEDOFILIA ON LINE 1 ottobre 2012, n. 172 (Ratifica convenzione di Lanzarote)

**"adescamento di minorenni"**: qualsiasi atto volto a carpire la fiducia di un minore di anni sedici attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete Internet (grooming) o di altre reti o mezzi di comunicazione per commettere i reati connessi all'abuso ed allo sfruttamento sessuale dei minori;

- le nuove condotte introdotte a integrazione del reato di **"prostituzione minorile"** tra cui quelle di "reclutamento alla prostituzione di un minore, gestione, controllo e organizzazione della prostituzione di un minore" (anche contro turismo sessuale);

- **il raddoppio dei termini di prescrizione** per i reati di abuso sessuale e sfruttamento sessuale dei minori;

- il reato di "**istigazione a pratiche di pedofilia e di pedopornografia**", configurabile nella condotta di chi con qualsiasi mezzo e con qualsiasi forma di espressione, pubblicamente istiga a commettere, in danno di minorenni, uno o più delitti di quelli previsti nel codice penale;

- l'ampliamento della gamma di reati a danno dei minori rispetto ai quali non si potrà più dichiarare di non essere a conoscenza della minore età della persona offesa, grazie al **principio dell'inescusabilità dell'ignoranza dell'età della persona offesa**, il cui limite è stato innalzato ai 18 anni;

- la modifica della fattispecie di **"corruzione di minorenne"**(art. 609 quinquies c.p.): il ddl prevede un inasprimento delle pene per chi compie atti sessuali in presenza di un minore di anni quattordici "al fine di farlo assistere" ;

- l'opportunità per i minori vittime di essere assistiti in ogni fase del procedimento giudiziario dal supporto emotivo e psicologico di operatori, di comprovata esperienza, legittimati a operare per la cura ed il sostegno alle vittime;

- il **"trattamento psicologico per i condannati per reati sessuali in danno di minori"**, con l'obiettivo di garantirne il recupero e ridurre i casi di rischio di recidiva.


YouTube

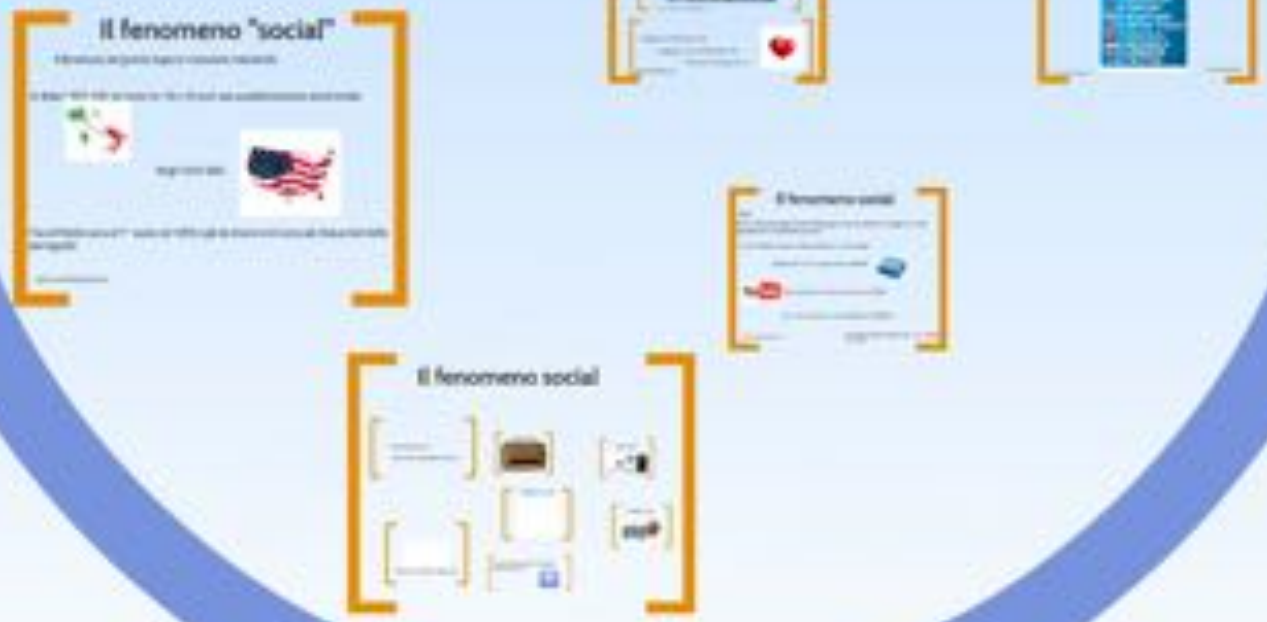
# Evoluzione e rivoluzione

La diffusione capillare di Internet a livello globale ha reso le comunicazioni digitali come il principale motore economico del pianeta.

L'andamento esponenziale dell'evoluzione tecnologica a portato gli esperti a definire il processo evolutivo come un fenomeno "rivoluzionario"

Sono cambiate le abitudini delle persone comuni

Si è adeguata la criminalità



# Evoluzione e rivoluzione

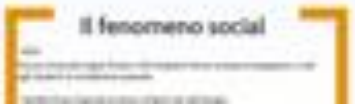
La diffusione capillare di Internet a livello globale ha reso le comunicazioni digitali come il principale motore economico del pianeta.

L'andamento esponenziale dell'evoluzione tecnologica a portato gli esperti a definire il processo evolutivo come un fenomeno "rivoluzionario"

Sono cambiate le abitudini delle persone comuni

Si è adeguata la criminalità



# Il fenomeno social

Fonte: socialnomics.net

Per arrivare a 50 milioni di utenti...

Radio 38 anni

Ipod: 3 anni

Televisione: 13 anni

Internet: 4 anni

Facebook: 100 milioni in meno 9 mesi

Apple store ha raggiunto 1 miliardo di Dowload in 9 mesi

Fonte: socialnomics.net

Per arrivare a 50 milioni di utenti...

# Radio 38 anni

# Televisione: 13 anni

# Internet: 4 anni

# Ipod: 3 anni


Facebook: 100 milioni in meno 9 mesi

Apple store ha raggiunto 1 miliardo di Dowload in 9 mesi

# Il fenomeno "social"

Il fenomeno più grande dopo la rivoluzione industriale

In Italia l' 80% delle persone tra 18 e 35 anni usa quotidianamente social media

Negli USA il 98%

I Social Media sono al 1° posto nel WEB e già da diversi anni sono più frequentati della pornografia

*ulrico.bardari@unibo.it*

# Il fenomeno social

OGGI:

Facebook: 1 miliardo e 350 milioni di utenti attivi al mese


**Di cui 1 miliardo e 200 milioni attivi via mobile**

Fonte: Marketing Projet Management

1 coppia su 5 si è formata on-line

3 coppie gay su 5 si sono formate on-line

1 divorzio su 5 è causato on-line

Fonte: socialnomics.net

# fenomeno social

OGGI:

Facebook: 1 miliardo e 350 milioni di utenti attivi al mese


**Di cui 1 miliardo e 200 milioni attivi via mobile**

Fonte: Marketing Projet Managemant

1 coppia su 5 si è formata on-line

attivi al mese

**Di cui 1 miliardo e 200 milioni attivi via mobile**

Fonte: Marketing Projet Managemant

1 coppia su 5 si è formata on-line

3 coppie gay su 5 si sono formate on-line

1 divorzio su 5 è causato on-line

Fonte: socialnomics.net

# Il fenomeno social

OGGI:

Alcune Università inglesi (Exeter a Birmingham) hanno smesso di assegnare e-mail agli studenti: le considerano superate

I bambini all'asilo imparano scrivendo sull'Ipad e non sulla lavagna

Ogni secondo ci sono 2 nuovi iscritti su LinkedIN

300 ore di video al minuto sono caricati su YouTUBE

più di 35 milioni di voci in oltre 280 lingue su WIKIPEDIA

# Popolazione mondiale

Il 50% della popolazione mondiale ha meno di 30 anni.
Il limite di età per iscriversi ai principali Social Network è di 13 anni


Fonte: socialnomics.net

ulrico.bardari@unibo.it


YouTube


Realtà
Virtuale
Virtuale?

# Realtà Virtuale

# Esposizione ad un'azione criminale

Il 46% degli utenti di Facebook ha accettato richieste di amicizia da sconosciutiL'89% degli utenti di età attorno ai 20 anni ha divulgato la propria data di nascita completa.

Quasi il 100% degli utenti ha pubblicato il proprio indirizzo e-mail.
Il 30-40% degli utenti ha elencato dati relativi alla propria famiglia e ai propri amici.

Fonte: Sophos

## L'inconsapevolezza

# L'inconsapevolezza

Le prime vittime dell'inconsapevolezza sono inglesi

Kimberly Swan dipendente IVELL perchè ha postato che "il lavoro è noiso" =LICENZIATA

Alcuni dipendenti di grandi magazzini hanno postato che i clienti sono "idioti"
=LICENZIATI

Dipendenti della British Airways definiscono su Facebook i viaggiatori "puzzolenti"
=LICENZIATI

## COMUNITA' VIRTUALI

L'essere umano è un animale sociale: la capacità di comunicare nasce dall'esigenza di condividere con i propri simili non solo informazioni utili per la sopravvivenza, ma anche emozioni, piaceri, interessi.

- Si scrivono due chiacchiere (chat)
- Si vede (tra sé nessuno con foto degli amici e video chat)
- Si leggono i quotidiani in edicola (news)
- Si partecipa a dibattiti e conferenze (forum e blog/wiki)
- Si gioca tutti insieme (giochi on-line)
- Si organizza per incontrarsi dal vivo

## COMUNITA' VIRTUALI

- Facebook è uno social network che fornisce gratuitamente ai suoi utenti la possibilità di contattare altre persone, anche se iscritte al servizio, mediante chat, e-mail, o gruppi di discussione comuni. Permette inoltre la condivisione di foto ed altri contenuti audiovisivi.
- Universi virtuali in 3D (MyCraft e Habbo): sono mondi virtuali tridimensionali multi-utente online, i cui ultimi fornitori di loro utenti (definiti "residenti") gli strumenti per aggiungere e creare nel "mondo virtuale" nuovi contenuti grafici oggetti, fisionomie dei personaggi, contenuti audiovisivi, ecc.

"Le comunità virtuali tendono a esacerbare, più che risolvere, l'atomizzazione e la frammentazione della società moderna, infatto danno ai membri un senso di appartenenza ad una comunità senza però dar loro quel senso di responsabilità che è tipico delle relazioni umane"

David Ehrenfeld, Pseudo communities - 1993

## SALVAGUARDIA DEI MINORI

Facebook ha già introdotto, negli Stati Uniti, un sistema automatico di riconoscimento facciale, che provvede da solo ad individuare i visiti delle persone nelle foto, senza bisogno che siano "taggati" da qualcuno. Questo consentirà ai social network – e quindi a chiunque – di mettere in correlazione le immagini con i fatti della vita reale, con scarso controllo da parte delle persone interessate.

Tra gli adulti che conosciamo, ce n'è sempre un'ampia quota che non vuole stare su Facebook, o che ci sta inserendo pochissime informazioni personali, perché preferisce un certo grado di riservatezza.

## *COMUNITA' VIRTUALI*

**L'essere umano è un animale sociale: la capacità di comunicare nasce dall'esigenza di condividere con i propri simili non solo informazioni utili per la sopravvivenza, ma anche emozioni, piaceri, interessi.**

- Ci si scambiano due chiacchiere (chat).
- Ci si vede (social network con foto degli iscritti o video chat).
- Si leggono i quotidiani in edicola (news).
- Si partecipa a dibattiti e conferenze (forum e bacheche).
- Si gioca tutti insieme (giochi on-line).
- Ci si organizza per incontrarsi dal vivo

# *COMUNITA' VIRTUALI*

- Facebook è uno social network che fornisce gratuitamente ai suoi utenti la possibilità di contattare altre persone, anch'esse iscritte al servizio, mediante chat, e-mail, o gruppi di discussione comuni. Permette inoltre la condivisione di foto ed altri contenuti audiovisivi.
- Universi virtuali in 3D (MyCraft e Habbo): sono mondi virtuali tridimensionali multi-utente online, i cui sistemi forniscono ai loro utenti (definiti "residenti") gli strumenti per aggiungere e creare nel "mondo virtuale" nuovi contenuti grafici: oggetti, fisionomie dei personaggi, contenuti audiovisivi, ecc.

**"le comunità virtuali tendono a esacerbare, più che risolvere, l'atomizzazione e la frammentazione della società moderna, infatti danno ai membri un senso di appartenenza ad una comunità senza però dar loro quel senso di responsabilità che è tipico delle relazioni umane"**

**David Ehrenfeld, Pseudo communities - 1993**

## *SALVAGURADIA DEI MINORI*

Facebook ha già introdotto, negli Stati Uniti, un sistema automatico di riconoscimento facciale, che provvede da solo ad individuare i volti delle persone nelle foto, senza bisogno che siano "taggati" da qualcuno. Questo consentirà al social network – e quindi a chiunque – di mettere in correlazione le immagini con i fatti della vita reale, con scarso controllo da parte delle persone interessate.

Tra gli adulti che conosciamo, ce n'è sempre un'ampia quota che non vuole stare su Facebook, o che ci sta inserendo pochissime informazioni personali, perché preferisce un certo grado di riservatezza.


2010 Rank: 407 Site Report [LV] SIA ASK.FM
ask.fm
Sei già registrato? Accedi
Chiedi e rispondi
REGISTRATI ADESSO!
Nome utente
Password
Accedi
Accedi tramite
Hai dimenticato la password o il tuo nome utente?
Guarda chi è già qui
Google play
App Store
English · Italiano · Français · Deutsch · Español · Türkçe · Polski · Русский · tutte le lingue ►
© SIA Ask.fm 2014 | Centro di sicurezza | Termini e politiche | Loghi | Pubblicità | Contattaci
Lingua: Italiano ▼

# *IL MONDO DELLE CHAT*

Le chat si presentano sotto forma di "stanze" virtuali nelle quali è possibile "chattare" con più persone contemporaneamente; un elenco delle persone presenti nella "stanza" è sempre visibile ed è inoltre possibile instaurare conversazioni private con uno o più utenti.

- Nick Name. Gli utenti delle chat usano identificarsi con un "nickname" (un nome fittizio). Per attribuirsi il nick è necessario, in genere ma non sempre, effettuare un'iscrizione presso i siti che ospitano le chat. E' possibile usare quanti nick si vogliono e creare un numero illimitato di identità. Le chat dunque offrono, oltre all'anonimato (non si è costretti, a fornire i nostri veri dati ed è possibile definire i profili con informazioni non vere), la possibilità di presentarsi agli altri nel modo che si ritiene più congeniale in un dato momento e con date persone.

# *I PERICOLI DELLE CHAT*

Sulle chat vige l'anonimato, nel senso che ogni utente sceglie un nome fittizio con cui verrà riconosciuto dagli altri. Questo significa che non sappiamo mai chi si cela veramente dietro questa "identità on line".

- Anonimato. Dietro un apparente ed innocuo nickname può nascondersi una persona totalmente diversa da ciò che si può intuire "chattando". Chiacchierare non è reato... ma è necessaria una certa cautela.

- Lo scambio di dati. Attaverso le chat è possibile scambiarsi dati di ogni genere: scambiare files, inviare e-mail e molto altro.

Svariati sono i casi di pedofilia telematica con l'utilizzo delle chat.


YouTube

## PERICOLI DI UNA ECCESSIVA FREQUENTAZIONE

- Allontanamento e progressivo "distacco" dalla vita reale, con gravi conseguenze sulla normale vita di relazione;
- Con la perdita del senso "del reale" inizia il disinteresse anche affettivo per le persone che ci circondano e con le quali si vive;
- Acquisizione di un crescente senso di impunità: in un mondo virtuale si tende a considerare virtuali e violabili, senza particolari remore, anche le norme che lo "regolano" . Ciò influisce invariabilmente anche sulla valutazione morale del proprio agire nella normale realtà.
- Svalutazione della propria reale personalità, a vantaggio dell'esaltazione del proprio alter-ego virtuale, spesso creato e costruito ad immagine e somiglianza di "modelli di perfezione" altrimenti irraggiungibili nel così detto mondo reale.

# DIVULGAZIONE ILLECITA DI IMMAGINI

Grazie a queste tecnologie della comunicazione, sempre più spesso, e soprattutto tra coetanei,
accade che vengano immessi nei blog, nelle chat, in emule, foto e video che ritraggono amici o partner in atteggiamenti intimi o sconvenienti, spesso accompagnati da commenti dispregiativi e lesivi della dignità.

Ciò accade anche con i telefonini, grazie alle videocamere e alle connessioni bluetooth.
Si tratta di episodi perseguibili penalmente, dei quali spesso non vengono correttamente valutate le gravi conseguenze.


Pubblicazione
Condivisione di immagini
Video
Fenomeno del Cyberbulling

# Virtuale?

# *Cyberbulling*

## *Rilievi penali*

Art. 612 Minaccia
Art. 615 bis Interferenze illecite nella vita privata Art. 594 Ingiuria Art. 595 Diffamazione
Art. 580 Istigazione o aiuto al suicidio

# *Cyberbulling*

Attività investigative e realtà operativa

Importanza dell'attività di prevenzione


YouTube

# *Il crimine informatico*

# Il crimine informatico

Il crimine informatico è un crimine commesso utilizzando un computer, una rete o un dispositivo hardware.

Il computer o il dispositivo può essere l'agente, il mezzo o l'obiettivo del crimine.

Un crimine può avere luogo sul solo computer o in combinazione con altre posizioni e luoghi.

I crimini informatici possono essere banalmente considerati come la "dematerializzazione" della classica criminalità

ulrico.bardari@unibo.it

# Il crimine informatico: definizioni

Il crimine informatico può essere generalmente definito come **un'attività criminale che coinvolge la struttura della tecnologia di informazione**, compreso l'accesso illegale (l'accesso non autorizzato), intercettazione (con mezzi tecnici di trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema informatico), interferenze di dati (danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici), sistemi di interferenza (interferenza con il funzionamento di un sistema informatico mediante l'immissione, trasmissione, danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici), uso improprio di dispositivi, contraffazione (o furto d'identità) e frodi elettroniche.
- Paul Taylor (autore del libro Hacker del **1999**) -

*ulrico.bardari@unibo.it*

# Il crimine informatico

Spam Frode

Diritto d'autore

Molestie

Spaccio di sostanze illecite
Terrorismo
Pedopornografia
Guerre informatiche

Contenuti sensibili ( crimini d'odio, blasfemia, sovversione politica, corruzione di minorenni, induzione della prostituzione)

*ulrico.bardari@unibo.it*

# Le organizzazioni criminali

*Criminalità organizzata transnazionale*
*I cartelli della droga*
*Terrorismo*
*Crimine contro l'umanità*
*Criminalità informatica*

# *Diffusione e motivazione*


YouTube

# Evoluzione degli attacchi informatici

Negli anni novanta gli attacchi erano principalemte di natura dimostrativa o autocelebrativa

Nel primo decennio degli anni duemila sono sorte motivazioni di profitto, organizzazioni criminali

Dopo il 2010 il crimine si è orientato più verso soggetti di alto profilo, infrastrutture critiche, attivismo politico, spionaggio.

# Acquisti on line in Italia

La tendenza ad acquistare on-line è in costante CRESCITA


Fonte: Netcomm e Human Highway, Indagine Natale 2014
Numero di acquirenti online di più di metà dei regali di Natale - trend ultimi anni

*ulrico.bardari@unibo.it*

# Cybercrime e piccoli passi

I criminali informatici sottraggono di proposito piccoli importi per non essere scoperti
Ma tutti questi importi alla fine si sommano.
Se non si comunica una perdita, si aiuta di fatto il crimine perché si impedisce alle forze dell'ordine di conoscere l'esatta entità del fenomeno e di perseguirlo penalmente.

Le pene in Italia per la Truffa e per la Frode Informatica sono tra i 6 mesi e i 3 anni di reclusione

=

Maggioranza dei casi vengono archiviati

Non esistono sistemi nazionali od internazionali coordinati per tracciare il crimine sulle truffe e le frodi on-line

*ulrico.bardari@unibo.it*

# Cybercrime vs Drugs

*Già dal 2008, un rapporto dell'FBI dichiarava che la criminalità informatica avrebbe a breve superato per la prima volta nella storia il business della droga , diventando la più grande specie di illegalità.*

| Putting Malicious Cyber Activity in Context | | | |
|---|---|---|---|
| CRIMINAL ACTION | ESTIMATED COST | PERCENT OF GDP | SOURCE |
| GLOBAL | | | |
| Piracy | $1 billion to $16 billion | 0.008% to 0.02% | IMB |
| Drug Trafficking | $600 billion | 5% | UNODC |
| Global cyber activity | $300 billion to $1 trillion | 0.4% to 1.4% | Various |
| US ONLY | | | |
| Car Crashes | $99 billion to $168 billion | 0.7% to 1.2% | CDC, AAA |
| Pilferage | $70 billion to $280 billion | 0.5% to 2% | NRF |
| US- cyber activity | $24 billion to $120 billion | 0.2% to 0.8% | Various |

Dati alla mano (E-Economic Impact 2013) l'effettivo sorpasso è avvenuto nel 2014 con un assestamento del costo dei crimini informatici stimato in 800 miliardi di dollari.

*ulrico.bardari@unibo.it*

Nel rapporto del 2013 la Europol Serious & Organized Threat Assessment scrive:
"Total Global Impact of CyberCrime [has risen to] US $3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined."

# Furto d'identità

**Tipi**

L'identità può essere creata ex novo disponendo di dati personali e/o sensibili del legittimo proprietario
L'identità esistente può essere rubata disponendo delle credenziali d'accesso
Un'identità può essere del tutto falsa ed utile ad ottenere informazioni

Soggetti spesso organizzati in vere e proprie associazioni a delinquere carpiscono i dati anagrafici di altri soggetti al fine di sostituirsi alla vittima nella sottoscrizione di contratti di acquisto di beni (es. autoveicoli) e sottoscrivendo in loro nome contratti di finanziamento, corredati da documenti di identificazione ovviamente falsificati.

**Da parte di chi**

Singoli soggetti che per un futile motivo decidono di creare o appropriarsi di un'identità virtuale.

Lo scopo principale e quello di arrecare danno al legittimo proprietario piuttosto che benefici all'utilizzatore illegale

*ulrico.bardari@unibo.it*

# Hacktivism

In tema di Hacktivismo:
"Non si è trattato solo di proteste e provocazioni.
I cybercriminali hanno continuato a semplificare e automatizzare la propria tecnica del momento fatta di attacchi a basso rischio e volumi elevati contro obiettivi vulnerabili."

*ulrico.bardari@unibo.it*

Fonte: Data Breach Investigation Report 2012 Verizon

# Quantificazione dei profitti

Il cybercrimine può far guadagnare oltre il 1000% dell'investimento iniziale. ( Trustwave Global Security Report 2015)
Si tratta di un ipotetico investimento effettuato acquistando "merce" disponibile sul mercato nero: "prodotti" messi in vendita da hacker senza scrupoli, i cosiddetti blackhat (cappello nero).

Si comincia con un trojan, di quelli che permettono di chiedere un riscatto per riavere i propri dati
Ransomware costa sul mercato nero circa 3mila dollari
Vettore di infezione, tipicamente un sistema automatizzato di invio massivo di email che utilizza una qualsiasi vulnerabilità scoperta di recente costa circa 500 dollari
Reindirizzamento di utenti del web: questo servizio costa invece circa 1800 dollari
Meccanismo di criptografia (di quelli che cambiano ogni giorno) per eludere gli antivirus, alla modica cifra di 600 dollari

| ITEM | TOTAL INVESTMENT |
|---|---|
| Payload | - $3,000 |
| Infection Vector | - $800 |
| Traffic Acquisition | - $1,800 |
| Daily Encryption | - $800 |
| **Total Expenses** | **- $6,800** |

Ipotizziamo di ricevere 20mila visitatori dal sistema di reindirizzamento utenti da altri siti e consideriamo poi che, di questi, solo il 10% venga realmente infettato e che, di questi ultimi, solo lo 0.5% decida di pagare il riscatto: otteniamo 100 vittime. Considerando un riscatto medio di 300 dollari, il ricavo medio è di 3000 dollari al giorno (arrivando facilmente anche a 5mila dollari per un singolo riscatto su utenti mirati).
Nell'ipotesi di riuscire a portare avanti l'attacco per 30 giorni - prima che venga rilevato dagli antivirus e dai vari sistemi di blacco - si ottiene un ricavo totale di 90mila dollari

| | |
|---|---|
| Victims | 20000 |
| Infection Rate | 10% |
| Payment Rate | 0.5% |
| Victims (Payments) | 100 |
| Average Ransom | $300 |
| Length of Campaign | 30 Days |
| **Total Revenue** | **$90,000** |

Riepilogando, si giunge a un ricavo di 90mila dollari a fronte di una spesa iniziale di circa 6mila, con un profitto di 84mila dollari. Si tratta di un ritorno dell'investimento di circa il 1400 percento (i dentisti, ad esempio si attestano intorno al 100 percento di ritorno sul capitale investito). Il bottino molto probabilmente incassato in modo non tracciabile, tramite Bitcoin.

| | |
|---|---|
| Total Expenses | - $7,000 |
| Gross Revenue | $90,000 |
| Net Revenue | $84,100 |
| **ROI (%)** | **1,429%** |

Si comincia con un trojan, di quelli che permettono di chiedere un riscatto per riavere i propri dati
Rasomware costa sul mercato nero circa 3mila dollari
Vettore di infezione, tipicamente un sistema automatizzato di invio massivo di email che utilizza una qualsiasi vulnerabilità scoperta di recente costa circa 500 dollari
Reindirizzamento di utenti del web: questo servizio costa invece circa 1800 dollari
Meccanismo di crittografia (di quelli che cambiano ogni giorno) per eludere gli antivirus, alla modica cifra di 600 dollari

| ITEM | TOTAL INVESTMENT |
|---|---|
| Payload | – $3,000 |
| Infection Vector | – $500 |
| Traffic Acquisition | – $1,800 |
| Daily Encryption | – $600 |
| Total Expenses | – $5,900 |

scatto per

massivo di
ta circa 500

a 1800 dollari
ludere gli

| ENT |
| --- |
| |
| |
| |
| |
| |

Ipotizziamo di ricevere 20mila visitatori dal sistema di reindirizzamento utenti da altri siti e consideriamo poi che, di questi, solo il 10% venga realmente infettato e che, di questi ultimi, solo lo 0.5% decida di pagare il riscatto: otteniamo 100 vittime. Considerando un riscatto medio di 300 dollari, il ricavo medio è di 3000 dollari, al giorno (arrivando facilmente anche a 5mila dollari per un singolo riscatto su utenti mirati). Nell'ipotesi di riuscire a portare avanti l'attacco per 30 giorni – prima che venga rilevato dagli antivirus e dai vari sistemi di blocco – si ottiene un ricavo totale di 90mila dollari

| | |
| --- | --- |
| Visitors | 20,000 |
| Infection Rate | 10% |
| Payout Rate | 0.5% |
| Ransom Amount ($) | $300 |
| Length of Campaign | 30 days |
| Total Revenue | $90,000 |

Riep
fron
profi
dell'
ad e
ritor
prob
tram

Riepilogando, si giunge a un ricavo di 90mila dollari a fronte di una spesa iniziale di circa 6mila, con un profitto di 84mila dollari. Si tratta di un ritorno dell'investimento di circa il 1400 percento (i dentisti, ad esempio si attestano intorno al 100 percento di ritorno sul capitale investito). Il tutto molto probabilmente incassato in modo non tracciabile, tramite Bitcoin.

| | |
|---|---|
| Total Expenses | – $5,900 |
| Gross Revenue | $90,000 |
| Net Revenue | $84,100 |
| ROI (%) | 1,425% |

# *Forme attuali di cybercrimine*

# Obiettivi sensibili

Per la prima volta in Italia un attacco di cyber-criminali ha violato il profilo Facebook di una grande azienda, il Gruppo Alpitour (il più importante Tour Operator italiano), per diffondere, attraverso falsi annunci di offerte, programmi pericolosi capaci di penetrare nel pc degli utenti per impadronirsi di dati importanti, come codici di carte di credito e credenziali di accesso (comprese quelle bancarie), dati personali.

ANSA.it > Tecnologia e Internet > News

SMS | NEWSMAP

## In Italia primo cyber-attacco da Facebook grande azienda

Violato il profilo del Gruppo Alpitour,

15 settembre, 13:59

+1 3 Tweet 2 Consiglia 24

Indietro | Stampa | Invia | Scrivi alla redazione | Suggerisci

Per la prima volta in Italia un attacco di cyber-criminali ha violato il profilo Facebook di una grande azienda, il Gruppo Alpitour, per diffondere, attraverso falsi annunci di offerte, programmi pericolosi capaci di penetrare nel pc degli utenti per impadronirsi di dati importanti, come codici di carte di credito e credenziali di accesso (comprese quelle bancarie), dati personali.

Alpitour

1 di 1 Guarda la foto

In Italia primo cyber-attacco da Facebook grande azienda

L'attacco è stato denunciato dalla stessa azienda nell'avviso ai 120.000 'amici' che su Facebook seguono le pagine Viaggidea, Francorosso, Villaggi Bravo e Alpitour. La situazione adesso è stata risolta, ma per gli esperti di sicurezza informatica quanto è accaduto è un campanello di allarme perché finora in Italia nessun gruppo criminale aveva mai preso di mira i social network. E' il primo caso italiano del genere, rilevano gli esperti, dopo che negli ultimi mesi si è assistito all'escalation di attacchi sui social media nei confronti di marchi internazionali importanti e con centinaia di migliaia di "amici" e "followers", come Associated Press, Burger King, Dodge, New York Times. L'attacco è iniziato la sera dell'11 settembre e, secondo gli esperti, il gruppo di cyber-criminali responsabile della violazione è sicuramente straniero. Inizialmente sono state rubate le credenziali degli amministratori del profilo Facebook dell'azienda e quindi sono stati postati annunci in italiano che pubblicizzavano viaggi inesistenti. Cliccando sugli annunci, link apparentemente innocui indirizzavano su pagine web che contenevano programmi pericolosi, progettati per impadronirsi delle coordinate bancarie di chi fa acquisti online. Secondo gli esperti l'attacco è durato oltre 48 ore e rilevano che " il tempo, sui social media, è un moltiplicatore esponenziale del danno".

*ulrico.bardari@unibo.it*

# Obiettivi sensibili

Da quanto confermato anche dalla casa nipponica, trà il 17 e il 19 Aprile 2011 il Playstation Network ha subito un attacco informatico al quale un agenzia competente stà ora indagando. "Mentre indaghiamo sui dettagli di questo incidente, riteniamo che un soggetto non autorizzato abbia ottenuto le seguenti informazioni da voi fornite in precedenza: nome, indirizzo (città, stato/provincia, codice postale), nazione, indirizzo email, data di nascita, password, login e online ID di PSN/portatile. Inoltre è possibile che i dati del vostro profilo siano stati rilevati, inclusi la cronologia degli acquisti, l' indirizzo di addebito (città, stato/provincia, codice postale) cosi' come la vostra domanda di sicurezza PlayStation networkQriocity.". Queste le parole della Sony alle quali aggiungono che è possibile che questi hacker siano arrivati anche ai dati delle carte di credito, quali il numero e la data di scadenza, ma rassicurano che il codice di sicurezza sia escluso da questo pericolo.

## Sony: 93,000 PlayStation, Online Entertainment accounts hacked


Sony's hacking problems aren't over yet.

On Wednesday morning, Philip Reitinger, Sony's newly hired chief information security officer, said that about 93,000 PlayStation Network and Sony Online Entertainment user accounts have been breached in a Web attack.

The attack is merely the latest for Sony, which has been dealing with online assaults on its user accounts most of the year. So far, more than 90 million Sony user accounts across the company's online services have been breached, which led to online video gaming services being suspended for more than a month.

The security breaches haven't been limited to Sony's gaming business either. Sony's cloud-based Qriocity music service, Sony music websites and Sony Pictures websites have been hacked this year too.

*ulrico.bardari@unibo.it*

# Spy Eye

Il 24enne Aleksandr Panin ha confessato la sua colpevolezza in una corte di Atlanta. Piuttosto che agire in persona, Panin vendeva il suo programma ad altri criminali per una cifra tra i mille e gli 8mila dollari. I crimini informatici compiuti grazie a SpyEye sono moltissimi, tra cui un caso eclatante di un attacco a conti bancari da ben 3 milioni di dollari. L'FBI è riuscito a incastrare definitivamente Panin grazie a una leggerezza: nel 2011 il ragazzo aveva venduto una copia del malware ad un agente sotto copertura.


*ulrico.bardari@unibo.it*

# War games

Malware Stuxnet per attaccare alcuni impianti di arricchimento dell'uranio iraniani (anche detta Cyber weapon)
Primo Worm che spia e riprogramma PC industriali creato e diffuso dagli USA e Israele
Nel febbraio 2011 Anonymous ha "trafugato" delle e-mail alla HBGary, contractor del governo USA. Una di queste e-mail era datata 28 luglio 2010, proveniva dalla McAfee e forniva all'azienda una copia di Stuxnet[15]. In seguito Crowdleaks ha decompilato parte di Stuxnet, il sorgente è ottenibile su github.com.
Nel luglio 2013 Edward Snowden ha confermato che Stuxnet è stato progettato dalla NSA con la collaborazione dell' "intelligence" israeliana, tramite un corpo speciale noto come Foreign Affairs Directorate (FAD)


*ulrico.bardari@unibo.it*

# Speculazioni

Ad Aprile fu sabotato il profilo della AP (Associated Press) e fu millantato un attacco alla Casa Bianca.


La Borsa Americana crollò di colpo


*ulrico.bardari@unibo.it*

# Auto e Hamburger: concorrenza leale?

A febbraio fu hackerato il profilo Twitter della Burger King e sostituito il logo con quello McDonalds.

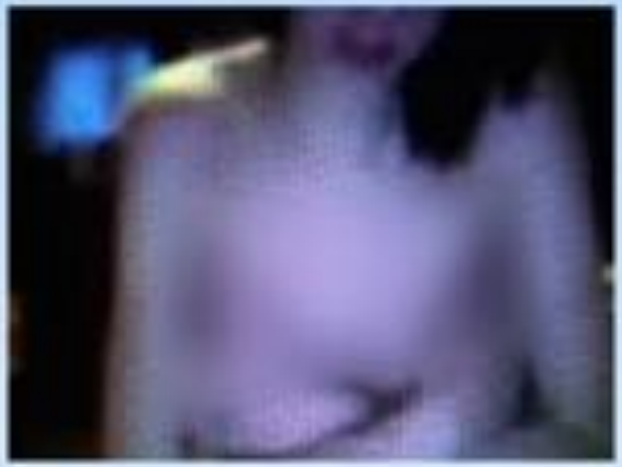
Stessa sorte per il profilo Twitter della "Jeep" dove fu sostituito con il logo della Cadillac


Per i vertici di una grande azienda è facile prendere le distanze da un bilancio falso.
Forse è facile non risultare immischiati neppure in questo...
ma in questo caso chi è il vero danneggiato?

*ulrico.bardari@unibo.it*

# Sextortion

Punti di contatto:
Social network per incontri (meetic, badoo...)
App per incontri (Tinder, Lovoo...)
Social tradizionali (Facebook, Likedin...)



CHI SONO:
Bande criminali dell'Est Europa e dell'Africa (Marocco e Costa D'Avorio) che arruolano belle ragazze e ragazzi nei loro paesi, li fanno navigare con dei profili fasulli

*Il fenomeno è conosciuto, ma non è studiato nel suo complesso*

*ulrico.bardari@unibo.it*

# Rasomware


*ulrico.bardari@unibo.it*


TIM 4G
21:23
Cerca
Post consigliato
Il trucco c'è ma non si vede
C'è chi sostiene che invecchiando si diventa più affascinanti... ma non è una regola che vale per tutti! Alcuni VIP, ad esempio, invecchiano proprio malissimo! Ecco la verità...
L'età avanza per tutti.
Belli e famosi... o solo famosi?
Mi piace
Commenta
Condividi
Juventus


TIM 4G
21:24
Messaggi
339 9942817
Dettagli
VIPRUMOR: abbonamento attivo! Costo 5,08E/sett. Partecipi al concorso vitafortuna.it Info e disattivazione al 0910651273 o su viprumor.it
Messaggio
Invia

# Rasomware Cryptolocker


- *Diffusione avviene via email*
- *Colpisce sistema operativo Windows*
- *E-mail in corretto stile grammaticale*
- *Cripta il contenuto di file word, excell e jpeg*
- *Non è possibile ripristinare il corretto funzionamento dei giochi nemmeno con una nuova installazione. I file vengono criptati con una chiave RSA a 2048 bit.*
- *Per ottenere la chiave privata necessaria alla loro decifrazione, l'utente è costretto a pagare un riscatto.*
- *La chiave viene conservata su un server e cancellata se il pagamento della somma richiesta non viene effettuato entro una certa scadenza*
- *Non è comunque garantito lo sblocco dei file.*

*ulrico.bardari@unibo.it*

# Cerber, il ransomware... parlante!

Cerber non è molto diverso dalle altre minacce e cifra con un algoritmo AES-256 i tipi di file più "importanti" per l'utente, come documenti, immagini, file audio, archivi e quant'altro, cambiando l'estensione dei file in .cerber

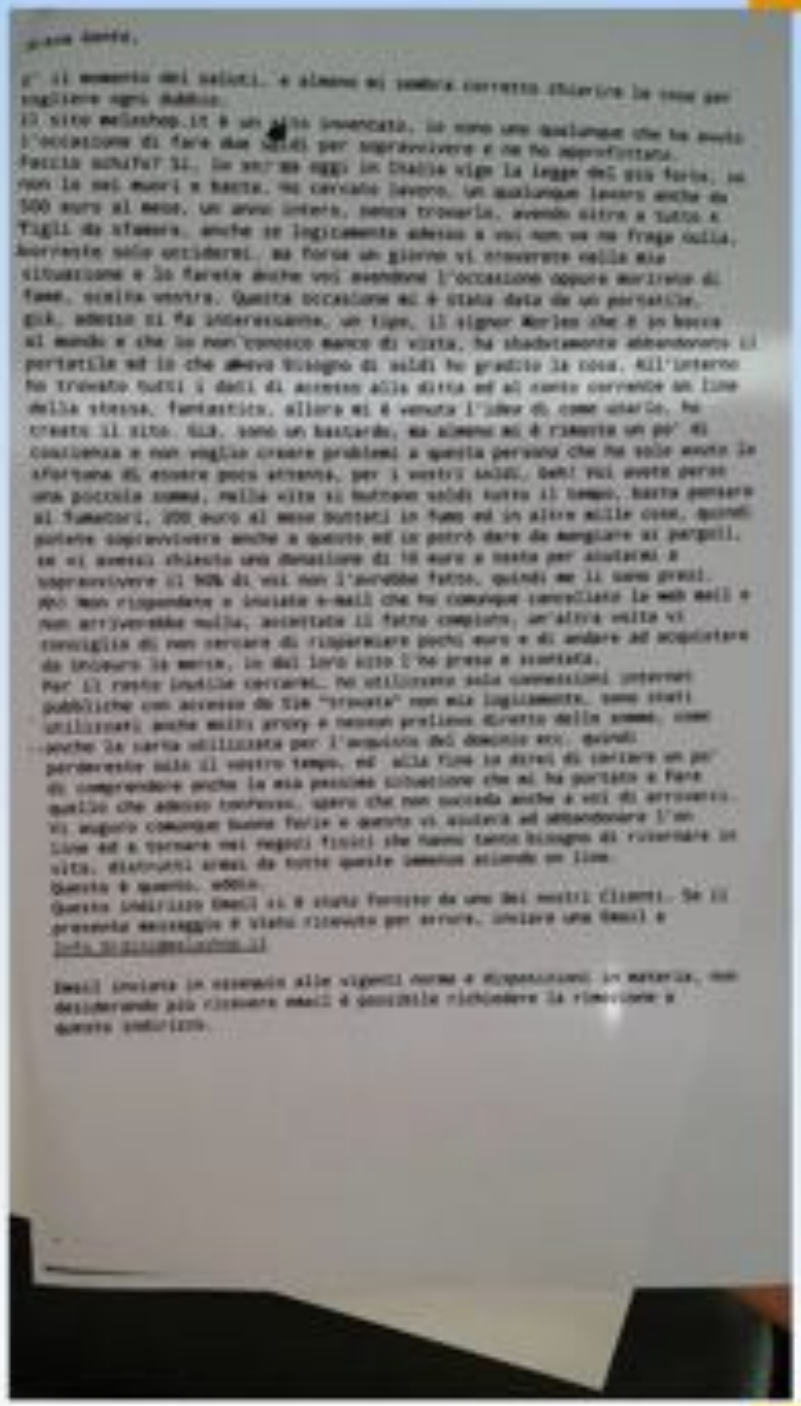
Il malware notifica all'utente, con un messaggio sonoro (text to speech) riprodotto attraverso l'audio di sistema, l'avvenuta infezione ed il conseguente blocco dei file e lo fa ripetutamente

# Money Mules (Muli del denaro)

Cioè i primi destinatari delle somme provenienti da frodi informatiche e campagne di phishing.
Dal 22 al 26 febbraio ed è stata condotta da diverse Forze di Polizia europee, con il coordinamento di Europol e con il continuo supporto di Eurojust e della Federazione Bancaria Europea (EBF) l'operazione EMMA (European Money Mules Action), ha portato all'arresto di 81 ed all'individuazione di circa 700 di questi "muli" in Europa, molti dei quali avevano collegamenti oltre oceano (Brasile, Nigeria, Qatar).
I "muli" sono elementi assolutamente indispensabili alle organizzazioni criminali dedite alle frodi informatiche, in quanto si tratta di persone che offrono la propria identità per l'apertura di conti correnti e/o carte di credito, sui quali vengono poi accreditate le somme frodate a ignari cittadini attraverso varie forme di aggressioni criminali ai sistemi di home banking e monetica. Dette somme vengono successivamente bonificate, secondo dirette e precise indicazioni, secondo cui il "money mule" trattiene una piccola parte per il "servizio" offerto, versando tutto il resto su conti nella disponibilità delle organizzazioni, aperti anche all'estero.
È stato dimostrato, ancora una volta, che la cooperazione internazionale può avere un grandissimo impatto nella lotta contro la criminalità organizzata. .

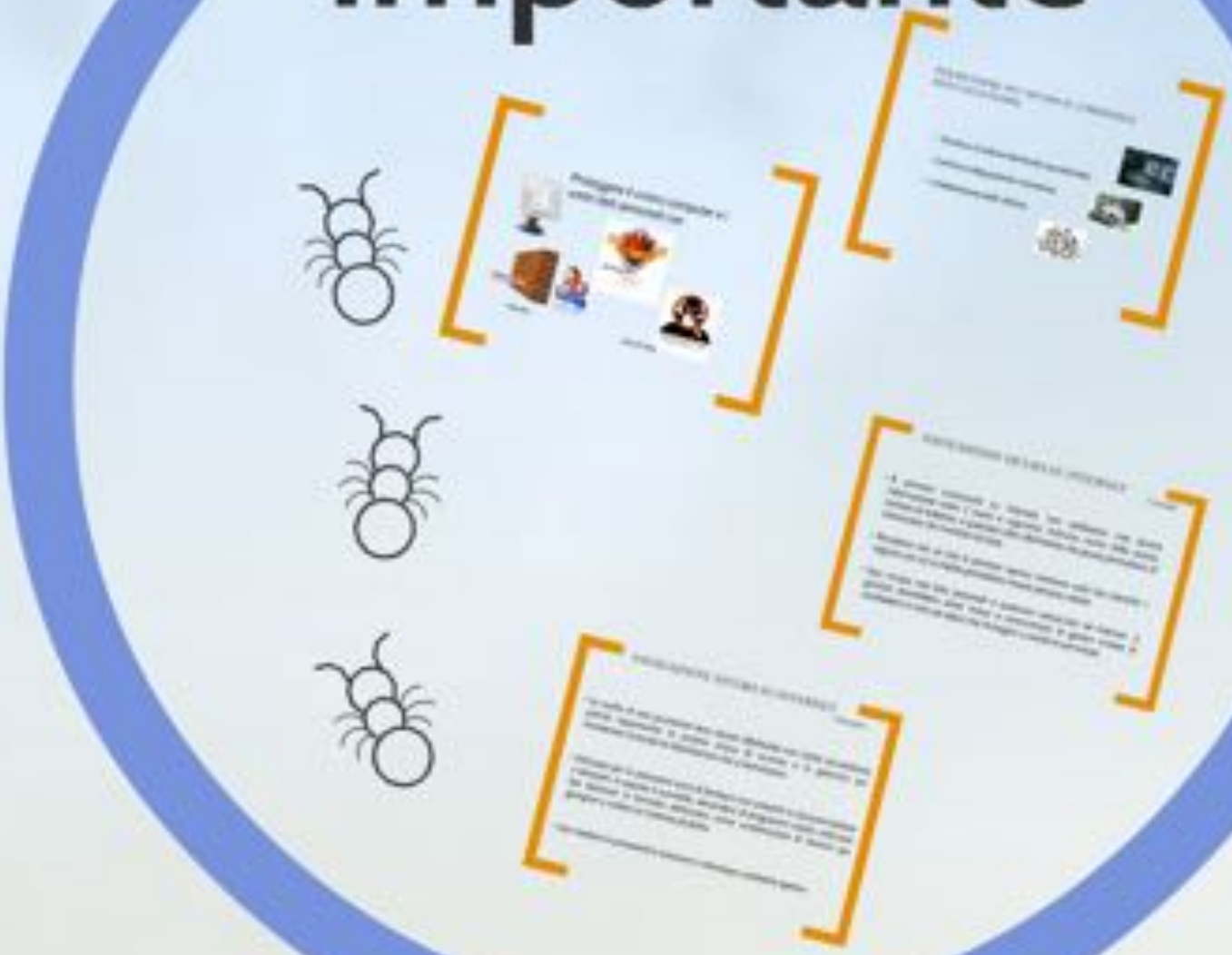
# C'è anche chi:

Questa è una mail di giustificazioni di un signore che ha fatto truffe per diverse migliaia di euro attraverso un falso sito di vendita on-line.
Dice che tutto è cominciato quando ha trovato un notebook dove ha trovato i tutti i dati del proprietario compresi i dati aziendali e di home banking.
Dice di aver dovuto "prendersi" i soldi per mantenere la propria famiglia (4 figli) e che per chi è stato truffato "200 euro al mese è come spesa di un fumatore in sigarette".



*ulrico.bardari@unibo.it*

# Importante



# Proteggere il vostro computer e i vostri dati personali con


ANTIVIRUS

FIREWALL

ANTISPYWARE

## *PER RENDERE PIU' SICURO IL CYBERSPACE SONO NECESSARIE:*

- Strutture di polizia altamente specializzate;

- Continuo adeguamento normativo;
- Collaborazione delle vittime;

# *NAVIGAZIONE SICURA SU INTERNET*

*Consigli:*

- A persone conosciute su Internet, non dobbiamo mai fornire informazioni come il nome e cognome, indirizzo, nome della scuola, numero di telefono, o qualsiasi altro riferimento che possa permettere di rintracciare chi immette tali dati.

- Ricordarsi che on line le persone spesso mentono sulla loro identità. I ragazzi con cui si chatta potrebbero essere persone adulte.

- Non inviare mai foto personali a qualcuno conosciuto via Internet (i genitori dovrebbero esser messi a conoscenza). In genere evitare di condividere in rete sia video che immagini a carattere personale.

# NAVIGAZIONE SICURA SU INTERNET

*Consigli :*

- La scelta di una password deve essere effettuata con molta accuratezza poiché rappresenta la propria chiave di accesso e la garanzia per mantenere riservate le informazioni che ci interessano.

- Utilizzare per le password nomi di fantasia non presenti in dizionari italiani e stranieri, in quanto è possibile, servendosi di programmi adatti, utilizzare tali dizionari in formato elettronico come combinazioni di termini per giungere a violare un sistema protetto.

- Non rivelare le password a nessuno e comunque cambiarle spesso.

ASSOCIAZIONE
NUOVA CIVILTÀ
DELLE MACCHINE

Forlì, 14 Marzo 2015


# Il crimine informatico: dalla criminalità organizzata al cyberbullismo

ulrico.bardari@poliziadistato.it
ulrico.bardari@unibo.it