
Corso di «INFORMATICA»

Prof. Franco Sivilli

Dott.ssa Ida Digennaro
Dott.ssa Michela Leone

a.a. 2017-2018

**CYBERCRIME, CRIMINAL
PROFILING, HACKING
GIOVANILE**

CYBERCRIMES

Attività illegali che comprendono una vasta gamma di reati, dal crimine contro dati riservati, alla violazione di contenuti e del diritto d'autore (Krone, 2005)

CYBERCRIMES

Fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica

Possono essere distinti in due macro categorie:

1. Crimini che hanno come obiettivo diretto le reti digitali e i computer ad essa connessi (virus);
2. Crimini facilitati dalle reti digitali e dai computer ad essa connessi.

CYBERCRIMES

Schneier (2000) ha distinto i crimini informatici in tre categorie:

1. Attacchi criminali propriamente intesi;
2. Attacchi non propriamente criminali;
3. Attacchi basati su sistemi legali.

CYBERCRIMES

Attacchi criminali propriamente intesi

Comprendono tutte quelle operazioni che hanno quale comune matrice la violazione di un sistema informatico allo scopo di ottenere in qualche modo, un guadagno economico;

CYBERCRIMES

Attacchi criminali propriamente intesi

- Frode informatica, consiste nell'alterare un servizio o un procedimento di elaborazione di dati con lo scopo di procurarsi un (ingiusto) profitto;
- Attacchi distruttivi, non sono perpetrati a prima istanza a fini di lucro, ma unicamente per danneggiare la proprietà altrui: dal singolo computer, reti aziendali fino a complessi sistemi di reti.

CYBERCRIMES

Attacchi criminali propriamente intesi

La differenza rispetto ad un sabotaggio fisico è data, ovviamente dal mezzo tecnologico utilizzato (virus) e dalla capacità di sfruttare le vulnerabilità del sistema informatico.

Furto d'identità, comprende sia

l'appropriazione di informazioni personali altrui (nomi e dati personali) sia l'impersonificazione totale, ovvero l'appropriazione dell'identità altrui mediante l'uso delle informazioni personali

CYBERCRIMES

Attacchi non propriamente criminali

Attacchi a scopo pubblicitario: attraverso una pubblica violazione di un sistema informatico, hanno come fine ultimo quello di provocare sufficiente disagio da richiamare l'attenzione della stampa e quindi suscitare un'eco mediatica. Spesso questo tipo di attacco ha il semplice scopo di segnalare un problema da risolvere, in genere relativo alla stessa sicurezza informatica; le conseguenze di tipo economico possono essere in molti casi rilevanti e possono causare numerosi effetti, dall'abbandono del servizio alla cattiva pubblicità.

CYBERCRIMES

Attacchi basati su sistemi legali

Attacchi che non sfruttano una debolezza del sistema informatico, ma si basano su una debolezza più generale del sistema giudiziario. Questi attacchi tentano di screditare da un punto di vista legale alcune apparenti sicurezze informatiche; lo scopo che si vuole raggiungere è molto simile agli attacchi a scopo pubblicitario.

CYBERSTALKING

- Stalking = “Sindrome del molestatore assillante” comportamenti fastidiosi o minacciosi che un individuo compie ripetutamente (pedinare una persona, innumerevoli telefonate, lasciare messaggi o oggetti inquietanti;
- Cyberstalking = indica l'uso di Internet, di caselle di posta o di altri dispositivi di comunicazione elettronica per molestare un'altra persona, una vera e propria persecuzione ossessiva, pedinamento cibernetico, in altri termini lo stalking on line;

CYBERSTALKING

- Insieme di comportamenti ripetuti ed intrusivi di sorveglianza e controllo, di ricerca di contatto e comunicazione nei confronti di una vittima che risulta infastidita e/o preoccupata da tali attenzioni e comportamenti non graditi;
- Art. 612 bis c. p. per il reato di Stalking;
- Sentenza 32404/2010 viene introdotta “*aggravante con sms, telefonate, determinando un'intrusione immediata nella sfera privata del destinatario con modifiche alle abitudini del soggetto*”

- Il Cyberstalking può risultare estremamente intimidatorio.
- Con il progredire della tecnologia è stato chiarito che gli atti persecutori possono realizzarsi anche a mezzo mail/chat in quanto gli smartphone consentono di ricevere in tempo reale (sistema notifiche) portando un'intrusione immediata (Sentenza 45332/2012)

- Sentenza di Cassazione 2011 *“È reato ingiuriare e minacciare tramite social network”*
- Legislazione molto scarna in quanto la normativa di riferimento non è tanto la condotta in quanto tale (comportamento oggettivo) quanto il danno psicologico causato alla vittima (stato soggettivo)
- Se la legge è carente nell'indicazione dei criteri oggettivi, la giurisprudenza non ignora il problema Sentenza 2011 ribadisce *“Divieto assoluto di avvicinamento ai luoghi frequentati dalla vittima”*

Cyberstalking nella vita quotidiana

Su internet, sui muri dei social network, nei commenti dei blog e dei video..

- Bombardamento di chiamate, messaggi o email offensivi;
- Diffamazione su Twitter, blog e forum aperti;
- Accesso non autorizzato agli account per scopi distruttivi;
- Accesso remoto ai dispositivi per spiare o alterare i dati;
- Registrazione dell'email altrui su siti di spam o dai contenuti offensivi
- Invio di contenuti osceno, sgradevoli o violenti
- Furto dell'identità per rovinare la reputazione della vittima

DIFENDERSI DAL CYBERSTALKING

- **Non farsi prendere dal panico:** mantenere la calma, raccogliere informazioni e osservare cosa succede senza compiere nessuna azione né rispondere. Condividere la tua situazione con una persona di fiducia: il sostegno emotivo è fondamentale;
- **Bloccare lo stalker o limitare il suo accesso:** la maggior parte delle reti sociali ha dei meccanismi per bloccare determinati utenti (ad esempio Facebook e Twitter). Le email possono essere filtrate utilizzando delle regole automatiche e anche le applicazioni di messaggistica hanno delle liste di contatti da bloccare.

DIFENDERSI DAL CYBERSTALKING

- **Proteggi il tuo PC dalle intercettazioni:** Un obiettivo tipico del cyberstalker è quello di ottenere delle informazioni su di te. Nei casi più gravi, ciò può avvenire attraverso l'accesso non autorizzato al tuo PC o al telefono. Impara a bloccare il PC e a rilevare i segni di un accesso non autorizzato.
 - **Proteggi la tua connessione WiFi:** una rete WiFi con la password di default è una porta spalancata per uno stalker, soprattutto se vive vicino a te. Pertanto, sarebbe consigliabile cambiare la configurazione di default del modem (cambia il nome della rete, usa la codifica WPA2-AES e cambia la password), usare e mantenere sempre aggiornato il firewall e spegnere il WiFi quando non lo usi.
-

DIFENDERSI DAL CYBERSTALKING

- **Imposta la privacy dei tuoi social network:** devi imparare a configurare la privacy dei tuoi profili su Facebook, Twitter, Google+ e su qualsiasi altra rete. Innanzitutto, vale la pena nascondere le cose che potrebbero essere sfruttate da un cyberstalker, come delle foto scomode, numeri di telefono o la lista degli amici.
 - **Usa password complesse e cambiale spesso:** utilizzare una password sicura e facile da memorizzare. Ricordati di cambiarla con frequenza, soprattutto dopo gli eventi significativi della tua vita, come una rottura, un divorzio o un cambio di lavoro. Non ti fidare: per quanto forte possa essere la tua password, esistono molti modi per sottrarla.
-

DIFENDERSI DAL CYBERSTALKING

- **Segnala il contenuto offensivo agli amministratori:** la maggior parte dei servizi offre la possibilità di segnalare agli amministratori il contenuto offensivo o inappropriato. Ciò non costituisce solo una possibile prova, ma permette anche l'espulsione definitiva dello stalker da determinati servizi. Puoi trovare le istruzioni nella pagina di supporto ufficiale dei vari social network (Facebook, Twitter, Gmail)
- **Installa applicazioni per bloccare chiamate e SMS:** sia Android che iPhone hanno delle applicazioni che permettono di bloccare le chiamate e i messaggi. Sono particolarmente utili per scoraggiare gli stalker telefonici, soprattutto quando l'operatore telefonico non vuole o non può aiutarti.

CYBERBULLISMO

- Si può definire cyberbullismo l'uso delle nuove tecnologie per intimidire, molestare, mettere in imbarazzo, far sentire a disagio o escludere altre persone.
- Tutto questo può avvenire utilizzando diverse modalità offerte dai nuovi media. Alcuni di essi sono:
 - Telefonate
 - Messaggi (con o senza immagini)
 - Chat sincrone
 - Social network (per esempio, Facebook)
 - Siti di giochi online
 - Forum online

CYBERBULLISMO

Le modalità specifiche con cui i ragazzi realizzano atti di cyberbullismo sono molte:

- pettegolezzi diffusi attraverso messaggi sui cellulari, mail, social network;
- postando o inoltrando informazioni, immagini o video imbarazzanti (incluse quelle false);
- rubando l'identità e il profilo di altri, o costruendone di falsi, al fine di mettere in imbarazzo o danneggiare la reputazione della vittima;
- insultando o deridendo la vittima attraverso messaggi sul cellulare, mail, social network, blog o altri media;
- facendo minacce fisiche alla vittima attraverso un qualsiasi media.

CYBERBULLISMO

Il termine cyberbullying è stato coniato nel 2006 dall'educatore Bill Belsey, distinguendo tra:

Cyberbullying (*cyberbullismo*), fenomeno che avviene tra minorenni;

Cyberharassment (“*cybermolestia*”), fenomeno che avviene tra adulti, tra un adulto e un minorenne.

CYBERBULLISMO

- Il **cyberbullo** può essere un estraneo o, più spesso, una persona conosciuta dalla vittima.
- E' possibile che metta in atto comportamenti denigratori verso la propria vittima singolarmente o, più spesso, che sia supportato da altri cyberbulli.
- L'altro elemento importante di questo tipo di bullismo è l'anonimato. Protetto da uno schermo di un computer, di un telefono cellulare o di un ipad, il cyberbullo può rivelare la propria identità o restare anonimo, protetto da un falso profilo, da un avatar, o da un nickname.
- **Le vittime** però non sono solo quelli che vengono presi di mira.
- **Le vere vittime degli atti di bullismo sono i ragazzi che non ne parlano.** Ogni volta che si preferisce il silenzio si è vittime dei cyberbullismo. E' allora importante parlarne, evitando che un primo cyberattacco possa diventare ripetuto e continuato nel tempo, finendo per provocare conseguenze anche gravi nella vittima.

CARATTERISTICHE DEL CYBERBULLISMO

- **Pervasività ed accessibilità:** il cyberbullo può raggiungere la sua vittima in qualsiasi momento e in qualsiasi luogo. La possibilità di avere i telefonini sempre accesi e spesso connessi ad internet permette al cyberbullo di attaccare la sua vittima ogni qualvolta voglia;
- **Persistenza del fenomeno:** il materiale diffamatorio pubblicato su internet può rimanere disponibile online anche per molto tempo;
- **Mancanza di feedback emotivo:** il cyberbullo, non vedendo le reazioni della sua vittima ai suoi comportamenti, non è mai totalmente consapevole del danno che arreca: questo lo rende più disinibito e abbassa i livelli di autocontrollo.

CARATTERISTICHE DEL CYBERBULLISMO

- **Spettatori:** le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate. La diffusione in rete è incontrollabile e non avviene con un gruppo di persone definito.
- **Moltiplicazione di cyberbulli:** la natura online del cyber bullismo permette che siano molti quelli che diventano cyberbulli, anche solo condividendo o promuovendo l'episodio di cyber bullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui social network) in modo indefinito.
- **Sottovalutazione:** molti adulti non comprendono la portata e la pervasività del fenomeno online.

CONSEGUENZE DEL CYBERBULLISMO

- Il cyberbullismo può essere molto dannoso per il benessere e la salute mentale dei ragazzi.
- Il cyberbullismo ha effetti negativi sul benessere sociale, su quello emotivo e su quello scolastico delle vittime.
- Il malessere per le vittime viene spesso espresso attraverso ansia, bassa concentrazione e un basso rendimento scolastico, e può sfociare in comportamenti più gravi come depressione e tentativi di suicidio, come anche recenti casi di cronaca hanno mostrato in Italia.
- Le conseguenze però coinvolgono anche i cyberbulli, che possono essere maggiormente a rischio di sviluppo di comportamenti antisociali e di problemi relazionali, delinquenza, abuso di sostanze e suicidio.

PEDO-PORNOGRAFIA ONLINE

Pedopornografia: qualsiasi rappresentazione di un minore in età prepubere in pose lascive, nudo o impegnato in atti sessuali.

Pedofilia on line: attività di produzione, diffusione e commercio sulla rete internet di materiale pedopornografico;

PEDO-PORNOGRAFIA ONLINE

Secondo la letteratura scientifica (Strano *et al*, 2006), le funzioni della pedopornografia online possono essere ricondotte a:

- gratificazione ed eccitamento (aumento della stimolazione sessuale),
- giustificazione del comportamento (ritenendolo condiviso da altre persone e come se fosse normale),
- seduzione (convincendo i minori reticenti che anche altri bambini fanno quanto loro richiesto),
- ricatto (al fine di garantire il silenzio del minore),
- profitto (vendendo le immagini).

DIFFUSIONE DEL MATERIALE

- Pedofili e child molester collezionano materiale erotico e pornografico, frutto di produzioni amatoriali, professionali o di pseudofotografie (immagini costruite o modificate al computer) consistente, principalmente, in fotografie, filmati, fumetti e web-cam dal vivo.
- La diffusione e lo scambio delle immagini avvengono attraverso l'acquisto su siti a pagamento, nelle chat line, nei newsgroup e attraverso le e-mail.

CODICE PENALE

- Art. 600 ter c.p. **“Pornografia minorile”**
Chiunque sfrutta minori degli anni diciotto al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico è punito con la reclusione da sei a dodici anni (...)
- Art. 600 quater c.p. **“Detenzione di materiale pornografico”**
Chiunque, al di fuori delle ipotesi previste nell'articolo 600-ter, consapevolmente si procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto è punito con la reclusione fino a tre anni (...)
- Art. 600 quater1 c.p. **“Pornografia virtuale”**
*Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.
 Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali*

AGGIORNAMENTO CODICE PENALE

- **La Convenzione di Lanzarote** per la protezione dei minori contro lo sfruttamento e l'abuso sessuale è finalmente **Legge 1° ottobre 2012**, n. 172 con la pubblicazione in Gazzetta Ufficiale 8 ottobre 2012, n. 235.
- Cambiano sia il codice penale che il codice di procedura penale, in particolare con **l'inserimento dell'articolo 414-bis c.p.** (Istigazione a pratiche di pedofilia e di pedopornografia) che introduce nel nostro ordinamento penale la parola **pedofilia**:
- *"Salvo che il fatto costituisca più grave reato, **chiunque**, con qualsiasi mezzo e con qualsiasi forma di espressione, **pubblicamente istiga a commettere, in danno di minorenni, uno o più delitti** previsti dagli articoli 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater e 609-quinquies **è punito con la reclusione da un anno e sei mesi a cinque anni**. Alla stessa pena soggiace anche chi pubblicamente fa l'apologia di uno o più delitti previsti dal primo comma. Non possono essere invocate, a propria scusa, ragioni o finalità di carattere artistico, letterario, storico o di costume".*

AGGIORNAMENTO CODICE PENALE

- **Art. 609-undecies. Adescamento di minorenni.**
- **"Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, **adesca un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni**. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante **l'utilizzo della rete internet o di altre reti o mezzi di comunicazione**".**

Art. 600 quater c.p. : Innovazioni della Suprema Corte di Cassazione

La condotta consistente nel procurarsi materiale pedopornografico “scaricato” (download) da un sito internet a pagamento, in quanto tale, offende la libertà sessuale e individuale dei minori coinvolti come il comportamento di chi lo produce.

In Italia costituisce reato solo la detenzione e/o il possesso di materiale pedopornografico

Cassazione penale, sez. III, sentenza 2013 n. 24808

“L’avvenuta cancellazione delle immagini pedopornografiche dai dischi rigidi del computer dell’imputato non influisce sulla permanente disponibilità delle stesse, perché ne sarebbe sempre possibile il recupero attraverso idonea procedura”

PEDO-PORNOGRAFIA ONLINE

- **Aprile 2016** - 12 denunce della Polizia Postale e delle Comunicazioni per la Liguria, al termine di una operazione internazionale di contrasto alla pornografia minorile online. L'operazione che ha coinvolto cittadini residenti tra le provincie di Milano, Como, Torino, Padova, Verona, Brescia, Palermo, Piacenza, Campobasso e Cagliari.
- Gli indagati, oltre a scambiare materiale pedopornografico utilizzando falsi profili social creati appositamente, riuscivano ad ottenere immagini intime di minori convinti di aver instaurato una chat erotica con ragazze coetanee. Grazie anche alle informazioni ottenute dal FBI è stato possibile individuare una casella di posta elettronica molto attiva nello scambio di materiale pedopornografico.
- Il responsabile è stato identificato in un 21enne genovese, utilizzatore di un account che aveva chiamato "cucciol@". Nella sua abitazione è stato sequestrato un ingente quantitativo di supporti informatici, due account e-mail ed un profilo social utilizzati per le attività illecite. Le indagini sul materiale sequestrato hanno consentito di individuare numerosi indirizzi di posta elettronica riconducibili a italiani responsabili dei reati di detenzione e diffusione di materiale pedopornografico.
- Sequestrato inoltre, un ingente numero di computer, smartphone e dispositivi digitali di memorizzazione

IL CHILD GROOMING

IL GROOMING

Tecnica psicologica utilizzata dai pedofili per adescare i minori in rete.

L'interazione che l'adulto, tramite l'uso di chat, e-mail, sms, social networks, telefonini ed in generale la rete internet, **stabilisce con un minorenne, ottenendone la fiducia allo scopo di ricevere benefici di tipo sessuale.**

Il pedofilo utilizza la rete internet anche per incontrare altri pedofili, per alimentare le sue fantasie sessuali, per rintracciare e scambiare materiale fotografico o video pedopornografici.

LA VITTIMA

Le Categorie più a rischio di adescamento, sono:

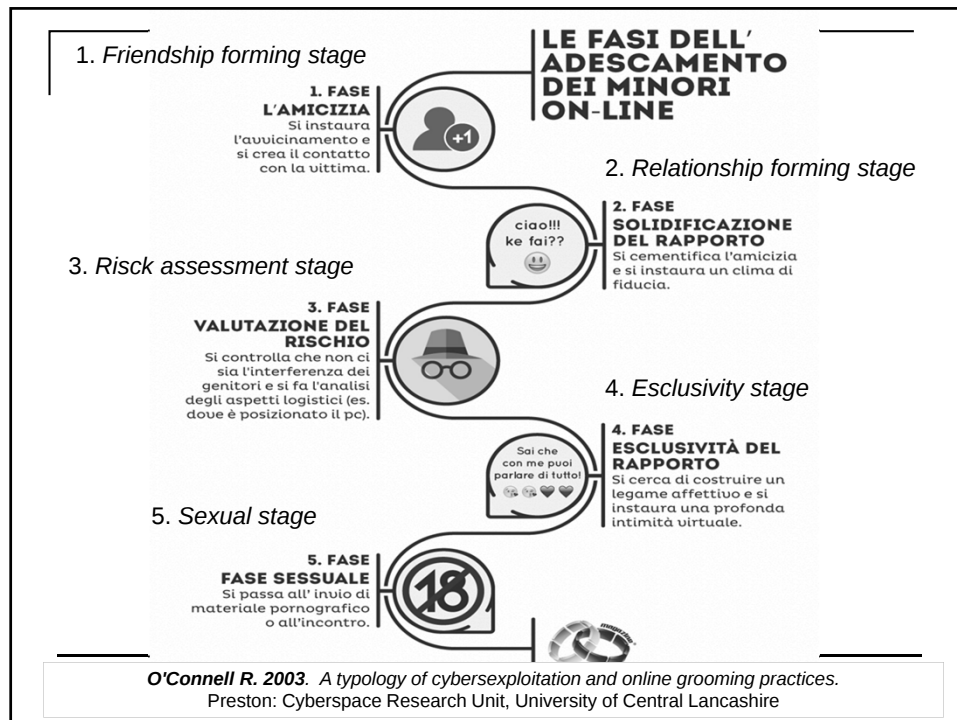
- ❖ **I BAMBINI** loquaci ed estroversi, disponibili a parlare di sé e delle proprie abitudini
- ❖ **GLI ADOLESCENTI** spinti dal desiderio di incontrare persone adulte e conoscere il mondo della sessualità

IL COMPORTAMENTO DEL CYBERPEDOFILO

Il cyberspazio consente a persone inibite nella realtà, di dare libero sfogo alle proprie perversioni; L'anonimato e il mimetismo del web offrono "sicurezza".

Comportamenti assunti dai Cyberpedofili al fine di adescare e molestare i minori:

- Raccolta dati anagrafici
- Accertamento che il minore sia solo in casa
 - Richiesta descrizione fisica e invio foto
 - Proposta argomenti e azioni sessuali
 - Tentativo di avere un contatto dal vivo



- ❖ Mezzi e forme di adescamento sono tra i più variegati in relazione alla personalità e ai comportamenti propri di ciascun pedofilo;
- ❖ Il Pedofilo avvia di norma la conversazione su tematiche banali riconducibili alla vita quotidiana del minore
- ❖ Il pedofilo è portato a mentire sulla propria età anagrafica, salvo poi rivelarla appena l'interazione con il minore si consolida e approfondisce
- ❖ Le richieste di confidenze sessuali, a volte, sono precedute da dichiarazioni di trasporto e di affectio sentimentale;
- ❖ La richiesta di immagini esplicite rappresenta il passo successivo che prelude, qualora ci sia la disponibilità del minore, alla richiesta di un appuntamento reale

TIPOLOGIE di CYBERPEDOFILI

(Bowker e Gray, 2002)

- **DABBLER**: curiosi che usufruiscono di pedopornografia;
- **PREFERENTIAL**: individui con interessi sessuali deviati che coinvolgono i minori;
- **CLUB**: individui che usano la rete per condividere con altri pedofili i suoi interessi.

PROGETTO DI RICERCA O.L.D. P.E. P.S.Y.*

On Line Detected Pedophilia Psychology

Progetto di ricerca clinica e criminologica sul fenomeno della cyberpedofilia

- Centro di Neurologia e Psicologia Medica della Polizia di Stato
- Investigatori della Polizia Postale e delle Comunicazioni

CAMPIONE: soggetti denunciati nell'arco degli anni per pedofilia (migliaia)

FILONI DI RICERCA:

1. un profilo criminologico, clinico e attinente al *modus operandi* (on-line) dei soggetti denunciati finalizzato allo sviluppo delle tecniche investigative sulla pedofilia on-line;
2. un programma di indagine e valutazione del rischio di abusi intrafamiliari tra i soggetti denunciati per scambio di materiale pedopornografico.

*Strano M., *Uno studio clinico e criminologico dei pedofili on-line, Relazione al Congresso internazionale della SOPSI* (Società Italiana di Psicopatologia), Roma, Hotel Hilton, 26 febbraio 2003.

P.C.C. Primo profilo criminologico

Analizzate le informazioni di tipo psicosociologico e criminologico all'interno dei fascicoli di soggetti denunciati (più di 1000).

DATI EMERSI:

Sesso degli indagati

Maschi 96%
Femmine 4%

Età degli indagati

10-20 anni: 3%
21-30 anni: 44%
31-40 anni: 27%
41-50 anni: 11%
51-60 anni: 14%
oltre 60 anni: 1%

Titolo di studio

licenza elementare: 0%
licenza media: 7%
licenza liceale: 65%
laurea 5%
dato non rilevabile: 23%

Stato Civile

celibe: 67%
coniugato (convivente): 29%
separato/divorziato: 1%
vedovo: 1%
convivente (non legalmente
coniugato): 1%
dato non rilevabile: 1%

Comparazione tra pedofilia classica e pedofilia on-line

soggetti che hanno solo
scambiato fotografie: 91%
soggetti coinvolti anche con
minori "dal vivo": 9%

Precedenti penali

specifici (sessuali, pedofilia): 2%
legati all'aggressività (lesioni, rissa,
omicidio): 1%
generici (altro): 5%
nessun precedente: 90%
dato non rilevabile: 2%

Il modus operandi dei pedofili on-line

La peculiarità della ricerca scientifica sul digital profiling è dovuta al fatto che il comportamento criminale telematico, **non lasciando sulla "scena del delitto" delle tracce fisiche**, rende di difficile applicazione le tecniche di profiling "classiche", basate prevalentemente sull'osservazione delle modifiche indotte dall'autore del crimine (e dalla vittima) in un determinato spazio fisico.



Realizzazione di profili criminologici digitali che si basano prevalentemente sull'analisi del loro comportamento sulla rete (specie nelle chat) in tre diverse situazioni:

- *mentre interagiscono tra loro (es. scambiandosi materiale o esperienze);*
- *mentre interagiscono con un agente sotto copertura della Polizia Postale e delle Comunicazioni che si finge un pedofilo;*
- *mentre interagiscono con un agente sotto copertura della Polizia Postale e delle Comunicazioni che si finge un bambino e si lascia molestare nella chat.*

Gli aspetti analizzati del comportamento "digitale" dei pedofili sono:

- ✓ le strategie di approccio
- ✓ le ricorrenze temporali (es. gli orari di collegamento)
- ✓ le scelte di luogo telematico (es. le chat più utilizzate)
 - ✓ la tecnologia utilizzata (hardware e software)
 - ✓ le peculiarità linguistiche e di digitazione
- ✓ il luogo da cui si connettono (l'abitazione, l'ufficio ecc.).

Orario di connessione

08-13: 9%
 13-20: 34%
 20-24: 32%
 01-08: 24%
 dato non rilevabile: 1%

Dimensione città di residenza dei pedofili on-line denunciati

0-500 abitanti: 2%
 500-5000 abitanti: 27%
 5000-100.000 abitanti: 15%
 100.000-1.000.000 abitanti: 28%
 più di 1.000.000 abitanti: 28%

Luogo di connessione

da casa: 93%
 dal luogo di lavoro: 6%
 da internet café: 1%

"TIPICO PEDOFILO SU INTERNET"

- Prevalenza sesso maschile di giovane fascia d'età (20-30 anni)
- Celibe (70% dei casi), 29% Coniugato [indice della possibilità di abusi intrafamiliari da parte dei soggetti].
- Soggetto ben integrato socialmente e che non si auto-percepisce come criminale (Incensurato 90%)
- Soggetti con titolo di studio medio-alto (Liceale 65%)
- Soggetti che risiedono in tutte le regioni italiane e vivono in centri abitati di tutte le dimensioni
- La pedopornografia viene cercata soprattutto negli orari pomeridiani e serali, al di fuori dell'ambito lavorativo e prevalentemente all'interno delle mura domestiche
- nel 10% dei casi la fruizione di pornografia è parallela al compimento di azioni più gravi rispetto al semplice scambio di fotografie (molestie, atti di libidine, tentativi di adescamento, violenze fisiche, stupri).

Pedofilia e Pornografia

I ricercatori del progetto O.L.D.PE.PSY. stanno da tempo tentando di verificare alcune ipotesi relative proprio alla modalità di fruizione della pornografia acquisita su internet da parte dei pedofili.

La ricerca vuole offrire informazioni scientifiche:

- 1. sulla modalità di fruizione del materiale pornografico da parte dei pedofili indagati** (incentivante, parallelo, o sostitutivo all'approccio fisico)



La relazione tra immagini pornografiche di minori ed eventuale incremento/decremento degli abusi sessuali da parte dei pedofili è ancora CONTROVERSA

- 2. sull'uso di internet (solo fruizione di pornografia, approccio in chat, tentativi di adescamento fuori dal web).**

IL PROFILO DEI CYBERPEDOFILI

(M. Strano, 2005)

➤ **Total No-Contact Oriented Internet Pedophile (TNOIP)**

Pedofilo "voyeuristico", centrato sulla fruizione di materiale pedopornografico (attività esclusiva) senza contatto fisico con i minori

➤ **Occasional-Contact Oriented Internet Pedophile (OOIP)**

Pedofilo caratterizzato da fruizione sistematica di materiale pedopornografico (attività prevalente) e da rari occasionali contatti con i minori

IL PROFILO DEI CYBERPEDOFILI

(Strano, 2005)

➤ **Contact-Oriented Internet Pedophile (COIP)**

Pedofilo caratterizzato da fruizione sistematica di materiale pedopornografico e comprendente frequenti e reiterati contatti fisici con i minori

➤ **Sex-abuse Oriented Pedophile (SOP)**

Pedofilo centrato sull'abuso fisico di minori, ricercato attraverso la prostituzione minorile e il turismo sessuale. La pedopornografia rappresenta un fattore di contorno.

METER*: REPORT ANNUALE 2015

- **SEGNALAZIONE DI SITI IN CRESCITA:** 9.872 siti rispetto ai 7.712 del 2014
- **L'Europa si conferma anche nel 2015 il "quartier generale" della cultura pedofila:** 51,92% delle segnalazioni (2.655)
- **10.000 SITI DENUNCIATI SOLO NEL 2015**
- **BAMBINI COINVOLTI ... DAI NEONATI AI 12-13 ANNI**
[0-3 anni FOTO (8.745), VIDEO (4.199); 4-13 anni FOTO (1.172.164), VIDEO (72.001)]
- **DEEP WEB, ULTIMA FRONTIERA ...**
- **SOCIAL NETWORK, BOOM DI SEGNALAZIONI:** dal 2011 al 2015
Vkontakte (da 34 a 107 segnalazioni), Lingbugs (da 63 ad 80), Facebook (da 32 a 66), Google+ (da 20 a 56)
- **ARCHIVI TELEMATICI, IL CLOUD AIUTA I PEDOFILI ...**

Dropbox Link (677) Foto (30.332) Video (12.634)	Box.com Link(83) Foto (50.637) Video (22.677)
iCloud Link (89) Foto (2.683) Video (3.791)	Mega Link (80) Foto (3.759) Video (3.009)

*METER: Associazione Italiana di contrasto alla pedofilia online e alla pedopornografia in convenzione con la Polizia Postale e delle Comunicazioni. Nel 2008 fonda l'OS.MO.CO.P. (Osservatorio Mondiale Contro la Pedofilia)

CONSIGLI PER UNA NAVIGAZIONE SICURA

GENITORI

- Abituare i bambini a parlare di tutto.
- Non posizionare il PC in camera dei bambini ma tenerlo in una zona centrale della casa.
- Seguire le navigazioni in Internet controllando anche la cronologia.
- Installare software di parental control (filtro e log).
- Se si sospetta che i minori siano esposti a materiale pedopornografico avvisare tempestivamente le Forze dell'Ordine.
- Leggere email evitando di aprire allegati e controllando mittente
- Stare vicini ai ragazzi quando creano nickname per chat
- Non lasciate i bimbi molte ore soli davanti al PC

BAMBINI

- Non fornire informazioni personali né inviare foto a nessuno.
- Non accettare mai appuntamenti.
- Non rispondere mai ad e-mail allusive, specie se di argomenti sessuali. Parlane con i genitori.
- Se ricevi minacce o offese avvisa subito i tuoi genitori.
- Se vuoi incontrare i tuoi amici virtuali, prendi appuntamenti in luoghi molto frequentati e fatti sempre accompagnare e non dimenticarti di avvertire i tuoi genitori su orario e luogo dell'incontro.

L'avvento dell'Information Technology ha condotto alla nascita di nuove forme criminali e al modificarsi di forme delinquenziali classiche o tradizionali.

Furto d'informazioni	vs	Pishing
Pedofilia	vs	Cyberpedofilia
Stalking	vs	Cyberstalking
Manifestazione	vs	Net-strike
Bullismo	vs	Cyberbullismo
Gioco d'azzardo	vs	On-line Gambling

L'impatto dell'information technology e i crescenti crimini informatici hanno portato al delinearsi in ambito criminologico del settore legato allo **studio del Computer Crime**.

Tale settore delinquenziale è legato all'influenza delle nuove tecnologie informatiche e telematiche sul sistema sociale e alle conseguenti risposte adattive multidimensionali.

L'impatto dell'Information Technology e del crimine informatico sull'uomo agisce su tre dimensioni interagenti tra loro:

Sociale: legata all'aumento dell'allarme politico-istituzionale e alla produzione di un **corpo normativo specifico**

Relativa alle organizzazioni: necessità da parte di aziende e istituzioni di affrontare il problema del cyberspazio attraverso prevenzione e contrasto alle azioni illegali informatiche

Individuale: Legata all'impatto dell'informatica sugli schemi cognitivi degli individui e alla sua induzione di alterazioni percettive che possono interferire sui livelli di consapevolezza dei delinquenti durante le loro azioni criminali.

ASPETTI PSICOLOGICI DEL CRIMINE INFORMATICO

(M. Strano, 2003)

Il terzo millennio rappresenta una fase di capillare diffusione di **una modalità socio-comunicativa nuova**, strettamente correlata alle tecnologie digitali.

In questa fase storica l'uomo e la sua capacità adattiva deve far fronte ad una **modifica rapida che incide sulle sue modalità percettive, cognitive e affettivo - relazionali**.

L'organizzazione delle immagini e esperienze del mondo reale comincia ad essere fortemente influenzata dalla logica digitale.

Le azioni che derivano dalle immagini costruite all'interno di un mondo digitalizzato necessitano dell'acquisizione di nuove abilità nello stile comunicativo, ma soprattutto nei processi di pensiero a cui è richiesta maggiore flessibilità e rapidità nel passaggio operativo **tra dimensione reale e virtuale**, tra una relazione mediata **da uno spazio emotivo-fisico** e quella mediata da **uno spazio emotivo-artificiale**.

La valutazione criminologica di un comportamento criminale implica la necessità di **una ricostruzione dell'influenza della dimensione digitale sulle modalità percettive del soggetto** nelle varie fasi di una azione illegale.

ALTERAZIONE NELLA PERCEZIONE DEL CRIMINE

Si rileva una certa difficoltà nell'identificare da parte dei soggetti il limite che separa la realtà dal virtuale o nella capacità di spostarsi rapidamente e con efficacia dalle interazioni digitali a quelle fisiche.

La chiave interpretativa di comportamenti disfunzionali



MODALITA' DI DISPERCEZIONE DELLE CONSEGUENZE DELLE PROPRIE AZIONI

ALTERAZIONE NELLA PERCEZIONE DEL CRIMINE

Gli uomini orientano il proprio comportamento in base ad informazioni che provengono soprattutto dall'interazione con altri individui, con le norme (giuridiche e sociali) attinenti a tale comportamento, con l'ambiente esterno e con il proprio sé.

Le azioni criminali risultano il frutto di dinamiche legate a tali processi di interazione.

“il computer si interpone tra l'autore del crimine e la vittima” alterando la percezione di gravità dell'azione criminale, la percezione della vittima, la stima dei rischi di essere scoperto o catturato.

La realtà digitale può facilitare comportamenti criminali in individui che difficilmente li attuerebbero al di fuori del cyberspazio:

- Pedofili che non avrebbero il coraggio di adescare un bambino per strada;
- Terroristi psicologicamente non adatti ad azioni militari;
- Truffatori che non reggerebbero il face-to-face;
- Donne che non avrebbero il coraggio di prostituirsi per strada;
- Impiegati scontenti che non avrebbero il coraggio di compiere azioni di sabotaggio nella propria azienda;
- Ladri di informazioni che non riuscirebbero ad introdursi in uno spazio fisico che contiene informazioni da sottrarre;
- Persone che non riuscirebbero ad insultare o molestare sessualmente nessuno senza la mediazione di email o sms.

“La rete è come un confessionale, condividi cose con le persone online che non diresti al tuo amico più intimo. Hai qualcuno con cui parlare che non conosce te, la tua famiglia e il tuo passato (...)”

Ti senti incredibilmente libero

*I rapporti sulla Rete diventano subito molto intimi, poiché puoi liberarti dai tuoi sentimenti più profondi **senza l'idea che ci saranno conseguenze.***

Ma hai lo stesso la sensazione di imbrogliare.

La colpa c'è, comunque, perché stai parlando con un estraneo invece di parlare alle persone con le quali vivi.. Corrode il tuo rapporto domestico, perché aspetti, più di ogni altra cosa, di andare online e confessarti con qualcuno là fuori (...) le persone online desiderano fortemente avere una interdipendenza con gli altri. La rete fornisce questa connessione a livello globale”

(Pensiero di un Agente di polizia)

La cybercriminologia ha condotto studi che hanno permesso di delineare il possibile “profilo” di un cyber-criminale:

- Tendenzialmente non-violento;
- **Capacità di pianificazione del comportamento** per sfruttare le opportunità dell'informatica;
- **Minori strumenti psicologici** di contenimento dell'ansia per l'assenza di contatto con la scena criminis e la vittima;
- Tendenza ad operare in solitudine;
- Tendenza ad acquisire il **know how criminale** in ambiente informatico;
- **Minore** tendenza ad **auto-concepirsi come soggetto criminale.**

LA TENDENZA AD UN AGIRE COMUNICATIVO
ATTRAVERSO I COLLEGAMENTI IN RETE
IMPLICA

**L'INSORGENZA DI PROBLEMATICHE
PERCETTIVE NUOVE** CHE INFLUENZANO IL
PROCESSO DI PERCEZIONE, VALUTAZIONE E
ATTRIBUZIONE DI SIGNIFICATO DEL
COMPORTAMENTO COSTITUENDO
**LA BASE DEL PERCORSO CHE CONDUCE GLI
INDIVIDUI DALLA FANTASIA DI UN
COMPORTAMENTO CRIMINALE ALLA
DECISIONE DI PORLO IN ESSERE,**
VIOLANDO LE LEGGI.

Computer – Criminals?

HACKER

Programmatore innovativo ed esperto di più linguaggi e sistemi operativi in grado di penetrare e scoprire i punti deboli dei più sofisticati sistemi di protezione.

Originariamente i c.d. pirati informatici erano esperti informatici che passavano il tempo, anche a scopo ricreativo, esplorando le funzionalità di programmi e sistemi operativi, con l'intenzione di perfezionarne le caratteristiche o scovare vulnerabilità.

A partire dagli anni '80 si configura negli Stati Uniti come una tipologia di criminale informatico in seguito ad un gruppo di giovani che iniziò a far uso delle proprie capacità con fini illeciti.

✓ **Hacker benevolo:** individui che non desiderano danneggiare qualcuno/qualcosa quando violano il sistema. L'attività di hacking è utilizzata dalle aziende per far testare sicurezza e affidabilità del proprio sistema.

✓ **Hacker “malevolo/cattivo”:** individui che hanno lo scopo di danneggiare o rubare informazioni nei sistemi.

CATEGORIE DI HACKER

Sulla base di diverse caratteristiche si possono distinguere:

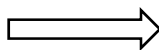
- 1. CRACKERS:** penetratori di più alto livello, larga conoscenza ed esperienza nella programmazione utilizzata per introdursi nel sistema e compiere atti vandalici per divertimento o trarne un vantaggio economico;
- 2. HACKERS:** veri e propri penetratori di livello medio; utilizzano la conoscenza e creatività per sviluppare nuovi software o individuare falle nel sistema;
- 3. RODENTS:** basso profilo di competenza; chiedono a chiunque e in pubblico aiuti di vario tipo o utilizza applicativi dei Cracker ad esempio per rubare password.

HACKING PROFILING

Campo di indagine legato ai crimini informatici e alla loro dimensione psicologica che si occupa dell'analisi e della costituzione dei profili anagrafici, socio-demografici, caratteriali e psicologici degli organizzatori di un attacco informatico.

Nello studio del mondo dell'hacking spesso gli attacchi informatici sono stati messi a confronto con i crimini delittuosi cercando di evidenziarne aspetti in comune e differenze facendo riferimento a fattori quali il modus operandi, la firma, la vittimologia ...

PROFILING



**DIGITAL
PROFILING**

ELEMENTI DI DIGITAL PROFILING

- **SIGNATURE:** “Firma” propria dell'autore del crimine, riscontrabile sulla scena del crimine o riconducibile al sospettato.

Si tratta di modelli comportamentali univoci e ripetuti:

- Es. dettagli linguistici, dettagli grafici,...

- **MODUS OPERANDI:** Modalità attraverso le quali il crimine è commesso.

- Es. sistema di penetrazione in un server, tecniche di occultamento dei log, tecniche di scansione...

ELEMENTI DI DIGITAL PROFILING

- **VITTIMOLOGIA:** Studio delle caratteristiche della vittima per ottenere l'identificazione del colpevole o dei possibili collegamenti con l'identità criminale

- Es. Reato sessuale *Quali caratteristiche in comune per le vittime?*
 Reato contro la proprietà *Quali caratteristiche sociali, economiche, lavorative in comune per i danneggiati?*

- **MOTIVAZIONE:** Elementi psicologici, economici, politici o sociali che spingono un individuo a commettere un reato

- Es. Convinzioni politiche (hacker), pulsioni sessuali (pedofilo), fattori economici (insider)

ELEMENTI DI DIGITAL PROFILING

- **FATTORI DI RISCHIO:** Possono riferirsi al livello di rischio al quale si espone l'individuo che compie l'atto criminale o al risultato della valutazione psicologica durante la fase vittimologica.
 - *Es. Il fattore di rischio per un criminale sessuale è legato a quanto è disposto ad esporsi fornendo informazioni personali alle potenziali vittime. Ciò può indicare urgenza delle pulsioni.*
- **STAGING:** Alterazione della scena del crimine o di elementi ad essa correlati.
 - *Es. Criminale informatico che tenta di far ricadere la responsabilità su un terzo*
 - *Es. Madre cancella dal computer della figlia, vittima di pedofilia, foto incriminanti per imbarazzo*

- **Il Modus Operandi** di un hacker è difficile da individuare perché le condotte sono standardizzate, utilizzate da diversi individui e non riflettono la personalità dei soggetti presi singolarmente;
- **Le strategie e metodologie di attacco** risultano differenti e rispecchiano motivazioni diverse da parte degli offenders; quelle dell'hacker si devono adattare alle caratteristiche del sistema che intendono esplorare e sfruttare;
- **La scena del crimine** dove vengono effettuati reati informatici non è un luogo fisico;
- L'analisi delle impronte digitali e delle tracce di DNA coincide con l'**analisi dei file del sistema informatico**;
- **L'arma del delitto** è lo stesso PC e il contesto coincide con il cyberspazio.

Alcuni recenti lavori hanno iniziato a spostare l'attenzione dalle competenze tecniche e dal tipo di attacco alle **dimensioni** che stanno alla base e guidano un crimine informatico.

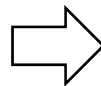
In particolare **un'accurata comprensione delle motivazioni** soggiacenti un attacco informatico e dell'utilizzo di profili psicologici degli individui permettono di **rispondere con maggiore efficacia alle intrusioni e consentono un certo grado di prevedibilità sugli attacchi futuri.**

(Beveren, 2001; Lafrance, 2004)

Perché studiare la dimensione psicologica della Motivazione?

✓ Le motivazioni attivano comportamenti specifici fornendo ***l'energia*** necessaria ad innescare e mantenere uno specifico comportamento.

✓ Le motivazioni possono rappresentare le ***componenti direzionali di orientamento*** di un comportamento verso uno specifico obiettivo



COMPRENDERE LE MOTIVAZIONI PUO':

- RESTITUIRE IL SENSO DI UN COMPORTAMENTO

- RIVELARE I VALORI DELLA PERSONA CHE LO HA MESSO IN ATTO

Marcus Rogers (1998) ha individuato 4 macro-categorie motivazionali che possono muovere le condotte di un hacker:

Curiosità

Vendetta

Notorietà

Motivazione Finanziaria

Attraverso le categorie motivazionali è possibile distinguere gli attaccanti in 5 classi:

(Y. Lafrance, 2004)

- ❖ **Attaccanti casuali** (*casual hackers*)
- ❖ **Attaccanti politici** (*political hackers*)
- ❖ **Crimine organizzato** (*organized crime*)
 - ❖ **Squatters**
 - ❖ **Insiders**

Attaccanti casuali (*casual hackers*):

Motivati solitamente dalla curiosità,
l'organizzazione di un attacco fornisce loro una
motivazione **di natura emotiva** più che
intellettiva.

Spesso sono gratificati dalla semplice
possibilità di utilizzare le sottoscrizioni altrui su
siti a pagamento.

Attaccanti politici (*political hackers*):

A differenza degli attaccanti casuali, si presentano
come **hackers militanti a favore di una causa**.

I loro attacchi, così come la loro conoscenza ed
esperienza, sono quasi sempre frutto di una loro
adesione ad un ideale.

In questa categoria è presente una **dimensione
razionale**, oltre che **emotiva**; il loro operato, si
configura spesso come una comunicazione
finalizzata a rendere pubblico il loro ideale.

Crimine organizzato (organized crime):

È costituito da attaccanti in genere professionisti ed esperti del settore.

Le **motivazioni** sono sostanzialmente di natura economica e gli attacchi scelti hanno come ultimo obiettivo il profitto.

Gli attacchi e gli obiettivi sono progettati e scelti con cura e difficilmente lasciano tracce del loro operato.

Squatters:

Sono caratterizzati dall'impersonalità dei loro attacchi.

I loro obiettivi sono spesso indipendenti dal destinatario e dall'identità del proprietario del sistema attaccato.

Spesso l'intento è quello di ottenere l'accesso a vasti database contenenti informazioni riservate, password, materiale video, musicale o immagini.

Le motivazioni spesso sono ludiche, con scopi di natura privata, non necessariamente criminale.

Insiders e Intruders:

Gli attacchi riconducibili a questa tipologia possono essere portati a termine:

- ***Insiders*** cioè ***dall'interno***, ovvero dagli operatori o utenti interni ad un'organizzazione o ad un sistema informatico
- ***Intruders*** cioè ***dall'esterno***, ovvero da attaccanti esterni come spie che si introducono illegalmente all'interno di un'organizzazione

TIPOLOGIE DI MOTIVAZIONE CHE GUIDANO INSIDERS E INTRUDERS

1. ***PROFITTO ECONOMICO***, ovvero la ricerca di un profitto atto in qualche modo a risarcire un'ingiustizia subita;
2. ***INTERESSI PRIVATI***, motivazioni che spingono ad operare contro persone sgradite nell'interesse di familiari o di persone a cui si è legati;
3. ***VENDETTA*** verso terzi;
4. ***PRESSIONI ESTERNE ALL'ORGANIZZAZIONE***, come attacchi commissionati da soggetti esterni verso parti terze

HACKING: LE PIU' GRANDI VIOLAZIONI NELLA STORIA

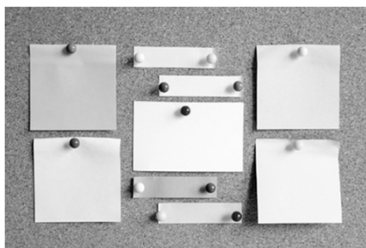


Epsilon (2011) – Stati Uniti

Sottratti dati (nomi e indirizzi di email) di milioni di persone, contenuti nei database di Epsilon, azienda americana che **forniva servizi di email marketing a migliaia di imprese** tra cui numerose banche come Barclay, JPMorgan Chase, Citi e Capital One. Questi dati vennero poi usati per campagne di phishing che miravano a impadronirsi dei veri e propri dati bancari dei destinatari.

Sony (2011) – Giappone

La PlayStation Network fu inutilizzabile per qualche giorno ... in casa dell'azienda giapponese Sony un hacker ostile si era infiltrato nella rete mettendo **a rischio circa 77 milioni di account** legati sia alla PlayStation Network sia al servizio di video e musica online Qriocity. In una seconda e successiva violazione della sicurezza furono coinvolti quasi 25 milioni di utenti registrati nei database di Sony.



Evernote (2013)

Nel 2013 Evernote comunica ai suoi clienti di aver rilevato "un tentativo organizzato di accedere alle aree protette del servizio Evernote". Gli hacker ostili **erano riusciti ad accedere alle informazioni sugli utenti: username, indirizzi email, password cifrate**. Proprio perché erano cifrate le password erano comunque protette, ma Evernote chiese a tutti i suoi utenti, per sicurezza, di sostituirle.

Adobe (2013)

Il cyber-attacco ad Adobe portò **una doppia sequenza di danni**.

- Vennero sottratti i dati di milioni di utenti: nomi, Adobe ID e soprattutto i dati delle carte di credito e debito associate ai servizi cloud di Adobe. Il numero di utenti coinvolti: Adobe ne indicò 38 milioni (all'inizio solo 2,9), altri osservatori ne stimarono circa 150 milioni.
- L'altro problema è che **gli hacker rubarono anche il codice** di alcune applicazioni Adobe.



2014 – ANNO DELLE VIOLAZIONI ALLA SICUREZZA

Target:
violare le
informazioni di **70
milioni di clienti**,
compresi dati
bancari



Apple:
Utenti (per lo più personaggi
famosi) compromessi dalla
violazione al **servizio
iCloud**. Circolarono in rete
le loro foto, comprese
alcune compromettenti.



LaCie:
Attacchi durati
quasi un anno.
Sottratti dati degli
utenti come nome,
indirizzi, email,
carte di credito,
login, password.

eBay :
Sottratti i dati di
145 milioni di
utenti eBay grazie
alle credenziali di
accesso di alcuni
ignari dipendenti.



Sony Pictures Entertainment:
migliaia di documenti finirono
online, dalle mail private con
commenti sgradevoli su attori e
registi a materiale
cinematografico.



Anthem (2015)

Furto di dati, compresi quelli sensibili, dei pazienti
dell'assicurazione sanitaria Anthem.
La violazione ha riguardato i clienti attuali di Anthem
ma anche quelli assicurati in passato
fino a 10 anni prima.

Hacking Team (2015)

Da cacciatori a prede. Violata l'azienda italiana
Hacking Team, che offriva servizi e software di
sicurezza e spionaggio. Alcuni dei loro strumenti
software sono stati usati per altre azioni di hacking
criminale.



Ashley Madison (2015)

Il gruppo Impact Team ha violato i sistemi di Avid
Media Life, l'azienda a cui fa capo il sito di incontri per
persone sposate Ashley Madison. **37 milioni gli
utenti coinvolti e a rischio di vedere esposto il
proprio tradimento.**



Hack di e-mail Comitato nazionale democratico (2016):

Le email di DNC, inclusi 19,252 messaggi di posta elettronica e 8,034 allegati da DNC, trapelate e pubblicate da WikiLeaks, che ha anche pubblicato email da account di campagna presidente John Podesta di democratici Hillary Clinton.

Violazione di Yahoo (2016):

Yahoo ha scoperto una violazione di dati che interessano 1 miliardo di utenti dando agli intrusi accesso a 500 milioni gli account senza password.



Dyn cyberattack (2016):

Un attacco informatico a Twitter, Spotify, Pinterest, Reddit e una miriade di altri siti. L'attacco è stato focalizzato su Dyn, un internet service provider che fornisce il supporto di back-end a questi siti. L'attacco ha anche causato interruzioni a CNN, GitHub, il guardiano e SoundCloud.

Cyberattack LinkedIn (2016):

Una violazione di più di 100 milioni di password e email di utenti LinkedIn.



La criminalità informatica è in espansione in tutto il mondo e anche l'Italia non è immune a tale fenomeno.

Gli incidenti colposi e gli episodi di natura dolosa aumentano costantemente e ciò ha portato gli studiosi e i professionisti ad una sorta di "ristrutturazione cognitiva".

Attualmente lo studio della criminalità informatica e la lotta al cybercrime si muove basandosi su conoscenze e competenze già acquisite in relazione a crimini simili ma commessi senza l'ausilio del computer.

In un futuro più o meno prossimo, quando il processo di adattamento alle nuove tecnologie sarà completo, non avrà più senso studiare le variabili indotte dal computer sul comportamento umano

Un giorno la telematica entrerà stabilmente nella struttura sociale, nelle organizzazioni, nell'antropologia e nella psicologia degli individui e il computer e la tecnologia digitale diventeranno elemento imprescindibile di ogni comparto della vita umana.

Allora il crimine informatico sarà semplicemente
un CRIMINE.

GRAZIE

fsivilli@unich.it