Corso di «INFORMATICA»

Prof. Franco Sivilli

Dott.ssa Michela Leone

Dott.ssa M. Ida Digennaro

Università degli studi "G. D'Annunzio" di Chieti - Pescara

A.A. 2018/2019

CYBERCRIME
CRIMINAL PROFILING
HACKING GIOVANILE

CYBERCRIMES

Fenomeni criminali che si caratterizzano nell'abuso della tecnologia informatica:

- **Reati informatici impropri** (*computer as a tool)* quando la condotta o l'oggetto materiale del crimine è correlato ad un sistema informatico o telematico.

- **Reati informatici propri** (*computer as a target)* quando l'illecito è perpetrato sfruttando o colpendo il sistema.

CYBERCRIMES

Da un punto di vista legale, è utile distinguere due sotto-categorie di condotte illecite:

Computer crimes

si riferiscono alle condotte di rilevanza penale che hanno come obiettivo primario i computer e gli altri devices elettronici (sabotaggio, virus);

Computer facilitated crimes

si realizzano attraverso l'impiego di strumenti informatici per procurare danni a individui/collettività, quali furto, appropriazione indebita, riciclaggio, clonazione di carte di credito, **cyberstalking** , diffamazione, **cyberbullismo**, pornografia, frode informatica, phishing.

CYBERCRIMES

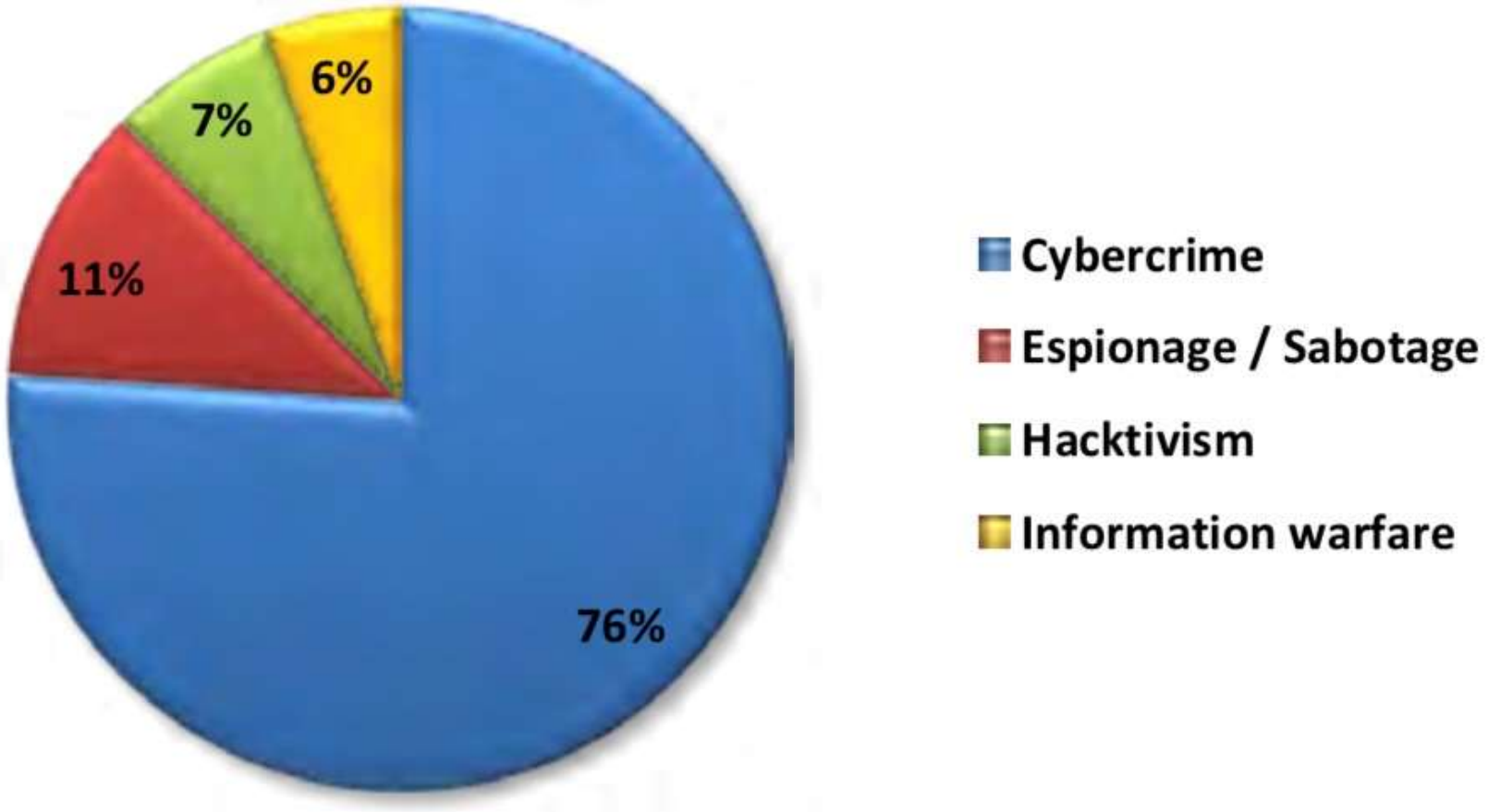
Gli autori di reati informatici agiscono, quasi sempre,
in base a due modelli:

1. individuano come obiettivo sistemi informatici di privati o istituzioni (pubbliche o private) per diffondere virus informatici o per **sottrarre, alterare e riutilizzare dati sensibili;**

2. utilizzano apparati o sottosistemi elettronici (come server, database, modem, terminali) per porre in essere reati di natura comune come **molestie, minacce, estorsioni, atti persecutori, ingiurie, compravendita di beni o servizi illeciti, scommesse illegali, reati pedopornografici**.

Rapporto Clusit 2019

Tipologia e distribuzione degli attaccanti 2017



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

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

1. Attacchi criminali propriamente intesi

Comprendono tutte quelle operazioni che comportano la violazione di un sistema informatico allo scopo di ottenere in qualche modo, un **guadagno economico**.

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.

CYBERCRIMES

1. 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, perpetrati unicamente per danneggiare la proprietà altrui e bloccare l'attività informatica di quel sistema.

- Furto d'identità (*identify theft*), comprende sia l'appropriazione di informazioni (nomi e dati personali), sia l'impersonificazione totale, ovvero l'appropriazione dell'identità altrui mediante l'uso delle informazioni personali

CYBERCRIMES

La macrocategoria delle frodi informatiche è regolamentata dall'art. 640-ter del Codice Penale, contenuto all'interno del Titolo XIII "dei delitti contro il patrimonio", Capo II "dei delitti contro il patrimonio mediante frode"

- art. 640-ter c.p. ("Frode informatica"): "***Chiunque***, *alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti,* ***procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032***.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

CYBERCRIMES

L'Associazione Italiana per la Sicurezza Informatica sulla sicurezza ICT in Italia, ha stimato che i costi generati globalmente dalle attività di **cyber crime** e dai vari reati informatici come la **frode informatica** sono stati, nel 2018, di **500 miliardi di dollari**

Per l'**Italia**, i dati a disposizione stimano che nel 2016, i danni derivanti dai **reati informatici** sono stati di circa **10 miliardi di euro**

CYBERCRIMES

2. Attacchi non propriamente criminali

- L’intento di questi attacchi non è quello di trarre profitto economico ma di suscitare l’interesse della stampa (es., grandi aziende di prodotti commerciali diffusi):

Attacchi a scopo pubblicitario: attraverso una pubblica violazione di un sistema informatico, hanno come fine ultimo quello di provocare sufficiente disagio da suscitare un’eco mediatica.

Alterazione non autorizzata di un sito web – “*Defacing*”

CYBERCRIMES

Nell’ambito della sicurezza informatica, per ***defacing*** si intende il cambiare illecitamente la home page di un sito web (la sua "faccia") o modificarne, sostituendole, una o più pagine interne.

In Italia, tale crimine si traduce in tre tipologie di reato, regolamentate dal codice penale:

- Art. 615 ter c.p. (Accesso abusivo al sistema telematico/informatico);
- Art 635 bis c.p. (Danneggiamento di sistemi informatici e telematici);
- Art. 595 c.p. (Diffamazione).

CYBERCRIMES

3. Attacchi basati su sistemi legali

Attacchi che si basano su una debolezza del sistema giudiziario.

Questi attacchi tentano di screditare da un punto di vista legale alcune apparenti sicurezze informatiche; l'obiettivo è molto simile agli attacchi a scopo pubblicitario.

La presenza e l'aumento di questi ***bug*** è direttamente proporzionale all'evolversi della rete stessa, lo scopo è quello di studiare il tipo di vulnerabilità e generare un programma (exploit) che ne sfrutti la debolezza per introdursi nel sistema e, di conseguenza, assumerne il controllo.

CYBER STALKING

PARLIAMO PRIMA DI STALKING…

Non esiste una definizione generalmente condivisa di **stalking**

Il reato di **stalking** è stato introdotto nella legislazione italiana con il D.L. 11/ 2009, poi convertito in **Legge n.38/2009**

Per potersi identificare come stalking, una condotta deve:

- essere **reiterata** (ripetuta più volte);
- produrre un **fondato timore** per la propria incolumità;
- creare compromissione nel **normale** svolgimento della quotidianità.

Non è necessario, quindi, che si verifichi un danno fisico alla salute, poiché è sufficiente che l'azione metta in pericolo

l'integrità psico-fisica del soggetto offeso.

CYBERSTALKING: Che cos'è?

Il *Cyberstalking* si riferisce a tutte quelle condotte persecutorie e vessatorie che mirano a molestare e perseguitare l'altro, attraverso l'utilizzo dei mezzi digitali di comunicazione (e-mail, messaggistica, social network,ecc.)

"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"

CYBERSTALKING NELLA VITA QUOTIDIANA

Nel *cyberstalking* appare più difficoltosa l'individuazione degli elementi costitutivi del reato.

Il *cyberstalker* agisce con diverse modalità di azione:

- invio ripetuto e incessante di chiamate, email, msg offensivi, osceni o sgradevoli (reiterazione);
- intrusione nel sistema informatico della vittima per assumerne il controllo (*trojan horses*) o danneggiarlo (*virus*);
- furto d'identità per rovinarne la reputazione (*chat*, *blog*, *forum*, *social network*).

STALKING & CYBERSTALKING

Lo stalker cerca in ogni modo di controllare la propria vittima attraverso atti intimidatori realizzati con l'ausilio di strumenti leciti e di comune utilizzo.

Pur essendo incentrato sui medesimi elementi costitutivi del reato di stalking, **il cyberstalking ne configura una forma aggravata** poiché presenta delle significative differenze:

- la molestia istantanea della vittima;
- la lontananza fisica e psicologica dalla vittima;
- maggior facilità nel mantenere l'anonimato;
- possibilità di impersonare la vittima per diffamazione.

CYBERSTALKING NELLA VITA QUOTIDIANA

C’è una percezione comune erronea sul fatto che il *cyberstalking* sia meno pericoloso dello *stalking* poiché non implica il contatto fisico.

Il *cyberstalker* decide di non confrontarsi con la vittima: **l’anonimato del cyberspazio consente al *cyberstalker* di superare le proprie inibizioni personali** e minacciare e molestare la vittima

L’anonimato rende difficile identificare anche localizzare e punire i *cyberstalkers* che, a loro volta, usano la tecnologia per eliminare e cancellare le loro tracce.

5 POSSIBILI PROFILI STALKER

- ***Il Risentito (ex patner)***. Il suo comportamento è guidato dal desiderio di vendicarsi per la rottura della relazione sentimentale;
- ***Il Bisognoso d'affetto***. Il suo comportamento è spinto dal bisogno di creare una relazione affettiva con la vittima; ogni segnale espresso viene riletto come espressione di contatto e vicinanza emotiva, che giustifica di conseguenza i suoi comportamenti;
- ***Il Corteggiatore incompetente***. Il suo inseguimento è in genere di breve durata perché, risulta inadeguato in termini relazionali, non riesce ad entrare in relazione con la vittima che, di conseguenza, si sente oppressa, "invasa" e aggredita;
- ***Il Respinto***. Spesso è stato davvero respinto dalla vittima e mira, non solo a recuperarne il rapporto, ma anche a vendicarsi;
- ***Il Predatore***. E' il più pericoloso perché solitamente è mosso dal desiderio di avere contatti di tipo sessuale con la vittima, direttamente proporzionale alle reazioni di paura di quest'ultima.

(Mullen e Purcell, 2000)

CYBERSTALKING: LA LEGGE

A livello legislativo

Non esiste il reato di cyberstalking

Per inquadrare la fattispecie giuridica del reato si fa riferimento ad un *excursus* tra i reati di molestia (art.660 c.p.), di minaccia (art.612 c.p.) e di atti persecutori (art.612-*bis* c.p. – *Stalking)*;

L'art.612-*bis* c.p., tuttavia, non contempla e non disciplina il reato di *cyberstalking*, menzionando soltanto in via generica gli "*strumenti informatici o telematici (...) da costringere lo stesso ad alterare le proprie abitudini di vita*".

CYBERSTALKING: LA LEGGE

- Sentenza 32404/2010 - viene introdotta "*aggravante con sms, telefonate, determinando un'intrusione immediata nella sfera privata del destinatario con modifiche alle abitudini del soggetto*"

- Sentenza 25488/2011 - La Cassazione ribadisce che "*anche l'invio di continui messaggi di minacce su Facebook, unitamente alle altre condotte persecutorie, integra il reato di stalking*"; "*È reato ingiuriare e minacciare tramite social network*"; "*Divieto assoluto di avvicinamento ai luoghi frequentati dalla vittima*".

- Sentenza 45332/2012 - 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*"

CYBERSTALKING: LA LEGGE

- Sentenza 36894/2015 - Il soggetto creava profili falsi della vittima su *social network* frequentati da maniaci sessuali, i quali la contattavano credendola disponibile per i propri interessi; la Corte di Cassazione definisce la "*condotta, insieme ai ripetuti episodi di minacce, persecuzioni e atti di violenza nei confronti della parte offesa che integravano senza dubbio il reato di stalking"*.

- Sentenza 1547/2018 La Corte di Cassazione ha stabilito che "*integra il reato di sostituzione di persona l'utilizzo di una foto altrui per il proprio profilo Facebook"*

CYBERSTALKING: LA LEGGE

- Sentenza 61/2019 La Corte di Cassazione ha stabilito che "*indipendentemente dall'incontro fisico il reato si configura nel momento in cui la condotta minacciosa del reo destabilizzi l'equilibrio psichico della persona offesa (…) indipendentemente dal limitato arco temporale nel quale si erano verificate*"

- **Una telefonata e 12 messaggi di WhatsApp** sono stati sufficienti ad accertare il reato (art. 612-bis c.p.)

- Le conseguenze che detti comportamenti causano alla persona offesa vengono espressamente individuate come elementi di prova (perdurante e grave stato di ansia e paura, fondato timore per la propria incolumità tale da modificare le proprie abitudini di vita).

CYBERSTALKING… e non solo

Nell'era digitale, la molestia non solo si verifica in ambiente familiare e/o lavorativo ma, grazie all'uso prolungato di internet, si è estesa anche al mondo "*cyber*" integrando il reato di cyberstalking.

- **Revenge porn -** condivisione pubblica di immagini intime, a scopo vendicativo o ritorsivo, tramite internet e senza il consenso); art. 612-ter '*chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate*' (2/4/2019)

- ***Stupro virtuale su Facebook* -** gruppi chiusi che incitano allo stupro e danno consigli su come violentare le donne, pubblicandone foto private a loro insaputa *(Blokes Avice, Babylone 2.0)*.

CONSEGUENZE NELLE VITTIME

Gargiullo e Damiani (2008) hanno riscontrato diverse psicopatologie:

- Il **Disturbo Post-Traumatico da Stress** (PTSD) conseguente a uno o più eventi di forte impatto emotivo, come ad esempio minacce di morte, gravi lesioni, atti persecutori persistenti e angoscianti.
- Il **Complex Post-Traumatic Stress Disorder** (C-PTSD) conseguente all'esposizione prolungata ad un trauma, quali abusi fisici, emozionali, sessuali e maltrattamenti ripetuti nel tempo; si tratta di un disturbo che produce in chi ne soffre perdita di sicurezza, di fiducia, di valore e di autostima, evidenti difficoltà a livello emozionale e interpersonale; difficoltà nella regolazione delle emozioni, alterazione nelle relazioni con gli altri.
- **Somatizzazione**, disturbi fisici che non hanno alcuna base organica che possa dimostrarne l'origine; in stretto rapporto con l'ansia e il grave disagio emotivo;
- **Avversione sessuale**; spesso episodi di stalking, con violenze fisiche o sessuali, portano la vittima a sviluppare un'avversione sessuale.; in particolare, il quadro psicopatologico si caratterizza per ansia, disgusto, paura, repulsione e diminuzione della libido.

COME DIFENDERSI DAL CYBERSTALKING?

- **Condividere e chiedere sostegno emotivo;**
- **Protezione della connessione WiFi;**
- **Spegnere il WiFi quando non si utilizza;**
- **Proteggere il PC da accessi non autorizzati;**
- **Impostare la privacy sui Social Network;**
- **Usare password complesse e cambiarle spesso;**
- **Segnalare contenuti offensivi agli amministratori;**
- **Installare applicazioni per bloccare chiamate e sms;**
- **Raccogliere e conservare le prove (screenshot, stampe);**
- **Denunciare alle Forze dell'Ordine (Polizia Postale);**

CYBERBULLISMO

CYBERBULLYING

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.

BULLISMO E CYBERBULLISMO

Per **bullismo** si intendono tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona.

Non un singolo atto, ma una serie di comportamenti portati avanti ripetutamente nel tempo, all'interno di un gruppo.

Queste aggressioni spesso avvengono negli ambienti di aggregazione: scuola, sport, centri sociali.

Se si limitano alla quotidianità dei ragazzi sono forme di **bullismo**.

Se, questi comportamenti si estendono anche alla vita online, si parla di **cyberbullismo**.

CYBERBULLISMO

Il **cyberbullismo** è una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali.

È una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come più debole.

Tutto questo può avvenire utilizzando:

- Telefonate
- Messaggi audio/video
- Chat/Social Network/App
- Giochi/forum online

Per insultare, offendere, minacciare, diffamare e/o ferire.

CARATTERISTICHE DEL CYBERBULLISMO

L'impatto: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online).

L'anonimato: chi offende online potrebbe rimanere nascosto dietro un nickname e cercare di non essere identificabile.

L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali (la vittima può essere raggiungibile anche a casa).

L'assenza di limiti temporali: il cyberbullismo può avvenire a qualsiasi ora.

L'assenza di empatia: non vedendo le reazioni della sua vittima alle sue aggressioni, il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni e questo ostacola ancor di più la possibilità di provare empatia, o eventualmente rimorso, per ciò che ha fatto.

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 bullismo permette che siano molti quelli che diventano cyberbulli, anche solo condividendo o promuovendo l'episodio di cyberbullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui social network) in modo indefinito.
- **Sottovalutazione del fenomeno**: molti adulti non comprendono la portata e la pervasività della situazione.

Chi è il Cyberbullo?

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**.

Tre tipologie di comportamento aggressivo:

- **Violenza fisica diretta**;
- **Aggressività verbale**;
- **Aggressività relazionale**, spesso anche indiretta, caratterizzata da violenza psicologica come diffamare, escludere, o isolare la vittima (Menesini, 2003).

LE MODALITÀ CON CUI SI REALIZZA IL CYBERBULLISMO

- 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.

DIFFUSIONE DEL FENOMENO

- Il 50% tra gli 11-17 anni ha subito un episodio offensivo di bullismo/cyberbullismo e la percentuale è maggiore al nord che al sud.
- Il 5,9% denuncia di aver ricevuto minacce/offese online;
- Il 10,4% riferisce di subire continue esclusioni/isolamento dai gruppi;
- Prevalenza di vittime di sesso maschile per quanto riguarda gli episodi di danneggiamento (13,7% di maschi contro 8,7% di femmine), minacce (7% contro 4,2%) e percosse (4,1% contro 2,5%).
- Le forme di bullismo indiretto (verbale e relazionale) sono molto più diffuse rispetto alle forme di bullismo fisico.

Le forme di prevaricazione più comunemente messe in atto sono:

- la diffusione di informazioni false/cattive sul proprio conto (25,2%),
- provocazioni e prese in giro ripetute (22,8%),
- essere ripetutamente oggetto di offese immotivate (21,6%).

Telefono Azzurro e Eurispes (2017)

Chi è la vittima?

Ipsos per Save the Children

La scelta della vittima non avviene mai a caso.

La “diversità”, nelle sue varie declinazioni, gioca un ruolo primario:

- l'aspetto estetico (67%),
- la timidezza (67%),
- il supposto orientamento sessuale (56%),
- l'essere straniero (43%),
- l'abbigliamento non convenzionale (48%),
- la bellezza femminile che 'spicca' nel gruppo (42%),
- la disabilità (31%),

Di minore importanza sono considerati orientamento politico o religioso

Chi è la vittima?

Ipsos per Save the Children

Genere femminile reagisce con tristezza e depressione;

Genere maschile invece esprime più spesso la rabbia;

(Fedeli, 2007)

Inoltre, **mentre le ragazze tendenzialmente denunciano le prepotenze subite** e, se spettatrici di episodi di bullismo perpetuati ai danni di altri, reagiscono cercando di difendere la vittima, **i ragazzi adottano più spesso un comportamento omertoso e complice**

(Sullivan, 2000)

Cyberbullismo e Salute

Conseguenze sulla vittima

Kowalski, Limber & McCord (2018)

Le vittime molto frequentemente sviluppano:

- problematiche nella regolazione emotiva,
- difficoltà di concentrazione,
- riduzione dell'autostima,
- aumento di uso di sostanze,
- depressione,
- ansia sociale,
- esclusione sociale,
- in casi estremi, suicidio.

Cyberbullismo e legge…

Conseguenze per il cyberbullo

Ad oggi, il Cyberbullismo è diventato un reato, può degenerare in azioni penalmente molto rilevanti…

Gli episodi più gravi di cyberbullismo possono sfociare in reati: come ad esempio, alcune azioni dei bulli che violano la privacy della vittima, molestie o adescamenti a fini sessuali, ma anche persecuzioni gravi e ripetute che alterano la normale vita quotidiana della vittima.

Sul piano legale…

Art. 97 Cod. Penale
Non è imputabile il minore di 14 anni, il quale tuttavia, se giudicato socialmente pericoloso, può essere sottoposto a misura di sicurezza

Art. 98 Cod. Penale
Per i minori tra i 14 e i 18 anni l'imputabilità va giudicata caso per caso dal Giudice

Art. 2043 del Cod. Civile
Oltre al reato la vittima subisce anche un danno ingiusto alla persona e alle cose

Comportamento umano	Norma del Codice Penale Violata	Pena prevista dal Codice Penale
Insulti, offese e voci diffamatorie sui social network	**Art. 594** – ingiuria **Art. 595** – diffamazione	Reclusione fino a 1 anno
Creare un profilo falso e insultare gli altri	**Art. 494** – sostituzione di persona	Reclusione fino a 1 anno
	Art. 595 – diffamazione	Reclusione fino a 1 anno (in casi gravi fino a 3 anni)
Entrare in un email o in un profilo di un social network dopo aver carpito la password di un compagno e fare delle modifiche	**Art. 615 *ter*** – accesso abusivo a sistema informatico	Reclusione fino a 3 anni (casi gravi fino a 8 anni)
	Art. 616 – violazione sottrazione o soppressione di corrispondenza	Reclusione fino a 1 anno (casi gravi fino a 3 anni)
Pubblicare su un social network, o inviare con lo smartphone, filmati o foto con atti sessuali dove sono coinvolti minori	**Art. 600 *ter*** – pornografia minorile	Reclusione fino a 5 anni
Detenere sullo smartphone o sul computer filmati o foto con atti sessuali dove sono coinvolti minori	**Art. 600 *quater*** – detenzione di materiale pornografico	Reclusione fino a 3 anni
Scattare foto ai compagni e senza il loro permesso pubblicarle sui social network	**Art. 615 *bis*** – interferenze illecite nella vita privata	Reclusione fino a 4 anni
Minacce gravi e reiterate anche a mezzo email, cellulare o social network	**Art. 612** – minaccia **Art. 612 *bis*** – atti persecutori	Reclusione fino a 4 anni

CYBERBULLISMO e LEGGE…

Legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"

Definizione: *"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo"*

La Legge a tutela dei minori che prevede misure prevalentemente a carattere educativo/rieducativo.

CYBERBULLISMO E LEGGE…

Legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"

Ammonimento da parte del questore: è stata estesa al cyberbullismo la procedura di ammonimento prevista in materia di stalking (**art. 612-bis c.p.**).
In caso di condotte di ingiuria (**art. 594 c.p.**), diffamazione (**art. 595 c.p.**), minaccia (**art. 612 c.p.**) e trattamento illecito di dati personali (**art. 167 del codice della privacy**) commessi mediante internet da **minori ultraquattordicenni nei confronti di altro minorenne**, fino a quando non è proposta querela o non è presentata denuncia è applicabile la procedura di ammonimento da parte del questore. A tal fine il questore convoca il minore, insieme ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale; gli effetti dell'ammonimento cessano al compimento della maggiore età.

CYBERBULLISMO E LEGGE…

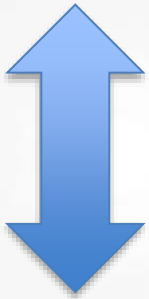
Legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"

TUTELA DEL MINORE:

Oscuramento del web: **la vittima di cyberbullismo**, che abbia compiuto almeno 14 anni, e i genitori o esercenti la responsabilità sul minore, **può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet**. Se non si provvede entro 48 ore, l'interessato può rivolgersi al Garante della Privacy che interviene direttamente entro le successive 48 ore.

PEDOFILIA E PEDOPORNOGRAFIA

PEDOPORNOGRAFIA: consiste nel **produrre**, **divulgare**, **diffondere** e **pubblicizzare**, anche per via telematica, **immagini video ritraenti minorenni coinvolti in comportamenti sessualmente espliciti**, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.



PEDOFILIA ON LINE: si riferisce al **comportamento di adulti pedofili che utilizzano la rete internet per incontrare altri pedofili** (chat, forum), 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.

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 e potere (convincendo i minori reticenti che anche altri bambini fanno quanto loro richiesto),
- profitto (vendendo le immagini).

DIFFUSIONE DEL MATERIALE PEDOPORNOGRAFICO

- Il 91% dei siti che ospitano materiale pedopornografico è di **natura non commerciale**, per cui **non finalizzati alla vendita** ma eventualmente allo scambio dello stesso;
- le vittime presenti nei contenuti foto e video pedopornografici analizzati sono di genere femminile nell'81% dei casi, e maschile nel 13% dei casi. Il restante 6% coinvolge entrambi i sessi;
- Si rileva un preoccupante abbassamento dell'età media delle vittime:
  - 7% i bambini che rientrano nella fascia della prima infanzia;
  - 72% pre-puberi (<=14anni);
  - 21% puberi (> 14 anni).

CNCPO - Centro Nazionale per il Contrasto della Pedopornografia Online (2017)

I dati del servizio 114 Emergenza Infanzia

CATEGORIE	2015	2016	2017
Immagini bambini nudi	1.1%	2.1%	1.02%
Crimini online	0.6%	2.8%	4.08%
Segnalazioni sito internet	8.6%	5.0%	6.12%
Adescamento di adulto su minore	5.7%	5.7%	6.12%
Pedo-pornografia online	5.2%	7.1%	6.12%
Sexting	5.2%	7.1%	6.12%
Abuso sessuale	69%	71.6%	70.41%

- Online, ogni 7 minuti una pagina web mostra immagini di bambini sessualmente coinvolti;
- Nel 2017 sono stati individuati 78589 URLs contenenti immagini di abuso sessuale su minori;
- Il 55% delle vittime < 10 anni;
- Nel 2018 sono pervenute 1.420 segnalazioni direttamente da minori di contenuti pedopornografici presenti sui media, 23 situazioni di incitamento alla pedofilia.

LA SITUAZIONE IN ITALIA

L'Osservatorio del Servizio Emergenza Infanzia 114 (2018):

- le vittime sono state per il 66,2% di sesso femminile;
- il 46,8% aveva meno di 10 anni;
- il 32,5% fra i 15 e i 17 anni;
- il 94,7% dei casi gestiti riguardava bambini e adolescenti di nazionalità italiana;
- la regione maggiormente coinvolta è stata il Lazio (20,3%), seguita dalla Lombardia (18,9%) e dalla Campania (14,9%).

- Per quanto riguarda l'abuso online (pedopornografia online, sexting, adescamento su minore) il presunto responsabile delle violenze è nel 37% dei casi un adulto estraneo al bambino

PEDO-PORNOGRAFIA: LA LEGGE

- 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".*

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"*

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***".

L’ADESCAMENTO DEI MINORI

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

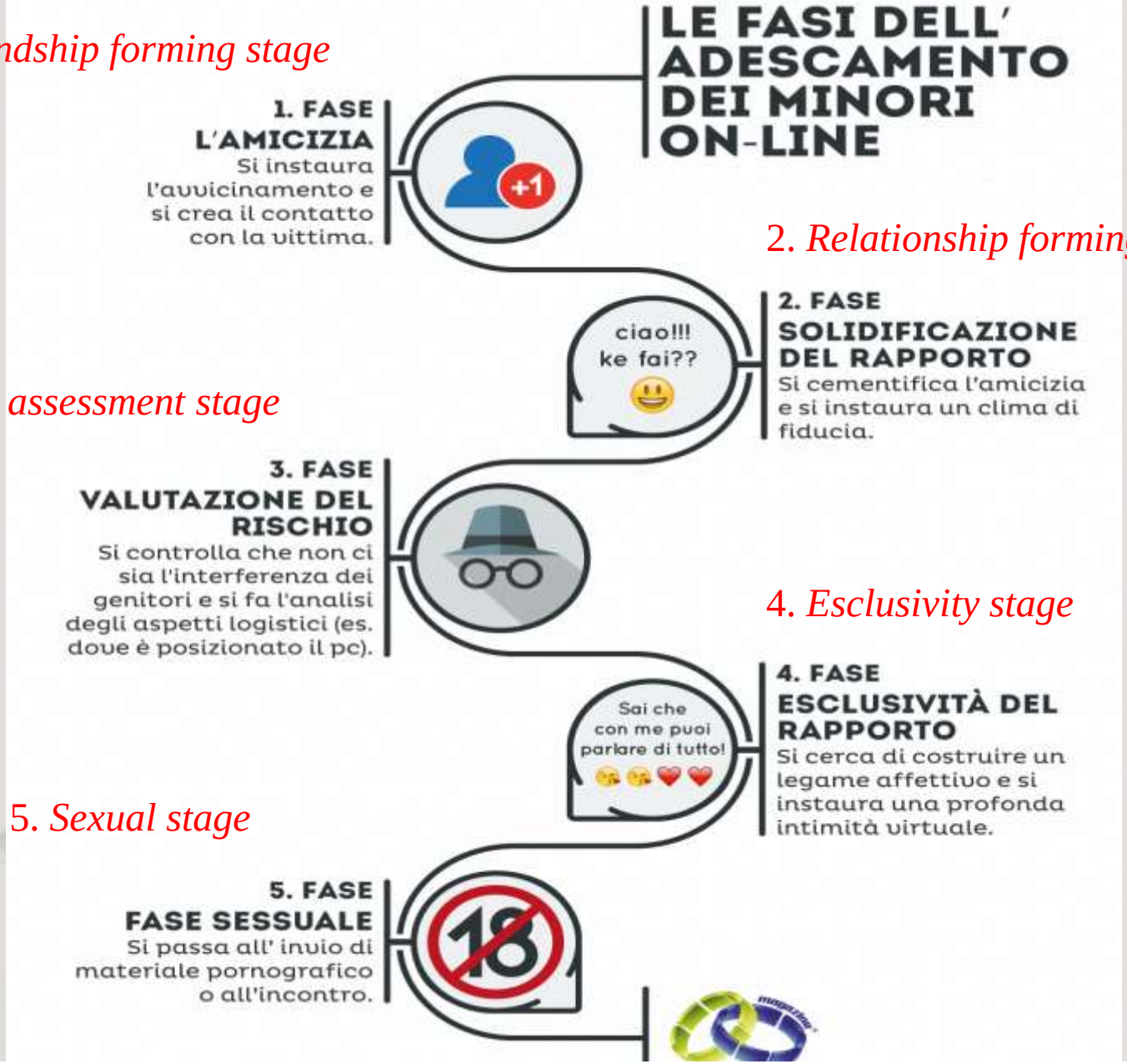
IL COMPORTAMENTO DEL CYBERPEDOFILO

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

1. *Friendship forming stage*



2. *Relationship forming stage*

3. *Risck assessment stage*

4. *Esclusivity stage*

5. *Sexual stage*

O'Connell R. 2003. *A typology of cybersexploitation and online grooming practices.* Preston: Cyberspace Research Unit, University of Central Lancashire

IL GROOMING

- 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

(M. Strano, 2005)

- ***€ontact-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 (63-80), Facebook (32-66), Google+ (20-56)

- ARCHIVI TELEMATICI, IL CLOUD AIUTA I PEDOFILI …

  Dropbox Link (677) Foto (30.332) Video (12.634)
  iCloud Link (89) Foto (2.683) Video (3.791)
  Box.com LinK(83) Foto (50.637) Video (22.677)
  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)**

- **Aprile 2016** - 12 denunce della Polizia Postale e delle Comunicazioni per la Liguria, al termine di un'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, 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

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 Tecnology 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.

ASPETTI PSICOLOGICI DEL CRIMINE INFORMATICO

(M. Strano, 2003)

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.

HACKER E DIGITAL PROFILING

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

✓**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

- **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…*

- **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,…*

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: violate 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**.

Hollywood Presbyterian Medical Center (2016)

Blocco del sistema informativo e delle attività cliniche causato dalla cifratura dei propri dati (strutturati e non strutturati). L'offensiva ha costretto l'ospedale a pagare **un riscatto di 17.000 dollari** per ottenere dai criminali la chiave di decifratura e ripristinare la propria operatività.

Hillary Clinton (2016)

Wikileaks ha pubblicato 19.252 email relative al Comitato Nazionale del Partito Democratico, ai suoi vertici e ai suoi collaboratori, alcune delle quali piuttosto compromettenti, in quanto sembrerebbero indicare che il partito abbia favorito la candidatura di Hillary Clinton sfavorendo il candidato Bernie Sanders.
La questione ha creato scandalo ed occupato i media per mesi, e probabilmente influito in qualche misura sull`esito elettorale dimostrando **la possibilità di interferire pesantemente con mezzi "cyber" nella vita democratica delle nazioni**.

Ministero degli Esteri Italiano (2016)

Attacco di matrice state-sponsored (forse originato dalla Russia), subito dalla Farnesina che avrebbe provocato **la compromissione di alcuni sistemi non classificati**.

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