KRATOS ACADEMY UNIVERSITÀ POPOLARE

ESA.ARCO CONFEDERAZIONE ESERCENTI AGRICOLTURA ARTIGIANATO COMMERCIO

ente bilaterale nazionale per la formazione - fei

TÜV SÜD

# Corso di Specializzazione II^ livello

## DIGITAL FORENSICS E I REATI INFORMATICI

## Esperto in Sicurezza Urbana, Sistemi di Videosorveglianza e Tecniche Investigative

**Prof. Salvatore Pignataro**

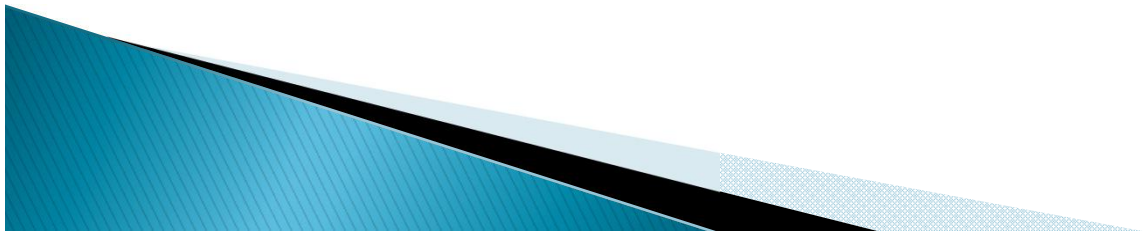
KRATOS ACADEMY
UNIVERSITÀ POPOLARE




# Digital Forensics
# Lezione

**Prof. Salvatore Pignataro**

# I REATI INFORMATICI



# COMPUTER CRIMES

Comportamenti illeciti attinenti alle scienze ed alle attività informatiche.

- Il **crimine informatico**, perciò, è una elaborazione che ha fatto ingresso in epoca piuttosto recente nel nostro sistema penale.
- Molti dei reati che oggi classifichiamo come crimine informatico esistevano prima della cosiddetta “rivoluzione telematica”, anche se in forme diverse (si pensi alle fotocopie dei libri), ma le nuove tecnologie hanno comportato una profonda modificazione nelle modalità operative e quindi nell’elemento materiale del reato stesso.

# IL LUOGO IN CUI SI CONSUMA IL REATO INFORMATICO

- L'illecito informatico, inoltre, è caratterizzato da un'elevata delocalizzazione rispetto ai reati tradizionali. E' possibile commettere un crimine, avvalendosi delle tecnologie informatiche, pur trovandosi a migliaia di chilometri di distanza dal luogo, ove il crimine produce i suoi effetti. Tutto ciò ovviamente rende più difficile l'accertamento delle responsabilità[GALDIERI P., *Internet e l'illecito penale*, in *Giur. Merito,* 1998].

- Per la **determinazione del luogo** ove è stato commesso il reato informatico, è necessario procedere all'analisi dello *spazio virtuale* nel quale si realizzano i collegamenti, i contatti e gli scambi d'informazioni tra gli elaboratori. Spesso nel perseguire tali reati occorre acquisire fonti di prova anche all'estero, con conseguente ricorso all'assistenza e rogatorie internazionali.

# National High Tech crime Unit

- A livello internazionale, la *National High Tech crime Unit,* per semplificare schematicamente ha fatto riferimento ad una duplice tipologia di *e-crime*:
- "**nuovi crimini-nuovi strumenti**", con riferimento alle nuove opportunità offerte ai criminali dallo sviluppo degli strumenti informatici o telematici, e di conseguenza nuove sfide per le Forze di Pubblica Sicurezza. (ad es. Denial of Service – che è un tipo di attacco informatico ad un server, il quale mira ad esaurirne le risorse disponibili con richieste inutili in modo che le legittime chiamate al server non ottengano risposta (la diffusione di virus e worms).
- "**vecchi crimini-nuovi strumenti**" per rappresentare crimini tradizionali supportati dall'uso di Internet e dell'alta tecnologia (ad es. frodi, estorsioni, pedofilia, furto d'identità).

# INFORMATICA E TELEMATICA

- La parola “informatica” è la *crasi* (infor/matica), che unisce le parole “informazione”; “automatica”.
- Essa indica il processo di gestione automatizzata delle informazioni, nato per ottimizzare e memorizzare tutto il lavoro che poteva essere fatto mediante un elaboratore elettronico nella gestione di informazioni complesse. Il termine telematica, invece, deriva dalla *crasi*: “informatica” e “telecomunicazioni” (tele/matica) e riguarda la gestione diffusiva delle informazioni, la loro comunicazione e la loro condivisione attraverso le reti informatiche.

# LA VULNERABILITA' DEL SISTEMA

- Con l'aumento e la capillarizzazione graduale delle macchine e delle reti, si è giunti ad un forte potenziamento dei sistemi informatici e telematici, ad una più diffusa possibilità di connessione, ad una maggiore estensione, ma per contro anche ad una accresciuta vulnerabilità degli stessi, incrementandosi così le esigenze di sicurezza.
- L'avvento di Internet, la "rete delle reti", uno spazio virtuale al servizio di finalità economiche, culturali e sociali ha determinato mutamenti in molti settori della società modificando, in particolare, l'assetto delle reti soppiantando il sistema delle reti locali chiuse.

# UN RETICOLATO INTERATTIVO

- Siamo oramai di fronte ad un reticolato interattivo, dove ogni rete interna si collega in un suo punto ad Internet non essendo pertanto più isolata.
- La prima sfida nel campo della sicurezza è quella di rendere sempre più complicato il modo per oltrepassare le difese di questo punto di contatto ed accedere così a dati non pubblici.

# LE TECNICHE DI RIMBALZO

- Non solo, ma sono state messe a punto tecniche di “rimbalzo” (*bouncing),* che permettono di accedere ai sistemi “rubando” l’altrui identità telematica. Con tali tecniche si accede ad un determinato sistema (di norma un server) per sfruttare l'indirizzo di quest'ultimo nelle successive scorrerie: chi viene attaccato per via del rimbalzo, attribuirà all’abusivo l’identità telematica di un altro utente, completamente ignaro. Solo un controllo accurato degli accessi (attraverso i file di log, cioè registrazioni di ciò che accade, e sfruttando sistemi di controllo ed identificazione degli accessi) permetterà di scoprire il vero autore dell'attacco (o quantomeno il suo precedente rimbalzo).

# HACKER

- L'hacker rappresenta lo stereotipo del "pirata" dei sistemi informatici, pertanto tale locuzione assume, nella comune accezione, una valenza del tutto negativa.
- La violazione dei sistemi rappresenta un illecito in sé, tuttavia, talvolta l'impresa dell'hacker ha soltanto finalità dimostrative delle sue capacità tecniche, altre volte invece essa persegue altre finalità criminose ulteriori.
- Assumendo questa accezione negativa, l'hacker identifica un soggetto "cyber-pericoloso" poiché attacca i sistemi telematici, accedendo a informazioni o addirittura danneggiandole.
- Nell'ottica di tracciare un profilo tipico di questi soggetti, si può utilizzare il parametro della motivazione, cioè della finalità ultima dell'attacco.

# Categorie di Hacker

- 1) ***hacker*** veri e propri, cioè quelli che in italiano definiamo pirati informatici: irrompono nei computer in primo luogo per la sfida di ottenerne l'accesso, allo scopo di dimostrare che la propria abilità consente loro di violare sistemi altamente protetti. Si traccia poi la distinzione tra gli *hacker* che operano con profonde finalità etiche quali, per esempio, dimostrare la vulnerabilità di un sistema; i *cracker*, che deturpano siti *Web* esibendosi in veri e propri atti vandalici, ed *lamer*, i quali intendono dimostrare la propria abilità per farsi accettare in un clan di *hacker*.
- 2) ***spy***, cioè le **spie**: penetrano nei sistemi, accedono alle banche dati e ne ricavano informazioni, per lo più per conseguire vantaggi in campo politico, ma non solo, dato che oggi l'informazione è una fonte di potere.
- 3) **terroristi** *(terrorist)* che accedono ai sistemi per scopi eversivi: si scambiano messaggi, svolgono delle azioni dimostrative dimostrando la loro potenza ed ingenerando così il terrore.
- 4) **predatori** *(corporate raider)*: soggetti (spesso impiegati delle aziende) che accedono alle banche dati dei concorrenti per avvantaggiarsi delle informazioni da questi detenute traendone profitti finanziari.
- La quinta categoria, è genericamente quella dei **criminali professionisti** (*professional criminal*), che sferrano i loro attacchi per trarre vantaggi finanziari e personali.
- La sesta categoria, infine, è quella dei **vandali** (*vandal*): irrompono nei *computer prima di tutto per provocare danni.*

# COME NASCE L'HACKER

- Il termine *hacker* nasce nei corridoi del Massachussets Institute of Technology negli anni '50, ad indicare fenomeni di goliardia animati da divertimento creativo ed innocuo. Veniva detto *tunnel hacker*, colui che noncurante delle porte chiuse e dei cartelli di divieto d'accesso, compiva scorrerie esplorative per i corridoi sotterranei dell'istituto, animato da spirito goliardico e curiosità.

# I Reati informatici

- crimini con finalità di profitto per l'autore e di danno per la vittima (rientrano in questo novero le azioni di appropriazione o di manipolazione di software o programmi elettronici, l'appropriazione di informazioni dai sistemi, le frodi elettroniche);
- crimini diretti contro il computer con scopi dannosi, distruttivi, di sabotaggio, di vandalismo informatico;
- crimini che mediante l'utilizzo del computer danneggiano l'individuo o la collettività (si pensi all'estorsione ai danni del singolo, oppure all'attentato ad impianti di pubblica utilità).

- Sul piano della repressione criminale la legge 23 dicembre 1993, n. 547 e più di recente la legge 18 marzo 2008, n. 48 (recettiva della convenzione di Budapest sulla criminalità informatica), hanno fornito un corpo normativo abbastanza armonico per il contrasto del crimine informatico.

- Tuttavia, andando ad analizzare la struttura di questi particolari reati occorre definire quale sia il bene giuridico tutelato dalle norme che puniscono i crimini informatici.
- Occorre cioè identificare il "**bene giuridico informatico**" per la cui tutela è stato creato quel nucleo essenziale di norme inserite nel codice penale sulla scia di un cambiamento che vede i sistemi informatici al centro delle dinamiche di comunicazione, di raccolta di informazioni e delle relazioni economiche.

- Secondo Cass. 3065/1999, il sistema informatico si configura con riferimento ad una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche solo in parte, di tecnologie informatiche.
- Questa definizione esclude dalla tutela i singoli personal computer, che assurgono a parti di un sistema informatico solo con l'impiego di periferiche per l'interconnessione anche parziale con altri sistemi elettronici.

- Una simile impostazione è stata rifiutata in dottrina con l'accusa di sottovalutare il notevole sviluppo tecnologico che oggi consente anche ai computer per uso domestico di contenere ed elaborare una notevole quantità di dati e informazioni.
- Cosicché, secondo questo particolare punto di vista, sarebbero oggetto di tutela anche i normali personal computer se dotati di potenzialità d'elaborazione di notevole portata, di una pluralità di pacchetti applicativi installati, di una notevole pluralità di informazioni immagazzinate ed elaborate.

- Per definire l'oggetto materiale dei reati di cui trattasi dobbiamo, infine, fare cenno al concetto di **sistema telematico**.
- Siamo di fronte ad un tale sistema quando sussiste un insieme combinato di apparecchiature capaci di trasmettere a distanza dati ed informazioni, con l'impiego di tecnologie deputate alla telecomunicazione. Occorre cioè che la connessione tra gli elaboratori sia di natura stabile o permanente e che lo scambio di informazioni avvenga necessariamente per il tramite del sistema interconnesso.
- La tendenza ad una convergenza tecnologica multimediale ed interattiva, cioè l'abbandono delle reti dedicate per accedere alla rete mondiale, peraltro, si traduce in una maggiore vulnerabilità

# Luogo in cui è commesso reato

- Il reato si consuma non al momento della diffusione del messaggio offensivo, ma al momento della percezione dello stesso da parte di soggetti che siano «terzi» rispetto all'agente ed alla persona offesa. Sul punto, ha avuto modo di pronunziarsi, sia pure implicitamente, la giurisprudenza di legittimità (Asn 199908118 – Rv 214128; Asn 199202883 – Rv 189928; Asn 198100847 – Rv 147558; Asn 198100847 – Rv 147405).

- 635-bis. cod. pen. - *«Danneggiamento di informazioni, dati e programmi informatici.*
- *Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
- *Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede*

- 635-ter. cod. pen. - *«Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità».*
- *Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*
- *Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.*
- *Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

- 635-quinquies. *«Danneggiamento di sistemi informatici o telematici di pubblica utilità».*
- *Se il fatto di cui all'art. 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*
- *Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.*
- *Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

- *615 quater. Cod. pen. «Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici».*
- *Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.*
- *La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617*

# TIPOLOGIE FREQUENTI DI CRIMINI INIFORMATICI

# 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)

Fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica

Possono essere distinti in:

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.

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.

## 1. 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

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.

## 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, 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.

## 2. Attacchi non propriamente criminali

- Attacchi a scopo pubblicitario: attraverso una 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.

## 3. 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

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 online**

**<u>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</u>**

# 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

# 5 POSSIBILI PROFILI STALKER

- ***Il Risentito***. Il suo comportamento è guidato dal desiderio di vendicarsi per un torto subito;
- ***Il Bisognoso d'affetto***. Il suo comportamento mira a convertire un ordinario rapporto di quotidianità in una relazione amorosa e la sua insistenza nasce dalla convinzione che prima o poi l'oggetto delle sue attenzioni capitolerà;
- ***Il Corteggiatore incompetente***. Il suo inseguimento è in genere di breve durata perché si tratta per lo più di un soggetto incapace di avere relazioni soddisfacenti;
- ***Il Respinto***. E' molto pericoloso perché di solito è stato davvero respinto dalla vittima e ciò a cui mira è non solo il recupero della rapporto con la stessa, ma anche vendicarsi;
- ***Il Predatore***. E' il più pericoloso perché il suo fine è solo a sfondo sessuale. Il suo comportamento mira ad inseguire delle vittime indifese e spaventarle poiché dalla loro paura ottiene eccitazione e gli fa provare un certo senso di onnipotenza.

# CYBERSTALKING: LA LEGGE

- 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*"

- 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*"

- **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**;**

- **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 e cambia la password), usare e mantenere sempre aggiornato il firewall e spegnere il WiFi quando non lo usi.

# COME DIFENDERSI DAL CYBERSTALKING?

- **<u>Segnala il contenuto offensivo agli amministratori</u>**: 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)

- **<u>Installa applicazioni per bloccare chiamate e SMS</u>**: sia Android che iPhone hanno delle applicazioni che permettono di bloccare le chiamate e i messaggi.

KRATOS ACADEMY
UNIVERSITÀ POPOLARE

ESA.ARCO CONFEDERAZIONE
ESERCENTI AGRICOLTURA ARTIGIANATO COMMERCIO

ente paritetico bilaterale nazionale per la formazione

TÜV SÜD

# Ferire con un click

Cognome Nome docente

# 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.

FENOMENO CHE AVVIENE TRA I **MINORENNI** ED IMPLICA **L'USO DELLE NUOVE TECNOLOGIE PER INTIMORIRE, MOLESTARE, METTERE IN IMBARAZZO, FAR SENTIRE A DISAGIO O ESCLUDERE ALTRE PERSONE**.

Tutto questo può avvenire utilizzando:

- Telefonate
- Messaggi (con o senza immagini)
- Chat sincrone
- Social network (per esempio, Facebook)
- Siti di giochi online
- Forum online

**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".*

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'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.

- 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.

# Chi è la vittima?

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

- **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**: molti adulti non comprendono la portata e la pervasività del fenomeno online.

# 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).

- 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.

# 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.

**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

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 |

# ASPETTI PSICOLOGICI DEL CRIMINE INFORMATICO

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.

# 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 <u>la percezione di gravità dell'azione criminale, la percezione della vittima, la stima dei rischi di essere scoperto o catturato</u>.**

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.

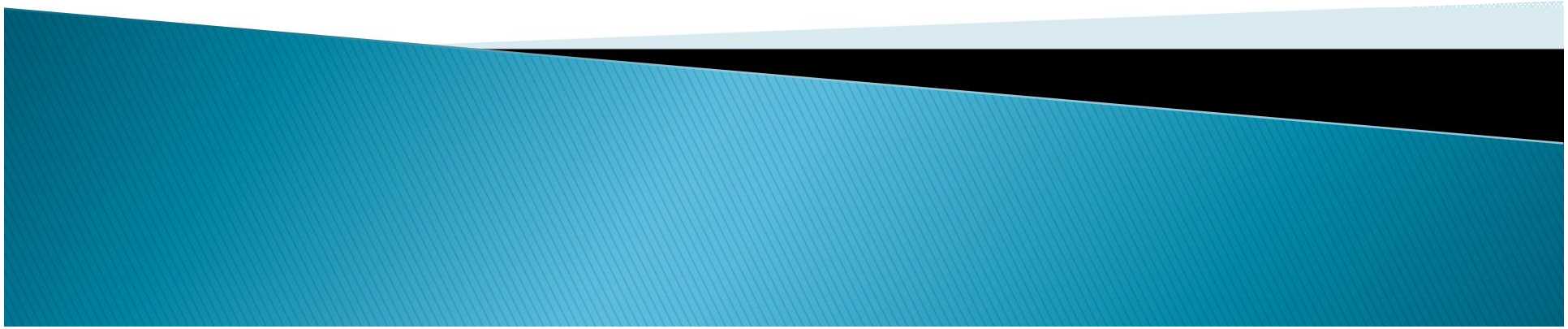



# SONO STATE AFFRONTATE LE DEFINIZIONI DI CYBERCRIMES, CYBERBULLISMO, GROOMING ECC.

Cognome Nome docente

# Digital Forensics
## Lezione 7

Prof. Salvatore Pignataro



- Criminologia e Criminalistica

# CYBERCRIME, PRIMINAL PROFILING HAKING GIOVANILE (approfondimenti)

# CYBERCRIMES

Attività illegali che comprendono una vasta gamma di reati, dal crimine contro dati riservati, alla violazione di contenuti e del diritto d'autore.
Fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica

Possono essere distinti in:

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.

# CYBERSTALKING: Che cos'è?

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 online**

**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

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

# COME 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**;**

- **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 e cambia la password), usare e mantenere sempre aggiornato il firewall e spegnere il WiFi quando non lo usi.

**Le vittime molto frequentemente sviluppano**

difficoltà di concentrazione;
ritiro dalla vita sociale (scolastica e personale);
ansia;
aggressività;
depressione;
nei casi peggiori il suicidio.

# Cyberbullismo e legge…

## Conseguenze per il cyberbullo

Il Cyberbullismo non è un reato, tuttavia può degenerare in azioni penalmente 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<br>**Art. 595** – diffamazione | Reclusione fino a 1 anno |
| Creare un profilo falso e insultare gli altri | **Art. 494** – sostituzione di persona<br><br>**Art. 595** – diffamazione | Reclusione fino a 1 anno<br><br>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<br><br>**Art. 616** – violazione sottrazione o soppressione di corrispondenza | Reclusione fino a 3 anni (casi gravi fino a 8 anni)<br><br>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<br>**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"

**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.

# L’ADESCAMENTO DEI MINORI

Cognome Nome docente

# ADESCAMENTO DEI MINORI NELLA RETE

**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 PEDOPORNOGRAFICO

- 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.

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


Cognome Nome docente

# 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