Corso di «Psicologia della salute, vecchie e nuove dipendenze»

Prof. Franco Sivilli
Dott.ssa Ida Di Gennaro
Dott.ssa Michela Leone

a.a. 2016-2017

CYBERCRIME, CRIMINAL PROFILING, HACKING GIOVANILE

CYBERCRIMES

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

CYBERCRIMES

Fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica

Possono essere distinti in due macro categorie:

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

CYBERCRIMES

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

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

CYBERCRIMES

Attacchi criminali propriamente intesi

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

CYBERCRIMES

Attacchi criminali propriamente intesi

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

CYBERCRIMES

Attacchi criminali propriamente intesi

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

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

CYBERCRIMES

Attacchi non propriamente criminali

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

CYBERCRIMES

Attacchi basati su sistemi legali

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

EVOLUZIONE

L'espansione dell'informatizzazione sia nel settore pubblico sia privato è un fenomeno in continua espansione che oltre ad avere i suoi evidenti benefici comporta anche dei costi in termini di sicurezza e vulnerabilità.

Fu per primo il Consiglio d'Europa "*Raccomandazioni sulla criminalità informatica*" (1989) a regolamentare la disciplina penale dei reati informatici, elaborando una doppia tipologia di crimini informatici, redigendo due liste diverse, una lista minima ed una facoltativa.

Le due liste furono poi unificate e, nel 1994, ulteriormente integrate.

NORMATIVA RECENTE

- LEGGE 06.02.2006 N. 38 (Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet)
- LEGGE 18.03.2008 N. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, norme di adeguamento dell'ordinamento interno, Budapest, 23 novembre 2001)
- CONVENZIONE CYBERCRIME 2001

Convenzione di Budapest sulla criminalità informatica.

- La **Convenzione**, firmata nel 2001 ed articolata in 4 capitoli, è entrata in vigore il 1° luglio 2004 con l'obiettivo di realizzare una politica Europea comune in grado di coordinare e rendere più efficace la **lotta ai crimini informatici**;
- la Convenzione tende ad **armonizzare i reati** legati alla criminalità informatica, a dotare i Paesi firmatari degli **strumenti adeguati** allo svolgimento delle indagini e al perseguimento dei crimini correlati all'area informatica e a costruire, infine, un **efficace regime di cooperazione internazionale**, che dovrà essere:

  a) fornita nella misura più ampia possibile;

  b) estesa a tutti i reati relativi ai sistemi e ai dati informatizzati;

  c) conforme agli accordi internazionali in materia.

- La Convenzione, realizzata da un Comitato di esperti in circa 4 anni di lavoro, è di fatto il primo accordo internazionale a inquadrare i crimini legati a internet e alle reti informatiche e ad estendere la portata dei reati informatici a *"…tutti i reati in qualunque modo commessi mediante un sistema informatico, anche nel caso in cui la prova del reato sia sotto forma elettronica".*

- Molti di questi temi - la frode informatica, l'accesso illecito ai sistemi informatici, la pedopornografia, le intercettazioni di dati telematici - sono in gran parte già contemplati dalla legislazione italiana, ma dovranno essere introdotte importanti modifiche al **D. Lgs. 231/2001** sulla responsabilità amministrativa delle persone giuridiche e al **Codice della Privacy**.

- Disposizioni decisamente più rigide sono infatti introdotte riguardo la **responsabilità amministrativa** per i cyber-reati: le imprese che non attuino **misure di prevenzione** dei crimini informatici commessi dal loro organico andranno incontro a gravi sanzioni di responsabilità patrimoniale.
- Inoltre la Convenzione prevede un'estensione del **potere delle forze dell'ordine nel reperimento dei dati presso gli operatori**: questi ultimi possono essere costretti a conservare e proteggere i dati relativi al traffico telematico per 6 mesi e sono tenuti al rilascio immediato delle informazioni e al mantenimento del segreto sugli ordini ricevuti pena sanzioni detentive fino a 3 anni di carcere

- Lo studio del computer crime è un nuovo settore della criminologia dove si evidenziano rapidi e continui cambiamenti di scenario e dove sembra manifestarsi con più insistenza, l'esigenza di analizzare nuove forme criminali indotte dal computer;

- Queste nuove forme criminali sono legate all'influenza delle nuove tecnologie informatiche e telematiche sul sistema sociale e alle conseguenti risposte multidimensionali- adattive

- Truffe e frodi vs Sniffing e Spoofing
- Pedofilia vs Cyberpedofilia
- Proselitismo delle sette sataniche vs Diffusione on-line
- Manifestazione vs Net-strike
- Gioco d'azzardo vs On-line Gambling

ALTERAZIONE NELLA PERCEZIONE DEL CRIMINE

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

- L'essere umano moderno necessita l'acquisizione di nuove abilità nello stile comunicativo
- Nei processi di pensiero è chiesta sempre maggiore flessibilità e rapidità nel passaggio operativo tra dimensione reale e dimensione virtuale, tra una relazione mediata da uno spazio **emotivo-fisico** a una relazione mediata da uno spazio **emotivo-artificiale**

- La valutazione criminologica di un comportamento criminale implica quindi la necessità di una ricostruzione dell ’ influenza della dimensione digitale sulla modalità percettiva del soggetto nelle varie fasi dell’ azione criminale/illegale.
- La chiave interpretativa di eventuali comportamenti disfunzionali di interesse criminologico, nelle modalità di percezione delle conseguenze delle proprie azioni, è racchiusa nella capacità dell ’ individuo di spostarsi rapidamente e con efficacia tra le interazioni digitali e quelle fisiche

CRIMINI INFORMATICI

- Il computer può essere il bersaglio del crimine;
- l'utente del computer può essere la vittima del crimine;
- l'informazione contenuta nel computer può essere l'obiettivo.

I CRIMINI INFORMATICI VENGONO DIVISI IN 4 CATEGORIE.

- Il computer preso come bersaglio;
- L’utente del computer come bersaglio;
- Le associazioni per delinquere;
- Minacce via internet.

- Le azioni criminali sono il frutto di dinamiche complesse, strettamente legate ai processi di interazione dell'autore con le norme sia penali sia sociali;
- I crimini vengono costruiti, elaborati attraverso un processo di pensiero che si basa sull'anticipazione degli effetti del proprio comportamento;
- Nel crimine informatico, il PC si interpone tra l'autore e la vittima o comunque rappresenta lo strumento principale per porre in essere una determinata azione criminale

Alcune forme criminali tradizionali sono rese più efficaci dalla telematica:

- comunicazione e organizzazione dei terroristi;
- comunicazione, organizzazione e attività della criminalità organizzata (es. riciclaggio);
- pedofilia organizzata;
- spionaggio industriale.

ASPETTI PSICOLOGICI DEL CRIMINE INFORMATICO

L'utilizzo dell'informatica nelle azioni criminali sembra produrre nuovi profili di personalità di delinquenti, rendendo "adatti al crimine" soggetti diversi dai crimini tradizionali.

ASPETTI PSICOLOGICI DEL CRIMINE INFORMATICO

La cybercriminologia ha condotto studi che hanno permesso di delineare alcuni "profili" tipici del cybercriminale:

- 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;
- Minore tendenza ad autoconcepirsi come soggetto criminale.

L’information technology può generare in alcuni individui,delle alterazioni della percezione del crimine, facilitando comportamenti criminali che difficilmente attuerebbero fuori dal cyberspazio,come ad es.:

- 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 nessun 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)

CYBERSTALKING

Il Cyberstalking può essere definito come un pedinamento cibernetico, in altri termini lo stalking on line;

- Il termine denota l'uso della tecnologia, in particolare internet, per molestare una persona. Fra le caratteristiche comuni vi sono false accuse, monitoraggio, minacce, furto d'identità,distruzione o manipolazione di dati;
- Insieme di comportamenti ripetuti ed intrusivi di sorveglianza e controllo, di ricerca di contatto e comunicazione nei confronti di una vittima che risulta infastidita e/o preoccupata da tali attenzioni e comportamenti non graditi;
- Art. 612 bis c. p. per il reato di Stalking

Il Cyberstalking può risultare estremamente intimidatorio.

Le molestie possono assumere varie forme, ma il comun denominatore è dato dal fatto che sono indesiderate, spesso ossessive e solitamente illegali.

I cyberstalker usano mail, msg, telefonate e altri dispositivi di comunicazione per compiere atti di stalking che possono assumere la forma di molestie sessuali, contatti inappropriati o semplicemente attenzione molesta nei confronti della quotidianità di una persona.

Da quanto internet è divenuto strumento di comunicazione tra persone usato in tutto il mondo hanno iniziato a manifestarsi ,con sempre maggiore frequenza,casi di minacce, intimidazione, di molestie e di persecuzione attuati attraverso i servizi classici della rete: e-mail, chat, social network.

In alcuni casi la caccia si può trasferire nel mondo fisico, dove avviene la vera violenza interpersonale(stalking).

- Tipologia di molestatore: uomo, 25 anni
- Vittima: donna, 35 anni
- Utilizzo primario: e-mail come strumento di stalking
- Relatizzazione pagine web, messaggi intimidatori indirizzati alla vittima
- Diffusione di informazioni private e riservate della vittima

DIFENDERSI DAL CYBERSTALKING

- Il contrasto risulta a volte difficile a causa delle numerose opportunità di anonimato offerte dalla rete.
- Fondamentale in tal caso è una stretta collaborazione tra i fornitori di servizi e organi investigativi.
- Per difendersi dalla molestia è di fondamentale importanza chiarire subito che il comportamento dello stalker non è gradito con una comunicazione con tono educato ma fermo ed inequivocabile.
- Se la molestia continua evitare di rispondere aspettando che questo smetta.
- Conservare tutte le e-mail ricevute e copia di eventuali pagine web offensive o minacciose (con relativa URL)

CYBERBULLISMO

Il Cyberbullismo (*bullismo online*) è il termine che indica atti di bullismo e di molestia effettuati attraverso mezzi elettronici come e-mail, messaggi, blog, cellulari, siti web.

Il termine cyberbullying è stato coniato nel2006 dall'educatore Bill Belsey, distinguendo tra:

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

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

CYBERBULLISMO

L ' utilizzo dei mezzi informatici,conferisce al Cyberbullismo alcune caratteristiche proprie:

- *Anonimato del molestatore*: un anonimato illusorio, dove ogni comunicazione elettronica lascia pur sempre delle tracce;

- *Difficile reperibilità*: se il cyberbullismo avviene via sms, email o forum online privato, è più difficile reperirlo o porvi rimedio.

CYBERBULLISMO

- *Indebolimento delle remore etiche*: l'anonimato e la difficile reperibilità, insieme alla possibilità di essere un' "altra" persona online, possono indebolire le remore etiche, considerando che un individuo non farebbe/direbbe nella vita reale;

- *Assenza di limiti spaziotemporali*: a differenza del bullismo tradizionale che avviene in luoghi e momenti specifici (contesto scolastico), il cyberbullismo investe la vittima ogni volta che è collegata al mezzo informatico utilizzato dal cyberbullo.

TIPOLOGIE DI CYBERBULLISMO

- *Flaming*: messaggi online violenti e volgari mirati a suscitare scontri verbali in un forum;
- *Molestie (harassment*): spedizione ripetuta di msg insultanti mirati a ferire qualcuno;
- *Denigrazione*: sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione, via email, sms, gruppi su social network;
- *Rivelazioni (exposure)*: pubblicare informazioni private e/o imbarazzanti su un'altra persona;

TIPOLOGIE DI CYBERBULLISMO

- *Inganno (trickery)*: ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri, le informazioni ottenute;

- *Esclusione*: escludere deliberatamente una persona da un gruppo online per provocare in essa sentimenti di emarginazione;

- *Cyberpersecuzione (cyberstalking):* molestie o denigrazioni ripetute e minacciose mirate ad incutere paura

PEDO-PORNOGRAFIA ONLINE

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

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

PEDO-PORNOGRAFIA ONLINE

- La rete mette in connessione pedofili di tutto il mondo, consentendo a molti di essi di soddisfare la loro parafilia dalla propria postazione telematica.
- Presso il Ministero dell'Interno costituito il Centro Nazionale per il monitoraggio della pornografia minorile su Internet, con il compito di raccogliere segnalazioni, anche provenienti dall'estero, sull'andamento del fenomeno su rete.

DIFFUSIONE DEL MATERIALE

- Chat line: materiale di produzione amatoriale;
- Sistemi *peer-to-peer*: attività di condivisione e scambio di materiali pedofili, interconnessioni tra gli utenti senza mediazioni;
- Siti web ad accesso libero, con iscrizione o a pagamento, aperti a tutti gli utenti o ad una ristretta comunità di individui.

CODICE PENALE

- Art. 600 ter c.p.“**Pornografia minorile**”

  Chiunque sfrutta minori degli anni diciotto al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico è punito con la reclusione da sei a dodici anni (…)

- Art. 600 quater c.p. “**Detenzione di materiale pornografico**”

  Chiunque, al di fuori delle ipotesi previste nell'articolo 600-ter, consapevolmente si procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto è punito con la reclusione fino a tre anni (…)

- Art. 600 quater1 c.p. “**Pornografia virtuale**”

  Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

  Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali

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

PROFILO CRIMINOLOGICO DEL PEDOFILO ONLINE

- Prevalenza di sesso maschile;
- Fascia di età relativamente giovane;
- Individuo ben integrato nella società;
- Tendenzialmente autopercepito come non inserito in ambiti criminali;
- Fenomeno “trans-classe” abbracciando soggetti di vario livello economico e di scolarizzazione.

TIPOLOGIE

- **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.

Approcci sistematici al fenomeno della delinquenza informatica

CRIMINOLOGICO

CIVILISTICO

PENALISTICO

Approccio criminologico

Prende in esame il crimine informatico da un punto di vista fenomenologico, individuando e descrivendo comportamenti illeciti, in modo indipendente rispetto alle categorie giuridiche

Approccio civilistico

Esamina il problema prevalentemente sotto l'ottica del danno arrecato ai singoli e ai mezzi di riparazione

Approccio penalistico

Ha come scopo l'analisi delle caratteristiche degli illeciti al fine di individuare le norme incriminatrici eventualmente applicabili esistenti nel sistema giuridico penale

Tipologie di computers-criminals: Hackers

Il termine indica qualcuno che riesce ad inserirsi nei sistemi informatici perpetrando atti vandalici di tipo informatico;

Tipologia criminale informatica comparsa negli Stati Uniti negli anni ’80.

TIPOLOGIE DI HACKING

Hacking benevolo: individui che non desiderano danneggiare qualcuno/qualcosa quando violano il sistema; è chiamato anche ethical hacking ed è utilizzato dalle aziende per far testare da hacker in maniera consapevole i loro sistemi di sicurezza;

Hacking "malevolo/cattivo": individui che hanno lo scopo di danneggiare o rubare informazioni nei sistemi.

Tipologie

La categoria degli hackers non è uniforme.

Si distinguono per:

1. Livello tecnico;
2. Condotta;
3. Motivazioni;
4. Modus operandi.

Classificazione di Baird e Ranauro (1987)

In base al livello di abilità gli autori distinguono:

1. Crackers: penetratori di più alto livello, larga conoscenza ed esperienza;
2. Hackers: penetratori di livello medio;
3. Rodents: penetratori di basso profilo.

Classificazione di Baird e Ranauro (1987)

In base alla struttura del comportamento attuato e alle diverse motivazioni gli autori distinguono:

1. Hackers: attribuiscono ad una qualsiasi informazione, lo stesso valore ad essa attribuito dal proprietario;

2. Crackers: sono veri e propri “info-maniacs”, persone che ricercano le informazioni in modo ossessivo.

Hacker profiling

Si occupa dell'analisi e della costituzione dei profili anagrafici, socio-demografici, caratteriali e psicologici degli organizzatori di un attacco informatico.

Studi recenti hanno evidenziato come un'accurata comprensione delle motivazioni soggiacenti un attacco informatico e l'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)

Profilo dell'Hacker (Lafrance, 2004)

La dimensione psicologica viene utilizzata per distinguere gli attaccanti in 5 categorie in base alle loro motivazioni:

1. Attaccanti casuali (*casual hackers*);
2. Attaccanti politici (*political hackers*);
3. Crimine organizzato (*organized crime*);
4. *Squatters*;
5. *Insiders*.

Profilo dell'Hacker

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.

Profilo dell'Hacker

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.

Profilo dell'Hacker

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.

Profilo dell'Hacker

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.

Profilo dell'Hacker

Insiders e *intruders*:

Gli attacchi riconducibili a questa tipologia possono essere portati a termine sia dall'interno, ovvero dagli operatori o utenti interni ad un'organizzazione o ad un sistema informatico (*insiders*), sia dall'esterno, ovvero da attaccanti esterni come spie che si introducono illegalmente all'interno di un'organizzazione (*intruders*).

Motivazioni di resistenza verso questa tecnica

- Carente documentazione sull'argomento
- Astrazione della natura umana propria dell'ambiente informatico
- Diffidenza manifesta verso le tradizionali tecniche di investigazione psicologica o profiling criminale generico
- Risultati discrepanti nel profiling criminale generico

Elementi principali del Cybercrime profiling

SIGNATURE

“ Firma ” propria dell ’ autore del crimine, riscontrabile sulla scena del crimine o riconducibile al sospettato. Può essere lasciata a livello conscio o meno e a differenza del *modus operandi* non cambia nella reiterazione del crimine.

Non si tratta del “Re di cuori” lasciato sulla scena del crimine ma di modelli comportamentali univoci e ripetuti

Es. dettagli linguistici, dettagli grafici,…

Elementi principali del Cybercrime profiling

MODUS OPERANDI

Modalità attraverso le quali il crimine è commesso. Utile nella correlazione di casi o individui, tuttavia può variare nel tempo (crescita tecnologica ed esperienziale).

Per questo si creano spesso falsi positivi o mancato link psicologico

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

Elementi principali del Cybercrime profiling

VITTIMOLOGIA

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

Particolarmente utile nelle analisi preventive di reti o strutture informatiche

Elementi principali del Cybercrime 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

Elementi principali del Cybercrime profiling

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 principali del Cybercrime profiling

STAGING

Alterazione della scena del crimine o di elementi ad essa correlati.

Può essere effettuato dal criminale per depistare o da persone legate in qualche modo al crimine in oggetto

Tipologie di analisi

PASSIVA

Costituita da vittimologia, analisi della motivazione, del modus operandi, della scena del crimine, delle caratteristiche del criminale e dalle altre tecniche analitiche applicabili ad un evento criminale già avvenuto o in fase di svolgimento

Tipologie di analisi

ATTIVA

Studio dell ’ ambiente e dei patterns comportamentali propri dell ’ ambiente digitale, attraverso l’interazione personale o automatizzata. Spesso è utilizzata come mezzo di prevenzione e creazione di piattaforme di dati utili.

FINE

fsivilli@unich.it