IL CRIMINE INFORMATICO O "CYBERCRIME".

Il **crimine informatico** è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica sia hardware che software.

Alcuni crimini in particolare sono finalizzati allo sfruttamento commerciale della rete Internet, a porre a rischio i sistemi informativi di sicurezza nazionale.

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

Agli esordi della sottocultura hacker, le condanne penali erano rare poiché l'approccio di quest'ultimi era rivolto alla conoscenza dei sistemi informatici e della loro sicurezza, violando i sistemi con azioni non dannose.

I sostenitori dell'hacking sono motivati da fini artistici e politici, ma spesso sono indifferenti sull'uso di mezzi illegali per raggiungerli. Con la crescita dell'industria informatica, sono emersi i casi di violazione dei sistemi informatici per esclusivo profitto personale.

Con la globale e capillare diffusione della rete Internet, si è sempre più sviluppata una diversa forma di hacker, infatti i criminali informatici attuali sono sempre più attivi nel procacciare denaro a scapito dei normali utenti della rete.

Come su indicato generalmente, il "cybercrime" può essere distinto nelle seguenti modalità:

- Il più abietto dei reati che si commette in rete è quello della pedo-pornografia, questo tipo di reato è contrastato da molti Stati membri dell'Europa che hanno realizzato un piano che è parte di una più ampia strategia adottata dal Consiglio d'Europa nel progetto "Costruire un'Europa per e con i bambini e le bambine", che trae origine dall'impegno assunto nel 2005 dai Capi di Stato e di Governo - riuniti a Varsavia in occasione del Terzo Summit del Consiglio d'Europa - di promuovere fattivamente i diritti dell'infanzia e di contribuire alla prevenzione e al contrasto di ogni forma di violenza, concretizzando una fattiva collaborazione e scambio di dati tra le forze di Polizia degli stati aderenti.
- Attacchi alle infrastrutture critiche: tale crimine informatico è portato al fine di danneggiare i grandi sistemi informatici delle aziende di stato o private.
- Cyberterrorismo: Secondo la definizione dell'**FBI**, il cyberterrorismo è un «premeditato attacco a sfondo politico, da parte di gruppi subnazionali o agenti clandestini, contro i mezzi d'informazione, sistemi, dati e programmi informatizzati, che si traduce in violenza contro obiettivi non combattenti».
- Copyright: non è altri che la protezione dei diritti d'autore, infatti lo sviluppo tecnologico e l'avvento di Internet nel XX secolo, l'avvento dei riproduttori ed in particolare del computer e delle Rete internet, ha sottratto uno dei cardini alla base del copyright in senso classico, ovvero il costo e la difficoltà di riprodurre e diffondere sul territorio le opere, aspetti fino ad allora gestiti dalla corporazione degli editori –SIAE- dietro congruo compenso o cessione dei diritti da parte degli autori. Ciò ha reso assai difficile la tutela del copyright come tradizionalmente inteso, e creato nuovi spazi per gli autori.
- Frode informatica: la frode informatica che consiste nell'alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto.

- La violazione dei dati personali: consiste nel procurarsi indebitamente dati, personali o sensibili. In effetti, la rete è in grado di offrire una vasta gamma di informazioni e servizi ma contemporaneamente può costituire un luogo pericoloso per la nostra privacy anche perché il mezzo stesso non è stato concepito per scambiare o gestire dati sensibili.
- Lo spamming: è uno dei fenomeni più fastidiosi di Internet consiste nell'invio di una stessa e-mail, contenente di solito pubblicità, a centinaia, se non a migliaia di persone, puntando sul fatto che la posta elettronica è gratuita. Oltre a violare la netiquette e a saturare la rete con messaggi inutili, lo spamming in Italia viola la legge sulla Privacy delle persone e di altri soggetti rispetto al trattamento dei dati personali.

In un contesto simile, mantenere l'anonimato risulta spesso arduo e con il proliferare dei conti on-line e lo spostamento delle aziende su Internet, risulta più semplice per i malintenzionati accedere alle nostre informazioni riservate. A tal proposito, una delle piaghe più dannose della rete è lo spyware che, installandosi spesso in maniera fraudolenta nel personal computer delle vittime, provvede ad inviare dati personali (pagine visitate, account di posta, gusti ecc) ad aziende che successivamente li rielaboreranno e rivenderanno.

Esiste perfino un metodo, chiamato social engineering, tramite cui i truffatori riescono a ottenere informazioni personali sulle vittime attraverso le più disparate tecniche psicologiche: si tratta di una sorta di manipolazione che porta gli utenti a rilasciare spontaneamente i propri dati confidenziali.

La miglior difesa per la nostra privacy, in questa situazione di precarietà, consiste nell'utilizzare il buon senso e nell'adottare semplici accorgimenti tra cui:

- Utilizzare password non banali e con codici alfanumerici.
- Evitare il più possibile di comunicare la propria password.
- Installare e configurare bene firewall e antivirus tenendoli in seguito costantemente aggiornati.
- Procurarsi un antispyware in grado di ripulire efficacemente il sistema.
- Tenere sotto controllo i cookies.
- Non aprire allegati di e-mail provenienti da utenti sconosciuti o sospetti per evitare fenomeni di cosiddetto phishing.
- Configurare il livello della privacy del nostro browser almeno a livello medio.
- Leggere attentamente le licenze e le disposizioni riguardo alla privacy prima di installare un qualsiasi software.
- Utilizzare efficacemente il browser con il sistema di anti tracciamento.

Esistono inoltre soluzioni meno immediate ma più efficaci come l'utilizzo della crittografia, che ci permette di criptare un messaggio privato attraverso particolari software facendo sì che solo l'utente destinatario possa leggerlo in chiaro, unito all'implementazione della firma digitale.

- Le molestie: Mentre alcuni contenuti possono offendere in maniera indiretta, le molestie informatiche possono colpire la sensibilità di chiunque quali commenti sul genere, etnia, religione e orientamento sessuale. Spesso si verificano nelle chat, nei newsgroup, nelle conferenze virtuali, ecc.
- Il cyberstalking: non esiste una definizione generalmente accettata di *stalking*, ma così come enunciato da studiosi delle molestie assillanti di lingua anglofona è comunque colui che segue la vittima nei suoi movimenti per poi intromettersi nella sua vita privata. Un'altra traduzione molto usata di "stalking" è "persecuzione", così come lo stalker è chiamato "persecutore" e la vittima "perseguitato".

Un fenomeno negativo che sta allertando la società con la massiccia diffusione tra i giovani dei social network, le chat e i forum è il cyberbullismo, forma diversa rispetto al bullismo tradizionale nella vita reale, l'uso dei mezzi elettronici conferisce al cyberbullismo alcune caratteristiche proprie:

- *Anonimato del molestatore*: in realtà, questo anonimato è illusorio: ogni comunicazione elettronica lascia pur sempre delle tracce. Per la vittima, però, è difficile risalire da sola al proprio molestatore; inoltre, a fronte dell'anonimato del cyberbullo, spiacevoli cose sul conto della vittima (spesse volte descritta in modo manifesto, altre in modo solo apparentemente non rintracciabile) possono essere inoltrate ad un ampio numero di persone.
- *Difficile reperibilità*: se il cyberbullismo avviene via SMS, messaggeria istantanea o mail, o in un forum online privato, ad esempio, è più difficile reperirlo e rimediarvi.
- *Indebolimento delle remore etiche*: le due caratteristiche precedenti, abbinate con la possibilità di essere "un'altra persona" online (vedi i giochi di ruolo), possono indebolire le remore etiche: spesso la gente fa e dice online cose che non farebbe o direbbe nella vita reale.
- *Assenza di limiti spaziotemporali*: mentre il bullismo tradizionale avviene di solito in luoghi e momenti specifici (ad esempio in contesto scolastico), il cyberbullismo investe la vittima ogni volta che si collega al mezzo elettronico utilizzato dal cyberbullo.

Come nel bullismo tradizionale, però, il bullo vuole prendere di mira chi è ritenuto "*diverso*", solitamente per aspetto estetico, timidezza, orientamento sessuale o politico, abbigliamento ritenuto non convenzionale e così via. Gli esiti di tali molestie sono, com'è possibile immaginarsi a fronte di tale stigma, l'erosione di qualsivoglia volontà di aggregazione ed il conseguente isolamento, implicando esso a sua volta danni psicologici non indifferenti, come la depressione o, nei casi peggiori, ideazioni e intenzioni suicidarie. Spesso i molestatori, soprattutto se giovani, non si rendono effettivamente conto di quanto ciò possa nuocere alla vittima.

Ulteriore forma più raffinata di cybercrime, è quella dello spionaggio industriale.

In sostanza il crimine informatico si sviluppa in molte forme e tipicità, lo Stato cerca di contrastarlo con leggi che tutelano la parte sana dell’utilizzatore, ma indubbiamente è difficile arginare i fenomeni criminali.