
Bullismo

INDICE

Chiara Belloni - Flavia Colamedici - Giorgia Musio
Classe: 3A - Largo Iannoni

BULLISMO, BULLYING, HARCÈLEMENT

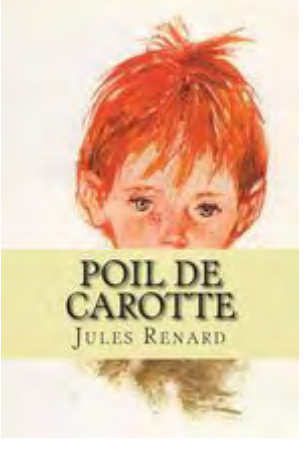
Il **bullismo** è un atto di violenza che certi studenti subiscono a scuola, sui social, in pubblico o di nascosto. Il **cyberbullismo** è la forma digitale del bullismo.

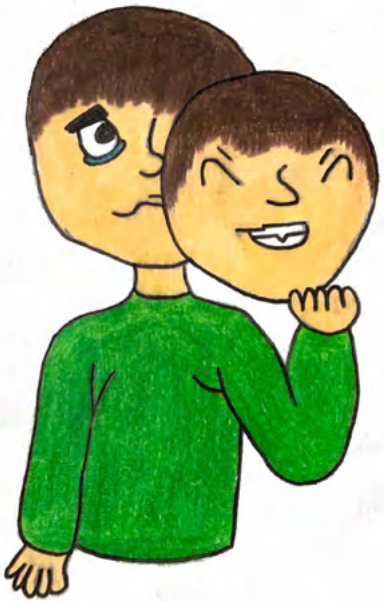
Bullying is an act of violence that some students suffer at school, on Interner, in public or secretely. **Cyberbullying** is the digital form of bullying.

Le **harcèlement** est un act de violence que certains collégiens subissent à l'école, sur les résaux, en public ou en cachette. Le **cyber-harcèlement** est la forme numerique du harcèlement.

Jules Renard

Jules Renard pubblicò "Poil de carotte" (Pelo di Carota) nel 1894. Il romanzo racconta la storia di un ragazzo, Français Lepic, soprannominato "Pelo di Carota" per i suoi capelli rossi. Non è un ragazzo molto educato perché è cresciuto in una famiglia che non ha dato lui il giusto affetto, odiato dalla madre e dai due fratelli; l'unico che lo supporta un po' è il padre, che però è influenzato negativamente dalla moglie. Allora il protagonista soffre tentando di soddisfare la madre, ma senza successo. Nonostante ciò, questo non è un romanzo triste.





PERSONAGGI

FAKE NEWS

Fake news è il termine inglese che indica le notizie false. Per essere considerata una “fake news” non basta che la notizia sia falsa. Deve anche essere stata inventata consapevolmente e con lo scopo di danneggiare qualcuno o di sostenere una propria tesi. Quindi, una notizia involontariamente sbagliata o imprecisa non è una fake news.

Qual'è la differenza tra fake news e bufale?

Ci sono delle differenze, sebbene piccole, tra fake news e tra bufale:

• Una bufala è indefinita nel tempo.

• Una fake news è una notizia relativa a qualcosa che è appena avvenuto.

• Una bufala è totalmente falsa e inverosimile.

• Una fake news potrebbe essere parzialmente vera o parzialmente verosimile

Nella storia

Fino a pochi anni fa una notizia falsa restava confinata tra chi l'aveva inventata e a chi l'aveva raccontata. Ci volevano anni perché la notizia falsa si diffondesse un po'. Sempre che non venisse dimenticata prima.
Oggi, invece, con la potenza di internet, dei social media e della televisione, qualunque notizia arriva in pochi istanti in ogni angolo del globo. E comincia a circolare anche se non è vera perché chi le inventa, spesso, guadagna dei soldi da quelle notizie e quindi organizza dei sistemi per farle circolare senza controllo.

Tipi

- **Collegamento ingannevole**: titoli, immagini o didascalie non sono relative al fatto di cui si parla
- **Contesto ingannevole**: il contenuto reale è accompagnato da informazioni contestuali false.
- **Manipolazione della satira**: il contenuto satirico viene utilizzato per trarre in inganno.

Come difendersi dalle fake news

Con i social, le fake news si diffondono sempre di più, ma si possono riconoscere con più attenzione. Si deve verificare che il sito sia affidabile, dato che spesso si fingono uno "più famoso" e spesso si può riconoscere il falso o dal nome leggermente modificato e la foto diversa, dall'originale. Nel caso si trattasse di un falso è bene verificare sul sito istituzionale vero e su altri siti affidabili; solo quando si è sicuri che la notizia è vera si può condividere. Sui siti bisogna anche controllare le foto e assicurarsi che non siano fotomontaggi; vanno controllate anche il lessico usato e se i termini siano corretti. Infine verifica se la notizia è vera e attuale basandosi su altre fonti e quello che si dice a riguardo.


VIENI QUI PICCOLETTO!
MA CHE COSA HO FATTO DI MALE?
HAHAH

INGEGNERIA SOCIALE

COSA È

Nel campo della sicurezza informatica, l'**Ingegneria Sociale** (dall'inglese *Social Engineering*) consiste nell'utilizzo, da parte degli *hacker*, di tecniche di manipolazione psicologica con l'obiettivo di ottenere informazioni personali, accesso o azioni da parte di altre persone tramite l'inganno.

Gli "attaccanti sociali" cercano di sfruttare le debolezze e le emozioni umane (paura, senso di urgenza, buona fede, curiosità, gentilezza, mancanza di consapevolezza, propensione a fidarsi e cooperare con gli altri), al fine di ottenere informazioni sensibili o per indurre le persone a compiere azioni che potrebbero essere dannose per la sicurezza personale o organizzativa.

Infatti, sebbene gli attacchi di ingegneria sociale prendano in genere di mira un singolo individuo, sempre più spesso stanno diventando solo una delle fasi di un attacco più ampio e complesso.

Queste tecniche non riguardano l'uso di vulnerabilità tecnologiche o di sistemi informatici, ma si concentrano principalmente sulla manipolazione delle persone stesse, basandosi su abilità comunicative, persuasive e psicologiche.

IL CICLO DEGLI ATTACCHI

Sebbene ogni attacco di ingegneria sociale possa apparire diverso in termini di tecniche e obiettivi, ciascuno segue lo stesso **ciclo** composto da **quattro fasi**:

- **Raccolta di informazioni**. L'autore della minaccia effettua ricerche sulla vittima per scoprire quale punto debole o mezzo funzionerà meglio per l'attacco.
- **Stabilire una relazione**. Il passo successivo consiste nell'entrare in contatto e stabilire una relazione con la vittima, al fine di guadagnarne la fiducia (fondamentale per ottenere la sua collaborazione).
- **Manipolazione psicologica**. In questa fase, l'attaccante sfrutta le informazioni raccolte e la relazione costruita con la vittima per abbatterne le difese e sferrare l'attacco vero e proprio. Utilizza la precedente fase di studio per influenzare, persuadere o ingannare la vittima, costruendo una menzogna (credibile). La vittima viene così manipolata dall'aggressore "fidato" affinché riveli dati o informazioni confidenziali oppure compia un'azione specifica.
- **Esecuzione**. In quest'ultima fase viene effettivamente eseguito l'attacco.

TIPI DI ATTACCO

I principali strumenti utilizzati nell'ingegneria sociale sono il telefono, l'e-mail e i siti web.

Le principali metodologie di attacco sfruttano tali tecnologie, avvantaggiandosi di tecniche psicologiche.

- **Pretexting** (creazione di un pretesto). Consiste nel creare una falsa ambientazione (un attaccante si finge una persona di fiducia o un dipendente di un'organizzazione) per ottenere accesso a luoghi o informazioni riservate.
- **Phishing e vishing**. Solitamente si invia una mail alla vittima, facendola assomigliare il più possibile ad un messaggio inviato da una certa azienda. La persona viene spinta a scaricare un allegato che presenta un malware o ad accedere a un sito in cui sono richieste informazioni. Nell'ambito dell'ingegneria sociale è di uso frequente il phishing telefonico, anche chiamato vishing.
- **Baiting** (esca). Consiste nell'utilizzare un'esca attraente (curiosità, avidità), come una chiavetta USB, contenente malware o software dannosi.

COME DIFENDERSI

A livello personale, sono consigliate tali azioni di prevenzione e difesa:

- **Verifica dell'Identità**: prima di condividere informazioni sensibili o concedere accesso, assicurarsi di verificare l'identità delle persone coinvolte.
- **Diffidare delle Richieste Urgenti**: gli aggressori spesso cercano di indurre le vittime a compiere azioni rapide e irrazionali. Prendersi sempre il tempo necessario per valutare le richieste.
- **Evitare di aprire** allegati o file eseguibili di dubbia provenienza.
- **Protezione delle Informazioni**: utilizzare password robuste, evitare di condividere informazioni sensibili tramite canali non sicuri e proteggere i dispositivi con soluzioni di sicurezza aggiornate.
- **Segnalazione di Attività Sospette**: in caso di sospetta attività di social engineering, segnalare immediatamente il problema alle autorità competenti.

PHISHING

La parola phishign è una versione alterata del verbo inglese *fishing*, "pescare"

Il *phishing* è un tipo di **truffa virtuale** che cerca di "prendere all'amo" le persone, convincendole a fornire dati personali per poterli **derubare**

TIPI DI PHISHING

Spear phishing → Lo spear phishing è un tipo di attacco di phishing mirato a singoli individui o piccoli gruppi. Si presenta come una persona conosciuta o di cui ci si fida, che richiede informazioni sulla vittima tramite i social media.

Angler phishing → L'angler phishing è un attacco in cui l'aggressore si presenta come un normale rappresentante del servizio clienti e convince le vittime a passargli le informazioni personali.

Deceptive phishing → Il deceptive phishing è il tipo di phishing più comune. Un hacker tenta di ottenere dalle vittime informazioni riservate da utilizzare per rubare denaro o lanciare altri attacchi.

Whaling → Parliamo di whaling quando gli hacker prendono di mira un "pesce grosso", ad esempio un CEO.

COME RICONOSCERE CHE E' PHISHING?

INDICAZIONI FORNITE DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI:

- **Massima allerta** - Banche, compagnie telefoniche, enti pubblici e aziende non chiedono mai di inviare dati sensibili per chat, mail o sms.
- **Controlliamo i link prima di aprirli** - Un'accortezza da adottare è quella di controllare il link di chi ci ha contatto posizionandoci sopra il puntatore del mouse (senza cliccare): ciò ci permetterò di leggere nel browser, in basso a sinistra, il vero nome del sito.
- **Non aprire allegati di messaggi sospetti** - Se non siamo sicuri al 100% della provenienza di un messaggio, non aprire mai né link, né contenuti allegati. Potrebbero contenere virus o farvi cadere in una truffa.
- **Attenzione agli errori e alle stranezze** - I contenuti di *phishing* spesso sono frutto di traduzioni molto poco accurate, con errori di grammatica, bug di formattazione e frasi costruite male.
- **Occhio alle minacce** - I messaggi di phishing spesso contengono frasi decisamente intimidatorie, con minacce di chiusura dei conti, multe salate o sanzioni penali qualora non venisse fatto quanto richiesto.
- **Installare antivirus validi** - Avere una buona protezione dei nostri dispositivi ci tiene al sicuro da spam, virus e trojan.
- **Non condividere i propri dati personali** - Non condividiamo mai i nostri dati sensibili con chi ce li chiede via mail, chat o sms.

QUANDO È DIFFAMAZIONE SUI SOCIAL?

Costituiscono **requisiti essenziali**: l'offesa della propria reputazione; l'impossibilità; soggetto passivo di percepire fisicamente l'offesa arretratagli; la presenza di due persone.

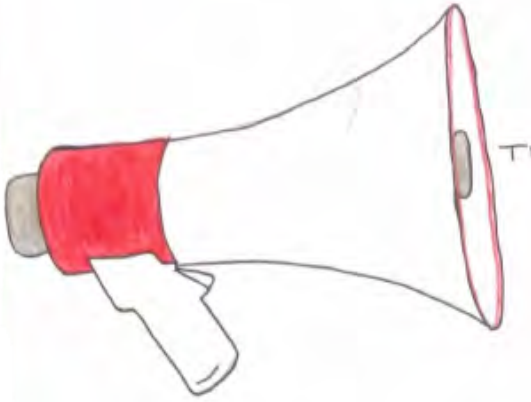
DIFFAMAZIONE

COSA SUCCEDE SE APPLICHI LA DIFFAMAZIONE?

La diffamazione è delitto previsto e punito dall'art.595 c.p. che così recita: "*chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a € 1.032.Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a € 2.065.Se l'offesa è arrecata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a € 516.Se l'offesa è arrecata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate*".

CHE COSA SI INTENDE PER DIFFAMAZIONE DEI SOCIAL NETWORK?

La diffamazione sui social si può manifestare attraverso commenti sui social quali Facebook, Instagram, Whatsapp ecc.
Ad esempio dare ad una persona del mafioso o del corrotto integra sant'altro il reato in oggetto. Il commento può consistere anche in una foto o in una vignetta offensiva.
Ovviamente su qualsiasi social si può criticare liberamente qualcosa o qualcuno.
Tale critica deve però essere fondata su fatti veri, espressa in termini misurati e rispettosi dell'altrui dignità morale e professionale e di interesse per la collettività.
Ad esempio dare
del pregiudicato può integrare il reato di diffamazione, anche se lo stesso è indirizzato ad un soggetto che sia già stato condannato con sentenza definitiva perché chi ha pronunciato tale espressione lo ha fatto in un contesto offensivo e diffamante.


TI DEVI SOLO VERGOGNARE


NESSUNO TI VUOLE
INFANTILE
BRUTTA
STUPIDA
IDIOTA
ANTIPATICA
VAI VIA
TI ODIO
TI DEVI SOLO VERGOGNARE

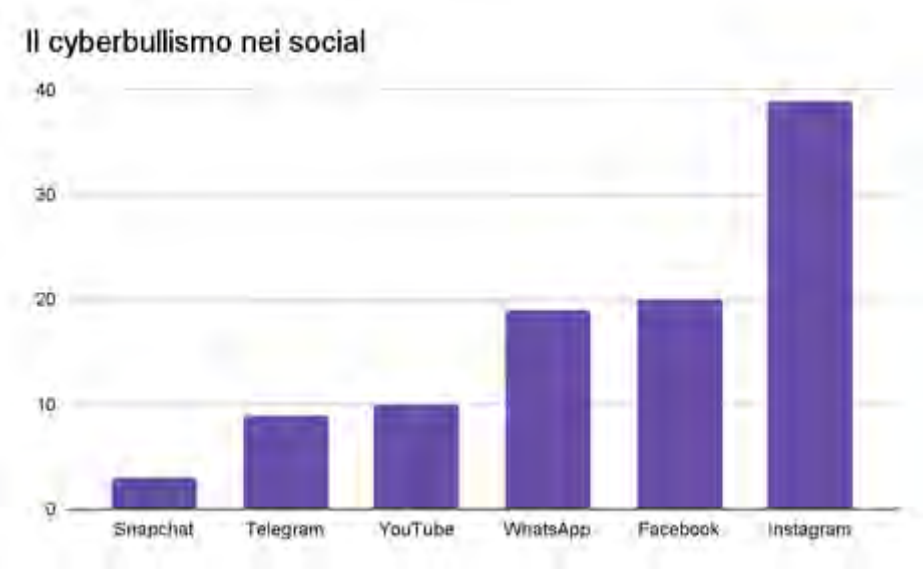

ANTIPATICA
SUICIDE

DATI

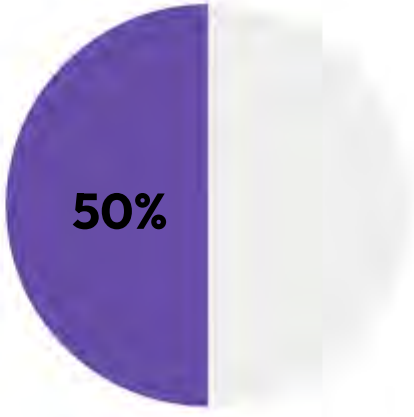
9 10 11 12 13 14 15 16

Tra 9-10 anni hanno più probabilità di essere vittime di cyberbullismo su giochi online

Tra 13-16 anni hanno più probabilità di essere vittime di cyberbullismo su social media



In Italia più del 50% degli studenti tra 11 e 17 anni ha subito bullismo



Instagram è il social network dove si verificano più atti di cyberbullismo.

2020

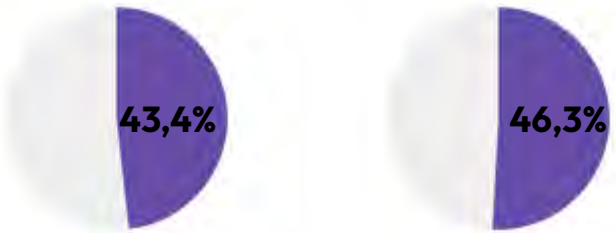
Bullismo: 44%
Cyberbullismo: 23%

2023

Bullismo: 54%
Cyberbullismo: 30%

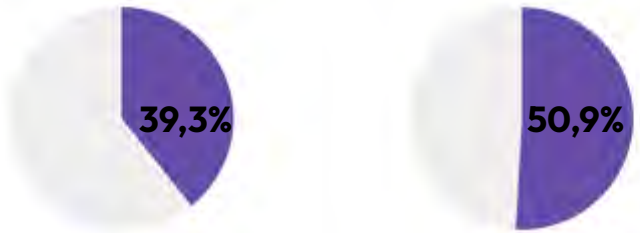
Negli ultimi anni le percentuali sono aumentate notevolmente.

Vittime di bullismo



Maschi Femmine

Vittime di cyberbullismo



Maschi Femmine

	Sesso	11 anni	13 anni	15 anni
Bullismo	Maschi	18,9%	14,6%	9,9%
	Femmine	19,8%	17,3%	9,2%
Cyberbullismo	Maschi	17,2%	12,9%	9,2%
	Femmine	21,1%	18,4%	11,4%