# Navigare sicuri: guida per un uso consapevole dei social media e del web


*E-book realizzato dagli studenti della classe 3B-IT per promuovere cittadinanza digitale, sicurezza online e responsabilità nel web.*

# IDENTITÀ DIGITALE E REPUTAZIONE ONLINE

Creato dal gruppo 1:

Sofia Mutoli

Gabriele Cammisa

Alessandra Benenati

# Identità digitale

Ogni volta che utilizziamo Internet, lasciamo una serie di informazioni che contribuiscono a formare la nostra **identità digitale**. Essa rappresenta l'insieme di tutti i dati, i contenuti e le attività che ci riguardano e che sono presenti online. L'identità digitale non è composta solo da ciò che decidiamo di pubblicare personalmente, ma anche da informazioni generate indirettamente durante la navigazione.

Le tracce digitali possono essere attive, quando condividiamo foto, video, commenti, messaggi o contenuti sui social network, oppure passive, quando siti web e applicazioni raccolgono automaticamente dati come la posizione geografica, le preferenze di navigazione, il tempo trascorso su una pagina o gli acquisti effettuati online. Queste informazioni vengono spesso utilizzate dalle piattaforme per personalizzare contenuti e pubblicità.

È importante ricordare che Internet ha una grande capacità di conservare le informazioni. Anche quando un contenuto viene eliminato, potrebbe essere stato copiato, scaricato o condiviso da altri utenti. Per questo motivo si parla spesso di impronta digitale, cioè dell'insieme delle tracce che lasciamo nel web nel corso del tempo. Essere consapevoli della propria identità digitale significa comprendere che ogni azione online contribuisce a costruire l'immagine che gli altri possono avere di noi.

# Reputazione online

La **reputazione online** è la percezione che altre persone hanno di noi sulla base delle informazioni disponibili su Internet. Oggi gran parte delle relazioni sociali avviene anche attraverso il web e i social network, perciò ciò che compare online può influenzare il modo in cui veniamo giudicati da amici, compagni di scuola, insegnanti e, in futuro, anche da università o datori di lavoro.

La reputazione online dipende da molti fattori: i contenuti che pubblichiamo, i commenti che scriviamo, le fotografie in cui compariamo, i tag ricevuti e perfino le interazioni con altri utenti. Una presenza digitale positiva può mettere in evidenza interessi, competenze, creatività e senso di responsabilità. Al contrario, comportamenti scorretti, contenuti offensivi o informazioni condivise senza attenzione possono creare una cattiva immagine difficile da modificare nel tempo.


Per proteggere la propria reputazione è fondamentale adottare comportamenti responsabili. Prima di pubblicare un contenuto è utile chiedersi se potrebbe creare problemi in futuro o essere interpretato negativamente da altre persone. È inoltre importante utilizzare correttamente le impostazioni della privacy, evitare di condividere dati personali sensibili e mantenere sempre un atteggiamento rispettoso nelle comunicazioni online.

In conclusione, identità digitale e reputazione online sono strettamente collegate: le tracce che lasciamo sul web contribuiscono a costruire l'immagine che gli altri hanno di noi. Per questo motivo è essenziale utilizzare Internet in modo consapevole, ricordando che ogni azione online può avere conseguenze sia nel presente sia nel futuro.

# Privacy, dati personali e GDPR

*Consapevolezza, rischi e tutele nell'era della condivisione online.*

Gruppo 2:
CAMPO PIERA
RANDAZZO PIETRO
LO GIUDICE ANTONINO

# Cosa sono i dati


I dati personali includono elementi comuni come nome, email, codice fiscale e posizione geografica. Esistono anche i **dati particolari** (ex sensibili). Questi ultimi rivelano l'origine etnica, le opinioni politiche, l'orientamento religioso, lo stato di salute e la vita sessuale di un individuo. I dati biometrici (impronte digitali) e genetici appartengono a questa categoria protetta.

# La privacy nei social network

I social network si basano sulla condivisione, ma espongono gli utenti a forti rischi di profilazione commerciale. Ogni "like", commento o tracciamento della posizione alimenta un identikit digitale usato dagli inserzionisti. Il furto di identità e il cyberbullismo sono pericoli reali legati alla sovraesposizione dei propri dati (oversharing). Le piattaforme estraggono valore economico dalle informazioni comportamentali degli iscritti.


## Concetti base del GDPR

Il Regolamento Generale sulla Protezione dei Dati (GDPR) è la normativa europea che tutela la privacy. Si fonda su principi rigidi: trasparenza nel trattamento, limitazione delle finalità e minimizzazione dei dati raccolti. Il GDPR garantisce diritti fondamentali ai cittadini. Tra i più importanti figurano il diritto all'oblio (cancellazione dei dati) e il diritto alla portabilità delle informazioni da una piattaforma all'altra.

## Protezione dei dati online

Difendere la propria identità digitale richiede l'adozione di strategie tecniche attive. L'uso di password complesse e uniche per ogni servizio è il primo passo essenziale. L'attivazione dell'autenticazione a due fattori (2FA) blocca gli accessi non autorizzati anche in caso di furto della password. Bisogna prestare massima attenzione ai tentativi di phishing via email o SMS e utilizzare reti protette (VPN).

# Checklist Privacy

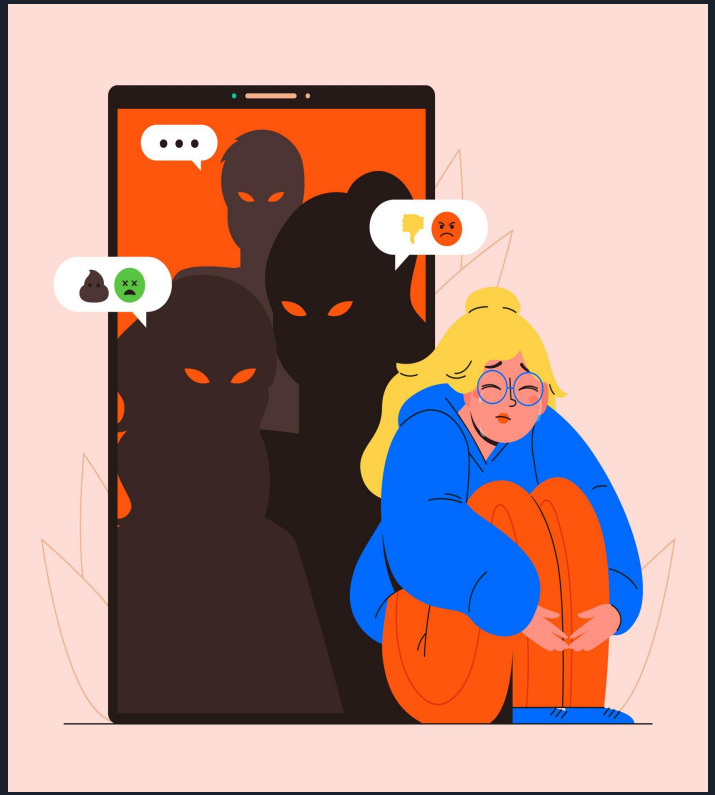
- **Verifica password:** Cambia le password deboli e usane una diversa per ogni sito
- **Attiva la 2FA**: Abilita l'autenticazione a due fattori su social ed email.
- **Pulisci i social**: Imposta i profili Instagram, TikTok o Facebook su "Privato".
- **Controllo permessi**: Revoca l'accesso a microfono e posizione alle app non necessarie.
- **Verifica link**: Non cliccare mai su collegamenti ricevuti tramite SMS o email sospette.
- **Gestione Cookie**: Rifiuta i cookie di tracciamento non essenziali sui siti web.

# CYBERBULLYING

SLIDE CREATE:
GASPARE GAMBINO
MATTEO COSTA VALERIO
SALAMONE FLAVIO
GRUPPO 3

# *Che cos'è il cyberbullismo ?*

Il cyberbullismo è una forma di aggressione, molestia e prevaricazione intenzionale e ripetuta nel tempo, attuata attraverso l'utilizzo di strumenti digitali come social network, chat ed e-mail. A differenza del bullismo tradizionale,si sposta nel mondo virtuale della rete Internet.



# Ruoli coinvolti nel cyberbullismo:

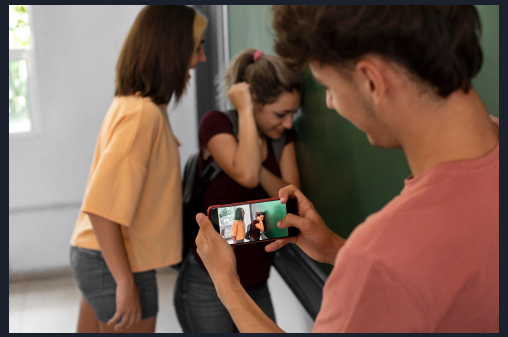
Ci sono due ruoli principali:

***cyberbullo***: A differenza del bullo tradizionale, che spesso usa la forza fisica o l'intimidazione visibile, il cyberbullo sfrutta la tecnologia come scudo. Le motivazioni possono essere agire spesso per il bisogno di controllo, per noia o a causa di una profonda incapacità di gestire le proprie frustrazioni.

***vittima***:La vittima di cyberbullismo si trova in una condizione di estrema vulnerabilità, poiché l'attacco digitale azzera i confini della propria area di sicurezza. L'isolamento e l'esposizione, la vittima si sente colpita ovunque, anche dentro la propria camera. Non esiste un luogo sicuro in cui rifugiarsi, perché gli attacchi arrivano sullo smartphone in qualsiasi momento del giorno o della notte.

Il legame tra cyberbullo e vittima è asimmetrico e distorto dalla tecnologia:

- ***Persecuzione h24***: Nel bullismo reale l'incontro si esaurisce a scuola o per strada. Online, l'azione del cyberbullo si frammenta in decine di notifiche, commenti e messaggi continui.
- ***Il pubblico come carburante***: Il cyberbullo si alimenta dei "like" e delle condivisioni degli spettatori. Più il pubblico interagisce, più il bullo si sente forte e più la vittima si sente schiacciata dal giudizio sociale.



# GUIDA ESSENZIALE SU PHISHING, MALWARE E SICUREZZA ACCOUNT


Creato dal gruppo 4:
Lo Piccolo Noemi
Ranieri Gioele
Lazar Alessio

# La sicurezza digitale ed il phishing

## La Sicurezza digitale

Oggi la nostra vita si sviluppa online tanto quanto nel mondo reale. Dalle foto di famiglia alle operazioni bancarie, dalle chat di lavoro, alla demotica di casa: **i nostri dati sono ovunque costantemente connessi.** Questa incredibile comunità porta con sé un rovescio delle medaglie: siamo diventati bersagli mobili per minacce sempre più sofisticate. Parlare di sicurezza digitale non è più un argomento per soli esperti di informatica, **ma una necessità quotidiana per chiunque .**
Capire come difendersi significa proteggere: la nostra identità, i nostri risparmi, la nostra privacy.

## Il Phishing

Il Phishing è una truffa basata sull'inganno. I criminali informatici si travestono da aziende affidabili come la tua banca, netflix ecc... per spingerti a compiere un'azione che normalmente non faresti. Il loro obiettivo principale è rubare le tue informazioni personali come:

1) Le Credenziali di Accesso
2) Il numero della carta di credito
3) Dati di Identità

I canali più usati per truffare l'utente spesso sono:
**Email**:ricevi un'email che sembra autentica con un messaggio urgente:"il tuo conto è stato bloccato, clicca qui per sbloccarlo"
**SMS**:La truffa arriva via sms. Spesso i messaggi si inseriscono nella stessa chat di messaggi veri, rendendo l'inganno quasi invisibile
**Chiamate**:un finto operatore ti chiama dicendo che c'è un attacco hacker in corso sul tuo conto e ti chiede di dettagli i codici di sicurezza per bloccarli

# Che cosa sono i malware e come combatterli

Il termine malware indica qualsiasi programma utilizzato per danneggiare un dispositivo, rubare dati o tenere dati d'accesso. Esistono varie tipologie di malware:

1) **Ransomware:** Attualmente una delle minacce più pericolose. Questo malware blocca il dispositivo o cripta tutti i file della vittima chiedendo poi un riscatto in cripto valute per sbloccarlo.
2) **Trojan Horse:** Si nasconde all'interno del programma apparentemente legittimo o utile.Quando l'utente lo installa il trojan si attiva aprendo una backdoor per dare il controllo del dispositivo agli hacker.
3) **Worm:** A differenza dei normali virus, il work non ha bisogno di attaccarsi a un file esistente o dell'azione dell'utente per diffondersi. Sfruttano le falle di sicurezza delle reti per replicarsi automaticamente da un computer all'altro.


Per combattere i malware non basta un buon software, serve anche prudenza digitale.

1) **Installa un buon antivirus**: Per gli utenti di Windows, Windows defender integrato è già un'ottima base, per una protezione extra si possono affiancare strumenti affidabili come Malwarebytes.
2) **Mantieni tutto aggiornato:** I criminali informatici sfruttano la vulnerabilità nei sistemi operativi e nelle app. Aggiorna sempre Windows e i browser che usi
3) **Scarica solo da fonti ufficiali:** Usa il google play store, l'App store o i siti web dei produttori ufficiali. Evita i siti di software piratati che sono la fonte primaria di malware
4) **Usa un account utente standard:**Sul computer non usare quotidianamente l'account da amministratore. Usando un account standard, se un malware dovesse entrare nel sistema, non avrà i permessi per fare danni profondi al sistema

# Sicurezza dell’account

La sicurezza del proprio account è fondamentale per proteggere i dati personali, l’identità e le informazioni finanziarie. Il furto d’identità digitale può avere conseguenze devastanti sulla vita reale come ad esempio le truffe a nome tuo. Se un hacker prende il controllo del tuo account potrebbe inviare messaggi ai tuoi contatti chiedendo denaro urgente a tuo nome. Oppure potrebbe essere usato per attività illecite come la diffusione di malware.

**Per garantire la protezione del proprio account dobbiamo:**

1) **Creare Password forti e uniche:** la password deve essere complessa, ovvero utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli. Non dobbiamo mai utilizzare la stessa password per diversi account e utilizzare un password manager affidabile.

2) **Fare l’autenticazione a 2 fattori**:Scegliere app come google Authenticator aiuta a garantire la sicurezza dell’account. Per gli account critici come l’email principale, l’uso di chiavi hardware come le YubiKey, offre il massimo livello di protezione.

3) **Monitoraggio e manutenzione dell’account:** Controllare gli accessi attivi, Aggiornare i software, verificare i dati di recupero.

# Le fake news ed il fact-checking

Che cosa sono le fake news e la disinformazione e come proteggersi

Create dal gruppo 5:
Pietro longo
Marco Campo
Damiano costantino

# Le fake news e la disinformazione


Le fake news sono un pericolo digitale altamente diffuso. È una strategia utilizzata dai cybercriminali per vari scopi, che siano ‘click baiting’ per consentirgli accesso al dispositivo della vittima, oppure che siano atti giornalistici falsi per diffondere disinformazione nel pubblico per manipolare idee o semplicemente causare danni nella vita di tutti giorni. La disinformazione è il metodo principale dei cybercriminali per spargere chaos, odio o per manipolare elezioni, idee e molto altro mentre rimangono in incognito allo stesso momento. disinformazione è un crimine e pericolo estremamente grave dato che ha il potenziale di rovinare la reputazione e vita di un individuo o comunità.

**<u>Degli esempi di disinformazioni e fake news sono:</u>**

- L’attacco al pentagono del 2023 era un caso di disinformazione online avvenuta tramite un’immagine creata dall’AI che causò un crollo economico momentaneo della borsa di wall street.
- Un’altro esempio sono le elezioni del 2016 dove un gruppo russo diffusero delle informazioni false creando odio nella popolazione americana e influenzando le elezioni presidenziali

# Il Fact-checking


La verifica delle fonti è il muro di difesa principale contro la disinformazione. Una cosa fondamentale è quello di non credere immediatamente a ciò che si legge, ma informarsi se quell'informazione è vera o no.

Ci sono vari metodi per scoprire siti falsi e fake-news:

uno di questi metodi è il controllo del URL dato che i siti falsi di informazione tipicamente copiano il nome del sito originale cambiando solo una lettera (IlFattoQuotidano → IlFattoQuotidiano)

altre strategie sono il cross-checking, cioè il controllo della stessa informazione in più siti affidabili per vedere se è vera o meno, oppure il context-checking, cioè controllare il contesto delle immagini o informazioni dato che una strategia comune è quella di prelevare avvenimenti avvenuti anni prima o in un altro paese e modificarli per causare confusione, paura o odio nella massa.

# Netiquette

Comunicazione online e comportamento responsabile
promuovere una comunicazione rispettosa e consapevole negli ambienti digitali.

**Gruppo 6**
Lo Piccolo Mattia
Marsala Federico
Pirrello Giulio

# Cos'è il Netiquette?

Netiquette è un insieme di regole informali disciplinano il buon comportamento di un utente sul web di Internet, soprattutto nel interagire agli altri utenti attraverso risorse.
Il rispetto della Netiquette non è imposto da alcuna legge, ma sotto un aspetto giuridico, è spesso richiamata nei contratti di fornitura di servizi di accesso da parte dei provider.
Il mancato rispetto della netiquette comporta a una disapprovazione generale da parte degli altri utenti della rete.
La normativa ufficiale del Netiquette fu creata nell'ottobre 1995, RFC 1855 fu creato da Sally Hambridge, che contiene tutte le regole ufficialmente e universalmente riconosciute dai netizen per un buon uso della rete.

# Normative Netiquette

La normativa ufficiale del Netiquette fu creata nell'ottobre 1995, RFC 1855 fu creato da Sally Hambridge, che contiene tutte le regole ufficialmente e universalmente riconosciute dai netizen per un buon uso della rete. Tante delle regole derivano semplicemente dal buon senso, per esempio,

- Se si ha necessità di intervenire in un luogo virtuale di discussione, scrivere nella lingua utilizzata dagli altri membri della discussione.
- Non parlare a nome di un gruppo, organizzazione, impresa o ente se non sei autorizzato a farlo
- Non incitare a compiere o fornire informazioni su come compiere attività illegali, immorali o pericolose per chi le fa o per terzi.
- Non insultare altre persone, scatenare flame o trollare, ma sostenere le proprie opinioni in maniera pacata e civile.
- Non condividere notizie o informazioni di natura complottista o pseudoscientifica, o comunque classificabili come "notizie false"(Fake News).

**Andando in dettaglio nelle seguenti slide, Il Netiquette parla anche:**

# Rispetto ed Empatia Digitale

Dietro ogni schermo c'è una persona reale con sensibilità e sentimenti, ma raramente viene considerato per colpa dell'effetto disinibizione, dove l'assenza di contatto visivo riduce l'empatia e facilita gli attacchi verbali, per contrastare questo effetto, è utile immaginare di essere faccia a faccia con l'individuo. E anche se pensi che cosa vuoi dire potresti anche dirglielo in faccia, è importante non alimentare i cosiddetti "flame".

# Lotta allo Spam e Rilevanza

Il tempo e l'attenzione degli altri utenti sono risorse preziose che non vanno sprecate, perciò evita di inoltrare messaggi di massa, bufale non verificate o allarmismi infondati, e nei forum o nei gruppi tematici, rimani rigorosamente fedele all'argomento principale della discussione. e più importante non usare i tag "@tutti" o "@follower" a meno che non si tratti di comunicazioni di vitale e reale importanza.


# Glossario, buone pratiche e decalogo finale.

*Francesco Piazza*
*Valerio Mazzola*
*Sophia Dia*
*Gruppo 7*

# INTERNET

## Buone pratiche online

Password complesse: Usa chiavi lunghe con lettere, numeri e simboli.

Password uniche: Non utilizzare mai la stessa password su più siti.

Autenticazione a due fattori (2FA): Attivala sempre per proteggere l'accesso ai tuoi account.

Aggiornamenti software: Installa subito gli aggiornamenti di sistema e delle app.

Backup periodici: Salva i tuoi file importanti su hard disk esterni o cloud.

Reti Wi-Fi pubbliche: Evita di accedere a conti bancari quando sei connesso ad esse.

Verifica dei link: Controlla bene l'URL prima di inserire dati sensibili su un sito.

# Decalogo del cittadino digitale

**Proteggi i tuoi dati personali**
Usa password sicure, attiva l'autenticazione a due fattori e condividi online solo ciò che è necessario.
**Verifica le informazioni**
Controlla sempre le fonti prima di credere o condividere notizie, immagini o video.
**Rispetta gli altri online**
Mantieni comportamenti educati nei social, nelle chat e nei forum. Evita insulti, hate speech e cyberbullismo.
**Difendi la tua identità digitale**
Ricorda che ciò che pubblichi può restare online a lungo e influenzare la tua reputazione.
**Usa la tecnologia in modo equilibrato**
Evita l'abuso di smartphone e social network, dedicando tempo anche alle relazioni e attività offline.
**Riconosci i rischi della rete**
Fai attenzione a phishing, truffe online, malware e richieste sospette.
**Rispetta il copyright e il lavoro altrui**
Non copiare contenuti senza autorizzazione e cita sempre le fonti.
**Aggiorna dispositivi e software**
Mantieni sistemi operativi e applicazioni aggiornati per aumentare la sicurezza.
**Partecipa in modo responsabile alla vita digitale**
Usa gli strumenti digitali per informarti, collaborare e contribuire in modo positivo alla società.
**Conosci i tuoi diritti e doveri digitali**
Informati su privacy, sicurezza, identità digitale e norme che regolano il mondo online.

# Questionario finale – Cittadinanza digitale

## Glossario digitale

1. Cos’è il phishing?
2. A cosa serve un antivirus?
3. Che cos’è la privacy online?

## Buone pratiche online

4. Perché è importante usare password sicure?
5. Cosa bisogna fare prima di condividere una notizia?
6. Come ci si deve comportare sui social network?

## Decalogo del cittadino digitale

7. Cosa significa essere un cittadino digitale responsabile?
8. Perché bisogna proteggere i dati personali?
9. Perché è importante rispettare gli altri online?
10. Quale regola del decalogo ritieni più importante? Perché?

# GLOSSARIO

- **Cyberbullismo** → forma di bullismo fatta tramite Internet, social, chat o telefoni.
- **Social network** → piattaforme online dove le persone comunicano e condividono contenuti.
- **Chat** → conversazione scritta online in tempo reale.
- **E-mail** → posta elettronica.
- **Internet** → rete mondiale che collega computer e dispositivi.
- **Virtuale** → qualcosa che esiste online e non fisicamente.

**Tipologie di cyberbullismo**

- **Denigration** → diffusione di bugie o contenuti offensivi per rovinare la reputazione di qualcuno.
- **Impersonation** → fingersi un'altra persona online usando il suo profilo o le sue credenziali.
- **Credenziali** → dati di accesso come username e password.
- **Flaming** → litigi online con messaggi aggressivi e offensivi.
- **Harassment** → molestie ripetute tramite messaggi offensivi o minacciosi.
- **SMS** → messaggio di testo inviato tramite cellulare.

**Privacy e sicurezza**

- **Privacy** → protezione delle informazioni personali.
- **Dati personali** → informazioni che identificano una persona (nome, foto, numero, indirizzo…).
- **GDPR** → legge europea che protegge i dati personali online.
- **Profilo privato** → account visibile solo alle persone autorizzate.
- **Posizione geografica** → luogo in cui si trova una persona.

**Truffe e sicurezza informatica**

- **Phishing** → truffa online che cerca di rubare dati fingendosi un ente ufficiale.
- **Link** → collegamento che porta a una pagina web.
- **Browser** → programma usato per navigare su Internet (es. Chrome, Safari).
- **Malware** → software dannoso creato per rubare dati o danneggiare dispositivi.
- **Software** → programma informatico.
- **Virus** → malware che si diffonde infettando altri file.
- **Spyware** → programma che spia le attività dell'utente.
- **Adware** → software che mostra pubblicità invasive.
- **Trojan** → malware nascosto dentro un programma apparentemente sicuro.
- **Hacker** → persona che entra illegalmente in sistemi informatici.
- **Password** → parola chiave segreta per accedere a un account.
- **Autenticazione a due fattori** → sistema di sicurezza che richiede due verifiche per accedere a un account.
- **Logout** → uscita da un account.
- **App** → applicazione installata su smartphone o computer.

**Informazione online**

- **Fake news** → notizie false diffuse online.
- **Fact-checking** → verifica dei fatti per controllare se una notizia è vera.
- **Fonte** → origine di una notizia o informazione.
- **Opinione pubblica** → insieme delle idee e dei pensieri delle persone su un argomento.

**Comportamento online**

- **Netiquette** → insieme di regole di buona educazione su Internet.
- **Network** → rete di collegamento tra dispositivi o persone.
- **Spam** → invio di messaggi inutili o indesiderati.
- **Like** → apprezzamento espresso sui social con un clic.
- **Commenti social** → messaggi scritti sotto post o contenuti online.
- **Flame** → provocazione o insulto usato per creare discussioni aggressive online.