SAFER INTERNET DAY 2021

#SID2021

Una maggiore consapevolezza del digitale per famiglie, studenti e docenti

SOSprivacy.net
LA PROTEZIONE DEI DATI È PROTEZIONE DELLE PERSONE
GDPR

TOPICS

- Introduzione al tema
- Alcuni dati statistici e non
- Video del Garante della Privacy
- Bonus e Malus della tecnologia
- Fenomeni negativi del web
- Cyberbullismo
- Risposte istituzionali
- Risposte individuali
- Question time

CHE COSA È IL SEFER INTERNET DAY?

Il Safer Internet Day (SID) è un evento annuale, organizzato a livello internazionale con il supporto della Commissione Europea nel mese di febbraio. Si tratta di una ricorrenza istituita nel 2004 promossa in Italia dal progetto «Generazioni Connesse» coordinato dal Ministero dell'Istruzione, dell'Università e della Ricerca.

GENERAZIONE Z: SEMPRE CONNESSA

Lo **smartphone è lo strumento più diffuso tra i ragazzi**, il 97% dei quali lo utilizza quotidianamente per andare online. La percentuale scende al 51% nella fascia d'età tra i 9 e i 10 anni. Le attività online più diffuse sono quelle relative alla comunicazione e all'intrattenimento: il **77% dei ragazzi di 9-17 anni usa internet tutti i giorni per comunicare con amici e familiari**, poco più della metà guarda video online e visita quotidianamente il proprio profilo sui social media. Il **84% usa internet come supporto ai compiti scolastici** . *(indagine di EU Kids Online)*

1 RAGAZZO SU 5 SI DEFINISCE PRATICAMENTE SEMPRE CONNESSO, 6 SU 10 SONO ONLINE DALLE 5 ALLE 10 ORE AL GIORNO (Fonte ricerca di Generazioni Connesse)

Tik Tok

Numeri raddoppiati rispetto allo scorso anno, complici anche i periodi passati a casa, lontano da scuola o da altre attività di socializzazione, durante la pandemia. I social «fanno da padroni».

WHATSAPP

L’app più diffusa resta Whatsapp, utilizzata per scambiarsi messaggi, foto, video e audio da tutti i ragazzi e non solo…

INSTAGRAM

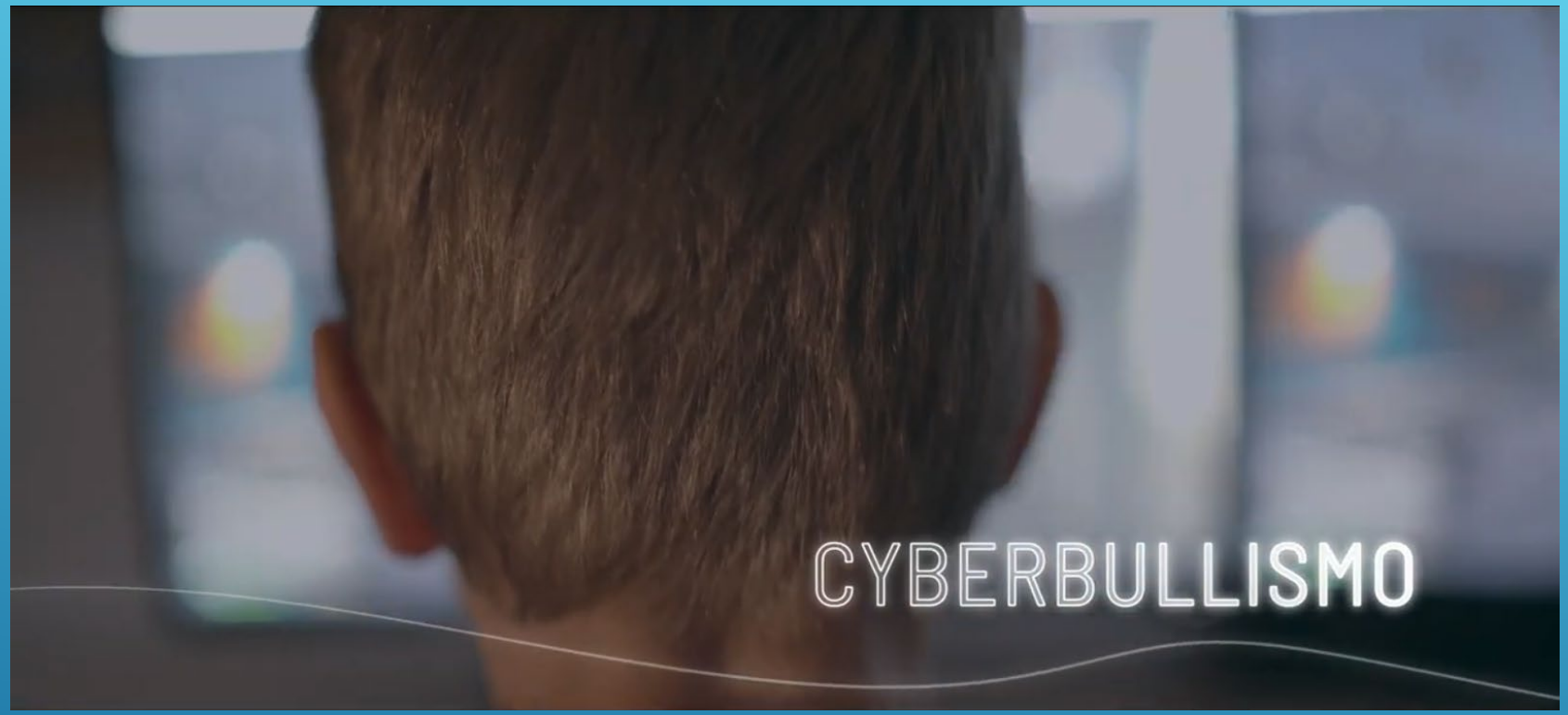
Instagram ha sostituito Facebook nelle preferenze dei «teen». Piace perché “permette maggiore interazione, prende le distanze da politica e da fake news, predilige le fotografie alle parole e si nasconde meglio dalla supervisione di genitori e adulti”.

(Fonte ricerca Unicusano)

TIK TOK

Dall’inizio del 2018, ha fatto registrare un boom di download superando quota 40 milioni. Gli utenti di questo social sono principalmente ragazzi e ragazze di età compresa tra i 13 e i 20 anni che condividono video della durata massima di un minuto in cui principalmente cantano e ballano le canzoni del momento.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Il video del Garante “I tuoi dati sono un tesoro” per raccontare cos’è la privacy
https://www.youtube.com/watch?v=DxQEk_G5gfU

IL COLLEGIO DELL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Insediatosi lo scorso 29 luglio.
Da sinistra verso desta:
Pasquale Stanzione (Presidente)
Ginevra Cerrina Feroni (Vice Presidente)
Agostino Ghiglia (Componente)
Guido Scorza (Componente)

COSA NASCONDONO I RAGAZZI AI PROPRI GENITORI

Una ricerca condotta da Kaspersky Lab rivela che il 36% dei ragazzi nasconde ai propri genitori un'attività online potenzialmente pericolosa. I ragazzi non si rendono conto dell'importanza della privacy, condividendo sistematicamente informazioni personali che possono essere utilizzate da malintenzionati.

BENEFICI DELLA TECNOLOGIA

In un periodo di emergenza pandemica la tecnologia ha permesso di non sospendere del tutto le attività didattiche.

Ha permesso anche di poter continuare a lavorare in smart-working.

Ha permesso di comunicare a distanza con i propri cari.

Ha anche permesso di godere di intrattenimento e di poter acquistare beni e prodotti diminuendo i rischi di contagio.

RISCHI DELLA TECNOLOGIA

Nell'ultimo anno si è riscontrare una massiccia sovra-esposizione dei nostri dati in rete.

Andare «offline» diventa sempre più difficile.

Nel 2020 c'è stato un aumento del 240% di attacchi informatici.

Un report della Polizia Postale rileva un aumento del 430% di segnalazioni di fake news.

La tecnologia è neutra, sono i comportamenti e gli utilizzi che ne fanno i soggetti a determinarne l'inclinazione.

CYBERBULLISMO

Il **fenomeno del cyberbullismo** viene definito nella **legge 71/2017**

"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"
entrata in vigore il 18 giugno 2017:

«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. (Art.1)». Inoltre indica misure di carattere preventivo ed educativo nei confronti dei minori (qualunque sia il ruolo nell'episodio) da attuare in ambito scolastico ed extrascolastico.

- Direttiva Ministeriale n. 16 del 5 febbraio 2007 - Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo
- Direttiva Ministeriale del 15 marzo 2007 - Linee di indirizzo utilizzo telefoni cellulari

SOSprivacy.net
LA PROTEZIONE DEI DATI È PROTEZIONE DELLE PERSONE

CYBERBULLISMO *RISCHI*

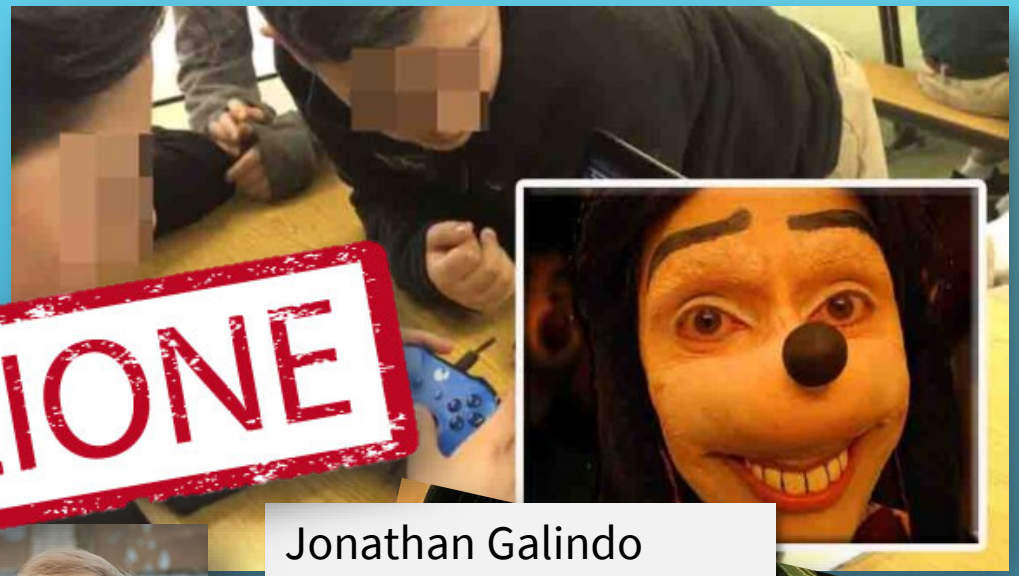
I **danni** del *cyberbullismo* alla sfera emotiva possono essere alla lunga anche molto **seri**.

Gli effetti negativi possono ricadere sul benessere sociale, su quello emotivo e su quello scolastico delle vittime:
il **malessere** viene spesso espresso attraverso ansia, bassa concentrazione e un rendimento scolastico che peggiora e (anche se raramente) può sfociare in comportamenti più gravi come depressione e tentativi di **suicidio**.
Alcune volte le vittime diventano a propria volta «carnefici».

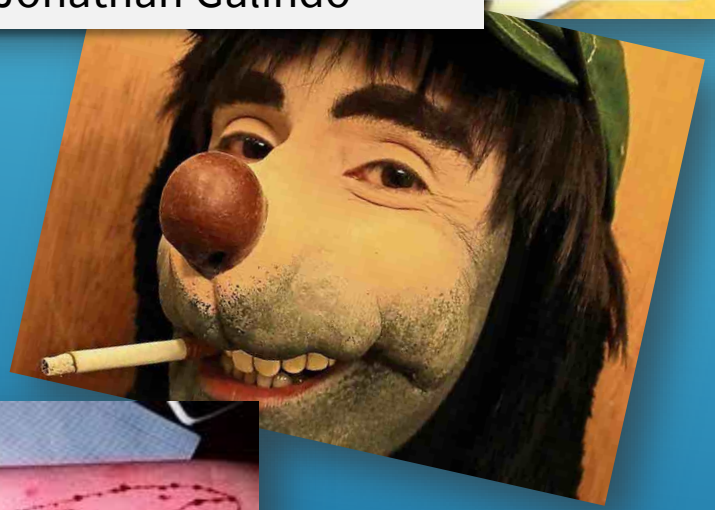
Ma ci sono conseguenze che coinvolgono anche i *cyberbulli*.
Questi ultimi infatti possono essere maggiormente a rischio di sviluppo di comportamenti antisociali e di problemi relazionali, **delinquenza**, abuso di sostanze e **suicidio**.
(D.ssa Cristiana Sclano, psicologa)

#MomoChallenge

ATTENZIONE



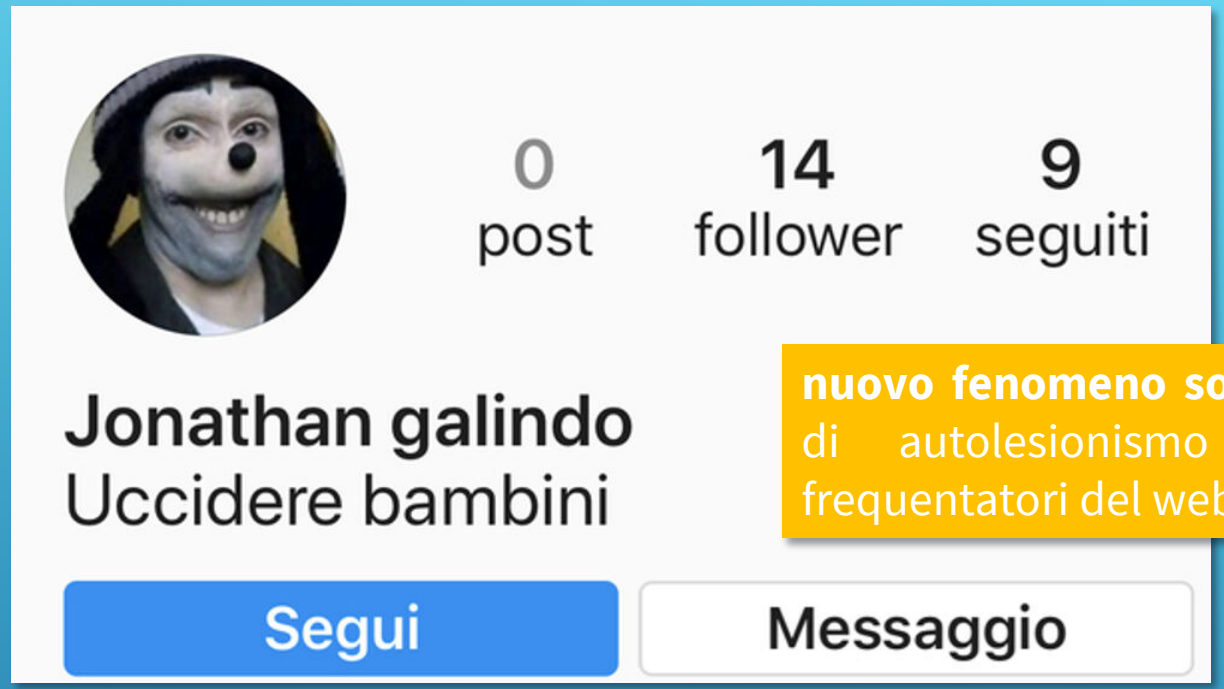
Jonathan Galindo



Selfie estremi

Blue Whale

SOSprivacy.net
LA PROTEZIONE DEI DATI È PROTEZIONE DELLE PERSONE
GDPR



nuovo fenomeno social che indurrebbe atti di autolesionismo tra i più giovani frequentatori del web.

Tale "Jonathan Galindo" **chiederebbe l'amicizia** a bambini e adolescenti su Instagram, Facebook e Tik Tok, mandando un messaggio privato e chiedendo se "**vogliono giocare**".

Chi si nasconde dietro l'account trascinerebbe le sue vittime in una serie di "**sfide**" che arriverebbero **fino all'autolesionismo** e al **suicidio**.

E' appurato che le immagini dei vari profili social di Jhonatan Galindo, che di volta appaiono e poi vengono chiusi, sono di un creatore di maschere speciali (creepy).

Sembra che **una o più persone** si **nasconderebbe** dietro le immagini per far partire le sfide.

CYBERBULLISMO

CARATTERISTICHE

- **PERVASIVITA':** il cyberbullo è sempre presente sulle varie tecnologie usate;
- **INDIFFERENZA**: nella volontarietà dell'aggressione: non sempre gli effetti negativi sono provocati da un'azione mirata in quanto, potendo osservare le reazioni della vittima, si commettono atti persecutori non comprendendo che ci si è spinti troppo oltre;
- **AMPIEZZA DI PORTATA:** i messaggi e i materiali inviati sono trasmessi, ritrasmessi e amplificati oltre la cerchia dei conoscenti;
- **ATTIVAZIONE MECCANISMI DI DISIMPEGNO MORALE**, come la *minimizzazione*: gli atti che si sono compiuti etichettandoli come «solo uno scherzo», «ciascuno è libero di buttarsi nel pozzo»;
- **DIFFUSIONE DELLA RESPONSABILITA':** «non è colpa mia, lo facevano tutti» oppure «io non ho fatto niente, ho solo postato un messaggio che mi era arrivato»;
- **AMPLIFICARE LE PROPRIE IMPRESE :** mettere un video in rete è un modo per ottenere apprezzamenti da una platea molto vasta e sentirsi dei leader;
- **NICKNAME:** il cyberbullo non si manifesta in contatto diretto, faccia a faccia, non è una presenza fisica;
- **NON RICEVERE IL FEED-BACK IMMEDIATO E TANGIBILE DELLA VITTIMA:** non vedere il dolore e i danni che la propria condotta può aver causato e non cogliere le conseguenze delle proprie azioni.

CYBERBULLISMO

TIPOLOGIE SU WEB

FLAMING: si tratta di messaggi online violenti e volgari che si trovano spesso sui forum, sui gruppi online che servono per aizzare, provocare e ovviamente umiliare i malcapitati;

IMPERSONATION: conosciuto come lo *scambio di persona*. Si mandano messaggi fingendosi altri per mandare messaggi online o pubblicarli ingannando la persona;

TRICKERY: Si cerca di ottenere la fiducia di un ragazzo o una ragazza per poi fare uno scherzo crudele;

CYBERSTALKING: come lo stalking, sono molestie ripetute sul web e minacce vere e proprie per provocare la paura;

DOXING: è la diffusione via internet di dati personali e sensibili;

DENIGRATION: sparlare di qualcuno sul web, danneggiarlo pubblicamente;

BODY SHAMING: l'individuo viene giudicato sui social per il proprio aspetto fisico;

CYBERBASHING: quando un gruppo di ragazzi maltratta o picchia un coetaneo (in certi casi anche docenti o adulti), e si aggiunge qualcuno che riprende il tutto facendo un video dell'aggressione e pubblicandolo su internet. Il video viene poi visualizzato da tantissime persone.

HARASSMENT: vere e proprie molestie via web. Arrivare a provocare danni fisici. Sono noti i casi di *Blue Whale, MomoChallenge, Jonathan Galindo.*

REVENGE PORN*:* la diffusione illecita di immagini o video sessualmente espliciti, spesso manipolati digitalmente, destinati a rimanere privati, senza il consenso delle persone rappresentate; sia da di chi le invia e da di chi le riceve che contribuisce alla loro ulteriore diffusione.

LE *CHALLENGE* ESEMPI

COSA SONO

Sfide che vengono **lanciate sui social** allo scopo di essere diffuse e diventare virali. **Alcune challenge espongono a rischi medici** (assunzione di saponi, medicinali, sostanze di uso comune come cannella, sale, bicarbonato etc), **altre inducono a compiere azioni** che possono produrre gravi ferimenti a se' o agli altri (selfie estremi, soffocamento autoindotto, sgambetti, salti su auto in corsa, distendersi sui binari, etc);

DOVE

Le azioni di vario tipo oggetto della sfida vengono fotografate o filmate, si taggano amici e conoscenti e si pubblicano sui vari canali **social** sperando di dare il via al contagio.

Secondo le ricerche pubblicate da Skuola.net 1 ragazzo su 6 conosce questa challenge online e 1 su 5 ha sfidato sé stesso almeno una volta.

I PROMOTORI

Sembra che la challenge della ***Blue Whale*** si dimostrò una bufala, frutto perlopiù della **psicosi** che si diffuse **tra genitori e parenti di adolescenti e preadolescenti** alle prime notizie riguardanti la stessa.

Anche il CICAP si è interessato della faccenda.

RISPOSTE ISTITUZIONALI

Il Garante per la Protezione dei Dati Personali ha creato sul proprio sito istituzionale una sezione apposita per la tutela dei minori (www.garanteprivacy.it/minori).

Nella sezione sono presenti alcune campagne di sensibilizzazione. Ad esempio: «Consigli ai "GRANDI" per un utilizzo sicuro da parte dei "PICCOLI"», «I suggerimenti del Garante per tutelare la tua privacy quando pubblichi immagini online»

LA CAMPAGNA INFORMATIVA DEL GARANTE E DI TELEFONO AZZURRO

HTTPS://WWW.YOUTUBE.COM/WATCH?V=9NCKMSLOAAU

CYBERBULLISMO

OBBLIGHI PER LA SCUOLA E RESPONSABILITÀ

La normativa prevede che ogni **scuola** individui un **responsabile al cyber bullismo** (un insegnante) e faccia formazione sul tema.
Dirigenti, docenti e personale hanno precisi obblighi in merito.

Chiunque assista a episodi di bullismo senza intervenire ne può rispondere in sede penale e civile.

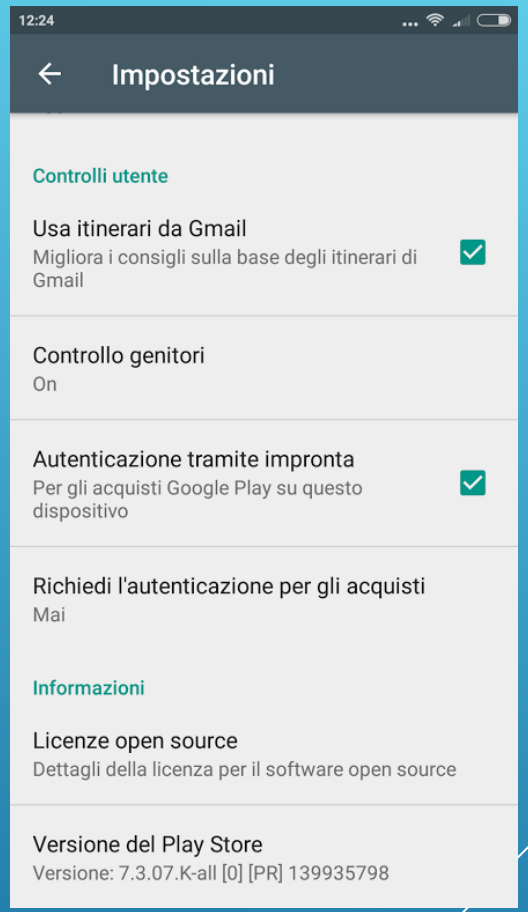
Anche i **genitori** del carnefice minore (bullo) **sono imputabili** per *culpa in educa*ndo.

RISPOSTE PERSONALI

La prima risposta immediate è il **Parental Control**, un sistema che permette ad un genitore di monitorare o bloccare l'accesso a determinate attività da parte del ragazzo e permette anche di impostare il tempo di utilizzo dell'apparecchio utilizzato.

PARENTAL CONTROL

Per Android: andare nelle impostazioni del Google Play Store, e scegliere Controllo Genitori, verrà chiesto di inserire un PIN che servirà a disattivare il controllo parentale. Fatta questa operazione si potranno impostare le varie restrizioni sui contenuti (un vero e proprio filtro bambini) e controllare quindi le applicazioni e i giochi che si potranno o meno scaricare su quel dispositivo. Un'altra opzione di Android molto utile permette di attivare un account famiglia con i numeri di tutti i cellulari presenti all'interno del nucleo familiare: in questo modo dopo averli aggiunti al gruppo creato attraverso il Google Play Store, il titolare del gruppo può decidere di limitare alcuni contenuti e l'acquisto delle applicazioni direttamente dalla gestione del gruppo, attivando il controllo parentale solo sugli account dei propri figli.



PARENTAL CONTROL

Per sistemi IOS basta entrare nelle “Impostazioni” del dispositivo, cliccare su “Generali” ed entrare ancora nella voce “Restrizioni”. Si entra così in una nuovo menù in cui si potrà impostare l'attivazione del controllo genitori, e anche in questo caso vi verrà richiesto un PIN che servirà a bloccare la pagina di sblocco del parental control. Una volta impostato il codice potrete scegliere le applicazioni che si potranno utilizzare, quelle che volete tenere sotto controllo genitori o bloccare in maniera totale. Il consiglio è di abilitare di sicuro il blocco bambini dell'acquisto in app, visto che anche in maniera distratta o non voluta un ragazzo potrebbe acquistare varie applicazioni o upgrade. Sarà opportuno attivare anche il blocco bambini sull'eliminazione delle applicazioni in modo da non ricevere brutte sorprese di perdita di dati, come magari nel caso di un’app in cui avete contatti di lavoro o appunti.

APP CONTROLLO GENITORI

Una tra le più utilizzate è sicuramente “Kids Place Parental Control”, app che permette di selezionare quali applicazioni e quali operazioni chi utilizza il cellulare può compiere; ovviamente anche in questo caso vi verrà richiesto di impostare un PIN prima di iniziare ad usarla. È possibile attraverso questo tipo di applicazione limitare l'accesso ad internet per un dato periodo di tempo e l'apertura di applicazioni -quali ad esempio i giochi- solo in una determinata fascia oraria. Sui vari store sono ormai molte le opzioni per il parental control e tutte di facile utilizzo.

CYBERBULLISMO

COME DIFENDERSI

- **non rispondere ai messaggi provocatori** e arrivare a bloccarne gli autori (su social, whatsapp ecc);
- **fare copia di qualche messaggio emblematico** per una successiva denuncia;
- **segnalare il contenuto e l'autore** alla piattaforma del *social*, che può così intervenire cancellando il primo e bloccando il secondo;
- **limitare la privacy dei propri contenuti e foto** e **controllare** chi ci possa taggare (limitando questa funzionalità);
- Per contenuti persecutori sul web, è possibile **chiedere a Google la rimozione dal motore,** così come **al gestore del sito** e **al suo hosting** provider (rilevabile via *Whois*).

➢ Il passo successivo è **denunciare il comportamento** e un giudice può tra l'altro, anche in via cautelativa, ordinare ai provider internet di oscurare quel contenuto illecito.

CYBERBULLISMO *TUTELA DEI MINORI*

Quando i reati sono commessi da minori tra 14 e 18 anni, a giudicare è il **Tribunale per Minori** che:

- in **sede civile** si attiva su ricorso dell'interessato o del pm minorile (su segnalazione da forze dell'ordine, scuole ecc);
- e in **sede penale** via procura minorile per episodi di (cyber)bullismo con rilevanza penale.

Episodi di bullismo sono perseguibili a querela **entro tre mesi** dall'accaduto: lesioni lievi (582 cp), minacce (612 cp), ingiurie (591 cp), diffamazione (595 cp).

Come fare : consigli della Polizia Postale - 1

1. **parlate** ai ragazzi **delle nuove sfide** che girano in rete in modo che non ne subiscano il fascino se ne vengono al corrente da coetanei o sui socialnetwork;
2. **assicuratevi che abbiano chiaro quali rischi** si corrono a partecipare alle challenge online. I ragazzi spesso si credono immortali e invincibili perché “nel fiore degli anni”: in realtà per una immaturità delle loro capacità di prevedere le conseguenze di ciò che fanno potrebbero valutare, come innocui comportamenti letali;
3. **monitorate la navigazione** e l’uso delle app social, anche stabilendo un tempo massimo da trascorrere connessi;
4. **mostratevi curiosi** verso ciò che tiene i ragazzi incollati agli smartphone: potrete capire meglio cosa li attrae e come guidarli nell’uso in modo da essere sempre al sicuro.

Come fare : consigli della Polizia Postale - 2

5. **se trovate** in rete **video** riguardanti **sfide pericolose**, **se** sui social compaiono **inviti** a partecipare a challenge, **se** i vostri figli **ricevono** da coetanei video riguardanti le sfide … **segnalateli** subito a **www.commissariatodips.it**
6. **tenetevi sempre aggiornati** sui nuovi rischi in rete con gli ALERT che vengono pubblicati sul portale
   - www.commissariatodips.it e
   - sulle pagine Facebook **Una Vita da Social** e **Commissariato di PS Online**
   - **sulla pagina del Garante della Privacy**
   - **sulle pagine delle diverse associazioni di tutela**

E RICORDIAMOCI CHE

NON ESISTE LA PRIVACY ONLINE, ogni nostra azione è memorizzata e analizzata da almeno 500 soggetti diversi, pochissimi dei quali interessati a tutelare noi, i nostri diritti, i nostri cari, la nostra salute.