S.O.S.C.

SEZIONE OPERATIVA per la SICUREZZA CIBERNETICA

BRESCIA

Vivere nel mondo digitale

RELATORI:

Ispettore Superiore Samantha FESTA

Assistente Capo Coordinatore Simone Olivieri

18 marzo 2025

LA POLIZIA POSTALE E DELLE COMUNICAZIONI

Le competenze specifiche sono state delineate dal cosidettto Decreto Minniti del 15/08/2017

Pedofilia e pedopornografia online – adescamento online - Cyberbullismo
Hacking e Ransomware
CyberTERRORISMO
Frodi finanziarie telematiche
Cybercrime indotto

Acquisizione notizie di reato,
attività investigativa d'iniziativa e su delega A.G.,
analisi forensi……
perquisizioni Informatiche.

INTERNET…LE OPPORTUNITA’

- ✓Facilità estrema nelle comunicazioni
- ✓Accessibilità di notizie
- ✓Scambio di informazioni in tempo reale
- ✓Possibilità di conoscere realtà e persone di tutto il mondo
- ✓Disponibilità di diversi servizi (e-commerce, e-mail, chat line,
- ✓pagine web piene di informazioni varie, newsgroup di diverse tematiche…)
- ✓Applicazioni (APP) che consentono di fare qualsiasi cosa (quasi tutto)….



Molestie, Adescamento

Bullismo/Cyberbullismo





Produzione/Divulgazione di Foto e/o Video inappropriati

Truffe e-commerce



POLIZIA POSTALE

I PERICOLI

NATIVI DIGITALI vs IMMIGRATI DIGITALI

TENDENZA ad abdicare ad una parte del loro ruolo educativo?????!!!!

MANCANZA DELLA CULTURA della sicurezza informatica-telematica

NATIVI DIGITALI vs IMMIGRATI DIGITALI

IGNORARE le più elementari regole di difesa da adottare durante la navigazione nella rete.

<u>sottovalutazione delle conseguenze</u> che possono scaturire da questa condotta omissiva nella delicata fase adolescenziale dei propri ragazzi.

sostanziale differenza di gusti e di obiettivi nello sfruttamento delle potenzialità del servizio telematico tra genitori e figli

I ragazzi utilizzano Internet ovunque….

4. I ragazzi creano dei profili estremamente personalizzati, esponendosi a tutti i pericoli della rete.

5. Esiste un pericolo reale legato a una scarsa attenzione dei ragazzi a proteggere le password degli account di accesso ai servizi internet.

6. **I ragazzi ignorano le regole che regolano il vivere civile** e, soprattutto nell'ambito virtuale, tendono a sottovalutare le conseguenze delle proprie azioni

Alcuni consigli.....

•Affiancate i più piccoli sin dalle prime navigazioni in rete in modo da capirne gli interessi e fornire consigli sui siti da evitare e su quelli che, invece, si possono visitare in sicurezza.

•Non lasciate i bambini e i ragazzi da soli a navigare troppe ore su internet: stabilite quanto tempo possono passare navigando per limitare l´esposizione ai rischi della Rete.

•Insegnate l'importanza di mantenere riservata l'identità in rete: spiegategli che è importante non fornire dati personali come nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici ad altri utenti di siti e social network, sia a garanzia della loro tutela che per quella della propria famiglia.

•Cercate di stare vicino ai bambini/ragazzi quando creano profili personali sui social network: valutate insieme quale foto sia migliore per il profilo, selezionate insieme le impostazioni di privacy scegliendo con accuratezza a chi saranno visibili i contenuti condivisi in rete, limitate la pubblicazione di contenuti/informazioni troppo personali. NB: la gran parte dei social network prevede, quale età minima per l'iscrizione ai social network, 13 anni.

•Spiegate ai bambini che può essere pericoloso compilare moduli on line e dite loro di farlo solo dopo avervi consultato.

•Dite ai bambini/ragazzi di non rispondere alle provocazioni sui social e nelle chat; invitateli a non usare un linguaggio volgare, inappropriato, aggressivo e a comportarsi correttamente in rete.

app FAMILY LINK

POLIZIA POSTALE

Alcuni consigli.....

•Qualora vostro figlio sembri non interessato a internet, ai social o agli smartphone spiegategli comunque come navigare in sicurezza: stimolato da amici o conoscenti o per mera curiosità, potrebbe avere voglia di usare questi strumenti ed è utile che conosca le forme principali di tutela.
•Se avete un computer fisso, collocatelo in una stanza centrale della casa piuttosto che nella camera dei ragazzi, per poter controllare in maniera discreta i contenuti visitati. Se invece avete tablet o smartphone, stabilite la semplice regola di consentirne l'uso in una zona centrale della casa in modo da sorvegliare senza far sentire vostro figlio "sotto controllo".
•Leggete le e-mail e i messaggi sui social dei minori più piccoli, visionando anche gli allegati. Se non conoscete il mittente non aprite i messaggi né eventuali allegati: questi possono contenere virus o spyware in grado di alterare il funzionamento del vostro dispositivo. Date le stesse indicazioni ai ragazzi più grandi.

Alcuni consigli.....

•Insegnate ai vostri figli di non acconsentire alle richieste di incontrare personalmente chi hanno conosciuto in Rete. Spiegate loro che le persone conosciute in chat o sui social network utilizzano, molto spesso, identità false per poter entrare in contatto con i minori e approfittare della loro buona fede.
•Spiegate ai ragazzi che ciò che fanno su internet non rimane anonimo ma lascia tracce informatiche che permettono di risalire agli autori delle condotte in rete.
Stabilite quanto tempo possono passare navigando su Internet.
La migliore garanzia di tutela per i minori, in generale, è non lasciarli soli in un ambiente popolato da adulti come la Rete.



IMPUTABILITA’ PENALE

Art. 98.

Minore degli anni diciotto.

E' imputabile chi, nel momento in cui ha commesso il fatto, aveva compiuto i quattordici anni, ma non ancora i diciotto, se aveva capacità d'intendere e di volere; ma la pena è diminuita.

ALCUNI REATI

- Truffa: art. 640 c.p.
- Frode informatica: art. 640 *ter* c.p. (phishing)
- Accesso abusivo a sistema informatico: art. 615 *ter* c.p.

ESEMPI

- Truffe on line: siti e-commerce truffaldini che dopo aver ricevuto il pagamento non inviano la merce ordinata;
- Falsa assicurazione auto/moto: soggetti che si sostituiscono a reali imprese assicuratrici vendendo polizze in realtà inesistenti;
- Truffa «romantica»: parte da una semplice richiesta di amicizia sui social fino ad arrivare a pressanti richieste di denaro.
- Truffa del bancomat
- Trading on line

ESEMPI DI PHISHING

- Si tratta di una truffa informatica finalizzata a carpire informazioni sensibili come account di home-banking per poi impossessarsi del credito giacente sul conto, ma anche informazioni personali utili per il furto di identità.

INVIO SMS (cd. «Smishing»)

Prevede l'invio, da parte dei rei, di sms apparentemente provenienti dall'istituto di credito, nei quali si avvisa l'utente che il proprio conto bancario ha avuto dei problemi e invita il titolare ad aprire un *link* , ove l'estensione dell'url a volte fa riferimento all'istituto di credito.

VOICE PHISHING (cd. «Vishing»)

Gli aggressori sfruttano la tecnologia della telefonia IP, per effettuare un gran numero di **chiamate fraudolente** e rubare così dati, password o informazioni bancarie da ignare vittime.

REATI CONTRO LA PERSONA

- PEDOPORNOGRAFIA ON LINE
- DIFFAMAZIONI ON LINE
- SOSTITUZIONI DI PERSONA
- REVENGE PORN
- MOLESTIE
- STALKING
- CYBERBULLISMO
- SEX EXTORTION

I REATI CONTRO LA PERSONA:
I DELITTI DI PEDOFILIA E PEDOPORNOGRAFIA ON-LINE

PRODUZIONE

COMMERCIALIZZAZIONE

DIFFUSIONE

DETENZIONE

MATERIALE PEDOPORNOGRAFICO



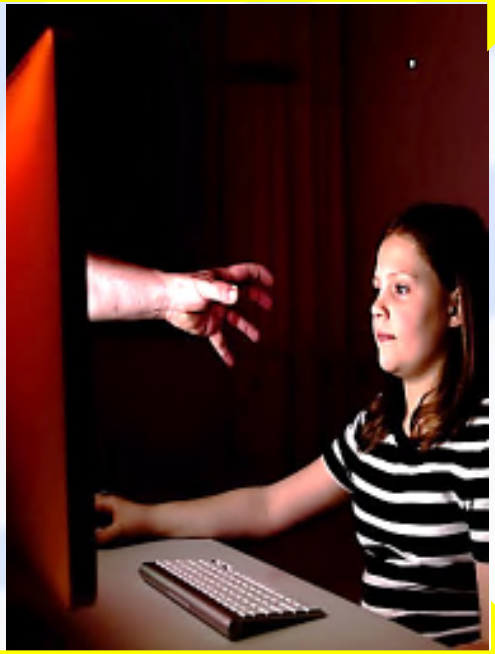
I REATI CONTRO LA PERSONA:
LE NUOVE FORME DI VIOLENZA «TECNOMEDIATA» SUI MINORI

EVOLUZIONE TECNOLOGICA DELLA COMUNICAZIONE



contatto FISICO tra carnefice e vittima

contatto VIRTUALE tra carnefice e vittima



NUOVE FORME DI VIOLENZA «TECNOMEDIATA» SUI MINORI

LA PEDOFILIA ON-LINE



Riprendere scene di sesso esplicito (anche col consenso dei soggetti ritratti) che possono in futuro essere "postate" su un *blog* o pubblicate in un sito o diffuse attraverso programmi di *file-sharing* può comportare gravi conseguenze

- ✓ Un file condiviso non può essere sottratto definitivamente dal circuito di condivisione (cfr. film "Social Network": su internet si scrive ad inchiostro, non a matita)
- ✓ Il rischio per gli autori è di essere perseguiti per produzione e/o divulgazione, o detenzione di materiale pedopornografico

Art.600 ter c.p.

Realizzazione o produzione di materiale pedo-pornografico

Art.600 quater c.p.

Procurarsi o detenere materiale pedo-pornografico

Art.595 co 3° c.p.

Diffamazione *on-line*

STRUMENTI NORMATIVI PER IL CONTRASTO ALLA PEDOPORNOGRAFIA

Art. 600-quater. Detenzione di materiale pornografico Chiunque, … , consapevolmente si procura o **detiene** materiale pornografico realizzato utilizzando minori degli anni diciotto…	**pena < 3 anni**
Art. 600-ter c.4. Pornografia minorile Chiunque, …, **offre o cede ad altri**, anche a titolo gratuito, il materiale pornografico…	**pena < 3 anni**
Art. 600-ter c.3. Pornografia minorile Chiunque, … , con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, **diffonde** o pubblicizza il materiale pornografico…	**pena 1< > 5 anni**
Art. 600-ter c.1 e 2. Pornografia minorile Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o **produce** materiale pornografico ovvero induce minori degli anni diciotto a partecipare ad esibizioni pornografiche… Chiunque ne fa commercio	**pena 6 < > 12 anni**
Art. 600-bis c.1. Prostituzione minorile Chiunque induce, favorisce o **sfrutta** la prostituzione…	**pena 6 < > 12 anni**

STRUMENTI NORMATIVI PER IL CONTRASTO ALLA PEDOPORNOGRAFIA

Art. 600-bis c.2. Prostituzione minorile Chiunque compie **atti sessuali** con un minore tra i quattordici e i diciotto anni in **cambio di denaro** o di altra utilità economica	**pena** **6 mesi < > 3 anni**
Art. 609-quater. Atti sessuali con minorenne Chiunque compie **atti sessuali** con persona che al momento del fatto **non ha compiuto** gli anni quattordici	**pena** **5 < > 10 anni**
Art.609-octies. Violenza sessuale di gruppo Chiunque commette atti di **violenza sessuale di gruppo** (partecipazione di più persone riunite) …	**pena** **6 < > 12 anni**

STRUMENTI NORMATIVI PER IL CONTRASTO ALLA PEDOPORNOGRAFIA

Art. 609-undecies - Adescamento di minorenni. Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, **adesca un minore di anni sedici**, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione.	**pena 1 <** **> 3 anni**

Cyberbullismo

IL CYBERBULLISMO E' UN FENOMENO RECENTE PER IL QUALE I MINORI UTILIZZANO I NUOVI MEDIA PER VEICOLARE O METTERE IN ATTO AZIONI VESSATORIE, PERSECUTORIE O LESIVE DELLA DIGNITA' DEI COETANEI.



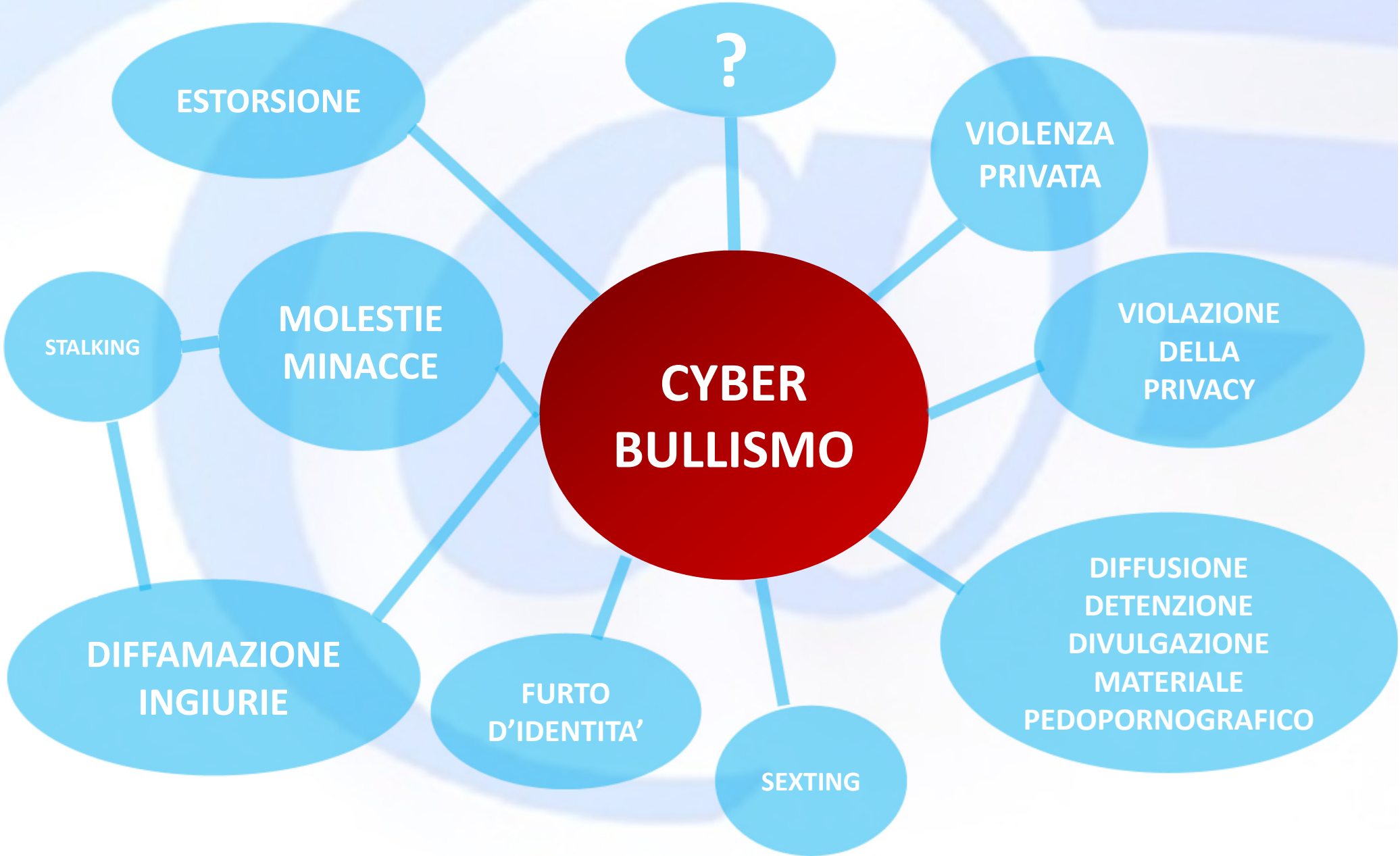
LA NUOVA LEGGE N.71 DEL 2017 RECANTE «*DISPOSIZIONI A TUTELA DEI MINORI PER LA PREVENZIONE ED IL CONTRASTO DEL FENOMENO DEL CYBERBULLISMO*» HA INTRODOTTO UNA DEFINIZIONE UNIVOCA DEL FENOMENO , STABILENDO CHE PER CYBERBULLISMO SI DEVE INTENDERE «*QUALUNQUE FORMA DI PRESSIONE, AGGRESSIONE, MOLESTIA, RICATTO, INGIURIA, DENIGRAZIONE, DIFFAMAZIONE, FURTO D'IDENTITA', ALTERAZIONE, ACQUSIZIONE ILLECITA, MANIPOLAZIONE, TRATTAMENTO ILLECITO DI DATI PERSONALI IN DANNO DI MINORENNI, REALIZZATA PER VIA TELEMATICA, NONCHE' LA DIFFUSIONE DI CONTENUTI ON LINE AVENTI AD OGGETTO ANCHE UNO O PIU' 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.*

AZIONI TIPICHE DEL CYBERBULLISMO

- **FLAMING: messaggi violenti e volgari che mirano a suscitare contrasti e battaglie verbali negli spazi web;**
- **MOLESTIE: invio ripetuto di messaggi offensivi e sgradevoli;**
- **DENIGRAZIONI: insultare o diffamare qualcuno online attraverso dicerie, pettegolezzi e menzogne, spesso offensive e crudeli, volte a danneggiare la reputazione di una persona;**
- **FURTO D'IDENTITA': l'aggressore ottiene le informazioni personali e i dati di accesso di un account della vittima, col lo scopo danneggiarne la reputazione;**
- **OUTING: diffondere online i segreti di qualcuno, informazioni scomode o immagini personali;**
- **EXCLUSION: escludere intenzionalmente qualcuno da un gruppo on line;**
- **CYBERSTALKING: invio ripetuto di messaggi intimidatori contenenti minacce e offese.**

FATTISPECIE DI REATI CONNESSI AL CYBERBULLISMO

(L.71/2017)-Prepotenza virtuale reiterate nel tempo fra pari.



PREVENZIONE E CONTRASTO IN AMBITO SCOLASTICO

- Art. 4 L. 127/2017 prevede la collaborazione della Polizia Postale per la prevenzione e il contrasto del cyberbullismo in ambito scolastico.



La legge n. 70 del 17 maggio 2024 prevede l'introduzione della definizione di "bullismo", che include aggressioni o molestie reiterate, da parte di una singola persona o di un gruppo di persone, in danno di un minore o di un gruppo di minori, idonee a provocare sentimenti di ansia, di timore, di isolamento o di emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni. Viene poi previsto dalla nuova legge il potenziamento del servizio di supporto psicologico agli studenti, consentendo alle Regioni di attivare, presso le istituzioni scolastiche, un servizio di assistenza psicologica per favorire lo sviluppo e la formazione degli studenti e prevenire situazioni di disagio, anche attraverso il coinvolgimento delle famiglie.La legge n. 70/2024 introduce anche nuove norme per la prevenzione e il contrasto del bullismo e del cyberbullismo negli istituti scolastici, prevedendo che ogni scuola istituisca un tavolo permanente di monitoraggio, composto da rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti di settore e che adotti un codice interno per la prevenzione e il contrasto di questi fenomeni.Inoltre, se un dirigente scolastico viene a conoscenza di atti di bullismo o cyberbullismo, è tenuto a informare tempestivamente i genitori e promuove adeguate iniziative di carattere educativo nei confronti dei minori coinvolti.

IL REFERENTE SCOLASTICO PER IL CYBERBULLISMO

- Ogni istituto scolastico deve individuare fra i propri docenti un **referente** con il compito di coordinare le iniziative di prevenzione e di **contrasto del cyberbullismo**.
- Questi ha il compito di promuovere l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche (anche avvalendosi della collaborazione della Polizia Postale).
- Salvo che il fatto costituisca reato, il referente d'intesa con il dirigente scolastico informa tempestivamente i soggetti esercenti la potestà genitoriale di ogni atto riconducibile al cyberbullismo.

L'AMMONIMENTO DEL QUESTORE

Art. 7 L. 71/2017

Viene ribadito il ruolo di «Autorità di Prevenzione Sociale» già emerso con i Decreti Legge n. 11/2009 (prevenzione di atti persecutori) e n.93/2013 (prevenzione delle violenze domestiche).



Procedura applicativa

Sono richiamate le medesime condizioni previste per l'ammonimento per atti persecutori (D.L. 11/2009), ovvero:

- Non deve essere stata proposta querela per i reati di cui agli art. 594 (ingiuria), 595 (diffamazione) e 612 (minaccia) del c.p. o per il reato di cui all'art. 167 del d. lvo n. 196/2003 (trattamento illecito di dati).

(non sono riportate tutte le condotte richiamate nella definizione di cyberbullismo)

- È necessaria una esplicita richiesta di ammonimento da parte dell'interessato, il Questore non può mai procedere d'Ufficio
- Ai fini dell'ammonimento il Questore convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale



- Non è necessaria una piena prova di fatti costituenti reato ma è sufficiente che dall'attività investigativa emergano oggettivi elementi di fatto in ordine al verificarsi di un comportamento riconducibile al cyberbullismo (ELEMENTI DI FATTO IDONEI)
- Il provvedimento di ammonimento deve non solo contenere indicazioni volte a rispettare la legge e a non commettere altri atti di cyberbullismo ma deve altresì essere ritagliato sulla persona del giovane ammonito
- Gli effetti del provvedimento cessano con il compimento della maggiore età

AL QUESTORE DELLA PROVINCIA DI .....

La sottoscritta Nata il_____a..... Residente in_____via_____

Avente n. tel..____ e-mail _

non avendo ancora sporto querela per i fatti di seguito narrati, non ravvisandosi reati procedibili d'ufficio

C H I E D E

che la S.V. proceda alla completa identificazione ed all'ammonimento nei confronti del/della Sig./Sig.ra il/la quale, con le proprie reiterate condotte di stalking qui allegate, ha costretto la sottoscritta a modificare radicalmente le proprie consuete abitudini di vita, ingenerando il fondato timore per la propria incolumità , causando, per tali motivi, un perdurante e grave stato di ansia e di paura.

La sottoscritta, si riserva inoltre la facoltà di sporgere querela nei confronti del/della Sig./Sig.ra_____, nei previsti termini di legge, OSSIA entro sei mesi dai fatti. Indica come testimoni dei fatti le seguenti persone:

Produce la seguente documentazione medica certificativa dello stato d'ansia:

Produce la seguente documentazione:

- Fotografie;
- Lettere;
- Sms;

Luogo e data _____

La Richiedente

RICAPITOLANDO:
Cosa fare contro il cyberbullo

MESSAGGI OFFENSIVI O TROPPO SPINTI

- Non rispondere alle provocazioni
- Blocca il mittente
- Cambia il numero di cellulare o l'indirizzo e-mail se possibile

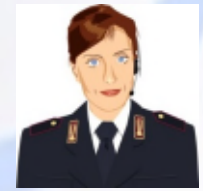
FURTO DI IDENTITA'

- Segnala l'abuso il prima possibile al social network (Facebook, youtube, etc.)
- Blocca e fai bloccare ai tuoi utenti il profilo falso
- Cambia la password

PUBBLICAZIONE DI VIDEO O IMMAGINI

- Segnala l'abuso alla piattaforma (youtube, intagram etc.)
- Non inserire commenti

Conserva tutte le tracce (messaggi, video, link) e parlane con un adulto (docenti, genitori, persone di fiducia)



polizia delle comunicazioni

www.poliziadistato.it
www.commissariatodips.it

SEXTING

ATTRAVERSO LE CHAT SI POSSONO RICEVERE FOTO E VIDEO DI COETANEI IN ATTEGGIAMENTI INTIMI O POCO CONVENIENTI SPESSO ACCOMPAGNATI DA COMMENTI DISPREGIATIVI.

CONDIVIDENDO TALI CONTENUTI PUOI PROVOCARE GRAVI CONSEGUENZE!

ELIMINA SUBITO DAL TUO TELEFONO IMMAGINI O VIDEO CHE RIPRODUCONO MINORENNI IN ATTEGGIAMENTI SESSUALI E AVVISA IL DIRETTO INTERESSATO ED I TUOI GENITORI

RISCHIO: adescamento online e sexting

Cosa puoi fare con lo smartphone?

Si possono scattare foto bellissime, anche selfie.

In un click puoi condividerle sui social e magari sui gruppi WhatsApp.

Puoi mandarle in modalità segreta su Telegram ad un amico/a o a qualcuno che ti piace

Per amore puoi decidere di fare foto o filmati speciali, segreti, intimi…

MA… (pensate alle conseguenze)

Cosa può succedere alle tue foto?

Le foto mandate ad altri possono essere condivise all'infinito.

Spesso i ragazzi non sanno che è reato condividere le immagini di minorenni in rete senza l'autorizzazione dei genitori.

Cancellarle dal proprio smartphone o dal profilo social non è sufficiente a cancellarle dal web.

E' estremamente difficile fermare la circolazione di immagini su social e messaggistica istantanea, talvolta anche se c'è una denuncia formale.

RISCHIO: adescamento online e sexting

Con chi chatti in rete?

- Amici conosciuti a scuola, sport, parrocchia, etc.
- Amici di amici reali mai incontrati
- Amici di amici sui social ma che non hai mai né incontrato né visto
- Perfetti sconosciuti



E' FANTASTICO POTER COMUNICARE CON PERSONE DI TUTTO IL MONDO

MA...

Con chi chatti in rete?

Più le persone sono lontane dalla tua vita reale minore deve essere la confidenza che gli dai:

Ci sono adulti con cattive intenzioni che usano la rete per «avvicinare» minorenni

Vogliono parlare via web, scambiare immagini/video e magari avere incontri di sesso

Sembrano affettuosi, sembrano interessati ma in realtà hanno altre intenzioni

NON RINUNCIARE AL CONTATTO MA

RICORDA COSA PUOI RISCHIARE

SE TI FIDI SOLO DI QUELLO CHE VEDI, LEGGI O SCRIVI IN RETE

Quando un contatto è pericoloso?

Se qualcuno dice di tenerci a te ma:

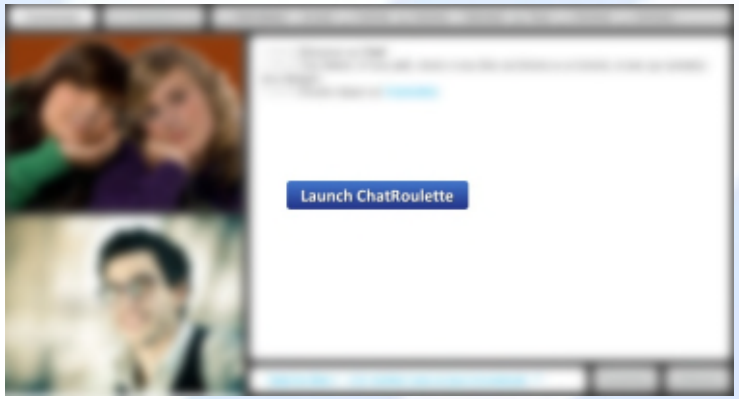
- Ti dice cose che ti sembrano troppo volgari o ti creano disagio
- Parla sempre di sesso in chat o nei messaggi
- Ti chiede insistentemente immagini private, intime
- Ti minaccia perché vuole altre immagini, altri video
- Ti chiede numeri o contatti di altri tuoi amici
- Vuole insistentemente incontrarti

NON ASPETTARE, NON AVERE PAURA, NON VERGOGNARTI

CHIEDI AIUTO AD UN ADULTO

POLIZIA POSTALE @

ESTORSIONE SU Facebook/Instagram (art. 629 c.p.)



gli autori contattano le vittime per mezzo di chat e servizi di messaggeria e li inducono a mostrarsi davanti alla webcam in atteggiamenti sessuali



Ad insaputa della vittima le immagini o il video vengono registrati



La conversazione on-line viene dirottata su Facebook al fine di individuare la lista di amici della vittima.

Polizia di Stato

ESTORSIONE SU FB/IG
(art. 629 c.p.)

Alla persona presa di mira viene infatti chiesto di versare una determinata somma di denaro (100 - 900 euro) tramite specifici corrieri (es. Western Union),

minacciando di pubblicare il video e/o le immagini in internet (es. Youtube)



Oppure di inviarli ai contatti Facebook della vittima.

Polizia di Stato

ESTORSIONE SU FB/IG (art. 629 c.p.)

I profili Facebook degli estorsori vengono creati artatamente con identità false





I recapiti telefonici forniti durante i contatti on-line corrispondono a numerazioni della Costa D'Avorio e nordafricane (Marocco)

Anche gli indirizzi IP di connessione ai profili Facebook utilizzati dagli estorsori afferiscono a provider stranieri



Diffamazione on line – casi pratici

- CREARE UN GRUPPO DIFFAMATORIO SU SPAZI DI SOCIAL NETWORK;
- INVIARE UNA MAIL DIFFAMATORIA AD UNA MAILING LIST;
- INSERIRE UN ANNUNCIO DIFFAMATORIO SU UNA BACHECA ELETTRONICA;
- INSERIRE UN VIDEO DIFFAMATORIO SU YOUTUBE O ALTRI SPAZI DI UPLOAD;
- DENIGRARE UNA PERSONA DURANTE UNA SESSIONE DI CHAT.

Polizia di Stato

Instagram

Quando ti trovi coinvolto in una disputa, fermati un attimo e pensa all'effetto che il tuo post successivo potrebbe avere. In questi momenti chiediti: “Ne vale la pena?” o “Cosa ci guadagno a continuare in questo conflitto?”. È più facile dirlo che farlo, ma accettare azioni moleste perpetrando a tua volta lo stesso tipo di azione può stimolare comportamenti negativi e incoraggiare l'altra persona a continuare nel suo comportamento aggressivo.

Pensa bene prima di commentare

Sostituzione di persona – casi pratici

- ✓CREARE UN FALSO PROFILO SU FACEBOOK CON RIFERIMENTO AD UN PROPRIO COMPAGNO O PROFESSORE;
- ✓CREARE UN FALSO PROFILO DI CHAT CON RIFERIMENTI ANAGRAFICI RIFERIBILI AD UN PROPRIO CONOSCENTE;
- ✓CREARE UN ACCOUNT DI E-COMMERCE CON I DATI DI UN PROPRIO COMPAGNO INCONSAPEVOLE.

IL RUOLO DELL'INTERNET PROVIDER

LA L. 127/2017 PREVEDE CHE IL MINORE ULTRAQUATTORDICENNE (LA POSSIBILITA' E' ESTESA AI GENITORI) PUO' INOLTRARE AL GESTORE DEL SITO INTERNET O DEL SOCIAL NETWORK UN'ISTANZA PER L'OSCURAMENTO DEL CONTENUTO.

QUALORA, ENTRO LE 24H SUCCESSIVE IL SOGGETTO RESPONSABILE NON ABBIA PROVVEDUTO ALL'OSCURAMENTO, O IN OGNI CASO IN CUI NON SIA POSSIBILE IDENTIFICARLO, L'INTERESSATO PUO' RIVOLGERE ANALOGA RICHIESTA AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, IL QUALE PROVVEDE ENTRO LE SUCCESSIVE 48 H.



Non passare troppo tempo al pc (o smartphone).
Esasperare la vita virtuale può comportare il rischio di essere fagocitati dalla rete e perdere il contatto con la realtà

Internet è utile solo se serve per completare la propria esistenza, non per viverla.
Spostare il proprio essere sul web significa perdersi un pezzo di vita e di sapori che diversamente non si percepiscono.

«LA VITA E' CIO' CHE ACCADE MENTRE SEI IMPEGNATO A GUARDARE IL TUO SMARTPHONE»

Breve cenno – INTERNET:

nasce nel 1989, da TIM Berners Lee, invento il «WorldWideWeb»
è composta da:

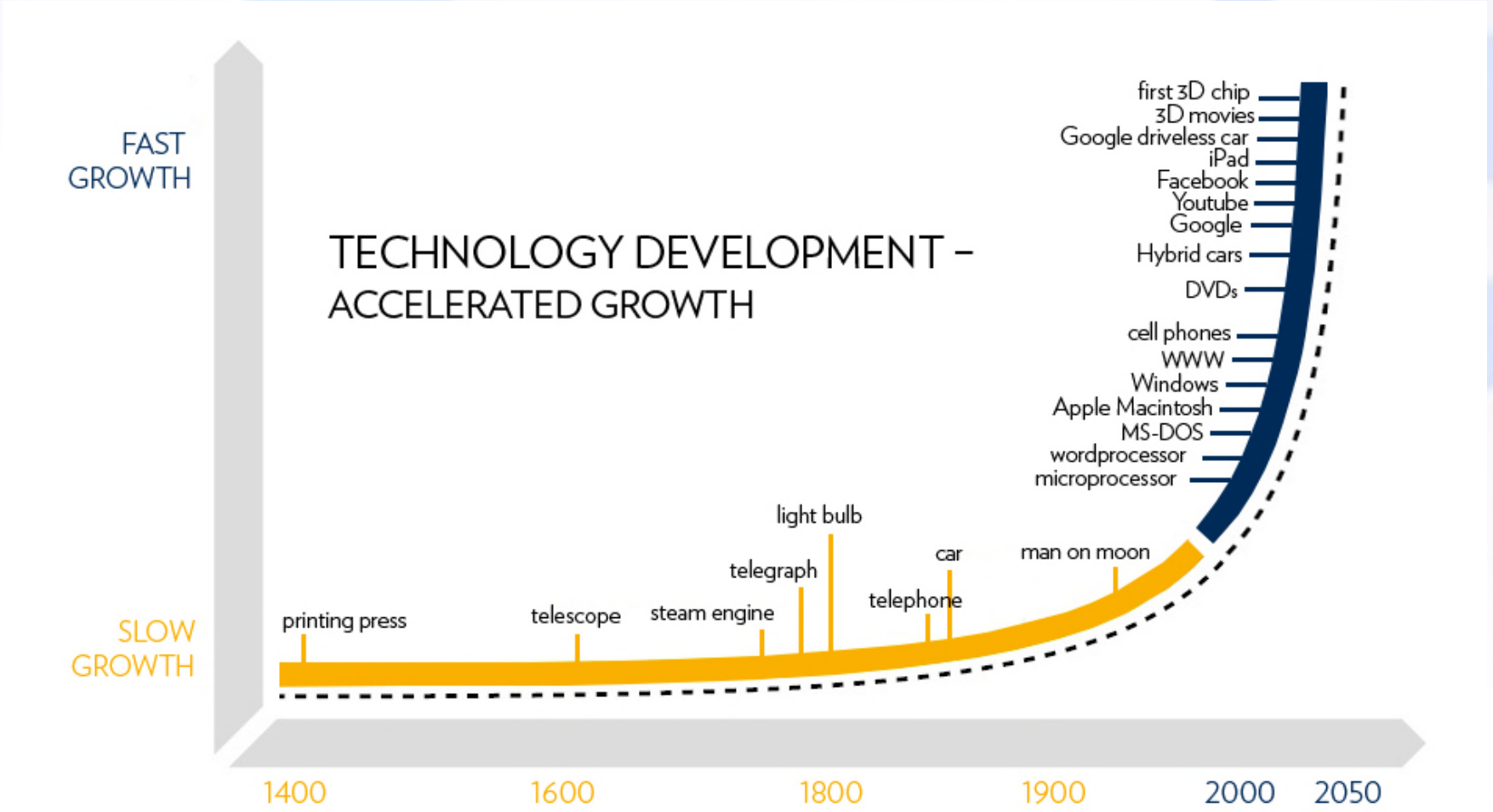
Parte fisica

- Server, sono delle grandi armadi dove vengono depositati i dati di tutto l'Internet, contengono dati di tutti i tipi.- Silicon Valley

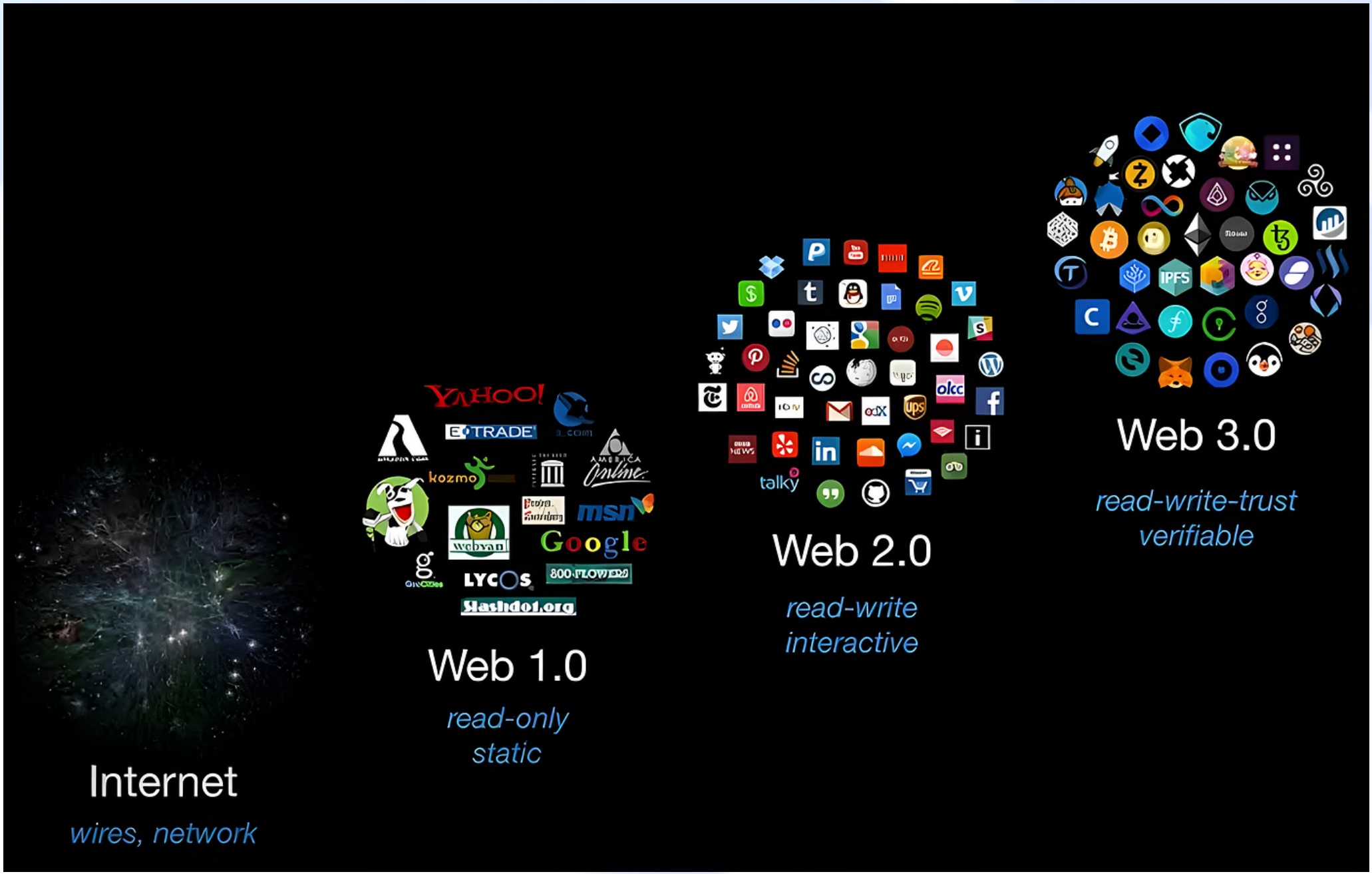
Parte virtuale

- La rete, dove trovo la stanza virtuale, in cui interagisco con il mio avatar o account, dove vedo le immagini e le informazioni che mi interessano.– dominio web, l'indirizzo della pagina

La tecnologia ha avuto una crescita repentina negli ultimi 50 anni



Evolversi del WEB da 1.0 a 4.0



Evoluzione da:

- WEB 1.0:
- Anni 1990 -2000 – siti web statici, posso solo consultare piccol archivi di dati, es biblioteca della scuola;



- WEB 2.0:
- Anni 2000-2006, interazione con i contenuti e condivisione dei contenuti es Forum o Blogs, Social Network



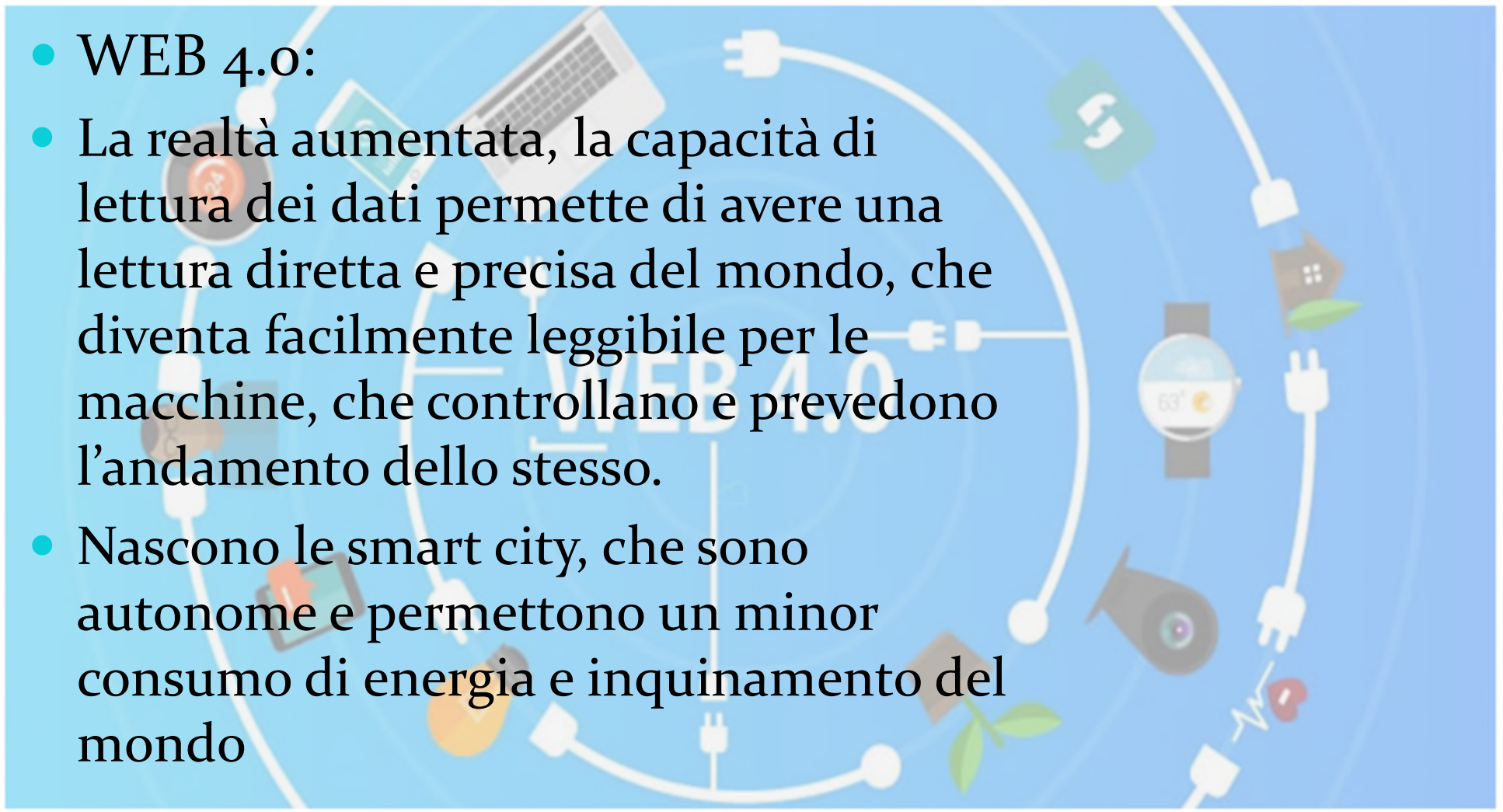
Evoluzione a:

- WEB 3.0:
- Anni 2006, «read-write-execute web»,
- La rete si potenzia, si potenzia, le pagine in automatico si adattano ai diversi dispositivi, migliore interazione con l'utenza, inizia un web in tre dimensione, 3d – Responsive Web;
- La rete come enorme database-miglioramento delle grafiche e della quantità di dati che le pagine possono ospitare;
- Compaiono le intelligenze artificiali;



Evoluzione a:

- WEB 4.0:
- La realtà aumentata, la capacità di lettura dei dati permette di avere una lettura diretta e precisa del mondo, che diventa facilmente leggibile per le macchine, che controllano e prevedono l'andamento dello stesso.
- Nascono le smart city, che sono autonome e permettono un minor consumo di energia e inquinamento del mondo



Polizia di Stato



Aumenta il bisogno di controllo e di aiuto per l'utente che è esposto a maggiori rischi, dato l'aumento della complessità delle tecnologie e dell'abbassamento dell'età media di chi naviga in Internet.

Contrastare altresì l'aumento dei criminali e crimini sul Web.

Come funzionano gli algoritmi sui social network

Gli algoritmi **sono alla base del funzionamento di motori di ricerca e social media** e conoscere il loro funzionamento permette di utilizzarli al meglio senza essere manipolati.

Sicuramente, se utilizzi di frequente i Social, avrai notato che **su** Facebook, Instagram, YouTube o **qualsiasi** altra **piattaforma compaiono determinati contenuti e suggerimenti** che sembrano fatti apposta per te

Questi contenuti non sono uguali per tutti i fruitori della piattaforma, bensì **cambiano in base a ogni persona**.

Come funzionano gli algoritmi sui social network

L'algoritmo è una successione di istruzioni per risolvere un problema, cioè per ottenere un preciso risultato a partire da un certo numero di dati iniziali

Nei social media, in particolare, hanno lo scopo di **filtrare** le numerosissime informazioni che popolano la rete e **creare ecosistemi su misura** per ciascun utente.

Lo scopo è quello di creare **esperienze positive**, che spingano le persone a **restare sulla piattaforma** per il maggior tempo possibile.

Aspetti positivi e negati degli algoritmi che regolano i social

E' positivo che l'algoritmo renda più affine ai tuoi gusti ed alla tua personalità il tuo ambiente social.

Il cosiddetto «feed» che l'algoritmo mostra a ogni utente si basa sull'***engagement***, ovvero sulle interazioni all'interno della piattaforma, ma non solo.

Le interazioni possono avvenire attraverso like, commenti, visualizzazioni o condivisioni.

L'algoritmo associa poi un valore alle varie interazioni compiute dal singolo utente e come risultato finale quest'ultimo vedrà un **feed personalizzato**, completamente diverso da qualsiasi altro utente della piattaforma.

Sulla base di quanto appena detto, ecco spiegato perché quando metti "mi piace" alle foto dei gattini ti ritrovi la home invasa da quei simpatici amici a quattro zampe.

Aspetti positivi e negati degli algoritmi che regolano i social

E assolutamente negativo il rischio di finire in una «***bolla social***» perché il continuo **filtraggio delle informazioni può essere un problema**.

Dopo anni di utilizzo, i social ti potrebbero mostrare solo quello che ha a che fare con le tue idee e i tuoi interessi più stretti, con il rischio che ti venga oscurato tutto il resto.

Lo stesso discorso vale per le informazioni, anche quando queste non sono del tutto veritiere – **fake news**. Es. «terrapiattisti»

In questo modo, portando il caso all'estremo, vengono a mancare due elementi fondamentali per la corretta esistenza sui social: il **confronto** e la **varietà di contenuti**.

È stato coniato un nome per questo fenomeno: ***echo chamber*** o, volgarmente, bolla social.

I BIG DATA

L'aumento delle informazioni che circolano su internet, richiedono ai computer una maggiore capacità di calcola, e di archiviazione, tale bisogno aumenta sempre di più. Nuove aziende offrono il servizio di affitto per i server.

Esempio: lo spazio che YouTube produce per l'archiviazione giornaliera, è l'impressionante cifra di un PETABYTE (PB), cioè 1000 Terabyte (TB), equivalente a 1.000.000 di GB.

CHAT GPT

E’ un modo alternativo a GOOGLE per cercare contenuti sul WEB, ma il metodo di interazione cambia, perché al posto delle indicizzazioni del motore di ricerca, CHATGPT simula una conversazione di chat con l’utente.

Chat GPT può rispondere direttamente a una domanda e adattarsi molto alla conversazione come potrebbe fare un essere umano, grazie all’uso dell’intelligenza artificiale.

C’è molta preoccupazione e scetticismo sull’invasività e sulla possibile evoluzione degenerativa di questo strumento e per questo in Italia era stata inibita momentaneamente dal Garante Privacy.

L’avvento delle A.I.

- Le intelligenze artificiali sono un insieme di codici che permettono a una macchina di imparare per tentativi, dato un iniziale problema, la macchina deve da sola, tramite tantissimi tentativi arrivare a una soluzione.



Diritto all’oblio

Il GDPR (regolamento europeo della Privacy) ha introdotto il diritto all’oblio, cioè il diritto di richiedere la cancellazione dei propri dati

Ma……..



OGNI TRACCIA SU INTERNET RIMANE !!

- Internet, avviene un fenomeno detto «viralità»

esempio il fenomeno dei «meme», un utente scarica un elemento e lo ripropone in maniera leggermente diversa, rendendone difficile la cancellazione. Lo stesso può ricomparire a distanza di anni.

Esempi di meme





Esempi di meme





ATTENZIONE ALLA TECNODIPENDENZA:



- Ti senti a disagio se non puoi connetterti
- Non riesci a stare senza mandare messaggi, controllare mail e app, profili e news in rete
- Ti senti ansioso, nervoso o triste se non puoi usare smartphone e tablet
- Passi molto del tuo tempo a pensare e partecipare a giochi online e non hai voglia di studiare, uscire o fare altro

PARLANE CON UN ADULTO PRIMA CHE SIA TROPPO TARDI

LE ABITUDINI POSSONO ESSERE CAMBIATE!

DIVIETO USO CELLULARI IN CLASSE

- Circolare ministeriale del 19 dicembre 2022
- Indagine del ministero dell'istruzione:

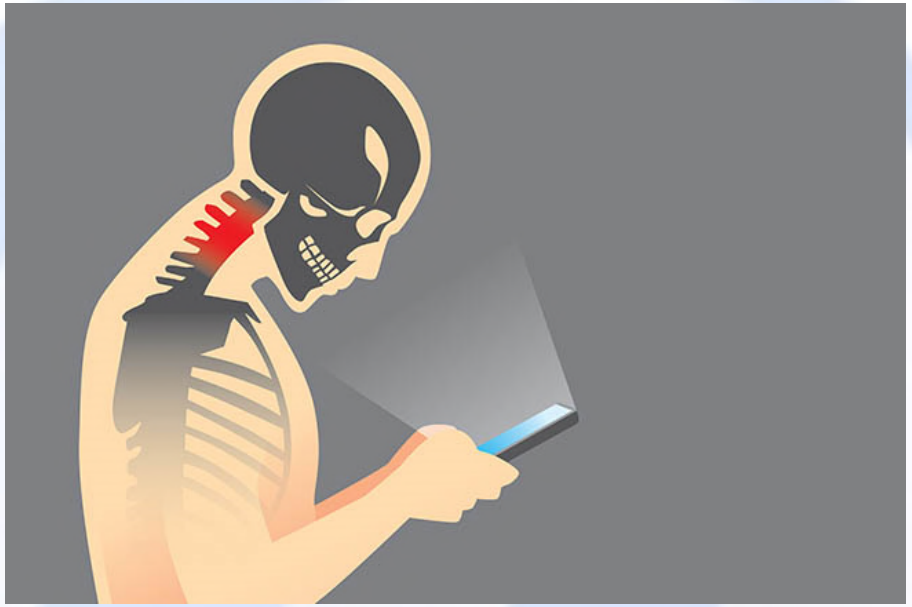
  -Crescente fenomeno «hikikomori» paesi asiatici;

  -Aumento dei crimini informatici (adescamento, sexting, cyberbullismo, Revenge Porn…)

  -[smartphone] definito come:

  «Una prigione senza muri in cui i prigionieri non sognano di evadere» cit. Aldous Huxley

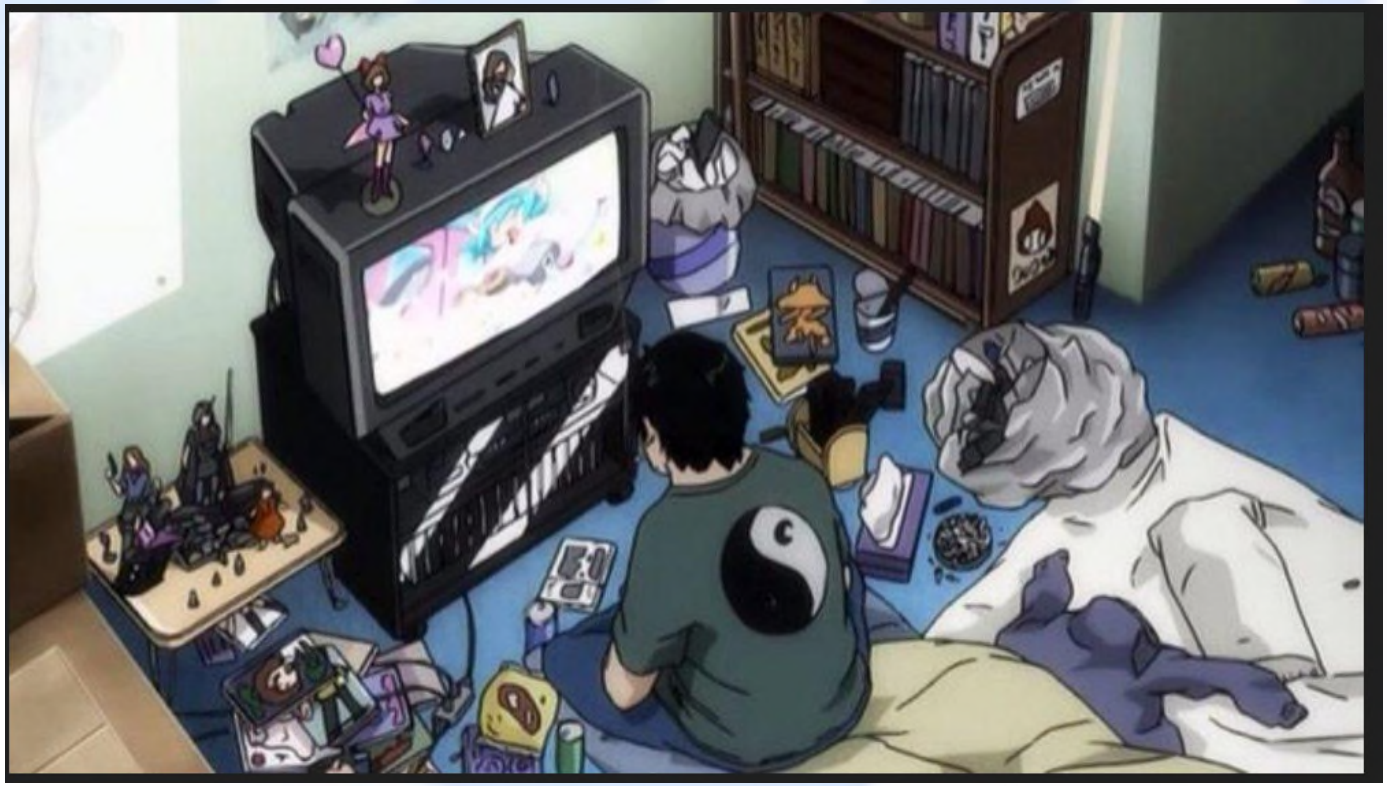
LOOK DOWN GENERATION



LA GENERAZIONE DI CHI HA PERSO LA CAPACITÀ DI COMUNICARE GUARDANDOSI NEGLI OCCHI

HIKIKOMORI

Termine giapponese che significa "stare in disparte", viene utilizzato per indicare chi decide di ritirarsi dalla vita sociale per lunghi periodi, alle volte anni. Rinchiusi nella propria abitazione, evitano qualunque tipo di contatto diretto con il mondo esterno, talvolta anche con i familiari.




09:22
91%
QUOTIDIANO NAZIONALE
Cronaca Economia Politica Esteri Sport
12 ott 2023
Suicidio di un 12enne a Centocelle, spunta un video choc girato da dei ragazzi: i carabinieri lo fanno cancellare prima dell'uscita su TikTok
Una ragazza stava girando un filmato per TikTok proprio nel momento del tragico gesto del ragazzino: i militari hanno fatto cancellare ogni traccia del video dai cellulari

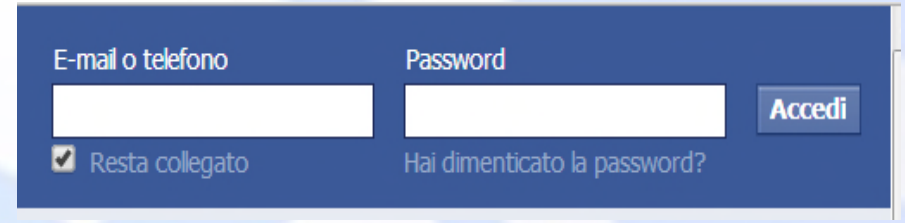

09:23
91%
www.quotidiano.net
QUOTIDIANO NAZIONALE
Cronaca Economia Politica Esteri Sport
LEGGI DI PIU >
Roma, 12 ottobre 2023 – C'era un video del suicidio del 12enne precipitato martedì dal terrazzo della sua abitazione nel quartiere Centocelle a Roma. Un filmato drammatico che è stato ripreso per caso e involontariamente da una ragazza che, proprio nel momento in cui accadeva la tragedia in piazza dei Mirti, stava girando assieme a un gruppo di amici un proprio video da pubblicare su TikTok. Dell'esistenza del video girato sul luogo della morte del ragazzino se ne sono accorti i carabinieri nel corso degli accertamenti svolti sul posto e un loro pronto intervento ha permesso che non venisse divulgato sui social.

SICUREZZA ON LINE
Come possiamo proteggerci?

Una password sicura e segreta



Digita la password ogni volta



Crea Password difficili:
numeri, maiuscole, minuscole,
simboli, lunghezza IA@*$&89



Cambia spesso la password

Se possibile non utilizzare lo stesso username e/o la stessa password per siti web diversi o per account importanti: email, banca…

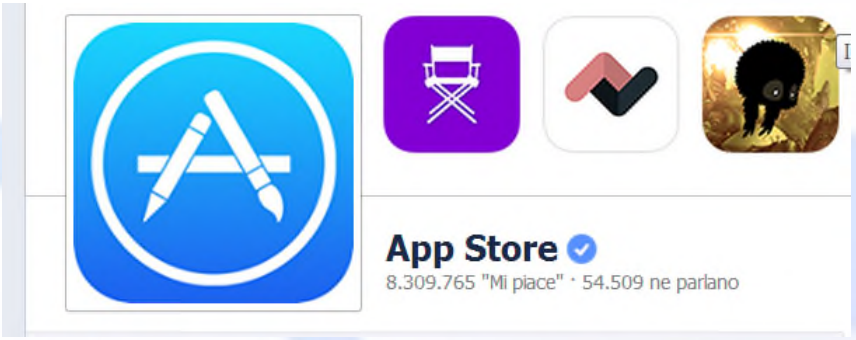
Non dire la tua password a nessuno!

CARATTERISTICA ESSENZIALE DELLA PASSWORD?

LA PASSWORD E' SEGRETA !



IL BUSINESS DEI *SOCIAL NETWORK*



La principale fonte di guadagno dei *social networks* proviene da:

- vendita a terzi delle informazioni sugli utenti
- pubblicità mirata (alle preferenze degli utenti)
- *Social commerce*
- *Testimonial pubblicitari involontari*
- *Ultimamente sono diventati a pagamento*
- *Es: Meta Verified 11,99 $*



COME GESTIRE I PROBLEMI?

Polizia di Stato

Se ti senti minacciato on-line o quando
hai paura parla con i tuoi genitori, gli insegnanti
oppure contatta la Polizia Postale e delle Comunicazioni
per segnalare immediatamente minacce che
vengono fatte a te o alla tua famiglia

Sez.poliziapostale.bs@poliziadistato.it

Tel.030.2913028

GRAZIE PER L'ATTENZIONE!