

CAPSULAE CUM OCULO DE VITRO OCCHIO AL WEB!

CAPSULAE CUM
OCULO DE VITRO
.....
OCCHIO AL
WEB!



GUIDA PRATICA

ISTITUTO COMPRENSIVO VALENZA "A"

CAPSULAE

CUM OCULO DE VITRO

...

OCCHIO AL WEB!

GUIDA PRATICA



Istituto Comprensivo
Valenza "A"

© Copyright 2021 - Tutti i diritti riservati.

Il contenuto in questo libro non può essere riprodotto, duplicato o trasmesso senza il permesso scritto diretto dell'autore o dell'editore.

In nessuna circostanza sarà attribuita alcuna colpa o responsabilità legale all'editore, o autore, per eventuali danni, riparazioni o perdite monetarie dovute alle informazioni contenute in questo libro. Direttamente o indirettamente.

Aviso legale:

Questo libro è protetto da copyright. Questo libro è solo per uso personale. Non è possibile modificare, distribuire, vendere, utilizzare, citare o parafrasare alcuna parte o il contenuto di questo libro senza il consenso dell'autore o dell'editore.

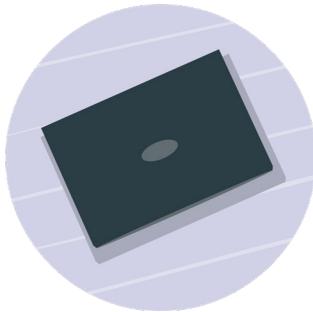
Aviso di esclusione di responsabilità:

Si prega di notare che le informazioni contenute in questo documento sono solo a scopo educativo e di intrattenimento. È stato compiuto ogni sforzo per presentare informazioni accurate, aggiornate e affidabili e complete. Nessuna garanzia di alcun tipo è dichiarata o implicita. I lettori riconoscono che l'autore non si impegna a fornire consulenza legale, finanziaria, medica o professionale. Il contenuto di questo libro è stato derivato da varie fonti. Si prega di consultare un professionista autorizzato prima di provare qualsiasi tecnica descritta in questo libro.

Leggendo questo documento, il lettore accetta che in nessun caso l'autore è responsabile per eventuali perdite, dirette o indirette, che sono sostenute a seguito dell'uso delle informazioni contenute in questo documento, inclusi, ma non limitati a, errori, omissioni o imprecisioni.

SOMMARIO

INTRODUZIONE	5
1 . CHI È UN NATIVO DIGITALE?	7
2 . CHI È UN CITTADINO DIGITALE?	9
3 . DIRITTO ALLA RISERVATEZZA	11
4. LA NETIQUETTE	15
5. I SOCIAL	19
6. CYBERBULLISMO E ADESCAMENTO ONLINE	23
7. FAKE NEWS	29
8. COPYRIGHT	33
9. ACQUISTI ON LINE	35
10. GIOCO E DIPENDENZA	39
CONCLUSIONI	41
SITOGRAFIA	43



INTRODUZIONE

L'istituto Comprensivo Valenza A e il suo Dirigente Scolastico, Maurizio Primo Carandini, hanno sempre dedicato grande attenzione alle sfide educative contemporanee e il rapporto tra adolescenti e tecnologia oggi è una delle più importanti.

Lo smartphone è diventato una sorta di protesi del sistema nervoso centrale; uno strumento che è al tempo stesso trasmettitore e ricevitore di messaggi, cosa mai accaduta nella storia della comunicazione di massa.

I giovani oggi sono sempre meno numerosi e più poveri rispetto alla generazione che li ha preceduti.

Un uso non consapevole della nuova tecnologia può arrecare più danni che vantaggi ed è proprio per questo motivo che abbiamo creato il progetto "Capsulae cum oculo de vitro".

La guida che hai tra le mani è uno strumento che nasce dall'esigenza di avere un valido supporto per i minori. Per realizzarla abbiamo chiesto l'aiuto del Responsabile Protezione dei dati dell'Istituto Comprensivo, la Dott.ssa Pagano Debora Marianna di DeePeformance.

QUESTA GUIDA SI PROPONE DI

- promuovere un uso consapevole e responsabile di internet, andando incontro al crescente bisogno di sicurezza digitale a favore degli utenti più giovani compresi nell'arco di età 8 – 13 anni;
- prevenzione dell'eventuale danno psicologico, morale o materiale che potrebbe scaturire dal difettoso utilizzo delle opportunità della rete attraverso attività di informazione;
- sensibilizzazione dei genitori verso il loro ruolo attivo nei confronti del figlio utente, relativamente all'uso sicuro di internet e dei nuovi media.

Attraverso una campagna informativa digitale i minori fruitori del Progetto saranno sensibilizzati ad un utilizzo responsabile e consapevole degli strumenti e delle opportunità che offre la rete internet.

Buona lettura.

Dirigente Scolastico

Carandini Maurizio Primo

1. CHI È UN NATIVO DIGITALE?

IL NATIVO DIGITALE È CHI FIN DALLA NASCITA È STATO A CONTATTO CON LE NUOVE TECNOLOGIE.

“Nativi digitali” sono, coloro che fin dalla nascita hanno passato l’intera vita circondati da computer, videogiochi, lettori di musica digitale, videocamere, telefoni cellulari e tutti gli altri giocattoli e strumenti dell’era digitale.

Stando a questa definizione la nostra generazione non può essere considerata “nativa digitale” ma abbiamo dovuto apprendere in maniera più o meno forzata questa nuova modalità di approccio alla realtà.

È come apprendere una nuova lingua e come tale è necessaria sia la conoscenza teorica che pratica ma procediamo con ordine.



2.

CHI È UN CITTADINO DIGITALE?

IL CITTADINO DIGITALE È CHI SI COMPORTA IN MODO CONSAPEVOLE ED EDUCATO NEL MONDO ONLINE.

Essere un nativo digitale non vuol però dire saper usare in modo corretto e consapevole gli strumenti digitali, spesso le tue competenze informatiche sono molto più limitate di quello che pensi. Avere tra le mani uno smartphone o un tablet non ci rende capaci di utilizzarlo al meglio o di proteggere le nostre informazioni.

1. MA QUALI SONO LE COMPETENZE CHE UN CITTADINO DIGITALE DOVREBBE AVERE?
2. SAPERE FARE RICERCHE ONLINE E VERIFICARE LE INFORMAZIONI
3. UTILIZZARE CORRETTAMENTE LE TECNOLOGIE PER COMUNICARE CON GLI

4. ALTRI
5. CREARE CONTENUTI DIGITALI
6. PROTEGGERE I PROPRI DATI E SE STESSI
7. RISOLVERE PROBLEMI TECNICI

Ognuna di queste aree prevede la presenza di sotto-competenze, qui sotto elencate, indispensabili alla piena realizzazione del concetto di cittadinanza digitale.

Area 1: Alfabetizzazione su informazioni e dati

- 1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali
- 1.2 Valutare dati, informazioni e contenuti digitali
- 1.3 Gestire dati, informazioni e contenuti digitali

Area 2: Comunicazione e collaborazione

- 2.1 Interagire attraverso le tecnologie digitali
- 2.2 Condividere informazioni attraverso le tecnologie digitali
- 2.3 Esercitare la cittadinanza attraverso le tecnologie digitali
- 2.4 Collaborare attraverso le tecnologie digitali
- 2.5 Netiquette
- 2.6 Gestire l'identità digitale

Area 3: Creazione di contenuti digitali

- 3.1 Sviluppare contenuti digitali
- 3.2 Integrare e rielaborare contenuti digitali
- 3.3 Copyright e licenze
- 3.4 Programmazione

Area 4: Sicurezza

- 4.1 Proteggere i dispositivi
- 4.2 Proteggere i dati personali e la privacy
- 4.3 Proteggere la salute e il benessere
- 4.4 Proteggere l'ambiente

Area 5: Risolvere problemi (*problem-solving*)

- 5.1 Risolvere problemi tecnici
- 5.2 Individuare fabbisogni e risposte tecnologiche
- 5.3 Utilizzare in modo creativo le tecnologie digitali
- 5.4 Individuare divari di competenze digitali

In quanto cittadini digitali dobbiamo essere consapevoli che, anche online, ognuno ha una propria identità e che questa ci definisce, che lascia delle tracce ed che è rintracciabile sulla base di una serie di informazioni che

ci identificano.

Questo significa che ogni nostra azione in rete è potenzialmente tracciata e memorizzata. Come?

Le tracce digitali di cui stiamo parlando sono i “cookie” che servono a migliorare la tua navigazione e a raccogliere dati sui tuoi interessi e preferenze.

Questi file sono come le briciole di Hansel e Gretel, memorizzano le tue attività precedenti associando un codice al tuo utente e al ritorno ti portano dove sei stato prima o ti mostrano notizie e pubblicità relative alle tue ricerche precedenti.

I cookie, quindi, da un lato migliorano la navigazione permettendoci di salvare e trovare più facilmente le informazioni che stiamo cercando, ma dall'altro raccolgono i nostri dati per inviarci pubblicità mirate al tuo profilo.

Esistono due macro tipologie di cookie:

Cookie tecnici - servono ad ottimizzare la navigazione e sono necessari per il corretto funzionamento dei siti web.

Cookie di profilazione - servono a creare un profilo dell'utente sulla base dei suoi interessi che sono utilizzati per attività di marketing e pubblicità.

Molti siti ci obbligano ad accettare tutti i cookies, ciò non è conforme alla normativa vigente ma ricorda che puoi cancellarli dal tuo browser in ogni momento.

RICORDA: prima di accettare i cookies è importante leggere sempre attentamente le informative.

Guarda il video sui Cookies

<https://www.youtube.com/watch?v=Mut-YXSExnw>



DIRITTO ALLA RISERVATEZZA

Le "tracce" che lasciamo navigando in rete sono dati personali.

DATI PERSONALI

Iniziamo cercando di capir quali sono le varie tipologie di dati che tutti i giorni troviamo sul web.

I dati presenti online vengono raggruppati in due macro-categorie:

- I dati non personali
- I dati personali

Sono non personali tutti quei dati che non possono essere collegati a una persona identificata o identificabile, quindi non fanno riferimento a noi. Le informazioni di

questo tipo includono per esempio i dati statistici come il tempo che dedichiamo ad un'applicazione del nostro smartphone.

I dati personali costituiscono qualsiasi informazione relativa a una persona fisica identificata o identificabile, sono quelle informazioni che ti riguardano.

Dati identificativi	Dati particolari
Nome e cognome	Stato di salute
Numero di telefono	Origine razziale o etnica
Immagine	Credo religioso
Orientamento religioso	Dato biometrico (impronta)

Secondo la Carta dei diritti fondamentali dell'Unione europea il diritto alla Protezione dei Dati personali è un diritto fondamentale dell'individuo e il 25 maggio 2018 in tutti i paesi dell'UE è entrata in vigore una nuova importante normativa, **Regolamento Generale sulla Protezione dei dati (GDPR)**.

Per la legge italiana ed europea, i dati personali possono riferirsi solamente a una persona fisica e non a una persona giuridica, come per esempio un'azienda.

MA PERCHÉ È COSÌ IMPORTANTE PROTEGGERE QUESTI DATI?

I dati che tutti i giorni inseriamo sul web sono tantissimi. Quando effettuiamo delle ricerche su Google o acquistiamo qualcosa online siamo costantemente controllato. Tutti questi dati, anche se apparentemente non ti sembrano “preziosi”, hanno in realtà un valore economico.

Le tracce che lasci vengono raccolte per creare una sorta di carta d’identità che quello che ti interessa, i luoghi virtuali e fisici che frequenti e di tanti altri aspetti che possono interessare a chi usa Internet per pubblicizzare prodotti o servizi, o per influenzarti.

La creazione di questa carta d’identità si chiama “profilazione” e determina il tipo di contenuti che vedi online, fa sì che le informazioni che vedi siano “filtrate” in base al tipo di utente che sei.

Per questo motivo è importante che tu sia consapevole di quello che accade mentre navighi sul web, e che adotti delle misure per tutelare la tua privacy e di chi ti circonda.

Tips: quando ti iscrivi ad un sito e crei un account leggi l’informativa, impara a distinguere motori di ricerca e siti sicuri. Se hai dubbi chiedi sempre ad un adulto.



PRIVACY PROTECTION

Lorem ipsum dolor sit amet, coecetur
adi sed do eiusmod tempor incididunt
Lorem ipsum dolor sit amet.

Learn more

Guarda il video sul Gdpr

**[https://www.youtube.com
watch?v=2CT8MyakS_s&t=79s](https://www.youtube.com/watch?v=2CT8MyakS_s&t=79s)**

4.

LA NETIQUETTE

Con “netiquette” o “galateo digitale” si intende la serie di regole di comportamento da seguire quando si interagisce su Internet in spazi virtuali pubblici come forum, chat, social media oppure tramite e-mail. La parola netiquette è composta da network, “rete” ed étiquette, “buona educazione”.

Saper comunicare online è una competenza che si apprende con il tempo e soprattutto con la pratica. Prima di scrivere su qualsiasi strumento è fondamentale pensare per evitare di essere maleducati nei confronti degli altri o creare incomprensioni.

La comunicazione online è priva degli elementi che facilitano la comprensione dei messaggi espressi, come la gestualità e il tono di voce, ciò rende più

frequenti i fraintendimenti. Per agevolare una corretta comprensione del messaggio, è importante scegliere con cura le parole da usare, utilizzare bene la punteggiatura e le emoticon. Le emoticon, usate con moderazione, possono infatti aiutarti ad aggiungere empatia a un messaggio che, in quanto virtuale, può risultare freddo o poco chiaro.

Non esiste una legge che regoli la netiquette ma dobbiamo comunque fare molta attenzione a quello che scriviamo perché un commento non appropriato potrebbe portare ad una denuncia per diffamazione (reato previsto dall'art. 595 del codice penale).

COME COMPORTARSI

1. Curare la grammatica e la forma dei messaggi, in caso di errore di altri non attaccarli pubblicamente;
2. Non scrivere in MAIUSCOLO, è associato ad un tono aggressivo;
3. Non inviare messaggi pubblicitari non graditi;
4. Non inviare e-mail a più contatti in copia visibile ma scegli l'opzione copia nascosta;
5. Non pubblicare il contenuto di messaggi privati o e-mail;

6. Non pubblicare foto di altre persone senza il loro consenso.

PRIMA DI PUBBLICARE USA

T.H.I,N.K. FERMATI E PENSA

True - quello che stiamo scrivendo o condividendo è vero?

Helpful - è utile al nostro interlocutore?

Inspiring - offre uno spunto in una conversazione?

Necessary - è necessario?

Kind - è "gentile"?

Diventare un leone da tastiera è molto più facile di quello che pensi ecco perchè è importante conoscere e leggere attentamente il manifesto delle parole ostili.

Il Manifesto della comunicazione non ostile

- 1. Virtuale è reale**
Dico o scrivo in rete solo cose che ho il coraggio di dire di persona.
- 2. Si è ciò che si comunica**
Le parole che scelgo raccontano la persona che sono: mi rappresentano.
- 3. Le parole danno forma al pensiero**
Mi prendo tutto il tempo necessario a esprimere al meglio quel che penso.
- 4. Prima di parlare bisogna ascoltare**
Nessuno ha sempre ragione, neanche io. Ascolto con onestà e apertura.
- 5. Le parole sono un ponte**
Scelgo le parole per comprendere, farmi capire, avvicinarci agli altri.
- 6. Le parole hanno conseguenze**
So che ogni mia parola può avere conseguenze, piccole o grandi.
- 7. Condividere è una responsabilità**
Condivido testi e immagini solo dopo averli letti, valutati, compresi.
- 8. Le idee si possono discutere. Le persone si devono rispettare**
Non trasformo chi sostiene opinioni che non condivido in un nemico da annientare.
- 9. Gli insulti non sono argomenti**
Non accetto insulti e aggressività, nemmeno a favore della mia tesi.
- 10. Anche il silenzio comunica**
Quando la scelta migliore è tacere, taccio.

Guarda il video sulla Netiquette

**[https://www.youtube.com/
watch?v=8YsFxB2uhQ8](https://www.youtube.com/watch?v=8YsFxB2uhQ8)**

5.

I SOCIAL

La parola Social Media indica le tecnologie e le pratiche che le persone adottano per condividere contenuti di testo, immagini, audio e video.

In altre parole, sono uno strumento che consente la creazione e lo scambio di contenuti generati dagli utenti.

Da qualche anno rappresentano un cambiamento sostanziale nelle modalità di lettura, apprendimento e condivisione di informazioni e contenuti da parte di ogni fascia di età.

Oggi tutti hanno almeno un account social ma sappiamo come funzionano? Innanzitutto dobbiamo sapere che per avere un account personale è necessario avere

almeno 13 anni e che un minore non può utilizzare i nostri account personali.

SOCIA APERTI - CHIUSI

Social Aperti: in genere sono per tutti; chiunque può iscriversi e partecipare o postare i suoi contenuti. Es. Facebook, Instagram

Social Chiusi: si differenziano perché l'iscrizione è limitata a soggetti che sono stati invitati da utenti già registrati alla rete. Es. Clubhouse, Edmodo

ATTENZIONE A COSA PUBBLICHI

È corretto o non corretto pubblicare foto o contenuti che riguardano o coinvolgono una terza persona?

Chi pubblica sul proprio profilo o su quello di altri la foto di un soggetto di cui non ha ricevuto l'autorizzazione, commette un **reato**. La legge sulla privacy, infatti, punisce **con la reclusione fino a tre anni l'illecito trattamento di dati personali sul web**.

Quando queste immagini sono di carattere "intimo", si commette il reato più grave di revenge porn.

Questo si applica a tutti i casi di diffusione non autorizzata di fotografie o video su WhatsApp, Telegram, Snapchat, Facebook, YouTube, Instagram.



6.

CYBERBULLISMO E ADESCAMENTO ONLINE

Un aspetto fondamentale legato alla nostra presenza online riguarda il comportamento che adottiamo nei confronti degli altri utenti. Non avere davanti una persona fisica porta spesso le persone a comportarsi in diversi modi rispetto alla vita reale.

Lo schermo, in questi casi, si trasforma in una barriera ma in quanto utenti e cittadini digitali dobbiamo ricordarci che i nostri comportamenti sul web hanno lo stesso valore di quelli che adottiamo offline.

Con lo sviluppo del mondo digitale si è sviluppato anche il fenomeno, di cui ormai abbiamo tutti sentito del cyberbullismo, ovvero di tutti quegli atteggiamenti

che avvengono online e che costituiscono episodi di bullismo.

Noi adulti dobbiamo saper riconoscere tale fenomeno per contrastarlo al meglio.

Il **cyberbullismo** è una forma di prepotenza attuata attraverso l'uso di internet e delle tecnologie digitali reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come più debole, in genere nel gruppo dei pari.

Il cyberbullismo è un reato grave e per questo sono previste sanzioni molto pesanti.

La legge 71/2017, "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", prevede delle misure di contrasto del fenomeno.

Il cyberbullismo può iniziare da un'azione semplice, una di quelle che tutti noi compiamo ogni giorno. Minacciare un collega o un conoscente attraverso mezzi digitali, fingersi di esser lui e parlare male degli altri, insultarlo e ridicolizzarlo sono tutte forme di cyberbullismo e quindi di reato perseguibile.

Proviamo a pensare a qual è la differenza tra una presa in giro tra amici e un'aggressione online.

Nel primo caso si tratta di una interazione tra amici che utilizzano espressioni scherzose in maniera affettuosa senza l'intento di far soffrire qualcuno o di recare danno.

Nel secondo caso invece si tratta di episodi in cui una o più persone rivolgono scherzi e battute contro una persona sola con l'intenzione di farle del male ed emarginarla dal gruppo

L'impatto: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online).

LE TIPOLOGIE

Cyberstalking (cyber-persecuzione) Consiste nel molestare e denigrare ossessivamente una persona online per incutere paura e terrore generando in essa una sensazione di insicurezza e facendola temere per la propria incolumità.

Exclusion (esclusione) Consiste nell'escludere deliberatamente e senza motivo una persona da un gruppo online per ferirla.

Exposure o outing (rivelazioni) Consiste diffondere online le informazioni confidate spontaneamente da un compagno.

Persecuzione esclusione rivelazioni molestie offensivi
sostituzione di persona denigrazione inganno

Personificazione fingersi un'altra persona per isolare la vittima, **è un reato previsto nel codice penale all'art.494.**

L'ADESCAMENTO ONLINE

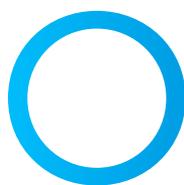
L'adescamento online, in inglese grooming ("groom" - curare, prendersi cura), è definibile come il tentativo da parte di un adulto di avvicinare un bambino/a o un adolescente per scopi sessuali, conquistandone la fiducia al fine di superare le resistenze emotive ed instaurare con lui/lei una relazione intima o sessualizzata.

Questi adulti sanno come conquistare la fiducia delle vittime e quindi bisogna fare molta attenzione ai cambi repentini delle abitudini dei nostri allievi e/o figli. E' importante pertanto instaurare un dialogo aperto e con loro.

In Italia quando un adulto vuole costruire una relazione particolare con un minorenne sta commettendo un reato, infatti dal 2012 è presente un articolo che lo prevede (**art. 609-undecies - adescamento di minorenni**)

7.

FAKE NEWS



ggi il web è la principale fonte di informazione ma perdersi è molto semplice.

Senza le giuste competenze vanificare il vantaggio di questo strumento così potente è facile.

Quello che leggiamo in rete non è sempre vero ed è importante riconoscere le notizie vere da quelle false.

La prima cosa da imparare è saper usare i motori di ricerca e riconoscere i siti affidabili e quelli non. Nel web il rapporto tra fonti e pubblico è diretto, spetta dunque a noi valutare se la notizia sia affidabile.

In gergo si parla di «bufale» o «fake news», notizie false, la cui circolazione spopola sui social, specialmente

su Facebook, proprio a causa della tendenza degli utenti a condividere senza verificare contenuti, magari leggendo solo i titoli o affidandosi alle immagini.

Notizie false create con l'obiettivo di danneggiare gravemente privati e aziende, influenzare l'opinione pubblica su temi importanti come la salute e la sicurezza, condizionare la politica, distruggere la reputazione di figure pubbliche e non solo.

MISINFORMAZIONE: Notizie false o distorte, create in buona fede, ma che presentano comunque rischi per il lettore finale.

MALINFORMAZIONE: Notizie false o distorte create in malafede. Raccontano solo parte di notizia vera, quella che meglio rappresenta i propri pregiudizi. L'informazione finale che arriva al lettore sarà distorta.

LE FAKE NEWS SONO UN REATO?

Sì, quando pubblicazione di notizie false, esagerate o tendenziose hanno la finalità di turbare l'ordine pubblico (art 656 codice penale)



COSA FARE?

1. Verificare che una notizia sia vera prima di condividerla;
2. Usare strumenti per verificare le notizie (fact-checkers per esempio);
3. Verificare le fonti e la loro attendibilità;
4. Chiedere aiuto a una persona esperta o a un ente competente;
5. Ricordare che anche internet e i social network sono manipolabili;
6. Riconoscere i vari tipi e gli stili delle notizie false;
7. Attenzione ai "titoli esca" che spingono a cliccare;

8. Abbiamo un potere enorme: usiamolo bene;
9. Diamo il buon esempio: non lamentiamoci del buio ma accendiamo la luce.



Guarda il video

**[https://www.youtube.com/
watch?v=5FROGYnhxGU](https://www.youtube.com/watch?v=5FROGYnhxGU)**

8.

COPYRIGHT

La produzione di materiale digitale oggi è molto semplificata grazie alla rete e per realizzare una ricerca, una relazione o un qualsiasi contenuto digitale non abbiamo bisogno di molto. Quando utilizzi informazioni prese dal web devi tener presente che ci sono regole precise da rispettare per l'utilizzo.

Con il termine **“Copyright”** si intende l'insieme di diritti dell'autore di un'opera dell'ingegno e che fa sì che le opere appartengano a chi le ha create e che le possa utilizzare economicamente attraverso la sua riproduzione, distribuzione e diffusione.

In Italia il diritto decade dopo 70 anni dalla morte dell'autore.

Se qualcosa è in rete non vuol dire che non sia coperto da copyright ed è importante esserne a conoscenza per evitare spiacevoli conseguenze legali, esiste infatti una legge **n.633/1941 che tutela il diritto d'autore.**

Come fare allora a realizzare i nostri contenuti senza violare alcuna legge?

Le regole
Prima di utilizzare un contenuto in rete devi sapere che

Regola 1
Cerca di produrre o utilizzare fotografie e grafiche originali

Regola 2
Prima di condividere un contenuto ricorda che è sempre necessario chiedere il permesso all'autore

Regola 3
Nei social, la condivisione deve permettere a tutti i di poter risalire all'autore

...

Possiamo utilizzare materiale libero da Copyright o realizzato da noi.

Siti su cui è possibile reperire materiale libero

Foto e video

www.unsplash.com
www.pexels.com
www.pixabay.com
www.stockfootageforfree.com
www.freepd.com
Musica
www.freemusicarchive.org

9.

ACQUISTI ON LINE

Durante la navigazione sul web è possibile essere vittime di truffe o messaggi ingannevoli specialmente negli acquisti on line.

Molti siti per effettuare acquisti richiedono la creazione di un account è bene leggere con attenzione i termini contrattuali applicati dall'e-commerce.

Quando facciamo un acquisto dobbiamo ricordare sempre di fare le seguenti verifiche:

1. Controllare il dominio e diffidare dei siti troppo vantaggiosi
2. Verificare il nome del sito

3. Leggere le recensioni degli altri utenti

4. Verificare che i testi siano scritti correttamente

Non immettere mai i dati di pagamento prima di aver verificato l'affidabilità del circuito di pagamento.

Le truffe possono arrivare dallo smartphone e dai device mobili attraverso la ricezione di e-mail e di sms ingannevoli; imparare a riconoscerli è l'unico modo per evitare di diventare vittime inconsapevoli.



COME RICONOSCERLI

SMS

1. Il messaggio spesso arriva da un numero sconosciuto o non inserito nella tua rubrica.
2. Contiene un link che non rimanda al sito del presunto mittente;
3. il testo del messaggio è spesso generico senza riferimenti al n° di pacco cui si riferisce o al n° di conto;
4. per effettuare le verifiche richieste richiede l'inserimento delle tue credenziali.

MAIL

1. Il mittente è sconosciuto o ha un indirizzo diverso dal solito;
2. L'oggetto non è chiaro o è generico;
3. Contiene link o allegati;
4. Generalmente cercano di farti cliccare sul link o scaricare l'allegato.

Ricorda: banche, poste, corrieri e pubbliche amministrazioni comunicano attraverso i loro canali ufficiali e non chiedono mai di inserire

o confermare dati personali o password o di aggiornare i metodi di pagamento.

In caso di dubbio chiedi ad un esperto o contatta il presunto mittente per verificare la veridicità del messaggio ricevuto. Se ricevi un messaggio o e-mail e sospetti che sia una truffa non cliccare su nessun link e cancellalo.

Guarda il video sulla cybersecurity

**[https://www.youtube.com/
watch?v=MJxtTlyuqll](https://www.youtube.com/watch?v=MJxtTlyuqll)**

10.

GIOCO E DIPENDENZA

I nativi digitali sono abituati ad usare internet per studiare, divertirti, per rimanere in contatto con gli amici. Questo utilizzo smodato può favorire lo sviluppo di forme di dipendenza da internet.

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo ed incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o portare a isolamenti, sintomi da astinenza, problematiche a livello scolastico e "craving" (irrefrenabile voglia di utilizzo della Rete).

Come riconoscerla?

- Viene trascorso tanto tempo online da perdere la concezione del tempo, della fame o del sonno;

- Quando non si riesce ad accedere ad internet si provano sentimenti di rabbia, ansia o depressione;
- Il desiderio di avere strumenti sempre migliori per essere online;
- Si manifestano segnali di isolamento sociale e un peggioramento del rendimento scolastico.
- Peggioramento rendimento scolastico

Se si manifestano alcuni di questi sintomi è importante cercare aiuto.



Guarda il video

<https://www.youtube.com/watch?v=-At3FI2IcTI>

CONCLUSIONI

La rete ci aiuta e ci supporta nella vita di tutti i giorni ed è importante conoscerne anche i rischi, in questa breve guida abbiamo voluto spiegarvene alcuni per imparare a tenere aperti e prenderti cura di te stesso.

Essere cittadini è una grande responsabilità, essere cittadini digitali lo è ancora di più perché le nostre idee, opinioni valicano i confini territoriali e hanno ricadute più grandi di quello che possiamo immaginare.

Utilizzare in modo corretto la rete può sembrare semplice ma non lo è ed per questo che noi adulti dobbiamo essere i primi a farlo per diventare un esempio per i nostri figli ed allievi.



SITOGRAFIA

<https://www.samsung.com/it/campaign/crescere-cittadini-digitali/>

<https://networkindifesa.terredeshommes.it/>

<http://factcheckers.it/>

<https://www.generazioniconnesse.it/site/it/home-page/>

<https://haveibeenpwned.com/>

<https://paroleostili.it/>