Vivi Internet, al meglio.

Curriculum per docenti

sull'educazione civica digitale

Vivi Internet, al meglio.

Cari Docenti,
vi presentiamo questa nuova guida nata dal lavoro di Telefono Azzurro con il supporto di Google nell'ambito del progetto Vivi internet, al meglio!

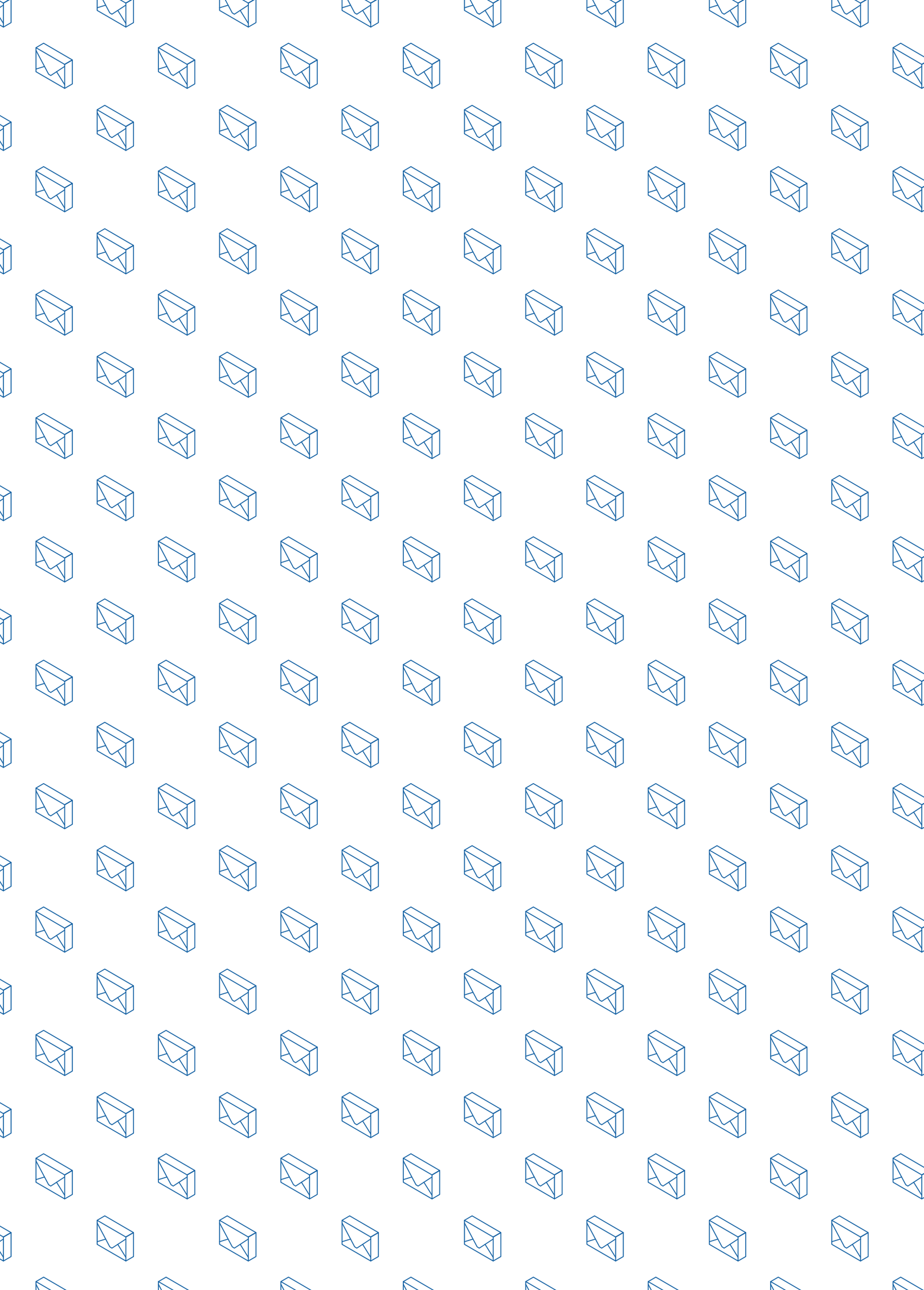
Ogni giorno Telefono Azzurro ascolta e aiuta bambini e adolescenti in difficoltà, tutelandoli da abusi e violenze che possono pregiudicarne il percorso di crescita. Al telefono, in chat, sul territorio Telefono Azzurro è storicamente ascolto, intervento e prevenzione.
Ma negli anni è cambiato, con e per i bambini e i ragazzi, interagendo con loro anche sui social. Una vera e propria piattaforma integrata – telefono, web, social media, app, centri territoriali, gruppi locali di volontari – per rispondere alle esigenze delle nuove generazioni di nativi digitali che impongono un approccio multicanale per affrontare abusi e disagi vecchi e nuovi, potenziali ed effettivi.
Da sempre è un osservatorio privilegiato e permanente sulla condizione dell'infanzia e dell'adolescenza, un punto di riferimento autorevole in grado di di dare risposta alle tante e nuove situazioni critiche che possono pregiudicare i diritti dei minori.
In costante aumento sono le richieste che pervengono da parte di bambini, ragazzi e adulti che riguardano il mondo digitale e le problematiche ad esso connesse. In questo contesto si inserisce la **Helpline di Telefono Azzurro 1.96.96** un servizio multicanale **attivo 24/7 attraverso la linea telefonica gratuita 1.96.96 e la chat -accessibile attraverso il sito www.azzurro.it- , attiva dal lunedì al venerdì (h 8-22) sabato e domenica (h 8-20).**
Da questa esperienza e dalla collaborazione con Google nasce questo Handbook dedicato a Voi docenti come supporto nel vostro lavoro. E' diviso in 5 aree tematiche che approfondiscono i temi trattati nel corso online Vivi Internet al meglio:

- **Condividi usando il buon senso**
- **Impara a distinguere il vero dal falso**
- **Custodisci le tue informazioni personali**
- **Diffondi la gentilezza**
- **Nel dubbio, parlane**

Per approfondire e trattare questi temi con i propri studenti sono state create inoltre delle semplici schede che contengono diverse attività pratiche da svolgere in classe.
Tutte le attività presentate sono da svolgersi con il proprio gruppo classe; si consiglia la partecipazione anche di un secondo docente supervisore che possa aiutare sia nella conduzione dei laboratori, che nell'osservazione e restituzione alla classe delle dinamiche relazionali che si creano durante lo svolgimento dei lavori.
Potrete scaricare gli allegati con le schede direttamente dal sito https://vivinternet.azzurro.it/

Contenuti

Temi	Aspetti ICT	eSkills/obiettivi	Pagina	Esercizi
Identità digitale 	Web reputation Ombra digitale Privacy Protezione di dati personali e password	Acquisire maggiore consapevolezza dei rischi connessi all'utilizzo delle nuove tecnologie; imparare a proteggere i propri dati personali e a rispettare la privacy altrui.		Allegato 1
Phishing 	Frode online - Manipolazioni dei dati - Protezione dei dati personali	Incoraggiare il pensiero critico e permettere di distinguere quelle che possono essere situazioni pericolose in cui possono essere rubati i propri dati personali e di conseguenza come proteggere quest'ultimi.		Allegato 2
Sicurezza digitale 	Protezione e condivisione delle password	Acquisire consapevolezza sui rischi legati alla rete; linee guida da seguire per la costruzione di password efficaci; evidenziare l'importanza della condivisione delle password con i genitori.		Allegato 3
Bullismo/ cyberbullismo 	Comunicazione online, Ruoli nei fenomeni di bullismo e cyberbullismo, diffusione di comportamenti gentili da contrasto ai fenomeni.	Conoscenza dei fenomeni di bullismo e cyberbullismo e relative norme di comportamento utili al contrasto. Acquisizione di consapevolezza sui temi della comunicazione digitale, nell'ottica di un suo utilizzo teso a promuovere comportamenti gentili e positivi.		Allegato 4
Adulti e digitale 	Nuova grammatica delle relazioni - Empatia - Dispositivi e minori	Strutturare un nuovo modo di parlare con i ragazzi del mondo digitale; implementare l'empatia e la condivisione; educazione all'uso consapevole del digitale.		Allegato 5



1.

Condividi usando il buon senso

Gli adolescenti vivono un periodo della loro vita in cui mostrarsi in pubblico significa prima di tutto definirsi ed essere definiti.
In questa fase cruciale del loro sviluppo si delinea quella che viene definita l'identità di un individuo. I ragazzi oggi hanno la possibilità di mostrarsi in pubblico, relazionarsi e socializzare non solo dal vivo, ma anche attraverso le tecnologie digitali.
L'utilizzo del digitale sin da giovanissimi e senza una corretta guida, può far sì che i ragazzi a volte non riescano a percepire l'importanza di ciò che deve restare privato e le conseguenze del pubblicare online le proprie informazioni personali.
Questo può accadere perché in questa fase delicata dello sviluppo i ragazzi possono confondere la propria identità personale con l'identità digitale. Vediamo nel dettaglio di cosa si tratta nei paragrafi successivi.

1.1. L'identità digitale

L'**identità personale** rappresenta l'insieme delle caratteristiche fisiche, psicologiche, culturali di un individuo, che lo distinguono da tutti gli altri, rendendolo unico.
Le attuali tecnologie hanno ormai trasformato le modalità attraverso cui un individuo costruisce la propria identità personale. Tutto ciò che facciamo viene "digitalizzato", dagli acquisti online alla posizione rilevata dal GPS del nostro smartphone, dalla condivisione di una foto sui social alla registrazione su un sito web.
Sono tutte azioni quotidiane che lasciano tracce su chi siamo, come pensiamo, cosa vogliamo, creando uno **specifico profilo** che definisce gli aspetti personali, economici e professionali, costruendo così la nostra **"identità digitale"** che, insieme a quella personale, contribuisce a fornire una descrizione completa dell'individuo. Per fare un esempio, le aziende si informano e si interessano ai profili social dei candidati, per ricostruirne, insieme ad altri elementi, il profilo socio-culturale, relazionale e valoriale e valutarne l'inserimento in azienda.
Mentre l'identità digitale di un individuo adulto - non nativo digitale - si costruisce successivamente e si innesta in un'identità personale già definita , forte e strutturata, pregressa e svincolata dall'online, per i millennials l'identità digitale si forma in quella fase dello sviluppo in cui si definisce anche l'identità personale , con la conseguenza che il confine tra le due può diventare molto sottile. [1]

[1] Per approfondimenti: Telefono Azzurro (2017)
"Il nostro post(o) nella rete – our place in the (e) space".
http://www.azzurro.it/it/content/ebook-il-nostro-posto-nella-rete

1.2 Ombra digitale e web reputation

Può essere difficile rendere consapevoli gli adolescenti che un post che oggi sembra innocuo, in futuro potrebbe essere malinterpretato da un pubblico diverso e più ampio rispetto a quello originario a cui era indirizzato. Alcuni "errori" commessi su Internet in età giovanissima possono "estendersi" come un'ombra e comportare danni permanenti alla **reputazione**.
Foto, audio, video, testi, post di blog e messaggi scritti o registrati sui propri account e profili, ma anche su quelli di amici o conoscenti, rimangono in rete come **impronte indelebili**.

Con l'espressione **"ombra digitale"** si fa riferimento ad una impronta alimentata dal modo con cui ci rapportiamo con la tecnologia. Quando pubblichiamo una foto, ci registriamo in un luogo, inviamo un messaggio vocale, lasciamo un commento, iniziamo a seguire una pagina o un gruppo, etc. alimentiamo la nostra ombra digitale.

È importante quindi riconoscere e valutare quali informazioni e quali azioni in Rete hanno un impatto maggiore sulla creazione della nostra ombra e identità digitale.

Web Reputation
La Reputazione Online è un aspetto molto familiare ai ragazzi. La costruzione della loro identità passa sempre più dall'online. Oggi, rispetto a quanto accadeva solo alcuni anni fà, le loro relazioni online, le loro prese di posizione, il loro aspetto esteriore, si palesano e definiscono prima in rete che offline. Per loro non vi è più una netta differenza tra le due dimensioni. Nel costruire la loro identità online mettono in atto una serie di comportamenti non corretti (oversharing, profili pubblici, numero di follower/amici altissimo), non considerando che tutte queste informazioni e azioni, una volta condivise, non appartengono più solo ai legittimi proprietari, ma restano in rete lasciando infinite tracce. Questi errori comuni commessi dai ragazzi sono in realtà azioni intenzionali e hanno uno scopo ben preciso, quello di ottenere una sorta di riconoscimento della propria identità nel mondo digitale.

1.3 I rischi per la privacy

La nostra ombra digitale può dire molte cose di noi e afferisce alla nostra privacy, termine che fa riferimento da un lato alla **riservatezza** della propria privata, dall'altro al controllo dei propri **dati personali**. A dichiararlo è il codice privacy (Decreto legislativo n. 196/2003, codice in materia di protezione dei dati personali) la cui finalità è garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e della sua identità personale.

Il concetto di privacy è dunque correlato a quello di dato personale, costituito da qualsiasi informazione relativa all'identità della persona, attraverso la quale è identificata o identificabile. Tra i dati personali ricordiamo:

- **Dati anagrafici** (nome e cognome, indirizzo mail, indirizzo di residenza e/o domicilio, numero di telefono, ecc.);
- **Dati finanziari** (codice fiscale, conto corrente, numero di carta di credito, ecc.);
- **Dati identificativi** (fotografie, video e qualsiasi cosa che permetta l'identificazione diretta dell'interessato);
- **Dati giudiziari** (processi, denunce, ecc.);
- **Dati sensibili** (informazioni utili a rivelare nazionalità, opinioni politiche, convinzioni religiose, ecc.).

La condivisione di queste informazioni online può comportare dei rischi per la privacy, soprattutto se non si è consapevoli delle possibili conseguenze; alcune di queste informazioni, infatti, possono contenere dettagli importanti sulla nostra vita e le nostre abitudini. E' quindi importante imparare a valutare il grado di rischio e di impatto sulla privacy che ogni elemento condiviso potrebbe avere.

Ecco alcuni esempi che potresti condividere in classe con gli studenti:

- Le informazioni sui luoghi e i locali che frequentiamo che, con un solo click, condividiamo grazie a servizi di geolocalizzazione possono rappresentare delle impronte e delle informazioni sensibili a disposizione, potenzialmente, di chiunque.

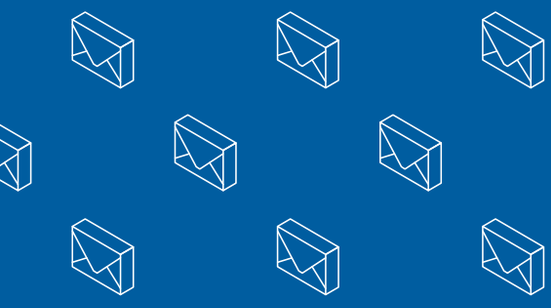
- La registrazioni dei ragazzi presso palestre, locali, scuole, può fornire informazioni molto precise sui loro spostamenti e le loro abitudini.

- Immagini e informazioni della propria abitazione possono fornire a malintenzionati materiale utile per possibili azioni fraudolente e dannose per noi e il nostro nucleo familiare.

- Il tag di un amico in una foto geolocalizzata può fornire informazioni, anche sul suo conto, che magari lui avrebbe evitato di condividere pubblicamente.

Sono tutte informazioni che i ragazzi sentono l'esigenza di condividere, ma spesso si tratta di contenuti che potrebbero rappresentare una confidenza intima, delle informazioni delicate, che varrebbe la pena tenere tra noi e poche altre persone (amici, intimi, familiari, colleghi) e che non dovrebbero mai essere condivise con leggerezza su piattaforme online o, in generale, in contesti pubblici, perché oltre alla reputazione personale potrebbe essere messa in pericolo anche la **sicurezza personale**.

Bisogna far comprendere ai ragazzi che situazioni diverse, richiedono impostazioni di privacy e accortezze diverse.



L'età del consenso digitale
Il d.lgs. 10 agosto 2018, n. 101 ha adeguato la normativa nazionale alle disposizioni del regolamento europeo 2016/679, fissando a 14 anni il limite di età per esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta di servizi della società dell'informazione (es. iscrizione ad un social network, accesso a servizi di messaggistica). Il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sul consenso, invece, è lecito solo se prestato da chi esercita la responsabilità genitoriale.

Dati sensibili e password

Sono diverse le circostanze in cui un ragazzo può essere sollecitato, più o meno direttamente, a condividere le informazioni sensibili che riguardano lui, e/o il suo intero nucleo familiare o il suo gruppo di amici. Riflettiamo insieme su alcuni punti ed invitate anche i vostri studenti alla riflessione. Vi ricordiamo che sono disponibili alcuni esempi nel corso online di Telefono Azzurro disponibile sul sito https://vivinternet.azzurro.it/

1. Quando si accetta che qualcuno ci inserisca in un gruppo di chat o si accetta l'amicizia sui social di persone che non si conoscono benissimo, bisogna chiedersi quali informazioni personali saranno anche e immediatamente a loro disposizione.
2. Ogni volta che si condividono codici di sblocco o password su social e chat di gruppo, ricordate che vi state esponendo a due tipologie di rischio, una goliardata più o meno scherzosa da parte del vostro gruppo di amici, ma anche la diffusione involontaria delle vostre password a estranei malintenzionati.
3. Tra le informazioni sensibili che ci riguardano ve ne sono alcune che possono causare problemi che vanno oltre la privacy e arrecare perdite finanziarie. Oltre alle pratiche di phishing vere e proprie, che spesso simulano richieste di istituti bancari o affini, ci sono anche delle cattive abitudini di condivisione che possono metterci a rischio (ad esempio condividere informazioni su carte di credito o il pin del bancomat).
4. Le password o le combinazioni di sblocco di sistemi di sicurezza e protezione, così come di sistemi di pagamento, non andrebbero mai condivise in Rete, su social e chat.
5. Cancellare la chat di gruppo non tutela chi ha perso involontariamente o condiviso volontariamente le informazioni in esso contenute prima dell'eliminazione del gruppo; anche la cancellazione del messaggio dopo qualche ora potrebbe risultare un gesto tardivo e inutile.

Se ci si dovesse trovare nella necessità di dover condividere questi dati personali è bene seguire queste semplici regole di buon senso:

- la persona deve essere di nostra conoscenza ed affidabile;
- evitare di condividere i dati e le informazioni con più persone contemporaneamente;
- non utilizzare le piattaforme web (o solo piattaforme web), se strettamente necessario, meglio suddividere la comunicazione dei dati su piattaforme e canali differenti (una parte di codice via mail, una parte su WhatsApp, una parte via telefono);
- evitare nelle comunicazioni di esplicitare che si tratta di password o numeri di carta di credito (es. “ecco il numero della carta”, “ecco la password del conto”, etc.);
- evitare di eseguire queste operazioni utilizzando un wifi pubblico.

Violazioni della privacy altrui

Ogni volta che condividiamo un contenuto, un’immagine, un video, un messaggio vocale, etc. dovremmo chiederci se quel contenuto riguarda solo noi o se sta, anche indirettamente, coinvolgendo o esponendo qualcun altro. È sempre importante **rispettare la privacy** delle altre persone, anche se si tratta di scelte che non condividiamo, o che riteniamo eccessive.
Riflettiamo insieme ai ragazzi, con esempi concreti, che ciò che per loro può rappresentare uno scherzo o un gioco, per qualche altra persona potrebbe rappresentare motivo di grande imbarazzo o disagio. Ricordiamo loro che tutti hanno il diritto a mantenere i propri segreti privati. Anche in questo caso potete utilizzare come spunto le storie tratte dal corso online di Telefono Azzurro disponibili sul sito https://vivinternet.azzurro.it/

(per le attività vedi Allegato 1 – disponibile sul sito https://vivinternet.azzurro.it/)

2.

Impara a distinguere il vero dal falso

È importante che i ragazzi capiscano che i contenuti che trovano o a cui vengono esposti online non sono necessariamente affidabili e che a volte potrebbe trattarsi di tentativi di rubare loro informazioni personali. Il **phishing** e altre **frodi online** incoraggiano gli utenti di Internet di tutte le età a rispondere a esche lanciate da persone che fingono di conoscerli o di contattarli per conto di brand conosciuti.
La percezione e la consapevolezza delle minacce informatiche è ancora molto bassa e spesso non vengono attuate le giuste misure di protezione. Diventa quindi importante imparare ad essere prudenti nel cyberspazio e acquisire le giuste competenze e conoscenze per poter contrastare i rischi della Rete.

Phishing Il termine phishing deriva da fishing ("pescare" in inglese), e allude al tentativo di "pescare" dati personali, finanziari e password di un utente. Questo tipo di attacco sta registrando una crescita costante.
Spear phishing Frode di phishing mirata in cui chi compie l'attacco usa le tue informazioni personali per sceglierti come bersaglio
Catena di Sant'Antonio Tipologia di phishing che utilizza strumenti apparentemente innocui come e-mail o post in cui viene chiesto di far girare un dato messaggio a tutti i propri contatti

I rischi che verranno analizzati in questo capitolo si riferiscono agli attacchi online quali il phishing; nello specifico cosa sono le frodi online, le catene di Sant'Antonio, i sender e link, i ransomware.

È importante aiutare i ragazzi a comprendere che le persone e le situazioni online non sono sempre ciò che sembrano. Saper distinguere il vero dal falso è molto importante, quando si parla di sicurezza online.

Riconoscere i segni di una potenziale frode

1. Se le affermazioni che promettono di "vincere" qualcosa o di averlo "gratis" sembrano troppo belle per essere vere, molto probabilmente non lo sono.
2. In uno scambio non dovrebbe essere chiesto di divulgare informazioni personali di alcun tipo.
3. Riflettere sempre prima di agire online. Fare attenzione al phishing, ovvero al tentativo di furto di dati di accesso o dettagli dell'account tramite email, SMS o altre comunicazioni online che sembrano provenire da un contatto fidato.

2.1 Non è tutto oro quello che luccica: il phishing e come si manifesta

Quando parliamo di phishing facciamo riferimento ad un tipo di truffa che consiste nel procurarsi, in maniera fraudolenta, dati riservati delle proprie vittime. Rientra nel phishing, ad esempio, la **sottrazione di dati sensibil** per rivenderli a società pubblicitarie, ma anche a rubare denaro tramite il furto di credenziali bancarie o semplicemente infettare i dispositivi con virus in grado di appropriarsi dell'elenco dei contatti dell'utente per inviare ulteriori email di phishing.

Questo tentativo fraudolento spesso utilizza Brand noti all'utente, verso i quali si nutre fiducia, per cercare di ottenere dati personali a fini illeciti.

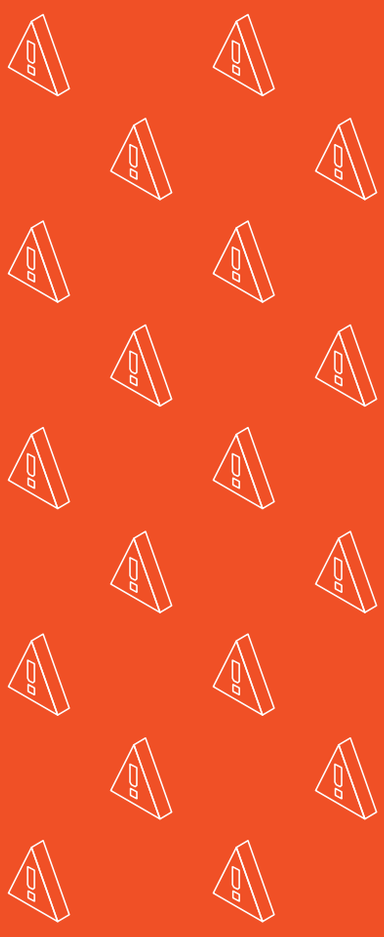
Entrando nel dettaglio, per meglio riconoscere il fenomeno, è bene comprendere come esso si manifesta. Accade che messaggi, spesso inviati via e-mail, apparentemente da entità note e reali come banche, siti di prenotazione, etc. sollecitano il destinatario a fare click su un link per verificare account personali al fine di rafforzare la sicurezza o in cambio di benefici o servizi gratuiti. Queste pratiche consentono ai malintenzionati di ottenere l'accesso da remoto ai dispositivi delle vittime malcapitate o di impossessarsi di informazioni sensibili come nome utente, password o nei casi peggiori dei dati della carta di credito o di altre forme di pagamento online.

A volte il phishing utilizza strumenti apparentemente innocui come e-mail o post in cui viene chiesto di far girare un dato messaggio a tutti i propri contatti; ne sono un esempio le famose catene di Sant'Antonio,sistemi utilizzati spesso da spammer per raccogliere massivamente indirizzi a cui inviare pubblicità di vario genere, o addirittura veicolare virus tramite link predisposti ad hoc, o nascondere vere e proprie truffe.
Molti tentativi di frode online possono avvenire anche tramite piattaforme social. Ad esempio, sulle pagine di personaggi pubblici o celebrità può accadere che tra i commenti ai post un utente inserisca un link per ottenere ingressi gratuiti, biglietti di concerti, etc.

Bisogna sempre **verificare con attenzione** un messaggio che offre, in modalità completamente gratuita, qualcosa che ha un valore economico oggettivo. Per questo motivo è importante prestare sempre la massima attenzione al controllo dei propri account sul web e attivare nella casella di posta i filtri antispam.
In questa situazione bisognerebbe consigliare ai propri alunni di ignorare il messaggio e non cliccare gli eventuali link presenti, nonchè di diffidare in futuro da questo tipo di messaggi e cancellarli ed infine informare tutta la classe delle truffe che si nascondono dietro questo tipo di messaggio.

2.2 Come riconoscere un tentativo di frode

Alcuni attacchi di phishing sono facilmente riconoscibili. Altri possono raggiungere un tale grado di sofistificazione da risultare estremamente convincenti anche per gli utenti più attenti. Per esempio, un truffatore potrebbe mandare un messaggio che già include alcune informazioni personali del destinatario: questo tipo di attacco è chiamato **“spear phishing”** e spesso si rivela efficace. Spesso i virus che si diffondono tra amici sfruttano proprio le reti di conoscenze per carpire informazioni da riutilizzare in azioni di phishing.



Campanelli d’allarme

Nell’email o in chat ti viene offerto qualcosa gratuitamente?
Normalmente le offerte gratuite non sono davvero tali.

Ti vengono richieste informazioni personali?
Alcuni siti ti chiedono informazioni personali apparentemente banali ma da cui è possibile desumere informazioni sensibili. Per esempio, i “test della personalità” potrebbero raccogliere dati per riuscire a indovinare la tua password o sottrarti altre informazioni private. La maggior parte delle imprese reali, viceversa, non richiede informazioni personali via email.

Si tratta di una catena o di qualcosa che le assomiglia?
Le email e i post in cui ti viene chiesto di far girare il messaggio a tutti i tuoi contatti possono mettere a rischio te e altre persone. Non farli girare a meno che tu non conosca la fonte e sappia con certezza che il messaggio è sicuro.

Contiene porzioni di testo scritte in piccolo?
In fondo alla maggior parte dei documenti puoi trovare delle note scritte con caratteri più piccoli. Questa parte di testo spesso contiene informazioni importanti scritte in piccolo di modo che tu non le legga. Per esempio, potrebbe esserci un titolo in cui ti viene annunciato che hai vinto un telefono in omaggio, ma in piccolo c’è scritto che per averlo devi pagare 200 euro al mese.

2.3 Le diverse tipologie di phishing

Come già evidenziato, il Phishing si può manifestare in diversi modi ed è importante saper riconoscere le forme più comuni in modo da non incorrere in questi rischi e poter navigare online in sicurezza.

Spear phishing

Sostanzialmente è un’evoluzione del phishing. L’obiettivo finale rimane lo stesso, ovvero sottrarre dati sensibili della vittima. La differenza principale tra le due minacce è che lo spear phishing non invia e-mail casuali a una moltitudine di utenti, ma a differenza del phishing si concentra su poche vittime, calibrando in modo mirato l’attacco.

Offerte gratuite e catene di Sant'Antonio

Altra forma di phishing molto usata sono le **catene di Sant'Antonio**. Esistono almeno due tipologie di catene sulle chat mobili: le prime, meno pericolose, sono ideate a scopo meramente ludico e basate sulla diffusione di bufale, o messaggi allarmistici e solitamente non contengono link; le seconde, invece, sono molto più pericolose e solitamente contengono un link e un invito al click. In quest'ultima tipologia il link, nella maggior parte dei casi, è collegato a un virus o all'attivazione di qualche servizio a pagamento. Tale virus potrebbe anche non compromettere l'hardware dello smartphone, ma solo i dati, allo scopo di ottenerne un vantaggio economico.

La formattazione di un dispositivo mobile o di un computer è una operazione tramite cui si può resettare il dispositivo e riportarlo alla sua "condizione iniziale".
Quando il dispositivo viene colpito da un virus, la formattazione consente di eliminare il fastidioso ospite, cancellando tuttavia anche gli altri dati presenti nella memoria.
Per questo motivo, quando si custodiscono dati importanti, è bene eseguirne un backup periodico, ovvero una copia dei dati, in modo da custodirli in un'altra memoria e poterli recuperare all'occorrenza.

Nel caso in cui si cada in questa tipologia di pericolo, formattando il dispositivo si può risolvere il problema, ma solo parzialmente. Con la formattazione di un dispositivo si possono, infatti, perdere tutte le informazioni salvate e che in realtà non vorremmo cancellare. Invece, per annullare l'iscrizione a un servizio a pagamento bisogna contattare il proprio operatore telefonico e diffidarlo, eventualmente anche per iscritto, dall'addebitarvi i costi per servizi a pagamento non richiesti ed attivati dal link infetto.

Anche il dominio che sottende il link è un elemento da considerare e guardare con attenzione perché può rappresentare un campanello d'allarme.

Sender e Link

I pirati informatici sono sempre al passo della tecnologia e per questa ragione hanno perfezionato le proprie tecniche di frode per raggiungere al meglio i propri intenti illeciti.
Gli indirizzi dei mittenti di email di phishing somigliano molto a quelle ufficiali dell'entità e/o delle aziende di brand che fingono di essere. Anche i siti web a cui gli utenti vengono indirizzati tramite i link incorporati in post o e-mail sono quasi identici a quelli originali, vedendo come unica caratteristica che cambia l'URL, ovvero l'indirizzo del sito.

Queste differenze sono spesso impercettibili ad un occhio inesperto, per questo motivo bisogna prestare sempre la massima attenzione quando navighiamo ed apriamo un link ed imparare ad osservare il dominio,ovvero l'indirizzo univoco attraverso il quale viene richiamato il sito internet sulla Rete) che sottende il link all'interno della mail, ma anche prestare attenziona all'indirizzo mail del sender, ovvero di colui che ci invia la mail di phishing.

Solo in questo modo sarà possibile riconoscere i tentativi di phishing e segnalare l'abuso via email ai titolari del sito ufficiale da cui sembrerebbe partire l'email, o denunciare l'avvenuto alla polizia postale.

HTTPS (Hypertext Transfer Protocol Secure) è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati tra i computer e i siti.
I dati inviati tramite HTTPS vengono protetti tramite il protocollo Transport Layer Security (TLS), che fornisce tre livelli di protezione fondamentali:

Crittografia: i dati scambiati vengono criptati per proteggerli dalle intercettazioni.

Integrità dei dati: i dati non possono essere modificati o danneggiati durante il trasferimento, intenzionalmente o meno, senza essere rilevati.

Autenticazione: dimostra che gli utenti comunicano con il sito web previsto.

Pertanto, potrebbe non essere sicuro visitare e in particolare lasciare informazioni sensibili come i dati di una carta di credito (su e-commerce per esempio) su siti web non protetti dai protocollo HTTPS.

Facendo un breve riepilogo, bisogna prestare attenzione se:

- l'indirizzo e-mail associato al messaggio, o il nome di colui che posta un commento ritenuto "pericoloso" contiene un lungo mix di lettere e numeri. Non sembra, quindi, il nome di una persona reale o un indirizzo email autentico (ad esempio andre58ax09@esempio.ru);
- il link contiene un dominio molto simile, ma non completamente uguale a quello reale (ad esempio www.goooogle.it al posto di www.google.it);
- il messaggio contenuto è in inglese o in un'altra lingua diversa dall'italiano;
- Il messaggio contiene errori grammaticali;
- il link rimanda a un sito che non utilizza connessioni HTTPS;
- l'allegato contiene una doppia estensione: nome.pdf.exe, o un'estensione strana come .pif e cliccandovi due volte si esegue invece un file malevolo.

2.4 Baiting e ransomware

Il "baiting" è una tecnica di phishing che consiste nell'offrire qualcosa al fine di consentire il download di un file dannoso che contiene un "ransomware", ovvero un tipo di virus che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.
Per questo motivo bisogna sempre controllare l'indirizzo email del mittente, ancora di più se lo scopo della mail è una richiesta di informazioni, ma anche verificare e accertarsi dell'estensione dell'allegato prima di scaricarlo (allegati immediatamente eseguibili come .exe, .bat o ancora .msi).

Inoltre, è sempre bene effettuare tutte le verifiche del caso prima di scaricare allegati o cliccare su link segnalati, per accertarsi della veridicità della email, oltre ad installare sul pc un buon antivirus e anti-phishing.

Cosa fare se un tuo alunno è vittima di una truffa?

La prima cosa che bisogna far comprendere ad un ragazzo o ad una ragazza vittima di una truffa è che quello che gli è capitato potrebbe capitare a tutti (anche agli adulti) e che non dovrebbe farsi prendere dal panico o sensi di colpa.

La migliore cosa da fare è individuare insieme a lui delle specifiche azioni che possano aiutare ad arginare possibili danni.

Bisogna consigliarli di parlare subito con i genitori o con un adulto di cui si fida, di cambiare le password degli account online ed in ultimo, accertato che si tratti di un tentativo di phishing o di frode, avvisare tutti i contatti che potrebbero essere il prossimo bersaglio.

In caso di dubbi è sempre possibile contattare il Telefono Azzurro per chiedere un supporto

Come comportarsi con gli sconosciuti in rete?

Ci sono casi in cui le persone che si trovano all'interno del cyberspazio fingono di essere qualcun altro, in alcuni casi per fare degli scherzi, in altri allo scopo di rubare informazioni personali.

Ai vostri studenti potrebbe capitare che degli sconosciuti chiedano di entrare in contatto con loro su svariate piattaforme web e social network.
Per far si che i ragazzi non incorrano in rischi, dovrebbero essere messi nella condizione di scegliere con consapevolezza chi aggiungere e cosa o come rispondere a questi inviti.

Ci sono degli elementi a cui prestare attenzione per verificare l'identità delle persone che ci contattano e identificare potenziali truffatori.

Ecco alcune domande che i ragazzi dovrebbero imparare a porsi quando contattati sul web da sconosciuti.

• **L'immagine del profilo è reale e se reale è sfocata?**
Se l'immagine non è una foto di una persona reale ma un'immagine/illustrazione sii prudente, ma anche se la foto è di una persona reale, verifica se si vede bene o è sfocata.
È facile nascondersi dietro a una foto sfocata.
Inoltre non è difficile per i truffatori rubare foto di persone reali per creare profili falsi.

• **Sul profilo ci sono informazioni personali dettagliate?**
Se ci sono sembrano scritte da una persona reale?
Gli account falsi spesso non hanno molte informazioni nella sezione "Su di me" e quelle che ci sono potrebbero essere state inventate solo per creare un profilo falso e particolarmente accattivante.

• **Da quanto tempo esiste questo account?**
Sugli account falsi spesso non si trovano molti post, né molte interazioni sociali, questo significa che i contatti non conoscono bene il proprietario del profilo e non intergiscono con lui. I contatti o sono molto eterogenei tra loro per nazionalità e interessi o possono essere molto pochi se il profilo è stato appena aperto.

In questi casi è bene suggerire agli studenti come dovrebbero comportarsi di fronte a queste tipologie di situazioni.
Un primo consiglio che si potrebbe dare in questi casi è di ignorare il messaggio, o bloccare il profilo della persona che li contatta, soprattutto se intuiscono che non ci siano buone intenzioni.
Si deve sottolineare di non inviare dei dati personali, come indirizzo di casa o altre informazioni personali e che invece bisogna verificare l'identità del soggetto anche quando si pensa possa essere una persona conosciuta, o che li incuriosisce.
In questo caso bisogna esortarli ad approfondire chi possa essere la persona dall'altra parte dello schermo e a fare delle domande che lo aiutino a capire chi sia.

(per le attività vedi Allegato 2 – disponibile sul sito https://vivinternet.azzurro.it/)

3.

Custodisci le tue informazioni personali

Ciò che facciamo per la nostra sicurezza online non è sempre del tutto corretto o sufficiente. **Per proteggere le informazioni personali e private** nella maniera corretta bisogna prima porsi le giuste domande e successivamente trovare le adeguate risposte. Tutto questo è possibile grazie all'acquisizione di conoscenze.

3.1 Custodire i segreti

La tecnologia digitale facilita e consente ai nostri ragazzi di accedere a informazioni e servizi online, e di comunicare con amici, compagni, insegnanti in qualsiasi parte del mondo.

Gli stessi strumenti potrebbero, però, permettere anche ad hacker e malintenzionati di rubare informazioni e usarle per danneggiare i nostri dispositivi, le nostre relazioni, o la nostra reputazione. Proteggere tutto ciò che riguarda la nostra reputazione online significa adottare semplici ma importanti misure come usare il blocco schermo sui nostri dispositivi, fare attenzione alle informazioni personali inserite che potrebbero andare perse o venire rubate e, soprattutto, **scegliere delle ottime password**. Infatti, siamo sommersi da codici, parole chiave da ricordare per accedere a servizi di social network, e-mail, musica o film in streaming, videogame, e per questo si tende ad utilizzare sempre la stessa password. Ad esempio, nel 2017 la più usata al mondo è stata «123456».

Ormai anche i vecchi consigli sulla creazione di password come "Scegli almeno un simbolo, un numero, una maiuscola, non usare parole comuni" non sono più sempre sufficienti rispetto alla sofisticazione delle azioni fraudolente in Rete. Una password come «1nt3rn3T - IntErneT» poteva essere sicura dieci anni fa, mentre oggi può essere scoperta in pochissimo tempo. Inoltre, è una sequenza faticosa da ricordare che, probabilmente, qualcuno salverà sul proprio pc, su un file chiamato «password.txt».

Conoscere alcuni dei maggiori metodi e cliché di hackeraggio può aiutare, noi e i nostri ragazzi, a scegliere password più sicure. Tra questi metodi di hackeraggio abbiamo:

- ✓ **l'ingegneria sociale**, tecnica di phishing che consiste nello sfruttare siti come social network o applicazioni online per parlare con la vittima e indurla a fornire informazioni su di sé, oppure per studiarne attentamente il profilo e capire dettagli importanti che potrebbero rivelare una password (nomi di figli, fidanzati, amici, data di nascita o di matrimonio, etc.);

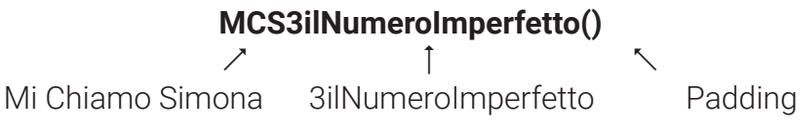
- **un attacco di forza bruta**, consiste nell'esecuzione di un programma capace di provare in brevissimo tempo moltissime combinazioni di password prese da un dizionario-database creato ad hoc, magari partendo da parole individuate dal social engineering, per cercare di individuare quella giusta. In questo senso, tanto più le nostre password sono prive di collegamenti ad eventi che ci riguardano, tanto più sarà difficile individuarle.

Ladri di segreti: Come creare la password per custodirli

La creazione di una password sicura è un aspetto importante per la protezione dei nostri account. Una password efficace protegge le nostre informazioni personali, le e-mail, i file inviati o ricevuti, e rende difficoltoso, se non impossibile, l'accesso illecito ai nostri account. Quando scegliamo una password dovremmo seguire alcune buone abitudini:

- scegliere **password lunghe** in quanto più sicure. Infatti, quando una password è troppo corta e utilizzata su tutti i siti, diventa più a rischio rispetto a una password lunga; la lunghezza è uno degli aspetti più importanti da considerare per creare password a prova di hacker;
- creare una password difficile da indovinare o comprendere da parte di terzi. Non è semplicemente una questione di complessità, ma di imprevedibilità della password. Le password efficaci sono facili da ricordare per noi, impossibili da indovinare per gli altri;
- evitare di scegliere una password che includa o contenga **dettagli personali** come nome, età o data di nascita;
- utilizzare una combinazione di **caratteri alfanumerici** (lettere e numeri) e simboli, non riconducibili a sé o ai nostri cari. Alcuni esempi e buone abitudini su come creare una password efficace, da condividere in classe con i tuoi ragazzi, potrebbero essere:
- **giocare con gli acronimi** di una frase semplice, ma ben rappresentativa della propria identità.
  Es. "Mi Chiamo Simona e Sono Nata il 3 Ottobre" potrebbe diventare "**MCSeSNi3O**";
- **costruire una passphrase**: creare un'unica stringa a partire da una frase composta e imprevedibile. Elimina gli spazi e, se credi, aggiungi le maiuscole all'inizio di ogni parola.
  Es. "3 è il numero imperfetto" potrebbe diventare "**3èilNumeroImperfetto**", "Risotto agli 8 formaggi" potrebbe diventare "**RisottoAgli8Formaggi**"
- **aggiungere caratteri extra** alla parte finale della password che usiamo solitamente (si chiama padding).
  Es. "ioReetuRegina" potrebbe diventare "**10ReetuRegina.11**" oppure "**IoReetuRegina((11))**" oppure "**Io,Re,e,Tu,Regina,11**".

Si potrebbe creare una password adottando tutte queste pratiche contemporaneamente. Ad esempio:



Questa tipologia di password risulta particolarmente difficile da violare e riprodurre.
In alternativa, si potrebbe utilizzare un **password manager**, ovvero un software di gestione delle password, che consente di criptare e custodire le nostre chiavi di accesso ai servizi online. Basta ricordare soltanto una password: quella principale per accedere al programma nel quale sono memorizzate tutte le altre password, salvate automaticamente mentre navighiamo ed effettuiamo l'accesso ai servizi online. Inoltre, consentono di generare password affidabili, tramite la combinazione di caratteri casuali.

3.2 Secondo livello di protezione

A questo primo livello di protezione, caratterizzato da un nome utente e una password, se ne aggiunge un secondo che, con un alto grado di affidabilità, permette l'accertamento dell'identità nel corso dell'attività di autenticazione.

I trucchi per evitare situazioni spiacevoli

La **verifica in due passaggi**, o **autenticazione a più fattori**, è una misura di sicurezza che richiede due passaggi per effettuare l'accesso a un servizio. Si usa per esempio per accedere al proprio internet banking o ai propri account di posta elettronica. Solitamente si tratta di un ulteriore codice di verifica che si genera di volta in volta tramite applicativi, dispositivi o può arrivare anche via sms sul telefono.
Una volta scelta la password perfetta, la verifica in due passaggi aggiunge un secondo livello di protezione.
Esistono decine di opzioni disponibili per proteggere i tuoi account, ma il secondo livello di verifica avviene tramite:

- ✓ codice monouso: viene inviato al telefono o generato da un'app sul telefono;
- ✓ token usb: chiave elettronica o altro piccolo dispositivo hardware da utilizzare per poter autorizzare l'accesso tramite la pressione di un pulsante o l'inserimento di un codice.
  Tra gli altri sistemi di autenticazione a più fattori ci sono l'impronta digitale o il riconoscimento vocale.

Inoltre si stanno compiendo studi su ulteriori metodi di verifica, come la localizzazione, l'analisi di quello che stiamo facendo, della forma in cui parliamo, del respiro, del battito cardiaco ecc. Cosa fare per evitare situazioni spiacevoli? Di seguito alcuni suggerimenti da seguire:

- ✓ non utilizzare password già usate in passato e comuni ad altri nostri account;
- ✓ evitare di lasciare note con le password sul computer o sulla scrivania ed effettuare il log out specialmente quando accediamo ai nostri account da un pc pubblico o utilizzando una rete pubblica;
- ✓ utilizzare, se possibile, sempre le opzioni per il recupero dell'account, che consentono di aggiungere ad esempio un numero di telefono o una email alternativa qualora non riuscissimo più ad eseguire l'accesso;
- ✓ non dare mai la nostra password a nessuno, neanche al nostro migliore amico. Infatti, lo scambio delle password come prova di amicizia è una pratica molto comune tra i preadolescenti e gli adolescenti.

Ma cosa succederebbe se due amici litigassero dopo aver condiviso le password?
Scambiarsi le password non è sinonimo di fiducia, poiché dando libero accesso ad un'altra persona al nostro mondo digitale, diventiamo vulnerabili e aumentiamo la possibilità di essere vittime di vendette online o episodi di cyberbullismo.
L'unica persona con cui si potrebbe, e in alcuni casi dovrebbe, condividere la password è un genitore o tutore.
È bene ricordare che un malintenzionato in possesso della nostra password potrebbe, da quel momento, impedirci di accedere ai nostri account e:

- ● controllare o eliminare le e-mail, i contatti, le foto, ecc;
- ● fingere di essere noi e inviare e-mail indesiderate o dannose ai nostri contatti;
- ● utilizzare il nostro account per reimpostare le password degli altri nostri account.

3.3 Condividere la password con i genitori

Il diritto alla privacy ed alla segretezza delle comunicazioni del minore si scontra con il diritto/dovere di vigilanza dei genitori. Infatti, non solo nel 99.9% dei casi i contratti con i provider di Rete sono intestati ai genitori anche se fruiti dai figli, ma il genitore ha il dovere di proteggere il ragazzo da eventuali pericoli ed è responsabile per quest'ultimo nel caso di azioni illecite. In entrambi i casi i genitori/tutori sono legalmente responsabili in misura differente. Per questo motivo è buona regola che i ragazzi condividano le loro password con i genitori; questi a loro volta devono porsi non come giudici-controllori dei figli ma costruire con loro un rapporto di reciproca fiducia.

(per le attività vedi Allegato 3 – disponibile sul sito https://vivinternet.azzurro.it/)

4.

Diffondi la gentilezza

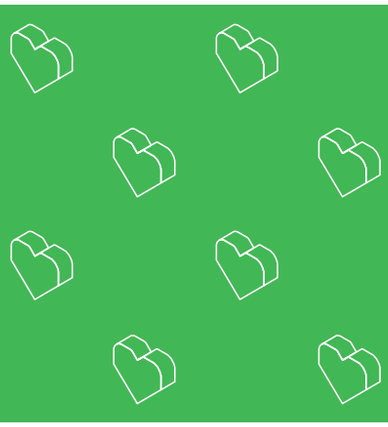
Gli indizi sociali possono essere più difficili da interpretare online, l'anonimato può incentivare comportamenti negativi, il bullismo online tende a ripetersi e l'ombra digitale ne lascia una traccia indelebile.
D'altra parte è necessario essere consapevoli di come internet possa essere utilizzato anche per amplificare la gentilezza.
Imparare a comportarsi con gentilezza ed empatia, così come acquisire strategie per rispondere alle molestie e ai comportamenti negativi, è indispensabile per costruire relazioni sane e ridurre il senso di isolamento che può sfociare in episodi di bullismo, depressione, difficoltà scolastiche o altre problematiche.

4.1 La comunicazione in rete e il cyberbullismo

Gli adolescenti di oggi, nativi digitali, amanti della tecnologia, inseparabili dal loro smartphone, appartengono ad una generazione in comunicazione continua, costantemente connessa ad una Rete (di dati e di persone). Messaggi, e-mail, chat, messaggi vocali, registrazioni video etc. rappresentano canali e mezzi di interazione ritenuti impensabili solo fino a qualche anno fa[2].
Tuttavia, la comunicazione online può annullare quasi completamente il contatto reale, ridurre l'empatia tra gli individui che ne usufruiscono, assottigliare le sfumature e, in alcuni casi, può dare adito a interpretazione diverse rispetto a quanto accadrebbe nella vita reale.
Anche i tempi, online, risultano molto più serrati.
Per questo, quando interagiamo online, è importante ricordare che dietro ad ogni nome utente o avatar c'è quasi sempre una persona reale, che prova sentimenti e che merita di essere rispettata. Questa infatti potrebbe essere ferita da un messaggio, una battuta o un commento frettoloso o superficiale, anche se prodotto senza intenti cattivi.
Non è infrequente che episodi di **bullismo/cyberbullismo** possano inizialmente essere considerati come semplici scherzi o battute inopportune. Nei casi più gravi, un'azione aggressiva, offensiva o denigrante mirata ad intimorire, molestare o procurare disagio a qualcuno, anche su internet, può infliggere un danno psicologico immediato con ripercussioni a lungo termine sulla vittima.

[2] Per un approfondimento si consiglia "Indagine Telefono Azzurro - DoxaKids 2018" - http://www.azzurro.it/it/content/telefono-azzurro-presenta-la-ricerca-spettatori-del-web-realizzata-con-doxakids

Introduciamo dunque il concetto di Cyberbullismo, come definito dalla Legge n.71 29 maggio 2017.



La legge 29 Maggio 2017 n.71 definisce Il cyberbullismo quale "qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identita', alterazione, acquisizione illecita, manipolazione, trattamento illecito i 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.

4.2 Cyberbullismo: chi coinvolge

Quando si verificano episodi di cyberbullismo o comportamenti inappropriati, vengono frequentemente coinvolte tre tipologie di soggetti:

- ✓ un bullo, o più di uno
- ✓ la vittima
- ✓ persone terze, ovvero spettatori o testimoni

In alcune situazioni può accadere che cyberbullo e vittima si conoscano; possono frequentare la stessa scuola o vivere nello stesso quartiere.
Potrebbero però essere perfettamente sconosciuti l'uno all'altro ed essere entrati in contatto con la vittima via internet, per esempio mediante i social networks. In Rete il cyberbullo può anche decidere di nascondersi dietro profili falsi o anonimi.
I testimoni spesso assumono un atteggiamento passivo, osservando senza un ruolo attivo, oppure possono incoraggiare o gratificare il bullo, o al contrario sostenere la vittima.
L'obiettivo della scuola e della famiglia deve essere finalizzato a prevenire e contrastare i comportamenti inappropriati e scorretti, utilizzando qualsiasi mezzo per affermare gentilezza e positività.
Piccoli gesti di gentilezza possono, infatti, fare una grande differenza online, ma è vero anche il contrario; piccoli gesti spiacevoli online possono trasformarsi in situazioni molto brutte e determinare conseguenze tragiche.
Ne è un esempio il fatto che un contenuto offensivo o allusivo messo in Rete da un bullo possa essere condiviso a cascata dai testimoni/osservatori, amplificando in maniera esponenziale l'effetto dell'aggressione, con risultati devastanti per la vittima che, anche a casa sua, non si sentirà mai sicura.
Internet infatti è un luogo senza confini, pervasivo, in grado di raggiungere ognuno ed ovunque.

[3] Per approfondimento si consiglia l'Handbook "Non stiamo Zitti" - Guida operativa per docenti. Realizzata da Telefono Azzurro e disponibile al seguente link: http://www.azzurro.it/it/content/handbook-non-stiamo-zitti

Forme di cyberbullismo: lessico essenziale

Gli attacchi e le ostilità online possono assumere diverse forme e sono così sintetizzabili:

- Il **Flaming** (da flame, fiamma), consiste nell'invio di messaggi offensivi allo scopo di innescare battaglie verbali online (ad esempio su una piattaforma di giochi online) tra due o più soggetti, che si trovano allo stesso livello. Il dislivello di potere, quindi, non è ritenuto necessario, ed è inoltre circoscritto alla durata di quella specifica attività online.

- L'**Harrassment** (molestia), è un comportamento simile al Flaming, ma si verifica quando vi è l'invio ripetuto di messaggi denigratori, che ha come obiettivo ultimo quello di ferire qualcuno.

- Quando si parla di **Cyberstalking** (persecuzione telematica) l'artefice dell'aggressione non si limita più ad offese, ma perseguita la sua vittima con vere e proprie minacce, tanto da farle temere per la propria incolumità fisica.

- La **Denigrazione** avviene attraverso la diffusione di pettegolezzi o immagini imbarazzanti sulla vittima allo scopo di ridicolizzarla e danneggiarne la reputazione.

- La **Sostituzione dell'Identità** ha luogo quando il cyberbullo si impadronisce dell'account della vittima e, fingendo di essere quest'ultima, invia messaggi ai suoi contatti al fine di rovinarne la reputazione.

- Si parla di **Trickery** (raggiro) quando il cyberbullo ottenendo la fiducia della vittima con l'inganno, ne rivela informazioni personali e riservate. Può metterlo in atto condividendo registrazioni/chat, o minacciando di farlo nel momento in cui la vittima non esaudisce le sue richieste.

- Cyberbullismo è anche **escludere** la vittima da chat di gruppo online, o piattaforme di gioco interattive. Infatti, oggi la leadership di un adolescente è dettata anche dalla sua rete di amicizie online, non solo da quella reale, e l'esclusione rappresenta una vera e propria punizione mirata a ledere la popolarità della vittima.

- Il **Cyberbashing o Happy Slapping** (letteralmente "schiaffeggio allegro"), è la forma più estrema di cyberbullismo che consiste nella ripresa di atti di violenza nei confronti della vittima, e nella successiva condivisione del video sulle piattaforme social. Si tratta di un vero e proprio comportamento criminale.

4.3 Contrastare il cyberbullismo

La vittima

Nella società odierna siamo abituati a pensare ai ruoli di bullo/cyberbullo e vittima come eccessivamente stereotipati: in molte circostanze il primo viene etichettato come un ragazzo arrogante e sicuro di sé che infastidisce e maltratta la vittima, idealizzata a sua volta come il compagno ritenuto più vulnerabile. Nella realtà questo non sempre può corrispondere al vero. Alla luce di ciò, ne risulta quindi che chiunque possa essere vittima di bullismo e/o cyberbullismo.

In molte circostanze le vittime riescono ad aprirsi soltanto in casi molto gravi, se non in presenza di veri e propri reati. Più spesso di quanto si pensi, **restano in silenzio**, arrivando anche a compiere gesti talvolta fatali. A volte le vittime potrebbero compiere un errore di valutazione, non riconoscendo ciò che stanno subendo online come cyberbullismo. Altre volte la vittima ne è consapevole, ma è emotivamente sopraffatta da un senso di tristezza e ingiustizia, o di colpa.

La maggior parte delle volte la vittima non ne parla con nessuno, oppure ha difficoltà nel confidarsi con un adulto. La famiglia e la scuola assumono un ruolo fondamentale per instaurare un rapporto di fiducia, nel quale i ragazzi non si sentono giudicati. L'immedesimazione da parte dell'adulto permetterebbe alla vittima di trovare conforto, e di bloccare il cyberbullo.

Gli osservatori

Nel verificarsi di un episodio di cyberbullismo il ruolo degli **osservatori** risulta essere particolarmente cruciale. Questi infatti, a seconda dell'atteggiamento che assumono, possono favorire o contrastare il dilagare delle prepotenze. Quasi sempre, infatti, gli episodi di cyberbullismo avvengono in presenza "digitale" dei coetanei, sui social o sulle chat. Questi infatti, proprio per le loro caratteristiche intrinseche, amplificano in maniera esponenziale e potenzialmente illimitata il numero degli osservatori.

Per questo motivo, è importante offrire ai ragazzi delle buone norme di comportamento nel caso in cui si trovassero nel ruolo di testimoni.

L'osservatore potrebbe offrire il buon esempio, facendo da mediatore nella relazione tra bullo e vittima e dimostrando gentilezza, così da diffondere positività. Per non far sentire la vittima sola, è importante che l'osservatore si ponga con essa in maniera amichevole, sia online che offline, in modo da offrire sostegno e supporto.

Non incoraggiare i comportamenti negativi assumendo il ruolo di "pubblico", evitando quindi di partecipare o rispondere a commenti o post offensivi. A volte infatti i bulli assumono tali comportamenti per attirare l'attenzione, ed è per questo che non vanno incoraggiati.

Un'altra buona norma può essere quella di non far girare messaggi offensivi, segnalandoli al mittente come contenuti sgradevoli. Questo è infatti un comportamento giusto e coraggioso, che può essere accompagnato da un sostegno alla vittima e che rappresenta una presa di posizione.

Il testimone potrà infine segnalare i comportamenti persecutori attraverso gli appositi strumenti di segnalazione online, o parlarne con un adulto di riferimento e con il suo gruppo di pari.
Sia ragazzi che adulti possono contattare il Telefono Azzurro in caso di dubbi per chiedere un supporto od una consulenza

4.4 Il ruolo degli educatori

Vittime, autori e osservatori di cyberbullismo spesso **nascondono** l'accaduto; per genitori e insegnanti risulta così difficile individuare il problema. Spesso il silenzio è ciò che permette al bullismo di perpetrarsi.

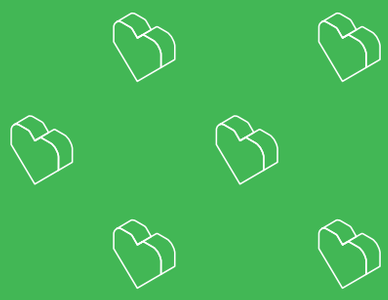
L'insegnante, direttamente e indirettamente, deve rassicurare e spronare i ragazzi a denunciare gli episodi di cyberbullismo. In ogni scuola si dovrebbero elaborare delle linee guida condivise che aiutino i docenti a riconoscere episodi di cyberbullismo, e che prevedano procedure standardizzate da adottare una volta individuato il problema. E' consigliabile prestare una maggiore attenzione a piccoli cambiamenti che possono avvenire nei comportamenti dei ragazzi, così da accorgersi se qualcosa li turba.

Secondo l'art. 361 C.P. gli insegnanti possono incorrere in una multa da 30 a 516 Euro se omettono o ritardano di denunciare alle autorità competenti un reato di cui ha avuto notizia nell'esercizio o a causa delle sue funzioni.

I ragazzi dovrebbero essere messi a conoscenze delle **conseguenze**, anche penali, che un atto di cyberbullismo può comportare.
Quando si scoprono casi di cyberbullismo andrebbero immediatamente avvisati i genitori, della vittima e del responsabile dell'episodio e, nelle situazioni più gravi anche gli organi di polizia.

Le vittime vanno sostenute completamente e ascoltate, poiché raccontare l'accaduto non sempre è facile e richiede tempo. Spesso la vittima non riesce ad aprirsi con una figura come quella del docente. I compagni di classe andrebbero coinvolti nella ricerca di una soluzione al problema. Allo stesso tempo anche il responsabile dell'atto di cyberbullismo va aiutato. Sospensioni o punizioni potrebbero ottenere l'effetto contrario, con ripercussioni negative immediate sulla vittima.

Per la Legge n. 71, in caso di episodi di cyberbullismo, è applicabile la procedura di ammonimento del minore da parte del questore.



Secondo l'art. 7 della legge 29 Maggio 2017 n. 71 "fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati [...] commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento [...]. Ai fini dell'ammonimento, il questore convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale. Gli effetti dell'ammonimento di cui al comma 1 cessano al compimento della maggiore età.

Un lavoro di gruppo in classe, che coinvolga bullo, vittima e testimoni può aiutare a risolvere il problema.
Parlare con i ragazzi e fare prevenzione resta la strada migliore da percorrere, e occorre farlo usando il loro linguaggio. Bisogna trasmettere ai più giovani l'importanza di creare relazioni positive con gli altri, basate sul confronto, la fiducia e l'accettazione delle differenze.

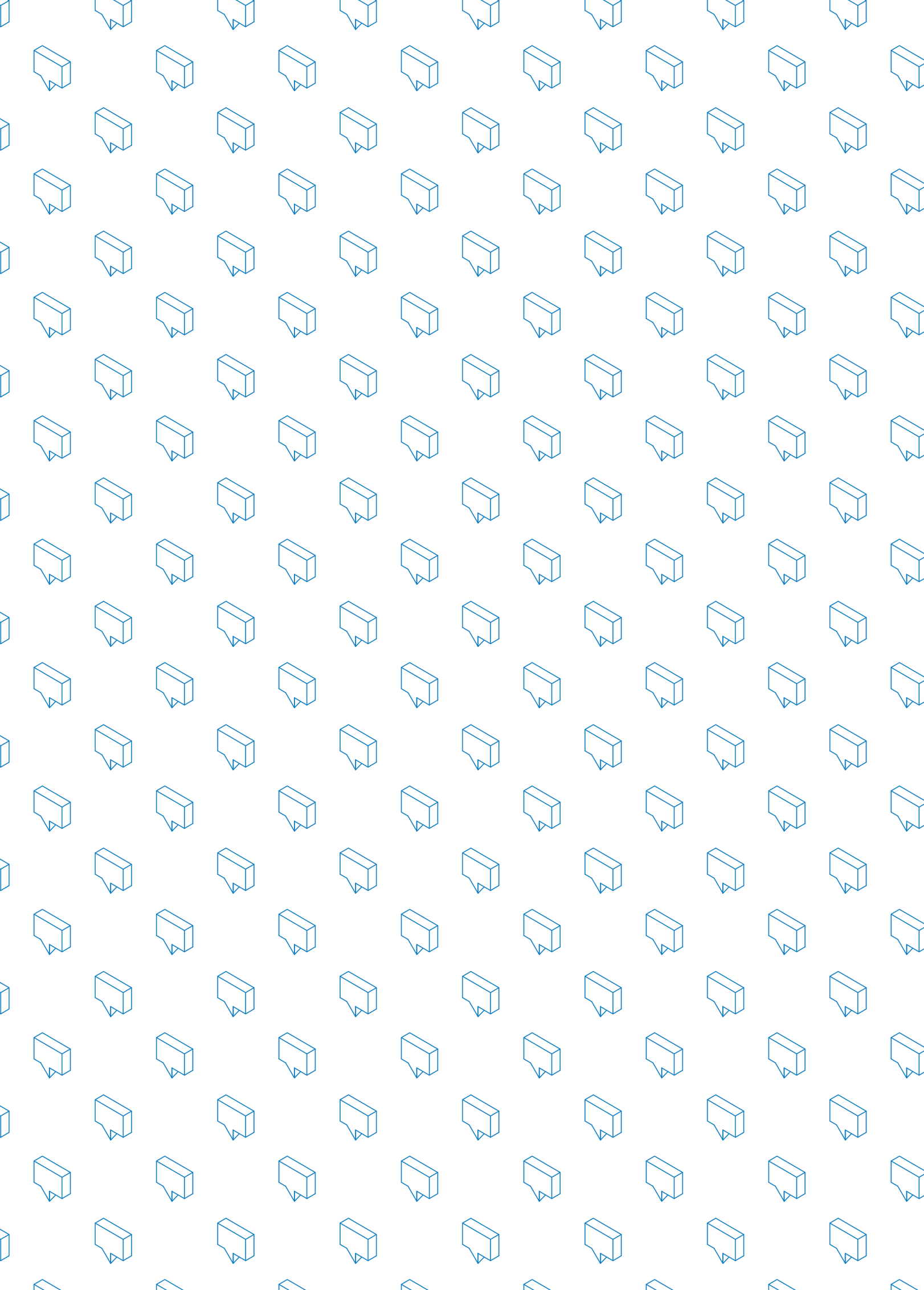
4.5 Reagire al cyberbullismo: sii gentile

E' sempre bene ricordare che il comportamento degli adulti può influenzare quello dei più giovani. Molto spesso i bulli stanno solo imitando comportamenti aggressivi che hanno visto in televisione, al cinema o a casa. In età adolescenziale si passa dall'infanzia all'età adulta, e questo passaggio avviene oggi per lo più in Rete, dove i giovani costruiscono la loro socialità e la loro identità.
E' quindi anche in Rete che si innescano comportamenti virtuosi e sani, così come quelli negativi.

Questo avviene in quanto spesso i ragazzi imitano adulti che umiliano o si rivolgono con prepotenza nei confronti di altri adulti, a scuola o a casa, talvolta perché sono stati loro stessi vittime di tale trattamento.

Il bullismo è un fenomeno sociale. Se un ragazzo compie atti di bullismo la colpa non è di un singolo individuo, ma è l'intero sistema familiare ed educativo ad aver fallito.
E' responsabilità e onere di tutti di farsene carico ed intervenire. Genitori e insegnanti hanno l'opportunità di dare il buon esempio, di insegnare ai ragazzi che la diversità è un valore e che i contrasti e le discussioni possono e devono esserci, ma vanno risolti in modo sereno e con gli strumenti appropriati, anche online.

(per le attività vedi Allegato 4 – disponibile sul sito https://vivinternet.azzurro.it/)



5.

Nel dubbio, parlane

L'impatto del digitale ha trasformato **la struttura delle relazioni interpersonali** da molteplici punti di vista, così come ha contribuito a determinare una nuova costruzione dell'identità personale degli adolescenti e modificare le modalità comunicative tradizionali. Tutto ciò pone come prioritaria la necessità di modulare nuovi approcci agli effetti che la realtà digitale può produrre.

Quando i nostri ragazzi si trovano ad affrontare una situazione complicata, di difficile gestione, che gli crea imbarazzo o addirittura paura, dovrebbero avere la serenità e la tranquillità di confidarsi con un adulto di fiducia. Non è semplice trovare la forza per farlo ma il ruolo giocato dagli adulti, in questo contesto, è fondamentale.
A volte, tuttavia, può capitare che gli stessi adulti - genitori e insegnanti in primis- abbiano la necessità di confrontarsi su situazioni di disagio e/o pericolo in cui si trovano i ragazzi al fine di essere orientati verso modalità di gestione efficace del problema; o ancora che i ragazzi stessi preferiscano confidarsi e chiedere aiuto a terzi proprio per il senso di vergogna e di imbarazzo.
La Helpline di Telefono Azzurro nasce proprio con l'obiettivo di fornire un aiuto competente e riservato a bambini, adolescenti e adulti. E' un Servizio gratuito e sicuro, uno spazio per chattare o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle tecnologie digitali e alla sicurezza online, da parte delle nuove generazioni.

5.1 La rete: uno spazio per scrivere insieme una nuova grammatica delle relazioni

Un errore, che spesso gli adulti commettono, è considerare Internet e tutti i suoi ambiti - siti, chat, app, messaggistica istantanea - un "mondo altro" rispetto a quello in cui trascorriamo la nostra giornata.
Una realtà con cui interagire per motivi di lavoro, magari anche di divertimento, ma raramente un contesto all'interno del quale crescere, esprimere la propria personalità, maturare esperienze.

Nasce anche da questo gap iniziale la difficoltà che oggi gli adulti incontrano nel comprendere atteggiamenti, approccio e mentalità di coloro - bambini e adolescenti - che all'interno di questo nuovo mondo non solo sono nati e cresciuti, ma che contribuiscono quotidianamente ad alimentare, plasmare e far crescere.

Il digitale ha introdotto, con un'accelerazione che non ha precedenti rispetto a questo tipo di processi, un cambiamento antropologico, psicologico e sociale di fronte al quale ci troviamo tutti impreparati: ha aperto frontiere e innescato sfide enormi rispetto alle quali non abbiamo ancora strumenti consolidati.

Sfide che riguardano soprattutto il rapporto con l'altro, con gli altri, e in particolare tutta la gamma di rapporti intergenerazionali attraverso i quali da sempre si strutturano i processi educativi, parentali, scolastici e formativi.

Registri comunicativi

Riuscire a parlare la lingua dei ragazzi per un adulto/educatore non è una sfida semplice. Il registro comunicativo dei ragazzi e le loro priorità non sono di facile comprensione, ma questo sforzo va compiuto allo scopo di **accrescere l'empatia** verso i loro problemi e disagi. Il linguaggio utilizzato, così come gli esempi che si propongono, il tono comprensivo e mai perentorio, daranno ai ragazzi e all'intera classe, la percezione che l'adulto comprenda davvero la loro situazione e il loro disagio.

Impostare, ad esempio, la discussione con i propri studenti chiedendo di rintracciare insieme le caratteristiche che differenziano lo scherzo dai fenomeni di bullismo può aiutarli a riconoscere alcuni stereotipi. La consapevolezza è la prima porta verso l'identificazione di un problema e dunque verso la conseguente e auspicata richiesta di aiuto.

Ancora un esempio. Una delle difficoltà più grandi che incontrano i ragazzi nel compiere la scelta di schierarsi a difesa della vittima è "la paura di fare la stessa fine". All'interno di ogni classe ci sono ragazzi più sensibili di altri ed è da loro che occorre partire per favorire una discussione allargata.

Quelle dei ragazzi sono paure reali e fornire istruzioni, dettare regole - o peggio ancora ammonire - non è affatto utile in questi casi. È importante, al contrario, che gli studenti abbiano la possibilità di confrontarsi fra loro per cercare soluzioni e strategie adeguate e condivise. In questo senso il ruolo fondamentale dell'insegnante è facilitare la discussione condivisa, dando spazio alle opinioni di tutti, cercando di immedesimarsi e fornendo spunti di riflessione.

L'importanza dell'empatia

Creare e accrescere l'empatia negli studenti è un compito fondamentale degli adulti/educatori. Significa cercare di ridurre la lontananza percepita dai ragazzi rispetto alle loro problematiche, così come agli ambienti in cui si muovono, Internet su tutti.

I ragazzi spesso ci sentono lontani e incapaci di poter comprendere i loro disagi, o le situazioni che stanno vivendo. Condividere esempi e storie con i ragazzi può essere un buon modo di dimostrare loro la vostra vicinanza e la vostra capacità di comprendere situazioni spiacevoli che in Rete possono essere capitate a chiunque, anche a voi o ai vostri conoscenti.

5.2 In Rete anche gli adulti sono fragili

In questo senso, un aspetto che va ricordato e condiviso con i ragazzi riguarda la fragilità a cui tutti indistintamente - adulti, ragazzi e bambini - siamo esposti quando navighiamo in Rete. Truffe, frodi online, phishing, perdita di dati, violazione della propria privacy, sono fenomeni che quotidianamente coinvolgono gli adulti quanto i ragazzi più giovani.
Molto spesso è la mancanza di strumenti adeguati e quindi, conseguentemente, una **scarsa consapevolezza** del mezzo a generare questa tipologia di inconvenienti. Quanto più gli adulti si dotano di mezzi di conoscenza sull'universo digitale e Internet, tanto più saranno in grado di condividere con i ragazzi buone pratiche e consigli.
E, come si diceva, la condivisione di esempi con i ragazzi di piccole situazioni spiacevoli capitate a se stessi o ad altri adulti in Rete è uno strumento fondamentale per creare empatia e aumentare il livello di immedesimazione.

Adulti solidi: punti di riferimento per i giovani

Quando un adulto/educatore decide di mettersi in gioco avvicinandosi alle problematiche dei ragazzi non deve mai dimenticare che l'intento ultimo è rassicurarli e far loro comprendere che l'esperienza pregressa di un adulto di cui si fidano rende più probabile che lo stesso sia in grado di raccogliere una loro confidenza, così come aiutarli a trovare una soluzione. Trasmettere solidità, fermezza, capacità di risolvere anche le situazioni apparentemente più complesse è altrettanto importante che creare empatia. Il concetto da trasmettere ai ragazzi è che gli adulti non sono giudici infallibili e che anzi sono spesso essi stessi vittime dei tranelli - grandi e piccoli - presenti in Rete; ma che al tempo stesso abbiano l'esperienza e i mezzi per risolvere più efficacemente e velocemente i problemi e le situazioni spiacevoli di imbarazzo che possono generarsi in Rete.

Non è facile per i ragazzi prendere apertamente una posizione. La paura e la confusione su quale sia l'atteggiamento corretto da tenere in circostanze spesso più grandi di loro è parte della loro crescita e formazione. È compito degli adulti e degli educatori far comprendere ai ragazzi, tramite esempi e racconti non necessariamente correlati ad un evento specifico, che vi sono delle situazioni che andrebbero biasimate apertamente e che mostrare vicinanza ed empatia è un atto di grande coraggio, e non di debolezza.

Anche nel caso in cui si provasse compassione o sgomento di fronte ad un racconto di cyberbullismo da parte di un ragazzo, occorrerebbe mostrare comunque fermezza e calma. Questo atteggiamento trasmetterà infatti ai ragazzi la certezza di aver fatto bene a confidarsi con un adulto e probabilmente gli farà percepire sin da subito che una soluzione è possibile.

5.3 Ruolo degli osservatori e dei testimoni

Gli spettatori o osservatori sono tutti quei bambini e ragazzi che assistono agli episodi di bullismo, o ne sono a conoscenza. Secondo una ricerca svolta in Italia da Telefono Azzurro e DoxaKids[4] nel 2016 su 600 studenti di diverse scuole secondarie di primo e secondo grado, di età compresa tra i 12 e i 18 anni, il 30% dei ragazzi italiani è vittima di bullismo online o offline (ovvero, è stato deriso o umiliato in Rete).
In particolare gli osservatori degli atti di cyberbullismo possono essere potenzialmente illimitati considerando che la diffusione è incontrollabile.
La mancanza di delimitazione dello spazio e del tempo è propria del fenomeno del cyberbullismo rispetto al bullismo tradizionale: non più solo classe, cortile o palestra in tempi circoscritti, bensì la vittima è raggiungibile potenzialmente in ogni momento della sua vita e ovunque essa si trovi, favorendo così l'insorgere della sensazione grave e totalizzante che nessun tempo e nessun luogo possano offrire una qualche forma di sicurezza e riparo.
Nella maggior parte dei casi gli spettatori o osservatori non denunciano gli episodi di cyberbullismo e non intervengono in qualche modo. Le ragioni che spingono i testimoni ad assistere senza intervenire possono essere diversi.
Pur non condividendo il comportamento del cyberbullo, ad esempio, temono di diventare a loro volta vittime del bullo.
In secondo luogo, potrebbero non comprendere la gravità dell'atto a cui stanno assistendo considerandolo alla stregua di uno scherzo e sottovalutando le conseguenze molto gravi che potrebbero insorgere. Oppure, infine, partecipano all'episodio in forma indiretta, ad esempio filmando l'episodio e condividendolo sui social.
La comprensione di queste possibili cause e della necessità di un processo rieducativo che coinvolga non solo i bulli, ma anche e soprattutto gli osservatori, è fondamentale per contrastare il silenzio. Il ruolo degli osservatori o testimoni è infatti fondamentale dal momento che possono favorire o frenare il dilagare delle prepotenze, per esempio difendendo la vittima e, anzitutto, chiedendo aiuto agli adulti.

Gli adulti/educatori hanno davanti a loro la sfida di sollecitare e supportare gli osservatori. La consapevolezza che di fronte ad atti di ingiustizia, violenza gratuita, o difficoltà di un conoscente o un compagno è giusto, oltre che moralmente necessario, prendere una posizione e fare il possibile affinché quel disagio abbia fine, è parte di un processo di formazione più ampio e di lungo termine. È un insegnamento che può passare dalla lettura di un libro in classe, a quella di articoli di giornale. Insegnare l'empatia e l'immedesimazione verso i disagi che un'altra persona sta vivendo è un processo che richiede tempo e un lavoro costante.

[4] Per un approfondimento si consiglia "Il tempo del web - Adolescenti e genitori online" - http://doitbetter.azzurro.it/wp-content/uploads/2016/02/Telefono-Azzurro-SID-2016_rev_pFS_DEF_3.pdf

Al contrario, biasimare atteggiamenti di reticenza non aiuterà i ragazzi a comprendere perché bisognerebbe agire diversamente: accusare infatti i testimoni di complicità allontanerà i ragazzi dal momento della consapevolezza. Chi ha taciuto da principio, o non si è schierato dalla parte giusta, infatti, avrà paura di essere additato e giudicato per sempre da adulti e coetanei.
Molto più produttivo sarebbe invece, ad esempio, dare ai ragazzi la possibilità di raccontare/denunciare, in modo anonimo e attraverso un mezzo a loro noto (es. numero Whatsapp), un atto di bullismo o cyberbullismo.

5.4 Dispositivi e minori

Quando si consente l'utilizzo di un dispositivo ad un bambino occorre sempre ricordare che non gli si fornisce insieme un libretto delle istruzioni; istruzioni che mancano sin dal principio anche a noi adulti il più delle volte.
In moltissimi casi poniamo con troppa leggerezza i dispositivi di ultima generazione nelle mani dei nostri ragazzi. I device di per sé non sono il nodo della questione - come non lo è la Rete - ma come qualsiasi mezzo potentissimo possono rappresentare al contempo una grande opportunità, ma anche un rischio concreto.

Occorre sempre ricordare che, in quanto adulti, siamo responsabili dell'uso passivo e poco consapevole che fanno i nostri ragazzi dei dispositivi che mettiamo loro a disposizione, ma anche legalmente responsabili - nel caso di genitori o tutori legali - delle azioni e delle conseguenze che possono scaturire da un loro utilizzo scorretto. È, quindi, uno specifico dovere morale e legale - nel caso di genitori e tutori - seguire i minori nell'utilizzo dei dispositivi, sia in fase di navigazione in Rete, che per l'uso e l'abuso che dei dispositivi stessi talvolta fanno i nostri ragazzi.

Le buone regole per accrescere la consapevolezza

E' fondamentale- sia come adulti/genitori che come educatori - tenere a mente alcune **buone regole**.
Prima di tutto è bene aver presente che i ragazzi apprendono e si formano anche semplicemente osservandoci: è dovere degli adulti/educatori impegnarsi per primi ad adottare condotte corrette per un utilizzo del digitale sicuro e consapevole.

In secondo luogo è opportuno creare un rapporto con i ragazzi basato sulla fiducia reciproca, sul confronto e sulla condivisione. E' importante che gli adulti di riferimento siano una guida per i ragazzi anche in questo ambito. Soprattutto in riferimento a genitori o tutori legali: non avere contezza di quante e quali applicazioni siano installate sui dispositivi dei nostri ragazzi non è una buona pratica. Questo non significa, però, che spiare o carpire informazioni sui nostri ragazzi con l'inganno sia consigliato: occorre invece spronare i ragazzi a comprendere fino in fondo come funziona il device che gli viene affidato e le sue applicazioni.
E, soprattutto, trovare momenti per discuterne insieme in uno scambio costruttivo tra adulti e minori.

I ragazzi vanno accompagnati all'utilizzo dei dispositivi con regole che occorre sempre condividere, spiegare e contestualizzare, e mai semplicemente imporre.
I divieti servono a poco e spesso sortiscono effetti contrari.

Ancora, buone pratiche risultano essere: approfondire in ambito scolastico con letture, seminari, workshop etc. le tematiche che ruotano intorno ai media digitali (social network, messaggistica istantanea, gruppi etc.); sottoporre continuamente i ragazzi, in maniera diretta e indiretta, ad esempi di atteggiamenti scorretti che si verificano in Rete e promuovere la gentilezza nei modi e nelle azioni verso chiunque; spronare, infine, i ragazzi a frequentare corsi sul coding - sia in ambito scolastico che extrascolastico.
Questo non farà passare loro più tempo davanti alle app e ai videogiochi, ma farà venire loro voglia di programmare da sé un videogioco o una nuova app, passando così da un utilizzo inconsapevole e passivo a un utilizzo attivo e consapevole della tecnologia.

Seguire, da ultimo, le attività dei nostri ragazzi sui social network per capire in che modo si relazionano con gli altri e quale impronta digitale stanno lasciando in Rete è importante: comprendere quale atteggiamento tengono in Rete più aiutarci, direttamente o indirettamente, a suggerire azioni di correzione. Questa attività tuttavia - è bene ribadirlo - non va fatta di nascosto, ma deve essere condivisa con i ragazzi e dovrebbe basarsi su un rapporto di mutua fiducia tra adulti e ragazzi. Seguire i loro profili pubblici può inoltre fornire preziosi campanelli d'allarme che denotano possibili situazioni di disagio.

Da parte degli educatori, inoltre, potrebbe essere molto produttivo dedicare un paio d'ore a trimestre per discutere con i ragazzi delle novità che la Rete offre e delle evoluzioni delle applicazioni più diffuse: questo servirà, da un lato, a tenere aggiornati gli insegnanti - in un'ottica di condivisione di know how ragazzi/insegnanti - dall'altro, darà ai ragazzi la percezione di vicinanza degli insegnanti a tematiche per loro estremamente interessanti.

Infine è bene ricordare che il Telefono Azzurro può fornire in questi casi un aiuto competente sia a ragazzi che adulti.

(per le attività vedi Allegato 5 – disponibile sul sito https://vivinternet.azzurro.it/)

ALTROCONSUMO

Google

Vivi Internet, al meglio.