REGIONE LAZIO

USR LAZIO
Ufficio Scolastico Regionale

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

ACL

A SCUOLA CONNESSI

Per le scuole della **Regione Lazio**

NAVIGHIAMO IN SICUREZZA.

COESIONE ITALIA 21-27

Cofinanziato dall'Unione europea

REPVBBLICA ITALIANA

REGIONE LAZIO

Introduzione

Comunicazioni più facili ed immediate, tante informazioni a disposizione per lo studio, il lavoro, gli hobby, servizi per lo scambio di contenuti, per le nostre interazioni sociali, per i nostri acquisti.. Internet è questo e tanto altro: viviamo ormai completamente e continuamente connessi.

“Siamo” nel mondo reale così come “siamo” nel mondo digitale - il mondo online influisce direttamente sulle nostre vite reali e viceversa.
La nostra identità e le nostre azioni nel mondo reale hanno i loro corrispettivi nel mondo digitale.
È quindi fondamentale conoscere cosa sia la nostra “identità digitale” e come comportarsi nel mondo digitale per sfruttare al meglio le opportunità che ne derivano, in piena sicurezza.

Le informazioni e i contenuti che riguardano la nostra persona e che utilizziamo o pubblichiamo navigando sul web ci rendono veri e propri “cittadini digitali”, in un mondo virtuale in cui valgono gli stessi principi di convivenza che regolano la società reale.

Il mondo digitale offre tante opportunità grazie a nuovi strumenti e tecnologie, dobbiamo saperli sfruttare.

Addentriamoci allora in questo piccolo approfondimento, per scoprire insieme come vivere al meglio e in sicurezza le opportunità che nascono dall’ interazione tra mondo reale e mondo digitale.

1 Protezione dell'identità digitale

1.1 Proteggi sempre le tue identità digitali

Dovremmo cercare di proteggere sempre le informazioni personali ogni volta che comunichiamo o pubblichiamo contenuti sul web. Per fare in modo che i nostri dati siano protetti, è importante utilizzare i propri account in maniera sicura, impostando password difficili e sempre diverse.

Proteggi le tue informazioni personali e i tuoi account utilizzando password difficili e sempre diverse.

Non fornire informazioni e dati personali se non necessario.

Non fornire dati di pagamento se non sei sicuro del servizio che stai acquistando.

1.2 Fornisci solo le informazioni strettamente necessarie

Dovremmo evitare di fornire informazioni personali per l'attivazione di servizi o account su canali non verificati e condividere solo le informazioni strettamente necessarie. Per esempio, occorre prestare attenzione all'utilizzo di servizi che richiedono un pagamento, evitando di inserire i dati delle carte di credito.

1.3 Utilizza le e-mail in modo consapevole

Per evitare truffe e spam dovremmo prestare attenzione a come e con chi condividiamo il nostro indirizzo e-mail. Per esempio, potrebbe essere utile utilizzare più di un indirizzo e-mail per iscriversi a differenti servizi e dotarsi di strumenti antispam.

Condividi il tuo indirizzo e-mail personale solo con persone che conosci.

Utilizza un secondo indirizzo e-mail per iscriverti a social, piattaforme e servizi.

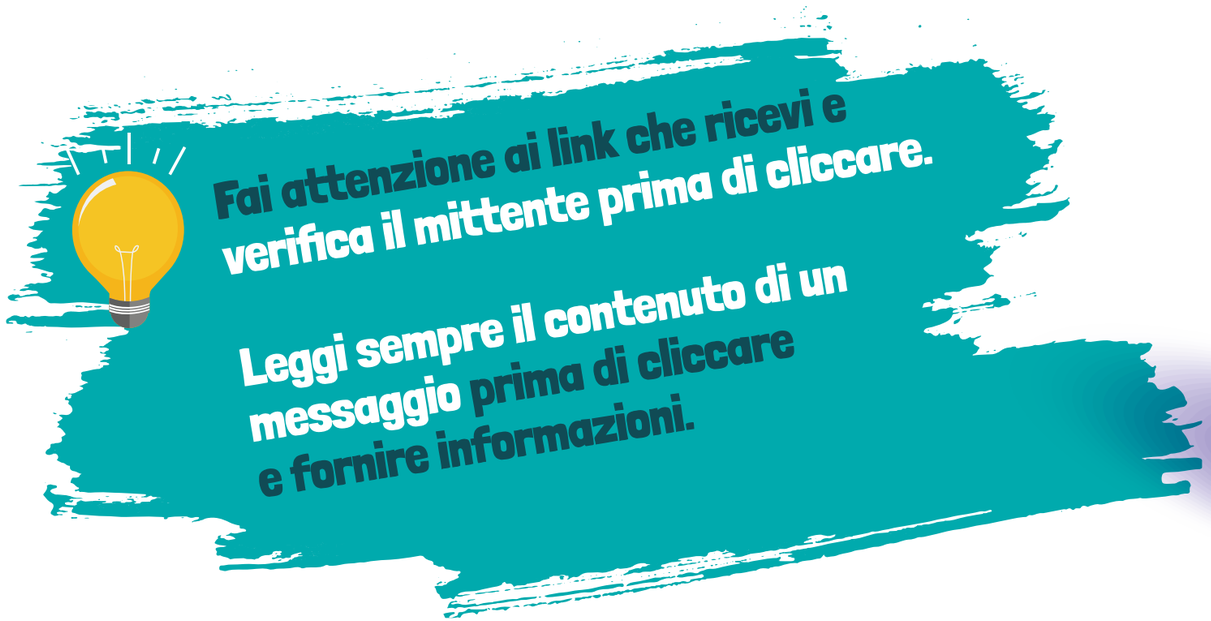
Proteggi le informazioni e i contenuti sui tuoi dispositivi utilizzando antivirus, firewall e password sicure.

1.4 Proteggi sempre i tuoi dispositivi

PC, mobile e tablet contengono quasi sempre informazioni e contenuti di carattere personale e intimo. È necessario quindi proteggere anche i nostri dispositivi da eventuali intrusioni, utilizzando un valido antivirus, firewall, password sicure ed eventualmente protocolli crittografici.

1.5 Fai sempre attenzione ai click

Siamo sempre sicuri di conoscere il mittente delle comunicazioni e dei messaggi che riceviamo? Sempre più spesso truffatori e hacker fingono di essere nostri conoscenti o istituzioni (come, ad esempio, banche) per spingerci a cliccare su un link pericoloso o a condividere informazioni personali come password o numero di carta di credito. Alcune truffe più comuni riguardano pubblicità, collegamenti relativi a giochi o vincite di denaro, viaggi e premi.
Prima di cliccare, è sempre consigliabile verificare l'affidabilità dei contenuti con cui interagiamo.



Fai attenzione ai link che ricevi e verifica il mittente prima di cliccare.

Leggi sempre il contenuto di un messaggio prima di cliccare e fornire informazioni.

2 Cittadinanza digitale consapevole

2.1 Tutto ciò che viene condiviso online è pubblico

Non esiste il “mio” profilo, la “mia” bacheca, la “mia” chat, il “mio” canale, il “mio” account Instagram, il “mio” spazio web, il “mio” blog. Tutto ciò che condividiamo è potenzialmente pubblico. Profili privati e gruppi chiusi non garantiscono necessariamente la nostra privacy.
Tag, screenshot e riproduzioni da parte di contatti o follower possono rendere pubbliche le nostre informazioni personali anche senza il nostro consenso. Occorre quindi riflettere bene su quali contenuti condividere online.

Ogni volta che condividi in chat o sui social testi, immagini o video ricordati che potrebbero essere ripubblicati da qualcun altro.

Tutto ciò che succede online può diventare di dominio pubblico, non solo foto e immagini, ma anche insulti, offese e conversazioni.

Segnala e blocca contenuti non appropriati o persone che utilizzano atteggiamenti aggressivi e offensivi.

2.2 Tutto ciò che viene condiviso online è amplificato

“Amplificato” significa poter raggiungere tantissime persone e tantissimi luoghi in pochissimo tempo. Da una classe o da un piccolo gruppo, una informazione può raggiungere tutto il mondo. Ad esempio, una foto privata, un insulto o uno scherzo offensivo possono facilmente diventare virali, raggiungendo un grande numero di persone. E se fossi proprio io la vittima di tutto questo? Oltre a prestare attenzione a ciò che pubblichiamo, diventa anche importante segnalare la presenza online di informazioni private di nostri conoscenti o di contenuti non appropriati.

2.3 Tutto ciò che viene condiviso online rimane per sempre

Le informazioni che abbiamo condiviso in rete sfuggono al nostro controllo. Diventa difficile dopo la pubblicazione eliminare ciò che abbiamo postato o inviato. L'unico modo per evitare di tornare sui nostri passi è quello di essere sempre sicuri di ciò che stiamo condividendo.

Ricordati che eliminare definitivamente un contenuto, dopo che è stato pubblicato, può risultare a volte molto difficile.

Rifletti sempre prima di imitare atteggiamenti che ritieni pericolosi, violenti o offensivi, anche se promossi da influencer o comunità popolari.

2.4 Non è sempre oro ciò che è virale

Popolarità e viralità non sempre hanno conseguenze positive. Influencer o persone molto popolari hanno maggiori difficoltà a proteggere la propria vita privata in quanto ogni informazione che condividono diventa quasi immediatamente di dominio pubblico. Inoltre, non sempre ciò che è virale deve essere imitato. Ad esempio, challenge o comportamenti violenti possono diventare popolari mettendo a rischio noi stessi e le altre persone.

2.5 Occorre proteggere la privacy propria e altrui

Oltre a tutelare la propria privacy, risulta fondamentale rispettare quella altrui. Dovremmo selezionare adeguatamente le informazioni e i contenuti personali da condividere e verificare in che modo questi vengono trattati. Una buona norma consiste nell'aggiornare e verificare frequentemente le impostazioni privacy dei canali web o social network utilizzati. Infatti, anche i dati generici come nome, cognome e indirizzo possono essere correlati con altre tipologie di dato, mettendo a rischio informazioni riservate relative alla nostra identità digitale. Allo stesso modo, dovremmo prestare attenzione a non invadere la privacy degli altri, evitando di condividere dati personali altrui senza aver ricevuto un consenso esplicito e segnalando eventuali abusi. La creazione di profili falsi con immagini appartenenti a un'altra persona può, in alcuni casi, costituire un reato.

Fai attenzione alle informazioni che riguardano te, i tuoi amici e la tua famiglia: non condividerle mai con persone sconosciute.

Mantieni le distanze da persone che hai conosciuto online e di cui non conosci la vera identità.

2.6 La diffidenza online è una virtù

Nell'ambiente digitale, la diffidenza può essere una virtù. Frequentando nuove comunità online e comunicando con persone non conosciute, è sempre opportuno essere prudenti. Alcune precauzioni come evitare di mostrare sé stessi o la propria abitazione in video, verificare l'identità del nostro interlocutore imparando a riconoscere i profili fake, ed evitare di fornire dettagli su sé stessi, costituiscono una prima linea di difesa. Essere prudenti significa, infine, fare attenzione a come la nostra vita quotidiana può essere influenzata dai rapporti che nascono online. Ad esempio, è sempre sconsigliabile incontrare di persona qualcuno di cui non conosciamo con certezza l'identità o compiere azioni pericolose seguendo le indicazioni di persone sconosciute.

2.7 Attenzione ai leoni da tastiera

Mascherarsi dietro a uno schermo può dare una falsa sensazione di sicurezza. Risulta molto più facile insultare o aggredire qualcuno digitando su una tastiera piuttosto che di persona. Se da un lato è opportuno evitare di assumere atteggiamenti violenti facendo attenzione al linguaggio utilizzato da noi e dai gruppi che frequentiamo, dall'altro è anche necessario sapersi difendere in caso di aggressione.

Mantieni sempre comportamenti rispettosi e non violenti

Impara a difenderti da chi usa un linguaggio violento o offensivo

3 Uso consapevole di strumenti e tecnologie

3.1 Social Network e gaming, fanne un uso sano

Le piattaforme di socializzazione sono parte della nostra vita quotidiana e non rappresentano di per sé un rischio, a patto che vengano utilizzate consapevolmente. L'utilizzo eccessivo o sproporzionato di social e videogiochi può avere degli impatti significativi sulla nostra vita e sulle nostre relazioni. Gli effetti negativi potrebbero riguardare non solo la nostra privacy ma anche la nostra sensibilità e il nostro benessere psicologico.

Impara a regolare il tempo che trascorri tra social network e videogiochi online.

Utilizza applicazioni di messaggistica sicure e protette

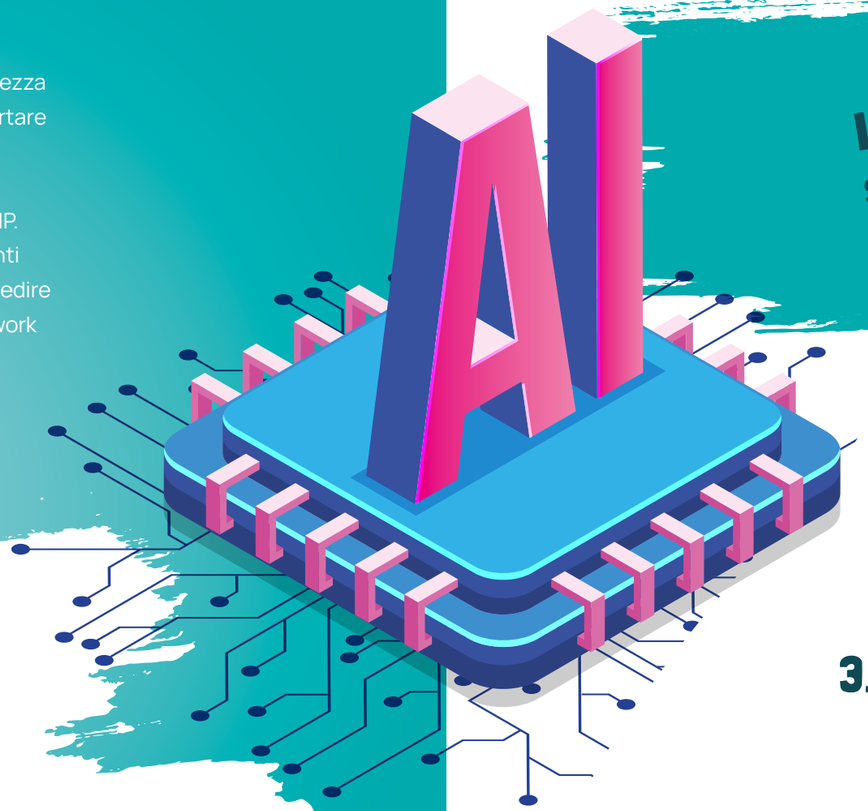
3.2 Strumenti e applicazioni di messaggistica, occhio ai dati

L'utilizzo di e-mail e chat risulta imprescindibile durante le nostre comunicazioni di tutti i giorni. Capita molto spesso di condividere contenuti personali o intimi. Proprio per questa ragione è sempre consigliabile informarsi su come gli strumenti che utilizziamo garantiscono la protezione dei nostri dati mediante, per esempio, l'utilizzo di crittografia e anonimizzazione.

3.3 Navigazione sicura

Non sempre possiamo conoscere con certezza il livello di sicurezza degli ambienti web durante la navigazione. Questo può comportare di incorrere inconsapevolmente in metodi di profilazione non espliciti come, ad esempio, il salvataggio di cookies e il tracciamento della nostra localizzazione e del nostro indirizzo IP. Durante la navigazione web possiamo utilizzare alcuni strumenti per mascherare il nostro indirizzo IP, la nostra posizione ed impedire il salvataggio di cookies come, ad esempio, Virtual Private Network (VPN), fake GPS app e navigazione privata.

Proteggi i tuoi dati durante la navigazione web utilizzando navigazione privata e disattivando la localizzazione



L'intelligenza artificiale è uno strumento molto utile, ma non sempre dà le risposte giuste.

3.4 Intelligenza Artificiale

I recenti modelli di intelligenza artificiale per la generazione di testi, immagini o video rappresentano uno strumento di forte innovazione sia nell'ambito lavorativo sia in quello scolastico, facilitando notevolmente l'elaborazione di contenuti. Tuttavia, ancora una volta, dovremmo prestare attenzione durante il loro utilizzo: da un lato i contenuti prodotti dall'AI non sempre risultano attendibili; dall'altro difficilmente i modelli di AI rappresentano un vero supporto senza avere una conoscenza pregressa delle tematiche ad essi sottoposte.

3.5 Fake news/Deep fake

Grazie all'utilizzo delle AI, è possibile creare facilmente contenuti multimediali, come video e foto, con un elevato grado di accuratezza. L'utilizzo di questi strumenti consente quindi di produrre delle imitazioni o degli elementi apparentemente realistici difficilmente riconoscibili a un primo sguardo. Ad oggi i contenuti fake creati mediante l'AI vengono condivisi quotidianamente tramite social e sul web. Dovremmo, quindi, imparare a distinguere le vere informazioni da quelle false, analizzando i contenuti consultati al fine di riconoscere fake news e deep fake.

Fai attenzione alle immagini, ai video e alle notizie false: confronta sempre le notizie che leggi con quelle fornite da fonti attendibili come giornali e quotidiani ufficiali.

Impatti sulla salute

L'utilizzo eccessivo o inadeguato di social network e, in generale, del web e di tecnologie per la comunicazione, può comportare alcuni rischi per la nostra salute come disturbi fisici e psicologici.

I rischi fisiologici derivano per lo più dall'utilizzo prolungato dei dispositivi come PC e cellulari e dalla conseguente esposizione ai campi elettromagnetici. Possiamo prevenirli, ad esempio, utilizzando gli auricolari per le telefonate oppure spegnendo o posizionando il cellulare lontano dal cuscino durante la notte.

I rischi psicologici che derivano sempre dall'utilizzo eccessivo di internet e dei social possono sfociare nello sviluppo di vere e proprie dipendenze, aumentando, per esempio, i livelli di insonnia, ansia e deconcentrazione. Possiamo prevenirli, ad esempio, dandoci un limite temporale giornaliero da rispettare per l'utilizzo di internet e social. Infine, un'altra importante conseguenza psicologica ed emotiva riguarda le vittime di comportamenti violenti o offensivi durante l'utilizzo di chat e social network. L'impatto psicologico derivante da questo tipo di trauma può essere molto difficile da superare.

Evitare esposizioni prolungate ai dispositivi e al web aiuta a prevenire potenziali problemi di salute e dipendenze psicologiche

Utilizza gli auricolari durante le telefonate e tieni lontano il cellulare lontano dal cuscino durante la notte

Le offese e la violenza sul web hanno le stesse conseguenze psicologiche che avrebbero nella vita reale

A chi rivolgersi

Quando navighiamo in internet, possiamo trovarci dinanzi a delle situazioni poco piacevoli e che ci spaventano.

Non bisogna vergognarsi, ma è importante parlarne e chiedere aiuto per tutelarci ad amici, insegnanti, alla propria famiglia, o alla Helpline istituita dal Telefono Azzurro. In caso di gravi violazioni è possibile contattare anche la Polizia Postale. Può anche capitare che un nostro compagno si trovi in una condizione di particolare disagio legata all'uso di internet. In questo caso, bisogna essere comprensivi e ascoltare il proprio compagno per aiutarlo, ma coinvolgere comunque degli adulti per gestire al meglio la situazione.

Se sul web vedi qualcosa che ti turba, ti spaventa o ti provoca disagio, parlane con i tuoi amici, i tuoi insegnanti o con la tua famiglia. Parlarne ti aiuterà a trovare una soluzione e a superare le tue paure.

In caso di situazioni di disagio o pericolo contatta la Helpline del Telefono Azzurro (1.96.96), o, in caso di gravi violazioni, contatta la Polizia Postale.

Se un compagno si trova in una situazione di difficoltà sul web, aiutalo: ascoltalo e poi coinvolgi gli adulti.

Consulta altre iniziative utili

Academy_Road to Cybersecurity
https://www.netgroup.it/en/academy/

Educazione Digitale
https://www.posteitaliane.it/it/educazione-digitale.html

INTERconNETtiamoci... ma con la testa!
www.facebook.com/interconnettiamoci

ITU Guidelines for children on Child Online Protection COP
https://www.itu-cop-guidelines.com/children

ITU Guidelines for parents and educators on Child Online Protection COP
https://www.itu-cop-guidelines.com/parentsandeducators

Manuale di prevenzione e primo soccorso per nativi digitali. Guida alle trappole e ai pericoli del mondo virtuale
https://www.digiacademy.it/nasce-young-cyber-security-academy

Modello di awareness interattivo
https://checkme.cyberiskvision.com/

Polizia Postale
https://www.commissariatodips.it/consigli/per-i-cittadini-e-i-ragazzi/consigli-contro-il-cyberbullismo-per-ragazzi/index.html

Progetto Generazioni Connesse
https://www.generazioniconnesse.it/site/it/le-tematiche/

cyber40.it

Roma, gennaio 2024