L2D

MEDIA LITERACY COMPETENCES
FOR YOUTH WORKERS

LINEE GUIDA PER UN USO SICURO ONLINE

MODULO SICUREZZA ONLINE

Titolo:	LINEE GUIDA PER UN COMPORTAMENTO SICURO ONLINE
Parole chiave :	Sicurezza online, Sicurezza Internet, Privacy digitale, Sicurezza informatica, Pratiche online sicure, Protezione delle informazioni personali, Sicurezza dei dati, Gestione delle password, Minacce online, Segnalazione di abusi, Impostazioni sulla privacy
Preparato da .	
Lingua:	Italiano
Obiettivi:	● Definire la sicurezza online: spiegare il concetto di sicurezza online e la sua importanza nel mondo digitale di oggi. ● Identificare le minacce online: aiutare gli studenti a riconoscere varie minacce online come phishing, malware, furto di identità, cyberbullismo e truffe. ● Comprendere i problemi di privacy: educare i partecipanti sull'importanza della protezione delle informazioni personali online e sulle potenziali conseguenze delle violazioni della privacy. ● Sviluppare password complesse: insegna le tecniche per creare password complesse e univoche per migliorare la sicurezza dell'account. ● Proteggersi dai tentativi di phishing: fornisci strategie per rilevare ed evitare di cadere vittima di e-mail, messaggi e siti Web di phishing. ● Proteggere i profili dei social media: offrire linee guida per la regolazione delle impostazioni sulla privacy, il controllo della condivisione delle informazioni personali e la gestione delle richieste di amicizia. ● Promuovere una comunicazione online sicura: Insegna modi efficaci per comunicare in modo sicuro sui social media, sui forum e sulle piattaforme di messaggistica, sottolineando l'evitare di condividere dettagli sensibili. ● Sviluppare capacità di pensiero critico: promuovere la capacità di valutare le informazioni e le fonti in modo critico, in particolare nel contesto delle notizie false e della disinformazione online. ● Affrontare le molestie e lo stalking online: offrire indicazioni su come rispondere e segnalare i casi di molestie o stalking online.
Obiettivi formativi :	
Indice dei contenuti :	1. SICUREZZA SU INTERNET 1.1.DEFINIZIONE DI SICUREZZA IN INTERNET

	1.2.COMPRENDERE L'AMBITO DI APPLICAZIONE E L'IMPORTANZA 1.2.1. Ambito di applicazione della sicurezza in Internet 1.2.2. L'importanza della sicurezza su Internet 1.3.EVOLUZIONE DEI CONCETTI DI SICUREZZA SU INTERNET 1.4.Componenti chiave di un'esperienza online sicura 2. MINACCE ONLINE 2.1.TIPI DI MINACCE ONLINE 2.2.RICONOSCERE I SEGNALI DI AVVERTIMENTO 2.3.CONSEGUENZE DELL'IGNORARE LE MINACCE ONLINE 3. SALVAGUARDIA DELLE INFORMAZIONI PERSONALI 3.1. IMPORTANZA DELLA PROTEZIONE DELLA PRIVACY 3.2.GESTIONE SICURA DELL'ACCOUNT ONLINE 3.3.CONDIVISIONE RESPONSABILE SUI SOCIAL MEDIA 4. NAVIGARE SUI SOCIAL MEDIA IN MODO SICURO 4.1.REGOLAZIONE DELLE IMPOSTAZIONI SULLA PRIVACY 4.2.GESTIONE DELLE RICHIESTE DI AMICIZIA E DEI MESSAGGI 4.3.SEGNALAZIONE E BLOCCO DI ACCOUNT ABUSIVI 5. SICUREZZA INFORMATICA E DISPOSITIVI MOBILI 5.1.PROTEZIONE DI SMARTPHONE E TABLET 5.2.AUTORIZZAZIONI DELL'APP E ACCESSO AI DATI

	5.3.PROTEZIONE DEI DISPOSITIVI MOBILI DA FURTI E SMARRIMENTI
Sviluppo dei contenuti:	1. SICUREZZA SU INTERNET 1.1. DEFINIZIONE DI SICUREZZA IN INTERNET La sicurezza su Internet, nota anche come sicurezza online, è la pratica di aderire a linee guida attuabili, acquisire una comprensione completa della tecnologia moderna e salvaguardare in modo proattivo i dispositivi digitali per difendersi dai vari aspetti dannosi del mondo online. Poiché il numero di utenti di Internet continua a crescere a livello globale, varie parti interessate, tra cui governi, organizzazioni e fornitori di servizi Internet, sono diventate sempre più preoccupate per la sicurezza delle popolazioni vulnerabili, come bambini, adolescenti e anziani, mentre entrano in contatto con il mondo virtuale. Statistiche allarmanti rivelano che oltre il 45% degli utenti di Internet ha riferito di aver subito una qualche forma di molestia informatica, sottolineando l'urgente necessità di promuovere pratiche online più sicure e di coltivare una cultura della responsabilità digitale. Per rispondere a queste pressanti preoccupazioni e sostenere un panorama digitale più sicuro, il Safer Internet Day viene celebrato su scala globale ogni febbraio. Questo evento annuale funge da piattaforma dedicata per aumentare la consapevolezza sulla sicurezza di Internet, incoraggiando gli individui e le comunità a essere vigili, informati e proattivi nelle loro interazioni online. I governi, le organizzazioni senza scopo di lucro e le aziende tecnologiche di tutto il mondo partecipano attivamente alle iniziative del Safer Internet Day, organizzando campagne di sensibilizzazione, workshop educativi ed eventi interattivi per fornire agli utenti di Internet le conoscenze e le competenze necessarie per navigare nel mondo online in modo sicuro. Nel Regno Unito, la campagna Get Safe Online è emersa come una risorsa importante nella promozione della sicurezza su Internet. Con la sponsorizzazione vitale dell'agenzia governativa Serious Organized Crime Agency (SOCA) e con la

	collaborazione con le principali società di Internet come Microsoft ed eBay, la campagna mira a fornire agli utenti di Internet una guida pratica e risorse per proteggersi dalle minacce informatiche. Attraverso informazioni, suggerimenti e strumenti facilmente accessibili, Get Safe Online si impegna a migliorare la resilienza digitale degli individui, rendendo la comunità Internet del Regno Unito più solida e meno suscettibile ai pericoli online. Poiché Internet continua a evolversi e a svolgere un ruolo sempre più importante nella nostra vita quotidiana, garantire la sicurezza di Internet diventa fondamentale. Promuovendo una cultura del comportamento online responsabile, sensibilizzando l'opinione pubblica attraverso iniziative come il Safer Internet Day e fornendo risorse accessibili come la campagna Get Safe Online, possiamo lavorare collettivamente per creare un ambiente digitale più sicuro e protetto per tutti. Nel nostro mondo sempre connesso, l'importanza della sicurezza su Internet è diventata fondamentale. Internet offre opportunità senza precedenti per l'apprendimento, la comunicazione e l'intrattenimento, ma espone anche gli utenti a potenziali rischi e pericoli. Man mano che la tecnologia avanza e le minacce online diventano più sofisticate, rimanere informati e proattivi sulla sicurezza di Internet è fondamentale per le persone di tutte le età. Per i bambini e gli adolescenti, che sono spesso nativi digitali, comprendere la sicurezza di Internet è essenziale per interazioni online responsabili e sicure. Genitori, educatori e tutori svolgono un ruolo fondamentale nel guidare i giovani utenti di Internet, insegnando loro i potenziali rischi della condivisione di informazioni personali, dell'interazione con estranei e della partecipazione ad attività online non sicure. Per migliorare la sicurezza di Internet, è fondamentale rimanere aggiornati sulle ultime tendenze e best practice in materia di sicurezza informatica. L'aggiornamento regolare di software e applicazioni, l'utilizzo di software antivirus affidabili e l'abilitazione degli aggiornamenti

automatici possono rafforzare la difesa dei dispositivi digitali dalle minacce emergenti. Inoltre, l'integrazione dell'autenticazione a più fattori, ove possibile, aggiunge un ulteriore livello di protezione agli account online.

Promuovere una comunità online positiva e sicura richiede anche di promuovere l'empatia e il rispetto digitali. Incoraggiare la gentilezza e l'empatia nelle interazioni online può contrastare il cyberbullismo e i comportamenti tossici, rendendo Internet uno spazio più accogliente per tutti.

1.2. COMPRENDERNE LA PORTATA E L'IMPORTANZA

1.2.1. Ambito di applicazione della sicurezza su Internet

- Protezione da minacce informatiche come virus, malware, phishing, ransomware e furto di identità.
- Salvaguardare le informazioni personali e l'identità digitale da accessi non autorizzati e uso improprio.
- Navigare sui social media in modo responsabile e affrontare il cyberbullismo o le molestie online.
- Garantire transazioni online sicure e proteggere le informazioni finanziarie durante gli acquisti o le operazioni bancarie online.
- Utilizzo e gestione sicura dei dispositivi mobili per evitare violazioni dei dati e della privacy.
- Riconoscere ed evitare truffe online, siti Web fraudolenti e tentativi di phishing.
- Insegnare a bambini e adolescenti la sicurezza online e aiutarli a sviluppare abitudini digitali responsabili.

1.2.2. Importanza della sicurezza su Internet

- Protezione delle informazioni personali e finanziarie: le misure di sicurezza su Internet salvaguardano i dati

sensibili, prevenendo il furto di identità e le frodi finanziarie.

- Mantenere la privacy e la reputazione digitale: essere consapevoli delle attività online aiuta le persone a preservare la propria privacy e proteggere la propria reputazione digitale.
- Salvaguardia dalle minacce informatiche: la consapevolezza dei rischi online e le seguenti pratiche di sicurezza difendono dalle minacce informatiche che possono interrompere la vita quotidiana, le operazioni aziendali o compromettere le informazioni sensibili.
- Potenziare le esperienze digitali positive: la sicurezza su Internet consente alle persone di vivere esperienze online positive e arricchenti senza timore di molestie o vittimizzazione.
- Promuovere la cittadinanza digitale: praticando la sicurezza su Internet, gli individui contribuiscono a costruire una comunità digitale responsabile e rispettosa.
- Impatto economico: gli incidenti di sicurezza informatica possono avere gravi conseguenze economiche per individui, aziende e governi, rendendo la sicurezza di Internet un aspetto essenziale della sicurezza generale.
- Proteggere i vulnerabili: la sicurezza su Internet è particolarmente importante per i bambini, gli adolescenti e le popolazioni vulnerabili che potrebbero essere più suscettibili ai pericoli online.

1.3. EVOLUZIONE DEI CONCETTI DI SICUREZZA SU INTERNET

L'"Evoluzione dei concetti di sicurezza su Internet" si riferisce a come la comprensione della sicurezza su Internet e le misure adottate per proteggere gli utenti dalle minacce online si sono evolute nel tempo. Con la crescita e la trasformazione di Internet, sono cresciute e si sono trasformate anche le sfide poste dalle minacce informatiche, che hanno portato allo sviluppo di nuovi concetti e strategie per garantire la sicurezza online. Questa sezione approfondisce il contesto storico e le tappe fondamentali che hanno plasmato le pratiche di sicurezza su Internet.

	• Internet agli albori: Agli albori di Internet, il concetto di sicurezza online era relativamente semplicistico. La maggior parte degli utenti erano individui o professionisti esperti di tecnologia che comprendevano i rischi associati alla condivisione di informazioni personali online. Tuttavia, c'era una scarsa consapevolezza tra il pubblico in generale sulle potenziali minacce informatiche. • Ascesa della comunicazione online: Con l'emergere delle piattaforme di comunicazione online e dei social media, la sicurezza su Internet ha assunto nuove dimensioni. Gli utenti hanno iniziato a condividere più informazioni personali, portando a maggiori preoccupazioni per la privacy e il furto di identità. Concetti come il phishing e le e-mail di spam hanno iniziato a guadagnare importanza quando i criminali informatici hanno cercato di sfruttare la fiducia degli utenti. • Misure di sicurezza informatica all'avanguardia: con il crescente panorama delle minacce, le misure di sicurezza informatica hanno iniziato a evolversi. I software antivirus, i firewall e le tecnologie di crittografia sono diventati strumenti essenziali per proteggersi da malware e accessi non autorizzati. Queste prime soluzioni di sicurezza informatica hanno gettato le basi per meccanismi di protezione più avanzati in futuro. • Campagne e iniziative di sensibilizzazione: Man mano che le minacce informatiche sono diventate più diffuse, varie organizzazioni, governi e aziende tecnologiche hanno iniziato a lanciare campagne e iniziative di sensibilizzazione per educare il pubblico sulla sicurezza di Internet. Questi sforzi miravano a sensibilizzare l'opinione pubblica sui rischi online più comuni e a incoraggiare gli utenti ad adottare pratiche online più sicure.

	• Crescenti preoccupazioni per il cyberbullismo: anche l'ascesa dei social media e della comunicazione online ha attirato l'attenzione sul problema del cyberbullismo. Con l'aumento degli episodi di molestie online e cyberbullismo, gli sforzi per la sicurezza su Internet si sono ampliati per affrontare questa forma di aggressione digitale e supportare le persone colpite. • Internet mobile e nuove sfide: l'avvento degli smartphone e dell'accesso a Internet mobile ha introdotto una nuova serie di sfide per la sicurezza di Internet. I rischi specifici associati ai dispositivi mobili, come le autorizzazioni delle app e il malware mobile, richiedevano misure di sicurezza su misura. • Progressi nell'autenticazione: poiché le password da sole si sono rivelate insufficienti per proteggere gli account online, l'autenticazione a due fattori (2FA) e l'autenticazione a più fattori (MFA) hanno guadagnato popolarità. Questi metodi hanno fornito un ulteriore livello di sicurezza, riducendo il rischio di accesso non autorizzato. • Enfasi sull'alfabetizzazione digitale: i concetti di sicurezza su Internet hanno iniziato a comprendere non solo le misure di sicurezza tecniche, ma anche l'alfabetizzazione digitale e le capacità di pensiero critico. Educare gli utenti sull'identificazione della disinformazione, delle fake news e delle truffe online è diventato fondamentale per combattere le minacce online. • L'ascesa del settore della sicurezza informatica: la crescente sofisticazione delle minacce informatiche ha dato origine a un solido settore della sicurezza informatica. Le aziende e i professionisti specializzati in servizi di sicurezza informatica, analisi delle minacce e risposta agli incidenti hanno svolto un ruolo cruciale nella difesa contro l'evoluzione dei rischi online.

- Integrazione della sicurezza su Internet nell'istruzione: riconoscendo l'importanza dell'educazione alla sicurezza su Internet, le scuole e le istituzioni educative hanno iniziato a incorporarla nel loro curriculum. Insegnare ai bambini e ai giovani adulti un comportamento online responsabile e la cittadinanza digitale è diventato un aspetto essenziale dell'istruzione moderna. L'alfabetizzazione mediatica è una materia didattica che nasce con l'obiettivo di fornire alle persone tutti gli strumenti necessari per comprendere meglio le dinamiche e i messaggi offerti dai media, e per rielaborarli in modo autonomo e critico. Oggi è necessario insegnare alle persone a gestire al meglio il loro rapporto con i social media, educarle e formarle su "cosa e come postare" o su come riconoscere le "fake news". L'utilizzo di Internet grazie agli smartphone offre infinite potenzialità di apprendimento, ma anche rischi legati all'"uso superficiale di questi strumenti". Gli "immigrati digitali" sono i più a rischio perché non sono abituati a fare i conti con le regole non scritte di un mondo virtuale a cui non appartengono. Spesso non conoscono i principali sistemi di comunicazione e non hanno la capacità di elaborare nuovi messaggi per offrire il proprio contributo alla comunità, rimanendo elementi passivi.

1.4. Componenti chiave di un'esperienza online sicura

I "Componenti chiave di un'esperienza online sicura" sono elementi essenziali che contribuiscono a creare un ambiente sicuro e protetto durante l'utilizzo di Internet. Questi componenti comprendono varie pratiche, comportamenti e strumenti che le persone possono utilizzare per garantire la propria sicurezza e privacy online. La comprensione e l'implementazione di questi componenti chiave sono fondamentali per un'esperienza Internet positiva e sicura.

	• Consapevolezza della sicurezza informatica: lo sviluppo di una forte consapevolezza della sicurezza informatica è fondamentale per un'esperienza online sicura. Ciò comporta rimanere informati sulle ultime minacce informatiche, comprendere i metodi di attacco comuni come phishing e malware e riconoscere i segnali di avvertimento di attività sospette. La consapevolezza consente alle persone di prendere decisioni informate e prendere le precauzioni necessarie durante la navigazione nel mondo digitale. • Protezione della privacy: Proteggere la propria privacy è un aspetto cruciale della sicurezza su Internet. Si tratta di essere consapevoli delle informazioni condivise online ed evitare di condividere eccessivamente i dettagli personali. La salvaguardia dei dati sensibili, come le informazioni finanziarie e i documenti di identificazione, è essenziale per prevenire furti di identità e frodi. • Autenticazione forte: l'utilizzo di metodi di autenticazione robusti per gli account online è fondamentale. Ciò include l'utilizzo di password complesse e univoche per ogni account e l'utilizzo di livelli di sicurezza aggiuntivi come l'autenticazione a due fattori (2FA) o l'autenticazione biometrica, se disponibile. Le misure di autenticazione avanzata aiutano a impedire l'accesso non autorizzato agli account e a proteggere le informazioni sensibili. • Pratiche di navigazione sicura: Praticare abitudini di navigazione sicure è necessario per evitare siti Web dannosi e potenziali minacce. Ciò include la verifica degli URL dei siti Web prima di inserire informazioni sensibili, evitare di fare clic su collegamenti o popup sospetti e utilizzare browser sicuri con protezioni integrate.

	• Aggiornamenti regolari del software: mantenere aggiornati il software, i sistemi operativi e le applicazioni è essenziale per mantenere un'esperienza online sicura. Gli aggiornamenti regolari spesso includono patch di sicurezza che risolvono vulnerabilità note, rendendo più difficile per i criminali informatici sfruttarle. • Reti sicure: la connessione a reti sicure e affidabili è fondamentale per proteggere i dati in transito. Evitare le reti Wi-Fi pubbliche senza adeguate misure di sicurezza è essenziale per prevenire potenziali intercettazioni di dati e accessi non autorizzati. • Pratiche sicure sui social media: Essere cauti durante l'utilizzo delle piattaforme di social media è fondamentale per proteggere le informazioni personali ed evitare di cadere vittima di attacchi di ingegneria sociale. Regolare le impostazioni sulla privacy, essere selettivi sulle richieste di amicizia e astenersi dal condividere pubblicamente dati sensibili sono pratiche essenziali per la sicurezza dei social media. • Vigilanza contro il phishing: essere vigili contro i tentativi di phishing è fondamentale. Ciò comporta la verifica dell'identità dei mittenti delle e-mail, il non fare clic su collegamenti sospetti o scaricare allegati da fonti sconosciute e la segnalazione di tentativi di phishing. • Parental Control e supervisione: per genitori e tutori, l'implementazione del parental control e il monitoraggio delle attività online dei bambini sono componenti fondamentali di un'esperienza Internet sicura per i giovani utenti. Ciò garantisce un accesso ai contenuti adeguato all'età e protegge i bambini da contenuti online potenzialmente dannosi.

- Alfabetizzazione digitale e pensiero critico: lo sviluppo dell'alfabetizzazione digitale e delle capacità di pensiero critico è fondamentale per identificare la disinformazione, le fake news e le truffe online. Capire come valutare le fonti di informazione e verificare la credibilità dei contenuti contribuisce a un'esperienza online più sicura.

2. MINACCE ONLINE

2.1. TIPI DI MINACCE ONLINE

I tipi di minacce online si riferiscono alle varie attività e attacchi dannosi che possono mettere a repentaglio la sicurezza, la privacy e l'integrità degli utenti di Internet e dei loro dati. Comprendere queste minacce è fondamentale affinché le persone prendano le precauzioni appropriate e si proteggano durante la navigazione nel panorama digitale. Ecco alcuni tipi comuni di minacce online:

Phishing: il phishing è una tecnica ingannevole utilizzata dai criminali informatici per indurre gli utenti a rivelare informazioni sensibili, come credenziali di accesso, dettagli finanziari o dati personali. I tentativi di phishing spesso coinvolgono e-mail, siti Web o messaggi falsi che imitano entità legittime per indurre le vittime a fornire le proprie informazioni.

Malware: il malware è un software dannoso progettato per infettare e danneggiare dispositivi o reti. Ciò include virus, worm, trojan, ransomware e spyware. Il malware può compromettere i dati, rubare informazioni, interrompere le operazioni o persino rendere inutilizzabili i dispositivi.

Ransomware: il ransomware è un tipo specifico di malware che crittografa i dati di un utente, impedendogli di fatto di accedere ai propri file o sistemi. I criminali informatici richiedono il pagamento di un riscatto per fornire la chiave di decrittazione, ma non vi è alcuna garanzia che il pagamento del riscatto comporti la restituzione dei dati.

	Ingegneria sociale: l'ingegneria sociale consiste nel manipolare gli individui per ottenere l'accesso non autorizzato a informazioni o sistemi sensibili. Questo può essere fatto attraverso l'impersonificazione, la manipolazione o lo sfruttamento della psicologia umana per indurre gli utenti a rivelare informazioni riservate. **Violazioni dei dati:** una violazione dei dati si verifica quando gli aggressori informatici ottengono l'accesso non autorizzato ai dati di un'organizzazione o di un individuo. Ciò può includere informazioni personali, registri finanziari o proprietà intellettuale. Le violazioni dei dati possono avere gravi conseguenze per la privacy delle persone e portare al furto di identità o a perdite finanziarie. **Furto di identità: il furto di** identità comporta il furto di informazioni personali, come numeri di previdenza sociale, dettagli della carta di credito o credenziali di accesso, per impersonare qualcun altro per scopi fraudolenti. I criminali informatici possono utilizzare queste informazioni rubate per ottenere un guadagno finanziario o per commettere altri crimini. **Cyberbullismo:** Il cyberbullismo è una forma di molestia o bullismo online, che si verifica in genere su piattaforme di social media o tramite app di messaggistica. Comporta l'invio di messaggi offensivi, la diffusione di voci o la condivisione di contenuti imbarazzanti con l'intento di danneggiare, intimidire o umiliare la vittima. **Attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS): gli attacchi DoS e DDoS** mirano a sopraffare un sito Web o un servizio online con un'inondazione di traffico, rendendolo inaccessibile agli utenti legittimi. Questi attacchi possono interrompere i servizi online e causare perdite finanziarie per le aziende. **Attacchi Man-in-the-Middle (MitM):** gli attacchi MitM comportano l'intercettazione e l'intercettazione delle comunicazioni tra due parti, ad esempio un utente e un sito Web. L'aggressore può quindi visualizzare o manipolare i dati scambiati all'insaputa delle parti che comunicano. **Exploit zero-day:** gli exploit zero-day prendono di mira le vulnerabilità del software che non sono ancora note al fornitore o agli sviluppatori. I criminali informatici

	utilizzano queste vulnerabilità per lanciare attacchi prima che sia disponibile una patch o una correzione, rendendoli difficili da difendere. **Vulnerabilità dell'Internet of Things (IoT):** man mano che sempre più dispositivi si connettono a Internet, le vulnerabilità dell'IoT sono diventate una preoccupazione. Le deboli misure di sicurezza nei dispositivi IoT possono essere sfruttate per ottenere l'accesso alle reti domestiche o compromettere la privacy. 2.2. RICONOSCERE I SEGNALI DI AVVERTIMENTO Riconoscere i segnali di allarme è un'abilità cruciale quando si tratta di sicurezza su Internet. Si tratta di prestare attenzione agli indicatori che qualcosa potrebbe essere sbagliato o potenzialmente dannoso durante l'utilizzo di Internet. Riconoscendo i segnali di allarme, le persone possono agire tempestivamente per proteggersi dalle minacce online ed evitare di cadere vittima di truffe, attacchi informatici o altre attività dannose. Ecco alcuni segnali di avvertimento chiave a cui prestare attenzione: **Comunicazioni non richieste:** fai attenzione alle e-mail, ai messaggi o alle richieste di amicizia non richieste provenienti da fonti sconosciute o sospette. I criminali informatici utilizzano spesso questi mezzi per avviare tentativi di phishing o distribuire malware. **Grammatica e ortografia scadenti:** molte e-mail di phishing e messaggi truffa contengono errori grammaticali, errori di ortografia o linguaggio imbarazzante. Questi errori possono essere un segno che la comunicazione non proviene da una fonte legittima. **Richieste di informazioni personali:** diffidate delle richieste di informazioni sensibili, come credenziali di accesso, dettagli finanziari o numeri di previdenza sociale, soprattutto se la richiesta arriva inaspettatamente o sembra non necessaria. **Linguaggio urgente o minaccioso: i** messaggi che utilizzano un linguaggio urgente o minaccioso per spingerti ad agire immediatamente potrebbero essere indicatori di una truffa o di un tentativo di phishing.

	Link o URL insoliti: passa il mouse sui link nelle e-mail o nei messaggi per visualizzare la destinazione effettiva dell'URL. Fai attenzione agli URL abbreviati o ai link che reindirizzano a siti Web sospetti. **URL non corrispondenti o falsi: fai** attenzione agli URL che sembrano legittimi ma presentano sottili errori di ortografia o variazioni. I truffatori possono utilizzare nomi di dominio che assomigliano molto a siti Web noti per ingannare gli utenti. **Mittenti di posta elettronica sconosciuti:** verificare l'identità dei mittenti di posta elettronica, soprattutto se il messaggio contiene allegati imprevisti o richieste di informazioni riservate. **Download imprevisti:** fai attenzione a tutti i download o gli allegati che non hai avviato o che non ti aspettavi, in quanto potrebbero contenere malware. **Attività insolita dell'account:** controlla regolarmente l'attività del tuo account online e fai attenzione a eventuali accessi o transazioni non autorizzati. **Comportamento inspiegabile del sistema:** se il computer o il dispositivo si comporta in modo insolito, ad esempio arresti anomali frequenti, rallentamenti o popup imprevisti, potrebbe indicare malware o altri problemi di sicurezza. **Avvisi dal software** di sicurezza: prestare attenzione agli avvisi o agli avvisi del software antivirus o di sicurezza, in quanto potrebbero indicare potenziali minacce o attività sospette. **Offerte e promozioni non richieste:** fai attenzione alle offerte o promozioni non richieste che sembrano troppo belle per essere vere, in quanto potrebbero essere truffe che tentano di indurti a fornire informazioni personali. 2.3. CONSEGUENZE DELL'IGNORARE LE MINACCE ONLINE Ignorare le minacce online può avere conseguenze gravi e di vasta portata che possono avere un impatto negativo sugli individui, sulle aziende e persino sulla società nel suo complesso. La mancata risposta o l'adozione di misure appropriate contro le minacce online può rendere vulnerabili a vari rischi informatici, con conseguenti perdite finanziarie,

	violazioni della privacy, danni alla reputazione e persino ripercussioni legali. Ecco alcune conseguenze chiave dell'ignorare le minacce online: **Perdita finanziaria:** Cadere vittima di truffe, attacchi di phishing o schemi online fraudolenti può comportare perdite finanziarie significative. I criminali informatici possono rubare credenziali bancarie, informazioni sulla carta di credito o condurre transazioni non autorizzate, con conseguente prosciugamento dei conti bancari e difficoltà finanziarie. **Furto di identità:** ignorare i segnali di avvertimento di un furto di identità può consentire ai criminali informatici di rubare informazioni personali, come numeri di previdenza sociale, date di nascita e indirizzi. Possono utilizzare queste informazioni rubate per commettere frodi finanziarie, aprire conti a nome della vittima o impegnarsi in altre attività criminali, causando gravi conseguenze a lungo termine per la vittima. **Violazioni dei dati: la mancata** implementazione di solide misure di sicurezza o la mancata risoluzione delle vulnerabilità può portare a violazioni dei dati per individui e organizzazioni. Una violazione dei dati può esporre informazioni sensibili, inclusi i dati dei clienti, i segreti commerciali o la proprietà intellettuale, con conseguenti sanzioni finanziarie, responsabilità legali e danni alla reputazione dell'organizzazione. **Attacchi ransomware:** ignorare le pratiche di sicurezza informatica può rendere gli individui e le aziende suscettibili agli attacchi ransomware. Quando i sistemi vengono compromessi da un ransomware, i dati preziosi possono essere crittografati e gli aggressori richiedono il pagamento per la chiave di decrittazione. Il pagamento del riscatto non garantisce il recupero dei dati e le vittime potrebbero subire perdite di dati o interruzioni operative. **Danni alla reputazione:** cadere preda del cyberbullismo o degli attacchi ai social media può causare danni significativi alla reputazione di individui e organizzazioni. Informazioni false, recensioni negative o contenuti dannosi diffusi online possono danneggiare la reputazione personale o del marchio, compromettendo la posizione sociale, le opportunità professionali e la fiducia dei clienti. **Perdita di privacy:** ignorare i problemi di privacy può portare all'esposizione di informazioni private, tra cui

	conversazioni personali, immagini o video. Questa perdita di privacy può avere conseguenze emotive e psicologiche, oltre a potenziali minacce di ricatto. **Conseguenze legali:** l'ignoranza delle minacce informatiche e la mancata implementazione delle misure di sicurezza necessarie possono portare a conseguenze legali. Gli individui o le organizzazioni possono incorrere in azioni legali, multe o sanzioni normative per violazioni dei dati, violazioni della privacy o non conformità agli standard di sicurezza informatica. **Interruzione dei servizi: le** aziende che ignorano le minacce online possono subire interruzioni delle loro operazioni. Gli attacchi informatici, come gli attacchi DDoS (Distributed Denial of Service), possono sovraccaricare i siti Web o le reti, rendendo i servizi inaccessibili ai clienti e con conseguente perdita di entrate e credibilità. **Impatto sociale ed emotivo:** ignorare il cyberbullismo, le molestie online o il comportamento predatorio può avere gravi conseguenze sociali ed emotive per le vittime. Può portare ad ansia, depressione, autoisolamento e persino pensieri di autolesionismo. **Preoccupazioni per la sicurezza nazionale:** ignorare le minacce online può estendersi oltre i livelli individuali o organizzativi e diventare una questione di sicurezza nazionale. Gli attacchi informatici alle infrastrutture critiche o ai sistemi governativi possono interrompere i servizi essenziali, compromettere le informazioni sensibili e minare la stabilità nazionale. 3. SALVAGUARDIA DELLE INFORMAZIONI PERSONALI 3.1. IMPORTANZA DELLA PROTEZIONE DELLA PRIVACY La protezione della privacy è di fondamentale importanza nell'era digitale di oggi a causa dell'uso diffuso della tecnologia e di Internet. Si riferisce alla salvaguardia delle informazioni personali, dei dati e delle attività online di un individuo da accessi non autorizzati, uso improprio e sfruttamento. L'importanza della protezione della privacy può essere compresa da vari punti di vista:

	Sicurezza e protezione personale: la protezione della privacy garantisce che le informazioni personali sensibili, come i numeri di previdenza sociale, i dati finanziari o gli indirizzi di casa, rimangano riservate e sicure. Impedire l'accesso non autorizzato a queste informazioni aiuta a prevenire il furto di identità, le frodi finanziarie e altre forme di crimini informatici che possono avere gravi conseguenze per gli individui. **Privacy e controllo dei dati:** gli individui hanno il diritto di controllare il modo in cui i loro dati vengono raccolti, archiviati e utilizzati dalle organizzazioni. La protezione della privacy garantisce che le persone possano fare scelte informate sulla condivisione dei propri dati e acconsentire al loro utilizzo per scopi specifici. **Mantenere la fiducia: la** protezione della privacy è essenziale per costruire e mantenere la fiducia tra individui e organizzazioni. Quando gli utenti si fidano del fatto che le loro informazioni personali saranno gestite in modo responsabile e sicuro, è più probabile che interagiscano con i servizi online, conducano transazioni e condividano informazioni con fiducia. **Preservare la libertà personale:** rispettare la privacy significa consentire alle persone di esprimersi liberamente, senza timore di sorveglianza o discriminazione in base alle loro attività o preferenze online. La protezione della privacy è essenziale per sostenere il diritto alla libertà di parola e di espressione. **Prevenzione delle molestie e dello stalking online:** la protezione della privacy protegge le persone dalle molestie e dallo stalking online. Limitando l'accesso alle informazioni personali, le misure sulla privacy riducono il rischio di attacchi mirati o cyberbullismo. **Protezione delle relazioni personali: la** protezione della privacy consente alle persone di comunicare e condividere informazioni entro i confini di relazioni di fiducia, garantendo che le conversazioni e le interazioni private rimangano riservate. **Evitare l'uso improprio dei dati:** la protezione della privacy riduce il rischio che i dati personali vengano sfruttati per scopi diversi da quelli previsti dall'individuo. Ciò include evitare campagne di marketing indesiderate, e-mail di spam o contenuti personalizzati che potrebbero violare lo spazio personale.

Prevenzione della discriminazione e della profilazione: la protezione della privacy può aiutare a prevenire la profilazione e la discriminazione delle persone in base alle loro informazioni personali o al loro comportamento online. La raccolta dei dati senza un'adeguata protezione della privacy può portare a un processo decisionale ingiusto e distorto.

Sicurezza informatica e fiducia digitale: la protezione della privacy e la sicurezza informatica sono interconnesse. Una violazione della privacy può portare a incidenti di sicurezza informatica e viceversa. Dando priorità alla privacy, gli individui e le organizzazioni possono promuovere una cultura della fiducia e della sicurezza digitale.

3.2. GESTIONE SICURA DELL'ACCOUNT ONLINE

La gestione sicura degli account online è un insieme di pratiche e strategie volte a proteggere e gestire i propri account online in modo da ridurre al minimo il rischio di accessi non autorizzati e violazioni dei dati. Una corretta gestione degli account online è fondamentale per mantenere la privacy delle informazioni personali, prevenire il furto di identità e salvaguardare le risorse digitali. Ecco alcuni aspetti chiave e best practice per una gestione sicura dell'account online:

Password complesse e univoche: utilizza password complesse e univoche per ogni account online. Evita di utilizzare password facilmente indovinabili, come "123456" o "password". Invece, crea password complesse con un mix di lettere maiuscole e minuscole, numeri e caratteri speciali.

Gestori di password: prendi in considerazione l'utilizzo di un gestore di password affidabile per generare, archiviare e gestire le password in modo sicuro. I gestori di password ti aiutano a mantenere password complesse e univoche per ogni account senza la necessità di ricordarle tutte.

Abilita l'autenticazione a due fattori (2FA): quando possibile, abilita l'autenticazione a due fattori per i tuoi account online. La 2FA aggiunge un ulteriore livello di sicurezza richiedendo una seconda forma di verifica, come un codice monouso inviato al tuo dispositivo mobile, oltre alla password.

	Monitora l'attività dell'account: controlla regolarmente l'attività del tuo account e fai attenzione a eventuali accessi non autorizzati o azioni sospette. Se noti attività insolite, intraprendi azioni immediate per proteggere il tuo account, ad esempio modificando la password e contattando il fornitore dell'account. **Evita computer pubblici e Wi-Fi:** evita di accedere ad account sensibili, come e-mail o operazioni bancarie, da computer pubblici o reti Wi-Fi non protette. I computer pubblici possono memorizzare le credenziali di accesso e il Wi-Fi non protetto può esporre i tuoi dati a potenziali intercettazioni. **Attenzione ai tentativi di phishing: fai** attenzione alle e-mail, ai messaggi o ai link non richiesti che richiedono informazioni sensibili o ti chiedono di accedere ai tuoi account. Verificare la legittimità del mittente e del sito web prima di fornire qualsiasi informazione. **Aggiorna regolarmente le informazioni sul recupero dell**'account: mantieni aggiornate le informazioni sul recupero dell'account, come indirizzi e-mail o numeri di telefono alternativi. Ciò garantisce che tu possa riottenere l'accesso al tuo account se dimentichi la password o riscontri altri problemi di accesso. **Rivedi le impostazioni di privacy e sicurezza: rivedi** periodicamente le impostazioni di privacy e sicurezza dei tuoi account online. Regola le impostazioni in base alle tue preferenze ed esigenze per garantire il giusto equilibrio tra privacy e funzionalità. **Disconnettiti e proteggi i dispositivi:** disconnettiti sempre dai tuoi account quando finisci di utilizzarli, soprattutto su dispositivi condivisi o pubblici. Inoltre, proteggi i tuoi dispositivi personali con password complesse o autenticazione biometrica. **Cambia regolarmente le password**: prendi in considerazione la possibilità di cambiare periodicamente le tue password, soprattutto per account critici come e-mail e servizi bancari. L'aggiornamento regolare delle password aggiunge un ulteriore livello di sicurezza. **Abilita le opzioni di recupero dell'account** : configura le opzioni di recupero dell'account, come domande di sicurezza o codici di backup, per riottenere l'accesso al tuo account nel caso in cui tu sia bloccato.

3.3. CONDIVISIONE RESPONSABILE SUI SOCIAL MEDIA

La condivisione responsabile sui social media si riferisce all'approccio consapevole e cosciente della condivisione di contenuti sulle piattaforme di social media in modo da rispettare la privacy, promuovere interazioni positive ed evitare di contribuire alla disinformazione o al danno. Praticare una condivisione responsabile sui social media è fondamentale per mantenere l'etichetta digitale, promuovere una comunità online positiva e proteggere il benessere personale e collettivo. Ecco alcuni aspetti chiave della condivisione responsabile sui social media:

Protezione delle informazioni personali: fai attenzione a condividere informazioni personali sensibili, come indirizzi di casa, numeri di telefono o dettagli finanziari, sui social media. La protezione delle informazioni personali aiuta a proteggersi dal furto di identità e da altri rischi legati alla privacy.

Regolazione delle impostazioni sulla privacy: rivedi e modifica regolarmente le tue impostazioni sulla privacy sulle piattaforme di social media. Personalizza il pubblico per ogni post, assicurandoti che solo il pubblico previsto possa visualizzare e interagire con i tuoi contenuti.

Rispettare il consenso: ottenere il consenso delle persone prima di condividere le loro foto o informazioni personali sui social media. Presta attenzione alle preferenze delle persone per quanto riguarda l'essere taggate nei post o menzionate nei contenuti.

Verifica dei fatti ed evitare la disinformazione: prima di condividere articoli, informazioni o immagini, verificane l'accuratezza da fonti affidabili. Evita di diffondere disinformazione o contenuti non verificati che potrebbero contribuire alla diffusione di voci o narrazioni false.

Essere consapevoli dei tempi e della frequenza: Evita la condivisione eccessiva o inappropriata, in quanto potrebbe portare a un sovraccarico di informazioni per i tuoi follower. Fai attenzione ai tempi dei tuoi post per rispettare i diversi fusi orari e le preferenze del tuo pubblico.

Promuovere contenuti positivi: condividi contenuti edificanti, informativi o stimolanti. La condivisione positiva

	contribuisce a un ambiente online più sano e favorisce un senso di comunità tra i tuoi follower. **Gestire le discussioni in modo rispettoso:** impegnarsi in discussioni rispettose e costruttive sui social media, anche quando non si è d'accordo con gli altri. Evita di impegnarti in discussioni online o di ricorrere ad attacchi personali. **Evitare contenuti dannosi o offensivi:** astenersi dal condividere contenuti che potrebbero essere offensivi, discriminatori o dannosi per gli altri. Sii consapevole del potenziale impatto dei tuoi post su diversi individui e comunità. **Protezione dei diritti d'autore:** rispettare le leggi sul copyright ed evitare di condividere materiale protetto da diritto d'autore senza un'adeguata autorizzazione o attribuzione. Fornisci i credits dei creatori originali quando condividi il loro lavoro. **Revisione dei contenuti condivisi:** rivedi regolarmente i tuoi contenuti condivisi per assicurarti che siano in linea con i tuoi valori e l'immagine che desideri ritrarre online. Elimina o aggiorna i post che potrebbero non riflettere più le tue prospettive attuali. **Promuovere la gentilezza digitale:** sii gentile ed empatico nelle tue interazioni sui social media. Evita di partecipare o diffondere cyberbullismo, incitamento all'odio o qualsiasi forma di comportamento dannoso. **Incoraggiare una cultura online positiva:** incoraggia gli altri a praticare la condivisione responsabile sui social media dando un esempio positivo. Partecipa a discussioni sulla cittadinanza digitale e sull'importanza di essere cittadini digitali responsabili. 4. NAVIGARE SUI SOCIAL MEDIA IN MODO SICURO 4.1. REGOLAZIONE DELLE IMPOSTAZIONI SULLA PRIVACY La regolazione delle impostazioni sulla privacy si riferisce al processo di personalizzazione del livello di accesso e visibilità delle informazioni personali su varie piattaforme, siti Web e applicazioni. Si tratta di fare scelte informate su quali dati vengono condivisi, con chi vengono condivisi e come vengono utilizzati da terze parti. Regolando le

	impostazioni sulla privacy, le persone possono mantenere un maggiore controllo sulla propria vita digitale e proteggere le proprie informazioni personali da un'esposizione non necessaria. Ecco una spiegazione dettagliata dell'importanza e dei passaggi necessari per regolare le impostazioni sulla privacy: **Importanza della regolazione delle impostazioni sulla privacy:** **Protezione delle informazioni personali: la** modifica delle impostazioni sulla privacy consente alle persone di limitare la quantità di informazioni personali visibili agli altri, riducendo il rischio di furto di identità, stalking o attacchi di ingegneria sociale. **Controllo della condivisione dei dati:** personalizzando le impostazioni sulla privacy, le persone possono controllare quali dati condividono con piattaforme di social media, siti Web e app, limitando la raccolta e l'utilizzo delle loro informazioni. **Prevenzione della pubblicità mirata: le** impostazioni sulla privacy possono aiutare le persone a disattivare la pubblicità mirata e i contenuti personalizzati, fornendo un'esperienza online più privata e meno intrusiva. **Evitare l'uso improprio dei dati:** la regolazione delle impostazioni sulla privacy riduce le possibilità di uso improprio dei dati da parte di terzi non autorizzati, proteggendo da potenziali violazioni e accessi non autorizzati a informazioni sensibili. **Migliorare la sicurezza online:** limitare l'accesso alle informazioni personali tramite le impostazioni sulla privacy può migliorare la sicurezza online e ridurre al minimo il rischio di attacchi di social engineering o phishing. **Passaggi per regolare le impostazioni sulla privacy:** **Rivedi le impostazioni dell'account** : sulle piattaforme di social media, rivedi le impostazioni dell'account o la sezione delle impostazioni sulla privacy per accedere alle opzioni per personalizzare le preferenze sulla privacy. **Scegli il pubblico per i post**: determina chi può visualizzare i tuoi post, ad esempio amici, amici di amici o pubblico. Opta per un pubblico più ristretto per limitare la visibilità dei tuoi contenuti.

Controlla le informazioni del profilo: decidi quali informazioni del profilo sono visibili agli altri, come il tuo indirizzo e-mail, il numero di telefono o la data di nascita. Riduci al minimo la visibilità dei dati sensibili, se possibile.

Gestisci le autorizzazioni delle app: nelle app per dispositivi mobili, rivedi e gestisci le autorizzazioni delle app nelle impostazioni del dispositivo. Consenti solo le autorizzazioni necessarie per ogni app e revoca le autorizzazioni per le app che non le richiedono.

Rifiuto esplicito della raccolta dei dati: alcune piattaforme e siti Web offrono la possibilità di rinunciare alla raccolta e alla condivisione dei dati per scopi pubblicitari. Sfrutta queste opzioni per ridurre il tracciamento dei dati.

Personalizza la condivisione della posizione: scegli quando e con chi condividere la tua posizione. Disattiva la condivisione della posizione quando non è necessaria o limitala a specifiche app attendibili.

Considera la navigazione anonima: utilizza modalità di navigazione privata o in incognito per impedire l'archiviazione della cronologia di navigazione e dei cookie sul tuo dispositivo.

Controlla l'accesso alle app di terze parti: esamina e gestisci le app di terze parti che hanno accesso alle informazioni del tuo account. Revocare l'accesso per le app che non sono più in uso o che non necessitano di accesso.

Fai attenzione alle impostazioni predefinite: molte piattaforme hanno impostazioni di privacy predefinite che potrebbero essere più permissive di quanto desiderato. Prenditi il tempo necessario per regolare queste impostazioni in base alle tue preferenze.

Rivedi e aggiorna regolarmente: rivedi e aggiorna periodicamente le tue impostazioni sulla privacy poiché le piattaforme e le app potrebbero introdurre nuove funzionalità o modifiche che influiscono sulla tua privacy.

4.2. GESTIONE DELLE RICHIESTE DI AMICIZIA E DEI MESSAGGI

Gestire le richieste di amicizia e i messaggi sulle piattaforme di social media e sulle app di messaggistica implica essere

	cauti, perspicaci e rispettosi nelle interazioni con gli altri. È essenziale mantenere i confini personali, proteggere la propria privacy e promuovere un'esperienza online positiva. Ecco alcune linee guida per la gestione delle richieste di amicizia e dei messaggi: **Gestione delle richieste di amicizia:** **Verifica l'identità:** prima di accettare una richiesta di amicizia, assicurati di conoscere la persona o di avere amici in comune. Fai attenzione quando accetti richieste da profili sconosciuti o sospetti. **Controlla le impostazioni sulla privacy:** modifica le impostazioni sulla privacy per controllare chi può inviarti richieste di amicizia. Limita le richieste di amicizia agli amici degli amici o a gruppi specifici per ridurre le possibilità di ricevere richieste da estranei. **Evita di accettare estranei:** sii selettivo nell'aggiungere nuove connessioni. Evita di accettare richieste di amicizia da persone che non conosci personalmente, soprattutto se non hanno legami reciproci. **Blocca o segnala account sospetti:** se ricevi richieste di amicizia da account sospetti o falsi, prendi in considerazione la possibilità di bloccarli o segnalarli agli amministratori della piattaforma. **Rivedi le informazioni del profilo:** prima di accettare una richiesta di amicizia, controlla il profilo del richiedente per assicurarti che appaia autentico e in linea con i tuoi valori e interessi. **Rispetta i limiti:** va bene rifiutare le richieste di amicizia se non ti senti a tuo agio nel connetterti con qualcuno. Rispetta i tuoi limiti e non sentirti obbligato ad accettare ogni richiesta. **Gestione dei messaggi:** **Sii rispettoso:** rispondi ai messaggi in modo educato e rispettoso. Tratta gli altri come vorresti essere trattato in una conversazione online.

	Verifica mittenti: se ricevi un messaggio da un mittente sconosciuto, fai attenzione. Evita di fare clic su collegamenti sospetti o di scaricare allegati da fonti sconosciute. **Evita di condividere informazioni sensibili:** astenersi dal condividere informazioni personali sensibili, dettagli finanziari o password tramite app di messaggistica. Sii cauto nel condividere informazioni private con persone che non conosci bene. **Segnala molestie o abusi:** se ricevi messaggi offensivi, minacciosi o molesti, segnala il mittente agli amministratori della piattaforma o al team di supporto dell'app di messaggistica. **Imposta la privacy dei messaggi:** modifica le impostazioni sulla privacy dei messaggi per controllare chi può inviarti messaggi. Limita l'accesso alla messaggistica ai tuoi amici o contatti. **Usa la funzione di blocco:** se qualcuno ti infastidisce o invia messaggi inappropriati, usa la funzione di blocco per impedire ulteriori contatti da quella persona. **Sii consapevole del tono e dell'intento:** i messaggi possono essere facilmente interpretati in modo errato a causa della mancanza di tono e delle espressioni facciali. Sii consapevole della tua comunicazione e cerca di evitare malintesi. **Prenditi delle pause dalla messaggistica:** va bene prendersi delle pause dalla messaggistica e dai social media per concentrarti su altre attività e ridurre il sovraccarico digitale. 4.3. SEGNALAZIONE E BLOCCO DI ACCOUNT ABUSIVI Segnalare e bloccare gli account abusivi è un passo cruciale per mantenere un ambiente online sicuro e positivo. Gli account offensivi possono assumere comportamenti dannosi, come cyberbullismo, molestie, incitamento all'odio e altre forme di abuso online. Segnalare e bloccare questi account aiuta a proteggere te stesso e gli altri dalle loro azioni dannose. Ecco una spiegazione di come funzionano le segnalazioni e i blocchi e perché sono importanti: **Segnalazione di account abusivi:**

	Identifica un comportamento dannoso: se ti imbatti in un account che si sta impegnando in comportamenti offensivi o dannosi, come molestie, minacce o incitamento all'odio, è importante riconoscerlo. **Segnala l'account: la** maggior parte delle piattaforme di social media e dei servizi online dispone di un meccanismo di segnalazione. Utilizza la funzione di segnalazione della piattaforma per informare gli amministratori o i moderatori del comportamento offensivo. **Fornisci prove:** quando segnali un account offensivo, può essere utile fornire prove, come screenshot o link a contenuti offensivi, a supporto della tua segnalazione. **Scegli la categoria appropriata: le** piattaforme di social media offrono spesso diverse categorie di report. Seleziona la categoria che meglio si adatta al tipo di abuso che stai segnalando. **Rispetta le linee guida per la segnalazione:** acquisisci familiarità con le linee guida per la segnalazione della piattaforma per assicurarti di segnalare gli account per motivi validi. Evitare le false segnalazioni, in quanto possono ostacolare l'efficacia del sistema di segnalazione. **Blocco degli account abusivi:** **Proteggiti:** il blocco di un account abusivo impedisce a quell'account di interagire con te. Può aiutarti a proteggere il tuo benessere mentale e creare uno spazio online sicuro per te. **Impedisci contatti indesiderati:** quando blocchi un account, l'utente dietro quell'account non sarà in grado di seguirti, inviarti messaggi o commentare i tuoi post. **Anonimato:** il blocco è di solito un'azione privata. L'utente bloccato non riceverà alcuna notifica di blocco. **Nessuna ulteriore interazione:** dopo aver bloccato un account, non vedrai più nessuno dei suoi contenuti o attività e lui non sarà in grado di vedere il tuo. **Perché la segnalazione e il blocco sono importanti:** **Prevenzione dei danni:** la segnalazione di account offensivi può comportare l'adozione di misure contro

	l'account, che possono prevenire ulteriori danni a te o ad altri. **Applicazione delle linee guida della piattaforma:** la segnalazione di comportamenti offensivi aiuta a far rispettare i termini di servizio e le linee guida della community della piattaforma, creando un ambiente più sicuro per tutti gli utenti. **Sostenere la salute della comunità:** segnalando e bloccando gli account abusivi, contribuisci a promuovere una comunità online sana e rispettosa. **Responsabilizzare gli utenti:** la segnalazione e il blocco consentono alle persone di assumere il controllo delle proprie esperienze online e di proteggersi da interazioni abusive o dannose. 5. SICUREZZA INFORMATICA E DISPOSITIVI MOBILI 5.1. PROTEZIONE DI SMARTPHONE E TABLET La protezione di smartphone e tablet è essenziale nel mondo mobile di oggi, in cui questi dispositivi memorizzano una grande quantità di informazioni personali e dati sensibili. La protezione di questi dispositivi aiuta a proteggersi da accessi non autorizzati, violazioni dei dati e attacchi malware. Ecco alcune misure chiave per garantire la sicurezza di smartphone e tablet: **Abilita la sicurezza della schermata di blocco:** configura un metodo di blocco sicuro della schermata, ad esempio un PIN, una sequenza, una password o dati biometrici (impronta digitale o riconoscimento facciale). In questo modo si impedisce l'accesso non autorizzato al dispositivo in caso di smarrimento o furto. **Mantieni aggiornato il software:** aggiorna regolarmente il sistema operativo e le applicazioni sul tuo dispositivo. I produttori rilasciano aggiornamenti per correggere le vulnerabilità di sicurezza, quindi mantenere aggiornato il dispositivo è fondamentale per rimanere protetti da potenziali exploit.

	Installa solo app attendibili: scarica app da app store ufficiali (ad es. Google Play Store, Apple App Store) ed evita di installare app da fonti sconosciute. Le app dannose provenienti da fonti non ufficiali possono compromettere la sicurezza e la privacy del tuo dispositivo. **Esamina le autorizzazioni dell'app:** fai attenzione quando concedi le autorizzazioni alle app. Esamina le autorizzazioni richieste da ogni app e valuta se sono necessarie per la funzionalità dell'app. Evita di concedere autorizzazioni non necessarie che potrebbero compromettere la tua privacy. **Usa una VPN su reti Wi-Fi pubbliche:** quando utilizzi reti Wi-Fi pubbliche, prendi in considerazione l'utilizzo di una rete privata virtuale (VPN) per crittografare il tuo traffico Internet e proteggere i tuoi dati da potenziali intercettazioni o ficcanaso. **Navigazione mobile sicura:** utilizza browser sicuri che offrono connessioni crittografate (HTTPS) per i siti web. Evita di accedere a informazioni sensibili, come l'online banking, su reti pubbliche o non protette. **Esegui regolarmente il backup dei** dati: esegui regolarmente il backup dei dati del tuo dispositivo su un servizio cloud sicuro o su un dispositivo esterno. Ciò garantisce che le tue informazioni importanti siano al sicuro anche se il tuo dispositivo viene perso, danneggiato o ripristinato. **Evita di fare clic su collegamenti sospetti:** fai attenzione a fare clic su collegamenti in e-mail, messaggi o pop-up provenienti da fonti sconosciute. Fare clic su collegamenti dannosi può portare a tentativi di phishing o all'installazione di malware. **Usa i blocchi delle app per le app sensibili:** prendi in considerazione l'utilizzo di blocchi delle app o di una funzione della modalità ospite per limitare l'accesso alle app o ai contenuti sensibili sul tuo dispositivo. Ciò fornisce un ulteriore livello di sicurezza, soprattutto quando si condivide il dispositivo con altri. **Crittografa i dati del dispositivo: se** il tuo dispositivo lo supporta, abilita la crittografia per proteggere i tuoi dati da accessi non autorizzati anche se qualcun altro accede fisicamente al dispositivo.

	5.2. AUTORIZZAZIONI DELL'APP E ACCESSO AI DATI Le autorizzazioni delle app e l'accesso ai dati si riferiscono alle autorizzazioni richieste dalle applicazioni mobili (app) per accedere a varie funzionalità e dati sul dispositivo di un utente. Quando gli utenti installano e utilizzano app sui propri smartphone o tablet, le app potrebbero richiedere l'accesso a determinate risorse del dispositivo e informazioni personali per funzionare correttamente. Queste autorizzazioni consentono alle app di fornire funzionalità specifiche e migliorare l'esperienza dell'utente. Tuttavia, è essenziale che gli utenti comprendano e gestiscano queste autorizzazioni per proteggere la propria privacy e sicurezza. Ecco uno sguardo più da vicino alle autorizzazioni delle app e all'accesso ai dati: **Tipi di autorizzazioni dell'app: le autorizzazioni dell'app** possono variare a seconda della funzionalità dell'app e della piattaforma (Android o iOS). I tipi comuni di autorizzazioni delle app includono l'accesso alla fotocamera, al microfono, alla posizione, ai contatti, al calendario, allo spazio di archiviazione, agli SMS, ai registri delle chiamate e altro ancora. Alcune app potrebbero anche richiedere l'autorizzazione per utilizzare altri dispositivi connessi, come le periferiche Bluetooth. **Richieste di autorizzazione:** quando gli utenti installano un'app, l'app può richiedere autorizzazioni specifiche necessarie per funzionare. Le richieste di autorizzazione vengono in genere presentate durante il processo di installazione dell'app o quando l'app tenta per la prima volta di accedere a una particolare funzionalità. Gli utenti possono concedere o negare queste autorizzazioni. **Scopo delle autorizzazioni dell'app: le autorizzazioni dell'app** sono necessarie per abilitare determinate funzionalità dell'app. Ad esempio, un'app di fotoritocco deve accedere alla fotocamera e allo spazio di archiviazione del dispositivo per acquisire e salvare le foto. Un'app di navigazione richiede l'accesso alla posizione per fornire indicazioni precise. **Protezione della privacy: sebbene le autorizzazioni dell'app** siano spesso essenziali per la funzionalità dell'app, gli utenti devono prestare attenzione nel concedere le autorizzazioni senza considerare lo scopo dell'app e se le autorizzazioni richieste sono ragionevoli. La concessione di

autorizzazioni eccessive potrebbe potenzialmente compromettere la privacy o consentire alle app di accedere a dati sensibili senza una legittima necessità.

Gestione delle autorizzazioni delle app: la maggior parte dei sistemi operativi moderni consente agli utenti di gestire le autorizzazioni delle app. Gli utenti possono rivedere e modificare le autorizzazioni delle app nelle impostazioni del dispositivo, consentendo loro di concedere o revocare autorizzazioni specifiche per le singole app in qualsiasi momento.

Leggere attentamente le autorizzazioni: prima di concedere le autorizzazioni, gli utenti devono leggere attentamente le autorizzazioni richieste da un'app. Se un'app richiede autorizzazioni che sembrano non correlate alla sua funzionalità, potrebbe essere un campanello d'allarme e gli utenti dovrebbero prestare attenzione o prendere in considerazione l'utilizzo di app alternative.

Autorizzazioni e aggiornamenti delle app: quando si aggiornano le app, è essenziale esaminare eventuali autorizzazioni nuove o modificate. A volte, gli aggiornamenti delle app possono introdurre autorizzazioni aggiuntive e gli utenti devono assicurarsi che siano in linea con le proprie preferenze ed esigenze.

Richieste di autorizzazione delle app per iOS e Android: mentre iOS e Android gestiscono le autorizzazioni delle app in modo diverso, entrambe le piattaforme offrono agli utenti la possibilità di gestire le autorizzazioni nelle rispettive impostazioni. Su iOS, gli utenti possono rivedere e gestire le autorizzazioni nelle impostazioni dell'app in "Privacy". Su Android, gli utenti possono gestire le autorizzazioni andando su "App e notifiche" o "Gestione applicazioni" nelle impostazioni del dispositivo.

5.3. PROTEZIONE DEI DISPOSITIVI MOBILI DA FURTI E SMARRIMENTI

Proteggere i dispositivi mobili da furti e smarrimenti è fondamentale per salvaguardare le informazioni personali, prevenire il furto di identità e preservare la privacy dei dati sensibili. I dispositivi mobili, come smartphone e tablet, sono spesso bersagli dei ladri a causa della loro portabilità e delle preziose informazioni che memorizzano. L'implementazione di misure di sicurezza può ridurre

	significativamente i rischi associati a furto o smarrimento. Ecco alcuni passaggi importanti per proteggere i dispositivi mobili: **Configura la sicurezza della schermata di blocco:** abilita un metodo di blocco sicuro, ad esempio un PIN, una sequenza, una password o dati biometrici (impronta digitale o riconoscimento facciale). In questo modo si impedisce l'accesso non autorizzato al dispositivo se cade nelle mani sbagliate. **Usa i servizi Trova il mio dispositivo: abilita la funzione "Trova il mio dispositivo"** o "Trova il mio iPhone" sul tuo dispositivo. Questi servizi ti consentono di localizzare, bloccare o cancellare il tuo dispositivo da remoto in caso di smarrimento o furto. **Mantieni aggiornati software e app:** aggiorna regolarmente il sistema operativo e le app del tuo dispositivo per assicurarti di avere le ultime patch di sicurezza e correzioni di bug. I produttori rilasciano aggiornamenti per risolvere le vulnerabilità e migliorare la sicurezza dei dispositivi. **Evita di lasciare i dispositivi incustoditi:** fai attenzione a lasciare il tuo dispositivo mobile incustodito in luoghi pubblici, come ristoranti, trasporti pubblici o palestre. Tieni il tuo dispositivo con te o conservalo in modo sicuro per ridurre il rischio di furto. **Rimani vigile nelle aree affollate:** presta attenzione a ciò che ti circonda nelle aree affollate, soprattutto dove è più probabile che si verifichino borseggi e furti. Prestare attenzione quando si utilizza il dispositivo in spazi affollati. **Conserva in modo sicuro il tuo dispositivo a casa:** conserva il tuo dispositivo mobile in un luogo sicuro quando non è in uso, soprattutto a casa. Evita di lasciarlo sul tavolo, vicino a finestre aperte o aree facilmente accessibili. **Usa i blocchi delle app per le app sensibili:** prendi in considerazione l'utilizzo dei blocchi delle app o delle funzionalità della modalità ospite per limitare l'accesso alle app o ai contenuti sensibili sul tuo dispositivo. Questo aggiunge un ulteriore livello di sicurezza, soprattutto quando si condivide il dispositivo con altri. **Crittografa i dati del dispositivo: se** il tuo dispositivo lo supporta, abilita la crittografia per proteggere i tuoi dati da

	accessi non autorizzati, anche se qualcun altro accede fisicamente al dispositivo. **Evita le stazioni di ricarica pubbliche:** astenersi dall'utilizzare stazioni di ricarica pubbliche o porte USB, poiché potrebbero essere compromesse e rappresentare un rischio di furto di dati o installazione di malware. **Esegui regolarmente il backup dei** dati: esegui regolarmente il backup dei dati del tuo dispositivo su un servizio cloud sicuro o su un dispositivo esterno. Ciò garantisce che le tue informazioni importanti siano al sicuro anche se il tuo dispositivo viene perso, danneggiato o ripristinato. **Usa protezioni per lo schermo per la privacy:** prendi in considerazione l'utilizzo di protezioni per lo schermo per la privacy per impedire a occhi indiscreti di visualizzare lo schermo negli spazi pubblici. **Registra i dispositivi presso le autorità: registra i** tuoi dispositivi mobili presso le autorità locali o i database pertinenti. Questo può aiutare nel processo di recupero in caso di furto del dispositivo.
Glossario:	1. Sicurezza online La pratica di seguire linee guida attuabili, comprendere la tecnologia moderna e proteggere i dispositivi digitali per difendersi da parti dannose del mondo online. 2. Sicurezza Internet Misure e pratiche adottate per proteggere computer, reti e dati da minacce informatiche, come malware, virus e accessi non autorizzati. 3. Privacy digitale Il diritto di controllare e proteggere le proprie informazioni e i propri dati personali dall'accesso, dall'utilizzo o dalla condivisione senza consenso. 4. Sicurezza informatica La protezione dei dispositivi digitali, delle reti e dei sistemi informativi dalle minacce informatiche, tra cui hacking, violazioni dei dati e attacchi informatici. 5. Pratiche online sicure L'insieme di linee guida e comportamenti che le persone dovrebbero seguire per garantire che le loro attività online siano sicure e proteggano la loro privacy.

	6. Protezione dei dati personali La salvaguardia dei dati sensibili e personali da accessi non autorizzati o usi impropri, prevenendo furti di identità e frodi. 7. Galateo dei social media Il comportamento corretto e rispettoso che le persone dovrebbero rispettare quando utilizzano le piattaforme di social media. 8. Sicurezza dei dati Misure e protocolli adottati per proteggere i dati digitali da accesso, modifica o distruzione non autorizzati. 9. Prevenzione del furto di identità Tecniche e pratiche per salvaguardare le informazioni personali e impedire ai criminali di utilizzarle per impersonare individui. 10. Gestione delle password La pratica responsabile di creare password complesse e univoche e di gestirle in modo sicuro per proteggere gli account online. 11. Minacce online Vari rischi e pericoli incontrati durante l'utilizzo di Internet, come phishing, malware, truffe e cyberbullismo. 12. Consapevolezza del phishing La capacità di riconoscere ed evitare i tentativi di phishing, in cui gli aggressori ingannano le persone per ottenere informazioni sensibili, spesso tramite e-mail o siti Web fraudolenti. 13. Impostazioni sulla privacy Le opzioni personalizzabili sulle piattaforme online che consentono agli utenti di controllare la visibilità delle proprie informazioni personali e il pubblico dei propri contenuti. 14. Segnalazione di abusi Il processo di informare gli amministratori o i moderatori della piattaforma in merito a comportamenti offensivi o dannosi sulla piattaforma, come molestie o incitamento all'odio. 15. Blocco degli account

	L'azione di impedire a un account abusivo o indesiderato di interagire con te o di visualizzare i tuoi contenuti sulle piattaforme dei social media. 16. Transazioni online sicure Garantire che le transazioni online, come acquisti o transazioni finanziarie, siano condotte in modo sicuro e protetto per prevenire le frodi. 17. Impronta digitale La scia di dati e informazioni lasciati dalle attività online di un individuo, inclusi i post sui social media, la cronologia delle ricerche e le interazioni online. 18. Prevenzione del cyberbullismo Misure adottate per fermare e prevenire molestie, intimidazioni o bullismo online. 19. Autenticazione a due fattori (2FA) Un ulteriore livello di sicurezza che richiede agli utenti di fornire due forme di identificazione (ad esempio, password e un codice univoco inviato al proprio telefono) per accedere a un account. 20. Abitudini di navigazione sicure Pratiche e linee guida per garantire una navigazione sicura e protetta in Internet, evitando siti Web e contenuti rischiosi.
Bibliografia:	Suggerimenti per la sicurezza su Internet e regole di sicurezza su Internet (kaspersky.com) Sicurezza online (per adolescenti) - Nemours KidsHealth Che cos'è la sicurezza online? | SWGfL Conversazione sulla sicurezza online | LearnEnglish Adolescenti (britishcouncil.org) Sicurezza in Internet - Wikipedia Problemi di sicurezza online - Consigli per supportare i bambini | Internet è importante Sicurezza in Internet: Introduzione alla sicurezza in Internet (gcfglobal.org) indianjournals.com/ijor.aspx?target=ijor:ijie&volume=8&issue=2&article=001 "Sicurezza in Internet" in: L'Enciclopedia internazionale dell'alfabetizzazione mediatica online (researchgate.net)

	İnternette Güvenlik İpuçları - Google Güvenlik Merkezi (safety.google) Essere al sicuro online | Commissario per la sicurezza elettronica Come rimanere al sicuro online: suggerimenti e risorse per la sicurezza in Internet (reviews.org)
Risorse (video, link di riferimento)	https://www.youtube.com/watch?v=qZE45J-MIUg&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=aO858HyFbKI&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=HxySrSbSY7o&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=EyQeUwqCDWg&pp=ygULc2FmZSBvbmxpbmU%3D