ROYAL HOLLOWAY UNIVERSITY OF LONDON

Digital Violence Info

IT · Italiano

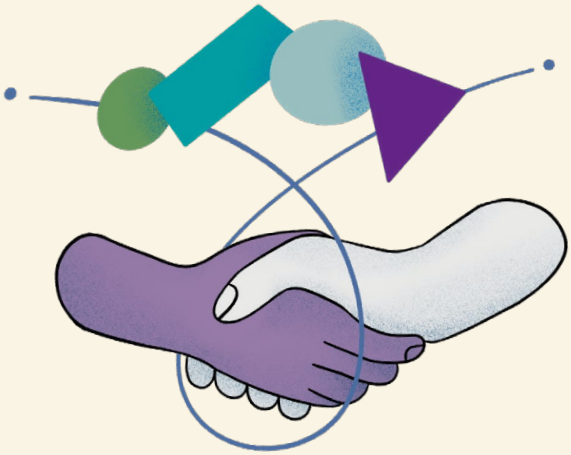


Manuale sulla violenza digitale

La tua guida alla sicurezzadigitale

La tecnologia, pur essendo utile, viene sempre più spesso strumentalizzata dagli aggressori per causare danni. Alcuni abusi legati alla tecnologia sono evidenti, ma altre forme sono più impercettibili, nascoste nelle impostazioni delle app e in connessioni invisibili tra dispositivi, account online o servizi. Questo manuale vuole aiutarti a riprendere il controllo. Non pretende di trattare ogni aspetto, ma si concentra su semplici misure che possono fare davvero la differenza.

Se qualcosa ti sembra poco chiaro, chiedi aiuto a un contatto fidato che se ne intenda di tecnologia o a un operatore o un'operatrice di supporto. Non devi fare tutto in una volta, e non devi affrontare tutto senza aiuto. Se ti trovi in una relazione violenta, rivolgiti prima a un centro di aiuto alle vittime, perché le misure tecniche possono esporti a un pericolo ulteriore.



© Royal Holloway e Bedford New College 2026
Pubblicato con licenza CC BY-NC-ND
Manuale sulla violenza digitale – Italiano (Svizzera) v1.0

La tua sicurezza digitale

Le nozioni di base

Ci sono alcuni semplici passaggi che puoi seguire per proteggere i tuoi account online e la tua privacy.

Protezione dell'account

Prenditi il tempo necessario per controllare uno per uno i tuoi account più importanti – tra cui e-mail, social media, ID Google o Apple, servizi di banking online, account di shopping online, app per la salute e il fitness, servizi di archiviazione cloud, servizi di streaming (ad esempio Netflix) e dispositivi domotici.

Dove possibile e sicuro, puoi sostituire gli account esistenti con dei nuovi account.

Nuove e-mail e nuovi account

Crea un nuovo account e-mail a cui solo tu puoi accedere. Servizi come ProtonMail sono gratuiti e ti consentono di creare un account senza fornire dati personali o un numero di telefono. Il tuo nuovo indirizzo e-mail può essere utilizzato per configurare in modo sicuro tutti gli altri account (ad esempio, sui social media e sulle app bancarie).

Password sicure

Utilizza nuove password difficili da indovinare per gli altri, ad esempio basate su una combinazione di tre parole casuali come "ViolaTazzaGiardino", caratteri speciali e numeri.

Per i dispositivi a cui puoi accedere solo tu, puoi utilizzare un gestore di password gratuito come Bitwarden per generare e salvare password uniche per tutti i tuoi account.



Autenticazione a due fattori (2FA)

Per una maggiore sicurezza, attiva l'autenticazione a due fattori (2FA). Anche se qualcuno fosse in possesso della tua password, non potrebbe accedere agli account protetti dalla 2FA senza il tuo telefono. Installa un'app come Google Authenticator, Microsoft Authenticator o Authy per iniziare.

Proteggere i tuoi account esistenti

Invece di creare nuovi account, puoi anche controllare le impostazioni dei tuoi account esistenti. Tieni presente che la modifica di alcune impostazioni (come l'indirizzo e-mail o il numero di telefono di recupero) potrebbe attivare l'invio di una notifica ai vecchi recapiti. Se qualcun altro ha accesso a tali informazioni, potrebbe venire a conoscenza delle tue azioni. Apporta le seguenti modifiche solo se ritieni che sia sicuro farlo.

- Sostituisci le password con altre nuove e sicure.
- Imposta un nuovo indirizzo e-mail sicuro come indirizzo di recupero dell'account.
- Elimina tutti i numeri di telefono (di recupero) sui quali non hai il pieno controllo.
- Aggiorna le domande di sicurezza utilizzando risposte che nessun altro potrebbe conoscere; se ti sembra più sicuro, puoi anche usare risposte inventate.
- Disconnettiti da tutte le sessioni attive e da tutti i dispositivi – non solo da quello che stai utilizzando – per impedire l'accesso ai tuoi account da altre postazioni.
- Disconnetti eventuali account collegati che potrebbero consentire a qualcuno di accedere di nascosto.



Tutela della privacy

I passaggi riportati di seguito ti aiutano a impedire che le tue informazioni personali vengano utilizzate per rintracciarti, monitorarti o causarti danni.

Verifica le impostazioni sulla privacy

Molte app condividono più informazioni su di te di quanto tu creda. Controlla i tuoi account e modifica le impostazioni relative a chi può vedere il tuo profilo, le tue foto e i tuoi post. Modifica le impostazioni in modo che la tua ultima connessione o la tua posizione non siano visibili. Di solito è possibile impostare queste opzioni su “Solo io” o “Privato”.

Disattivazione degli account

Se necessario, disattiva i tuoi account e poi disinstalla le app per maggiore tranquillità.

Attenzione alla condivisione dei dati

Evita di pubblicare aggiornamenti sui social media o nello stato di WhatsApp. Valuta la possibilità di rimuovere vecchi post o foto che rivelano la tua posizione, le tue abitudini o le tue relazioni. Chiedi ad amici e familiari di non pubblicare foto, taggarti o menzionare la tua posizione online.

Cercati online

È una buona idea cercare il proprio nome o nome utente su siti come Google per vedere cosa viene fuori. Puoi anche cercare le tue foto online per verificare se sono state utilizzate senza autorizzazione. Se trovi qualcosa che non dovrebbe esserci, di solito puoi segnalarlo alla piattaforma affinché venga rimosso.

Per i genitori

Gli account e i dispositivi dei bambini (ad esempio tablet, Xbox, Nintendo Switch) possono essere utilizzati in modo improprio per tracciare, monitorare o causare danni. Proteggerli contribuisce a garantire una maggiore sicurezza online sia per i vostri figli che per voi stessi.

Applicare misure generali di protezione degli account e della privacy

Le stesse misure di protezione che adotti per i tuoi account (password complesse, opzioni di recupero sicure e impostazioni di privacy rigorose) possono essere applicate anche agli account e ai dispositivi dei tuoi figli.

Controlla le liste degli amici e le chat

Se necessario, controlla i contatti dei tuoi figli nelle app e nei giochi. Elimina tutti quelli che non riconoscete e disattiva le funzioni che consentono agli sconosciuti di inviare loro messaggi.

Disattiva la condivisione della posizione

Molte app e giochi consentono agli utenti di condividere la propria posizione. Disattiva queste funzioni in modo che nessuno possa tracciare i movimenti dei tuoi figli.

Verifica la presenza di account extra sui dispositivi

Su tablet e console di gioco, verifica se sono presenti account “famiglia”, “ospite” o account da amministratore che non hai configurato tu. Elimina quelli che potrebbero consentire a qualcuno di accedere di nascosto.

Abuso finanziario



Esempi di rischio

Rendere impossibile l’accesso ai soldi

Qualcuno ti impedisce di utilizzare il tuo conto corrente, le tue carte o le tue app finanziarie, oppure dirotta somme di denaro come sussidi o assegni di mantenimento per i figli in modo che tu non possa accedervi.

Uso improprio dei tuoi dati personali

I tuoi dati personali vengono utilizzati senza il tuo consenso – ad esempio, per richiedere un credito, richiedere sussidi sociali o registrare beni a tuo nome – il che può comportare problemi legali o finanziari a lungo termine.

Monitoraggio delle tue spese

Ogni transazione viene monitorata: potresti dover rispondere a domande, subire giudizi o addirittura punizioni per come spendi i tuoi soldi, indipendentemente dall’entità della somma.

Come proteggersi

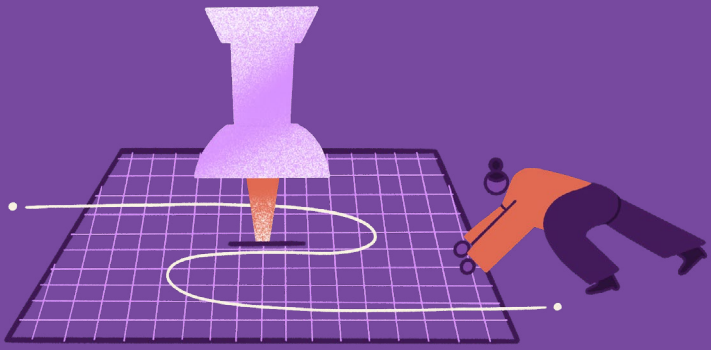
- Apri un nuovo conto corrente intestato esclusivamente a te, per impedire che si possa accedere alle tue risorse finanziarie tramite un conto cointestato, legami familiari o rapporti giuridici come il matrimonio.
- Attiva gli avvisi sulle transazioni accedendo alle impostazioni del tuo servizio di online banking, solitamente nella sezione “notifiche” o “avvisi di sicurezza”, per monitorare in tempo reale qualsiasi attività sul tuo conto.
- Controlla regolarmente gli estratti conto per individuare eventuali transazioni sconosciute o sospette.
- Controlla regolarmente le tue informazioni creditizie e finanziarie per verificare se risultano prestiti, carte di credito o altri impegni finanziari registrati a tuo nome a tua insaputa.
- Contatta il servizio di assistenza della tua banca se noti qualcosa di sospetto.

Risorse aggiuntive

Indicatori di abuso economico e supporto

Informazioni e assistenza a cura di digital-violence.info

«Non era solo una questione di soldi; si trattava di controllo, di rendermi completamente dipendente.»



Geo-localizzazione

Esempi di rischio

Stalkerware

Sul tuo telefono, tablet o computer potrebbero essere installate app nascoste che consentono a qualcuno di tracciare la tua posizione, accedere alla fotocamera o al microfono, visualizzare lo schermo o registrare ciò che digiti, comprese le password.

Tracker nascosti

Piccoli dispositivi di localizzazione, come gli AirTag o i tag Bluetooth, possono essere infilati nelle borse, nelle tasche o nascosti nell'auto.

Uso improprio delle app di geo-localizzazione

App legittime come "Trova il mio dispositivo", Google Maps, Snapchat o persino app di fitness possono essere utilizzate per tracciare i tuoi spostamenti, spesso tramite account condivisi o collegati, oppure tramite impostazioni che non sapevi fossero attive.

Spionaggio tramite dispositivi intelligenti in casa

I dispositivi per la casa intelligente (come i videocitofoni, gli altoparlanti intelligenti o persino il tuo router Wi-Fi) possono essere utilizzati per monitorare quando sei a casa e chi viene a trovarti.

Come proteggersi

- Disattiva i servizi di geo-localizzazione per qualsiasi app per cui tu non ne abbia strettamente bisogno, tramite il menu “Privacy” o “Impostazioni” del tuo telefono.
- Controlla se app come “Trova il mio dispositivo”, Google Maps, Snapchat o i tracker di fitness dispongono di cronologia delle posizioni o condivisione in tempo reale e disattiva queste funzioni.
- Esegui una scansione alla ricerca di spyware; su Android puoi utilizzare app come Incognito Spyware Detector; su iOS, esegui un “Controllo di sicurezza” in Impostazioni -> Privacy e sicurezza per verificare chi ha accesso alle tue informazioni.
- Controlla fisicamente la tua borsa, il cappotto, l’auto e gli oggetti personali (come peluche o portachiavi) alla ricerca di localizzatori nascosti; in caso di dubbi, chiedi a un meccanico di fiducia di controllare la tua auto per verificare la presenza di dispositivi di geo-localizzazione.
- Per individuare gli Apple AirTag, utilizza l’app “Trova il mio dispositivo” su iPhone oppure scarica l’app gratuita Tracker Detect su Android per cercare localizzatori nelle vicinanze non registrati a tuo nome.

«Hanno nascosto un AirTag nello zaino dei miei figli e un altro nella mia auto. È come se non potessimo andare da nessuna parte senza essere seguiti.»

Risorse aggiuntive

Controllo di sicurezza (iOS)

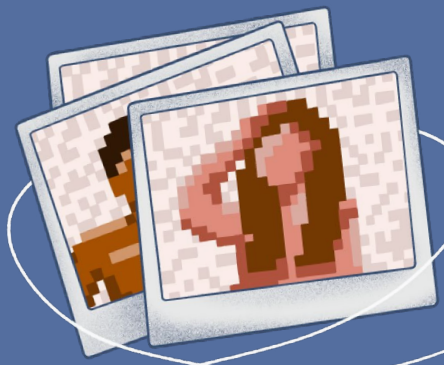
Controllo di sicurezza (Android)

Impostazioni di geo-localizza-zione (iOS)

Impostazioni di geo-localizza-zione (Android)

App per il rilevamento dei dispositivi di tracciamento

Immagini e video intimi



«Mi ha costretta a mandargli delle foto, poi lewwha condivise senza il mio consenso. E ora, con l'intelligenza artificiale, possono persino crearne di false. È come se il mio stesso corpo non mi appartenesse più.»

Esempi di rischio

Coercizione nell'invio di immagini intime

Qualcuno potrebbe costringerti, manipolarti o minacciarti affinché tu invii immagini o video intimi.

Condivisione non consensuale con altri

Le tue immagini intime vengono diffuse, pubblicate online o mostrate ad altri senza il tuo consenso.

Immagini generate dall'intelligenza artificiale o false

Qualcuno utilizza strumenti di intelligenza artificiale per creare contenuti sessuali falsi o manipolati utilizzando il tuo volto o il tuo corpo per umiliarti, fingere di essere te o incastrarti.

Ricatto

Ricevi minacce di divulgazione di immagini intime a meno che tu non faccia ciò che la persona che ti minaccia esige.

Come proteggersi

- Segnala qualsiasi condivisione non consensuale di immagini intime utilizzando strumenti come StopNCII.org e le opzioni di segnalazione presenti sulle piattaforme social e sui motori di ricerca.
- Puoi anche creare in modo proattivo una segnalazione su StopNCII.org: questo ti permette di inviare in modo sicuro le impronte digitali delle tue immagini intime, in modo che le piattaforme possano bloccarle prima ancora che vengano condivise online.
- Conserva qualsiasi prova di minacce o abusi relativi alla tua immagine, nel caso in cui dovessi segnalarli alla polizia o a una piattaforma in un secondo momento. Per i casi che coinvolgono minori, consulta clickandstop.ch per ricevere assistenza.
- Se online compaiono immagini di te generate dall'intelligenza artificiale («deepfake»), segnalale come abuso relativo alla tua immagine. In Svizzera, tali immagini possono violare i tuoi diritti della personalità e, a seconda del loro contenuto e delle circostanze, possono anche essere rilevanti ai sensi del diritto penale.
- Evita di creare o condividere nuove immagini o video intimi.

Risorse aggiuntive

Segnalazione di immagini/video (minori di 18 anni)

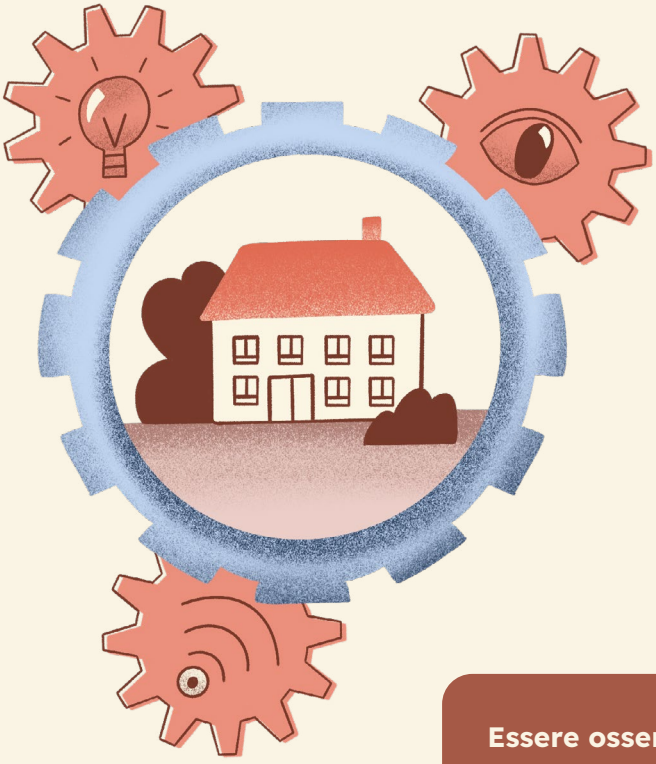
Segnalazione di immagini/ video

Segnalazione di URL e Supporto

Modello di Segnalazione (minori di 18 anni)

Prevenzione della diffusione sulle piattaforme online

Domotica



Esempi di rischio

Rimanere chiusi fuori o dentro casa

Qualcuno usa serrature intelligenti o sistemi di allarme per impedirti di entrare in casa tua – o per impedirti di uscirne.

Essere osservati o ascoltati

Speaker intelligenti, telecamere o microfoni nascosti vengono utilizzati per ascoltare di nascosto le tue conversazioni o osservare ciò che fai a casa.

Destabilizzare il tuo ambiente domestico

Luci, televisori, speaker, riscaldamento o altri elettrodomestici potrebbero essere accesi, spenti o manomessi a distanza per confonderti, spaventarti o metterti a disagio.

Come proteggersi

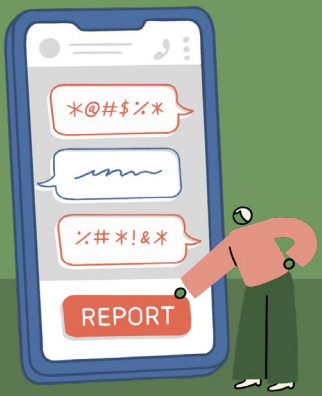
- Togli l'accesso alla persona responsabile eliminando i suoi account utente o le sessioni attive dalle app per la casa intelligente come Amazon Alexa, Google Home, Apple HomeKit (app Home), Ring, Nest, SmartThings o Hue.
- Utilizza un'app gratuita per la scansione della rete come Fing per visualizzare tutti i dispositivi connessi al vostro Wi-Fi: questo può aiutare a individuare telecamere nascoste, microfoni o dispositivi di tracciamento.
- Esegui una scansione dei dispositivi Bluetooth nelle vicinanze dalle impostazioni Bluetooth del tuo telefono per individuare dispositivi sospetti che potrebbero tracciarti o ascoltarti nelle vicinanze.
- Cambia la password del Wi-Fi per impedire che i dispositivi configurati dall'autore del reato rimangano connessi: di solito puoi farlo accedendo al tuo punto di accesso Wi-Fi.
- Ripristina tutti i dispositivi intelligenti (come telecamere connesse, termostati, contatori intelligenti o serrature digitali) alle impostazioni di base oppure scollegali completamente se non ne hai strettamente bisogno.

Risorse aggiuntive

Informazioni e guida a cura di digital-violence.info

«La mia casa intelligente si è trasformata in una trappola. Lui mi chiudeva fuori, manometteva il riscaldamento, e sapevo che le telecamere mi osservavano e mi ascoltavano sempre. Mi sembrava che la mia stessa casa mi stesse spiando.»

App di messaggistica e social media



Esempi di rischio

Essere controllati tramite i messaggi

Potresti essere sottoposto a pressioni affinché tu ti faccia sentire costantemente o risponda immediatamente, oppure i tuoi messaggi potrebbero essere usati contro di te nelle chat di gruppo per creare tensioni o isolarti dagli altri.

La sorveglianza della tua vita online

Qualcuno potrebbe tenere traccia del tuo “ultimo accesso”, monitorare ossessivamente i tuoi post e le liste di amici e follower, o addirittura pedinare i tuoi contatti (ad esempio, la loro posizione su Instagram) per tenerti d’occhio.

Danneggiare la tua reputazione o la Tua carriera

Potrebbero essere pubblicati contenuti falsi (potenzialmente generati dall’intelligenza artificiale) o compromettenti con l’intento di metterti in imbarazzo pubblicamente, oppure qualcuno potrebbe interferire con le tue e-mail, le tue candidature di lavoro o i tuoi contatti professionali per impedirti di cogliere nuove opportunità.

Geo-localizzazione tramite i social media

I post, le foto, i tag ogli accessi su app come Snapchat o TikTok possono essere utilizzati per individuare o confermare la tua posizione, anche se non era tua intenzione condividerla.

«Controllavano i miei messaggi, tenevano d'occhio ogni mio post e hanno persino interferito con il mio lavoro. Mi sembrava che tutta la mia vita digitale fosse diventata un modo per rintracciarmi e intrappolarmi.»

Come proteggersi

- Modifica le tue impostazioni sulla privacy per limitare chi può vedere il tuo profilo, contattarti, visualizzare i tuoi post o controllare il tuo "ultimo accesso": la maggior parte delle piattaforme ti permette di impostare tutto su "Privato".
- Evita di rispondere ai messaggi offensivi.
- Salva i messaggi o fai degli screenshot come prova. Tieni presente che alcune app inviano notifiche quando si fa uno screenshot.
- Utilizza gli strumenti integrati nelle piattaforme per segnalare molestie, minacce o furti d'identità: spesso la segnalazione può essere effettuata all'insaputa dell'altra persona.
- Valuta la possibilità di bloccare la persona responsabile e qualsiasi account collegato a questa persona, inclusi amici o profili falsi, ma solo se ritieni che ciò non aggraverà la situazione.

Risorse aggiuntive

Strategie per contrastare l'incitamento all'odio

Segnalazione dell'incitamento all'odio razzista

Helpline LGBTIQ

Supporto per giovani

© Royal Holloway e Bedford New College 2026 Pubblicato con licenza CC BY-NC-ND Manuale sulla violenza digitale – Italiano (Svizzera) v1.0

Questo manuale è stato realizzato dall'Information Security Group (ISG) della Royal Holloway, University of London (RHUL), in collaborazione con la Public Discourse Foundation e Tech against Violence. La sua realizzazione è stata resa possibile grazie al sostegno finanziario di Soroptimist International Switzerland, dell'Ufficio federale per l'uguaglianza fra donna e uomo, del Cantone di Ginevra e della Fondation pour l'égalité de genre (FEG).

La versione originale del manuale sulla violenza digitale è stata realizzata nel 2025 dall'ISG della RHUL in collaborazione con il Surrey Domestic Abuse Partnership (SDAP), nell'ambito di un progetto finanziato dall'Economic and Social Research Council tramite il programma Social Science Impact Accelerator di Royal Holloway.

I diritti d'autore del presente manuale appartengono al Royal Holloway and Bedford New College, ed è possibile utilizzarlo in base alla licenza Creative Commons CC BY-NC-ND. Se desiderate modificare il presente manuale o utilizzarlo per scopi commerciali, vi preghiamo di contattare TechAbuse-Research@rhul.ac.uk per discutere i termini di una licenza.

Numeri di telefono importanti per un aiuto e un sostegno immediati

Polizia

117

In caso di pericolo immediato o di situazioni minacciose

Servizio di soccorso

144

In caso di ferite o emergenze mediche

Aiuto alle vittime di reat

142

Gratuito, confidenziale, anonimo e disponibile 24 ore su 24, 7 giorni su 7

Sostegno per bambini e giovani

147

Gratuito, confidenziale e disponibile 24 ore su 24, 7 giorni su 7

Ulteriori risorse online

Informazioni sulla violenza digitale
www.digital-violence.info/it

Aiuto alle vittime di reati in Svizzera
www.opferhilfe-schweiz.ch/it

Supporto sulla violenza nella coppia
www.violencequefaire.ch/it

Archivio online per le prove di violenza domestica e stalking
www.with-you.ch/it/safe-withyou

Riconoscere le relazioni tossiche e la violenza domestica
www.with-you.ch/it

Strategie per contrastare l'incitamento all'odio
www.stophatespeech.ch/it