# MANUALE DI AUTODIFESA DIGITALE

# SOMMARIO

# INTRODUZIONE

Internet è una parte essenziale della nostra vita quotidiana. Lo usiamo per restare in contatto con familiari e amici, per gli acquisti, per informarci, per avere indicazioni su dove andare o sui mezzi di trasporto, per pagare i conti, per ascoltare musica e molto altro.
Non dobbiamo dimenticare che oltre a offrire molte possibilità internet potrebbe farci correre dei rischi.
Ci possono essere persone sia conosciute che sconosciute che attraverso internet cercano di avere informazioni su di noi anche senza il nostro consenso.
La buona notizia è che si possono intraprendere azioni semplici per essere protetti da queste persone e dalle minacce della rete in generale.

È importante prendere coscienza del fatto che in primo luogo la nostra sicurezza online è nelle nostre mani: siamo noi a gestire la nostra identità online.
Nella gestione delle nostre informazioni in Internet dobbiamo mettere la stessa cautela che mettiamo nel gestire le cose nel mondo reale.
Non daremmo mai delle informazioni personali o riservate a uno sconosciuto che incontriamo per strada. Lo stesso dobbiamo fare online. Descriveremo di seguito le cose fondamentali da sapere sulla gestione della nostra **identità online.**
Un altro importante mondo, del quale è necessario conoscere regole e rischi è quello delle App di messaggistica e dei **social**

# USO DELLO SMARTPHONE

## Buone consuetudini generiche

### CAMBIO PASSWORD

Il cambio password periodico, oltre a essere necessario per prevenire potenziali truffe informatiche o furti di identità, è buona norma anche per evitare che una persona non autorizzata acceda ai nostri dispositivi o ai nostri profili.

### INSTALLAZIONE APP E PERMESSI RELATIVI

Migliaia di applicazioni invadono i nostri smartphone, meteo, giochi, App di gossip, applicazioni per aggiungere filtri di bellezza ai nostri scatti...

Che cosa può nascondersi dietro alcune di queste applicazioni?

Quando installiamo una nuova App ci viene mostrato a quali risorse bisogna accedere per lavorare al meglio; per esempio, un'App di modifica foto chiederà il consenso per accedere alla nostra galleria o un'App mappa chiederà di accedere alla nostra posizione. Questo può aver senso, giusto?

Spesso però, per la fretta di utilizzare l'applicazione, l'utente non presta attenzione alle risorse richieste in fase di installazione ma il rischio che ne deriva è davvero molto alto!

Perché un'applicazione di modifica foto dovrebbe richiedere l'accesso ai miei contatti? O un'App meteo alla mia galleria? È come se una pattuglia ci fermasse e ci chiedesse patente, libretto e l'ultimo film che ci ha commosso... non suonerebbe un po' strano?

Molti furti di informazioni avvengono proprio in questo modo,

sotto gli occhi dell'utente che ha acconsentito al rilascio delle sue informazioni più care!
Il consiglio è di non avere fretta e prestare sempre molta attenzione a che cosa si installa, valutando se l'App risulta verificata, se è scaricata da un numero elevato di utenti, se le recensioni la dichiarano affidabile! Ma non basta! Conviene sempre fare qualche ricerca online per scegliere l'App più adatta alle proprie esigenze valutandola fra le proposte di chi, prima di noi, si è preoccupato di effettuare la ricerca... e magari... di fornire anche una recensione affidabile presentando pregi e difetti!

## "PULIZIA / BLOCCO" CONTATTI

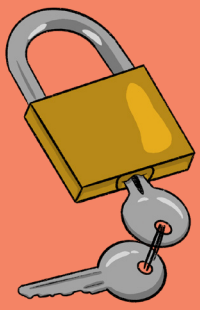
Sui social network più diffusi (Facebook e Instagram) e nelle applicazioni di messaggistica è (WhatsApp, Telegram) possibile eliminare o, ancora meglio, bloccare qualsiasi contatto non gradito. L'eliminazione, nel caso in cui siano impostate le misure di sicurezza della privacy, impedisce al contatto eliminato di visualizzare i nostri dati o le nostre azioni ma non impedisce che il contatto non gradito ci contatti. Il blocco del contatto, invece, oltre a impedire la visualizzazione, impedisce in ogni modo che la persona sgradita ci contatti. È possibile bloccare un contatto, oltre che sui social network o sulle App, anche nella rubrica interna del telefono.

## NON ACCETTARE CONTATTI CHE NON SI CONOSCONO

È buona norma non accettare contatti che non si conoscano personalmente; trattandosi di "persone virtuali", è difficilmente verificabile chi sia effettivamente alla tastiera e quali siano le sue reali intenzioni.

## "NON CANCELLARE" CHAT IMPORTANTI

In caso di chat personalmente sgradite, è consigliabile bloccare il contatto ma senza eliminare il contenuto della chat (o facendone almeno uno screenshot) in modo da avere una testimonianza da presentare alle autorità, qualora vi sia necessità di interpellarle.



## ATTENZIONE A CHI USA IL NOSTRO TELEFONO

Sembra banale, ma anche prestare il proprio telefono a qualcuno (anche se si tratta di familiare o altra persona conosciuta) potrebbe metterci in situazioni di potenziale pericolo. Infatti, in questa situazione, non si ha il controllo di che cosa stia facendo questa persona con il telefono con il rischio che

faccia, anche solo per leggerezza o errore, cose non corrette.

## USARE PIN / SEQUENZE DI SBLOCCO / IMPRONTA DIGITALE

Lo smartphone deve essere SEMPRE dotato di una sequenza o un codice di sblocco conosciuta solamente al proprietario dello stesso. In questo modo, anche in caso di smarrimento o furto dello stesso, non sarà possibile accedere a tutti i contenuti.

## SONO IN DUBBIO? CANCELLO L'ACCOUNT O SMETTO DI USARE LA APP!

Qualora, per qualsiasi motivo, abbia il dubbio che l'applicazione che sto usando non sia sicura, la soluzione migliore è sempre e soltanto quella di cancellare l'account o disinstallare l'applicazione. E ridurre così il rischio al minimo possibile.

## GPS

Ogni smartphone ha la capacità di dirti sempre in che posto ti trovi, tramite il GPS (Global Positioning System ovvero Sistema di Posizionamento Globale). Questa funzionalità però è usata anche per trasmettere la tua posizione, pensa ad esempio al navigatore, alla condivisione con Whatsapp, alle applicazioni per segnalazioni di emergenza, ecc.

Per garantirti che nessuno ti stia "tracciando", controlla che il GPS sia sempre disattivato come impostazione predefinita e attivalo solamente quando effettivamente ti serve e solo per il tempo strettamente necessario.

# Cattive abitudini e cose da non fare!

## CONDIVISIONE ACCESSO ALLA NOSTRA POSTA ELETTRONICA

Se non usiamo molto la posta elettronica potremmo pensare che dare la password della nostra mail ad altri o condividere l'account con altre persone non sia un grande problema, ma ci sbaglieremmo.

Non stiamo considerando che spesso tramite la mail possiamo recuperare le password di molti altri account, per i quali spesso si utilizza la propria e-mail in fase di registrazione. Inoltre, sia nel mondo Android che nel mondo iPhone, l'indirizzo mail è la base su cui viene costruita la nostra identità online che include molti servizi e informazioni, per cui anche in questo caso dando accesso alla nostra e-mail stiamo dando accesso anche ai nostri documenti, alle fotografie e potenzialmente alla cronologia delle nostre posizioni.

## TAGGING

Taggare qualcuno significa creare un link al suo profilo e il post in cui la persona viene taggata verrà aggiunto anche al suo diario. Essere taggati da un amico nel suo aggiornamento di stato significa che tutte le persone che vedono l'aggiornamento possono cliccare sul nome della persona taggata e visualizzarne il profilo.

Non bisogna dimenticarsi che dalle impostazioni personali è possibile attivare il controllo dei tag e autorizzarne (o meno) la pubblicazione. In questo modo è possibile impedire che qualcosa di sgradito possa essere pubblicato (e quindi essere visibile) sul proprio diario/bacheca o profilo personale.

L'autorizzazione, se si ha un contatto bloccato condiviso con altri contatti, può essere utile anche nel momento in cui si blocca un contatto: tale persona non avrà visibilità di alcuna informazione, post o fotografia che sia in qualche modo collegata al proprio utente. Qualora invece il tag non venisse autorizzato, non si impedisce al contatto che lo sta creando di pubblicare il post; in questo modo, anche se non citati direttamente, l'utente bloccato potrebbe acquisire informazioni sul nostro conto.

## CONDIVISIONE CONTENUTI "SENSIBILI"

Bisogna sempre e comunque stare attenti a qualsiasi contenuto che condividiamo. Non si può e non si deve condividere tutto in piena tranquillità. Ormai una foto non è più "solo una foto", ma presenta una serie di elementi che consentono a chi la guarda di capire esattamente dove siamo, quando ci siamo, con chi siamo e quindi capire molte cose sulla nostra vita.

## PARTECIPAZIONE A GRUPPI

Quando si partecipa ad un gruppo (anche se "privato"), non bisogna dimenticare che tutto quello che viene condiviso all'interno diventa disponibile a tutti i membri del gruppo. Tutti i partecipanti del gruppo possono fare screenshot, scaricare filmati o immagini salvandoli sul proprio dispositivo e magari poi inviarli ad altri anche non membri del gruppo!

## INSTALLAZIONE APP INUTILI

Installare App (anche "non rischiose") solo perché sono gratis è un comportamento sbagliato. Installo solo quello che mi serve. Oltre ad aiutare "la vita" dello smartphone (meno consumo di batteria, aggiornamenti, appesantimento generale) è un ottimo modo per evitare di essere infettati da virus.

## FARSI "CONFIGURARE" IL TELEFONO

È buona norma non farsi configurare il telefono da altre persone, soprattutto se non conosciute. Se proprio non abbiamo alternativa perché non ci sentiamo siamo in grado di fare alcune operazioni, allora possiamo farle controllare da uno specialista o da qualcuno di cui davvero ci fidiamo ciecamente.

# SOCIAL NETWORKS - CONSIDERAZIONI GENERICHE

A oggi non avere un social network è per molti impensabile! Eventi interessanti, gruppi di persone che, con noi, condividono le stesse passioni, notizie di cronaca e pagine divertenti… ormai tutto è veicolato da questi servizi.
Ma abbiamo veramente il controllo di tutte le informazioni che condividiamo? Ci siamo mai chiesti come queste informazioni possano crearci fastidi o addirittura gravi situazioni di disagio?
Siamo convinti di avere pieno controllo dei nostri profili social ma come esserne certi? Spesso cadiamo nell'errore di pensare che limitando la visibilità di una fotografia ai soli amici ci garantisca che ognuno di essi abbia cura della nostra privacy come faremmo noi stessi. Nella realtà che cosa impedisce a un conoscente di scaricare quella foto e condividerla altrove o addirittura, renderla pubblica?
Molteplici sono le storie di persone danneggiate pubblicamente perché convinte di aver affidato informazioni sensibili a utenti fidati che invece hanno poi deluso le loro aspettative (ex fidanzati, ex colleghi, vecchi amici).
Non dobbiamo MAI dimenticarci che, indipendentemente da come abbiamo configurato i nostri social, TUTTO quello che condividiamo potrebbe potenzialmente diventare pubblico! Conviene quindi pensarci sempre prima di pubblicare qualcosa e soprattutto conviene cancellare ciò di cui non andiamo più fieri, ove possibile! A oggi, il diritto alla cancellazione e all'oblio ci deve essere garantito!

## PROFILI PRIVATI (ANCHE PER ALCUNE APP, MA SOPRATTUTTO PER I SOCIAL)

La prima cosa saggia è tutelare la propria privacy limitando l'accesso ai propri profili e la visibilità delle informazioni ai soli contatti e non lasciandoli aperti a chiunque. La maggior parte dei social e delle App di messaggistica consentono di impostare tali misure di sicurezza sul proprio account rendendo visibili soltanto alla rete di amici o di contatti salvati in rubrica le proprie fotografie di profilo o di stato, i dati di accesso o i post pubblicati.

## PROFILI IN COMUNE

Perché utilizzare due profili quando se ne può condividere uno con il/la proprio/a fidanzato/a)? Dopotutto si è legati dagli stessi interessi e/o passioni! Niente di più sbagliato! La privacy è un tuo diritto! Non sai che cosa ti potrà riservare il futuro e l'unica persona di cui ti puoi davvero fidare sei tu! Condividendo un account i rischi sono infatti molteplici! Il consiglio è dunque assolutamente quello di avere un tuo profilo personale e non condiviso con nessuno.

## FACEBOOK E INSTAGRAM

Instagram e Facebook sono ormai i social network per eccellenza! Ogni informazione che condividiamo sui social, usati da influencer e VIP di ogni sorta, in realtà ha un lato oscuro che tutti noi dovremmo conoscere.

Facciamo un esempio: siamo a un ristorante cinese in periferia con una cara amica e scegliamo, come molti fanno, di condividere una storia con la foto del nostro piatto menzionando l'amica e inserendo la posizione con il nome del locale.

Questo è sicuramente divertente perché tutti i nostri contatti vedranno quanto sia piacevole la nostra serata, magari proveranno quel ristorante anche loro dandoci un feedback… ma ATTENZIONE! non è tutto qui!

In realtà stiamo facendo sapere a tutti i nostri contatti dove siamo e quindi come trovarci, facciamo sapere che siamo in periferia (zona meno frequentata) e in compagnia solo di una cara amica (magari non esperta di kung fu)…

ma non solo! Stiamo comunicando anche che non siamo a casa e, se viviamo soli e qualcuno ci conosce bene (come un ex fidanzato rancoroso), stiamo indicando che la nostra abitazione è incustodita.

Instagram e Facebook rendono disponibili alcune opzioni per tutelare la nostra privacy, ad esempio per limitare la visibilità dei post, per bloccare utenti, silenziare account ma la vera difesa della nostra privacy siamo solo ed esclusivamente noi!

E se la storia del nostro piatto la pubblicassimo dopo essere tornati a casa? Che cosa cambierebbe?

E non accettare indistintamente tutte le richieste di amicizia/follow per "sentirci un po' più famosi", anche questo ci aiuterebbe molto!

E anche disabilitare poi le nuove funzionalità che indicano, su Facebook, gli amici geolocalizzati nella tua zona ci tutela.

Pensiamo sempre e abituiamoci a pensare che qualcuno potrebbe utilizzare contro di noi le informazioni che condividiamo, purtroppo potrebbe succedere!

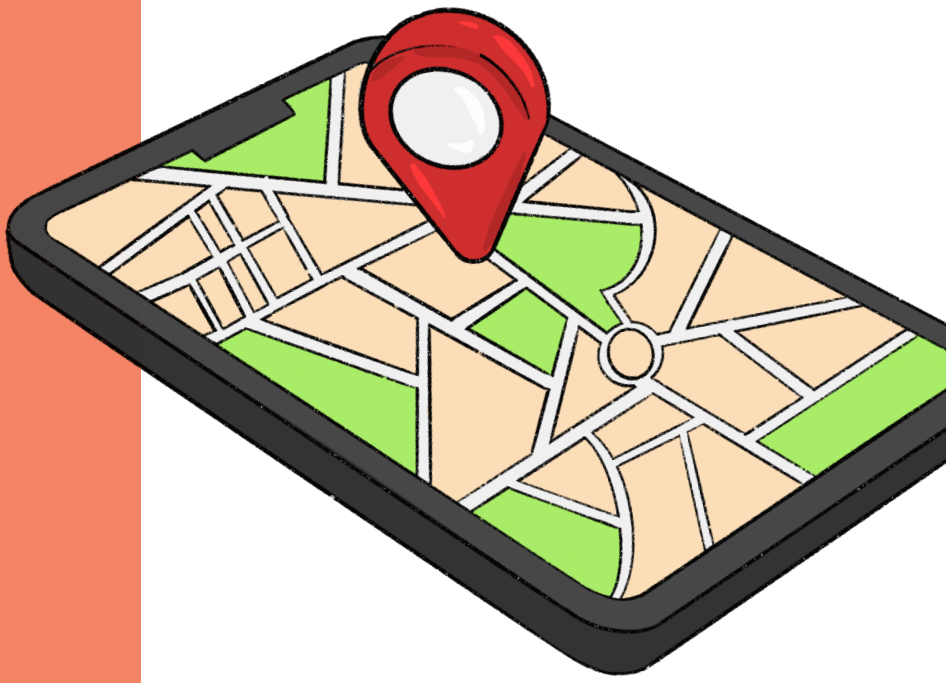
# CONSIDERAZIONI SU WHATSAPP E TELEGRAM

## STATO

Sui social è possibile applicare regole sulla visualizzazione del proprio stato o su quello dei messaggi ricevuti. Dalle impostazioni, infatti, è possibile scegliere se rendere visibile (o meno) la data e l'ora dell'ultimo accesso all'applicazione o la lettura (e relative tempistiche) dei messaggi ricevuti.

## POSIZIONE

Come detto nelle considerazioni generali, bisogna fare estremamente attenzione alla condivisione della propria posizione. In particolare dobbiamo far attenzione a condividere la nostra posizione (se proprio è necessario) solo una volta e non lasciare "condividi in tempo reale" perché l'applicazione continuerebbe a far vedere dove ci troviamo in ogni momento.



# LISTA APP / SITI E TELEFONI UTILI

**112 Where ARE U** è un'app collegata alle centrali del 112 che consente, in caso di emergenza, di effettuare una chiamata al 112 e contemporaneamente inviare la propria posizione. Nel caso si sia impossibilitati a parlare, l'App consente di effettuare una chiamata "muta" e di segnalare il tipo di soccorso richiesto attraverso appositi pulsanti. L'App funziona tramite GPS o rete e/o rete dati; è quindi importante, in questo caso, avere il GPS attivo.

**1522** numero verde (quindi a costo zero) antiviolenza e stalking, attivo 24 ore su 24 e accessibile sia da rete fissa che mobile.

zerounoinformatica

Stati Generali dell'Innovazione

TSCAI
THE SMART CITY
ASSOCIATION ITALY

WMD ITALIA

ROMA

Municipio Roma VII

Realizzazione grafica a cura della scuola di Grafica e Comunicazione dell'Accademia di Belle Arti SantaGiulia.

SANTAGIULIA
HDEMIA
DI BELLE ARTI