

DIGITAL SECURITY LAB

Guida pratica alla privacy, alla protezione dei tuoi dati e della tua vita online

DISPENSA

SICUREZZA PERSONALE ED INFORMATICA.

Ing. Luciano De Rosa

PREMESSA

L'obiettivo del seguente corso potrebbe essere facilmente raggiunto con poche semplici regole: non usare né computer né cellulari, restare sempre chiusi in casa, non ricevere ospiti né farsi fotografare nemmeno negli ambienti chiusi.
E' evidente che tutto ciò non è compatibile con un minimo di vita sociale e "social" che al giorno d'oggi ha la stessa importanza della vita reale, l'essere "connessi" è diventato ormai parte integrante della nostra vita ed il semplice uscire di casa ci espone a telecamere di sorveglianza, riprese involontarie ed incontri inaspettati che rendono sempre più facile fare individuare la nostra posizione.

Quanto segue sono **una serie di raccomandazioni utili** sia a ridurre al minimo i rischi connessi alla vita quotidiana sia normale che digitale che alla possibilità che i propri account vengano violati, fermo restando che maggiore è la situazione di rischio in cui ci si trova esposti maggiore dovrà essere l'attenzione che si pone all'esporsi pubblicamente
fino al dover necessariamente accettare di vivere in parziale, se non completo, isolamento.

ESSERE CONSAPEVOLI DEI RISCHI, ANCHE QUELLI NASCOSTI

Il primo passo da effettuare è essere pienamente consapevoli dei rischi che si possono correre svolgendo anche le più semplici attività quotidiane che ormai sono diventate così naturali e pervasive da non farci pensare alle potenziali insidie e rischi di sicurezza correlati.

L'IMPOSSIBILITÀ DI NON FARSI LOCALIZZARE

Anche senza computer e cellulare, pienamente disconnessi, basta uscire di casa per poter essere individuati e localizzati. **L'ambiente è ormai pieno** di telecamere di sorveglianza, webcam cittadine che inviano le riprese su internet, gente che fotografa in continuazione e posta sui vari social, incontri fortuiti con gente che non si dovrebbe / vorrebbe incontrare nonostante ci si trovi a distanza dalla propria abituale dimora, dobbiamo essere pienamente consapevoli che il mondo è diventato incredibilmente più piccolo e isolarsi in una area remota non è più sufficiente per sparire dal mondo.



RISCHI CONNESSI ALL'USO DI BENI E DISPOSITIVI PERSONALI

La prima insidia da evitare si trova nei **beni personali in uso quotidianamente**, quelli che quando si scappa via si portano comunque con sé, senza pensarci troppo.

Ancora più insidioso è il fatto che non devono essere necessariamente apparati informatici di comunicazione o cellulari, basta un semplice capo di abbigliamento, una borsa, un portachiavi, il giocattolo preferito di un figlio, tutti oggetti che mai potremmo pensare possano essere pericolosi.



LA LOCALIZZAZIONE TRAMITE AIR TAG E DISPOSITIVI SIMILI

Un Air Tag (dispositivo Apple, esistono oggetti equivalenti per Android) è un dispositivo di geolocalizzazione, ovvero fa arrivare al proprietario **la posizione esatta** del dispositivo **in qualsiasi momento.**

Perchè è così pericoloso?

Perché è un **oggetto microscopico** che può essere facilmente inserito e camuffato nei posti più impensabili, la dimensione può essere quella di una moneta, o essere sottile quanto una carta di credito. Inserirlo in modo invisibile in un vestito, una borsa, un giocattolo, un dispositivo elettronico, un portachiavi, ma anche il tacco di una scarpa (!) è facilissimo ed individuarlo molto difficile. Inoltre non ha bisogno di essere ricaricato frequentemente, una volta attivato la batteria interna dura dei mesi, è sufficiente che un qualsiasi telefono cellulare arrivi a portata del dispositivo e la posizione esatta viene trasmessa al proprietario.



MALWARE E SOFTWARE DI TELECONTROLLO

Un Malware **è un software** realizzato appositamente per carpire informazioni personali e spiare le persone. Normalmente si viene infettati casualmente durante le normali attività in rete, ma può essere installato anche volontariamente da qualcuno che vuole tenerci perennemente sotto controllo.

Quindi **Compute**r portatili e non, **Tablet**, **Cellulari**, ma anche **Smartwatch** (!) possono diventare oggetti tramite i quali qualcuno può conoscere sia la nostra posizione che spiare le nostre comunicazioni.

Non è strettamente necessario che i nostri dispositivi abbiano un GPS integrato: per posizionarci su una mappa **basta il rilevamento delle reti WiFi vicine**, la cella telefonica a cui si è agganciato il telefono, monitorare le telefonate ed i messaggi in cui magari diciamo a un amico o a una persona fidata dove ci troviamo, ma anche il solo rilevamento dell'indirizzo IP associato alla connessione pubblica del nostro dispositivo può essere sufficiente.





ACCOUNT DI MESSAGGISTICA E SOCIAL

Il primo rischio è quello di intercettazione dei messaggi inviati: non c'è mai la garanzia di sapere con certezza con chi si sta parlando, gli account possono essere violati e clonati, e magari al posto del nostro fidato amico o familiare c'è proprio la persona da cui dovremmo tenerci lontano.
Anche mantenendo il più assoluto riserbo nelle comunicazioni la sola conoscenza del numero di cellulare associato al nostro account può essere sufficiente per fare individuare la nostra posizione.

UTENZE DOMESTICHE, CELLULARI, CONTRATTI VARI

Sono tutti dati pubblici, o comunque facilmente reperibili da una persona motivata, quindi avere un qualsiasi contratto intestato non è compatibile col voler diventare invisibili.
Semplicemente, non si deve essere titolari di nessuna utenza, e se proprio necessario avere una persona di riferimento che possa sottoscriverla per voi.



STRATEGIE PER LIMITARE I RISCHI

Quelle che seguono sono una serie di strategie da attuare per limitare i rischi. E sottolineo limitare, in quanto **sarà impossibile** svolgere una qualsiasi attività a **rischio zero.**
E' importante capire che maggiori sono i rischi associati all'essere individuati maggiore dovrà essere la consapevolezza che si dovrà rinunciare a parte della propria libertà e semplicemente non svolgere alcune attività.

SICUREZZA FISICA



I seguenti accorgimenti **da attuare nella normale vita reale** possono aiutare, alcuni potrebbero essere considerati eccessivi ma in realtà il rischio è molto più alto di quanto il normale senso comune possa farci pensare.

- **Evitare i luoghi turistici o facilmente riconoscibili dove essere accidentalmente fotografati.**

Per quanto possa sembrare improbabile, una foto ricordo finisce sui social, e se in quella foto siete presenti e riconoscibili la probabilità che veniate individuate e localizzate diventa molto più alta di quanto il senso comune possa suggerire.
Esistono motori di ricerca per immagine che scansionano tutta la rete alla ricerca di corrispondenze, essere individuati è diventato estremamente facile.

- **Evitare di mostrare apertamente il viso in luoghi pubblici**

Valgono le stesse considerazioni del punto precedente: oltre ai turisti ci sono le telecamere di sorveglianza, le webcam cittadine, la gente che fa selfie e pubblica sui social, gli incontri inaspettati.
Non rivelare mai la vostra condizione ai nuovi amici o conoscenti.

- **Il miglior modo di mantenere un segreto è...mantenere il segreto**.

Confidare a qualcuno, per quanto fidato possa sembrare, il proprio stato, è il modo migliore per fare propagare una voce che potrebbe arrivare alle orecchie della persona sbagliata.

- **Non accettare regali, oggetti, vestiario, beni vari, giocattoli etc durante le visite programmate.**



Ricordate il rischio che possano contenere dispositivi di localizzazione, possono diventare il cavallo di troia che porta direttamente alla porta della vostra residenza protetta.

SICUREZZA INFORMATICA

I seguenti accorgimenti sono relativi alla vita social, sarebbe meglio non averla ma se proprio non se ne può fare a meno almeno cercare di attuare comportamenti prudenti:

- **Non usare i propri computer o cellulari e, se proprio non se ne può fare a meno, resettarli alle condizioni di fabbrica**

La motivazione è quella relativa alla manomissione con installazione di Tag o di Malware, l'ideale sarebbe usare dispositivi nuovi di fabbrica. Nell'impossibilità, almeno fare verificare che non contengano dispositivi nascosti e resettarli alle condizioni di fabbrica in modo da cancellare tutto ciò che era stato precedentemente installato PRIMA di prenderne possesso e portarli presso la propria abitazione.

- **Non usare le vecchie schede telefoniche, attivare una nuova numerazione con un titolare di comodo non associabile alla vostra persona.**

Mantenere il vecchio numero implica non solo poter essere contattati da persone indesiderate, ma anche il rischio di essere localizzati soprattutto se il numero è associato a qualche account social. Quindi è indispensabile usare un numero nuovo completamente svincolato da qualsiasi account social e non associabile in nessun modo alla vostra persona.





- **Non usate i vecchi profili social o di messaggistica**

Sono il modo perfetto per spiarvi e localizzarvi, sarebbe bene non averne nessuno. Ogni persona della precedente vita, per quanto fidata, è un rischio inaccettabile per la vostra incolumità.

- **Non contattare vecchi amici, conoscenti, familiari**

Come sopra, bisogna entrare nell'ottica di tagliare i ponti col passato, i familiari e gli amici. Per quanto fidati ed in buona fede potrebbero essere manipolati per rintracciarvi.

- **Non aprire profili social né di messaggistica, o almeno se proprio non se ne può fare a meno, non col vostro nome e senza foto né personali né dei luoghi dove vivete**

Sarebbe meglio non averne, ma se proprio dovete almeno createne di nuovi evitando di inserire le proprie foto e le proprie generalità e dove inserirete solo persone "nuove", evitando accuratamente familiari e vecchi conoscenti ed amici.

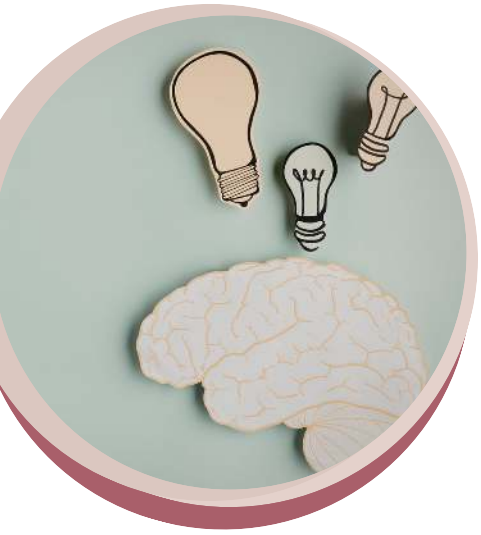
- **Non farsi fotografare, né fotografare e pubblicare o inviare foto dell'interno della casa con uno sfondo riconoscibile, nemmeno l'orizzonte o l'esterno visibile dalle finestre.**

Per quanto possa sembrare assurdo, è sufficiente un qualsiasi dettaglio esterno anche il più insignificante, per individuare la vostra abitazione.
I motori di ricerca per immagine riescono a riconoscere anche i luoghi apparentemente più anonimi senza segni di riconoscimento caratteristici.

SUGGERIMENTI PER CREARE UNA IDENTITÀ DIGITALE SICURA

Si deve essere consapevoli che **non è più possibile creare un account digitale sicuro** protetto da una semplice password: è necessario utilizzare dei sistemi di protezione avanzati che purtroppo si appoggiano ad altri account e/o dispositivi, col risultato finale che si potrebbe essere apparentemente blindati ma in realtà esposti in quanto un elemento della catena non è stato blindato a sufficienza.

Il sistema principale per rendere sicuro un account è quello di utilizzare il metodo dell'**autenticazione a due fattori,** ovvero dopo l'inserimento di login e password è necessario inserire un altro valore variabile nel tempo che possiamo inserire solo noi e non chi sta cercando di rubarci l'account.
Per implementare questa funzionalità ci sono diversi metodi, che vanno dal messaggio o email col codice di controllo da inserire a una app di autenticazione da installare sul cellulare che genera un codice variabile nel tempo e non duplicabile.



Il problema è che se per esempio l'account google che abbiamo sul cellulare non è sufficientemente blindato oppure se il cellulare non è protetto da password e ce lo rubano, esiste un anello debole che permette di scardinare la protezione e rubarci gli account.

Quindi **le linee guida** per minimizzare questi rischi si riassumono in:

a) creare un accoung google nuovo, con password sufficientemente complicata

b) ottenere un cellulare nuovo con SIM (numero) nuovo

c) impostare sul cellulare l'account google appena creato

d) impostare sul cellulare una password di accesso e/o lo sblocco con impronta

e) installare sul cellulare una app di autenticazione, per esempio quella di google

f) blindare l'account google con l'autenticazione a due fattori usando l'app installata

g) stampare e conservare in un posto sicuro i codici di ripristino di emergenza per recuperare l'accesso all'account google ed all'autenticatore se si perde il cellulare.

ATTENZIONE: i codici vanno solo stampati,

NON devono essere mai salvati su un dispositivo digitale. E' importante stamparli perché se non si riesce a ripristinare l'autenticatore non sarà più possibile accedere a nessuno degli account protetti.
Se dovete usarli a causa del furto del telefono, una volta ripristinate le funzionalità sul nuovo telefono fateli rigenerare daccapo in modo da invalidare quelli vecchi e ristampateli.

Una volta creato un nucleo blindato account google / cellulare intorno a questo si possono attivare gli altri account social ognuno dei quali dovrà essere blindato con l'autenticazione a due fattori.



La presente guida è realizzata nell'ambito della coprogettazione provinciale sul contrasto alla violenza di genere_annualità 2026.
Risorse statali (DPCM 28/11/2024 Violenza di Genere - DPCM 28/11/2024 CUAV)
e regionali (L.R. 32/2008)
finalizzate alle attività di prevenzione e contrasto alla violenza di genere nella Regione Marche



© **Ing. Luciano De Rosa**
www.drl.it –
riproduzione non autorizzata
non consentita