CORSO PER UN USO CONSAPEVOLE DELLO SMARTPHONE (ultimo agg. 26 02 2024)

Sommario

QUALE MODELLO SCEGLIERE?

Le due grandi famiglie di Sistemi Operativi

Android è il sistema operativo per smartphone più diffuso al mondo ed è sviluppato da **Google**, sulla base di un progetto open source. Può contare su un parco di applicazioni e giochi davvero sconfinato e concede tantissima libertà all'utente. Si può personalizzare in ogni suo aspetto, tanto è vero che molti produttori equipaggiano i loro telefoni con versioni personalizzate del sistema operativo e applicazioni aggiuntive. Fra i suoi aspetti negativi c'è la frammentazione con cui i produttori distribuiscono gli aggiornamenti rilasciati da Google (che non arrivano allo stesso momento su tutti i terminali, anche se in questi anni si sta cercando di migliorare la situazione).

iOS è il sistema operativo di **iPhone**, cioè degli smartphone della **Apple**. Non è personalizzabile o flessibile quanto Android, ma vanta un parco di applicazioni molto vasto e in generale l'App Store viene visto dagli utenti come un negozio digitale ben curato. Gli aggiornamenti arrivano subito su tutti i modelli di "melafonino" supportati e in generale Apple cerca di mantenere il più possibile il suo sistema operativo alla larga da malware e potenziali problemi di sicurezza.

Lo schermo: LCD – AMOLED

Uno smartphone che non punta a dimensioni "compatte", invece, generalmente rientra nel "range" che va da 5,7 pollici a quasi 7 pollici. In genere, la maggior parte dei dispositivi va da 6 pollici in su.

Sulla **risoluzione** e la densità di pixel non c'è molto da dire: più sono ampi, più pixel ci sono e meglio è (in quanto le immagini e le scritte risultano più nitide). C'è solo da fare un appunto sulla reale utilità degli schermi **QHD** o **2K**, i quali hanno una risoluzione che è sicuramente maggiore rispetto al classico **Full HD (1920 x 1080 pixel)** o **Full HD+** ma difficilmente i loro benefici si riescono a notare nella maggior parte dei contesti.

I **display LCD** possono essere di tipo **TFT** o **IPS**. Gli schermi LCD TFT sono utilizzati spesso sui device a basso costo. Forniscono una qualità dell'immagine generalmente buona ma presentano problemi con i colori, che risultano sbiaditi

quando si varia l'angolo di visione. Inoltre consumano parecchia batteria. Gli schermi LCD IPS consumano una quantità inferiore di energia.

I **display AMOLED** sono ormai presenti su molti smartphone e garantiscono bassi consumi grazie al fatto che i pixel non necessitano di retroilluminazione. Questo significa che i contenuti di colore nero riprodotti su schermo sono formati da pixel "spenti" che non gravano sulla batteria del cellulare. Assicurano una buona riproduzione dei colori, anche quando si varia l'angolo di visione, ma risultano leggermente meno visibili sotto la luce del sole rispetto ai migliori IPS.

La memoria RAM e di archiviazione

Il quantitativo di **RAM** presente su uno smartphone determina la sua capacità di gestire più applicazioni contemporaneamente (multitasking). Al giorno d'oggi 2/3 GB di RAM sono il minimo accettabile per un dispositivo. Tuttavia, risulta una scelta saggia per un utente che usa spesso lo smartphone **puntare almeno su 4GB di** RAM o più.

La **capacità di storage** di uno smartphone, a cui comunemente ci riferiamo con il termine "memoria", può essere espandibile o non espandibile. Si parla di memoria espandibile quando la capacità di storage del dispositivo (espressa in GB) può essere ampliata mediante l'utilizzo di schede microSD (o standard proprietari come l'NM di Huawei). Serve a immagazzinare tutti i dati, file, le applicazioni sul terminale. Al giorno d'oggi, molti dispositivi dispongono già di base di **64 o 128GB**.

Gli smartphone della **Apple** non hanno la possibilità di espansione della memoria.

Il processore

La potenza del processore viene misurata in GHz (frequenza operativa, in gergo), ma moltissimi processori adottano ormai soluzioni multi-core (dual, quad, esa, octa): i core sono delle unità fisiche distinte che permettono di parallelizzare i calcoli e offrire prestazioni superiori in multitasking.

La fotocamera

I parametri in base ai quali devono essere valutate le prestazioni delle **fotocamere** (posteriore e frontale) sono diversi: il numero dei **Megapixel** (ossia la risoluzione delle foto scattate); la presenza o meno del Flash; l'apertura del diaframma (che indica il livello di nitidezza degli scatti fatti al buio); la tecnologia utilizzata per la

stabilizzazione dell'immagine e altro ancora. Il mio consiglio è di cercare su Internet degli esempi di foto scattate con i terminali che ti possono interessare e valutare qual è il migliore secondo il tuo personalissimo metro di giudizio.

Dual SIM – e-SIM

I cellulari **dual-SIM** sono quelli che consentono di usare due SIM contemporaneamente e quindi di avere due numeri di cellulare sullo stesso numero di telefono. Attenzione però, non sono tutti uguali! I telefoni dual-SIM si dividono in smartphone Dual-SIM Dual Stand-by e Dual-SIM Full Active: i primi, che sono la maggioranza, rendono irraggiungibile la seconda SIM mentre la prima è impegnata in una chiamata; i secondi invece mantengono le due SIM sempre attive.

La **eSIM** si può chiamare anche "SIM virtuale", perché la scheda SIM viene sostituita da un servizio virtuale. In poche parole non si deve più possedere fisicamente una tesserina (SIM, nanoSIM o microSIM) per avere un numero di telefono, ma questo diventa attivato virtualmente sul proprio smartphone in pochi passaggi.

I vantaggi della eSIM sono molteplici: il primo e più evidente è l'impossibilità di perdere o rompere la scheda SIM.

Poi c'è il risparmio di materiali tecnologici ad alto valore.

In più i produttori potranno realizzare smartphone con batterie più capienti o usare lo spazio della SIM (che nel disegno di uno smartphone non è poco) per altre tecnologie.

La batteria

La potenza di una **batteria** viene espressa in **milliampereora (mAh)**. Questo significa che maggiore è il numero dei mAh e maggiore è l'autonomia del telefono, ma non sempre vale questa affermazione visto che il consumo energetico dello smartphone varia in base alle operazioni che svolgi. **La navigazione GPS o i giochi, ad esempio, consumano parecchio**, mentre la navigazione sul Web o l'uso delle app tradizionali è meno aggressivo nei confronti della batteria. Il display acceso è anch'esso determinante – spesso molto determinante – ai fini del consumo di batteria. Ricordo inoltre che la maggior parte degli smartphone implementa dei metodi software per risparmiare batteria. Per il resto, potrebbe interessarti anche la questione della **ricarica**. Alcuni dispositivi possono usufruire di una ricarica più rapida di altri, così come magari possono essere ricaricati anche tramite wireless.

Touch ID o Riconoscimento facciale (2D, 3D)

Alcuni modelli di smartphone, ormai praticamente la maggior parte fra quelli presenti sul mercato, sono equipaggiati con un sensore biometrico per il rilevamento delle impronte digitali che consente di sbloccare il device, confermare gli acquisti negli store e autenticarsi in varie app semplicemente poggiando il dito sul cellulare (o meglio, sul sensore). Possono essere più o meno veloci e più o meno affidabili (ad esempio quando si hanno le dita bagnate), con i migliori che si trovano naturalmente sui modelli della fascia medio-alta in su. In ogni caso, esistono varie tipologie di sensori di impronte digitali, dato che esistono soluzioni posizionate sotto allo schermo, integrate sul pulsante d'accensione laterale o piazzate sul retro. La tecnologia ha ormai raggiunto una maturità tale da offrire velocità e affidabilità in pressoché tutti i contesti.

Su molti modelli esiste anche il **riconoscimento facciale**, che può consentirti di sbloccare rapidamente lo smartphone semplicemente inquadrando con la fotocamera anteriore il tuo viso. In questo caso, esistono soluzioni più sicure e meno sicure, dato che in genere si fa riferimento a **2D** (meno sicure, che spesso consentono lo sblocco anche con una semplice foto del proprietario del telefono) e **3D** (più sicuri, che eseguono una scansione tridimensionale del volto dell'utente).

La tecnologia NFC

Con la sigla NFC si fa riferimento alla tecnologia Near Field Communication, molto utile quando gli utenti hanno necessità di inviare dei dati da un dispositivo ad un altro. **Per c**onnettere due dispositivi tramite NFC **non si utilizzano** cavi **e non si devono** inserire delle credenziali d'accesso. Rispetto al Bluetooth, la tecnologia NFC permette di identificare, autenticare ed associare i due dispositivi in modo del tutto automatico.

PIN e password non servono per il trasferimento dei dati, ma è sufficiente che i dispositivi dotati di tecnologia NFC vengano avvicinati tra loro. La vicinanza tra i due device e l'attivazione dei dispositivi per ricevere e inviare dati, presuppone che il trasferimento tramite NFC avvenga effettivamente da chi intende eseguire quest'operazione.

La comunicazione avviene quando i dispositivi si trov**a**no ad una distanza non superiore a 10 centimetri **(**è consigliabile tenere i dispositivi ad una distanza di 3 o 4 centimetri l'uno dall'altro**)**.

La tecnologia NFC è molto utilizzata anche nei **pagamenti elettronici**. Tutte le volte che completi un pagamento, utilizzi la comunicazione NFC. Il trasferimento di denaro è immediato e anche questo gesto quotidiano diventa più semplice e **molto più sicuro**.

Ricordati: Non avviene nessuna comunicazione se il cellulare è bloccato. Quindi se qualcuno lo ruba o lo ritrova perché smarrito, non può fare niente se c'è un sistema di blocco (codice, touch ID, riconoscimento facciale).

Il prezzo

Dipende: lo compri tu o te lo regalano?

LE IMPOSTAZIONI

Le impostazioni si trovano cliccando sull'icona che ha il simbolo dell'ingranaggio.

L'account

È l'utenza associata al sistema operativo dello smartphone ed è sempre un indirizzo email (che magari non usate mai o non sapete di avere perché è stata creata da chi vi ha configurato il telefono).

Connessioni

Wi-Fi

Bluetooth

Hotspot

Suoni e vibrazione

Un momento meraviglioso è quando si tritano i m… alle persone che abbiamo intorno perché vogliamo scegliere una nuova suoneria.

In quest'area possiamo modificare la suoneria, variarne il volume e aggiungere o togliere l'effetto vibrazione.

La vibrazione è utile soprattutto quando mettiamo il telefono in modalità silenziosa per accorgerci che arriva una chiamata. Ma ricordiamoci che anche la vibrazione fa un leggero rumore e se siamo in un ambiente silenzioso (a teatro, a Messa) si sente benissimo.

Possiamo risolvere mettendo, se possiamo, il telefono in modalità AEREO.

Le notifiche

Ma quanto è bello farsi i fatti delle persone che ci stanno intorno leggendo le notifiche dei messaggi che compaiono sui loro display?

Le notifiche sono quegli avvisi che compaiono sullo schermo quando lo smartphone registra qualche evento: messaggi, appuntamenti di calendario, mail, promemoria.

Le notifiche sono utili, ma fino ad un certo punto. Possiamo limitarle, sia come effetto sul display (dove compaiono, quanto viene mostrato e per quanto tempo), sia alle applicazioni veramente importanti.

Schermo

Una corretta impostazione dello schermo consente di ridurre il consumo della batteria e il fastidio alla vista.

Possiamo regolare il livello di illuminazione, il variare dei colori seguendo l'alternanza giorno/notte, introdurre effetti per la protezione degli occhi, le dimensioni del carattere ed eventualmente il grassetto, lo zoom del display per mostrare il contenuto con dimensioni più o meno grandi.

Un fattore importante, soprattutto per il consumo della batteria è lo spegnimento dello schermo, cioè il tempo di ritorno dello smartphone in standby dopo il nostro ultimo tocco; 30" sono già un tempo sufficiente.

Vediamo anche di evitare l'utilizzo del telefono in ambienti bui (cinema e teatri).

Schermata Home

Contiene le impostazioni della schermata, come ad es. il numero di icone nella griglia.

Solitamente va già bene così com'è.

Schermata di blocco

PIN PIN Cavalin

È INDISPENSABILE che l'accesso alle funzionalità del nostro smartphone sia protetto almeno nell'immediato o in caso di furto da parte di uno che non sia un hacker.

Ma è comunque una protezione ancora debole.

Dati biometrici e sicurezza

Vedi il capitolo dedicato quando abbiamo parlato di acquisto dello smartphone.

Touch ID e Riconoscimento facciale sono un importante elemento di sicurezza per la protezione dello smartphone e delle nostre attività, come ad esempio accessi ad aree sensibili come INPS, Agenzia delle Entrate, Homebanking, Fascicolo Sanitario, ecc.

Impronta digitale (touch ID) è la più comoda e rapida.

Conviene sempre impostare almeno due impronte di dita diverse (se vi fate male e avete un cerotto?).

Riconoscimento facciale: vedi differenza tra 2D e 3D. Non cambiate spesso pettinatura o trucco e non fate a botte con i vicini.

Tenete poi presente che se si reimposta il touch ID o il riconoscimento facciale dovete reimpostare quasi tutti gli accessi regolati in quel modo. Quindi dovete ripartire da: disinstallazione dell'app, reinstallazione dell'app, accesso con Utenza e password, reinserimento dell'accesso con dato biometrico.

Privacy e Posizione

Privacy riguarda la gestione delle autorizzazioni. Riflettiamo bene soprattutto su chi autorizziamo a vedere la nostra posizione o la nostra galleria delle foto: siamo proprio sicuri di voler far sapere sempre i fatti nostri?

Soprattutto per la posizione possiamo scegliere per ogni applicazione se permettere l'accesso alla nostra posizione SEMPRE, SOLO QUANDO IN USO, MAI.

Di solito le applicazioni per le quali non abbiamo concesso l'autorizzazione ci propongono la scelta quando è necessario.

Ricordiamo che le applicazioni utilizzano questi dati per darci informazioni utili (come quelle turistiche), ma anche potenzialmente fastidiose come quelle pubblicitarie. Tutti i dati che raccolgono vengono poi utilizzati o venduti per le ricerche di mercato e le scelte commerciali di grandi aziende (avete mai sentito parlare dei Big data?).

È utile invece concedere l'autorizzazione alle funzionalità dello smartphone. Se abilitiamo la Camera alla posizione, aggancerà i dati ad ogni foto che faremo.

Si deve infine sapere che più autorizzazioni vengono date, specie per la posizione, maggiore sarà il consumo della batteria.

Sicurezza ed emergenza

Da non sottovalutare è l'importanza di quest'area, accessibile ai soccorritori anche quando non siete in grado di sbloccare il telefono.

In essa trovano le vostre informazioni mediche (condizioni mediche, allergie, cure correnti, gruppo sanguigno e altre notizie utili), i contatti di emergenza che intendete segnalare e che possono chiamare anche con telefono bloccato.

Si possono anche predefinire particolari azioni sui tasti dello smartphone per segnalare una situazione di emergenza. In questo caso il nostro smartphone attiva automaticamente la geolocalizzazione, invia messaggi SMS di emergenza e fare chiamate automatiche ai contatti che abbiamo memorizzato.

Assistenza dispositivo e batteria

È utile controllare periodicamente la salute della batteria, in particolar modo quando notiamo che dobbiamo ricorrere alla ricarica con maggior frequenza. Se la batteria è ancora efficiente, allora è il caso di ripensare alle nostre abitudini.

In quest'area possiamo controllare anche quanta memoria dello smartphone abbiamo occupato (e quindi quanta è ancora disponibile) e soprattutto quali applicazioni la utilizzano maggiormente. In questo modo possiamo intervenire per liberarne un po'.

Aggiornamenti software

Ogni tanto il sistema operativo viene aggiornato, così come vengono aggiornate le applicazioni residenti (come internet, rubrica, calendario, ecc.) e le app che abbiamo scaricato.

Si consiglia di mettere l'aggiornamento in automatico, in un orario notturno.

Gestione generale

In questo spazio troviamo le funzionalità per impostare la lingua della tastiera (se ne possono attivare più di una) e altri aspetti della digitazione (correzione automatica, maiuscola ad inizio frase, …).

Informazioni sul telefono

È un'area che contiene alcuni dati importanti:

- Il numero del telefono
- Il nome del modello (che vi chiedono quando comprate la cover)
- Il codice IMEI (utilissimo in caso di furto)

Altro

Se non avete trovato quello che vi serve, cercatelo con l'apposita funzione o ricorrendo alla lentina in alto.

IL PRIMO GRANDE CAPITOLO DELLA SICUREZZA DELLO SMARTPHONE

Una trappola alquanto efficace e subdola è quella denominata **ingegneria sociale**.

Come viene perpetrata questa particolare tecnica? Semplice, il cybercriminale avvicina la sua potenziale vittima e fa leva sui suoi sentimenti per sottrargli il cellulare (ad esempio chiede alla sua vittima di prestargli il cellulare per contattare i suoi familiari). L'utente, pensando di fare una buona azione, cede ben volentieri alla richiesta cedendo il proprio smartphone e il criminale informatico, così, ha via libera per carpire **informazioni confidenziali** presenti sul cellulare dell'utente o, peggio ancora, per scaricare **software-spia** e monitorarlo da remoto, senza che questo se ne accorga.

Se vuoi evitare di cadere in una situazione simile a quella che ti ho appena descritto, **guardati bene dal prestare il tuo smartphone** a perfetti sconosciuti o a persone che conosci da poco tempo. Come si dice in questi casi: la prudenza non è mai troppa.

I cybercriminali utilizzano inoltre un'altra tecnica riconducibile all'ingegneria sociale che è alquanto insidiosa: il **phishing**. In cosa consiste? Anche in questo caso si mira ai sentimenti degli utenti, inviando via chat o e-mail dei **link** che rimandano a **siti Web falsi** che spingono il malcapitato a inserire informazioni confidenziali o a scaricare file e applicazioni malevole, magari facendo leva su una **presunta situazione di urgenza**. L'unico modo per evitare di cadere in questa trappola, che rientra nelle tecniche di social engineering, è **ignorare link e messaggi sospetti**.

Come controllare? Imparate a leggere il link: vedrete che è diverso dall'indirizzo del sito istituzionale, pur richiamando qualche elemento.

Un'altra situazione di pericolo si crea quando accediamo alle reti pubbliche è pericolosissimo.

Ricorrere alle VPN (abbreviazione di Virtual Private Network, cioè rete virtuale privata) è un ottimo modo per proteggere la propria privacy quando si naviga sul Web con lo smartphone, e non solo.

Grazie a un particolare sistema chiamato tunneling, infatti, è possibile sia rendere invisibili le proprie attività online a malintenzionati, provider Internet e agli stessi gestori delle VPN, sia mascherare l'indirizzo IP (cioè l'indirizzo identificativo) da cui si accede al Web potendo così superare censure e restrizioni regionali.

Questo risultato viene ottenuto realizzando una sorta di rete privata che risulta accessibile soltanto agli utenti autorizzati. Dal momento che la rete in questione non viene creata tramite l'ausilio di dispositivi fisici, bensì tramite una connessione a Internet, è definita virtuale.

Se vi arrivano messaggi truffa o malauguratamente ne siete stati vittime, denunciate alla Polizia Postale o segnalatelo alle aziende coinvolte.

LE IMPOSTAZIONI DELLE CHIAMATE

Avviso di chiamata

Cosa succede in caso di attivazione? Se sei già impegnato in una conversazione e qualcun altro ti chiama, quest'ultimo riceve il segnale di linea libera, mentre tu ricevi un segnale acustico e sul display compaiono le icone per:

- Mettere in attesa la telefonata in corso e rispondere all'altra
- Chiudere la telefonata entrante e continuare la telefonata in corso.

Come attivare l'avviso di chiamata?

- Aprire il **dialer** (cioè la schermata di composizione dei numeri)
- Pigiare sul pulsante ☰ o **Altro** e selezionare la voce **Impostazioni** dal menu che compare.
- Andare su **Altre impostazioni/Impostazioni aggiuntive**, individuare l'opzione relativa all'**avviso di chiamata** e attivarla o disattivarla spostando la levetta.

ID chiamante

Si può nascondere il proprio numero quando si fa una telefonata (Numero Privato, Sconosciuto).

Per nascondere/ripristinare il proprio ID si deve:

- Aprire l'app **Telefono** (l'icona della **cornetta** che risiede nella schermata Home del dispositivo), o la schermata di composizione dei numeri
- Pigiare sul pulsante ☰ o **Altro** e selezionare la voce **Impostazioni** dal menu che compare.
- Andare su **ID Chiamante** e attivare o disattivare spostando la levetta.

Attenzione: il vostro numero viene nascosto solamente nelle telefonate. Nei messaggi social e negli SMS risulterà sempre visibile.

Chiamate a 3 (conferenze)

È possibile parlare con più interlocutori contemporaneamente.

Ad es. **A** vuole parlare con **B** e **C** contemporaneamente.

Chiama prima **B**, poi quando questo risponde, clicca su **+ AGGIUNGI** e chiama **C** (nel frattempo **B** viene messo in attesa).

Quando anche **C** è in linea, clicca sul tasto **UNISCI**.

Attenzione: Anche se si tratta apparentemente di una telefonata sola, il gestore le addebita come telefonate singole.

Inoltro di chiamata (o deviazione di, trasferimento di)

Avete due telefoni e avete bisogno di ricevere le telefonate solo su uno? Vi si sta scaricando il cellulare e dovete ricevere una telefonata importante?

Basta attivare l'inoltro di chiamata dal telefono **A** al telefono **B** e tutte le telefonate vi arriveranno solo sul telefono **B**.

Per attivare la deviazione di chiamata su **Android**, apri l'app **Telefono** (l'icona della **cornetta** che risiede nella schermata Home del dispositivo), tocca il pulsante **(⋮)** situato in alto a destra e scegli la voce **Impostazioni**, dal menu che compare.

Attenzione: il telefono **A** sosterrà il costo della chiamata a **B** (quindi in questo caso la telefonata sarà pagata due volte: da chi vi chiama e dal vostro telefono **A**)

Messaggi di risposta o risposte automatiche

Si possono dare istruzioni per rispondere automaticamente alle chiamate dopo un certo numero di squilli o inviare un messaggio automatico quando siete impegnati in un'altra conversazione.

La rubrica

Eliminare un numero dalla rubrica: si seleziona il contatto, si clicca su MODIFICA e si scorre la schermata fino a trovare ELIMINA.

Chiamate veloci: o anche numeri PREFERITI. Sono quei numeri che troviamo in un elenco dedicato. Per indicare i nostri contatti preferiti si procede dalla rubrica (selezionare contatto > modifica > preferito) o direttamente dall'elenco che troviamo nella schermata del tastierino (dialer).

LO SPID

Lo **SPID** è il **Sistema Pubblico d'Identità Digitale** con cui accedere ai servizi della Pubblica Amministrazione (e non solo) in modo semplice, sicuro e piuttosto veloce.

È un'unica credenziale (**username e password**) che rappresenta l'identità digitale e personale di ogni cittadino, con cui è riconosciuto dalla Pubblica Amministrazione per utilizzare in maniera personalizzata e sicura i servizi digitali.

Per attivare lo SPID è necessario avere:

- Almeno 18 anni
- Un documento di riconoscimento italiano valido
- La tessera sanitaria o il codice fiscale
- Un indirizzo email e un numero di cellulare

Chi fornisce il nome utente, le password e tutto ciò che serve per creare lo SPID sono i cosiddetti **Gestori di Identità Digitale** (o Identity Provider), aziende riconosciute ufficialmente dalle autorità.

La certificazione dell'identità digitale viene effettuata a pagamento.

Lo SPID è necessario per l'accesso a servizi della Pubblica Amministrazione, quali INPS, Fascicolo Sanitario, Agenzia delle Entrate, ecc., e avviene con tre possibili livelli di sicurezza:

- Il **primo livello** permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente.

- Il **secondo livello** – necessario per servizi che richiedono un grado di sicurezza maggiore - permette l'accesso attraverso un nome utente e una password scelti dall'utente, più la generazione di un codice temporaneo di accesso (one time password), fornito attraverso sms o con l'uso di un'app (fornita dal gestore di identità digitale) fruibile attraverso un dispositivo, come ad esempio smartphone o tablet.

- Il **terzo livello** di sicurezza SPID, oltre al nome utente e la password, richiede un supporto fisico particolare che gestisce delle chiavi crittografiche. Tale supporto può essere una smart card o un dispositivo per la firma digitale remota (HSM).

Come attivare lo SPID

1

Prepara
- un documento di riconoscimento italiano
- la tessera sanitaria o il tuo codice fiscale
- un indirizzo email e un numero di cellulare

2

Accedi al sito di uno dei **gestori di identità digitale** (Identity Provider) riconosciuti e vigilati da AgID.

3

Procedi all'attivazione
- registrati
- effettua il riconoscimento

4

Modalità di riconoscimento
- di persona
- via webcam
- audio-video con bonifico
- CIE, CNS o firma digitale

5

Le differenze tra i livelli di sicurezza
- livello 1
- livello 2
- livello 3

LA CIE

La **Carta di Identità Elettronica (CIE)** è il documento d'identità dei cittadini italiani emesso dal Ministero dell'Interno e prodotto dal Poligrafico e Zecca dello Stato che, grazie a sofisticati elementi di sicurezza e anticontraffazione, permette l'accertamento dell'identità del possessore e l'accesso ai servizi online delle Pubbliche Amministrazioni sia in Italia che nei Paesi dell'Unione Europea.

Oltre ad accertare l'identità del titolare, la CIE è dotata anche di una componente elettronica che – grazie all'adozione delle più avanzate tecnologie disponibili e in conformità alla normativa europea – rappresenta l'identità digitale del cittadino.

I cittadini possono accedere ai servizi online aderenti con le credenziali CIE in maniera semplice e veloce; in funzione del servizio richiesto dal cittadino, l'autenticazione può avvenire attraverso 3 livelli di autenticazione a sicurezza crescente:

livello 1: accesso mediante una coppia di credenziali (username e password),

livello 2: l'accesso prevede, in aggiunta alle credenziali di livello 1, l'impiego di un secondo fattore o meccanismo di autenticazione che certifichi il possesso di un dispositivo (es. codice temporaneo OTP, scansione QR code),

livello 3: è richiesto l'utilizzo di lettore o uno smartphone dotato di tecnologia NFC per la lettura della CIE.

LA POSTA ELETTRONICA

Creare un indirizzo email

Siete proprio sicure di non avere già un indirizzo di posta elettronica?

Se vi ricordate, nel capitolo sulle IMPOSTAZIONI DEL TELEFONO, abbiamo parlato di ACCOUNT.

L'account è l'utente del telefono, la persona, tra le altre cose, che accede al PLAYSTORE o all'APPLESTORE, per scaricare le app. questo utente è identificato, nella quasi totalità delle volte, da un indirizzo email.

Per utilizzare questo mezzo di comunicazione (che ha soppiantato quasi del tutto la posta tradizionale) è necessario avere:

- Un indirizzo (quello con la chiocciolina in mezzo)
- Una password

Se non avete un indirizzo potete crearne uno accedendo ad una delle tante piattaforme che li forniscono gratuitamente: Gmail[1] (di Google), Yahoo!, Email, Hotmail, Libero, Virgilio, TIM, …

Al momento di registrare il nuovo indirizzo, verranno chiesti nome e cognome, un nome utente (quello con la chiocciolina) che dovete inventare voi, una password. Per l'opportuno controllo da parte della piattaforma, vi verrà chiesto un numero di cellulare o di trascrivere un codice contenuto in un riquadro.

La piattaforma controllerà anche che il nome utente non sia già esistente; nel caso vi proporrà alcune soluzioni alternative o vi chiederà di indicarne un altro.

Dopodiché vi invierà un messaggio sul cellulare, per controllo e per l'attivazione.

A questo punto siete pronte per accedere alla vostra casella di posta elettronica da qualsiasi dispositivo collegato ad internet (pc, cellulare, tablet, …) anche non vostro (ma sarebbe preferibile di no, **soprattutto per la sicurezza,** per non lasciare tracce – se non lo sapete, vi informo che ogni operazione sul vostro smartphone, o tablet o PC, lascia tracce più di Pollicino).

[1] https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp

Come accedere alla casella di posta dallo smartphone

Vi sono tantissime app per gestire la posta elettronica. Le piattaforme che vi ho indicato (ma anche quelle che per brevità non ho indicato) hanno una loro app che potete scaricare.

Quando aprite l'app per la prima volta vi verrà chiesto di effettuare il login, cioè l'accesso.

Inserite quindi il vostro indirizzo email e la vostra password. Non dimenticateli, perché sicuramente vi serviranno ancora per eventuali altri servizi offerti dalla piattaforma che avete scelto.

A questo punto siete pronte per utilizzare la posta elettronica.

Come utilizzare la posta elettronica

Di solito vengono fatti corsi completi sull'utilizzo della posta elettronica, quindi sintetizzarli in mezza paginetta è impossibile. Vediamo di provarci e come esercizio vi consiglio di scambiarvi email a vicenda.

- Lettura di una mail che vi è arrivata: basta cliccare sopra e si apre permettendovi di leggere il testo. Controllate sempre se ci sono allegati (segnalati sempre con il simbolo di una graffetta). Per leggere gli allegati è necessario aprirli a loro volta.
- Leggere un allegato: potrebbe capitare che l'allegato non si apre; nella maggior parte dei casi, il formato elettronico dell'allegato richiede che venga installata un'applicazione particolare. In questo caso è meglio chiedere consiglio **(soprattutto per la sicurezza)**.
- Rispondere ad una mail: per rispondere ad una mail si deve cliccare sul simbolo freccia o sulla scritta RISPONDI. Ci sono due possibilità: RISPONDI e RISPONDI A TUTTI; evitate quest'ultima se non sapete quanti sono i destinatari.

  Attenzione che ci sono email nelle quali trovate in fondo la scritta "Non rispondere a questa mail": se anche rispondete non succede niente, ma sappiate che nessuno leggerà quello che avete scritto.
- Scrivere una mail: cercate il simbolo che di solito contiene anche una penna; vi aprirà la schermata con gli elementi del messaggio:

- **A**: è il destinatario, vi si deve inserire un indirizzo valido (cioè con la @). Se è un indirizzo che avete già utilizzato o che avete salvato in rubrica, allora ve lo proporrà.
- **CC**: serve per inserire qualche altro destinatario solo per informarlo.
- **CCN**: copia per conoscenza nascosta; chi la riceve vedrà la mail, ma i destinatari in **A** e in **CC** non sapranno che l'avete inviata anche a questo destinatario.
- **Oggetto**: è il titolo della vostra mail, ciò che contiene. Breve e chiaro.
- **Testo**: è il contenuto
- **Allegati**: per inserire qualcosa che avete salvato sullo smartphone (ad es. una foto) cercate il simbolo della graffetta e poi scegliete cosa allegare)

- Cercare una mail: utilizzate il simbolo della lente e inserite qualche elemento di testo (destinatario, mittente, argomento, parole contenute); vi saranno proposte le mail che contengono quegli elementi.
- Cartelle: le cartelle consentono di organizzare le mail per poterle poi trovare più facilmente. Basta trascinarle dentro. Per creare una cartella utilizzare il menù che trovate in un angolo.
- Cancellare le mail: attenzione che le mail occupano memoria. Cancellate subito quelle che non vi servono, disiscrivetevi dalle mailing list che non vi interessano, e ogni tanto fate un po' di pulizia.

Le email pericolose (fishing, …)

Dedichiamo il prossimo capitolo a questo delicato argomento.

Il consiglio è di non aprirle mai.

Ricordate quel film?

IL SECONDO GRANDE CAPITOLO DELLA SICUREZZA DELLO SMARTPHONE[2] - EMAIL E SMS TRUFFA

Una trappola alquanto efficace e subdola è quella denominata **PHISHING**, pesca di chi abbocca.

L'obiettivo di questo genere di truffa consiste proprio nel **pescare i dati sensibili** di un utente, attraverso false comunicazioni create appositamente per confonderlo.

Le *email phishing* infatti imitano messaggi legittimi, sia nell'aspetto che nel contenuto: messaggi come quelli generalmente provenienti da un fornitore di servizi, un istituto bancario o magari un negozio online.

La procedura classica prevede l'invio massiccio di messaggi di posta elettronica in cui si invita l'utente a visitare una pagina Web attraverso la quale gli vengono rubati il maggior numero possibile di dati personali. Di solito si tratta di **una pagina contraffatta**, che riporta i loghi e la grafica di un social network o di una banca online, e il messaggio inviato all'utente lo invita a visitare la pagina perché "*è necessario confermare i propri dati*"

Messaggi che arrivano via **mail, SMS, Messenger**:

- È successo un problema con la vostra carta di credito, dateci le vostre coordinate
- È stato bloccato il vostro account, confermateci i vostri dati.
- Avete vinto un premio, dateci le vostre coordinate bancarie
- C'è da ritirare un pacco, mandateci 200€.

Si concludono sempre con un link che vi rimanda ad una pagina dove:

- VOI STESSI FORNIRETE I DATI DELLE VOSTRE CARTE BANCOMAT O DEL VOSTRO CONTO CORRENTE
- OPPURE VI DARANNO UN IBAN AL QUALE INVIARE DENARO
- OPPURE SCARICHERANNO VIRUS, SPYWARE O UN MALWARE NEL VOSTRO SMARTPHONE.

Come riconoscerle, soprattutto se imitano alla perfezione siti di grandi aziende?

- Lingua italiana infarcita di errori

[2] Leggere attentamente l'articolo di Aranzulla "Come riconoscere una mail falsa"

- Link ad un indirizzo che non è quello ufficiale dell'azienda, ma lo ricorda soltanto
- Presenza dell'indirizzo di altri destinatari oltre al vostro.

E per finire: secondo voi c'è qualcuno al mondo così generoso da regalarvi soldi con un messaggio, senza voler niente in cambio?

Se vi capita di essere vittime di una cosa del genere:

- Se avete fornito le vostre credenziali, MODIFICATE SUBITO LA PASSWORD
- Modificate la password anche del vostro account di posta
- Andate subito a fare denuncia alla POLIZIA POSTALE.

Se volete farvi una cultura, visitate il sito della POLIZIA POSTALE.

Ricordatevi che le esche, più sono succulente, più nascondono ami acuminati.

Se leggi richieste di accesso a un portale di home banking (conto corrente online), di un servizio per la reimpostazione di una password o altre credenziali, se ti chiedono documenti o ti avvisano che hai del denaro da riscuotere e non sei stato tu a richiedere in prima persona la ricezione di un messaggio del genere, **NON CLICCARE SUI LINK** e cestina immediatamente il messaggio.

C'è un'elevata probabilità che si tatti di un **tentativo di phishing**, in cui, oltre a replicare la tua identità, gli hacker potrebbero accedere al tuo conto corrente. Ricorda: la tua banca, o qualsiasi altro istituto bancario e postale, non chiede mai via email dati sensibili dell'utente, così come non lo fanno le diverse piattaforme online, note e serie, sulle quali hai aperto un account.

Ricordate poi una cosa fondamentale: Banche, Posta, Assicurazioni, ***NON vi chiederanno mai dati per mail o SMS o per telefono****. Al massimo vi diranno che c'è una comunicazione per voi nella vostra area riservata. A questo punto andate sul sito istituzionale, accedete alla vostra area riservata e fate quello che vi viene richiesto.*

Vi mostro una mail delle Poste che raccomanda la massima attenzione e dà consigli utili:

Gentile Marco,

con l'evoluzione dei mezzi digitali anche i tentativi di truffa sono diventati più raffinati, ma è sufficiente fare attenzione ad alcuni dettagli e, soprattutto, non

condividere mai dati riservati o codici di accesso con nessuno, per evitare di cadere vittima di una frode:

***Ricorda che Poste Italiane S.p.A. e PostePay S.p.A. non chiedono mai** in nessuna modalità (e-mail, sms, chat di social network, operatori di call center, ufficio postale e prevenzione frodi) e per nessuna finalità:*

Le tue credenziali di accesso al sito poste.it e alle App di Poste Italiane (il nome utente e la password, il codice PosteID);

I dati delle tue carte (il PIN, il numero della carta con la data di scadenza e il CVV);

I codici segreti per autorizzare le operazioni (codice PosteID, il codice conto, le OTP-One Time Password ricevute per sms).

***Non ti sarà mai richiesto** di disporre transazioni di qualsiasi natura paventando falsi problemi di sicurezza sul tuo Conto o la tua Carta tantomeno spingendoti a recarti in Ufficio Postale o in ATM per effettuarle. Se qualcuno spacciandosi per un operatore di Poste Italiane S.p.A. o PostePay S.p.A., ti dovesse chiedere tali informazioni, puoi essere sicuro che si tratta di un tentativo di frode, quindi non fornirle a nessuno;*

***Controlla sempre l'attendibilità di una e-mail prima di aprirla:**verifica che il mittente sia realmente chi dice di essere e non qualcuno che si finge qualcun altro (ad esempio controlla come è scritto l'indirizzo e-mail da cui ti è arrivata);*

***Non scaricare gli allegati delle e-mail sospette** prima di aver verificato che il mittente sia noto o ufficiale;*

***Non cliccare sul link contenuto nelle e-mail sospette**; se per errore dovesse accadere, non autenticarti sul sito falso, chiudi subito il web browser;*

***Segnala a Poste Italiane eventuali e-mail di phishing**inoltrandole all'indirizzo antiphishing@posteitaliane.it. Immediatamente dopo cestinale e cancellale anche dal cestino;*

***Digita direttamente l'indirizzo Internet https://www.poste.it/**nella barra degli indirizzi del web browser per visitare il sito di Poste Italiane;*

***Utilizza le App ufficiali** di Poste Italiane S.p.A e Postepay S.p.A per usufruire anche del servizio gratuito di push notification ed essere informato in tempo reale sulle operazioni di pagamento effettuate con il tuo Conto Corrente e le tue Carte di pagamento. In alternativa attiva il servizio di notifica tramite SMS sul tuo telefono cellulare, gratuito per i pagamenti su siti internet e su app. Per ulteriori informazioni*

sul servizio consulta i fogli informativi nella sezione Trasparenza Bancaria del sito Poste.it.

A proposito di link e allegati presenti nelle email, sebbene la maggior parte dei client di posta elettronica siano in grado di bloccare i file eseguibili per i sistemi operativi Windows, macOS e Linux (quelli con estensioni .exe, .dmg, .java, .vba, ecc.) quando non si è certi della provenienza di un messaggio è sempre bene non scaricare documenti inclusi e non aprire i link presenti nel testo. Potrebbero contenere virus, spyware e malware di vario genere. Da email sospette, non scaricare nemmeno archivi .zip, .rar, oppure file di Office, PDF o immagini.

Adesso ci sono anche le telefonate

Ora giungono telefonate da un numero che appare come quello del call center della vostra Banca e vi chiedono di controllare o autorizzare un'operazione che loro definiscono "sospetta".

È una truffa!

Come potete difendervi?

Rispondete così: "La ringrazio. Guardi in questo momento sto facendo un lavoro. Se mi lascia il suo nominativo ed il numero da chiamare, la richiamo tra 10 minuti".

Dal sito della BPM

Una delle tipologie di truffe più recenti è stata definita come la "Truffa dello storno", principalmente rivolta a coloro che hanno installato sul cellulare l'applicazione della propria banca.

La truffa inizia con un SMS inviato dai truffatori, spacciato per comunicazione ufficiale della banca e con il quale la vittima viene informata che è stata richiesta autorizzazione per la disposizione di un bonifico. Per negare l'autorizzazione è necessario cliccare su un link. Il messaggio è solitamente seguito da una telefonata di un sedicente operatore bancario che chiede informazioni relative alle operazioni bancarie effettuate sul conto della vittima, la invita a cliccare sul link e a seguire le istruzioni riportate nella procedura di storno.

La procedura di storno implica l'installazione di applicazioni che permettono la condivisione dello schermo (come TeamViewer, remote desktop, ecc.) e che

consentono ai truffatori di controllare da remoto il dispositivo del cliente, accedere al suo conto bancario, ed effettuare operazioni malevole.

Al termine di ogni operazione la vittima viene avvisata, tramite sms, che l'operazione è stata stornata con successo. Un'altra variante di truffa prevede il contatto telefonico o via SMS da parte del truffatore, che informa la potenziale vittima che i suoi soldi sono in pericolo e che è necessario trasferirli su un nuovo conto corrente di una presunta banca partner: coglie quindi l'occasione per assisterla nella creazione del nuovo conto corrente, appropriandosi delle credenziali di accesso che utilizzerà in seguito per svuotare il nuovo conto.

In alternativa, il truffatore può chiedere alla potenziale vittima di inviargli un suo documento d'identità, insieme a una foto del suo viso e ai suoi dati personali (ad esempio nome, cognome, email, indirizzo), per richiedere in totale autonomia l'apertura del nuovo conto corrente a suo nome. Chiede quindi alla potenziale vittima di effettuare un bonifico sul "suo" nuovo conto, non fornendogli mai le credenziali dello stesso, di cui è in possesso fin dall'inizio.

Wangiri

Il Wangiri è la truffa dello squillo telefonico: riceviamo un solo squillo, proveniente di solito da un numero estero, e se chiamiamo tale numero per capire chi fosse si attiva una segreteria telefonica, oppure non sentiamo nulla dall'altro capo del telefono. Però ci costa, e anche parecchio, perché il numero internazionale che abbiamo chiamato è in realtà un numero a tariffazione speciale che può arrivare anche a diverse decine di euro al minuto.

Ci sono varianti di Wangiri ancora più pericolose, che invece di svuotarci il conto telefonico subito attivano a nostra insaputa servizi in abbonamento. In questo modo ci accorgiamo di essere stati truffati solo in un secondo momento ed è assai difficile capire chi è il colpevole.

IL CALENDARIO

Su uno smartphone trovate sempre un calendario da consultare o in cui salvare ricorrenze ed appuntamenti. Ci sono anche app di calendari, più o meno colorati e con altre funzionalità più o meno utili.

Le ricorrenze

Si possono salvare anniversari, compleanni, onomastici e predisporre uno o più allarmi che ci avvisino della scadenza. Possiamo anche fare in modo che si ripetano ogni anno

I nostri appuntamenti e le scadenze

Possiamo salvare gli appuntamenti, le visite, le scadenze aggiungendo anche altri elementi utili oltre a data e ora:

- La posizione (che può attivare il navigatore)
- Invitare altre persone (inviando loro una mail con i dati del calendario)
- Inserire uno o più allarmi (per il giorno stesso o per i giorni precedenti)
- Una nota (ad esempio se devo portare qualcosa o preparare qualcosa o un numero di telefono)
- Posso fare in modo che si ripetano a cadenza giornaliera, settimanale, annuale, anche per un periodo limitato

Come fare?

- Si va sul giorno e si clicca su un più o su un icona simbolo dell'evento
- Si digita la descrizione
- Si compilano successivamente gli altri campi che interessano
- Si SALVA

Consultazione

Ci sono diverse viste (anno, mese, settimana, giorno, icone o agenda) e ci sono anche i widget (quei simpatici riquadri dove si vede un po' del contenuto della funzione).

I SOCIAL

Ma quanti social ci sono?

Decine e decine, se non centinaia.

Ma i più usati sono Facebook, Youtube, Whatsapp.

Servono per mettere in contatto le persone, per veicolare messaggi, ma soprattutto per raccogliere dati delle persone e venderli ad aziende e Stati; sì, avete letto bene: Stati.

Avete mai sentito parlare di Big Data? Servono a chi li compra per conoscere e studiare gusti e abitudini della gente, fare di conseguenza le migliori scelte in termini di prodotti e, perché no?, orientare le persone. Non solo in cosa comprano, ma anche in cosa pensano o scelgono.

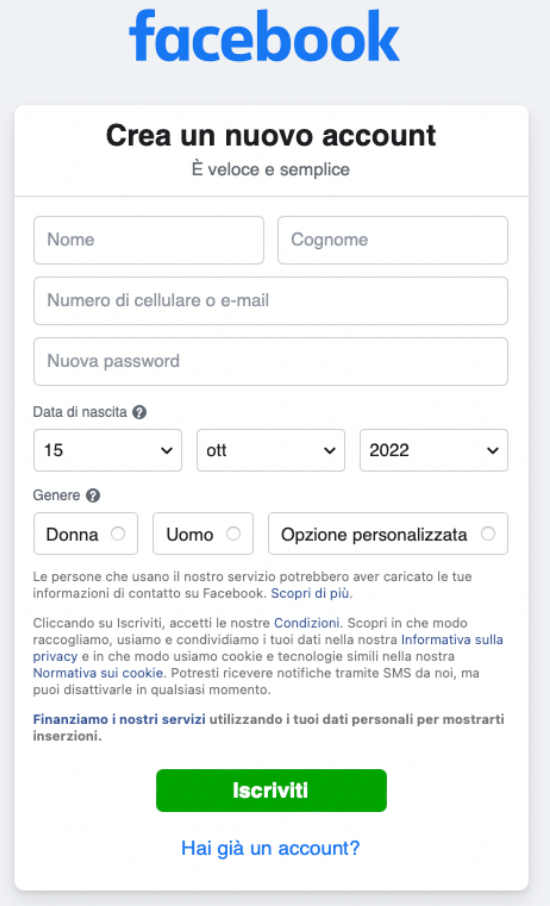
FACEBOOK

Come registrarsi

Bastano pochi dati per registrarsi e creare il proprio Account (così si dice).

Controlli? Pochi pochi.

Ma una cosa importante scritta in fondo e in piccolo: "Finanziamo i nostri servizi utilizzando i tuoi dati personali per mostrarti inserzioni". E basta? Mah …



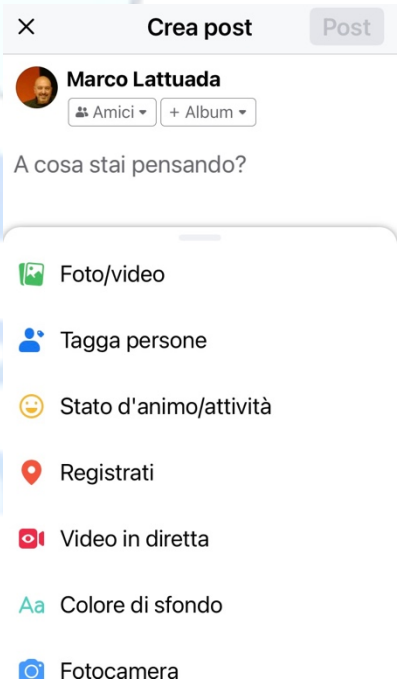
Cosa si può fare su Fb?

- Lentina per cercare qualcosa, compresi gli amici
- Icona di Messenger, servizio di messaggistica di Fb
- Scrivere un post, accompagnandolo con foto e video
- Registrarsi in un posto o ad un evento
- Scorrere i post dei nostri amici o di chi seguiamo
- Passare alle pagine delle notifiche o delle impostazioni

I Post

Cosa posso fare con un post?

- Scrivere un mio pensiero
- Inserire foto e video
- Citare persone (anteponendo il simbolo #)
- Dire come mi sento o cosa sto facendo
- Registrarsi in un posto o ad un evento (FB propone in automatico quelli più vicini)
- Fare video in diretta
- E tante altre cose



Le notifiche

In questo spazio troviamo l'annuncio di nuovi post o azioni dei nostri amici, suggerimenti o richieste di amicizia, notizie dei compleanni, ecc.

Il Menù e le Impostazioni

Il menù contiene i collegamenti rapidi al contenuto del nostro account: pagine che seguiamo, amici e gruppi, lo spazio mercato, ricordi, elementi salvati, …

Ma una cosa importante è la rotellina delle Impostazioni, che trovate in alto:

- Il nostro Account, con i dati che abbiamo inserito e possiamo modificare, compresa la password.
- Le Preferenze

- Pubblico e visibilità: “Controlla chi può vedere i tuoi post, le tue storie e il tuo profilo”
- Autorizzazioni: “Gestisci quali informazioni usa Fb per migliorare la tua esperienza, come i tuoi interessi e la tua posizione”.

  Se entrate nelle impostazioni della posizione e selezionate MAI, trovate sotto questa simpatica frase: “Non riceveremo la posizione esatta di questo dispositivo, ma usiamo comunque informazioni come il tuo indirizzo IP (praticamente la targa del dispositivo, *ndr*) per calcolare la tua posizione”
- Le tue informazioni
- Informazioni varie su privacy e normative

Come chiedere l’amicizia o accettare l’amicizia

Quando si trova una persona che si conosce si clicca sul tasto AGGIUNGI e si invia la richiesta di amicizia

Se una persona mi invia una richiesta di amicizia, trovo la comunicazione nella pagina delle NOTIFICHE.

Trovo due tasti: CONFERMA e RIMUOVI

WHATSAPP (e altri servizi di messaggistica)

Per utilizzare Whatsapp è necessario scaricare l’app gratuita e dare alcune indicazioni.

Per registrarsi sono necessari alcuni passaggi:

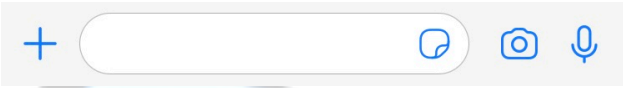
1. Clicca sul pulsante “ACCETTA E CONTINUA” per accettare i termini di servizio.
2. Scegli il paese dal menù a tendina per selezionare il corretto prefisso internazionale e inserisci il numero di telefono che vuoi registrare nell’apposito spazio. Clicca sul bottone “AVANTI”.
3. Controlla che il numero inserito sia corretto e clicca su “OK”.
4. A questo punto WhatsApp ti manderà un codice per confermare la registrazione al numero telefonico da te inviato. Inserisci il codice numerico nello spazio dedicato.
5. Fornisci tutti i consensi necessari.
6. Inserisci il nickname che vuoi utilizzare e scegli la tua immagine di profilo e clicca su pulsante “AVANTI”.

7. Scegli la frequenza con cui effettuare i backup, l'account su cui effettuarlo e clicca su "FINE".

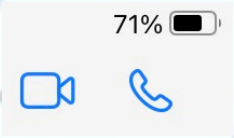
Cosa fare con WA

Whatsapp individua automaticamente i contatti della rubrica che si sono registrati su WA (in caso contrario li si può invitare) e mi permette di inviare loro:

- Foto scattate al momento
- Foto o video salvati nella mia galleria
- Documenti
- Posizione
- Contatti
- Messaggi audio



Posso anche fare videochiamate o telefonate



Il mondo delle faccine

Quanto usiamo le emoji (o emoticon o, più simpaticamente "faccine") nelle nostre chat?

Ci permettono di esprimere un'emozione, fare un commento, sintetizzare un pensiero, con un semplice disegnino.

Impariamo ad usarle e ad usarle bene ;-).

Memorizzare le chat WA

Non tutto quello che ci scambiamo su WA merita di essere destinato ad imperitura memoria. Quindi ogni tanto svuotiamo queste benedette chat, anche singolarmente, oppure dalle Impostazioni.

Se però vogliamo salvare qualcosa abbiamo due soluzioni:

1. Eseguire il backup delle chat

Vai su WhatsApp > tocca Altre opzioni > Impostazioni > Chat > Backup delle chat > ESEGUI BACKUP.

2. Esportare la cronologia chat

È possibile usare la funzione Esporta chat per esportare una copia della cronologia chat da una chat individuale o di gruppo.

Apri la chat individuale o di gruppo.

Tocca Altre opzioni > Altro > Esporta chat.

Scegli se includere i file multimediali.

A questo punto, la tua cronologia chat verrà allegata a un'email sotto forma di file .txt.

Un po' di cautela sui Social

Nella nostra vita adottiamo tante cautele:

- Non apriamo la porta a sconosciuti
- Chiudiamo la porta a chiave
- "Non accettare caramelle dagli sconosciuti"
- Non diciamo sempre quello che pensiamo

Con i social ci si deve comportare nello stesso modo. Anche se ci troviamo da soli nella nostra casa e non abbiamo di fronte nessuno, fare qualcosa con i social è come farlo in piazza.

Quindi:

- Forse è meglio non dire che siamo in vacanza e postare foto di posti ameni
- Stiamo MOLTO attenti a inviare foto di minori
- Non facciamo i leoni da tastiera (quelli che spargono odio e zizzania proprio perché sono soli)
- Evitiamo a nostra volta queste persone

IL TERZO GRANDE CAPITOLO DELLA SICUREZZA DELLO SMARTPHONE – I MOSTRI DEI SOCIAL

Sui Social circolano liberamente dei mostri.

Stiamo molto attenti noi stessi e diamo un occhio anche a figli e nipoti.

Qui faccio un elenco, ma vi invito caldamente ad andare a leggere gli articoli sull'argomento, soprattutto quelli di Polizia Postale e Carabinieri.

- Le **fake news:** non fermiamoci al titolo, leggiamo tutto con criterio e, se è il caso, verifichiamo su internet. Ricordiamoci che le fake news possono rovinare vite ed aziende.
- Che fine fanno foto e video messe in rete?
- Il grande campionario delle **truffe** (leggi attentamente il prossimo paragrafo)
- Sexting minorile (e non)
- **Revenge porn**
- Istigazione al suicidio
- Bullismo on line

Le truffe più comuni sui Social (soprattutto Facebook)

- La truffa "Chi ha visitato il mio profilo". In sostanza, ricevi una notifica su Facebook che ti invita a installare un software grazie al quale potrai scoprire chi visualizza il tuo profilo, quando in realtà stai scaricando un virus che può compromettere i tuoi dati personali. Al momento, infatti, non è possibile sapere chi visualizza il tuo profilo Facebook.
- Le truffe via webcam (chiamate anche "sextortion"). Con questo tipo di truffa i criminali risalgono ai video più intimi di una persona, minacciandola di pubblicarli e chiedendo una somma di denaro in cambio.
- Concorsi falsi, accesso a video privati di celebrità o ad articoli speciali, cambio di colore del profilo Facebook o quiz vari. Questi stratagemmi utilizzano lo stesso sistema della truffa relativa alle visite al profilo. Per ottenere i vantaggi promessi, dovrai scaricare un programma che installerà un virus sul dispositivo per accedere ai tuoi dati personali.
- Richieste di amicizia da account falsi. Quando ricevi una richiesta di amicizia da una persona sconosciuta fai sempre molta attenzione, circa il 10% dei profili Facebook è falso.

Stratagemmi sentimentali[3], campagne di disinformazione o tentativi di ottenere i tuoi dati sono le truffe più comuni messe in atto utilizzando degli account falsi. Alcuni profili sono addirittura gestiti in modo completamente automatico tramite robot e non da persone reali. Questo tipo di truffa può avvenire anche tramite l'account hackerato di uno dei tuoi amici su Facebook.

- Messaggi sospetti su Facebook Messenger. Se ricevi un messaggio sospetto da uno dei tuoi contatti con note del tipo "Guarda, questo ti assomiglia!" insieme a un link, evita di cliccare sul link: potrebbe trattarsi di un tentativo di phishing. In generale, quando ricevi un messaggio impersonale o strano da uno dei tuoi contatti su Messenger che ti invita a cliccare su un link, ti chiede denaro o ti annuncia che hai vinto un concorso, è molto probabile che si tratti di qualcuno che sta cercando di truffarti.

Come riconoscere un account Facebook falso

Una persona che non conosci ti ha contattato su Facebook? Questo potrebbe essere il primo segnale di allarme. Ecco alcuni consigli per capire se un profilo Facebook è autentico:

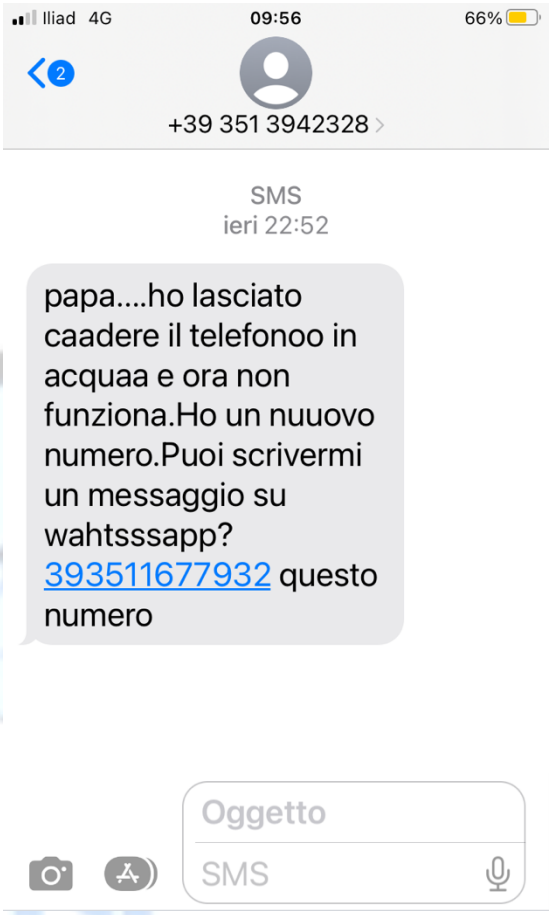
- Copia l'URL della foto del profilo in Google Immagini. In questo modo, scoprirai se il proprietario dell'account ha utilizzato una foto presa da Internet.
- Verifica che l'URL del profilo corrisponda al nome dell'account. Se l'account è stato violato, questi due dati potrebbero essere differenti tra loro.
- Dai un'occhiata alle informazioni disponibili sull'account, compresi i gruppi di cui la persona fa parte, gli amici e la sua posizione. Se gli amici sembrano sparsi in tutto il mondo o se le informazioni visibili sono poche, si tratta probabilmente di un profilo falso.
- Nel caso delle pagine Facebook, assicurati che siano verificate. Se hanno pochi o nessun post, sono piene di errori ortografici o hanno pochi "mi piace", ti consigliamo di fare sempre molta attenzione.

Mi raccomando:

[3] In questo tipo di truffe i frodatori prendono di mira le vittime su app e siti di incontri, social media o via email. **Lavorano per mesi** spacciandosi per veri amanti, cosi' da ottenere la **fiducia** della vittima, la quale e' convinta di star costruendo una **relazione autentica**. A un certo punto, con una scusa, viene chiesto denaro, regali o dettagli del conto corrente. Le richieste aumentano, ma **il denaro non viene mai restituito**e non si incontra mai il "partner".
https://vocearancio.ing.it/truffe-sentimentali-riconoscerle-e-difendersi/?intcmp=Cross-dem-lp_button-bd-Love%20Fraud

I messaggi di figli o parenti

Capita di ricevere messaggi (SMS o Whatsapp) con richieste di aiuto da parte dei figli, come questo che ho ricevuto pochi giorni fa:



È FALSOOOOO!

Guardate quanti errori di ortografia o di scrittura.

Non richiamate quel numero e non mandategli messaggi.

Lo scopo è:

Farvi chiamare numeri a tariffazione speciale

Attivare a nostra insaputa abbonamenti a servizi telefonici a pagamento

Creare un canale di conversazione, una porta aperta che permette al cybercriminale di costruire una storia credibile (perché magari arriva a conoscere il nome di un figlio, di un genitore, un indirizzo, la sede di lavoro e così via) su cui basare possibili e prevedibili futuri attacchi.

Come detto, la soluzione è solo una: non cliccare sui link, non scrivere, non richiamare e dubitare continuamente. E magari provare a contattare il figlio sul numero che già si ha, il suo vero numero. Sicuri che risponderà come sempre.

Come potete difendervi?

Non cliccate sui link, non scrivete, non richiamate e dubitate continuamente. E magari provate a contattare il figlio o la figlia sul numero che già si ha, il suo vero numero. Vedrete che risponderà.

Revenge porn e Sexting minorile

Sono due fenomeni che possono essere devastanti per una persona. Ve ne parlo perché possono colpire ragazzi e ragazze vicino a voi.

Il Sexting minorile è lo scambio di messaggi, audio, immagini o video, in special modo attraverso smartphone o chat di social network, a sfondo sessuale o

sessualmente espliciti, comprese immagini di nudi o di seminudi, di soggetti minorenni.

Queste immagini possono essere frutto di un inganno o di una scelta deliberata ("Mandami una tua foto nuda/o come prova d'amore"), ma il guaio è se finiscono in rete e sfuggono ad ogni controllo.

Il Revenge porn è la condivisione pubblica di immagini o video intimi tramite Internet, senza il consenso dei protagonisti degli stessi.

Può nascere da un desiderio di vendetta ("Mi hai lasciato? Allora faccio vedere a tutti quanto sei … ") oppure si tratta di immagini immortalate ad insaputa del soggetto (telecamere nascoste) o frutto di violenze (droga dello stupro).

Con il termine, quindi, ci si riferisce al più ampio fenomeno della "pornografia non consensuale".

In entrambi i casi, quando il soggetto si rende conto di quanto sta subendo, subisce un tracollo psicologico che può sfociare in una vera e propria devastazione e spesso in gesti inconsulti.

Il Manifesto di Parole O-Stili

1. **Virtuale è reale**

   Dico e scrivo in rete solo cose che ho il coraggio di dire di persona.

2. **Si è ciò che si comunica**

   Le parole che scelgo raccontano la persona che sono: mi rappresentano.

3. **Le parole danno forma al pensiero**

   Mi prendo tutto il tempo necessario a esprimere al meglio quel che penso.

4. **Prima di parlare bisogna ascoltare**

   Nessuno ha sempre ragione, neanche io. Ascolto con onestà e apertura.

5. **Le parole sono un ponte**

   Scelgo le parole per comprendere, farmi capire, avvicinarmi agli altri.

6. **Le parole hanno conseguenze**

   So che ogni mia parola può avere conseguenze, piccole o grandi.

7. **Condividere è una responsabilità**

   Condivido testi e immagini solo dopo averli letti, valutati, compresi.

8. **Le idee si possono discutere. Le persone si devono rispettare**

   Non trasformo chi sostiene opinioni che non condivido in un nemico da annientare.

9. **Gli insulti non sono argomenti**

   Non accetto insulti e aggressività, nemmeno a favore della mia tesi.

10. **Anche il silenzio comunica**

    Quando la scelta migliore è tacere, taccio.

FOTO E VIDEO

Fare foto e video con lo smartphone è molto semplice e (quasi) gratuito.

Hanno l'inconveniente di occupare tanto spazio della memoria del dispositivo.

Vediamo come comportarci.

La fotocamera

Abbiamo già visto che le app di messaggistica ci consentono di scattare foto senza passare dalla fotocamera.

Utilizzare la fotocamera ci consente di non solo di fare foto e video, ma anche di regolare alcune variabili:

- Scegliere le impostazioni che si preferiscono (dal menù Impostazioni – rotella – che c'è in alto)
- Selezionare l'obiettivo fronte o retro (se ci sono)
- Uso del flash (vi consiglio di lasciarlo su AUTOMATICO
- Ritardo dello scatto (così con un meraviglioso scatto ci mettiamo in posa con gli altri)
- Regolare la luminosità
- Fare foto particolari, come panoramiche o foto ravvicinate.

Un suggerimento finale: ogni tanto, diamo una pulitina alle lenti della camera.

La Galleria

Foto e video vengono salvate nella app GALLERIA (o FOTO).

Si possono organizzare in Album, evidenziare come Preferite, ordinare per data o per località.

Simpatica può essere la possibilità di modificare la foto:

- Ritaglio: consente di eliminare parti della foto (compare un orribile cartello pubblicitario? Via!). La funzione consente di eliminare le parti esterne trascinando i cursori laterali.
- Colore ed effetti speciali
- Scrittura: aggiungere scritte o evidenziare zone

Ogni smartphone ha il suo menù, quindi vi suggerisco di navigare un po' e fare delle prove.

Parliamo di MEMORIA

Come abbiamo detto, lo smartphone ha due tipi di memoria:

- RAM (o di lavoro): paragoniamola alle cose che teniamo sul tavolo
- Archivio o Storage: le cose che teniamo negli armadi

Ma se la memoria si sta esaurendo, come posso risolvere il problema?

1. Le memorycard

Molti dispositivi Android hanno spazi dove inserire questi rettangolini piatti.

Il cellulare vi chiederà spesso se quello che avete fatto volete salvarlo nella memoria del telefono o nella memorycard.

La comodità di questo aggeggino è che si può estrarre e leggere anche su un PC, nel quale si possono trasferire, ad esempio, foto e video.

2. Il cloud

È un servizio che consente di acquistare a pagamento spazio di memoria in magazzini virtuali (ma non poi tanto) cosiddetti server, che costituiscono una rete globale.

Due vantaggi: è sempre disponibile e non si perde quello che si salva.

3. Pendrive o chiavetta

Su molti cellulari è possibile inserire una chiavetta esterna, sulla quale copiare o trasferire foto, video e altri documenti.

In genere si inserisce nello stesso buco dove va il caricabatterie e il cellulare poi guida per effettuare tutte le operazioni di installazione e gestione.

La chiavetta si può poi leggere con il cellulare stesso o con un PC (sul quale anche salvare)

4. PC

Un'ultima soluzione è quella di importare foto e video direttamente su un PC.

Con un cavo USB o per mezzo del bluetooth si collegano i due dispositivi e dal PC si utilizza la funzione ESPLORA FILE per individuare foto e video e salvare quello che interessa.

Per finire: non è il caso ogni tanto di fare pulizia di tutte le foto inutili?

Andiamo anche a controllare nelle impostazioni quali sono le applicazioni che occupano più memoria e valutiamo se svuotarle un po' o no.

IL QUARTO GRANDE CAPITOLO DELLA SICUREZZA DELLO SMARTPHONE – APPROFONDIMENTO SULLE FAKE NEWS

Torniamo a parlare delle fake news per dare qualche notizia in più. Ed è anche un omaggio al grande Piero Angela, grande antagonista delle fake news; aveva anche fondato un'organizzazione che ha tra i suoi scopi combattere questo fenomeno (visita il sito www.cicap.org).

Le Fake News

Le fake news sono notizie false che vengono diffuse deliberatamente. A prima vista, le fake news assomigliano alle notizie o ai reportage classici. Tuttavia, gli autori non si preoccupano di adempiere all'obbligo di informazione; tramite le fake news, cercano invece di manipolare l'opinione pubblica scatenando emozioni come la paura e l'insicurezza.

Gruppi con opinioni estreme riguardo a temi discutibili, xenofobi o con una visione del mondo un po' particolare abusano di internet per fomentare gli animi e diffondere opinioni unilaterali o manipolare i fatti (fatti alternativi). Anche il mondo della politica e della scienza sono spesso bersaglio delle fake news.

Le fake news si diffondono principalmente attraverso le reti sociali, come Facebook, Twitter, Instagram, YouTube, o servizi di messaggeria come Telegram o WhatsApp. Ricevono molta attenzione soprattutto quando evocano forti emozioni. Le notizie false che seminano dubbi, ridicolizzano una tesi o escludono le minoranze ricevono facilmente un «like» o vengono condivise e commentate più rapidamente. Di conseguenza, si diffondono in brevissimo tempo.

Come riconoscere le Fake News?

TITOLI

Sono l'elemento che attira di più anche perché, spesso, l'utente medio non si sofferma sul resto. Per questo le fake news fanno leva su titoli esagerati e altisonanti, scritti in maiuscolo e con un uso eccessivo di punti esclamativi. Dubita di affermazioni contenute in un titolo che possono sembrare troppo esagerate: c'è un'alta probabilità che siano false.

URL

Spesso vengono storpiate le url di siti di informazione, così da renderle credibili a un occhio poco attento. Una notizia riportata da una url molto simile a quella di un sito esistente potrebbe indicare che siamo davanti a una fake news. Tra i casi più famosi, ricordiamo "Il fatto quotidaino",

che gioca sull'inversione della I e della D di "quotidiano" per confonderlo con la testata. Confronta la url con quella della fonte attendibile.

IMMAGINI

Anche le immagini, così come i titoli, sono spesso pensate per catturare l'attenzione del lettore. Le notizie false contengono frequentemente foto o video ritoccati, altre volte invece le immagini possono essere autentiche, ma prese fuori dal loro contesto. Come consiglia anche Facebook, è possibile fare una ricerca tramite immagine per verificarne l'origine: uno strumento molto utile in questo senso è il sito TinEye.

FORMATTAZIONE ED ERRORI

Gli errori capitano a tutti, ma i siti che diffondono fake news sono spesso zeppi di errori di battitura o hanno formattazioni di testo anomale. Se il contenuto che stai leggendo presenta questi due elementi, meglio farsi venire qualche dubbio prima di condividerlo.

FONTI

Anche se il tempo a disposizione non è tanto, assicurati che la notizia provenga da una fonte di cui ti fidi e o da un sito attendibile. Se la notizia viene riportata da un'organizzazione che non conosci e, soprattutto, se è l'unica a riportarla, dubita. Visita la sezione "informazioni" della pagina, così almeno da avere un'idea di chi c'è dietro.

DATE

Controlla la data di pubblicazione della notizia, spesso potrebbe essere vecchia e riproposta con il solo intento di acchiappare qualche like sui social. Anche le date riportate all'interno del contenuto (come quelle degli avvenimenti, per esempio) potrebbero essere sbagliate e la loro cronologia potrebbe non avere alcun senso.

TESTIMONIANZE

Verifica le fonti e assicurati che siano attendibili. Se si fa riferimento a esperti di cui non viene fatto il nome o se mancano le prove, probabilmente si tratta di una notizia falsa.

ALTRE FONTI

Una notizia vera viene sempre riportata da più di una fonte. Questo significa che se nessun altro sito riporta la stessa notizia, probabilmente siamo davanti a un falso. Se la notizia è stata ripresa da diversi siti che ritieni attendibili, allora è più probabile che sia vera.

È UNO SCHERZO?

Esiste una serie di siti satirici che pubblicano notizie false, al solo scopo di far divertire. Anche se a volte può risultare difficile distinguerle dalle notizie vere, è bene almeno porsi delle domande. Controlla la fonte e verifica che non sia già nota per le sue parodie.

INTENZIONALMENTE FALSE

Attenzione perché alcune notizie sono intenzionalmente false. Utilizza le capacità critiche quando leggi le notizie e condividile sono se non hai dubbi sulla loro veridicità.

Considerazioni sulle Fake News

Alcune osservazioni:

- Spesso leggiamo quello che vogliamo sentirci dire
- C'è gente che guadagna montagne di soldi con i LIKE e con i CLICK
- Ci sono fake news che possono rovinare aziende o persone
- Chi scrive su un argomento, ha la competenza per trattarlo?

SOS EMERGENZA - AREU

AREU (WHERE ARE U?)

E' un'app per l'emergenza collegata alle Centrali del Numero Unico dell'Emergenza (NUE) 112 della Lombardia. Permette di effettuare una chiamata di emergenza con il contestuale invio della posizione esatta del chiamante.

Attivo in Lombardia tutti i giorni, 24 ore su 24, è gratuito sia da telefono fisso che da mobile - con o senza scheda (si può chiamare anche se si è esaurito il credito).

Garantisce la localizzazione e l'identificazione del chiamante e una gestione centralizzata delle richieste di soccorso verso:

- le forze di sicurezza
- i Vigili del Fuoco
- il Soccorso Sanitario

In cosa consiste l'eccezionalità di questa app?

Sta nel fatto che "dialoga" con il sistema informativo delle centrali pubbliche del NUE 112 della Lombardia permettendo una localizzazione puntuale anche nei casi in cui il chiamante non sa o non è in grado di fornire dati precisi sulla sua posizione.

Come funziona l'app?

L'app rileva la posizione tramite GPS e/o rete dati e la mostra sul telefono; al momento della chiamata la posizione viene trasmessa tramite rete dati o tramite SMS se la rete dati non è disponibile. Il doppio canale di trasmissione assicura sempre l'invio della posizione ogniqualvolta sia possibile effettuare una telefonata.

E se non posso parlare?

L'app consente di effettuare volontariamente una chiamata muta; con appositi pulsanti è possibile segnalare il tipo di soccorso richiesto.

È utile sempre?

Sì. L'informazione sulla posizione del chiamante è disponibile al NUE-112 della Lombardia ma Where ARE U è utile sempre perché indica la località e la via in cui si è o la sola posizione GPS, se non si è in ambito urbano. Queste informazioni sono quelle da riferire sempre a qualsiasi servizio di emergenza per consentire di effettuare un intervento.

Come faccio ad averla?

WHERE ARE U è disponibile per IOS, ANDROID e WINDOWS PHONE.

La trovi su www.areu.lombardia.it oppure su Apple app store, Google Play store o Windows phone app store, cercando "112 Where ARE U".

Posso essere localizzato se chiamo senza usare l'app?

Il NUE-112 tramite il CED Interforze del Ministero dell'Interno riesce a conoscere un'area di probabilità in cui si trova l'utente che chiama con cellulare, ma non l'esatta posizione.

Se non uso l'app e chiamo facendo il 112 cosa succede?

Viene effettuata solamente la chiamata vocale senza l'invio delle coordinate della posizione

Devo avvisare che chiamo con l'app?

No Il sistema informatico del NUE segnala che la chiamata é stata fatta con app

Come vengono usati i miei dati?

I dati vengono utilizzati esclusivamente per la gestione della chiamata di emergenza

Chiamando con l'app perdo tempo?

No. La telefonata avviene negli stessi tempi e inoltre l'uso dell'app per la chiamata riduce complessivamente i tempi consentendo una puntuale e rapida localizzare dell'utente.

Può essere richiesta la mia posizione tramite APP?

No, l'app non è utilizzabile dall'esterno.

CHIAMATE DI EMERGENZA AUTOMATICHE

I cellulari hanno anche la possibilità di effettuare chiamate di emergenza a numeri prestabiliti: figli, parenti, medico, …

In genere questi numeri sono programmabili dalle *Impostazioni* > *Sicurezza ed emergenza* o dal menù del display per le telefonate (tastierino).

Questi numeri sono chiamabili anche da eventuali soccorritori che non hanno accesso al vostro telefono, ma possono sbloccarlo per questa sola funzione come abbiamo visto nelle Impostazioni (ad es. premere tot volte il tasto laterale).

Sicurezza ed emergenza

Come abbiamo già detto nel capitolo delle Impostazioni, in quest'area possiamo memorizzare le nostre informazioni mediche (condizioni mediche, allergie, cure correnti, gruppo sanguigno e altre notizie utili), i contatti di emergenza che intendiamo segnalare e che possono essere chiamati dai soccorritori, anche con telefono bloccato.

Si possono anche predefinire particolari azioni sui tasti dello smartphone per segnalare una situazione di emergenza. In questo caso il nostro smartphone attiva automaticamente la geolocalizzazione, invia messaggi SMS di emergenza e fa chiamate automatiche ai contatti che abbiamo memorizzato.

SEGNALARE LA PROPRIA POSIZIONE

Può essere importante segnalare la propria posizione per un qualsiasi motivo, anche per la propria sicurezza.

Smartphone con sistema Android

Con questo tipo di cellulari si ricorre all'app Google Maps; se non la trovi, si può scaricare dal Google Play Store.

È necessario avere una connessione Internet attiva e attivare la geolocalizzazione.

Per iniziare a condividere la posizione si deve aprire l'app e cliccare sull'icona dell'avatar posta in alto a destra.

Procedere poi con questi passaggi:

dal menu che si apre cliccare sulla voce Condivisione della posizione

nella schermata che si apre, cliccare sul pulsante Nuova Condivisione

nella nuova schermata, indicare la durata della condivisione e selezionare o indicare la/e persona/e alla quale comunicare i dati

cliccare sul pulsante Consenti.

Smartphone con sistema iOS (iPhone Apple)

Negli iPhone c'è una app dedicata: DOV'È.

Funziona solo tra persone che possiedono l'iPhone. Se non è così, si torna al metodo dewgli Android.

Per iniziare a condividere la posizione, si deve aprire l'app, cliccare sulla scheda Persone posta nella barra in basso e poi cliccare sul pulsante Inizia a condividere la posizione.

Nella schermata che compare si seleziona il contatto con cui desideri condividere la posizione e si clicca poi sul pulsante Invia posto in alto a destra: dal pop-up che appare a schermo si sceglie una delle seguenti opzioni, ovvero Condividi per un'ora, Condividi fino a fine giornata o Condividi per sempre.

LA APP "FASCICOLO SANITARIO"

Un'app molto utile, che non dovrebbe mancare mai su uno smartphone, è quella relativa al Fascicolo Sanitario per i residenti nella regione Lombardia.

Il Fascicolo Sanitario Elettronico (FSE) è l'insieme dei tuoi dati e documenti digitali di tipo sanitario e socio-sanitario che puoi consultare e avere a disposizione online. Puoi decidere di rendere consultabile il tuo Fascicolo anche al personale sanitario che ti prende in cura. Per farlo dovrai esprimere il consenso alla consultazione.

Cosa trovo nel mio Fascicolo Sanitario?

- i dati di assistenza sanitaria (medico di medicina generale, esenzioni, assistenza temporanea, budget celiachia, ecc.);
- i tuoi documenti sanitari (es. referti di esami e visite specialistiche, referti dei test COVID-19, ricette farmaceutiche, ricette specialistiche, lettere di dimissione, verbali di pronto soccorso, ecc.);
- il tuo percorso di presa in carico (se sei un paziente cronico);
- le tue vaccinazioni;
- i tuoi appuntamenti;
- le certificazioni verdi COVID-19 rese disponibili dalla piattaforma nazionale del Ministero della Salute.

Chi può vedere il mio Fascicolo Sanitario Elettronico?

Solo tu puoi consultare online il tuo Fascicolo Sanitario.

Esprimendo il consenso alla consultazione del Fascicolo, si autorizza l'accesso anche al personale sanitario che ti ha in cura o nelle situazioni di emergenza.

Si può decidere quali documenti non rendere visibili al personale sanitario.

I documenti contenuti nel Fascicolo sono contrassegnati da icone con lucchetti aperti o chiusi e di differenti colori che ne indicano la visibilità al personale sanitario.
I documenti visibili (lucchetto aperto, icona verde), sono consultabili da te, e se hai espresso il consenso alla consultazione, anche dal personale sanitario che ti prende in cura.

I documenti non visibili (lucchetto chiuso, icona rossa o icona marrone), sono consultabili solo da te. Anche se hai espresso il consenso alla consultazione, il personale sanitario non può vedere questi documenti.

LE APP “SALUTILE”

Prenotazione visite ed esami

Scaricando l’applicazione di Regione Lombardia è possibile prenotare visite o appuntamenti, prescritti dal medico con ricetta elettronica, per tutta la famiglia, direttamente da cellulare.

Si entra con CODICE DI ACCESSO (8 numeri) oppure con SPID oppure con CIE.

Trova il Pronto Soccorso più vicino e più libero

SALUTILE Pronto Soccorso è l'app di Regione Lombardia con la quale puoi consultare l'elenco di tutti i Pronto Soccorso del territorio lombardo, conoscere qual è il numero di persone in coda in quel momento e l’indice di affollamento.

Puoi visualizzare sulla mappa le strutture più vicino a te ed eventualmente avviare la navigazione guidata verso il Pronto Soccorso scelto.

VIDEOCHIAMATE

Abbiamo già visto come effettuare videochiamate da Whatsapp.

Diciamo che è la strada più comoda.

Ci sono però anche altre app che offrono lo stesso servizio (e pure qualcosa di più):

- telegram
- skype
- instagram
- facebook messenger

Ovviamente, anche la persona che chiamiamo deve essere registrata sul servizio dal quale chiamiamo.

Cosa dobbiamo imparare anche per le videochiamate?

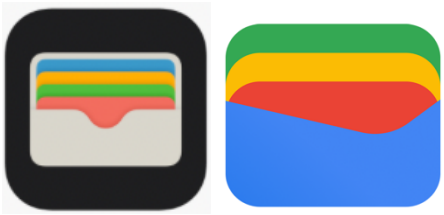
- Comando per mettere in MUTO il microfono
- Comando per togliere il video (se ci accorgiamo che il segnale non regge sia video che audio).

PAGAMENTI CON TELEFONO O SMARTWATCH

Gli smartphone più recenti possono sfruttare la funzionalità dei servizi di pagamento sul POS dei negozi.

Le app sono:

- Android: Google Pay (o Google Wallet)
- iPhone: Wallet .



Come funziona?

Innanzitutto si deve scaricare l'app che ho citato sopra.

Poi si devono registrare i dati del vostro bancomat o carta di credito (non tutte sono abilitate).

A questo punto siamo pronti:

quando il negoziante ci avvicina il POS, apriamo l'app e selezioniamo la carta (se ne abbiamo più di una), avviciniamo il cellulare ed il pagamento è fatto. In tutta sicurezza: non dobbiamo inserire il PIN, i dati della carta vengono utilizzati in. Modalità "Usa e getta".

Vantaggi:

- non dovete tenere in tasca carte o bancomat (che se vi rubano dovete bloccare, sostituire, …) o, quanto meno, non dovete tirarli fuori dalla borsetta
- La carta del telefono non può essere clonata perché i dati sono criptati e valgono una volta sola (per quel pagamento)
- Se vi rubano il cellulare protetto da PIN o altro sistema di riconoscimento, non dovete preoccuparvi di bloccare le carte
- Utilizziamo meno i contanti (che possono essere falsi, sono sicuramente zozzi, se ce li rubano sono persi e basta)

Svantaggi:

- il telefono può scaricarsi
- Qualche punto vendita non è attrezzato (es: rifornimento carburante)

Attenzione:

- il telefono deve essere protetto da PIN o da Touch ID

HOMEBANKING

Ormai tutte le banche e la Posta permettono di seguire il proprio conto corrente (e gli eventuali investimenti) sul proprio cellulare: il cosiddetto Homebanking.

I vantaggi sono evidenti:

Non è più necessario andare fisicamente in banca per ogni operazione

Risparmiamo quindi tempo e denaro (se dobbiamo andare in macchina)

Possiamo fare le operazioni in tutta sicurezza.

Come funziona?

Bisogna scaricare l'app della propria Banca o della Posta

Dobbiamo farci abilitare dalla Banca (che ci fornirà istruzioni e credenziali - Utenza e Password)

Ci registriamo sull'app e da quel momento possiamo procedere.

Ci verrà proposto uno di questi sistemi di sicurezza, che ci possono aiutare:

OTP, cioè One Time Password o password Usa e Getta

Touch ID o Riconoscimento facciale (Token)

Ricordiamoci di quanto detto in merito alle truffe via mail, sms o social: nessuna banca, la posta o altro istituto ci chiederà mail le credenziali per telefono, via mail o accedendo ad un link.

Se c'è da svolgere qualche operazione, accediamo alla nostra AREA RISERVATA tramite app o PC.

Attenzione:

- il telefono deve essere protetto da PIN o da Touch ID

NAVIGATORE

Se Cristoforo Colombo avesse avuto il navigatore, non avrebbe scoperto l'America.

I navigatori sono strumenti utilissimi, se li sappiamo adoperare bene:

- Ci possono dare indicazioni sui limiti di velocità
- Suggerire percorsi alternativi in caso di traffico bloccato
- Farci sapere in tempo reale quanto durerà ancora il viaggio
- Organizzare le nostre tappe

Ma anche:

- NON DOBBIAMO FARE TUTTO QUELLO CHE CI DICONO ("Fare immediatamente un'inversione a U" e siamo in autostrada!!!)
- NON FACCIAMOCI DISTRARRE

Le opzioni di viaggio

Ogni bravo navigatore che si rispetti ha bisogno di ricevere istruzioni da noi. Queste istruzioni potrebbero essere valide in genere o solo per il viaggio che stiamo per intraprendere.

Consiglio di fare un giro in queste opzioni, così da sapere cosa si potrà poi modificare se serve:

- Mezzo preferito (Auto, piedi, mezzi pubblici)
- Evitare pedaggi
- Evitare autostrade
- Evitare strade sterrate
- Mostra posizione parcheggio
- Segnala limiti di velocità
- Evita o segnala ZTL
- E tanto altro …

La meta

Ormai tutti i navigatori hanno imparato ad interpretare quello che scriviamo.

Se una volta era obbligatorio seguire un certo ordine, oggi possiamo scrivere l'indirizzo con una certa libertà. Il navigatore, se non trova esattamente quello che scriviamo, ci proporrà le soluzioni più simili.

Ma controlliamo che poi venga selezionato l'indirizzo giusto. Se per caso dobbiamo andare in via Roma – che c'è in tutti i comuni italiani e non – verifichiamo di andare nella via Roma giusta.

Se invece selezioniamo solo la località, verremo indirizzati al centro del paese.

Il display

Cosa vogliamo vedere durante il viaggio?

Possiamo modificare il display scegliendo le opzioni più utili

- Km mancanti, tempo mancante
- Limiti di velocità
- Punti interessanti (ristoranti, negozi, distributori, musei, …)
- 2D o 3D?

Buon Viaggio e guidate con prudenza!

ALCUNE SIMPATICHE APP

Stocard

Salviamo qui tutte le nostre tessere di supermercati, negozi, catene commerciali, …

Quando arriveremo alla cassa, basterà mostrare la tessera sul cellulare e verrà letta con la pistola della cassa.

Junker

Dove buttare questa confezione nella raccolta differenziata?

ATM, Trenitalia, Trenord, Italo

Sì, viaggiare. Come cantava Lucio Battisti.

Con queste app possiamo:

- Calcolare percorsi e orari
- Acquistare i biglietti
- Vedere la situazione del treno o del mezzo pubblico
- Ricevere notizie in tempo, quasi, reale

Poste Italiane

Una app utile per:

- Prenotare un appuntamento in un ufficio postale e velocizzare le tue operazioni a sportello. Si sceglie sulla mappa Ufficio Postale e orario più comodi. Si riceve un promemoria dell'appuntamento. È possibile compilare in app i dati richiesti e risparmiare ancora più tempo allo sportello per effettuare trasferimenti di denaro, ricariche telefoniche e delle carte prepagate Postepay, invio di corrispondenza.
- Gestire i tuoi Conti BancoPosta e le tue Carte Postepay, pagare in sicurezza bollettini e bolli auto e moto, effettuare pagamenti PagoPA (quelli della pubblica amministrazione), e molto altro.
- Spedire online e tracciare pacchi e posta. Inviare pacchi in pochi click comodamente da casa, e possono essere ritirati anche a domicilio. Non solo: si possono scrivere e spedire online anche raccomandate, telegrammi o lettere. E seguire lo stato (o tracking) di tutte le tue spedizioni in un colpo d'occhio.

RaiPlay e RaiPlay Sound

Sono due app con le quali guardare o ascoltare gratuitamente i programmi RAI della tv e della radio (RPSound), sia in diretta, che on demand (su richiesta).

C'è proprio di tutto, anche programmi della tv di quando eravamo ragazzi.

E su RPSound ci sono audiolibri, gialli, sceneggiati radio (a me fanno compagnia nei viaggi in auto).

Due ottime piattaforme multimediali per farci compagnia.

Sono gratuite, è sufficiente registrarsi.

Spotify

Spotify è un'app gratuita per ascoltare le tue canzoni e i tuoi podcast (brani audio) preferiti, un'enorme libreria di canzoni gratis.

Si può scegliere sia il genere che gli autori, creando una playlist (sequenza predefinita di brani) o ascoltando in modalità shuffle (casuale, l'ordine lo stabilisce la app)

Come in molte app, troviamo una versione gratuita (o free) che ha alcune limitazioni e una versione a pagamento (o Premium) che offre molti servizi.

allertaLOM

allertaLOM è l'App di Regione Lombardia che permette di ricevere le allerte di Protezione Civile emesse dal Centro Funzionale Monitoraggio Rischi naturali di Regione Lombardia, in previsione di eventi naturali con possibili danni sul territorio.

Le allerte riguardano i rischi naturali prevedibili (idrogeologico, idraulico, temporali forti, vento forte, neve, valanghe e incendi boschivi) e presentano livelli crescenti di criticità (codice verde, giallo, arancione, rosso) a seconda della gravità ed estensione dei fenomeni.

Le allerte sono uno strumento per sapere quando adottare le misure di auto-protezione, seguendo le indicazioni dell'Autorità locale di Protezione Civile.

Con l'App si può:

- restare sempre aggiornati sulle allerte di Protezione Civile in Lombardia;
- seguire l'evoluzione su mappa dei livelli di allerta nell'arco di 36 ore;
- scegliere dei Comuni preferiti per i quali ricevere notifiche all'emissione di allerte sui rischi prescelti;

DinDonDan

È giunto il momento di far contento il nostro parroco, con una app che ci dà informazioni sugli orari delle S. Messe nelle chiese vicine a noi.

GAMES

L'utilizzo dello smartphone per giocare è sempre più diffuso. Migliaia sono le proposte di videogiochi disponibili per essere scaricati dagli store, gratuitamente o a pagamento.

Possono essere utili per tenere in allenamento il nostro cervello o i nostri riflessi, per distrarci nella sala d'attesa del dentista o per farci passare un po' di tempo in un lungo viaggio.

Tutto bello, ma qualche rischio piccolo o grande c'è:

- Dipendenza, ancor più grave se ci troviamo ad aver a che fare con veri e propri giochi d'azzardo
- Manipolazione del cervello (aggressività, sentimenti ostili, …)
- Messaggi subliminali
- Distacco dalla realtà (uccidere persone, fare incidenti, sfidare pericoli, …).

Utilizziamoli quindi solo come un passatempo e impariamo a smettere.

Come recita il detto: "Un bel gioco dura poco"

IL GALATEO DELLO SMARTPHONE

La suoneria

Che bisogna tenere sotto controllo il volume della suoneria, non è di certo una novità, ma anche la scelta della stessa è importante: anche se vi viene voglia di impostare quel brano punk che tanto amate, è preferibile optare per un trillo discreto tra quelli in dotazione della casa produttrice: ricordate che less in more!

A tavola (e a letto)

Lo smartphone non deve mai essere posato sulla tavola (così come il portafogli, le chiavi, la borsetta, ecc.) sia che siate al ristorante, al bar o, soprattutto, a casa di qualcuno: tenete il cellulare in borsa, spento o in modalità silenzioso.

Se siete in compagnia, ve lo dovete dimenticare del tutto e dedicare la vostra attenzione a chi è con voi.

Se proprio dovete fare una telefonata urgente, chiedete il permesso e allontanatevi, per il minor tempo possibile, ma mai nel corso di un pranzo o di una cena.

I motivi per cui non si dovrebbe utilizzare lo smartphone a tavola sono molteplici. La buona educazione è sicuramente in testa: quante volte ti è capitato di vedere coppie o interi gruppi a cena al ristorante che scorrono con le dita sugli schermi dei telefoni invece di fare della sana conversazione? L'igiene è un altro ottimo motivo per lasciare lo smartphone in tasca o in borsa. Inoltre, per chi non è ancora convinto dell'importanza di escludere il cellulare dal tavolo di una cena, si può fare un veloce ripasso guardando il film Perfetti sconosciuti...

Alla guida (qui non si tratta di Galateo, ma di Codice della Strada)

Qui il galateo c'entra davvero poco: è l'attenzione alla sicurezza nostra e degli altri che dovrebbe distoglierci dall'insano proposito di sbirciare lo smartphone mentre si è alla guida. Peggio: di scattare fotografie, girare video, inviare messaggi, registrare dirette da trasmettere sui social. Troppe volte abbiamo letto sui giornali il triste epilogo che queste azioni apparentemente innocue possono avere.

Se siete passeggeri di una persona che guida così, chiedete cortesemente si smetterla o, al limite, chiedete di scendere.

Io l'ho fatto con un autista di mezzo pubblico.

Orari

Si sa – o si dovrebbe sapere – che è di cattivo gusto chiamare qualcuno al di fuori di certi orari. Nel dubbio limitatevi agli orari d'ufficio, perché a nessuno fa piacere essere disturbati prima delle 9 di mattina; nell'orario di pranzo; nell'orario di cena, e dopo cena.

La regola vale sia per le telefonate che per i messaggi, in qualunque forma (Facebook, Instagram, SMS, WhatsApp, mail, ...): l'avviso sonoro che ne sussegue, per chi, ahimè, non spegne il cellulare nemmeno di notte, disturberà sia il destinatario che il resto della famiglia!

Luoghi pubblici

La regola è trattenersi il meno possibile al cellulare, rigorosamente a bassa voce e senza agitarsi: camminare avanti e indietro per i marciapiedi, urlando frasi sconnesse, non solo vi fa sembrare fuori di testa ma anche maleducati.

Stessa regola vale per l'utilizzo dello smartphone sui trasporti pubblici: telefonate brevi e a bassa voce. Nelle lunghe tratte, magari a bordo treno o in aereo, ad esempio, vi è consentito distrarvi con giochi o video, in tal caso utilizzate sempre gli auricolari.

Teatro e cinema

Lo smartphone va tenuto rigorosamente spento! Non è ammissibile nemmeno la vibrazione.

Lo dovete letteralmente dimenticare e non cedere all'impulso di controllare se vi è arrivata qualche chiamata o messaggio, soprattutto quando le luci della sala sono spente, perché la luminosità dello schermo abbaglia e disturba chi siede dietro di voi.

Stesse regole valgono nel corso di manifestazioni sportive, il che comporterebbe il rischio di innervosire lo sportivo, mentre sta per fare un matchpoint!

Vivavoce

Le telefonate in vivavoce sono accettabili solo in due situazioni: quando siete alla guida o quando siete a casa. In pratica, solo se siete soli.

Se vi capiterà di dover fare una telefonata in vivavoce mentre non siete soli, magari in auto, comunicatelo immediatamente al vostro interlocutore, in modo che sappia che non siete l'unica persona ad ascoltare ciò che sta per dirvi.

Video-chiamate

Bellissimo strumento in grado di accorciare le distanze, permettendovi di parlare guardando negli occhi parenti, fidanzato/a, ecc., magari mentre siete in vacanza.

Però fate attenzione a non far comparire in video il vicino d'ombrellone, sempre per una questione di privacy. In ogni caso, è sempre preferibile utilizzare gli auricolari, magico strumento che eviterà di far sapere i fatti vostri e del vostro interlocutore, a tutto il vicinato.

Insistenza

Importantissimo tra le buone maniere al telefono: avete chiamato qualcuno che non vi ha risposto? Se è il caso, lasciate un messaggio in segreteria o spedite un messaggio di testo anticipando il motivo della vostra chiamata. Non insistete nel richiamare: il destinatario vedrà il vostro tentativo di chiamata e ve la restituirà appena vorrà e/o gli sarà possibile farlo.

Gli smartphone non sono babysitter

Lo sappiamo: i bambini sono una fonte inesauribile di energia, a differenza dei loro genitori che purtroppo devono sostenere dei ritmi non sempre rilassanti. Questo, però, non significa che gli smartphone debbano diventare gli usuali babysitter dei nostri figli. Ammette di usare il cellulare per "far stare buoni" i propri figli addirittura il 60% delle coppie con figli sotto i due anni. Positivo il dato per cui la maggior parte di loro li utilizza insieme al bambino e per riprodurre contenuti educativi, meno positiva l'abitudine di lasciare i piccoli da soli con dispositivi che l'Accademia americana di pediatria sconsiglia (per non dire vieta!) ai bambini sotto i 18 mesi.

Non diventare uno Smombie

È da poco entrata **nel dizionario Treccani** ed è la fusione delle parole "*smartphone*" e "*zombie*". Siamo sicuri che anche tu, almeno una volta nella vita, sei stato uno o una smombie. Chi ti scrive, ad esempio, lo è spesso: per lavoro, per non annoiarsi o perché sta nutrendo le sue relazioni affettive utilizzando una chat.

Smombie è chi cammina per strada senza alzare lo sguardo dallo smartphone, rischiando di inciampare, scontrarsi con altre persone, attraversare la strada in modo pericoloso.

Il concetto di smartphone zombie viene dall'Inghilterra ed è entrato nella cultura popolare perché la società si è riempita di persone che camminano, mangiano, bevono, viaggiano e praticamente vivono con gli occhi incollati allo schermo del proprio smartphone. Testa bassa, spalle curve, sguardo spento: sono le caratteristiche delle persone che hanno smesso di guardare la realtà che le circonda per vederla filtrata dal display di un telefono cellulare. Non diventare uno di loro.

Perché immortalare tutto?

Oltre al fatto che voler documentare qualunque cosa, comporti osservare il mondo da un piccolo schermo (scelta personale, esclusa dal contesto di quest'articolo), ci sono occasioni dove è davvero di cattivo gusto farlo:

- Matrimoni: c'è già un fotografo, pagato, che riprenderà l'intera cerimonia. Dalle mille foto scattate, saranno gli sposi a scegliere, con cura, quali desiderano rendere pubbliche e, le vostre, non sono di sicuro fra queste: non è la vostra festa quindi tenete lo smartphone in borsa.
- Concerti: alzare il vostro smartphone per riprendere lo spettacolo, vi farà diventare 50 cm più alte, e ciò toglierà la visione ad altri. Godetevi il momento, piuttosto
- Incidenti sulla strada.

Proprio per questa abitudine, quando qualcuno vi fa vedere alcune foto sul suo cellulare, non scorrete tutto l'album …

Scollegatevi per ricollegare il cervello (e il cuore).

È ormai assodato anche da ricerche che prendersi una pausa dalla tecnologia (lunga, corposa, sincera, senza rimpianti) è un modo per migliorare il benessere e alleviare tensioni, ansie, stress che neanche ci accorgiamo di accumulare. Lo smartphone può aspettare, non vi rendete conto che è sintomo di ansia controllare meccanicamente email e facebook ogni 10 minuti?

Non serve mica passare un week end nel deserto. Basta "disconnettersi" un po' tutti i giorni. Magari la sera, un'ora prima di andare a letto.

Aiutate parenti ed amici a vivere momenti "smartphone free", "disconnessi", in altre parole, "LIBERI".

E PER FINIRE ... IL PISTOLOTTO

Siamo cresciuti/e con i nostri genitori che ci controllavano solo se eravamo a portata di vista (compresa quella degli altri abitanti del paese o rione), abbiamo scritto a fidanzate e fidanzati lettere e cartoline, siamo andati in giro guardando il panorama e sbagliando ogni tanto strada.

Ora abbiamo in mano uno strumento che non avevamo mai nemmeno immaginato. E che abbiamo visto quanto esserci utile; può addirittura salvarci la vita.

Ma abbiamo anche visto quanto può essere nocivo.

Non bisogna averne paura o diffidarne.

Abbiamo imparato a cucinare usando il cucchiaio di legno, ma oggi siamo Masterchef con una planetaria.

Come tutte le cose che adoperiamo, non sono loro ad essere buone o cattive; il problema è sempre nel manico.