



COMANDO GENERALE DELLA GUARDIA DI FINANZA
DIREZIONE TELEMATICA – SERVIZIO TELECOMUNICAZIONI

SICUREZZA E PRIVACY

I RISCHI CONNESSI ALL'USO DEI DISPOSITIVI MOBILI

I MODERNI DISPOSITIVI MOBILI SONO SEMPRE PIÙ SPESSO UTILIZZATI COME VERI E PROPRI COMPUTER PORTATILI.

Leggere le e-mail, accedere ai *social network* e ai servizi di *online banking* sono diventate attività che svolgiamo ormai abitualmente tramite i nostri *smartphone*, nei quali memorizziamo, spesso inconsapevolmente, una grande quantità di informazioni personali, anche sensibili, tra cui ad esempio:

- nomi, indirizzi (e-mail e fisici) e numeri di telefono di amici e parenti;
- cronologia della navigazione in Internet;
- informazioni sulla propria posizione e sui propri spostamenti;
- SMS, Email e messaggi inviati e ricevuti;
- PIN e password;
- foto e documenti personali o di lavoro, contenenti potenzialmente informazioni riservate, magari sincronizzati tramite servizi di archiviazione dati virtuali c.d. Cloud non affidabili;
- dati delle applicazioni, che possono includere credenziali di accesso ad account di servizi online.

Tutte queste informazioni, in caso di smarrimento, furto o compromissione del dispositivo, potrebbero cadere in mano di estranei o criminali informatici con gravi rischi per la sicurezza dei nostri dati, la privacy e spesso anche per il portafoglio. Pensiamo ad esempio ad acquisti che un malintenzionato potrebbe fare a nostro nome usando servizi collegati alla nostra carta prepagata o anche tramite acquisti *in-app*.

Perfino la nostra stessa incolumità e i nostri beni fisici possono essere messi a rischio dalla quantità di informazioni sulle nostre abitudini che tendiamo a condividere online.

Anche le app che spesso installiamo ed utilizziamo con superficialità, solo per provarle, possono presentare potenziali rischi, specialmente se non si pone attenzione alla loro provenienza e alle informazioni a cui consentiamo loro di accedere.

COME RENDERE SICURO IL PROPRIO SMARTPHONE

Alcuni semplici accorgimenti su come configurare ed utilizzare in maniera sicura i nostri *smartphone*, possono evitare la maggior parte dei rischi.

Le indicazioni fornite non si intendono naturalmente esaustive di tutte le possibili minacce per la sicurezza e la privacy derivanti dall'uso dei dispositivi mobili, ma costituiscono un elenco di buone pratiche volto ad aumentare l'attenzione e la consapevolezza degli utenti nei riguardi di tali problematiche.

Le modalità tecniche specifiche per configurare opportunamente le opzioni di sicurezza degli *smartphone* dipendono dal dispositivo utilizzato e non sono dettagliate in questa guida.





1. BLOCCARE SEMPRE LO SMARTPHONE CON UNA PASSWORD.

Questo è uno degli accorgimenti di sicurezza più elementari, ma che è spesso completamente ignorato a favore di tecniche di blocco più semplici, come l'uso di sequenze da tracciare col dito sullo schermo.

Attenzione, perché, oltre ad essere questo un metodo intrinsecamente insicuro, le tracce di sebo sullo schermo potrebbero rivelare la sequenza usata molto facilmente.

Usando un PIN di quattro/sei cifre si ottiene già un buon livello di protezione, ma l'ideale è utilizzare una password alfanumerica dotata anche di caratteri speciali abbastanza robusta e non facilmente indovinabile.

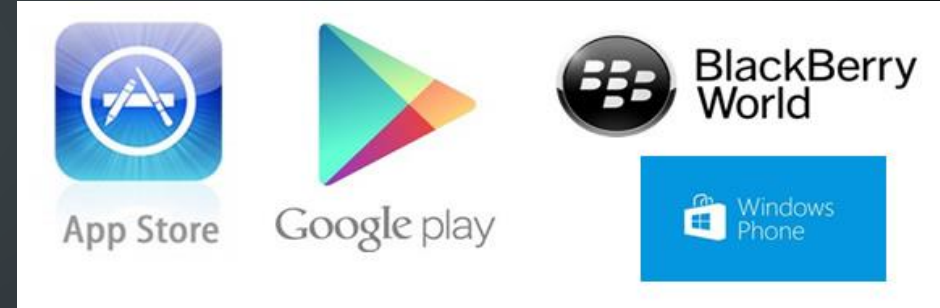
2. CONFIGURARE OPPORTUNAMENTE IL BLOCCO AUTOMATICO DELLO SCHERMO

Dover continuamente sbloccare il telefono può essere considerato da alcune persone molto scomodo, ma un tempo di inattività troppo lungo prima del blocco dello schermo potrebbe risultare eccessivamente rischioso e vanificare il beneficio della password.

Si consiglia di impostare tempi non superiori al minuto.

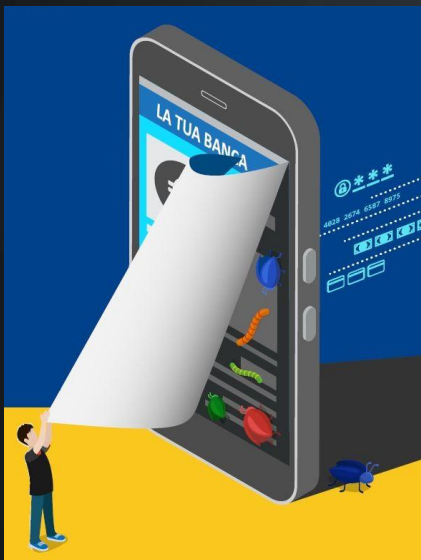
3. INSTALLATE APPLICAZIONI PROVENIENTI SOLO DA FONTI ATTENDIBILI

- Acquistate le vostre app solo da store affidabili — Prima di scaricare un'app, fate una ricerca sia sull'app che sugli autori. Siate cauti con i link che ricevete per e-mail e fate attenzione ai messaggi di testo che potrebbero indurvi a installare app di terze parti o fonti sconosciute.
- Date un'occhiata alle recensioni di altri utenti, se disponibili.
- Verificate le autorizzazioni di un'app — Controllate a quali tipologie di dati può accedere l'app e se può condividere i vostri dati con parti esterne. Se avete dei sospetti o non vi fidate delle condizioni, non scaricate l'app.



4. ATTENZIONE A CLICCARE SUI LINK O SUGLI ALLEGATI CONTENUTI IN E-MAIL O MESSAGGI DI TESTO NON RICHIESTI.

- Non fidatevi dei link contenuti in e-mail o messaggi di testo non richiesti (SMS e MMS). Eliminateli non appena li ricevete perché potrebbe trattarsi di "Phishing".
- Fate un controllo incrociato degli url abbreviati e dei codici QR in quanto potrebbero condurre a siti dannosi o scaricare direttamente un malware sul vostro dispositivo. Prima di fare clic, cercate di visualizzare l'anteprima dell'url per verificare che l'indirizzo web sia affidabile. Prima di effettuare la scansione di un codice QR, selezionate un lettore di codici QR in grado di visualizzare l'anteprima dell'indirizzo web a cui fa riferimento e utilizzate un software per la sicurezza mobile in grado di segnalare la presenza di link rischiosi.

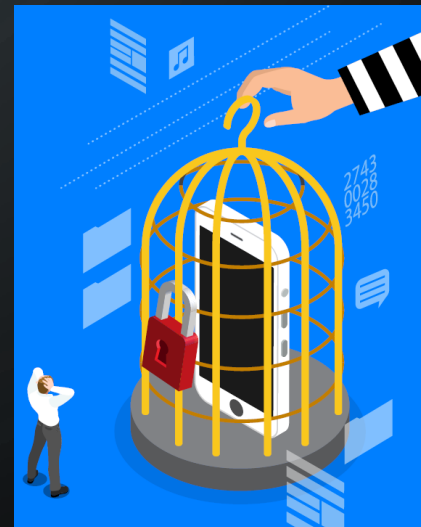


5. DISCONNETTETEVI DA UN SITO DOPO AVER EFFETTUATO UN PAGAMENTO.

- Non salvate mai username e password nel browser o nelle app del vostro dispositivo mobile — In caso di smarrimento o furto del vostro telefono o tablet, chiunque potrebbe accedere ai vostri account. Una volta completata una transazione, disconnettetevi dal sito invece di chiudere semplicemente il browser.
- Non effettuate operazioni bancarie o acquisti online utilizzando connessioni Wi-Fi pubbliche — Effettuate operazioni bancarie e acquisti online utilizzando esclusivamente reti note e attendibili.
- Fate un controllo incrociato dell'url del sito — Assicuratevi che l'indirizzo web sia corretto prima di effettuare l'accesso o inviare dati sensibili. Valutate la possibilità di scaricare l'app ufficiale della vostra banca per essere certi di collegarvi sempre al sito autentico.

6. EVITATE DI FORNIRE I VOSTRI DATI PERSONALI.

- Non rispondete mai fornendo i vostri dati personali a messaggi di testo o e-mail che apparentemente sono stati inviati dalla vostra banca o un da un'altra azienda affidabile. Cercate invece di contattare direttamente l'azienda in questione per verificare che la loro richiesta sia autentica.
- Controllate periodicamente il dettaglio del vostro traffico mobile per verificare la presenza di eventuali spese sospette — Se dovete individuare spese che ritenete di non aver mai effettuato, contattate immediatamente il vostro gestore telefonico.



7. DISATTIVATE IL WI-FI, I SERVIZI DI LOCALIZZAZIONE E IL BLUETOOTH SE NON LI USATE.

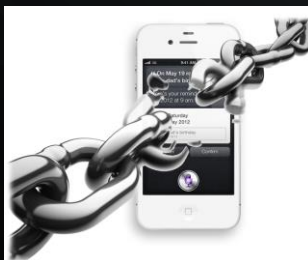
Disattivate il Wi-Fi se non lo utilizzate — I cybercriminali possono accedere ai vostri dati se la connessione non è protetta. Connettere il dispositivo solo a reti Wi-Fi conosciute e con riferimento alle quali le politiche di amministrazione e sicurezza risultino trasparenti all'utenza. Se possibile, utilizzate una connessione dati 3G o 4G anziché un hotspot. Potete anche optare per un servizio di rete privata virtuale (VPN) per mantenere i dati in transito crittografati.

- Non consentite alle app di utilizzare i servizi di localizzazione, a meno che non sia indispensabile — Queste informazioni potrebbero essere condivise o trapelate ed essere utilizzate per l'invio di annunci basati sulla località in cui vi trovate.
- Disattivate il bluetooth quando non lo utilizzate — Assicuratevi che sia completamente disattivato e non solo in modalità invisibile. Le impostazioni predefinite sono spesso preimpostate per consentire ad altri di connettersi al dispositivo a vostra insaputa. Eventuali utenti malintenzionati potrebbero potenzialmente copiare i vostri file, accedere ad altri dispositivi collegati o addirittura accedere in remoto al vostro telefono per effettuare chiamate e inviare messaggi di testo e far lievitare i costi della vostra bolletta.



8. NON EFFETTUATE IL JAILBREAK/ROOT DEL VOSTRO DISPOSITIVO.

- Il jailbreak/root consiste nella rimozione delle limitazioni di sicurezza imposte dal fornitore del sistema operativo per acquisire l'accesso completo al sistema operativo stesso e alle sue caratteristiche. Effettuando il jailbreak/root del vostro dispositivo, la sua sicurezza può essere compromessa in modo significativo e aprire falle a livello di sicurezza che potrebbero non risultare subito evidenti.



Aggiornamento Sistema Operativo



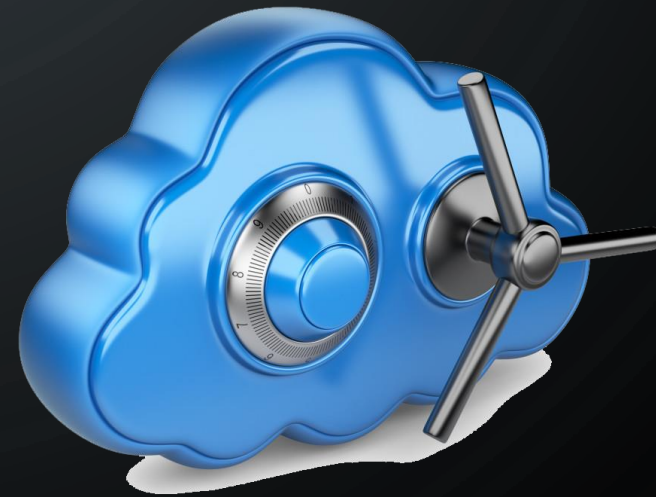
download in corso...

9. TENETE SEMPRE AGGIORNATI IL VOSTRO SISTEMA OPERATIVO E LE APP.

- Scaricate gli aggiornamenti per il sistema operativo del vostro dispositivo mobile non appena vi viene chiesto — Installando gli ultimi aggiornamenti, il dispositivo non solo è più sicuro ma garantisce anche prestazioni migliori.

10. EFFETTUATE IL BACKUP DEI VOSTRI DATI.

- Il backup può essere salvato sia su pc sia sul dispositivo mobile. molti smartphone e tablet sono in grado di effettuare il backup dei dati in modalità wireless — Verificate le opzioni esistenti a seconda del sistema operativo del vostro dispositivo. Effettuando il backup del vostro smartphone o tablet potrete ripristinare facilmente i vostri dati personali in caso di smarrimento, furto o danneggiamento del dispositivo.





COMANDO GENERALE DELLA GUARDIA DI FINANZA
DIREZIONE TELEMATICA – SERVIZIO TELECOMUNICAZIONI



... si ringrazia per l'attenzione