Foto: https://pixabay.com/photos/girl-smartphone-iphone-1192032/

Hai mai pensato che il tuo iPhone possa essere esposto a rischi legati alla sicurezza? Effettui regolarmente aggiornamen ti del sistema operativo del tuo iPhone, di modo che sia sempre aggiornato e protetto al meglio da minacce informatiche e non solo?

In questo articolo, ti spiegheremo come proteggere al meglio il tuo iPhone per evitare attacchi informatici, ma anche per impedire ad occhi indiscreti di accedere al tuo dispositivo e di rovistare tra i tuoi messaggi, immagini o, ancor peggio, rubare dati sensibili.

Perché è importante proteggersi?

Negli ultimi anni, le connessioni e, più in generale, il mondo della rete sono cresciuti a dismisura; questo fenomeno ha portato sia benefici che svantaggi, come la raccolta e diffusione dei dati personali. Per questo motivo, è necessario imparare a proteggersi adottando misure consone per la propria sicurezza, la sicurezza dei propri contenuti e la privacy online.

Un esempio banale è il fenomeno denominato "*violazione dei dati personali*". Consiste dell'accesso, da parte di terzi non autorizzati, a dati sensibili che vengono divulgati o usati senza alcuna autorizzazione; questo può verificarsi a causa di attacchi informatici, furti del proprio dispositivo o vulnerabilità dovute ad applicazioni o a un sistema operativo obsoleto.

Tale fenomeno può portare, nel peggiore dei casi, all'accesso da parte di terzi non autorizzati al proprio account bancario, ad applicazioni di messaggistica (WhatsApp, Telegram, Messaggi e caselle di posta) o ai contenuti multimediali presenti nel dispositivo, che potrebbero essere diffusi o utilizzati per richiedere un riscatto.

Best Practices per il proprio iPhone

In questa sezione elencheremo alcune di quelle che sono le "Best Practices" (pratiche migliori) da adottare nella vita quotidiana e nel proprio iPhone, per cercare di evitare attacchi informatici e mantenere i propri dati al sicuro.

Usare un gestore delle password

Il primo consiglio che ci sentiamo di darti è quello di utilizzare un "*gestore delle password*". Si tratta di uno strumento, che può essere installato sul proprio dispositivo o utilizzato come estensione nel browser, e che consente di creare e archiviare (in maniera criptata) delle password robuste, da usare per accedere a piattaforme e applicazioni.

Attualmente, esistono diversi “password manager”, come NordPass , sviluppato dal colosso NordVPN, che ti consentirà di dormire sonni tranquilli al solo costo di un cappuccino!

Aggiornamento di sistema

Un’altra buona prassi è quella di mantenere sempre aggiornato il proprio iPhone all'ultima versione di iOS (meglio se la versione stabile): effettuare questa operazione non ha alcun costo, basterà verificare nelle impostazioni del telefono se è disponibile un aggiornamento e, in tal caso, scaricarlo ed effettuarlo.

È essenziale mantenere aggiornato il proprio dispositivo, in quanto i nuovi aggiornamenti nella maggior parte dei casi includono correzioni a bug di sicurezza, al fine di proteggere l'iPhone da vulnerabilità ed attacchi.

Abilitare Face ID e Touch ID

Una buona pratica da adottare sul proprio iPhone, per proteggerlo da occhi indiscreti, è quella di abilitare le funzionalità integrate: Face ID o Touch ID (per i modelli meno recenti).

Con Face ID sarà possibile sbloccare il proprio iPhone in seguito al riconoscimento del volto (in altre parole, si sbloccherà solo dopo aver identificato il volto del proprietario del dispositivo); Touch ID, d’altra parte, consentirà lo sblocco del telefono solo dopo aver riconosciuto l'impronta digitale del proprietario.

Similmente all'aggiornamento di sistema, queste funzionalità possono essere abilitate all'avvio del dispositivo (nel caso in cui questo venga acceso per la prima volta), oppure attivate dalle impostazioni di sistema: Configura Face ID o Touch ID e codice.

Gestire le autorizzazioni delle app installate

Per mantenere un buon controllo delle applicazioni che hanno accesso ai nostri dati, è necessario verificare e gestire le autorizzazioni concesse alle app installate sul dispositivo.

Andando nella sezione delle impostazioni dedicata alle applicazioni, sarà possibile verificare, per ciascuna app, a cosa questa ha accesso, come ad esempio: al microfono (e alla possibilità di registrare), ai contenuti multimediali (Foto), ai contatti, alla localizzazione e molto altro ancora.

Per evitare sorprese spiacevoli, si consiglia di attivare solo le autorizzazioni strettamente necessarie al corretto funzionamento di ciascuna app installata.

Attivare la funzionalità “Trova il Mio iPhone”

Prevenire è sempre un ottimo modo per mettersi al riparo da possibili eventi poco simpatici. Per questo motivo, si raccomanda caldamente di attivare la funzionalità offerta da Apple "*Trova il mio iPhone*", presente su tutti i dispositivi prodotti dall'azienda di Cupertino.

Grazie a questa funzionalità, è possibile conoscere sempre la posizione dei propri dispositivi Apple, opzione che si rivela indispensabile nel caso di smarrimento o furto. Inoltre, questa funzionalità offre anche la possibilità di eliminare, da remoto, i contenuti presenti nel dispositivo per evitare che terzi ne abbiano accesso senza alcuna autorizzazione.