Scaricare programmi e app in modo sicuro

Il consiglio di ottenere software solo da fonti affidabili è ben noto. Ma come si determina se una fonte è affidabile?

Punti principali:

- Installate le app per dispositivi mobili solo dallo Store ufficiale (Apple App Store o Google Play Store).
- Installate i programmi per i computer tradizionali solo dal sito ufficiale del produttore.
- Prestate particolare attenzione al software che consente l'accesso remoto al dispositivo.
- **La vostra banca non vi chiederà mai di scaricare un software di terze parti!**

Per i dispositivi mobili, gli App Store ufficiali (per iOS l'iTunes Store e per Android il Google Play Store) sono considerati una fonte piuttosto sicura. Per questo, le app andrebbero sempre scaricate da lì. Non fidatevi delle app dalla reputazione scarsa o delle raccomandazioni di persone che non conoscete. Prima di installare un'app raccogliete informazioni sul fornitore, se non lo conoscete già. Ulteriori informazioni sull'installazione e l'utilizzo di app per dispositivi mobili e, in particolare, di un'app per il Mobile Banking sono disponibili qui (https://www.ebas.ch/it/app-per-il-mobile-banking/) .

Ora anche per i computer tradizionali sono disponibili cosiddetti store che permettono di ottenere software. Tuttavia, è ancora diffusa la pratica di scaricarli e installarli anche da vari siti Internet. L'importante è fare attenzione ad aprire il sito ufficiale del produttore del software. Se non se ne conosce l'indirizzo, è opportuno cercare conferme in diverse fonti. Per esempio, si possono confrontare i risultati dei motori di ricerca con una voce in un'enciclopedia online (p. es. Wikipedia) o con le indicazioni dall'App Store del dispositivo mobile.

Nota bene: la vostra banca non vi chiederà mai di scaricare un software di terze parti!

E poi non trascurate il vostro istinto, specialmente quando osservate il sito Internet. Andrebbero evitate le pagine che sembrano poco serie, magari perché offrono il download gratuito di ogni tipo di software di diversi produttori, sono zeppe di pubblicità ingannevole o mostrano il link per il download solo alla fine di un conto alla rovescia.

Inoltre, prestate particolare attenzione alle applicazioni che consentono l'accesso remoto al dispositivo. Possono essere sfruttate dai truffatori per accedere al dispositivo e raccogliere informazioni sensibili sull'utente o persino riuscire a entrare, ad esempio, nel sistema di e-banking. Prestate particolare attenzione se, ad esempio, qualcuno al telefono vi chiede di installare un programma o un'app che consente l'accesso remoto. Nella maggior parte dei casi si tratta di una truffa.

In generale, è necessario tenere presenti anche le norme di protezione di base, applicando le nostre «5 operazioni per la vostra sicurezza digitale (https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) ». In particolare, per quanto riguarda il download di programmi e app, i punti «2 – monitorare con antivirus e firewall (https://www.ebas.ch/it/2-monitorare-con-antivirus-e-firewall/) » e «3 – prevenire con aggiornamenti software (https://www.ebas.ch/it/3-prevenire-con-aggiornamenti-software/) ».

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

Il termine «software» (parola inglese che letteralmente significa «merce morbida») indica programmi informatici e applicazioni o app (come il sistema operativo, Word o Excel) che rendono il dispositivo funzionale, utilizzabile e utile.

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica