Media e reti sociali

I media sociali come Facebook, Instagram o YouTube sono in pieno boom. A prima vista sembrerebbero non porre nessun problema immediato per l'e-banking. La loro ampia diffusione, unita al loro utilizzato indiscriminato, invece, li rende interessanti anche per i malintenzionati.

Proteggetevi così:

- Pubblicate su di voi soltanto informazioni che condividereste anche con un completo sconosciuto per strada.
- Limitate l'accesso alle informazioni che pubblicate (impostazioni per la privacy).
- Accettate come «amici» soltanto persone che conoscete anche da contesti diversi (p. es. di persona).
- Abbiate una «sana dose di sfiducia» quando ricevete messaggi da persone sconosciute.
- Non fate clic su link provenienti da fonti sconosciute ed eseguite una verifica prima di aprire documenti, immagini, video ecc.
- Utilizzate assolutamente password diverse e sicure per i vari servizi.
- Utilizzate software aggiornato (browser, sistema operativo, antivirus ecc.).

Gli hacker amano i media sociali

Collocando in modo mirato i loro link, i criminali riescono spesso a sfruttare i media sociali come cosiddette «fionde per virus», diffondendo così il proprio software dannoso.

Inoltre, tramite queste reti è possibile acquisire informazioni personali che in una seconda fase potrebbero risultare utili per sferrare attacchi mirati.

Informazioni personali

Nei media sociali si condividono foto e dati personali con gli «amici». Si tratta però di informazioni che possono essere utilizzate anche da un malintenzionato, p. es. per sferrare un attacco di «social engineering» (https://www.ebas.ch/it/social-engineering/) .

Vi invitiamo quindi a riflettere attentamente su quali informazioni pubblicate sul vostro profilo: condividete soltanto dati personali che rivelereste anche a un completo sconosciuto per strada.

Una «sana» dose di sfiducia dovrebbe sempre esserci quando si usano queste reti. Andrebbero accettate soltanto le richieste di amicizia di persone che si conoscono anche di persona o da contesti diversi.

File come documenti, immagini, video ecc. andrebbero sempre verificati prima con un software antivirus. Questo a prescindere che provengano da una fonte affidabile o meno.

Post e interazioni

Non dimenticate che i gestori di un servizio analizzano non solo i dati personali che pubblicate ma anche tutti i vostri contributi (post) e forme di interazione come like, condivisioni ecc.; tutti questi dati vengono poi aggre-

gati in un profilo utente (che potrebbe anche essere sfavorevole o magari errato) e rivenduti, ad esempio per scopi pubblicitari. Questi profili generati si diffondono rapidamente su altri social network, vengono conservati per diversi anni e spesso eliminarli è un'operazione difficoltosa o impossibile.

Nei siti di social networking, quindi, la regola è questa: comunicate non solo con riservatezza, ma sempre in modo ben ponderato!

Link

Basta un clic su un link a un sito Internet dannoso per scaricare del malware sul vostro dispositivo (download drive-by (https://www.ebas.ch/it/download-drive-by/)). Per questo motivo, prima di qualsiasi clic è consigliabile pensare se si vuole davvero vedere il contenuto di quella pagina e se si tratta di una fonte affidabile.

Su www.getlinkinfo.com (http://www.getlinkinfo.com) è possibile eseguire un controllo degli indirizzi cui puntano i link abbreviati (vedi Maggiori informazioni (#moreInfo)).

Oltre a questo è indispensabile mantenere sempre aggiornati all'ultima versione soprattutto il browser, il sistema operativo e il programma antivirus, come pure tutti gli altri software installati («fase 3 – prevenire» (https://www.ebas.ch/it/3-prevenire-con-aggiornamenti-software/)).

Login e password

I requisiti validi per una buona password valgono anche per i media e le reti sociali. I dati d'accesso devono essere trattati con la massima riservatezza.

Inoltre è fondamentale avere password diverse per i diversi servizi. **Non utilizzate in nessun caso la stessa password dell'e-banking per i media e le reti sociali!**

Per proteggere meglio il vostro account social, è sempre opportuno attivare anche l'autenticazione a due fattori (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/).

Protezione dei dati

Quando si parla di media sociali e del loro utilizzo non si può trascurare l'aspetto della protezione delle informazioni personali. Informazioni e regole di condotta a questo riguardo sono pubblicate sul sito Internet dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) (https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/visione-generale/protezione-dei-dati.html).

Impostazioni consigliate

I media sociali presentano molte possibilità di configurazione. Le nostre liste di controllo vi offrono supporto per impostare Facebook (https://www.ebas.ch/it/impostazioni-di-facebook/), Twitter (https://www.ebas.ch/it/impostazioni-di-twitter/), Instagram (https://www.ebas.ch/it/impostazioni-di-instagram/) e LinkedIn (https://www.ebas.ch/it/impostazioni-di-linkedin/) in modo sicuro.

Solo in apparenza i media sociali non hanno nulla a che fare con la sicurezza dell'e-banking, perché per i truffatori va bene qualsiasi fonte quando si tratta di ottenere informazioni.

Bastano pochi provvedimenti efficaci per gestire i nuovi media senza preoccupazioni.

Promemoria: *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2020/01/socialmediaSKP_it.pdf)*

Maggiori informazioni

Alcuni media sociali limitano la lunghezza massima dei post pubblicati. Twitter, ad esempio, consente di scrivere soltanto messaggi da 140 caratteri. Per poter inviare anche link più lunghi, diversi siti Internet offrono un servizio di abbreviazione dei collegamenti. Per esempio,

«https://www.ebas.ch/it/cosa-puo-fare-ognuno/protezione-estesa/social-engineering»

diventa

«http://bit.ly/2lGF1qx»

L'indirizzo abbreviato non consente più di riconoscere direttamente quale sia la destinazione reale del collegamento. È un sistema perfetto per i criminali, che possono abbreviare link che puntano a siti Internet infetti.

Prima di aprire un link abbreviato, quindi, bisognerebbe verificare qual è l'indirizzo originale. Su www.getlinkinfo.com (https://www.getlinkinfo.com), per esempio, è possibile eseguire questo tipo di controllo. Oltre all'indirizzo originale vengono visualizzate anche ulteriori informazioni sulla pagina Internet.