03.03.2022

Facciamo impazzire i truffatori delle banche

I criminali informatici usano metodi sempre nuovi per carpire denaro alle loro vittime. Vi segnaliamo un video che con molto umorismo richiama l'attenzione su un pericolo attuale.

Anche se per scopi di intrattenimento, il video presenta un metodo molto attuale utilizzato dai criminali informatici – giudicate con i vostri occhi: www.youtube.com/watch?v=8_5eQw-kdyM (http://www.youtube.com/watch?v=8_5eQw-kdyM)

Le seguenti misure vi proteggono dai rischi menzionati nel video, nel quale l'indirizzo dell'istituto finanziario per accedere al portale di e-banking viene inserito nella finestra di ricerca di Google:

- Inserite l'indirizzo del vostro istituto finanziario sempre manualmente, direttamente nella barra degli indirizzi del browser – non nella finestra di ricerca di Google!
- Non digitate mai frasi come «login miabanca» o «e-banking miabanca» o simili nella finestra di ricerca di Google. Google mostra gli annunci (anche quelli dei truffatori!) prima dei risultati effettivi della ricerca. Non fate mai clic su questi annunci, se contengono il nome del vostro istituto finanziario.
- Assicuratevi che la connessione sia sicura (icona a forma di lucchetto, nome dell'istituto finanziario giusto e nome del dominio corretto).

Nel video si parla anche dell'assistenza remota. Si tratta di una tecnologia utilizzata per ottenere aiuto esterno per il proprio dispositivo senza che un tecnico debba recarsi sul posto. Anche gli istituti finanziari si avvalgono di questa possibilità come parte del loro supporto o helpdesk. Quando utilizzate questa tecnologia, prendete questi provvedimenti:

- Non digitate numeri telefonici dell'assistenza o dell'helpdesk che vedete negli annunci su Google.
- Instaurate connessioni soltanto con persone di fiducia. Agite sempre con particolare cautela soprattutto quando non siete voi ad avviare la connessione.
- Utilizzate una connessione sicura (icona a forma di lucchetto, nome dell'istituto finanziario giusto e nome del dominio corretto).
- Non conferite mai autorizzazioni di accesso completo al vostro sistema. Chi vi aiuta dovrebbe avere soltanto la possibilità di osservare passivamente.
- Ricordate che tutto ciò che viene visualizzato sullo schermo può essere visto e anche registrato dall'altra persona.
- Non aprite siti Internet che non hanno nulla a che vedere con la sessione in questione – nemmeno se vi viene chiesto di farlo.
- Assicuratevi che la connessione di assistenza remota venga chiusa dopo aver ricevuto l'assistenza, così da impedire ulteriori accessi al vostro dispositivo.