

Qualche consiglio per ridurre il rischio di subire un furto di identità o una frode creditizia

Alcuni suggerimenti per evitare che qualcuno ti rubi l'identità e la utilizzi per richiedere finanziamenti o danneggiarti in altri modi.

1. Hai ricevuto un'e-mail che richiede i tuoi dati personali o credenziali d'accesso? Non rispondere

Se ricevi email in cui ti richiedono dati personali, **username e password del servizio di home-banking** o di collegarti al sito della banca per delle verifiche tecniche, **non rispondere mai**, anche se il mittente sembra essere davvero un istituto di credito. Ricorda, infatti, che una banca **non ti chiederà mai via email le tue credenziali** di accesso al servizio di home-banking, gli estremi delle tue carte di credito o altre informazioni personali. Se hai un dubbio, contatta direttamente il tuo istituto.

2. Stai per comprare su un sito di e-commerce? Controlla che sia attendibile e sicuro

Quando fai acquisti on line, ricordati di verificare sempre gli strumenti di sicurezza del sito. Prima di fornire gli estremi della tua carta, assicurati che la pagina su cui stai effettuando la registrazione o il pagamento **sia contrassegnata dalla presenza di un lucchetto**, caratterizzata dall'estensione **"https" anziché "http"**, visualizzabile nella barra degli indirizzi del browser di navigazione. Questi elementi indicano la presenza di un canale sicuro che ci consente di poter comunicare in sicurezza i tuoi dati, **compresi quelli della tua carta di pagamento.**

3. Distruggi tutta la documentazione che riporta i tuoi dati personali prima di cestinarla

Uno dei modi più frequentemente utilizzati dai ladri d'identità per raccogliere informazioni personali sulla vittima è quello di **rovistare tra i rifiuti (trashing)** o impadronirsi della loro posta. Presta particolare attenzione, quindi, alla tua corrispondenza, **agli estratti conto bancari e alle ricevute di pagamento** che contengono numero e data di scadenza della tua carta.

4. Ti hanno chiesto una copia dei tuoi documenti? Attenzione agli occhi indiscreti

Spesso viene richiesto di lasciare copia dei propri documenti, non solo quando andiamo in un albergo ma anche per espletare pratiche burocratiche di varia natura. È bene farlo **solo se strettamente necessario** e soprattutto se sei sicuro della serietà con cui vengono trattati i tuoi dati personali. Inoltre, in caso di variazione dell'indirizzo di residenza, comunica tempestivamente il tuo nuovo recapito alla tua banca e a tutti i soggetti con cui intrattieni rapporti. Se ritrovi, infine, un documento di cui avevi precedentemente denunciato il furto o lo smarrimento comunicalo all'ufficio di Polizia più vicino.

5. Prenditi cura della tua identità e della tua privacy sul web e i social network

Molti utenti utilizzando i social network non si preoccupano di proteggere i propri dati personali.

Impara a gestire la tua identità digitale: quando ti iscrivi, **utilizza una email personale** e non quella di lavoro, non consentire al social network di memorizzare la tua password, **imposta correttamente il livello di privacy sul tuo profilo**, seleziona con attenzione foto, video e informazioni personali da pubblicare, utilizza la funzione di log out per uscire dal social network, una volta conclusa la navigazione. Molti di questi elementi possono essere utilizzati da male intenzionati per costruire una falsa identità.

6. Aggiorna sempre l'antivirus del tuo pc

Per salvaguardare la sicurezza dei tuoi dati è fondamentale **tenere aggiornato il sistema antivirus** del tuo computer. È importante, inoltre, dotarsi di un programma capace di controllare le comunicazioni che avvengono tra il computer e la rete, in modo da poter bloccare tempestivamente quelle non autorizzate. **Questo programma è chiamato il firewall.**

7. Tieni sotto controllo i movimenti del tuo conto corrente con l'home-banking

Oggi i sistemi di home-banking ti consentono di avere sempre a portata di click i tuoi conti, quindi approfittane per controllare frequentemente il tuo estratto conto e segnala subito alla tua banca eventuali transazioni che non riconosci. Questo ti consentirà di intercettare tempestivamente anche l'addebito di rate di finanziamenti ottenuti fraudolentemente a tuo nome.

8. Non perdere di vista la carta o il bancomat quando paghi

Non perdere mai di vista la tua carta di credito e il tuo bancomat quando effettui i tuoi acquisti.

Le frodi causate da utilizzi impropri delle carte di pagamento sono in forte aumento. Controlla che non ci siano **manomissioni o anomalie** nell'apparecchiatura del bancomat; non digitare i codici segreti sotto occhi indiscreti; non gettare le ricevute di pagamento che contengono numero e data di scadenza della carta; **non perdere mai di vista la tessera** (es. al ristorante). In caso di furto o smarrimento, contatta immediatamente le società emittenti per **richiedere il blocco della carta**. Inoltre, controlla sempre che le buste con cui la banca invia la tessera e, successivamente, il Pin siano integre ed originali e conserva i codici segreti della carta di credito e bancomat separatamente, **evitando di tenerli nel portafoglio.**

9. Non fornire le tue informazioni a sconosciuti

Custodisci con cura le informazioni che ti riguardano e non lasciarti convincere a fornire i tuoi dati a persone che non conosci a meno che non sussistano motivazioni reali. Le informazioni **non vengono sottratte solo accedendo ai PC**, ma anche sfruttando il **Fattore Umano**, ovvero convincendo e raggirando le persone per ottenerle, con o senza l'ausilio di strumenti tecnologici.