COMUNICATO CONGIUNTO

# Banche, Vademecum per una ulteriore sicurezza e protezione dei dati personali

ABI e Polizia di Stato promuovono un Vademecum con i consigli utili per mantenere sempre alto il livello d'attenzione alla protezione dei propri dati personali.

Si tratta di pochi semplici accorgimenti e buone prassi, forniti con un linguaggio semplice e diretto per ridurre i fattori di vulnerabilità e i comportamenti potenzialmente rischiosi.

Il progetto è stato realizzato dall'Associazione Bancaria in collaborazione con prestigiosi e qualificati interlocutori quali OSSIF (il centro di ricerca dell'ABI sulla sicurezza anticrimine), CERTFin (l'iniziativa cooperativa pubblico-privata diretta dall'ABI e dalla Banca d'Italia finalizzata a innalzare la capacità di gestione dei rischi cibernetici degli operatori bancari e finanziari), la Polizia Postale e le Associazioni dei Consumatori (ACU, Adiconsum, Adoc, Asso-Consum, Assoutenti, Casa del Consumatore, Centro Tutela Consumatori Utenti (CTCU), Cittadinanzattiva, Codacons, Confconsumatori, Federconsumatori, Lega Consumatori, Movimento Difesa del Cittadino, Movimento Consumatori, Unione per la Difesa dei Consumatori (UDICON), Unione Nazionale Consumatori).

Il Vademecum, da oggi facilmente consultabile sul sito dell'Associazione Bancaria nella sezione dedicata https://www.abi.it/Pagine/Mercati/Crediti/Crediti-alle-persone/Le-guideabi.aspx e sul portale della Polizia Postale www.commissariatodips.it va ad affiancarsi agli strumenti e alle iniziative già realizzate in materia di sicurezza dall'ABI, istituzioni e singole banche. Un esempio è la campagna di comunicazione avviata nei mesi scorsi "I Navigati" sulle buone pratiche da adottare per un uso "informato e sicuro" degli strumenti e dei canali digitali.

Infine, oltre a fornire indicazioni su come meglio comportarsi per agire in sicurezza, il Vademecum offre anche delle informazioni rispetto a cosa fare quando si è vittima di truffe.

Ecco i 12 semplici accorgimenti da seguire per proteggere la propria identità:

1. In caso di smarrimento o furto di documenti personali, recarsi immediatamente dalle Autorità di polizia preposte per sporgere denuncia. In caso di furto o smarrimento di carte di credito e/o di debito, dopo averne ordinato il blocco chiamando il numero messo a disposizione, la denuncia va comunicata anche alla propria banca.

2. Fare molta attenzione nello smaltimento della documentazione cartacea che contiene informazioni personali (es. estratti conto, utenze domestiche): è opportuno rendere illeggibili i dati sensibili riportati nei documenti prima di cestinarli.

3. Proteggere con cura le credenziali di accesso ai conti online e i codici delle carte di credito e/o di debito e tutti gli altri codici di accesso (es. lo SPID); se si sceglie di salvare questi dati sui propri dispositivi (es. computer e/o cellulare) assicurarsi che siano adeguatamente protetti (es.

cifrati). Allo stesso modo occorre tenere sempre attentamente custodite le credenziali e i codici utili a disporre della propria firma digitale.

4. Salvaguardare le proprie carte di pagamento dotate di tecnologia cd. "contactless" (ovvero quelle per cui non è richiesto l'inserimento nel POS per effettuare la transazione), con custodie schermate (rivestite in alluminio) per ridurre al minimo la possibilità di essere vittime di truffe che prevedano la lettura del chip [es. con comunicazione RFID (identificazione con la radiofrequenza) e NFC (identificazione attraverso comunicazione di prossimità)]. Occorre comunque ricordare che ci sono delle regole che limitano i rischi: il PIN è sempre richiesto per le operazioni al POS sopra i 50 euro; dopo 5 pagamenti consecutivi al POS senza digitare il PIN, il successivo, anche se di piccolo importo, necessita dell'autenticazione forte del cliente (c.d. SCA) e cioè dell'inserimento del codice segreto/PIN; analogamente se l'ammontare dei pagamenti disposti al POS "senza contatto" a partire dalla data dell'ultima applicazione della SCA supera complessivamente i 150 euro occorre inserire il codice segreto/PIN.

5. Cambiare frequentemente le credenziali di accesso (le password) per entrare nei conti online ed evitare di utilizzare password che potrebbero essere facilmente individuate dai frodatori (es. la data di nascita). In generale, una password, per avere un livello di sicurezza considerato adeguatamente tutelante, deve essere caratterizzata da lettere maiuscole e minuscole, numeri e caratteri speciali.

6. È importante imparare a riconoscere i messaggi autentici dai messaggi fraudolenti. Le banche: non chiedono mai, né tramite posta elettronica, né telefonicamente, né con messaggi sms, le credenziali di accesso al conto e i codici delle carte del cliente. Qualora si ricevano richieste di questo tipo, avvisare la propria banca per avere conferma della sua estraneità all'invio ed evitare di dare alcun riscontro alla richiesta ricevuta; non inviano mai e-mail contenenti link se non nell'ambito di un processo avviato dall'utente (es. modifica e-mail personale, aggiornamento documento di riconoscimento). Qualora il cliente ricevesse un messaggio con link dalla banca senza preventiva richiesta da parte sua, occorre avvisare la propria banca per avere conferma della sua estraneità all'invio ed evitare di dare alcun riscontro alla comunicazione ricevuta.

7. Ogni volta che si usa un computer pubblico per accedere al proprio conto online, occorre poi ricordarsi di chiudere la sessione (logout). Inoltre, è sempre preferibile digitare personalmente l'indirizzo online della propria banca e non cliccare su indirizzi già memorizzati. Se la connessione è pubblica, è maggiore il rischio che possibili malintenzionati sfruttino la connessione precedentemente aperta per carpire informazioni.

8. I messaggi fraudolenti contengono spesso link malevoli (attraverso cui il computer e/o cellulare vengono violati) o collegamenti per reindirizzare l'utente su siti clone (utilizzati per carpire informazioni personali). Per questo motivo, è fondamentale non cliccare mai su questi link.

9. Diffidare da presunti operatori che contattano le potenziali vittime affermando di aver bisogno di informazioni personali, bancarie o di credito, per verificare l'identità o per sapere dove inviare pacchi, denaro, vincite fasulle o documenti legati alla giustizia.

10. Nel caso il proprio cellulare non sia più in grado di effettuare/ricevere chiamate, verificarne i motivi contattando il proprio operatore telefonico: si potrebbe essere vittima di una frode effettuata tramite scambio della tua scheda telefonica (ovvero una truffa denominata Sim Swap).

11. Utilizzare con attenzione e prudenza i canali social e soprattutto non comunicare e non condividere mai attraverso questi canali dati personali o finanziari.

12. Scegliere un programma antivirus e mantenerlo sempre aggiornato, installare regolarmente gli aggiornamenti del sistema operativo utilizzato in modo da proteggere tutte le apparecchiature e i dispositivi in uso da infezioni da malware.

Roma, 28 aprile 2022