BANCHE: accesso non autorizzato a dati di clienti Unicredit

28 Ottobre 2019

Comunicato stampa Unione Nazionale Consumatori

Attenti al phishing. I consumatori prestino cautela nei prossimi mesi. Il decalogo da seguire.

Roma, 28 ottobre 2019 – Unicredit ha identificato un caso di accesso non autorizzato a dati relativi a un file generato nel 2015 che conteneva circa 3 milioni di records, composto solo da nomi, città, numeri di telefono ed e-mail. Lo comunica la banca stessa, che rassicura sul fatto che non sono stati compromessi altri dati personali, né coordinate bancarie in grado di consentire l'accesso ai conti dei clienti o l'effettuazione di transazioni non autorizzate.

"Bene ha fatto Unicredit ad avvisare la sua clientela. Anche se non sono stati acquisiti dati per l'accesso ai conti o per transazioni non autorizzate, si tratta di un fatto comunque preoccupante sul quale speriamo la polizia postale riesca a fare piena luce" dichiara Massimiliano Dona, presidente dell'Unione Nazionale Consumatori.

"I consumatori devono ora prestare molta attenzione e avere particolari cautele, seguendo speciali precauzioni nei prossimi mesi. Ad esempio potrebbe esserci un aumento delle truffe informatiche, il cosiddetto phishing. Gli hacker potrebbero inviare ai clienti Unicredit e-mail personalizzate, con il logo contraffatto dell'istituto di credito, invitandoli ad accedere al sito per motivi di sicurezza, prendendo a pretesto proprio il loro attacco" prosegue Dona.

"Non per niente Unicredit stessa si è premurata di informare che contatterà i clienti solo tramite posta tradizionale e/o notifiche via online banking e ha messo a disposizione un numero verde dedicato. Suggeriamo, comunque, il cambio della password" conclude Dona.

Di seguito alcuni consigli:

1. **Attenti al phishing.** Non accedete a nessun sito, anche se a voi noto, cliccando da un indirizzo elettronico ricevuto via email. Può essere un'email contraffatta con grafica e logo della ditta e/o banca a voi nota che vi chiede di riassumere dati personali o vi rimanda ad una finta pagina web del tutto simile all'originale;
2. **Non rispondete** mai ad email senza aver prima verificato l'indirizzo di provenienza. Non basta, infatti, che il nome dell'utente corrisponda. Quello che conta è l'indirizzo email;
3. **Mai aprite allegati** senza aver prima accertato l'effettiva provenienza dell'email;
4. **Dati riservati.** Non date mai online il vostro nome, indirizzo, telefono, età, nome o altri dati personali ad indirizzi email di persone a voi ignote;

5. **Dati segreti.** Non date mai online a nessuno, neanche a persone note, il vostro numero di codice fiscale, il luogo e la data di nascita o il numero della carta d'identità;
6. **Verificate** se il sito della vostra banca è protetto. I siti delle banche, quando si accede al proprio conto, devono essere protetti da sistemi di sicurezza internazionali come SSL e SET: sono riconoscibili dal simbolo di un lucchetto chiuso nella barra di indirizzo.
7. **Cambiate la password.** Periodicamente è opportuno cambiarla, meglio ogni 3 mesi. Prima di effettuare il cambio, controllate se il sito è in connessione cifrata "Ssl". Usate password con come minimo 10 caratteri, con combinazioni di numeri e lettere, maiuscole e minuscole e almeno un carattere speciale, tipo virgola, punto e virgola o due punti. Il proprio nome con l'aggiunta di un numero, magari la propria data di nascita, è decisamente da evitare. Mai password, insomma, con propri dati personali. Nemmeno le sequenze di tasti, tipo asdf, qwerty, 1234 sono sicure. Non utilizzare, infine, le stesse password per più account. Non lasciare la password scritta in posti raggiungibili da altri. Meglio se riuscite a memorizzarla.
8. **Estratto conto.** Dopo aver fatto un acquisto non sarebbe male controllare i successivi estratti conto.
9. **Utilizzare software e browser completi ed aggiornati:** il primo passo per la sicurezza è avere un buon antivirus aggiornato. Per una maggiore sicurezza online, inoltre, è necessario aggiornare all'ultima versione disponibile il browser utilizzato per navigare.
10. **Download.** Non **s**caricate nulla e non installate programmi da siti che non siano sicuramente affidabili.