

11 novembre 2019 16:04

Attacco hacker a Unicredit: rubati dati di 3 milioni di clienti. Banca non chiara. Denuncia al Garante Privacy. Come tutelarsi

di [Emmanuela Bertucci](#)



Alcuni correntisti **Unicredit** hanno ricevuto una lettera da parte della banca, altri hanno scovato la stessa comunicazione “imboscata” nel proprio profilo di homebanking, spulciando in una di quelle sottopagine di cui tanti di noi quasi ignorano l'esistenza: **a seguito di un “accesso non autorizzato” sono stati hackerati nome, cognome, comune e provincia di riferimento, numero di telefono cellulare e indirizzo email di 3.000.000 (tre milioni...) di clienti Unicredit.**

Questa una segnalazione ricevuta da un risparmiatore che ha scritto ad Aduc

“Gentili Signori,

che cosa bisognerebbe dire o fare in casi simili? Unicredit non ha mandato nessun avviso e-mail o sms di invio di documentazione importante, nè, accedendo all'internet banking, si ha alcun alert di documentazione in giacenza da leggere. Per curiosità, oggi ho voluto aprire tutte le categorie di documenti, in una di queste denominata "altri documenti" mai aperta prima, mi appare miracolosamente una lettera che avvisa: "è stato individuato un accesso non autorizzato a dati relativi a clienti tra cui anche i Suoi" ecc.ecc. a seguire consigliato il "decalogo di sicurezza" per i correntisti. Sembra una beffa... dopo il danno. Rubano i miei dati a te e tu dici a me di prestare attenzione! ma io cosa dovrei fare ora che i miei dati sono in mano a chissà chi e questo chissà chi chissà cosa se ne farà? (scusate il gioco di parole) Non so cosa dire a riguardo, davvero imbarazzante, preoccupante, disarmante... vorrei chiedere se ci sono consigli "seri" che potete dare in questi casi per tutelarci, per rispondere alla banca, per essere risarciti del danno (?) o cos'altro... dicono che sono stati carpiati "solo" dati anagrafici come se fosse poca cosa... ma davvero? cos'altro non lo sapremo mai? Grazie per il sempre cortese ascolto e scusate lo sfogo. Cordiali saluti”

Non è la prima volta che accade.

Il **25 luglio 2017** Unicredit ha segnalato al [Garante per la protezione dei dati personali](#) una **intrusione informatica a danno di 762.000 clienti**, nel corso della quale sono stati trafugati **dati anagrafici e di contatto, professione, livello di studio, estremi identificativi di un documento di identità nonché informazioni relative a datore di lavoro, salario, importo del prestito, stato del pagamento, “approssimazione della classificazione creditizia del cliente” e identificativo Iban.**

Il **22 ottobre 2018** Unicredit ha segnalato al Garante per la protezione dei dati personali un attacco informatico a seguito del quale sono stati **individuati 735.519 codici identificativi personali** per accedere all'home banking e, tra questi, sono state individuate **6.859 password di conti** che Unicredit ha bloccato. In ragione di quanto accaduto, il [Garante](#) ha ordinato ad Unicredit di comunicare a ciascun cliente interessato dell'avvenuto hackeraggio, la natura della violazione, il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni, descrivere le probabili conseguenze della violazione dei dati personali, descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Quest'ultimo attacco hacker ha causato l'accesso ad una mole imponente di dati (**3 milioni di nomi, cognomi, numero di telefono e indirizzi email**) ma a nostro avviso Unicredit non ha finora comunicato efficacemente ai propri clienti l'accaduto:

- ha pubblicato un comunicato stampa, non sul sito utilizzato dai correntisti (<http://www.unicredit.it>) ma sul [sito di Unicredit Group](#), pochi quindi lo leggeranno (probabilmente solo chi, come noi, l'ha appositamente cercato);

- il testo del comunicato non spiega quando è avvenuto l'attacco ma si limita a dire che i dati rubati facevano parte di un file del 2015 (che vuol dire ben poco, in tanti dal 2015 ad oggi continuano ad avere lo stesso nome, cognome, numero di telefono, indirizzo email);
- nelle lettere cartacee che sta inviando ai clienti per informarli dell'accaduto, a nostro avviso non è sufficientemente chiara ed esplicita nello spiegare quali possono essere le conseguenze di tale furto. Si "*limita*" a ricordare che il furto ha riguardato "*esclusivamente dati anagrafici*" (come se si trattasse di dati irrilevanti) e che non essendo stati rubate credenziali di accesso, sta ai singoli clienti non divulgare codici personali e password poiché Unicredit non chiede mai via email o telefono di fornire tali dati;
- la comunicazione inviata via homebanking è – stando a quanto ci riferiscono alcuni utenti – priva di alert o notifiche di comunicazioni importanti, inserita sì nei meandri del profilo homebanking ma non immediatamente visibile o adeguatamente segnalata.

Abbiamo quindi inviato una [segnalazione al Garante per la protezione dei dati personali](#), affinché ordini a Unicredit di comunicare, in modo adeguato, a tutti i clienti coinvolti quanto accaduto, le possibili conseguenze della violazione dei dati personali e descrivere le misure adottate per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Ai risparmiatori coinvolti suggeriamo di non sottovalutare l'accaduto, poiché il pregiudizio che può derivare dal furto è particolarmente grave, trattandosi di dati univocamente e direttamente identificativi che possono essere utilizzati come chiavi di ricerca per individuare in rete l'interessato e conseguentemente accedere anche ad altre informazioni a lui riferibili, e che potrebbero essere utilizzate per rivolgere agli interessati comunicazioni telefoniche o messaggi di [phishing a scopo fraudolento](#).

A scopo cautelativo, sarebbe opportuno cambiare indirizzo di posta elettronica e numero di telefono, chiedere a Unicredit che fornisca una informativa chiara e completa su quanto è accaduto e, qualora ciò non accadesse, inviare una segnalazione al Garante Privacy e valutare l'opportunità di cambiare banca.