La guida

di Antonio Scuglia

Sono in costante aumento i tentativi di truffe informatiche

Falsi sms, email e chiamate I trucchi per svuotarci il conto

Le truffe segnalate allo sportello pisano dell'associazione Adusbef Ecco come evitarle e, se ci siamo cascati, come limitare i danni

Pisa Accade sempre più spesso che gli utenti di servizi di pagamento on line cadano vittima di una nuova e sempre più sofisticata frode nota come la truffa del "messaggino", che consiste nell'invio da parte del malfattore di un messaggio all'ignaro utente, del tutto simile a quelli autentici già ricevuti dalla propria banca, con il quale viene avvisato della violazione del conto on line, oppure del prossimo blocco su di una sua carta.

«La forza suggestiva di questa frode informatica – spiega l'avvocato Alberto Foggia, responsabile provinciale dell'Adusbef – risiede, appunto, nella capacità del messaggio sms di rendersi apparentemente autentico agli occhi di chi lo riceve».

Il truffatore infatti riesce a camuffare il numero mittente dell'sms e sostituirlo con una stringa alfanumerica in grado di assomigliare in tutto e per tutto agli sms originali inviati dall'istituto di credito al proprio cliente.

Ricevuto il messaggio – che può arrivare anche per email – l'utente, intimorito dalla possibile effettuazione di operazioni fraudolente sul proprio conto, seguirà le istruzioni, cliccando un link che in realtà lo manderà su una pagina web identica a quella della propria banca e che servirà a carpire le credenziali per finalizzare l'operazione fraudolenta: «Il punto di forza degli attacchi spoofing è certamente quello di far credere alle vittime di stare realmente interagendo col proprio istituto bancario», continua l'avvocato.

Una finalità che può essere raggiunta anche attraverso un diverso schema di attacco: il caller id spoofing, nel quale la frode si svolge anziché via sms attraverso un contatto telefonico, nel quale l'id chiamante è quello del servizio clienti della propria banca.

Queste tipologie di frodi riescono molto spesso a carpire la fiducia dei consumatori, anche perché gli schemi di attacco sono ben curati e non più grossolani come un tempo (ovvero quando venivano inviate per lo più email da indirizzi improbabili e con testi sgrammaticati) e, soprattutto, anche i colloqui del falso operatore sono ben strutturati e capaci sempre di superare le possibili resistenze dell'interlocutore che, ricordiamolo, non ha dubbi sulla veridicità di quanto accade poiché apparentemente il numero chiamante è quello del proprio intermediario.

I ricorsi all'Abf

Dato il sofisticato meccanismo della frode e la sua complessità anche sotto il profilo informatico, non sono mancate decisioni favorevoli al rimborso degli importi sottratti al consumatore da parte dell'Arbitro Bancario Finanziario (Abf) , sistema di risoluzione delle controversie che possono sorgere tra i clienti e le banche e gli altri intermediari in materia di operazioni e servizi bancari e finanziari alternativo a quello della tutela giudiziale; il vantaggio del ricorso all'ABF è sicuramente rappresentato dai tempi (meno di un anno per ottenere una decisione) e dai (minimi) costi (20 euro) .

Nella più recente giurisprudenza Abf, infatti, viene particolarmente valorizzata la complessità dell'attacco sotto il profilo della sua capacità di convincere la vittima sulla veridicità delle comunicazioni, resa possibile da un illusionismo informatico in grado di far apparire come realmente provenienti dalla banca messaggi e comunicazioni telefoniche.

L'avvocato Alberto Foggia, responsabile della delegazione pisana dell'Adusbef (Associazione Difesa Utenti Servizi Bancari e Finanziari)

> La frode è basata sull'apparente "genuinità" del messaggio e di chi lo invia

> I malfattori sono abilissimi nel fingere di essere davvero la nostra banca

L'ingenuità non è ammessa

Precisa l'avvocato Foggia: «Non possiamo trascurare, però, come proprio l'Abf abbia valorizzato l'importanza degli aspetti legati al testo dell'sms ed al suo attento esame. Infatti, qualora lo stesso presenti errori evidenti di testo o contenga un link la cui stringa sia del tutto inconferente con lo scenario di frode costruito dal cosiddetto "attaccante" (ovvero l'hacker) non vi sarà possibilità di rimborso per l'utente a causa di una sua condotta negligente nel non aver prestato attenzione alla inattendibilità della comunicazione».

La delegazione pisana di Adusbef ha registrato numerosi casi di clienti vittime di sms spoofing, anche con significative varianti nella fase di attacco. Non sono infatti mancati casi nei quali la vittima ha ricevuto non solo l'sms, ma anche la chiamata del falso operatore dell'istituto di credito. «Come associazione di consumatori, – spiega il legale, – Adusbef sta curando casi di numerosi utenti di servizi di pagamento e ottenendo diversi rimborsi».

Tra le varie attività svolte vi è stata anche quella divulgativa, per cercare di mettere in guardia i consumatori. In primo luogo, bisogna ricordare sempre che la banca non risolve problemi di sicurezza dei nostri conti on line contattandoci al telefono o chiedendoci dati, che vi è obbligo per l'utente di conservare con cura e non cedere mai le proprie credenziali di accesso al conto on line. Infine, davanti a simili scenari di frode, la necessità di contattare subito il proprio istituto di credito per opportuni accertamenti e il blocco delle operazioni.

Un caso pratico

Tra i molti casi affrontati dalla delegazione pisana di Adusbef, sono ricorrenti quelli dell'sms apparentemente proveniente dalla propria banca nel quale viene segnalato un alert di sicurezza. Poco dopo segue anche una telefonata nella quale un sedicente operatore conferma il (falso) problema, annunciando l'invio di un codice sul cellulare utile alla risoluzione del problema. In realtà, con tali attività venivano poste in essere le operazioni fraudolente.

Che fare?

Una volta disconosciute (come tali) dette operazioni e richiesto il rimborso delle somme sottratte al proprio intermediario, tale domanda viene puntualmente respinta (solitamente il diniego è standardizzato). «A quel punto – dice l'avvocato, – nell'interesse dell'associato abbiamo proposto ricorso all'Abf per veder riconosciuto il diritto al ristoro degli importi prelevati dall'hacker, evidenziando, tra gli altri, la particolare decettività della frode eseguita con sms spoofing e sinergico "attacco" di caller id spoofing, che di fatto non aveva permesso alla vittima di avvedersi in tempo del piano criminoso posto in essere a suo danno». Iniziativa risolta positivamente stante la particolare aggressività della frode in esame, capace di fatto di intromettersi nel canale di comunicazione cliente /banca attraverso il quale l'istituto di credito invia i codici Otp autentici, utili ad eseguire realmente le operazioni di pagamento telematiche.

© RIPRODUZIONE RISERVATA

Il glossario

Si chiama spoofing la manipolazione dei dati del mittente

Viene chiamata Sms spoofing la tecnica che consiste nella manipolazione dei dati relativi al mittente di un messaggio per far sì che appaia provenire da un soggetto differente, rimpiazzando il numero originario con un testo alfanumerico (ossia quello utilizzato dall'intermediario per i propri messaggi genuini). In tal modo, il truffatore può inviare sms civetta che sembrano provenienti da numeri o contatti legittimi.

Caller id spoofing è invece la tecnica con la quale viene falsificato l'identificativo del chiamante in una telefonata.

In genere si distingue fra phishing, vishing e smishing, ma la sostanza è sempre la stessa. cambia solo lo strumento. Il phishing propriamente detto inizia con l'invio di un'email che contiene un'offerta allettante o richiede un'azione sollecita come compilare un modulo, cliccare su un link o aprire un allegato. Il vishing è quello effettuato tramite servizi di telefonia: qui i truffatori si spacciano per un call center (di una banca ad esempio) e chiedono alla vittima di fornire i suoi dati ad un operatore. Nello smishing invece viene utilizzato l'Sms.

La sede pisana dell'associazione Adusbef può essere contattata al numero di tel. 050.542786, email foggiamerico@gmail.com

L'avvocato Alberto Foggia è anche curatore, insieme all'avvocato Edoardo Ferragina, della collana giuridica di cui fa parte il volume di Francesco Cocchi "Phishing e nuovi attacchi informatici. Modalità operative e strategie difensive", che si può acquistare su Amazon (www.amazon.it/Phishing-informatici-operative-strategie-difensive/dp/8894863069).