HOME BANKING

Truffa online: ecco quando la banca rimborsa in caso di phishing

I servizi di home banking consentono di accedere e gestire il conto corrente in tutta semplicità, ma allo stesso tempo ci espongono al rischio elevato di truffa online via phishing. Ecco come riconoscere una trappola, cosa fare se rimaniamo vittime di un raggiro e quando abbiamo diritto al rimborso

30 Mar 2021

Camillo Campli
associate, De Berti Jacchia

Giuseppe Cristiano
partner, De Berti Jacchia

L'accesso al proprio conto corrente mediante i **servizi di home banking** è sempre più diffuso: che avvenga dal PC o dallo smartphone, si tratta di un **sistema molto pratico** ma allo stesso tempo **esposto a numerosi rischi** e, per questo motivo, non è difficile rimanere vittime di una truffa online.

Indice degli argomenti

Cosa accadrebbe, infatti, se le nostre credenziali di autenticazione, custodite nei dispositivi, dovessero finire nelle mani di un malintenzionato e ci trovassimo con il conto corrente svuotato il giorno dopo? Le truffe online, al giorno d'oggi, sono molteplici e possono presentarsi in diversi modi. Inutile dire che, nell'era dello smart working e della connessione costante ai nostri dispositivi personali, il fenomeno delle truffe online ha vissuto un vero e proprio boom. Secondo un report della Polizia Postale, nel 2020 sono stati ben 98.000 i casi di truffa online. Una delle modalità più diffuse è il cosiddetto **phishing**, un particolare tipo di attacco informatico che consente ai criminali di ottenere codici utente e password che permettono l'accesso a conti correnti o altri servizi utilizzati dalle vittime. Il nome stesso di questa peculiare tecnica di sottrazione dei dati personali richiama il termine inglese "fishing", ossia pescare; il riferimento alla pesca è quantomai pertinente in quanto il criminale, gettata l'esca, attende che la vittima abbocchi così da "pescarne" i dati.

terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

SCARICA ORA

Come avviene una truffa online

Solitamente, il phishing comincia con l'invio di un messaggio di posta elettronica alla vittima. Tale messaggio proviene apparentemente da banche, istituti finanziari, erogatori di servizi (società elettriche, idriche, del gas, società di servizi di pagamento online o simili), da agenzie governative (persino dall'agenzia dell'entrate) o siti web (ad esempio, siti di e-commerce) e allerta la vittima di un problema che è stato riscontrato su queste piattaforme. Per risolvere il problema, la vittima viene quindi invitata a visitare la pagina internet del servizio, tramite un apposito link contenuto nell'email. Se l'utente clicca sul link, viene rimandato a una pagina Web che, riproducendo artatamente quella originale del servizio utilizzato, gli consente di digitare le proprie credenziali di accesso al servizio. Qualora l'utente inserisca lo username e la password nella finta pagina Web, la truffa online è praticamente compiuta. I dati saranno nella disponibilità dei criminali, che li utilizzeranno per accedere ai profili realmente controllati dalla vittima (conti correnti, servizi di pagamento ecc.). Quella sopra descritta è solo una delle tante tipologie di truffa online. I criminali del web hanno infatti architettato e affinato le più svariate tecniche per ottenere accesso ai dati delle carte di credito o dell'home banking del malcapitato di turno. Oltre al phishing

“tradizionale”, tramite e-mail, abbiamo lo smishing, dove il messaggio fraudolento è inviato tramite SMS, o il caller ID spoofing, che consiste nel mascherare il numero del chiamante facendolo apparire come il numero verde di un istituto bancario, in modo che la vittima si fidi e comunichi le proprie credenziali di autenticazione. Non da ultimo, il SIM Swapping: una particolare tipologia di truffa con cui il criminale dichiara falsamente, contattando o recandosi in un centro assistenza, di aver smarrito o subito il furto del cellulare. Il truffatore chiede quindi di disabilitare la vecchia SIM (in realtà appartenente ad altro soggetto) al fine di ottenerne una nuova con lo stesso numero, impossessandosi, di fatto, del numero della vittima. Questa tecnica risulta particolarmente efficace se combinata con il possesso delle credenziali di accesso dell’home banking della vittima, in quanto consente di aggirare anche i sistemi di autenticazione a due step basati sull’invio di SMS con One Time Password da parte degli istituti bancari per autorizzare le transazioni. La vittima di SIM Swap constaterà semplicemente la perdita di segnale sul proprio cellulare (dovuta alla disattivazione della sua SIM originale), mentre il truffatore riceverà sulla nuova SIM clonata le OTP per eseguire le operazioni desiderate.

Cosa può fare la vittima in caso di truffa online dovuta al phishing

Naturalmente, prestando un minimo di attenzione, è possibile riconoscere un tentativo di phishing e, quindi, difendersi da questa particolare tipologia di truffa. Per poterlo fare, è bene osservare alcune generali regole di prudenza. In primo luogo, si deve diffidare

dalle comunicazioni provenienti da istituti di credito o servizi finanziari che richiedono di confermare o aggiornare le proprie credenziali di autenticazione, rimandando l'utente a un apposito link: queste procedure non vengono mai avviate tramite e-mail dai reali titolari dei servizi in questione. Se si riceve un'e-mail sospetta, quindi, occorre chiamare il proprio istituto di credito e chiedere conferma del contenuto del messaggio. Se invece l'e-mail ricevuta dovesse sembrare autentica, è bene non utilizzare il link ricevuto ed effettuare l'operazione richiesta direttamente dal portale del servizio normalmente utilizzato. Attenzione anche agli allegati al messaggio e-mail: file in formato .exe, .doc o .pdf possono celare virus, come ad esempio financial malware o trojan banking, in grado di captare le credenziali di accesso inserite da parte di una vittima sui portali dei propri servizi finanziari. Inoltre, è sempre bene verificare che i siti che richiedono l'inserimento di dati relativi a carte di credito o credenziali di accesso all'home banking siano protetti da protocolli di trasmissione cifrati (i cosiddetti Secure Sockets Layer, contraddistinti dal prefisso: HTTPS). Altra accortezza fondamentale è quella di controllare che il nome del sito corrisponda al nome del dominio normalmente utilizzato per quel servizio: ad esempio, se "bancaxyz.it" è il portale di accesso al proprio home banking, "bancaxyz.com" è certamente un sito di cui diffidare. Buona prassi è quella di cambiare la propria password con frequenza e, in ogni caso, non appena ci si accorga o si sospetti di un accesso non autorizzato. Inoltre, occorre privilegiare, come sistema di autenticazione forte, l'utilizzo di apposite app (ad es. la app che fornisce i secure code della banca, o Google Authenticator

ecc...) invece degli SMS con OTP. Tale scelta tutela, infatti, gli utilizzatori dal SIM Swapping, in quanto le password necessarie ad autorizzare l'operazione saranno generate direttamente sul dispositivo dell'utilizzatore e non saranno collegate al suo numero di cellulare (che, come visto, può essere clonato). In tutti i casi in cui si approdi su pagine sospette, è bene che l'utente informi dell'accaduto i titolari dei servizi oggetto di imitazione. Nell'ipotesi in cui l'utente abbia malauguratamente inserito i propri dati su tali pagine, occorrerà anche allertare le autorità competenti (Polizia Postale). Se il furto dei dati coinvolge i dati bancari della vittima, infine, la cosa migliore da fare è contattare l'istituto bancario al fine di bloccare quanto prima i servizi coinvolti nella truffa (carte di credito, conti correnti, bancomat). Nel caso in cui risultino pagamenti non autorizzati, la vittima dovrà inoltre comunicare all'istituto di pagamento di non aver autorizzato l'operazione. Il tempismo, in questi casi, può fare la differenza. Bisogna agire con la massima prontezza non solo per tentare di limitare i danni, ma anche per rispettare la normativa applicabile.

Cosa dice la Cassazione in caso di truffa online

L'art. 7 del D.lgs. 11/2010 (per l'attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno) stabilisce che l'utilizzatore di un servizio di pagamento debba comunicare al prestatore del servizio lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne abbia conoscenza. Nel caso in cui l'utilizzatore dei servizi di pagamento neghi di aver effettuato un'operazione, spetta

al prestatore dei servizi dimostrare che l'operazione è stata autenticata, correttamente registrata e contabilizzata, e che non si sono verificati malfunzionamenti o inconvenienti durante la sua esecuzione (art. 10 comma 1 del D.lgs. 11/2010). Anche qualora il prestatore riuscisse a dimostrare tali circostanze, rimarrebbe comunque responsabile nei confronti dell'utilizzatore, in quanto "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo" (art. 10 comma 2 del D.lgs. 11/2010). Bisogna tener presente, inoltre, che i prestatori di servizi di pagamento trattano, in qualità di titolari, i dati personali dei loro clienti. Sotto la vigenza del D.lgs. 196/2003 ante GDPR, l'ormai abrogato art. 15 stabiliva che chi cagionava danno ad altri per effetto del trattamento dei dati personali, fosse tenuto a risarcire tale danno ex art. 2050 c.c. (esercizio di attività pericolosa, fattispecie di responsabilità semi-oggettiva). Con l'entrata in vigore del GDPR e la successiva adozione del D. Lgs. 101/2018, l'art. 15 del D.lgs. 196/2003 è stato abrogato. La norma che ora attribuisce la responsabilità al titolare (o al responsabile del trattamento) è l'art. 82 del GDPR, per cui, chiunque subisca un danno, materiale o immateriale, causato da una violazione del GDPR, ha diritto al risarcimento del danno. Tale disposto non pare alleggerire l'onere probatorio dell'istituto di pagamento (vale a dire il titolare dei dati), in quanto il **principio di accountability** che permea il GDPR enuncia chiaramente che spetta al titolare dimostrare il pieno rispetto delle previsioni del Regolamento (tra cui, ad es., la liceità dei trattamenti effettuati,

l'adozione di idonee misure di sicurezza ecc.). Non c'è dunque da stupirsi che, anche prima dell'entrata in vigore del GDPR, la Cassazione si fosse pronunciata sulla responsabilità del prestatore di servizi nei casi di truffa online e sul relativo onere probatorio: dato che l'istituto di pagamento risponde ai sensi dell'art. 2050 c.c., in virtù dell'art. 15 del Codice Privacy (oggi abrogato), esso risulta onerato della prova liberatoria consistente nell'aver adottato tutte le misure idonee a evitare il danno. La vittima, invece, è onerata soltanto della prova del danno riferibile al trattamento del suo dato personale (Cass. Civ. Sez. I, Sent. n. 10638/2016). Su questa scia si colloca anche una più recente ordinanza della Corte (Cass. Civ. Sez. VI, Ordinanza n. 9158/2018) che chiarisce, a prescindere dai richiami alla normativa sulla protezione dei dati personali, che la responsabilità del prestatore di servizi trovi fondamento nella posizione di garanzia che l'istituto di credito riveste nei confronti del cliente, per cui al prestatore dei servizi è imposta una diligenza qualificata (quella del "bonus nummarius") nell'adempimento dei propri obblighi, ai sensi dell'art. 1176 comma 2 c.c.. Nella pronuncia in esame, che vedeva due correntisti agire in giudizio contro un prestatore di servizi di pagamento per il rimborso di quanto sottratto a seguito di un episodio di phishing, la Corte ritiene "*ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo; ne consegue che la banca, cui è richiesta una diligenza di natura tecnica da valutarsi*

con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente" (nello stesso senso, Cass. Civ. Sez. I, Sent. n. 2950/2017). In definitiva, pare concretarsi una responsabilità di tipo semi-oggettivo in capo all'istituto di credito, che deve provare, da un lato, di aver adottato tutte le misure idonee a garantire la sicurezza del sistema di pagamento e, dall'altro, la riconducibilità dell'operazione al cliente (circostanza tutt'altro che agevole da dimostrare, se non vera e propria probatio diabolica).

Come si procede per ottenere il rimborso in caso di phishing

L'art. 11 del D.lgs. 11/2010 stabilisce che il prestatore dei servizi di pagamento è tenuto a rimborsare l'importo sottratto alla vittima mediante un'operazione di pagamento da questa non autorizzata. La vittima che intende far valere le proprie ragioni deve in primo luogo comunicare all'istituto di pagamento di non aver autorizzato l'operazione contestata. Se la banca non riconoscesse la propria responsabilità e negasse il rimborso, il soggetto truffato dovrebbe adire le vie legali. Prima di esercitare in giudizio un'azione relativa a una controversia in materia di contratti bancari, l'interessato deve esperire il procedimento di mediazione obbligatoria, che costituisce una condizione di procedibilità della domanda giudiziale. Una possibile alternativa alla proposizione di una domanda giudiziale è il ricorso all'Arbitro Bancario Finanziario (ABF), strumento di risoluzione alternativa delle controversie (stragiudiziale, appunto) che può essere adito previa dimostrazione, da parte del correntista,

di aver tentato di risolvere la controversia con l'istituto di pagamento tramite reclamo scritto non andato a buon fine. Se la decisione dell'ABF (non vincolante, peraltro) non è ritenuta soddisfacente dalle parti, queste possono adire l'autorità giudiziaria senza esperire la mediazione obbligatoria, in quanto il ricorso all'ABF fa venir meno tale obbligo.

Quando la vittima non ha diritto al rimborso

Come esaminato nei paragrafi precedenti, il prestatore dei servizi di pagamento è gravato da una responsabilità di tipo semi-oggettivo. Ciò significa che esistono casi, seppur limitati, in cui il prestatore è liberato dall'obbligo di rimborsare gli importi sottratti alla vittima con operazioni non autorizzate sul proprio conto. Per poter fare ciò, esso deve fornire prova liberatoria di un fatto imprevedibile e inevitabile che sfugge alla sua sfera di controllo. Il prestatore è esente da responsabilità e non deve, pertanto, rimborsare o risarcire alcunché, ai sensi del combinato disposto degli artt. 7 e 12 del D. Lgs. 11/2010, qualora dimostri la frode dell'utilizzatore o il suo inadempimento, per dolo o colpa grave, degli obblighi di cui all'art. 7 del già menzionato decreto. L'art. 7, infatti, stabilisce l'obbligo di utilizzare i servizi di pagamento secondo i termini d'uso pattuiti con il prestatore e, come visto, l'obbligo di comunicare senza indugio l'eventuale perdita di disponibilità dello strumento di pagamento, non appena l'utilizzatore ne sia venuto a conoscenza. Il comma 2 dell'art. 7, poi, attribuisce all'utilizzatore l'obbligo di custodire diligentemente le proprie credenziali di accesso ai servizi. Se, dunque, appare intuitivo ravvisare elementi di colpa nella

condotta del correntista che, pur accortosi di una transazione non autorizzata, ne dia comunicazione all'istituto di pagamento con notevole ritardo, meno agevole è distinguere quali siano le condotte colpose ascrivibili alla violazione dell'obbligo di custodia che incombe sulla vittima. Il distinguo circa i comportamenti che possono integrare la "colpa grave" del danneggiato è più delicato in considerazione del fatto che il phishing è una tipologia di truffa e, in quanto tale, presenta elementi di insidia che mirano a ingannare la vittima. Quest'ultima, da parte sua, ha l'obbligo di proteggere le proprie credenziali di autenticazione personalizzate, per cui la diffusione o comunicazione dei dati identificativi e dispositivi del proprio conto potrebbe sembrare sufficiente a integrare un elemento di responsabilità del danneggiato tale da escludere la responsabilità della banca. In realtà, non è sempre così. L'ABF distingue, infatti, l'ipotesi in cui la vittima di un'operazione non autorizzata si sia vista sottrarre le credenziali di accesso a causa di un virus (financial malware, ad esempio, o similari) da quella in cui la stessa vittima abbia, incautamente, comunicato le proprie credenziali di autenticazione al di fuori del circuito operativo del prestatore dei servizi. Nel primo caso, l'ABF sostiene che non possa ravvisarsi un comportamento colposo della vittima. Nel secondo caso, invece, il comportamento di chi "abbocchi" a una tradizionale e-mail di phishing integra ipotesi di colpa grave (e, quindi, la banca non risponderà, qualora riesca a dimostrare tale circostanza) in quanto, nell'opinione del collegio giudicante, tali modalità di truffa online sono ormai largamente note anche agli utenti non necessariamente esperti della navigazione su Internet (ABF Roma

396/2020). A tale conclusione, naturalmente, si giungerà sulla base delle valutazioni operate, di volta in volta, nel caso concreto, anche a seconda del grado di “insidia” della truffa e di “sofisticazione” della vittima.

@RIPRODUZIONE RISERVATA

Personaggi

- Camillo Campli
- Giuseppe Cristiano

Argomenti

- Gdpr
- password
- phishing
- Privacy
- smishing
- trojan

Canali

- Malware e attacchi hacker