OPINION

Occhio alle frodi

Si moltiplicano i tentativi di carpire online le credenziali degli utenti
Il quadro normativo non sempre tutela i clienti truffati

DI **PAOLO FRANCESCO BRUNO***

I prestatori di servizi di pagamento si trovano a fare i conti con tentativi sempre più frequenti di frodi informatiche. Si tratta di procedure **finalizzate ad appropriarsi in modo illegale delle credenziali di accesso ai servizi bancari online**, per poi effettuare operazioni di pagamento non autorizzate presso i conti bancari del malcapitato: il caso più noto è rappresentato dal phishing, ossia dalla richiesta via e-mail alla vittima di inserire dati personali attraverso un link a un sito clone di quello della propria banca, con le varianti del vishing (phishing per telefono) e dello smishing (phishing per sms).

La nuova frontiera dello spoofing

Illeciti più articolati sono lo spoofing, che si verifica quando terzi mascherano e nascondono la propria identità, assumendo quella del prestatore dei servizi di pagamento, indirizzando e-mail, sms o telefonate in modo che il mittente sembri l'intermediario e, infine, il man in the browser, che è costituito **da un software malevolo (malware) che si interpone tra il computer della vittima e il sistema messo a disposizione dal prestatore del servizio di pagamento**.
Al fine di prevenire ed evitare il compimento di tali illeciti, ovviamente, oltre a un servizio reso secondo standard tecnici e giuridici adeguati, è richiesto **un dovere di adeguata custodia delle credenziali di accesso** al cliente e, a tal riguardo, sono stati molti ed eterogenei gli interventi pubblicitari volti alla sensibilizzazione dei clienti sull'aspetto legato al comportamento concernente la custodia delle credenziali. Queste campagne, diventante ormai notorie, pongono l'utente dinnanzi a un dovere di diligenza non più scusabile e, sempre più spesso, sono citate dalla giurisprudenza che si è pronunciata su questi temi.

Tra consenso e ordine

Perno centrale della disciplina è il consenso del pagatore ossia il soggetto titolare di un conto di pagamento a valere sul quale viene impartito un ordine di pagamento ovvero, in mancanza di un conto di pagamento, il soggetto che impartisce un ordine di pagamento. Sulla distinzione tra consenso e ordine di pagamento la recente pronuncia del Tribunale di Milano, 28 febbraio 2023, n. 1596, ha avuto modo di soffermarsi, sottolineando che **l'ordine di pagamento è l'istruzione formale data dall'utente**, il consenso invece rappresenta il presupposto volitivo dell'ordine di pagamento.
Questa considerazione non è evidentemente oziosa o fine a sé stessa, dal momento che la disciplina dettata dal dlgs 11/2010, come ricorda la pronuncia di merito sopra citata, recepisce la distinzione tra i due concetti in armonia con l'evoluzione tecnologica e le procedure di autenticazione che consentono ai clienti di identificarsi e di disporre, a distanza, gli ordini di pagamento, istituendo, pertanto, una procedimentalizzazione della **manifestazione del consenso** da parte del pagatore. Si tratteggiano e distribuiscono così le aree connesse ai rischi derivanti, tra le altre cose, dalle condotte fraudolente dei terzi che simulano un consenso del pagatore, dando avvio a un'operazione di pagamento non voluta.

Le barriere antintrusione

Venendo così agli obblighi cui è tenuto l'utente, vi è quello principale

Il caso più noto è rappresentato dal phishing, ossia dalla richiesta via e-mail alla vittima di inserire dati personali attraverso un link a un sito clone di quello della propria banca, con le varianti del vishing (phishing per telefono) e dello smishing (phishing per sms)

per cui, non appena riceve uno strumento di pagamento, deve realizzare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate.
Le condotte che possano determinare una dispersione delle credenziali, ovviamente, non possono essere tutelate ed è per questo che viene richiesto all'utente non solo di custodire in luoghi sicuri le credenziali, ma anche di **non attuare comportamenti che compromettano la segretezza dei dati ricevuti**.
Recentemente la Suprema Corte ha avuto modo di rimarcare l'esclusiva responsabilità del cliente che abbia consegnato i codici personali a terzi, rispondendo verosimilmente a una e-mail di phishing, così da consentire l'effettuazione di una disposizione di bonifico dal conto del danneggiato (Cass. 13 marzo 2023, n. 7214).

Carenza di custodia

In conclusione, al di là di comportamenti legati alla volontaria consegna di credenziali a favore di soggetti terzi, che escludono in apicibus la possibilità di imputare responsabilità in capo al prestatore del servizio di pagamento, le condotte colpose con cui l'utente consegna - a seguito di un comportamento illecito di terzi - le credenziali personali non sono tutelate dal nostro ordinamento, dal momento che attraverso l'uso delle credenziali da parte di un terzo, che assume a tutti gli effetti le vesti dell'utente, viene a formarsi il consenso del pagatore che esenta da responsabilità il prestatore del servizio.

*Salary partner dello studio legale Zitiello e Associati