L'Economia
del CORRIERE DELLA SERA

PAGAMENTI DIGITALI

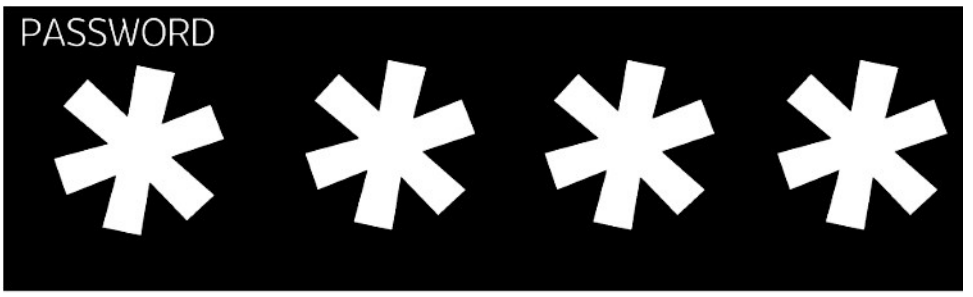
SONO TANTO COMODI MA I NOSTRI CONTI SONO DAVVERO AL SICURO?

di **Ferruccio de Bortoli**

2

L'ecommerce vola. Ma che certezza abbiamo che la nostra identità finanziaria non sia violata? Se il rischio è passare dall'arcaico segreto bancario alla trasparenza involontaria, il vero problema è l'accesso ai dati da parte di terzi, sul web. Perciò fate sempre attenzione al piccolo lucchetto sulla barra di navigazione...

CHI È AL SICURO SULLA RETE?



di **Ferruccio de Bortoli**

La semplicità e la comodità dei pagamenti digitali sono sempre più apprezzate. Anche in un Paese nel quale l'uso dei contanti resta massiccio e la diffusione delle carte di credito non è paragonabile a quella dei nostri partner commerciali. La fisicità degli acquisti poi, è ancora un piacere irrinunciabile. Ma gli italiani che comprano online, almeno una volta al mese — secondo il rapporto Netcomm — sono ormai più di 15 milioni. Grosso modo la metà degli utenti Internet. Sono cresciuti in un anno del 23 per cento. Un mercato, quello dell' ecommerce, in vorticosa

espansione. Ma non solo, c'è anche la gestione del denaro che gli operatori della Rete, con costi di transazione molto più bassi, tendono a sottrarre al sistema bancario tradizionale. I pagamenti digitali sono cresciuti in Italia, nell'ultimo anno, del 9 per cento. Ora, acquisito che il futuro ruota attorno alle infinite applicazioni dei nostri smartphone, o qualcos'altro che sicuramente verrà, resta aperto l'interrogativo sulla riservatezza reale dei nostri conti.

Occhi indiscreti

Il segreto bancario — come scritto nel precedente numero de *L'Economia* — è ormai al tramonto. Ma nell'era digitale come potremo proteggere al meglio le nostre identità finanziarie (e non solo) dagli occhi più indiscreti e pericolosi? Non quelli del Fisco e della magistratura, ma altri della cui natura non abbiamo che vaghi sospetti. Stiamo passando troppo in fretta dall'arcaico segreto bancario alla trasparenza involontaria? Dal caveau svizzero alla foresta digitale? Ha colpito molto, nel luglio scorso, la denuncia di Unicredit alla procura della Repubblica di Milano. Un' intrusione informatica sui dati di 400 mila clienti, per fortuna senza conseguenze sulle loro password e sui codici di accesso ai conti bancari.

L'Abi, l'Associazione bancaria italiana, sostiene che il settore spende 250 milioni l'anno per la sicurezza informatica. Il 95 per cento delle operazioni fraudolente viene sventato. I clienti vittime di frode sono lo 0,002% di quelli che operano sull'home banking. Uno su 50 mila. Sulle frodi tradizionali possiamo stare relativamente tranquilli.

Un po' meno se pensiamo alla misteriosa potenza di hacker in grado di condizionare, o tentare di farlo, anche i risultati elettorali. Ma qui la risposta non può essere che a livello di organizzazioni internazionali, come l'Ocse, o il G7 che ha scritto le linee guida sulla cybersecurity.

Sul versante più domestico molto dipende dalla nostra attenzione. La sicurezza è alta se si seguono tutte le norme di comportamento del cliente bancario. Ignorare, per esempio, ogni richiesta di dati relativi a carte o conti online, connettersi al sito della banca scrivendo nella barra di navigazione, controllare l'aggiornamento del sistema operativo del nostro computer, la validità degli antivirus. Se però la custodia dei nostri conti e delle nostre carte, operando sulla Rete, è pari alla facilità con la quale forniamo notizie e fotografie sulla nostra vita privata ai social network, qualche motivo di preoccupazione ulteriore è fondato.

«All'interno del mondo bancario — spiega il presidente dell'Abi, Antonio Patuelli — la responsabilità della sicurezza è tutta nostra con l'ovvia collaborazione dei nostri clienti. Diverso è quando intervengono terze parti, per esempio operando sulla Rete».

Le regole

La liberalizzazione e la disciplina delle nuove società che offrono sistemi alternativi di pagamento è contenuta soprattutto in una direttiva europea, la Payments service directive, in sigla Psd2. Entro il 13 gennaio del prossimo anno gli Stati membri dovranno recepirla nei loro ordinamenti. Oltre ad alcune disposizioni, ovvero regulatory standard, dell'Eba, l'Autorità bancaria europea. «Le principali reti private — sostiene Vincenzo Cosenza, strategist a BlogMeter e autore de *La società dei dati*, edito da 40K — offrono elevati standard di sicurezza. È estremamente difficile, anche per il più sofisticato degli incursori, frapporsi tra un browser e i server di un grande gruppo.

Le multinazionali delle carte di credito, Visa, Mastercard e le altre, hanno alzato i livelli di sicurezza con codici di accesso che vengono inviati via smartphone. PayPal garantisce l'utente anche dagli eventuali acquisti fraudolenti. Piuttosto il consumatore non sempre fa caso a quel piccolo e prezioso lucchetto che compare nella barra di navigazione. Se non c'è, e a meno che non si tratti di indirizzi stranoti, la sicurezza negli eventuali pagamenti non è garantita».

La Psd2 e il sistema di strong authentication, di autenticazione rafforzata, dell'Eba sono stati elaborati anche tenendo conto di alcuni fatti clamorosi. La totale visibilità sui conti dei propri clienti degli americani di Swift — e la teorica possibilità di accesso da parte di agenzie federali — ha suscitato dubbi e polemiche. Un altro caso analogo ha riguardato l' operatore tedesco Sofort nel 2011 con le associazioni dei consumatori che hanno contestato la facilità con cui poteva scrutare nei conti correnti.

Fino a che punto i nostri dati bancari sono a disposizione del servizio cui affidiamo un pagamento?

La questione ha anche aspetti strategici rilevanti. I russi pensano di farsi proprie carte di credito e di sfidare il monopolio statunitense.

«La nuova normativa — spiega Giovanni Sabatini, direttore generale dell'Abi — impone alle banche alcuni oneri e costi supplementari per consentire l'accesso delle terze parti. E dovrebbe evitare che, nel richiedere le credenziali bancarie, l'operatore privato possa fare quello che in gergo si chiama screenscraper, cioè accedere a tutti i dati dell'utente. La questione è ancora aperta. La creazione di un' applicazione che dovrebbe impedire alle terze parti di conoscere anche dati che non sono necessari per completare un pagamento, non è però sufficiente per scongiurare incursioni sgradite. La posizione della commissione europea è condizionata da forti pressioni».

Il doppio livello

«I pagamenti digitali sono di tante tipologie ed è necessario conoscerle bene — dice Massimo Arrighetti, amministratore delegato di Sia, leader europeo nei servizi innovativi di pagamento per il settore finanziario — . Quando si opera su reti private (Sianet e Swift sono le principali), la possibilità di frodi è veramente ridotta a percentuali irrisorie. Dal 2018, con l'avvento della Psd2, si sperimenterà la delega ad accedere ai conti concessa a operatori terzi che dovranno sottostare ai regolamenti bancari. Alcuni di questi sono su Internet dove i livelli di sicurezza sono più bassi e il rischio di hackeraggio più elevato. Lì ci sono tutti, un mondo aperto. Quindi è più sicuro crittografare i dati e farli viaggiare su reti separate

anche se ciò ha un costo maggiore. La direttiva Psd2 non distingue, purtroppo, tra reti private e Internet».

Il passaggio, dunque, non è di portata trascurabile. Lo sviluppo dei pagamenti digitali comporterà un monitoraggio continuo, soprattutto nella fase sperimentale. Gli incidenti di percorso non mancheranno.

Ma è indubbio che l'utente dovrà avere un atteggiamento diverso, più consapevole dei rischi che può correre. Un sito di giochi online non garantisce lo stesso livello di sicurezza, nell'uso dei dati bancari, di un grande circuito privato. I dati essenziali delle nostre vite, non soltanto dei nostri conti, sono custoditi in server e cloud sul cui destino mostriamo un ingenuo disinteresse.

L'entusiasmo per la tecnologia e l'ebbrezza della comodità mal si conciliano con la noia dei codici e dei controlli. Non è tutto smart, purtroppo.

I numeri

+23%

La spesa online
annuale degli italiani che acquistano via Internet almeno una volta al mese
Sono 15 milioni

250

milioni
gli investimenti annuali delle banche per la sicurezza informatica, dice l'Associazione bancaria italiana

95%

Le frodi sventate
al sistema informatico bancario, secondo l'Abi. Ne è vittima un cliente su 50 mila