Tecnologia e sicurezza

Truffe nel web: i ladri di identità

Chiunque può prendere il nostro posto in rete: 7 milioni di vittime in Europa

Immaginate di voler comprare una casa. Finalmente, dopo anni di sacrifici, riuscite ad accedere all'ipoteca trentennale che vi assicurerà un focolare tutto vostro, dove far crescere i vostri figli. Però, quando tutto sembra andare per il verso giusto, la banca vi nega il prestito perché avete acquistato qualche mese prima un televisore a rate, senza mai pagarle. Voi non ve ne ricordate, perché in realtà non siete voi ad averlo acquistato, ma qualcuno che vi ha impersonato, incastrandovi grazie ai dati sempre più diffusi su Internet tramite i social network. Se ne parla poco, perché è un fenomeno ancora difficile da quantificare, ma più di 7 milioni di persone in Europa sono stati vittime di furto di identità. D'altronde i social network sono ormai una parte della nostra vita di cui quasi non possiamo fare a meno: scriviamo delle nostre storie sentimentali o delle nostre vacanze. Tutte queste informazioni ci identificano talmente tanto che possono essere usate da un perfetto sconosciuto per trasformarsi in noi. Per non parlare delle piccole, superficiali distrazioni quotidiane. Sicché basta un estratto conto gettato nella spazzatura o una parola di troppo sul nostro profilo in Facebook per trasformare la nostra vita in un inferno.

OCCHIO A FACEBOOK
Lasciare troppe informazioni private sui social network consente ai ladri di identità di acquisire facilmente molte informazioni «sensibili» su di voi per poi utilizzarle a proprio favore.

PAGINA DI ALESSIO PALMERO APROSIO

In ogni momento della nostra giornata, senza che nemmeno ce ne rendiamo conto, siamo potenziali vittime di una truffa vecchia quanto l'uomo che però ha ritrovato una nuova giovinezza grazie a Internet: il furto di identità. Questo reato si verifica quando un malfattore raccoglie molte informazioni su una persona riuscendo poi a sostituirsi a lei e a compiere azioni illecite a nome del malcapitato.

Ci fu chi ci rimise la testa

Nella storia c'è un caso illustre di furto di identità, accaduto alla regina di Scozia Maria Stuarda più di 500 anni fa. Durante i suoi anni di prigionia, per i giochi di potere con la cugina Elisabetta I, Maria Stuarda aveva adottato un sistema di cifratura piuttosto sicuro per scambiare corrispondenza con alcuni nobili che stavano congiurando contro la sovrana. Tuttavia il sistema fu intercettato dall'abile crittoanalista Phelippes, che decifrò i biglietti e aggiunse intere frasi ai messaggi di Maria Stuarda, imitandone addirittura la calligrafia. In queste aggiunte egli chiedeva informazioni precise su date e luoghi del piano per l'assassinio di Elisabetta I. Naturalmente i congiurati caddero nel tranello e furono identificati e torturati e Maria Stuarda decapitata.

Attenzione al trasloco

L'intercettazione della corrispondenza, che alla fine del Cinquecento incastrò la regina di Scozia, in realtà è da sempre uno dei metodi classici per attuare un furto di identità, in particolare prima dell'avvento di Internet. Molto banalmente, all'indomani di un trasloco capita spesso che la posta del vecchio inquilino finisca nelle mani del suo successore. Se quest'ultimo non fosse abbastanza onesto, potrebbe utilizzare alcune di queste lettere, come ad esempio gli estratti conto bancari, per ottenere denaro in modo illecito.

Rovistare nella spazzatura

Un altro stratagemma spesso utilizzato dai truffatori è quello del *bin raiding*: rovistare nella nostra spazzatura alla ricerca di vecchia corrispondenza che a noi non serve più, ma che può essere utilizzata dai malfattori. Un problema simile è stato quello dei numeri di carta di credito stampati sugli scontrini dopo gli acquisti: i clienti buttavano gli scontrini nella spazzatura e i ladri di identità li recuperavano per poi utilizzarli per gli acquisti di servizi online. L'utilizzo della carta di credito su Internet non prevede infatti alcuna firma, ma solo l'inserimento del numero della carta e della data di scadenza, cioè informazioni stampate sullo scontrino. Negli ultimi anni il fenomeno è stato fortunatamente arginato grazie alla cancellazione di alcune cifre del numero di carta di credito sugli scontrini.

Phishing: le informazioni le fornisci tu stesso

Su Internet invece il metodo più utilizzato per ottenere denaro illecitamente tramite il furto di identità è quello di chiedere direttamente agli utenti, tramite l'inganno, le credenziali di accesso al proprio conto corrente sul sito web della banca. La tecnica, chiamata phishing, prevede l'invio di un'email in cui si chiede la conferma dei dati di accesso, pena l'interruzione del servizio e il congelamento del conto. L'utente, intimorito, segue il link presente nell'email e inserisce i propri dati, non sapendo che la pagina web appena visitata è in realtà una riproduzione identica a quella della banca in cui il malcapitato tiene i suoi risparmi. Una volta ottenuti i dati, i truffatori entrano nel vero sito di home banking della vittima e ne prosciugano il conto.

Con i social network so chi sei e dove sei

L'ultima frontiera del furto di identità sono i social network. Spesso inseriamo in Rete, visibili a molte persone tramite fotografie e commenti, parecchi elementi della nostra vita quotidiana. Così, per esempio, un'informazione in apparenza innocua come il periodo di ferie diventa un dato fondamentale per un ladro, che scopre quando non siamo in casa per svaligiarcela.

Per il momento il Ticino è tranquillo

Non ci sono però solamente cattive notizie. Nonostante l'aumento dei casi registrati in Europa, la polizia cantonale fornisce dati tranquillizzanti: «In Ticino il fenomeno è praticamente sconosciuto». Non dobbiamo però dormire sugli allori, perché lo SCOCI, il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet, consiglia di rimanere sempre vigili: «Ci sono modi diversi in cui il furto di identità si manifesta, anche nel nostro Paese. Il più semplice è registrarsi a nome di un'altra persona senza che questa lo sappia. Il passo successivo consiste nella sottrazione delle informazioni di autenticazione dell'utente (la password, ad esempio) e avere accesso a informazioni riservate nella posta elettronica, nel conto online o nel profilo su Facebook. Infine può capitare che il criminale cerchi, tramite l'utilizzo di documenti sottratti o falsificati, di commettere dei reati facendo ricadere la colpa sulla vittima». I suggerimenti per gli utenti sono i soliti: «Stare sempre attenti, specialmente su Internet, e non fornire mai credenziali di accesso o dati personali. Utilizzare password sicure, una diversa per ogni servizio, e cambiarle spesso. Qualora si sospettasse di essere vittima di furto di identità, contattare immediatamente la polizia e segnalare il fatto allo SCOCI».

COME FARE PER PROTEGGERSI?

I consigli di Paolo Attivissimo «Dubitare di tutto e dubitare sempre»

L'INTERVISTA

Paolo Attivissimo non ha quasi bisogno di presentazioni: esperto di sicurezza informatica, giornalista, voce nota della radio, negli ultimi anni si è occupato proprio di smascherare bufale e truffe, sempre più diffuse e semplici da realizzare grazie alla capillarità del web. E ci ha dato qualche consiglio.

Il furto di identità è un fenomeno che ha radici antiche come l'uomo, ma è diventato di applicabilità molto più semplice grazie a Internet. Quali sono i consigli di un esperto di sicurezza per gli utenti della Rete, in particolare per i frequentatori dei social network?

«Fondamentalmente, dubitare di tutto e dubitare sempre. Lo so: la paranoia è una brutta compagna di viaggio. Ma il furto di identità è molto diffuso, sia a livello amatoriale, come scherzo o provocazione nei forum, nei social network e nella corrispondenza, sia a livello professionale, sotto forma di intrusioni informatiche, danni economici, spionaggio industriale piccolo e grande. Per cui va considerato come una realtà nella quale tutti possiamo incappare».

Ciò significa che falsificare la propria identità o simulare quella di un altro è un'operazione semplice.

«Purtroppo sì. Anche se molti non lo sanno, i nomi degli utenti in Blogger, per esempio, sono modificabili a piacere. Un messaggio polemico iniettato da un provocatore a nome di qualcun altro può causare uno scompiglio di dimensioni epiche. In un social network come Facebook non c'è nessun controllo che impedisca a un disturbatore di registrarsi come utente dando il nome di un'altra persona: non c'è alcun controllo di identità».

Allora come si fa a capire che un contributo su un blog o su un forum è un falso?

«Se si esamina ogni mail, ogni post e ogni commento con l'idea di fondo che potrebbe trattarsi di un falso, diventa più facile e quasi automatico rendersi conto dei sintomi quasi inevitabili di un'impostura. Di solito un po' di buon senso è sufficiente: noi umani siamo bravi a riconoscere il contesto, a captare lo stile di scrittura individuale e a notare quando qualcuno cerca di imitare il modo di scrivere di qualcun altro. Anche i fotomontaggi e i finti documenti, spesso usati dai professionisti del furto di identità, sono facilmente smascherabili se li si osserva con attenzione e distacco. Anzi, il distacco, cioè l'analisi razionale, non emotiva, è una delle chiavi della sicurezza informatica. Un impostore di talento cercherà sempre di far leva sulle nostre emozioni per farci mettere da parte la cautela razionale, offrendoci qualcosa di altamente desiderabile o inquietante, dalle immagini osé fino alle rivelazioni scottanti e agli allarmi fasulli. Oltre al distacco, comunque, occorre disporre di una serie di conoscenze informatiche di base e di strumenti di verifica. Si impara molto provando a essere impostori e osservando come si comportano coloro che tentano il furto di identità. Ci sono anche strumenti che permettono di essere avvisati se ci si imbatte nelle trappole informatiche più diffuse. Ma alla fine è l'utente a giocare il ruolo più importante, con la propria abilità nel discriminare».

Sta dipingendo uno scenario inquietante.

«Il fenomeno è molto diffuso, tuttavia la sicurezza va proporzionata al rischio. Un commento di un impostore in un blog non ha la stessa pericolosità di un'email fasulla che ci invita a visitare il sito della nostra banca per rettificare un problema, ma in realtà ci porta a un sito-fotocopia nel quale ci verrà chiesto di immettere le nostre credenziali d'accesso, regalandole così al malfattore».

Spesso bastano una telefonata e due informazioni comunicate a voce perché un'azienda o un ente pubblico si fidi di noi e ci permetta di eseguire operazioni potenzialmente pericolose. Quali sono le precauzioni da prendere da parte di coloro che devono confermare la nostra identità tramite Internet o il telefono?

«Anche in questo caso le procedure vanno commisurate al rischio. Le verifiche di identità dovranno essere molto più accurate nel caso di una transazione finanziaria che per una chiacchierata informale via chat o Facebook. Per i casi più importanti è meglio uscire del tutto da Internet e trovare un canale di verifica indipendente e tradizionale. Un incontro a faccia a faccia, uno scambio diretto di documenti di identità, non però fotocopie o scansioni bensì documenti originali, oppure una serie di telefonate di verifica. Per carità, tutti questi sistemi sono superabili da parte di un impostore agguerrito e determinato, ma è rarissimo avere a che fare con professionisti di questo genere. In generale comunque occorre partire dal presupposto del dubbio. In Rete vengono a mancare molti degli elementi di verifica automatica sui quali contiamo nella comunicazione tradizionale, come il timbro e il tono della voce, il modo di esprimersi, l'aspetto fisico, la gestualità. Quindi la simulazione è molto più facile. Siamo animali sociali e la diffidenza nei confronti dei nostri simili non ci viene spontanea. Quando entriamo in un mondo in cui questi elementi di verifica normali mancano, tendiamo a compensarli in senso positivo, creandoli dove non ci sono. Per esempio, quando leggiamo un'email di una persona che conosciamo, tendiamo a interpretarla immaginando la voce di chi l'ha scritta: questo crea una falsa autenticazione emozionale del messaggio. È una trappola istintiva nella quale è facilissimo cadere. Occorre allenarsi a osservare con distacco le situazioni e chiedersi su quali basi reali abbiamo stabilito l'identità del nostro interlocutore. E poi procedere a una verifica. Concludo con un esempio pratico. Un giorno, dopo aver scritto un articolo nel mio blog a proposito di una puntata di "Matrix", ho ricevuto un'email da Enrico Mentana, che all'epoca conduceva il programma. L'email proponeva una consulenza basata sull'articolo. Come ho fatto a sapere che non si trattava di una burla? L'esame del contesto dell'email era impraticabile: il testo era costituito da un paio di frasi prive di elementi di conferma. Così ho risposto invitando Mentana a telefonarmi e dandogli un numero di telefono che poteva conoscere soltanto tramite la mia email. Lo squillo di quel telefono e la voce inconfondibile di Mentana hanno autenticato l'email pochi minuti dopo».