

# Tecnologia

## «Altolà, parola d'ordine!», disse il PC

### Esistono poche ma buone regole da rispettare per evitare grossi dispiaceri

**Come ricordare decine di password per la banca, la posta elettronica, il sito Web e la miriade di altri servizi online? Molto più semplice usarne una sola per tutti, magari facile da ricordare, vero? Invece il rischio è elevato**

**SERVIZIO A CURA  
DI LUCA ACCOMAZZI**

Le nostre parole d'ordine, cioè quelle password che dovrebbero servire a identificarci, sono merce preziosa. E per questo motivo truffatori e criminali hanno evoluto una nutrita serie di trucchi per cercare di rubarle o indovinarle. Falsificare un assegno oggi è più difficile e rischioso. La password a volte non basta per commettere una truffa: chi indovina il numero della nostra tessera Bancomat non se ne fa niente se non riesce a mettere mano anche sulla tessera stessa. A volte, però, azzeccare una parola d'ordine permette di fare grandi danni.

Un intenso utilizzatore della rete Internet si registra e lascia frequentemente i propri dati su una buona percentuale dei siti Web visitati, e l'indirizzo di posta elettronica è sempre tra questi, insieme a una password. Poiché nessuno è disposto a mandare a mente centinaia di parole d'ordine differenti, tutti ricorrono a qualche trucco. I più diffidenti usano password diverse per ogni sito e lasciano che sia il loro calcolatore a memorizzarle. Molti però riciclano in continuazione le stesse parole e frasi, riutilizzando su tutti i siti o su tutti i siti del medesimo tipo. I malfattori lo sanno e, quando riescono a infrangere le protezioni di un sito Web, rubano immediatamente i dati degli utenti che vi sono memorizzati. A volte i criminali scoprono una miniera d'oro sotto forma di archivio che contiene anche numeri di carte di credito, e ne approfittano per acquistare merce truffaldinamente. Ma, anche quando l'archivio dei visitatori non contiene informazioni tanto preziose, i criminali possono provare a collegarsi con i maggiori siti di commercio elettronico usando gli indirizzi email e le password appena rubate, nella speranza di incappare in una password riciclata, riuscendo così a fare acquisti a nome del malcapitato.

Le password possono anche essere indovinate per tentativi. Per esempio, la posta elettronica viene consegnata al legittimo desti-

nario quando questi si presenta con una password, ma nulla impedisce a un delinquente di tentare un collegamento a ripetizione, provandole tutte. I moderni sistemi usati dai criminali informatici comportano l'uso di programmi automatici che tentano milioni di combinazioni. Si comincia con le più popolari combinazioni di 6 lettere, da aaaaaa fino a zzzzzz. Vengono tentate tutte le parole del vocabolario e tutti i nomi del dizionario dei nomi. Se ancora non basta, si ripete aggiungendo da una a tre cifre all'inizio e alla fine, ma anche i simboli come @ oppure \*, i numeri da 1900 a 2007 e i codici di avviamento postale validi. Infine si provano alcune sostituzioni comuni, come la cifra zero al posto della lettera O e viceversa. Secondo le statistiche degli esperti di sicurezza, quest'approccio indovina il 24 per cento delle password entro i primi 100 mila ten-



tativi e oltre il 55 per cento quando tutte le combinazioni (circa 308 milioni) sono state esaurite. I migliori fornitori di servizi Internet (non certo tutti, purtroppo) mettono in azione contromisure. Per esempio, un ufficio postale Internet che attende un secondo pri-

ma di restituire il messaggio «password sbagliata» è già sufficiente a scoraggiare tutti i criminali tranne quelli più dedicati. Però 100 mila secondi sono circa 27 ore: un tempo non impossibile. Inoltre le password vengono usate non solo per proteggere i nostri segreti e

la nostra privacy su Internet, ma anche sui documenti elettronici. Per esempio, moltissimi utilizzatori del popolare pacchetto Microsoft Office affidano informazioni privilegiate ai documenti Word, Excel e PowerPoint chiudendoli con una parola d'ordine. Ma, se quel documento va in mano a un malintenzionato, allora è possibile fare circa 350 mila tentativi al secondo di indovinare la password, che dunque resisterà solo se è estremamente lunga e ben congelata. Un documento compresso con WinZIP 7.0 può essere testato oltre un milione di volte al secondo, mentre uno protetto con PGP (uno stimato software di crittografia) solo 900 volte. Un delinquente organizzato potrebbe però disporre di molti calcolatori e farli funzionare in parallelo per tentare tutte le combinazioni

possibili il più in fretta possibile. Un programma di questo tipo è il PRTK della AccessData, un'azienda molto stimata che cerca di vendere il proprio software soltanto alle forze dell'ordine e a chi deve recuperare informazioni archiviate dentro documenti la cui password è stata dimenticata (ma distinguere la gente per bene dai criminali non è sempre facile). Abbiamo un consiglio per i nostri lettori che vogliono scegliersi una parola d'ordine sicura: sceglietela lunga, che contenga almeno una cifra nel mezzo (ma non una banale sostituzione di una lettera con una cifra) e un mix di lettere maiuscole e minuscole. Se volete tenerla a memoria, scegliete la password basandovi su una frase mnemonica, per esempio memorizzate il titolo del film di Lina Wertmüller *Stamattina alle 10 in via dei Fiori in una nota casa di tolleranza* e scrivete «Sa10ivdFi1ncdt». Ma non c'è bisogno di memorizzare. Se usate un calcolatore con Mac OS X affidate le vostre password al Portachiavi, una funzionalità incorporata in quel sistema operativo. Se invece preferite Windows, scaricate il programma gratuito Password Safe 3.0.

#### POSTA ELETTRONICA

## I subdoli trucchi per sommergerci con lo spam e i virus

Uno spot di 30 secondi alla televisione costa circa 3 centesimi per ogni spettatore. Una pagina a colori su una rivista un centesimo e mezzo. Spedire una busta con una pubblicità e il coupon per aderire (abbonarsi, sottoscrivere) è di gran lunga più costoso: si può sfiorare il franco per ogni destinatario. Il mezzo più economico per contattare un potenziale cliente è anche il più odioso per i consumatori: la posta elettronica indesiderata, o spam. In questo caso il costo di mercato è di circa un franco per ogni diecimila email consegnate.

Tra i nostri lettori, quelli più affezionati alla posta elettronica a questo punto faranno un balzo sulla sedia e osserveranno che la spam è odiosa a tal punto che tutti la gettano senza degnarla di un secondo sguardo. Purtroppo non è così. Secondo alcune stime circa 7 persone ogni milione contattato non soltanto leggono, ma cadono anche vittima di una

potenziale truffa proposta nel messaggio. Per lo spam di tenore pubblicitario (come le copie di orologi e prodotti di ancor più basso gusto) si sale a 1 ogni 100 mila. Una percentuale comunque bassissima, certo, ma sufficiente a rendere redditizia la spedizione di miliardi di messaggi indesiderati.

Il problema, per gli artefici di questo traffico fastidiosissimo, è come recuperare un numero sufficiente di indirizzi a cui spedire la posta-spazzatura. Nel tempo, si sono sviluppate numerose tattiche. Noi vogliamo informarvi i nostri lettori, in modo che possano cercare di evitare di cadere vittima.

Innanzitutto gli spammer consultano gli elenchi di tutti i nomi registrati su Internet, come per esempio cdt.ch oppure microsoft.com, e li combinano con un dizionario dei nomi, provando tutte le combinazioni possibili. Proveranno abele@cdt.ch, abra-

mo@cdt.ch, achille@cdt.ch e così via sino a zuzzurellone@cdt.ch, tentando sia i nomi sia i cognomi più diffusi. La stragrande maggioranza dei messaggi spediti rimbalzerà, ma quelli che risulteranno consegnati da quel momento saranno vittime di invii massicci. Quindi chi vuole evitare la spam favorisca gli indirizzi del tipo nome.cognome@cdt.ch. Una fonte preziosissima di indirizzi e-mail è il Web. Sono stati creati sofisticati programmi che leggono tutte le pagine Web al mondo alla ricerca di un testo che somiglia a qualcosa@qualcosaltro. Si chiamano in gergo *harvester* (che significa all'incirca «mietitrebba») e le versioni moderne sono in grado di aggirare anche i più diffusi *escamotage* messi in atto dalle persone per bene alla ricerca di una difesa, come gli spazi inseriti prima del simbolo @ oppure l'inserimento di parole extra, per esempio luca@RIMUOVIacco-

mazzi.it. La maggior parte del raccolto viene mietuto sugli spazi dove i giovani si scambiano messaggi: i forum, i cosiddetti newsgroup. Ma ci sono anche vasti e pubblici elenchi, come le pagine bianche del telefono, accessibili in Rete: un esempio è directories.ch. Quindi per scamparla dovremmo mantenere privato il nostro indirizzo e usarlo esclusivamente per corrispondere privatamente con amici e conoscenti.

Gli autori di spam sono spesso in combutta con i criminali che scrivono virus. Quando un moderno virus prende il controllo di un PC all'insaputa del suo proprietario, viene spessissimo usato per due scopi. Primo: tutti gli indirizzi presenti nella rubrica di contatti personale del titolare viene mietuta e trasmessa via Internet per future spedizioni. Secondo: il PC stesso viene usato per inoltrare pubblicità indesiderate (non necessariamente alle persone appena

citare). E qui è davvero difficile restare immuni, perché basta che un nostro contatto poco prudente si lasci infettare per violare la nostra privacy.

Una volta che un indirizzo è diventato di dominio degli spammer, nulla si può fare per liberarsi di questi appiccicosissimi molestatori. Un esempio preso dalla vita personale dello scrivente: io anni fa utilizzavo l'indirizzo luca@accomazzi.net. Quattro anni fa, nauseato dalle montagne di spazzatura che mi raggiungevano, l'ho chiuso e ho preso a usare altri indirizzi. Per una prova, poco fa ho riattivato il vecchio indirizzo compromesso. Ho creato nuovamente la casella mentre stavo scrivendo le parole «una volta» all'inizio di questo paragrafo. Nel momento in cui scrivo questa riga, l'indirizzo luca@accomazzi.net ha accumulato esattamente 107 messaggi pubblicitari. E io scrivo piuttosto velocemente... I.a.

#### CYBERBUSSOLA

## LEGO BIOLOGICO, LEGO INFORMATICO E UNIVERSITÀ DELLA SVIZZERA ITALIANA

DAVIDE GAI

Esiste un ponte tra biologia e informatica? Si possono trovare dei ragionamenti che, mutatis mutandis, siano applicabili ad entrambi gli universi? L'analogia tra codice genetico, basato sul DNA ed i suoi mattoni, i nucleotidi, e l'alfabeto binario delle macchine digitali, che pone le sue fondamenta sui numeri 0 ed 1 è forse un po' scontata. Proviamo ad andare oltre.

Supponiamo quindi di affrontare l'universo biologico con lo stesso spirito dei matematici, cercando di costruirlo a partire da un foglio di carta bianca: quali sono gli elementi che servono a costruire la geometria della vita? Dobbiamo trovare l'equivalente di rette, semirette, segmenti, curve, a partire dai quali costruire dei poligoni, o delle figure più complesse; che abbiano per di più il dono dell'esistenza.

L'unica famiglia di molecole che si presta a questo scopo è quella delle proteine. Queste sono delle costruzioni tridimensionalmente molto complesse che si ottengono combinando tra di loro una ventina di molecole più semplici, dette aminoacidi. Gli aminoacidi sono le lettere di un alfabeto che consente di costruire delle frasi e dei periodi molto complessi, che collettivamen-



te costituiscono il grande romanzo della vita. È possibile definire la complessità in modo più preciso, nel senso della sua valenza tridimensionale. Le cellule, che accostate insieme formano i tessuti i quali a loro volta si aggregano per creare gli organi, riescono in questo difficile compito grazie a degli

incastri di miliardi di proteine. Volendo banalizzarle le cose si tratta di una combinazione tra Lego e Geomag. Partendo da questi ragionamenti l'industria farmaceutica ha cercato di descrivere anche le malattie in termini di funzionalità molecolare, provando quindi a cercare il nesso tra certe forme proteiche e talune malattie. Ciò consente di trovare dei farmaci che abbiano forme complementari rispetto alle proteine patologiche identificate, che abbiano quindi la capacità di influenzarne il comportamento. Volendo riassumere il tutto con una semplice analogia, la ricerca biotecnologica è una sorta di complicatissimo gioco del Lego, dove un incastro tra due

componenti può essere contemporaneamente la causa di una malattia, oppure la terapia della stessa.

Perché parliamo di tutto questo all'interno di una rubrica informatica? Per il semplice motivo che questo gioco di Tetris i biologi non lo possono fare da soli: hanno bisogno dei computer più potenti del mondo, che siano in grado di simulare in pochi secondi le possibilità che due proteine abbiano di «combaciarsi» in modo stabile. Ciò è molto importante perché consente di trovare «a tavolino» la forma possibile di un potenziale farmaco, per poi cercare di costruirlo. E qui vengono gli informatici, soprattutto gli esperti di supercomputing e di simulazioni tridimensionali.

A Lugano è presente uno dei gruppi di ricerca più avanzati in questo settore, che opera all'interno dell'USI, ed è guidato da uno scienziato di fama mondiale, il professor Parrinello. Questo gruppo può costituire un asset estremamente importante per delle industrie biotecnologiche che vogliono avvalersi delle metodiche di simulazione da affiancare al lavoro più «tradizionale» (ammesso che si possa utilizzare questo termine) del biologo molecolare. La fusione

di questi due filoni di competenze può accelerare notevolmente il progresso della biologia molecolare che sta alla base delle ricerche biotecnologiche oltre che offrire nuovi stimoli che si possano affiancare alle attività classiche del supercomputing, come, ad esempio, le simulazioni meteorologiche, la scienza dei materiali e la pur importante modellistica finanziaria.

Allontanandosi di un paio di passi, per cogliere una visione d'insieme, non si può fare a meno di notare come a Lugano si stiano formando delle condizioni quadro estremamente interessanti per delle aziende innovative nel campo biotecnologico, che potrebbero mettersi in rete con le strutture di ausilio allo startup, come il CP Startup, che costituisce un ottimo trampolino di lancio per gli studenti di USI e SUPSI, il Tecnopolo e Ticino Transfer. A livello cantonale si andrebbero ad aggiungere a grandi centri di eccellenza come l'IRB e lo IOSI, numerose industrie farmaceutiche e CRO, Clinical Research Organizations, società che si occupano degli studi clinici. Come si può vedere, il codice informatico e quello biologico hanno molto in comune, e il loro anello di congiunzione passa attraverso un supercomputer.