Banalità sempre utili

/ 15.08.2022
di Alessandro Zanoli

Sembra impossibile che circolino ancora email di questo tipo, eppure succede: «Buongiorno, da un controllo effettuato sui nostri server risulta che alcune informazioni legate al vostro account xy@abc.ch non sono corrette. Vi preghiamo di aggiornare i vostri dati cliccando sul seguente link (…) Grazie per la collaborazione». Il messaggio arriva apparentemente dai gestori del nostro account di posta elettronica, e l'email, del resto è indirizzato proprio a noi, personalmente. Si tratta di uno degli innumerevoli tentativi di acquisire la nostra password personale. Abboccando alla richiesta verremmo indirizzati su un sito probabilmente uguale a quello del nostro provider, ma in realtà finto. I dati che inseriremo saranno rubati e usati in seguito per qualche effrazione poco simpatica.

Noi speriamo proprio che i nostri lettori siano i grado di riconoscere ormai questi tentativi truffaldini. Il punto a cui vorremmo mirare, in realtà è un altro. Ammesso e concesso che il web sia abitato da un gran numero di «curiosoni» che vogliono impossessarsi delle nostre password, voi le vostre dove le tenete? Fatti veloci calcoli, chi scrive deve purtroppo rendersi conto che tra sistemi di posta elettronica, di e-banking, abbonamenti a vari servizi informativi, musicali e a shop online, la sua lista delle password (notare: sono escluse dall'elenco quelle di uso professionale) contiene all'incirca 45 voci. Sono tantissime, ma chi segue la raccomandazione di non usare mai la stessa pass per più di un servizio, deve forzatamente adattarsi a questa complessità.

Detto questo, di nuovo: ma voi dove le tenete tutte queste password? Alcune persone le annotano puntigliosamente su un librettino che tengono poi nel cassetto della scrivania. È un sistema comodo ma da un punto di vista della sicurezza non è proprio il massimo, soprattutto in ufficio. Pare che quello sia il primo posto in cui gli hacker aziendali vanno a cercare per intrufolarsi nei computer altrui. Chi scrive ha tentato di aggirare il problema, annotando tutti suoi dati sensibili su un file apparentemente innocuo, dal titolo fuorviante «ricette_della_nonna.doc». Da tempo porta con sé quel file in una chiavetta USB appesa al suo portachiavi. Inoltre, su ognuna delle macchine che usa per il lavoro e per il tempo libero ne ha parcheggiata una copia, in una cartella altrettanto innocua «Menu di cucina».

Ma purtroppo, nella sua ingenuità chi scrive ha dimenticato una cosa: ogni sistema operativo offre la possibilità di ricercare eventuali files dispersi all'interno delle singole macchine. La ricerca non verte soltanto sul nome del file stesso (da qui l'idea che è meglio non nominare «password.doc» quel documento), ma può essere compiuta anche «all'interno» nel contenuto dei files. Se dunque per combinazione il file «camuffato» contiene parole sensibili, quali «password; pass; user; utente; account» o altre definizioni generiche, esse verranno trovate e impietosamente messe in luce. A un malintenzionato basterà quindi poter usare per pochi secondi il nostro computer per smascherare con relativa certezza il nostro escamotage.

Che fare per difendersi? Un sistema relativamente semplice c'è: è mettere una password anche sul

file delle password. Se usate un programma di videoscrittura come MSWord o altri suoi analoghi non salvate il file semplicemente come documento «.doc» o «.docx», ma trasformatelo in un file protetto da password. Su PC, cliccare su «Salva con nome», poi scegliere «Strumenti», «Opzioni generali»: scegliete l'opzione relativa e inventate la password per il documento, confermatela e, una volta salvato, il documento chiederà alla sua apertura di inserirla. Se seguite questo consiglio avrete definito la «password suprema» o la «password delle password». La cosa non semplifica la vita, anzi, pare aggiungere una complicazione. Qui entra in gioco però un altro principio, quello della creazione di password efficaci ma facilmente memorizzabili. Ne parleremo in una prossima rubrica.

Detto questo, occorre una precisazione: forse sarebbe più prudente salvare le proprie password in un file protetto da password ma che sia in formato PDF (si riesce a generarlo partendo direttamente dal file MSWord di cui sopra). Per qualche motivo viene più facile fidarsi dei protocolli di sicurezza di Adobe, che di quelli di Microsoft, costantemente nel mirino dei malintenzionati.