GESTIONE DELLA PROFESSIONE E SOFTWARE, Nuove tecnologie e Studio digitale

La sicurezza delle password dello studio professionale

di **Giuseppe Vitrani**

Un tema che si pone sempre più all'ordine del giorno negli studi legali è quello della sicurezza delle dotazioni informatiche o degli strumenti informatici d'ausilio alla professione.

Molto si è detto e scritto della necessità di dotarsi di antivirus o di effettuare periodici (o meglio, quotidiani) backup dei dati al fine di non disperdere il lavoro dell'avvocato; si tratta di temi importantissimi, che richiedono adeguate trattazioni e continui aggiornamenti.

In questa sede non si tratterà però di tali argomenti, bensì di alcune utili risorse "a costo zero" che il professionista può sfruttare sia per fare un check-up sulla sicurezza delle proprie dotazioni che per migliorare la gestione di alcuni strumenti cruciali per la professione, prime fra tutte le miriadi di password con le quali ci si trova a confrontarsi ogni giorno.

È dunque un buon consiglio quello di verificare se la password scelta è sicura; lo si può fare sottoponendola alla verifica da parte di un sito specializzato a tal fine (https://howsecureismypassword.net), che calcolerà quanto tempo occorre per violarla; si scoprirà così che la maggior parte delle password utilizzate ("qwerty", "123456", "password") sono tra le più insicure e possono essere decifrate in pochissimi secondi.

L'ulteriore problema posto dalle password è che sono richieste per sempre più servizi e, se diversificate (come dovrebbe avvenire), sono difficili da ricordare; per ovviare a tale difficoltà si scelgono allora opzioni altamente insicure, come quella di scriverle su fogli volanti che possono essere smarriti o sottratti da malintenzionati, oppure come quella di utilizzare una sola password (e magari un unico username) per tutti i servizi utilizzati. Con il risultato che il furto delle credenziali nel corso di un attacco hacker può compromettere l'utilizzo di una miriade di servizi.

Per ovviare a tali inconvenienti esiste in realtà una soluzione ottimale, che è quella di utilizzare un *password manager*, una vera e propria cassaforte all'interno della quale racchiudere tutte le proprie credenziali di autenticazione. Utilissimo (e gratuito) esempio in tal senso è keepass (https://keepass.info), grazie al quale attraverso un'unica master password, che potrà essere anche piuttosto complicata, potrà essere creato un database che contiene tutti gli username e le password utilizzate dallo studio; e di più: inserendo anche l'indirizzo internet del servizio utilizzato sarà possibile collegarsi ed autenticarsi direttamente sullo stesso. Inoltre, il software offre anche un servizio di generazione casuale di password, che potrà essere sfruttato grazie al fatto che queste non dovranno essere ricordate a memoria ma potranno essere lette direttamente accedendo al database protetto dalla master password.

Altra utile verifica che si potrà condurre è relativa all'indirizzo di posta elettronica (anche certificata). Esistono infatti risorse (es. https://haveibeenpwned.com) attraverso le quali è possibile verificare se il proprio account risulti coinvolto in *data breaches* avvenuti su server esterni e quale tipologia di credenziali sia stata eventualmente sottratta (es. indirizzo mail, password, password crittografate). Evidentemente, laddove la verifica avesse risultato positivo, si potrebbero porre in essere le necessarie contromisure, come ad esempio il cambio delle password dei servizi compromessi in modo da limitare e nella maggior parte dei casi porre fine ai problemi.