Cyberinsicurezza

La password più usata è sempre lei, la sequenza numerica "123456". Lo ha svelato il Centro Nazionale per la Cybersecurity del Regno Unito in occasione del World Password Day, la ricorrenza nata per ricordare l'importanza di adottare precauzioni di sicurezza quando si naviga sul web. Oltre alle banali combinazioni alfanumeriche, tra le parole più utilizzate ci sono date di nascita, nomi di figli e di animali domestici. Sono scelte che mettono in pericolo i nostri dati personali e che aumentano la possibilità che malintenzionati violino computer, servizi bancari o account.
"Il World Password Day è una giornata che aveva un significato quando gli strumenti tecnologici non permettevano a chiunque di adottare altre modalità di autenticazione. Nove anni dopo la sua istituzione, è doveroso un cambio di prospettiva sulla base dello scenario attuale con buona pace di chi spera ancora che le password possano proteggere i nostri dati", spiega Alessio Pennasilico, membro del Comitato Scientifico del Clusit, l'Associazione italiana per la sicurezza informatica che periodicamente redige un rapporto. Dall'ultimo si evince che nel 2021 sono stati registrati 2.049 attacchi informatici gravi, un aumento di circa il 10% rispetto ai dati rilevati nel 2020. La proposta degli esperti del Clusit è quindi, provocatoriamente, di intitolare una giornata non alla password ma alla "Secure Authentication", dedicata cioè "a creare consapevolezza a tutti i livelli nella maniera più efficace per garantire la sicurezza degli accessi", come la biometria.
La società di sicurezza Check Point Software Technologies in vista del World Password Day delinea le cinque regole da seguire per creare una password sicura: utilizzare una combinazione di caratteri; avere una password diversa per tanti servizi; più è lunga, più è sicura; cambiare le password regolarmente; essenziale l'autenticazione a due fattori. Su questo ultimo punto insiste anche Marco Ramilli, Ceo della società di sicurezza Yoroi. "Oggi è fortemente consigliabile l'utilizzo di generatori di password randomiche e complesse salvate in una password chain, ovvero una cassaforte cifrata utilizzata come contenitore di tutte le password generate - avverte Ramili - e, per evitare un possibile data leak del contenuto della "cassaforte" si deve utilizzare un secondo fattore di autenticazione preferibilmente attraverso app e non attraverso sms, per ridurre il rischio dello sim swapping, la sostituzione o duplicazione fraudolenta della Sim".