PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1252 di mercoledì 25 maggio 2005

Password da annotare?

La risposta non è scontata. Consigli per scegliere e gestire le password di accesso al PC e ai servizi via web.

Pubblicità

Che sia la password del programma di posta o quella dell'home banking, o quella utilizzata per fare acquisti on line, la sua perdita, o peggio l'intercettazione da parte di un malintenzionato, può dare seri grattacapi.

Non sono infrequenti i casi di furti di identità, tramite i quali malviventi, dopo essere riusciti a carpire password altrui, le utilizzano per modificare l'indirizzo postale in modo da ricevere i prodotti acquistati, per seguire bonifici da un conto corrente bancario o per richiedere prestiti e finanziamenti, ma anche per assumere l'identità "rubata" in chat o altri servizi online, come le aste.

Le password devono essere scelte, quindi, attentamente; una password facile da ricordare può essere anche una password facile da scovare. Gli hacker utilizzano attacchi basati su "dizionari" e altri strumenti software in grado di specificare rapidamente migliaia di password comuni, cercando le possibili corrispondenze.

"È quindi importante - afferma Microsoft nelle sue indicazioni di sicurezza - proteggere i dati utilizzando password complesse, gestire con attenzione le password e monitorare i propri account."

A tal proposito Microsoft ha individuato alcune caratteristiche che rendono sicura una passworD:
- lunghezza di almeno sette caratteri. Una password è tanto più sicura, quanti più caratteri include;
- deve contenere lettere maiuscole e minuscole, numeri e simboli;
- deve avere almeno un simbolo in una posizione compresa tra il secondo e il sesto carattere;
- deve utilizzare almeno quattro caratteri differenti (senza ripetizioni);
- deve presentarsi come una sequenza casuale di lettere e numeri. A tal riguardo è bene: Non usare per la password alcuna parte del nome di accesso, non usare alcuna parola o nome reale in nessuna lingua, non usare numeri al posto di lettere simili, non riutilizzare alcuna parte della password precedente, non usare lettere o numeri consecutivi (come "abcdefg" o "234567), non usare lettere corrispondenti alle posizioni dei tasti sulla tastiera, come "qwerty.

Costruita seguendo queste indicazioni la password diviene più difficile da individuare, ma certamente più difficile da ricordare. E' allora necessario fare uno sforzo mnemonico o annotarla?
Tra le indicazioni di sicurezza sul sito italiano si Microsoft si legge: "non annotare la password", e anche "non utilizzare le funzionalità per la memorizzazione automatica della password senza prima considerare il valore dei dati protetti dalla password".
Ma come ricordare allora le diverse password per accedere ai vari servizi (utilizzare una sola password per tutti è infatti altamente insicuro...)?

Una diversa indicazione viene da un esperto di sicurezza della stessa Microsoft. Secondo quanto riportato da un quotidiano on line italiano di informatica, l'esperto Jesper Johansson avrebbe affermato che "l'industria di settore per anni ha sbagliato nel dire agli utenti che non c'è motivo di scriversi le password utilizzate. [...]L'uso di un'unica password per una molteplicità di servizi è dai più considerata una leggerezza che può costar cara. [...].Se scrivo le password e proteggo quel pezzo di carta - o il supporto dove le ho scritte - non c'è davvero nulla di male. Questo ci consente di ricordare più password e di scegliere password migliori".