

Non c'è solo la letteratura: **L+d2csc=a2csi**. Chi non ricorda il teorema di Pitagora? La somma dei quadrati costruiti sui cateti equivale al quadrato costruito sull'ipotenusa (il cui acronimo è appunto L+d2csc=a2csi).

I chimici possono suggerire miriadi di formule: **CH3CH2OH** è la formula dell'etanolo, lo spirito di vino.

La storia, ricca di date, può aiutarci a costruire con facilità stringhe molto lunghe: **i14i1789ipdPaIBeIRF** (il 14 luglio 1789 il popolo di Parigi assale la Bastiglia è la Rivoluzione Francese).

Chi difetta di ricordi scolastici può ricorrere al vivere quotidiano: **Pft1ce1t** (Piazza Ferretto tra 1 chiesa e 1 torre); quanti sanno che a casa vostra **Lcel2padx** (La cucina è la seconda porta a destra), oppure che **is12IdGA** (in salotto dodici litografie di Gianni Aricò)?

Un particolare accenno meritano le PASS per l'*home banking*. Queste sono le più importanti e riservate, dunque vanno costruite con particolare attenzione. Inoltre per aumentare la sicurezza dell'accesso spesso i siti web legati alla movimentazione del denaro, obbligano a cambiare la PASS ogni pochi mesi e impediscono di riutilizzare la medesima PASS per un certo periodo, generalmente un anno. Una semplice soluzione può essere quella di riutilizzare la stessa PASS seguita da un numero progressivo: **IpsdAMx1**, deve sciogliersi così: «I promessi sposi di Alessandro Manzoni» - x1 (per primo ciclo), cui seguiranno **IpsdAMx2**, **IpsdAMx3**..., per poi ricominciare. In questo modo anche se non si ricorda il ciclo esatto le possibilità di sbagliare sono limitate. Questo è importante perché spesso i siti delle banche consentono un limitato numero di tentativi, dopodiché l'account viene bloccato e bisogna recarsi allo sportello per richiedere nuove modalità di accesso.

Importante: mai e poi mai la banca, o la posta, chiederà l'invio o la modifica della vostra PASS per e-mail: si tratta di phishing, una truffa per carpire i vostri dati sensibili e usarli fraudolentemente.

Un'ultima nota per quei siti che permettono, o talvolta obbligano, anche l'utilizzo di un carattere speciale. Il consiglio è quello di attribuire a questi caratteri un significato in un acronimo: **i25dcsi*** (il 25 dicembre cadono spesso i "fiocchi di neve"), oppure **\$&fsl2sdA** (dollari & sterline sono le 2 sponde dell'Atlantico).

I.T.I.S. «Carlo Zuccante»
CORSO SERALE PER ADULTI
corsi di Informatica e di Elettronica

LE PICCOLE GUIDE PRATICHE

INFORMATICA

1

PASSWORD

sede del corso serale:

Via Astorre Baglioni 22 – 30173 Mestre-Venezia

<http://serale.zuccante.it>

serale@zuccante.it

PERCHÉ SERVE UNA PASSWORD

Oggi sempre più siti web richiedono un'identificazione per poter accedere ai servizi offerti. Questa avviene attraverso due elementi:

1. ID USERNAME (o ID)
2. PASSWORD (o PASS)

L' ID è il nome con cui vogliamo essere conosciuti in quel sito, mentre la PASS è l'elemento che verifica che siamo veramente noi, e non qualcun altro che si spaccia per noi.

Poiché molto spesso l' ID è pubblico (è il caso, per esempio, della posta elettronica) in molti hanno la possibilità di impostare i dati per accedere alla nostra casella di posta.

Per esempio, l'indirizzo e-mail: pinco@pallino.it significa che accedendo al dominio <http://www.pallino.it> si può arrivare alla pagina in cui si può consultare la posta (probabilmente <http://mail.pallino.it>) a questo punto si inseriscono l'ID (in questo caso «pinco») e la PASS. Se qualcuno disponesse della nostra PASS potrebbe dunque accedere alla nostra posta: leggerla, cancellarla o rispondere, sostituendosi a noi.

E questo per tutti i siti che richiedono un'identificazione, siano siti che propongono ricette di cucina o che ci permettono di operare, tramite le banche on-line, sul conto corrente e qui, se qualcuno si appropria della nostra identità, può essere pericoloso e costoso.

Dunque una PASS dev'essere:

1. tenuta rigorosamente segreta;
2. facile da ricordare;
3. bastevolmente complessa.

QUANTE PASSWORD BISOGNA AVERE

Vi sono diversi orientamenti in questo campo. Per alcuni bisogna avere una PASS per ogni sito web a cui si è iscritti, mentre per altri tre buone PASS (una per la posta, una per la banca e servizi che richiedono comunque pagamenti on-line, e un'altra per tutte le altre occasioni) possono bastare.

LE PASSWORD DA EVITARE

Il proprio nome (o quello del coniuge, dei figli o dei genitori), data o luogo di nascita sono in generale informazioni che si possono reperire con facilità, e dunque sono da evitare. Vi sono anche dei programmi che cercano da soli tutte le combinazioni possibili con i dati conosciuti (es: sapendo che la data di nascita è il 9 gennaio 1950 provano: 090150, 9150, 19500109, 500109 ..., combinandolo

con il nome).

Eguale comune (e dunque facile da trovare) è la PASS uguale all'ID, magari ripetuta o a specchio (es: ID paolo; PASS paolo, oppure paolopaolo, o ancora paolooloop).

Generalmente le PASS più usate sono molto semplici, come: **1234** oppure **qwerty** (le prime lettere della tastiera del computer) o **pippo**, il simpatico personaggio dei *cartoons*.

Vi sono inoltre dei programmi che cercano le PASS tra tutte le parole presenti nel vocabolario; quindi sono da evitare parole, o frasi, di senso compiuto.

QUALCHE CONSIGLIO PER UNA BUONA PASSWORD

Già oggi molti siti web richiedono una PASS costruita con dei criteri di sicurezza che sono:

1. almeno 8 caratteri (generalmente tra 8 e 12);
2. almeno una cifra;
3. almeno una lettera maiuscola.

Nella generazione e memorizzazione della PASS alcuni siti richiedono che questa contenga anche un carattere speciale (es. £, \$, &, *, %, ...), mentre in altri siti i caratteri speciali non sono accettati.

In linea di principio le PASS più impenetrabili sono quelle generate a caso (es. **mgD7p2sKq**), ma queste sono però difficili da ricordare: bisogna necessariamente scriverle e dunque qualcuno può carpirle. Conviene allora generare una PASS, ragionata e memorizzabile. Il consiglio è di trasformare delle semplici frasi in acronimi, cioè una parola o una sigla ricavata dalle iniziali di più parole o frasi.

IfMP2266 può sembrare una scritta a caso; invece è l'acronimo di un celebre romanzo, «Il fu Mattia Pascal» (**IfMP**) e contando le lettere che compongono le parole abbiamo **2** (Il), **2** (fu), **6** (Mattia) e **6** (Pascal). Questo meccanismo può essere ulteriormente arricchito con numerose varianti (**If22MP66**, oppure **I2f2M6P6** e così via).

Dunque basta ricordare un titolo per ricostruire velocemente una PASS che risponde ai criteri di sicurezza e che si può anche facilmente memorizzare, evitando di scriverla e riducendo così il rischio che possa essere sottratta.

Romanzi, poesie, commedie, tragedie, melodrammi, musical, canzoni, proverbi, aforismi, brocardi, detti e sentenze: tutto può essere utilizzato, rendendo così enorme il numero delle possibilità.