

ABBONAMENTI

ARCHIVIO

PIÙ VISTI

SOCIAL

METEO

TUTTOAFFARI

LAVORO

LEGALI

NECROLOGIE

SERVIZI



LA STAMPA.it

TECNOLOGIA

Cerca...

TORINO - CUNEO - AOSTA - ASTI - NOVARA - VCO - VERCCELLI - BIELLA - ALESSANDRIA - SAVONA - IMPERIA e SANREMO

VOCI DI MILANO

ATTUALITÀ OPINIONI ECONOMIA SPORT TORINO CULTURA SPETTACOLI MOTORI DONNA CUCINA SALUTE VIAGGI EXTR@ FOTO VIDEO

HOME POLITICA ESTERI CRONACHE COSTUME TECNOLOGIA SCIENZA AMBIENTE LAZAMPA I TUOI DIRITTI MARE MONTAGNA SPECIALI

Consiglia

0

Tweet

0

0



Rimuovi dalla timeline di Facebook

TECNOLOGIA

30/09/2010

Perché una password sicura non significa sicurezza

Da programmi "spia" a requisiti errati per le chiavi d'accesso, ecco tutti i pericoli in cui possiamo incorrere mentre navighiamo

GIUSEPPE FUTIA

Facebook, Twitter, Youtube. Sono soltanto alcuni dei servizi a cui accediamo quotidianamente in rete. Ed utilizzare tanti servizi, per gli utenti più accorti, significa dover pensare ad almeno altrettante password d'accesso per i propri account. In molti casi, però, anche andare alla ricerca di una parola o un'espressione apparentemente inattaccabile può rivelarsi uno sforzo infruttuoso. Questo perché il senso di sicurezza da potenziali attacchi informatici che ne deriva può provocare una serie di disattenzioni rispetto ad altri pericoli in cui rischiamo di incorrere. Esistono, ad esempio, alcuni software denominati keyloggers, depositati all'interno dei nostri computer da virus informatici, che inviano furtivamente in rete tutte le password che utilizziamo. Secondo Cormac Herley, ricercatore Microsoft che si occupa di sicurezza informatica, preservare i nostri sistemi dalla presenza di keyloggers è molto più importante di una chiave d'accesso resistente.



I dubbi e le incognite legate alla difesa dei propri dati spesso non dipendono dal comportamento dell'utente. Herley rivela che in molti casi sono gli amministratori dei sistemi a non riflettere sul fatto che requisiti bizzarri, se non addirittura inesistenti, per la definizione della password possono indurre gli utilizzatori a comportamenti errati. Non è plausibile, sottolinea Herley, che siti web sottoposti a enormi quantità di traffico, attraverso cui si accede a informazioni di natura finanziaria e personale, abbiano delle policy così "rilassate" nei requisiti delle password.

Nell'ambito dell'e-commerce, ad esempio, Amazon impone un'unica regola: inserire una password di sei caratteri. È pur vero che sistemi di questo genere sono in grado di resistere ai cosiddetti "attacchi a forza bruta", bloccando l'account per ventiquattro ore nel caso in cui siano falliti diversi tentativi di accesso. Tale espediente impedisce l'azione di tutti quei software che provano a intrufolarsi nei sistemi, provando l'accesso attraverso innumerevoli combinazioni di password.

Donald E. Norman, co-fondatore del gruppo Nielsen Norman, pone invece la propria attenzione sul problema inverso. In un saggio intitolato "When security gets in the way", in cui si discute del rapporto esistente tra sicurezza, privacy e usabilità, Norman evidenzia il caso della Northwestern University che obbliga gli utenti a rispettare ben quindici regole nella scelta delle proprie password. Un sistema di questo genere, che tra l'altro costringe l'utente a rinnovare la parola segreta ogni centoventi giorni, può sortire effetti contrari a quelli sperati.

Davide Pozza del Dipartimento di Automatica e Informatica del Politecnico di Torino suggerisce alcuni metodi per poter assemblare password resistenti: scegliete una frase non banale oppure immaginate una scena divertente, che vi dia qualche emozione positiva, e descrivetela con una frase. Quindi, per costruire la password, prendete la lettera iniziale di ogni parola, ed eventualmente anche la lettera finale, in modo tale da includere le lettere accentate presenti in molte parole della lingua italiana. Inoltre, considerate la punteggiatura della frase e, per renderla ancora più resistente, sostituite alcune lettere con

Ultimi Articoli

+ Tutti gli articoli

OPEN LETTER TO SKYPE

FROM CONSUMERS' PROTECT ASSOCIATES, INTERNET ACTIVITY, JOURNALISTS & OTHER ORGANIZATIONS

(Gennaio 2012)



+ Appello a Microsoft e Skype su privacy e trasparenza



+ Google guida la lotta per limitare l'accesso delle autorità ai dati personali



+ Web Movies in streaming dal 31 gennaio



+ Il Web "svela" la Corea del Nord



+ È il Dna l'hard disk del futuro

+ Google, Apple, The Pirate Bay Wikileaks: il cinema racconta il Web

Condividi gli articoli con i tuoi amici

Con l'app Facebook LaStampa.it puoi condividere immediatamente le notizie e gli approfondimenti che hai letto.

Attiva l'app sul tuo profilo e segnala a tutti i tuoi amici le tue news preferite!

Scopri di più su facebook.lastampa.it!

Accedi a Facebook

numeri o simboli, secondo delle regole che avete definito in precedenza. Per esempio, stabilite che la lettera “a” sia sostituita con il simbolo “@” e che la lettera “e” diventi un “3”.

Pozza sottolinea che non bisogna focalizzarsi soltanto sulla robustezza della password, ma che occorre prestare attenzione anche al modo in cui la validità delle password viene verificata dai sistemi a cui queste vengono inviate. Se la password viene spedita “in chiaro”, allora un attaccante può carpirlo semplicemente osservandola passare nel traffico di rete. Per questo motivo, afferma Pozza, un elemento molto importante è quello di effettuare la trasmissione della password su una connessione dati protetta e sicura. A tal fine, i protocolli crittografici sono utilizzati per garantire la segretezza e l'integrità dei dati inviati, ed evitare che precedenti trasmissioni di dati vengano in qualche modo “riciclate”.

SPECIALE ELEZIONI



NEWS /
MULTIMEDIA



SCOPRI LE
NOSTRE APP



LE VOCI DELLA
POLITICA



PREMIO 1APP
4DEMOCRACY



I RISULTATI DEL
2008



GOOGLE
ELEZIONI

Annunci PPN



Un angelo chiede aiuto
dona una speranza ad un
bambino maltrattato
[Adottalo a distanza](#)



Gli Headhunter
ricercano
candidati per posizioni
senior. Inserisci il tuo profilo
www.experteer.it



Conto Corrente
Arancio
Zero spese, carta di credito
gratis. Scopri i vantaggi!
contocorrentearancio.it