

# Ogg.: Allarme violazioni email

Gentile Cliente,

la news che sto inviando scaturita da una informazione vista su google, deve essere letta con molta attenzione. Si parla di password, di robustezza delle password, di cambio password, della lunghezza delle password, insomma tutte quelle cose sulle password che si sanno, ma che non sempre si mettono in pratica. Allora attenzione alle password non solo su Gmail, ma anche alle password aziendali. Avere password corrette aiuta anche in caso di disputa tra lavoratore e Titolare.

Ecco l'avviso comparso sull'interfaccia della casella di posta Gmail di milioni di utenti per consigliare di porre particolare attenzione alle password in uso.

## **Se riutilizzi la tua password di Gmail in altri siti web, cambiala adesso**

Google suggerisce quindi di non utilizzare la password scelta su Gmail anche su altri siti, (specialmente per account importanti come web banking, posta elettronica, o banche dati aziendali), e questo lascia presagire una possibile impennata delle violazioni tanto nelle prossime ore, quanto nei prossimi giorni. E l'iniziativa intrapresa da Google, rivela che in effetti il problema c'è, ed è di dimensioni tutt'altro che trascurabili.

Le migliaia di violazioni degli account Gmail che sono stati registrati, tutti provenienti dall'est Europa, sono stati in realtà accessi indesiderati con **password** del tutto elementari, e questo rispolvera il vecchio problema della diffusa ed incauta scelta di parole chiave semplici come la data di nascita, il proprio nome, se non addirittura parole banali come "pippo" o sequenze di numeri come "123456".

Da non dimenticare poi che, se chi utilizza la posta elettronica non lo fa solo per uso personale ma anche per lavoro, magari per conto della propria azienda, in tal caso oltre alla beffa dell'accesso da parte degli hacker, c'è anche la responsabilità della violazione del Codice della Privacy per la mancata adozione delle misure minime di sicurezza ai sensi dell'art. 33 del Dlgs 196/2003 e come prescritto nella Regola 5 dell'ivi annesso Disciplinare Tecnico: "La parola chiave (...) è composta da almeno otto caratteri (...); essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi."

Quanto può costare aver deciso di mettere in modo superficiale la prima parola che ci è venuta in mente come password di una mail aziendale o di una qualunque altra banca dati senza prestare attenzione a quanto previsto dalla legge?

Se qualcuno in buona fede pensa che si tratti di una leggerezza di trascurabile, si sbaglia di grosso: ai sensi dell'art.169 dello stesso Codice della Privacy, "Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni."

Quali sono allora i comportamenti e le cautele da adottare con la nostra mail, personale o aziendale che, sia per evitare di cadere vittima di un hacker correndo il pericolo di vedere violata la privacy della nostra corrispondenza elettronica?

Riporto a tal proposito un breve vademecum (rivolto sia all'azienda che all'incaricato):

### **Come creare password efficaci**

Per proteggere i dati riservati dell'azienda, così come per evitare che i dipendenti possano leggere la posta personale altrui, la soluzione opportuna è l'adozione di password adeguate che rispettino almeno le prescrizioni minime contenute nel Codice della Privacy. Ma, proprio perché di misure minime si tratta, non è detto che una password scelta con i criteri del Dlgs 196/2003, pur garantendo una discreta affidabilità, risulti pienamente efficace nel nostro caso. Le password consentono effettivamente di salvaguardare i dati riservati dagli sguardi indiscreti e accessi illeciti solo se veramente robuste e aggiornate regolarmente, tanto è vero che lo stesso Legislatore, dopo aver prescritto i requisiti minimi per le password, raccomanda poi l'adozione di idonee misure da individuare a seconda dell'importanza dei dati e del grado di rischio al quale si è esposti nel caso specifico.

Quanto sono efficaci le password che attualmente usi? E' necessario prima di tutto porsi le seguenti domande:

- Usi password che altri potrebbero indovinare facilmente, come la data di nascita o il nome di tuo figlio, o di tua moglie ?
- Utilizzi parole di senso compiuto?

- Selezioni abitualmente la casella di controllo per la memorizzazione della password, in modo da non doverla digitare ogni volta?
- Annoti le password in documenti che potrebbero essere letti da altri?
- Usi la stessa password per qualsiasi risorsa o sito web?

**Se hai risposto affermativamente a una qualsiasi di queste domande, i dati presenti nel tuo computer sono vulnerabili e l'applicazione delle password non è sufficientemente rigorosa.**

### **Vulnerabilità**

Ecco i rischi che i criteri appena esaminati comportano e alcuni suggerimenti per eliminarli:

**Password facili da indovinare:** se al tuo computer possono accedere altri colleghi, è anche probabile che questi siano a conoscenza di informazioni private quali il tuo nome o quello dei tuoi familiari, che è pertanto sconsigliabile utilizzare come password. Evita di utilizzare informazioni generalmente note o facilmente reperibili quali indirizzo, data di nascita, hobby, animali domestici, squadre di calcio preferite, etc.

**Parole di senso compiuto:** gli hacker possono utilizzare programmi che consentono di identificare le password basate su parole di senso compiuto in più lingue. Evita pertanto di utilizzare tali parole per le password. E' più sicuro utilizzare una combinazione di lettere, numeri e simboli.

**Password automatiche:** quando selezioni le caselle di controllo per la memorizzazione della password frequenti nei siti web, alle visite successive le caselle di testo per la password risultano precompilate con i dati memorizzati, visualizzati sotto forma di punti o di asterischi. Questa funzionalità può essere pericolosa se altri utenti hanno accesso al computer. Sono disponibili programmi poco costosi o persino gratuiti che consentono la decodifica di tali punti e asterischi. La soluzione consiste nell'evitare di memorizzare le password e nell'assicurarsi, in ogni caso, che per l'accesso a Windows sia configurata una password complessa, da digitare ogni volta che si accede al sistema. In questo modo, si elimina il rischio di intrusioni.

**Annotazione delle password:** le password sono utili solo se le si ricorda: difficili per i potenziali intrusi, ma facili per noi. D'altra parte, annotarle in un foglietto e lasciarlo alla portata di tutti non è una soluzione opportuna. Più avanti saranno esaminati alcuni metodi per creare password facili da ricordare. Se disponi di più password, puoi archivarle nel PC in forma crittografata, proteggendole a loro volta con una password realmente efficace e che sei in grado di ricordare.

**Utilizzo della stessa password:** molti utenti usano la stessa password, o piccole variazioni della stessa, per qualsiasi risorsa. Ovviamente, questo accorgimento riduce la necessità di tenere a mente un gran numero di password differenti, ma comporta il rischio che altri, qualora riescano a indovinarla, possano accedere a qualsiasi risorsa protetta dell'utente. È pertanto consigliabile utilizzare password differenti e, anzi, modificarle spesso.

### **Password robuste**

Una password robusta ha le seguenti caratteristiche:

- Ha una lunghezza di almeno otto caratteri (se è più lunga meglio ancora)
- Include lettere maiuscole e minuscole, numeri e simboli
- Viene cambiata di frequente (il Codice Privacy prevede ogni 6 mesi per dati comuni o ogni 3 mesi per dati sensibili, ma nulla toglie di decidere di cambiarla anche più spesso)
- Ogni nuova password è sensibilmente diversa dalla precedente

Alcuni esempi di password robuste:

- d&2!Zp>19
- \* M@b9(bE

L'inconveniente di queste password, è che sono sì difficili da decifrare, ma sono anche difficili da ricordare, in particolare se sono numerose e tutte con questo livello di complessità.

Il nostro sforzo, sarà invece quello di creare password complesse, e quindi robuste ma che siano facili da ricordare.

Le password in forma di frase sono per esempio più facili da ricordare:

- Tdo1schiaffo!
- sonole8xchènouvai?

Un'altra tecnica consiste nello scegliere una frase, ma utilizzando solo la prima lettera di ogni parola. Per esempio:

- Imgèni18s! (Il mio gatto è nato il 18 settembre!)

- Imcèf&sxm. (Il mio cane è felice & stravede x me.)

Un altro trucco per creare password facili da ricordare consiste nell'unire una coppia di parole tramite numeri e simboli. Per esempio:

- 2patate+fagioli=€4
- 44gatTinflAx3

Ci sono svariati modi per creare password facili da ricordare. Poiché le dovrai modificare periodicamente, puoi scegliere un evento particolarmente significativo. Per esempio:

- 25°anniversarioDmami&papi
- berlino2006italia-francia6a4

Una volta create password complesse o in forma di frase, ci sono 3 modi per garantirne l'efficacia:

1. Sconnettersi sempre dal sistema quando si deve lasciare il PC incustodito
2. Cambiare le password almeno ogni 6 mesi (se trattiamo dati sensibili, ogni 3 mesi)
3. Non condividere le password con nessuno, neanche con persone di cui ci fidiamo

Sfruttando l'efficacia delle password complesse, potrai garantire alle informazioni riservate la segretezza che meritano.

Come sempre sono a sua disposizione per tutte le informazioni aggiuntive necessarie

Cristina Cicogni

CAST Group  
Viale Virgilio, 54G I-41123 Modena  
T. +39.59.885.711 F. +39.59.885.799  
cell. 348 7314546  
<http://www.castgroup.it>

Cristina Cicogni  
Consulente Privacy  
T. +39.59.885.705

Avvertenze ai sensi del D.Lgs.196 del 30/06/2003

Le informazioni contenute in questo messaggio di posta elettronica e/o files allegati, sono da considerarsi strettamente riservati. Il loro utilizzo è consentito esclusivamente al destinatario del messaggio, per le finalità indicate nello stesso. Costituisce violazione ai principi dettati dal D.Lgs. 196/2003: trattenere il messaggio stesso oltre il tempo necessario, divulgarlo anche in parte, distribuirlo ad altri soggetti, copiarlo od utilizzarlo per finalità diverse. Ricordiamo che in ogni momento potrete richiederci la sospensione da parte nostra dell'impiego dei vostri dati, ad esclusione delle comunicazioni effettuate in esecuzione di obblighi di legge. Qualora riceveste questo messaggio senza esserne il destinatario Vi preghiamo cortesemente di darcene notizia via e-mail e di procedere alla distruzione del messaggio stesso, cancellandolo dal Vostro sistema. Grazie.