Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di mercoledì 2 aprile 2014

SOLUZIONI TECNOLOGICHE

I pericoli della rete

di **Teamsystem.com**

www.teamsystem.com

Tenere i **dati al sicuro** non spetta solo all'antivirus, la nostra attenzione gioca un ruolo fondamentale.

Il 63,5 % degli italiani naviga su Internet. La percentuale sale al 90,4% nel caso dei giovani e arriva all'84,3% per le persone più istruite, diplomate o laureate (fonte Censis). Con l'aumento continuo degli internauti cresce però anche il numero di **truffe** che ormai sempre più spesso vedono il web come palcoscenico preferito. Ma di cosa si tratta? Ce n'è per tutti i gusti: dai **raggiri via posta elettronica** alle finte aste o ai furti veri e propri di dati sensibili che avvengono tramite software maligni che scarichiamo inconsapevolmente facendo clic su un allegato o su un programma proveniente da Internet. **Tutti siamo potenzialmente vulnerabili**, ma spesso cadere vittime di una truffa ha un responsabile insospettabile: la disattenzione.

Anche il miglior antivirus o il firewall più potente non possono fare nulla se siamo noi a servire su un piatto d'argento i nostri dati ai potenziali malintenzionati. Lo dice una ricerca condotta da Splashdata che ha stilato un elenco delle **25 password più usate del 2012**. Bene, le prime tre sono: password, 123456 e 12345678.

Di seguito le riportiamo tutte e 25.

1. password
2. 123456
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball
11. iloveyou
12. trustno1
13. 1234567

14. sunshine
15. master
16. 123123
17. welcome
18. shadow
19. ashley
20. football
21. jesus
22. michael
23. ninja
24. mustang
25. password1

Il fatto più grave emerso da quest'ultima ricerca è che la maggior parte delle password riportate, erano presenti anche nella lista dello scorso anno, quindi vuol dire che nonostante la costante crescita delle truffe online, si **stenta a cambiare cattive abitudini** in fatto di protezione dei dati sensibili. Proviamo a immaginare cosa succederebbe se un malfattore che ha il nostro indirizzo di posta elettronica entrasse nella nostra casella di posta utilizzando una di queste parole. Statisticamente le possibilità che possa riuscirci ci sono, ma può farlo anche sfruttando altre informazioni che gli italiani utilizzano molto spesso, ovvero il nome del figlio o la sua data di nascita, il nome della moglie, del cane e così via. E dove si trovano tutte queste informazioni? Quasi sempre su Facebook. È lì che pubblichiamo, forse troppo ingenuamente, informazioni personali che possono aiutare eventuali malintenzionati, per non parlare del fatto che una serie di foto provenienti dai nostri luoghi di villeggiatura segnala al mondo che a casa nostra in quel momento non c'è nessuno.

Ma parlavamo di **codici e sicurezza**. Se qualcuno riuscisse ad accedere alla nostra casella mail, potrebbe entrare in possesso di **dati sensibili** nostri, ma non solo. Pensiamo per esempio alle informazioni confidenziali dei nostri clienti, della banca. Insomma un vero disastro. Se stiamo pensando che la nostra password è sicura perché il nome di nostra moglie Irene lo abbiamo scritto in codice alfanumerico, ovvero 1r3n3, stiamo prendendo una cantonata. I malfattori conoscono molto bene questo trucco e ormai non funziona più.

Per essere tranquilli dobbiamo usare **password sicure** composte da **lettere numeri e caratteri speciali** tipo "@" "!" "_" ecc... Inoltre, dovremmo cercare di **non usare lo stesso** codice per tutte le caselle di posta o gli account che apriamo sui vari servizi online. Anche questa rappresenta una cattiva abitudine molto diffusa. Una volta scoperta la password, tutti gli account che la usano diventano vulnerabili. Bisognerebbe poi cambiare spesso la password, magari una volta ogni due o tre mesi, anziché utilizzare la stessa per tutta la vita. Queste precauzioni aumentano notevolmente il nostro livello di sicurezza, ma diventano inutili se nel nostro computer abbiamo un antivirus inefficiente o non aggiornato. Esistono alcuni software maligni, chiamati malware che possono entrare nel computer attraverso un messaggio di posta o facendo clic su quegli avvisi che appaiono sullo schermo mentre stiamo navigando e che magari ci chiedono di misurare le prestazioni del computer o di verificare che sulla nostra

macchina non siano presenti virus.

Tra i software maligni più diffusi ci sono quelli che appartengono alla **categoria dei Trojan**, ovvero cavalli di Troia. Si chiamano così perché una volta installati sul computer aprono la porta ai virus veri e propri e li fanno entrare a nostra insaputa proprio come fece Ulisse a Troia. Tra questi ci sono i keylogger, ovvero dei software che non cancellano i dati o rendono il computer inutilizzabile, fanno un'altra cosa molto semplice. Registrano tutto quello che viene digitato sulla nostra tastiera e lo inviano a colui che li ha creati. Quindi email, codici di accesso e numeri di carte di credito che digitiamo durante un acquisto online vengono immediatamente intercettati.

Ecco perché **un antivirus aggiornato è indispensabile** per non fare entrare programmi dannosi, ma la nostra attenzione è fondamentale per non rendere vano il suo lavoro e dormire tranquilli.