

Sophos, 10 regole anti cyber-crime

La società che produce sistemi anti-intrusione lancia il suo "decalogo" di protezione

Il malware viaggia nella Rete al ritmo di una pagina web infetta ogni 14 secondi. SophosLabs, la rete mondiale dei centri di monitoraggio Sophos dislocati in tutto il mondo, identifica oltre 15.000 nuove pagine web virali al giorno e una e-mail infetta in media ogni 25.000. Solo un sito infetto su 5 è stato realizzato dagli hacker per attirare ignari utenti, il restante è rappresentato da siti autentici contagiati.

Considerando che la cyber-criminalità sta diventando sempre più insidiosa anche da un punto di vista finanziario, Sophos, società leader a livello mondiale nel settore della sicurezza informatica e nella tecnologia di controllo dell'accesso alla rete (NAC), ha stilato un decalogo di regole di sicurezza IT.

Usare un software antivirus e tenerlo sempre aggiornato.

È importante disporre di un sistema in grado di aggiornare tutti i computer regolarmente e tempestivamente.

Non effettuare mai acquisti suggeriti da e-mail non richieste

Il pericolo è di vedere inserito il proprio indirizzo e-mail nelle liste che vengono vendute agli spammer.

Usare un client firewall sui computer collegati a Internet

Un client firewall protegge i computer collegati con il mondo esterno.

Non rispondere allo spam e ignorare i link al suo interno

Rispondere ai messaggi spam non fa altro che confermare la validità dell'indirizzo e-mail allo spammer.

Non usare la modalità "anteprima" nel client di posta

L'opzione "anteprima" apre il messaggio e comunica agli spammer che la loro e-mail è andata a buon fine.

Utilizzare indirizzi secondari e fornirli solo a persone fidate

Si consiglia di comunicare l'indirizzo principale solo ad amici e colleghi e di utilizzare gli indirizzi secondari per i moduli web. Non pubblicare mai l'indirizzo principale su forum, newsgroup o altri siti pubblici.

Non rispondere mai ai messaggi che richiedono informazioni finanziarie personali

Diffidate delle e-mail che richiedono di inserire password e dettagli relativi a conti bancari o che includono link per effettuare tali operazioni.

Visitare i siti internet delle banche digitando l'indirizzo nell'apposita barra

Non selezionate i link presenti nei messaggi di posta indesiderata. I "phisher" possono utilizzare questi collegamenti per reindirizzare l'utente su un sito web fantasma.

Non cliccare sui popup

Se appaiono popup inattesi, come quelli che avvertono della presenza di virus sul computer e che offrono una soluzione, non selezionate il link e non autorizzate nessun download. Potreste scaricare e installare software potenzialmente dannosi.

Non salvare le password sul computer o su dispositivi online

Gli hacker potrebbero essere in grado di accedere al vostro computer e trovare le password.

(M.d.A.)

