

Sophos, il decalogo per la sicurezza informatica

Dieci regole di comportamento, utilizzabili da tutti, per limitare i pericoli derivanti dalla Rete.

Il malware viaggia in Internet al ritmo di una pagina web infetta ogni 14 secondi. Secondo Sophos, solo un sito infetto su cinque è stato realizzato dagli hacker per attirare ignari utenti, il resto sono siti autentici contagiati. Per aiutare gli utenti, la società ha stilato un elenco di semplici e pratiche norme di sicurezza per proteggere le reti aziendali.

Usare un software antivirus e tenerlo sempre aggiornato.

È importante disporre di un sistema in grado di aggiornare tutti i computer regolarmente e tempestivamente: il nuovo malware può diffondersi con estrema rapidità. Inoltre, vanno installate regolarmente le patch del sistema operativo utilizzato, in modo da poter chiudere eventuali vulnerabilità che possono esporre il Pc al pericolo di attacchi virali.

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, con il duplice svantaggio di ricevere ulteriore e-mail spazzatura e di aumentare il rischio di finire vittime di frodi.

Usare un client firewall sui computer collegati a Internet.

Un client firewall protegge i computer collegati con il mondo esterno, ecco perché anche chi utilizza un portatile e/o lavora da casa ha bisogno di una protezione firewall.

Non rispondere allo spam e ignorare i link al suo interno.

Rispondere ai messaggi spam, anche semplicemente per cancellare l'abbonamento alla mailing list, non fa altro che confermare la validità dell'indirizzo e-mail allo spammer, che spedisce una maggiore quantità di messaggi.

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. Quando si controlla la posta è possibile capire, anche solo in base all'oggetto e al mittente, se si tratta di un messaggio spazzatura.

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; gli spammer potrebbero facilmente intercettarli con l'utilizzo di programmi che navigano in internet alla ricerca di indirizzi e-mail.

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. Le banche e le società di e-commerce di solito non spediscono messaggi di questo genere.

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. Meglio digitare l'indirizzo del sito nell'apposita barra per navigare all'interno della pagina autentica.

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 on-line.

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