

Un decalogo contro il phishing

Come combattere le frodi online

SonicWall, società specializzata nelle soluzioni per la sicurezza, ha pubblicato una nuova serie di linee guida volte ad aiutare gli utenti a evitare le frodi online durante il periodo festivo. I dati forniti dalla società indicano che il volume di spam, il principale meccanismo di attuazione di minacce alla sicurezza e truffe, è triplicato nel corso del 2006. Sebbene stia aumentando la consapevolezza del pubblico dell'esistenza del phishing, il rischio per i consumatori continua ad essere elevato. Un recente sondaggio condotto dal gruppo Gartner indica che il guadagno medio ottenuto con truffe perpetrate dai phisher è cresciuto di circa cinque volte, passando da 257 dollari a vittima lo scorso anno a 1.244 dollari nel 2006.

Il decalogo

1) Se non siete clienti dell'azienda che sembra inviarvi un messaggio, ignoratelo.

2) Anche nel caso siate clienti dell'azienda, non rispondete mai direttamente alla richiesta di informazioni finanziarie o personali contenuta nel messaggio di e-mail ricevuto dall'azienda, soprattutto se vi viene richiesto il numero di previdenza sociale. Piuttosto verificate l'autenticità della richiesta inviando un messaggio ad un indirizzo di posta elettronica che sapete essere valido oppure telefonando a una persona che conoscete all'interno dell'azienda.

3) Non collegatevi mai a un sito Web attraverso un link contenuto nel messaggio e-mail. Aprite invece un'altra finestra del browser e digitatevi direttamente l'indirizzo del sito che sapete essere legittimo.

4) Diffidate dei messaggi e-mail che chiedono una risposta immediata. La maggior parte delle frodi di tipo phishing hanno successo perché creano un falso senso di urgenza.

5) Controllate l'estratto conto della carta di credito e del conto bancario immediatamente dopo averlo ricevuto. Cercate di individuare costi o transazioni anche di piccola entità, ma inaspettate. I cybercriminali spesso, prima di prelevare cifre di grossa entità, testano le vittime prescelte prelevando un importo che può passare inosservato.

6) Se ritenete di aver fornito involontariamente dati sensibili a un potenziale truffatore, contattate immediatamente la vostra banca o azienda di credito segnalando che potreste essere a rischio. Collaboreranno con voi per evitare che le informazioni fornite possano danneggiarvi.

7) Fate attenzione alle copie identiche. Molti siti Web indesiderati si basano sulla mistificazione di Url comuni per attirare vittime ignare. Questi siti sono covi ad alto rischio che nascondono minacce quali keystroke logger, spyware e spam.

8) Non scaricate allegati di messaggi e-mail a meno che non siate assolutamente certi della loro provenienza.

9) Prendete confidenza con i trucchi adottati in modo da individuare i messaggi fraudolenti. Utilizzate il test gratuito di SonicWall "Phishing IQ test" (<http://www.sonicwall.com/phishing/>) e imparate dall'analisi dei risultati come distinguere un attacco di tipo phishing da un messaggio legittimo. Oppure ascoltate le registrazioni in digitale "Phishing Patrol" collegandovi al sito Web <http://www.sonicwall.com/alert/>. Si tratta di sei brevi tutorial che forniscono suggerimenti pratici su cosa può fare l'utente per proteggersi.

10) Non dimenticate che l'aggiornamento costante è essenziale. Assicuratevi che il sistema operativo e gli applicativi software di sicurezza, come anti-spam, anti-phishing, anti-virus e antispyware, siano aggiornati.

Virtual snc

di Fiorelli Daniele e Quacquarelli Luca

Tel./fax 075 8044288

www.assisivirtual.it