

TECHNOLOGY & YOU

Come sfuggire al furto della privacy

Si moltiplicano i programmi per combattere il fenomeno del phishing. Non sempre efficienti

Le motivazioni di chi scrive virus e lancia attacchi ai computer sono oscure. Ma l'obiettivo dei phisher, che cercano di attirare gli utenti su finti siti per rubare password e altre informazioni sui loro conti, è chiaro: il puro e semplice furto. Questi dati li ottengono principalmente ingannando le loro vittime ignare, piuttosto che sfruttando dei buchi nei software. Ciò spiega perché il phishing prolifera. Ed è la ragione per cui è giunto il momento di affrontare il problema alla radice: l'inadeguatezza delle password. Per i siti web dove il danno economico potenziale è grande, come i siti di e-banking, una password da sola, non importa quanto ben costruita, è diventata troppo pericolosa. Il problema, ammesso che siate la stessa persona che dichiarate quando siete online, è l'autenticazione. Anche la password più solida può essere rubata con il phishing. Dunque per una vera sicurezza, le password dovrebbero avere a complemento qualche altro strumento di riconoscimento: biometrico, come un'impronta digitale, o un codice. Nella maggior parte dei casi, quest'ultimo è una password elettronica che cambia a ogni login e che è generata da un apparecchio portatile.

Gli strumenti biometrici funzionano bene nelle reti aziendali, dove la registrazione iniziale può essere condotta di persona, ma diventano problematici per le transazioni che si realizzano esclusivamente online. Gli apparecchi generatori di codici possono avere un più ampio utilizzo. Il più noto è il Securid di Rsa security: assomiglia a un portachiavi elettronico, ma dispone di una piccola finestra che mostra un numero di sei cifre, che cambia ogni minuto. Per entrare in un sistema protetto da Securid, occorre inserire il proprio nome utente, la password e il numero riportato sulla chiave elettronica. Se coincide con il numero che il sistema si attende, si entra. La principale controindicazione di Securid è il costo, sia del portachiavi sia della tecnologia necessaria per mantenere una stretta sincronizzazione temporale tra l'apparecchio e il server che deve concedere l'accesso. Fino a oggi è stato utilizzato soprattutto per l'accesso a conti e servizi aziendali, ma America online ne offre una versione, chiamata Passcode, agli utenti che vogliono una maggiore sicurezza

per le proprie transazioni online. Alcune banche europee hanno cominciato a offrire un'alternativa a più basso contenuto tecnologico. Inviando ai propri clienti una carta o un foglio che contiene una serie di numeri da cancellare, un po' come nei biglietti delle lotterie. Per avviare una transazione, il cliente deve cancellare il numero successivo e inserirlo nel campo di login. Se coincide con il numero atteso dal sistema, il cliente entra. Una volta terminati i numeri della carta, il cliente ne riceve una nuova. Entrust, società canadese, ha trovato una soluzione molto intelligente. Identityguard è una griglia con un numero su ognuna delle cinque righe, una lettera su ognuna delle dieci colonne e un'altra cifra in ogni cella della griglia. Ciò permette di costruire casualmente miliardi di combinazioni con una probabilità prossima allo zero di generarne due uguali. Quando si accede a un sistema protetto con Identityguard, questo chiede all'utente di inserire il proprio nome utente, la propria password e le cifre che compaiono in tre o quattro celle. L'utente cerca le informazioni sulla griglia, e le inserisce per completare il log-in. Se questo sistema è semplice, presenta tuttavia serie limitazioni. Le persone non vorranno portare con sé una diversa carta per ciascuno dei siti web che visitano. Fino a che non disporremo di un sistema di log-in comune, qualcosa di simile al progetto Passport, fallito, di Microsoft, ma con un ampio supporto da parte dell'industria, l'uso di approcci simili a quello di Identityguard sarà limitato a dati sensibili come quelli dei conti bancari o delle cartelle sanitarie.

Alcune istituzioni finanziarie stanno rafforzando i propri sistemi di sicurezza online per proteggere i propri clienti e se stesse. Bank of America, per esempio, ha firmato un contratto con Verisign per sviluppare un sistema complementare alle password, possibilmente un apparecchio a codice, per le transazioni online. Ciò probabilmente renderà un po' meno conveniente fare affari online, ma è un male necessario. Il passo in più richiesto agli utenti sarà una noia molto meno seria che non riparare il danno di un furto di identità.

Stephen H. Wildstrom
(Copyright Business Week)