Proofpoint : Se prÃ©munir contre les attaques ciblÃ©es par mail
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 17/10/2013 15:00:00

Le manque de formation et la curiositÃ© exposent les utilisateurs aux cyberattaques. **Proofpoint**, lâ□□un des principaux prestataires de solutions de sÃ©curitÃ©-service (SaaS), dÃ©voile son initiative Â« **It Only Takes One** Â» pour rappeler aux internautes le risque de cyberattaque pesant sur eux et les rÃ©flexes Ã avoir afin dâ□□Ã©viter ces menaces.

Aujourd'hui, les attaques les plus nuisibles n'arrivent pas par hasard. Soigneusement planifiÃ©es et ciblÃ©es, elles se font dans la plupart des cas par e-mail. Les experts en sÃ©curitÃ© de Proofpoint ont constatÃ© que le nombre d'attaques, notamment par hameÃ§onnage, par manipulation au travers des mÃ©dias sociaux Ã©taient de plus en plus importantes et ciblÃ©es. Selon un sondage en ligne rÃ©alisÃ© par YouGov, moins de la moitiÃ© des salariÃ©s (43 %) qui travaillaient dans un bureau avaient suivi, sur leur lieu de travail actuel, une formation consacrÃ©e Ã la protection des donnÃ©es et de la confidentialitÃ©.

Pour que les salariÃ©s restent vigilants, Proofpoint recommande une approche en cinq points :

1. Ne partagez jamais vos informations personnelles : mÃ©fiez-vous toujours des e-mails vous demandant des codes personnels, des informations financiÃ¨res, des noms d'utilisateur ou des mots de passe.

2. Ne cliquez pas : si vous recevez un e-mail suspect, ne cliquez pas sur les liens qu'il contient et ouvrez les piÃ¨ces jointes provenant uniquement de sources fiables Ã 100 %.

3. Ne remplissez pas les formulaires envoyÃ©s par e-mail : ne remplissez jamais les formulaires se trouvant dans le corps d'un e-mail, en particulier quand des informations personnelles vous sont demandÃ©es. PrÃ©fÃ©rez visiter le site Web de la sociÃ©tÃ© en question.

4. MÃ©fiez-vous des mÃ©dias sociaux : l'e-mail n'est pas le seul moyen employÃ© par les cyber criminels. Les sites de mÃ©dias sociaux tels que Facebook et Twitter sont de plus en plus utilisÃ©s pour envoyer le mÃªme type de canulars et de liens malveillants Ã des utilisateurs qui ne se mÃ©fient pas.

5. Sachez identifier les menaces : soyez capable d'identifier les attaques par e-mail. Soyez prudent face aux adresses e-mail d'expÃ©diteurs inconnus, des objet dâ□□email gÃ©nÃ©riques, des fautes d'orthographe et des demandes inhabituelles.

Selon **Ismet Geri**, Directeur de Proofpoint France, Â« *on estime que 95 % des menaces lancÃ©es par des campagnes de phishing ont abouti. Il s'agit d'e-mails extrÃªmement ciblÃ©s, envoyÃ©s Ã quelques individus seulement, Ã©laborÃ©s avec un objectif prÃ©cis. Une fois que le pirate a fait des recherches sur les destinataires visÃ©s au moyen de sites de mÃ©dias sociaux tels que Facebook et LinkedIn, les e-mails de phishing sont habilement maquillÃ©s en messages lÃ©gitimes envoyÃ©s par des proches, des collÃ¨gues ou des personnes de confiance. Les pirates se servent des principes du marketing direct pour crÃ©er des contenus pertinents.* Â»

Â« *Rien ne rÃ©siste Ã la curiositÃ© humaine. Combinez-la Ã du contenu d'ingÃ©nierie sociale visant Ã soutirer une rÃ©ponse, et vous obtenez une menace potentielle. Si les solutions de sÃ©curitÃ© du rÃ©seau constituent la premiÃ¨re ligne de dÃ©fense d'une entreprise contre les menaces avancÃ©es, ses salariÃ©s reprÃ©sentent collectivement sa derniÃ¨re ligne de dÃ©fense. Avec une formation appropriÃ©e, le personnel d'une sociÃ©tÃ© peut radicalement limiter la propension de celle-ci Ã se retrouver victime d'une attaque ciblÃ©e* Â», **Ismet Geri**.