Les arnaqueurs passionnÃ©s par le footBall, phishing chez les aficionados.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 30/4/2013 15:30:00

Les arnaqueurs ont rÃ©cemment montrÃ© un fort intÃ©rÃªt pour le football. En effet, une grande variÃ©tÃ© dâ□□attaques de phishing (faux sites web) se basant sur le football a Ã©tÃ© observÃ©e en 2012. Les arnaqueurs se sont dÃ©jÃ intÃ©ressÃ©s Ã la Coupe du Monde de la FIFA 2014, mais aussi aux stars et aux clubs phares du ballon rond.

Lâ□□arnaque ciblant les fans de Lionel Messi et celle visant les supporters du FC Barcelone sont de bons exemples de ces pratiques. Les pirates informatiques comprennent quâ□□utiliser des cÃ©lÃ©britÃ©s avec une Ã©norme base de fans offre un plus grand choix de cibles, et augmente ainsi leurs chances de rÃ©colter les identitÃ©s des utilisateurs.

Ces arnaques persistent encore en 2013 avec une stratÃ©gie toujours identique consistant Ã mettre en place de faux sites web en utilisant des hÃ©bergeurs gratuits.

Les sites de phishing ont incitÃ© des internautes Ã entrer leurs codes dâ□□accÃ¨s Facebook sur des pages consacrÃ©es Ã Lionel Messi, au FC Barcelone ou Ã Cristiano Ronaldo. Ces derniÃ¨res affichent ostensiblement des images de Lionel Messi, du FC Barcelone ou de Cristiano Ronaldo, et essaient de donner lâ□□impression quâ□□elles en sont les pages Facebook officielles. Certains de ces faux sites sont intitulÃ©s, Â« premier rÃ©seau social dans le monde Â». Les utilisateurs sont ensuite incitÃ©s Ã entrer leurs identifiants Facebook afin de se connecter Ã leur compte.

Une fois que les identifiants ont Ã©tÃ© renseignÃ©s, les utilisateurs sont redirigÃ©s vers une page communautaire dÃ©diÃ©e Ã **Lionel Messi**, au FC Barcelone, ou Ã **Cristiano Ronaldo** pour crÃ©er lâ□□illusion quâ□□une session lÃ©gitime sâ□□est ouverte.

Si les utilisateurs sont victimes de sites de phishing en ayant entrÃ© leurs identifiants, alors les

pirates ont rÃ©ussi Ã voler leurs donnÃ©es Ã des fins dâ□□usurpation dâ□□identitÃ©.

Pour Ã©viter les attaques de phishing, les internautes sont invitÃ©s Ã suivre les conseils ci-dessous :

ï□§ Faites attention lorsque vous cliquez sur des liens qui semblent trop attractifs, envoyÃ©s par email ou postÃ©s sur les rÃ©seaux sociaux

ï□§ Ne renseignez pas de donnÃ©es personnelles lorsque vous rÃ©pondez Ã un email

ï□§ Nâ□□entrez pas de donnÃ©es personnelles dans un pop-up qui apparaÃ®t dans une page ou Ã lâ□□Ã©cran. Composez plutÃ´t, de faÃ§on manuelle, le site web que vous souhaitez consulter, au lieu de cliquer sur un lien suspect.

ï□§ Assurez-vous que le site web est cryptÃ© avec un certificat SSL en vÃ©rifiant que la mention Â« https Â» soit prÃ©sente dans la barre dâ□□adresse, ou que celle-ci soit de couleur verte lorsque vous entrez des donnÃ©es personnelles ou financiÃ¨res

ï□§ Utilisez des suites de sÃ©curitÃ© comme Norton Internet Security ou Norton 360, qui vous protÃ¨gent contre le phishing et les fraudes sur les rÃ©seaux sociaux

Rapportez les faux sites web, emails ou pages Facebook via phish@fb.com.