

Le phishing (contraction des mots anglais « fishing », en français pêche, et « phreaking », désignant le piratage de lignes téléphoniques), traduit parfois en « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations.

Le phishing repose sur les techniques d'ingénierie sociale en usurpant des identités d'autres personnes (physiques ou entreprise) via l'envoi de mails qui incitent les utilisateurs à fournir des informations sensibles au pirate.

Le but de notre étude est de comprendre les concepts de phishing, ces techniques, et construire un système capable de traquer ce genre de fraude et protéger les utilisateurs.

Le présent mémoire est organisé comme suite :

Dans le premier chapitre qui constitue une introduction à notre travail nous exposons les différentes définitions de concepts, le jargon de ce monde.

Dans le deuxième chapitre nous exposons les différentes techniques du phishing, ainsi que les méthodes utilisées pour contrer ces attaques.

Dans le troisième et dernier chapitre nous adoptons une approche de lutte contre le phishing et nous essayons de la mettre en œuvre, avec la création d'un système capable de différencier des adresses légitimes et des adresses de phishing.

Comme nous avons vu à travers cette étude le phishing est un sérieux danger en ligne, chaque jour en signale des milliers de nouveaux sites de phishing. Les techniques évoluent aussi très vite.

Une vraie guerre où les mesures de contre-attaque restent un pas en arrière car il y a toujours des adresses de phishing qui échappent des filtres quoi que se soit les performances des systèmes ils n'atteindront jamais le maximum.

Pour notre application qui reste un peu simpliste, il y a beaucoup d'améliorations en perspective, comme l'utilisation des techniques anti-spam avec l'intégration de plus d'heuristiques, et prendre en considération le site en lui-même en utilisant différentes méthodes statistiques et probabilistes, et l'intégration du Protocol WHOIS qui peut nous donner des informations sur le domaine et son âge.

Le seul élément clef de ce combat reste l'humain utilisant la machine, il faut réveiller son attention pour assister ces systèmes à identifier ces dangers.