Qu'est-ce que le filoutage (*phishing en anglais*) ?

Le filoutage est une technique utilisée par des personnes malveillantes dans le but d'obtenir des informations confidentielles sur leurs victimes puis de s'en servir. Pour ce faire les fraudeurs contactent leurs victimes sous différents prétextes en usurpant l'identité d'un tiers dans lequel la victime pourrait avoir confiance (par exemple le rectorat, une banque, un site commercial, …). Ces arnaques visent aujourd'hui principalement les clients des sites bancaires, mais il n'est pas rare de constater qu'elles peuvent aussi s'attaquer aux sites institutionnels.

Principe de fonctionnement

Généralement la victime reçoit dans sa messagerie électronique un courriel, semblant provenir d'un organisme de confiance, lui indiquant qu'un problème est survenu sur son compte. Le contenu du mail est vraisemblable, il utilise le logo de l'organisme *(ou de d'une administration)* et invite la victime à cliquer sur le lien contenu dans le courrier afin de résoudre ce soi-disant problème.

Exemple d'un courriel de filoutage envoyé à des clients d'une banque.

Cher client de [redacted]

Le département technique de [redacted] procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.[redacted].net/banque/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

Le lien internet masqué, contenu dans le mail, conduit en fait à un site ressemblant à s'y méprendre au site de la banque ou de l'organisme de confiance. Cette imitation du site a été déposée par une personne malintentionnée sur un autre site internet compromis. Dès qu'une victime saisit des informations personnelles (coordonnées bancaires, identifiants, mots de passe), celles-ci sont immédiatement envoyées à la personne malveillante qui s'empressera de les utiliser pour vider le compte bancaire de sa victime ou pour prendre le contrôle de votre messagerie.

Ces courriers frauduleux ne sont généralement pas ciblés mais envoyés à des milliers d'adresses.

Comment s'en protéger ?

- **Les banques ou les administrations n'envoient jamais ce genre de courriel** : d'une manière générale, une banque ne demandera pas à ses clients de venir saisir leurs informations personnelles dans un courrier électronique. Pour se connecter au site de sa banque, il vaut mieux entrer manuellement l'adresse réticulaire (URL) du site dans votre navigateur.

- **Ne pas cliquer sur les liens contenus dans les courriers électroniques** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux. En cas de doute, il est préférable de saisir manuellement l'adresse dans le navigateur.

- **Être vigilant lorsqu'un courriel demande des actions urgentes**.

- **Ne jamais répondre ou transférer ces courriels**.

- **En cas de doute ou de problème, prendre contact rapidement avec la division informatique.**