



Éviter l'hameçonnage

Contexte

L'hameçonnage (ou phishing) est une tentative d'escroquerie qui vise à obtenir des renseignements personnels et financiers d'internautes, afin de les utiliser pour détourner des fonds.

La manoeuvre consiste à l'envoi de courriels en prétendant faussement représenter une entreprise réputée et de confiance, comme une institution financière, une agence gouvernementale ou une entreprise commerciale reconnue.

Dans le courriel hameçon typique, un message au caractère urgent vous demande de cliquer sur un lien menant vers un site Web qui imite l'apparence d'une institution reconnue, où vous êtes invité à divulguer des renseignements confidentiels sur votre compte bancaire, vos cartes de crédit, etc.

Les pirates informatiques peuvent ensuite utiliser ces renseignements pour contrôler votre compte bancaire, ouvrir de nouveaux comptes, transférer des fonds, obtenir des cartes de crédit ou acheter des biens et services.

Un nouveau type d'hameçonnage est apparu récemment. Un formulaire est déposé dans le courriel, ce qui élimine la nécessité d'un lien vers un site Web frauduleux. Lorsque vous cliquez sur le bouton en bas de la page, après avoir rempli le formulaire, vos données personnelles et financières sont envoyées au fraudeur.

Les signes d'un courriel frauduleux :

- n'est pas personnalisé (nom, numéro de client);
- suscite un sentiment d'urgence (qui incite à une action immédiate et irréfléchie de la part de l'internaute);
- peut contenir des images conformes à la marque de l'institution; est rédigé uniquement en anglais;
- contient souvent des fautes d'orthographe ou des erreurs grammaticales;
- ne provient pas d'une institution qui devrait connaître votre courriel.

Principe

Méfiez-vous des courriels demandant des informations personnelles. Les entreprises sérieuses ne demandent jamais des renseignements importants par le biais d'un simple courrier électronique. Dans le doute, contactez directement votre institution par téléphone.

Règles et bonnes pratiques

- Lorsque vous recevez un message provenant d'une institution bancaire ou d'un site de commerce électronique, posez-vous les questions suivantes :
 - Ai-je communiqué mon adresse de messagerie à cette institution ?
 - Ce courriel possède-t-il des éléments permettant de vérifier sa véracité (numéro de client, nom de l'agence, etc.) ?
- Vérifiez l'adresse de l'expéditeur du courriel, par l'envoi d'un message demandant des précisions.
- Évitez de cliquer sur des liens à l'intérieur d'un courriel provenant d'inconnus. Ouvrez plutôt votre navigateur et saisissez l'URL d'accès au service.
- Lors de la visite d'un site, portez une attention particulière à l'adresse Web : le nom de domaine doit correspondre à celui annoncé. Examinez-en minutieusement l'orthographe.
- Ne pas communiquer de renseignements personnels si le site Web n'est pas en mode sécurisé : l'adresse de la barre du navigateur doit débuter par « https:// » et la barre d'état au bas de votre navigateur doit contenir un cadenas.
- Tenez-vous au courant des nouvelles technologies préventives. Netcraft et Microsoft ont développé des barres d'outils pour enrayer l'hameçonnage.
- Si vous croyez avoir fourni des renseignements personnels ou financiers à des fraudeurs, communiquez avec votre banque ou votre compagnie de carte de crédit. Vous devriez également signaler le cas au service de police de votre municipalité et à des organismes de signalement de délit (Recol et PhoneBusters).

Dernière mise à jour : **9 mai 2007**