Club informatique

Homeçonnage – 10 février 2022
Présentateur : Michel Gagné

Contenu de la séance

Sécurité informatique

- L'hameçonnage
    - L'hameçonnage par courriel
    - Les autres formes d'hameçonnage
- La vérification du domaine avant la saisie d'un mot de passe

L'hameçonnage

Définition

L'hameçonnage est l'envoi d'un message piégé par un pirate informatique dans le but de vous faire faire une action qui aura des conséquences négatives pour vous. Dans le cas des virus, c'est le virus qui fait une action malveillante comme détruire vos données ou transmettre vos informations personnelles à un pirate. Dans le cas d'un hameçonnage, le pirate vous utilise et c'est vous qui faites une action qui aura des répercussions négatives pour vous.

L'hameçonnage peut se faire par courriel ou à travers un autre outil de communication comme le téléphone, Skype, un réseau social, un site de rencontre, etc.

L'hameçonnage par courriel – le vol d'identité

Description

Les pirates s'intéressent principalement à deux types d'identité :

- l'identité des comptes de courrier électronique (c'est-à-dire, l'adresse électronique et le mot de passe associé)
- l'identité des comptes où on manipule de l'argent (c'est-à-dire, l'identifiant et le mot de passe de comptes comme les comptes de Desjardins, de la Banque de Montréal, d'une autre banque, des cartes de crédit, de PayPal, d'Apple, etc.).

Une attaque typique se produit comme suit : un pirate, simulant un courriel provenant d'un fournisseur de courrier électronique ou d'une institution financière, prétend qu'il y a un problème avec votre compte et vous demande des informations personnelles comme un identifiant et un mot de passe pour corriger le problème. Souvent, le courriel contient un lien menant à une page semblable à la page de connexion du fournisseur de courrier électronique ou de l'institution financière, mais contrôlée par le pirate. L'internaute inexpérimenté peut penser qu'il est en contact avec son fournisseur habituel et il fournit l'information demandée. Malheureusement, ce n'est pas à son fournisseur qu'il fournit l'information, mais au pirate.

Moyens de se protéger

Il faut apprendre à reconnaître les courriels de vol d'identité. Voici quelques trucs qui vous permettront de les reconnaître :

- les courriels écrits en mauvais français ou contenant de fautes de français proviennent toujours de pirates informatiques; jamais une compagnie sérieuse ne vous enverra de tels courriels, mais attention il y a maintenant des courriels d'hameçonge qui sont écrits dans un très bon français;
- certains courriels mentionnent des problèmes avec votre compte, puis vous demandent de fournir certaines informations pour corriger le problème (cliquez **ici** pour voir un exemple)
- d'autres courriels contiennent un lien menant à une page identique à une page de la compagnie dont ils usurpent l'identité; voici un exemple en trois étapes :
    - cliquez **ici** pour voir un courriel envoyé par le fraudeur; ce courriel contient une confirmation de commande que le destinataire n'a pas faite; comme le destinataire est intrigué par cette commande et qu'il ne veut pas payer pour une commande qu'il n'a pas faite, il aura tendance à cliquer sur le courriel pour avoir des informations supplémentaires;
    - cliquez **ici** pour voir la page obtenue en cliquant sur le courriel précédent, cette page demande un identifiant Apple;
    - cliquez **ici** pour voir la page obtenue après avoir fourni l'identifiant Apple, cette page demande le mot de passe du compte Apple; si l'internaute fournir son mot de passe, c'est au pirate qu'il donne le mot de passe;
- le nom de domaine de l'expéditeur du courriel ne contient pas le nom de la compagnie dont l'identité est usurpée (cliquez **ici** pour voir un courriel provenant d'un fraudeur qui simule un courriel de la compagnie Apple; notez que l'adresse électronique de l'expéditeur se termine par **@aspeaxselr.net**, une adresse de Apple se terminerait par **@apple.com**);
- l'adresse de la page demandant des informations personnelles n'appartient pas au domaine de la compagnie dont l'identité est usurpée (cliquez **ici** pour voir une page d'un pirate simulant une page de la compagnie Apple et demandant un mot de passe; notez que le domaine de la page est **pagopagomanago.com**, le domaine d'une page de Apple serait **apple.com**);
- le courriel mentionne souvent qu'une action urgente est requise dans le but de vous énerver et de vous amener à agir sans confirmer la véracité du courriel.

N'accédez jamais sur un site sur lequel vous faites des transactions financières en cliquant sur un lien; entrez plutôt vous-même l'adresse du site désiré sur la barre d'adresse.

N'entrez jamais un mot de passe sur un site de courrier électronique ou un site de transactions financières sans vérifier le domaine apparaissant sur la barre d'adresses.

Vérifiez vos relevés pour identifier rapidement des transactions frauduleuses.

Comment réagir à un vol d'identité

Si vous croyez être tombé dans un piège de vol de mot de passe d'une institution financière, appelez l'institution financière dont l'identité a été simulée par le pirate et demandez-lui de l'aide.

Si vous croyez être tombé dans un piège de vol de mot de passe de courrier électronique, changez votre mot de passe.

L’hameçonnage par courriel – le transfert d’argent

Description

Dans un courriel, un fraudeur affirme posséder une importante somme d'argent (souvent plusieurs millions de dollars provenant d’un héritage, de pots-de-vin, de comptes tombés en déshérence, de fonds à placer à l'étranger à la suite d'un changement de contexte politique, etc.) et fait part de son besoin d'utiliser un compte existant pour transférer rapidement cet argent hors de son pays.

Le fraudeur demande de l'aide pour effectuer ce transfert d'argent, en échange de quoi il offre un pourcentage sur la somme qui sera transférée. Si la victime accepte, le fraudeur lui demandera petit à petit d’avancer des sommes d’argent destinées à couvrir des frais imaginaires (notaires, entreprises de sécurité, pots-de-vin…) avant que le transfert ne soit effectué. Même si la victime fournit les sommes demandées, le transfert n’aura évidemment jamais lieu.

Cliquez **ici** pour voir un exemple de courriel proposant un transfert d’argent.

Moyens de se protéger

Ne répondez jamais à des courriels vous proposant de vous impliquer dans des transferts d’argent.

L’hameçonnage par courriel – les loteries et les cadeaux

Description

Un fraudeur indique que le destinataire a gagné un prix à une loterie ou a mérité un cadeau. Pour recevoir son prix ou son cadeau, le destinataire doit contacter un agent qui lui demande de payer des frais avant de recevoir le prix ou le cadeau. Les frais sont présentés comme des frais d'administration, des taxes, des frais de douanes ou d'autres frais qui peuvent sembler légitimes. Le fraudeur demande aussi parfois des informations personnelles lors des communications. Pour appliquer de la pression sur le destinataire, le fraudeur indique parfois que le destinataire doit répondre en moins de 5 minutes après avoir ouvert le message ou lui dit qu'il gagnera un second prix s'il répond rapidement.

Cliquez **ici** pour voir un exemple d’hameçonnage à travers une offre de cadeau.

Moyens de se protéger

Ne répondez jamais à des courriels indiquant que

- vous avez gagné un prix à un concours auquel vous n’avez pas participé;
- vous avez mérité un cadeau.

Ne payez jamais de frais pour recevoir un prix ou un cadeau. Ne fournissez jamais d’informations personnelles pour recevoir un prix ou un cadeau.

L’hameçonnage par courriel – les offres de produits

Description

Un fraudeur offre des produits pharmaceutiques connus (Viagra ou Cialis), des produits miracles (par exemple, pour maigrir) ou d’autres produits attrayants. Ces produits sont souvent contrefaits ou d’efficacité douteuse.

Cliquez **ici** pour voir un exemple de courriel offrant un produit miracle.

Moyens de se protéger

Achetez seulement des produits de compagnies de confiance. N'achetez jamais des produits de compagnies qui vous contactent. Achetez des produits de compagnies que vous connaissez et que vous contactez vous-mêmes. Dans le domaine de la santé, ne faites confiance qu'à votre médecin ou à des professionnels reconnus qui sont régis par un ordre professionnel.

L'hameçonnage par courriel – les sondages

Description

Un fraudeur vous invite à répondre à un sondage en vous promettant un prix si vous le faites. Après avoir posé quelques questions pour simuler un sondage, le fraudeur demande des informations personnelles pour vous faire parvenir votre prix, ou il demande de payer des frais (comme des taxes ou des frais de manutention) avant d'envoyer le prix, ou il tente d'infecter l'ordinateur du destinataire au cours du sondage.

Cliquez **ici** pour voir un exemple de faux sondage. Notez que l'adresse de l'expéditeur se termine par **@fitfarms.co.uk** alors que l'adresse d'un message provenant de Samsung se terminerait par **@samsung.com**.

Cliquez **ici** pour voir un autre exemple de faux sondage. Notez que l'adresse de l'expéditeur se termine par **@hfdrfd9875802.itchware.org.uk** alors que l'adresse d'un message provenant d'Air Canada se terminerait par **@aircanada.ca**.

Moyens de se protéger

Ne répondez jamais à des sondages si vous n'êtes pas certain de la provenance du sondage. Ne payez jamais de frais pour recevoir un prix. Ne fournissez jamais d'informations personnelles en répondant à un sondage.

Les autres formes d'hameçonnage – les appels téléphoniques de techniciens

Description

Un fraudeur affirmant travailler pour Microsoft (ou une autre compagnie informatique connue) prétend que votre ordinateur est infecté et offre de vous aider.

Comment prévenir des problèmes

Une personne qui vous appelle et qui indique que votre ordinateur est infecté est toujours un pirate. Raccrochez dès que vous reconnaissez un tel appel.

Comment réagir à une demande d'argent

Si vous poursuivez l'appel et faites ce que le pirate propose, le pirate contaminera votre ordinateur, puis il vous dira que vous devez acheter une application pour le nettoyer. Si vous êtes rendu à cette étape, n'achetez pas l'application. Une personne expérimentée, un instructeur du club informatique, ou une boutique informatique pourra restaurer votre ordinateur et vos données… si vous avez une sauvegarde récente.

Les autres formes d'hameçonnage – les autres offres d'aides techniques

Description

Cet hameçonnage est semblable à l'hameçonnage par téléphone, sauf qu'il vient par Internet. Par exemple, un courriel ou un message sur Internet peut vous proposer d'accélérer votre ordinateur, de corriger des problèmes sur votre ordinateur ou de mettre à jour vos pilotes.

Comment prévenir des problèmes

Ignorez tous les messages vous proposant de l'aide pour améliorer les performances de votre ordinateur. Tous ces messages sont frauduleux ou, au minimum, inefficaces.

Ne faites jamais affaire avec des personnes qui vous contactent, car vous ne pouvez vérifier leur identité. Faites uniquement affaire avec des personnes que vous contactez et contactez uniquement des personnes de confiance (pas des personnes ou des compagnies trouvées au moyen de recherches sur Internet).

Les autres formes d'hameçonnage – l'arnaque amoureuse

Description

Le fraudeur communique avec une cible à travers Facebook, Skype, un site de rencontres ou un autre moyen. Ensuite, il établit patiemment une relation de confiance avec la victime, possiblement une relation amoureuse. Lorsque la victime est bien accrochée, il propose de rencontrer la victime ou il prétend avoir besoin d'argent et il commence à soutirer de l'argent à la victime.

Prévention

N'acceptez pas de communications de personnes inconnues et, si vous le faites, ne vous attachez pas à un inconnu et surtout ne lui envoyez jamais d'argent.

Comment réagir à une fraude

Avisez la police.

Les autres formes d'hameçonnage – la complicité… suivie du chantage

Description

C'est une arnaque particulièrement humiliante. Comme dans le cas précédent, le fraudeur communique avec une cible à travers Facebook, Skype, un site de rencontres ou un autre moyen. Après avoir établi une relation de confiance avec la victime, il lui propose de jouer à des jeux sexuels en ligne. Lors de ces jeux sexuels, il filme la victime, puis la menace de mettre les vidéos en ligne ou de les envoyer aux proches et aux amis de la victime si la victime ne paie pas une rançon.

Prévention

N'acceptez pas de communications de personnes inconnues et, si vous le faites, ne jouez pas à des jeux sexuels avec des inconnus sur Internet.

Comment réagir à une fraude

Avisez la police.

Les autres formes d'hameçonnage – les demandes de rançon

Description

- Un message affirmant provenir du FBI ou de la Gendarmerie royale du Canada indique que vous avez enfreint des droits d'auteur et que vous devez payer une amende de 250 $ sinon vous serez poursuivi en justice et vous risquez une amende plus élevée et une peine de prison.
- Ou un message prétend que vous avez visité des sites pornographiques ou que vous avez des images pornographiques sur votre ordinateur et que cette information sera révélée à la police et aux personnes apparaissant dans votre carnet d'adresses si vous ne payez pas une rançon.

Comment se protéger

Ignorez ces messages. N'engagez pas la conversation avec les expéditeurs.

Ne payez jamais une rançon. Si vous ne pouvez vous débarrasser du message demandant la rançon, faites une restauration de l'ordinateur à une date antérieure (si vous ne savez pas comment le faire, une personne expérimentée, un instructeur du club informatique ou une boutique informatique peut vous venir en aide).

La vérification du domaine avant la saisie d'un mot de passe

Un mot de passe est une information personnelle très importante. Avant la saisie d'un mot de passe, surtout sur un compte de courrier électronique ou sur un site où vous gérez de l'argent, il faut toujours vérifier sur la barre d'adresses que vous êtes vraiment sur le site de l'entreprise avec laquelle vous voulez communiquer.

Cliquez **ici** pour voir une page du site de Desjardins demandant mon mot de passe. Les mots **desjardins.com** avant la première barre oblique sur la barre d'adresses m'assurent que je suis bien sur le site de Desjardins.

Cliquez **ici** pour voir une page du site d'Outlook.com demandant mon mot de passe. Les mots **live.com** avant la première barre oblique sur la barre d'adresses m'assurent que je suis bien sur le site d'Outlook.com.